Bui Hoang Phuc

Elasticsearch, Fluentd, and Kibana: Open Source Log Search and Visualization

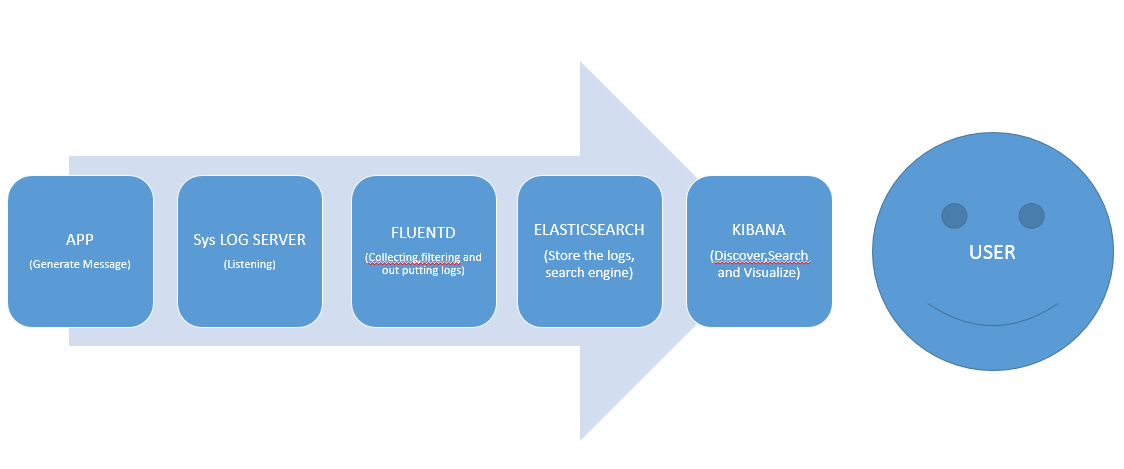
Requirement

Have a sample program logging random messages and emitting them over syslog. (Use a Log4J syslog appender).

Have fluentD in the picture to process those syslog messages and push it to an ElasticSearch instance.

See the messages in Kibana.

Workflow



Prerequisites

**Ubuntu 12.04.4 LTS (precise)**

**User with [sudo](https://www.digitalocean.com/community/tutorials/how-to-add-and-delete-users-on-an-ubuntu-14-04-vps) privileges**

**Need to download some sources: elasticsearch-2.3.3, fluent-plugin-elasticsearch-master, kibana-4.5.1-linux-x64.**

**OpenJDK-7**

Installing and Configuring Elasticsearch

After download elasticsearch-2.3.3, you need to extract to a folder “**elasticsearch-2.3.3**”.

1. Configure host and port for elasticSearch at **“elasticSearch-2.3.3/config/elasticsearch.yml”** (we can use default localhost:9200)
2. Go to folder “elasticSearch-2.3.3/bin”, execute file elasticsearch to start up:

**./elasticsearch**

Installing and Configuring Kibana

After download **kibana-4.5.1-linux-x64**, you need to extract it to a folder “**kibana-4.5.1-linux-x64**”.

1. Configure host/port for Kibana at “**kibana-4.5.1-linux-x64/config/kibana.yml**”

In this step, we can change the host ip and keep default port.

1. Run Kibana from the install directory**: bin ./kibana**

## Installing and Configuring Fluentd

Before installing Fluentd, we should do a preparation, refer to: <http://docs.fluentd.org/articles/before-install>

In fact, we have a shell script to install fluentd automatically, refer to: <http://docs.fluentd.org/v0.12/articles/install-by-deb>

but because I have a problem with my server when installing by that script so I have installed base on Ruby Gem

and the steps which I installed as below:

1. First, we need install ruby:

Download and extract source ruby 2.0.0

Install:

- Cd to folder of ruby and run file and command:

**./configure**

**make**

**sudo make install**

1. Next you need install rubygem:

Download and extract source ruby gem 2.6.4

Cd to folder of ruby gem 2.6.4 and run command:

**Sudo** **ruby setup.rb**

# Installing Fluentd

Install Fluentd with the following command.

**sudo gem install -p http://<proxyHost>:<proxyPort> fluentd -v '~> 0.10.0‘**

# Installing Plugins

We need a couple of plugins:

1. out\_elasticsearch: this plugin lets Fluentd to stream data to Elasticsearch.
2. out*record*reformer: this plugin lets us process data into a more useful format.

The following commands install both plugins (the first apt-get is for out\_elasticsearch: it requires make andlibcurl)

**sudo apt-get install make libcurl4-gnutls-dev --yes**

**sudo /opt/td-agent/embedded/bin/fluent-gem install fluent-plugin-elasticsearch**

**sudo /opt/td-agent/embedded/bin/fluent-gem install fluent-plugin-record-reformer**

**Using proxy: adding “-p http://<Host>:<port>” if you are using proxy, example:**

***sudo /opt/td-agent/embedded/bin/fluent-gem install -p http://10.10.10.10:8080 fluent-plugin-record-reformer***

# Config Fluentd:

Next, we configure Fluentd to listen to syslog messages and send them to Elasticsearch. Open /etc/td-agent/td-agent.conf and add the following lines at the top of the file:

<source>

type syslog

port 5140

tag system

</source>

<match system.\*.\*>

type record\_reformer

tag elasticsearch

facility ${tag\_parts[1]}

severity ${tag\_parts[2]}

</match>

<match elasticsearch>

type copy

<store>

type stdout

</store>

<store>

type elasticsearch

logstash\_format true

flush\_interval 5s #debug

</store>

</match>

### Starting Fluentd

Start Fluentd with the following command:

**sudo service td-agent start**

## Forwarding rsyslog Traffic to Fluentd

Rsyslog configurations are stored in /etc/ryslog.conf file and the files under /etc/rsyslog.d/ directory.

If remote rsyslogd instances are already collecting data into the aggregator rsyslogd, the settings for rsyslog should remain unchanged. However, if this is a brandnew setup, start forward syslog output by adding the following line to /etc/rsyslogd.conf

**\*.\* @192.168.92.127:5140**

You should replace "127.0.0.1" with the IP address of your aggregator server.

And you need remove # for following component to enable it:

(Note: Enable UDP if the log4j version < 2.0, TCP if the log4j version >= 2.0 )

**# provides UDP syslog reception**

**$ModLoad imudp**

**$UDPServerRun 514**

**# provides TCP syslog reception**

**$ModLoad imtcp**

**$InputTCPServerRun 514**

Add following line to the top of config file “/etc/rsyslog.d/50-default.conf”

syslog.\* /var/log/syslog-app.log

Restart rsyslogd as follows:

**sudo service rsyslog restart**