i-generation - 機能追加 #606
アクセスログ解析ツールelasticsearch+kibana導入

2015/12/16 00:29 - 山本 義治

ステータス:	新規	**開始日:**	2015/12/16
優先度:	通常	**期日:**	
担当者:	山本 義治	**進捗 %:**	0%
カテゴリ:	システム全般	**予定工数:**	0.00時間
対象バージョン:		**作業時間の記録:**	0.00時間

説明

履歴

#1 - 2015/12/16 03:05 - 山本 義治

[49.212.214.23]

host名変更

[root@haloo src]# vi /etc/hosts

```
127.0.0.1   localhost admin.i-generation.jp localhost4 localhost4.localdomain4
::1         localhost admin.i-generation.jp localhost6 localhost6.localdomain6
```

[root@haloo src]# vi /etc/sysconfig/network

```
NETWORKING=yes
HOSTNAME=admin.i-generation.jp
```

[root@haloo src]# hostname admin.i-generation.jp

fluentdインストール

[root@haloo admin]# curl -L http://toolbelt.treasure-data.com/sh/install-redhat.sh ¦ sh
[root@haloo src]# vi /etc/td-agent/td-agent.conf

```
<source>
  type forward
  port 24224
</source>

<match apache.**>
  type copy

  <store>
    type stdout
  </store>

  <store>
    type elasticsearch
    host localhost
    port 9200
    type_name access_log
    logstash_format true
    logstash_prefix apache_access
    logstash_dateformat %Y%m
  </store>

 </match>
```

[root@haloo src]# /etc/init.d/td-agent start

elasticsearch pluginインストール

[root@haloo admin]# /usr/lib64/fluent/ruby/bin/fluent-gem install fluent-plugin-elasticsearch

javaインストール

[root@haloo admin]# yum install java-1.8.0-openjdk-devel

[root@haloo admin]# rpm --import http://packages.elasticsearch.org/GPG-KEY-elasticsearch
[root@haloo admin]# vi /etc/yum.repos.d/elasticsearch.repo

```
[elasticsearch-1.4]
name=Elasticsearch repository for 1.4.x packages
baseurl=http://packages.elasticsearch.org/elasticsearch/1.4/centos
gpgcheck=1
gpgkey=http://packages.elasticsearch.org/GPG-KEY-elasticsearch
enabled=1
```

elasticsearchインストール

[root@haloo admin]# yum install elasticsearch
[root@haloo src]# vi /etc/elasticsearch/elasticsearch.yml

```
http.cors.allow-origin: "*"
http.cors.enabled: true
```

[root@haloo admin]# chkconfig --add elasticsearch
[root@haloo admin]# chkconfig elasticsearch on
[root@haloo admin]# chkconfig --list ¦ grep elasticsearch

```
elasticsearch      0:off    1:off    2:on    3:on    4:on    5:on    6:off
```

[root@haloo admin]# service elasticsearch start

```
Starting elasticsearch:                    [  OK  ]
```

[root@haloo admin]# service elasticsearch status

```
elasticsearch (pid  27105) is running...
```

[root@haloo admin]# curl 127.0.0.1:9200

```
{
  "status" : 200,
  "name" : "Protector",
  "cluster_name" : "elasticsearch",
  "version" : {
    "number" : "1.4.5",
    "build_hash" : "2aaf797f2a571dcb779a3b61180afe8390ab61f9",
    "build_timestamp" : "2015-04-27T08:06:06Z",
    "build_snapshot" : false,
    "lucene_version" : "4.10.4"
  },
  "tagline" : "You Know, for Search"
}
```

[root@haloo admin]# tail /var/log/elasticsearch/elasticsearch.log

```
    at java.net.InetAddress.getLocalHost(InetAddress.java:1500)
    ... 29 more
[2015-12-16 01:31:56,036][INFO ][node                ] [Protector] initialized
[2015-12-16 01:31:56,036][INFO ][node                ] [Protector] starting ...
[2015-12-16 01:31:56,128][INFO ][transport           ] [Protector] bound_address {inet[/0:0:0:0:0:0:0:0:9300]}, publish_address
{inet[/49.212.214.23:9300]}
[2015-12-16 01:31:56,150][INFO ][discovery           ] [Protector] elasticsearch/TJ4WW2fST0C_5IHYAJVb5A
[2015-12-16 01:31:59,927][INFO ][cluster.service     ] [Protector] new_master
[Protector][TJ4WW2fST0C_5IHYAJVb5A][localhost][inet[/49.212.214.23:9300]], reason: zen-disco-join (elected_as_master)
[2015-12-16 01:32:00,026][INFO ][http                ] [Protector] bound_address {inet[/0:0:0:0:0:0:0:0:9200]}, publish_address
{inet[/49.212.214.23:9200]}
```

[2015-12-16 01:32:00,027][INFO][node] [Protector] started
[2015-12-16 01:32:00,047][INFO][gateway] [Protector] recovered [0] indices into cluster_state

kinabaインストール

[root@haloo src]# wget https://download.elasticsearch.org/kibana/kibana/kibana-3.1.0.tar.gz
[root@haloo src]# tar zxvf kibana-3.1.0.tar.gz
[root@haloo src]# mkdir -p /var/www/i-generation/www/
[root@haloo src]# mv kibana-3.1.0 /var/www/i-generation/www/kibana
[root@haloo src]# vi /etc/httpd/conf/httpd.conf
[root@haloo src]# vi /var/www/i-generation/www/kibana/config.js

elasticsearch: "http://localhost:9200",

[root@haloo src]# /etc/init.d/httpd restart

[web2.i-generation.jp]

ファイルディスクリプタリミット、カーネルパラメータ調整

[root@web2 admin]# ulimit -n

1024

[root@web2 admin]# vi /etc/security/limits.conf

root soft nofile 65536
root hard nofile 65536
* soft nofile 65536
* hard nofile 65536

[root@web2 admin]# vi /etc/sysctl.conf

net.ipv4.tcp_tw_recycle = 1
net.ipv4.tcp_tw_reuse = 1
net.ipv4.ip_local_port_range = 10240 65535

[root@web2 admin]# /sbin/sysctl -p

net.ipv4.ip_forward = 0
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
kernel.sysrq = 0
kernel.core_uses_pid = 1
net.ipv4.tcp_syncookies = 1
kernel.msgmnb = 65536
kernel.msgmax = 65536
kernel.shmmax = 68719476736
kernel.shmall = 4294967296
net.ipv4.tcp_tw_recycle = 1
net.ipv4.tcp_tw_reuse = 1
net.ipv4.ip_local_port_range = 10240 65535

fluentdインストール

[root@web2 admin]# curl -L http://toolbelt.treasuredata.com/sh/install-redhat.sh ¦ sh

エラー: https://packages.treasuredata.com/GPG-KEY-td-agent: インポート読み込みに失敗しました(-1)。

firewallで許可していないためssl通信拒否される

参考URL

http://qiita.com/murachi1208/items/73ca933fb3dc4457b224

#2 - 2015/12/16 04:11 - 山本 義治

[root@web2 admin]# wget https://packages.treasuredata.com/GPG-KEY-td-agent
--2015-12-16 03:23:29-- https://packages.treasuredata.com/GPG-KEY-td-agent
packages.treasuredata.com をDNSに問いあわせています... 54.230.109.7, 54.230.109.244, 54.230.109.55, ...
packages.treasuredata.com¦54.230.109.7¦:443 に接続しています... 接続しました。
OpenSSL: error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure
SSL による接続が確立できません。

[root@web1 admin]# wget https://packages.treasuredata.com/GPG-KEY-td-agent
--2015-12-16 03:50:21-- https://packages.treasuredata.com/GPG-KEY-td-agent
packages.treasuredata.com をDNSに問いあわせています... 54.230.109.131, 54.230.109.88, 54.230.109.244, ...
packages.treasuredata.com¦54.230.109.131¦:443 に接続しています... 接続しました。
OpenSSL: error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure
SSL による接続が確立できません

#3 - 2015/12/16 04:15 - 山本 義治

firewallの設定で解決できなければ
rsyncでcronでアクセスログを転送する方向で...

#4 - 2015/12/16 19:41 - 山本 義治

[49.212.176.26]

garollでテスト

[root@www14012uf logs]# curl -L http://toolbelt.treasuredata.com/sh/install-redhat.sh ¦ sh
[root@www14012uf logs]# vi /etc/td-agent/td-agent.conf

```
<source>
  type tail
  path /etc/httpd/logs/garoll.net-access_log
  tag apache.combined
  pos_file /var/log/td-agent/httpd-access.log.pos
  format apache2
</source>

<match apache.**>
  type copy

  <store>
    type stdout
  </store>

  <store>
    type forward
    buffer_chunk_limit 256m
```

```
    buffer_queue_limit 128
    flush_interval 5s
    <server>
      host 49.212.214.23
      port 24224
    </server>
  </store>
</match>
```

```
[root@www14012uf logs]# /etc/init.d/td-agent start
[root@www14012uf logs]# tail -f /var/log/td-agent/td-agent.log

    2015-12-16 19:16:02 +0900 [error]: Permission denied - /etc/httpd/logs/garoll.net-access_log
    ...
```

パーミッション変更

```
[root@www14012uf logs]# vi /etc/init.d/td-agent

    - DAEMON_ARGS=${DAEMON_ARGS---user td-agent}
    + DAEMON_ARGS=${DAEMON_ARGS---user root}
```

```
[root@www14012uf logs]# /etc/init.d/td-agent restart
[root@www14012uf logs]# tail -f /var/log/td-agent/td-agent.log

    2015-12-16 19:18:39 +0900 [info]: adding source type="tail"
    2015-12-16 19:18:39 +0900 [info]: adding match pattern="apache.**" type="copy"
    2015-12-16 19:18:39 +0900 [info]: adding forwarding server '49.212.214.23:24224' host="49.212.214.23" port=24224 weight=60
    2015-12-16 19:18:39 +0900 [info]: following tail of /etc/httpd/logs/garoll.net-access_log
    2015-12-16 19:18:41 +0900 apache.combined:
    {"host":"136.243.36.97","user":null,"method":"GET","path":"/entry/529448","code":200,"size":29532,"referer":null,"agent":"Mozilla/5.0
    (compatible; BLEXBot/1.0; +http://webmeup-crawler.com/)"}
    2015-12-16 19:18:39 +0900 apache.combined:
    {"host":"66.249.66.127","user":null,"method":"GET","path":"/tag/Internet%20Explorer","code":200,"size":31721,"referer":null,"agent":"Mozilla/
    5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"}
    ...
```

#5 - 2015/12/16 19:45 - 山本 義治

http://49.212.214.23/kibana/index.html#/dashboard/file/guided.json

#6 - 2015/12/16 20:53 - 山本 義治

http://www.slideshare.net/Satully/elasticsearch8-elasticsearchkibana-30reqday?related=1

＜取得したい項目＞

・クリック、コンバージョン、退会、リタゲのリクエスト数時系列ヒストグラム
・レスポンスタイムの時系列ヒストグラム