Guide to setup centralized
Logging with EFK stack

Components

1. Elasticsearch (a NoSQL database and search server)
2. Fluent-bit (a log shipping and parsing service)
3. Kibana (a web interface that connects users with the Elasticsearch database and enables visualization and search options for system operation users).

Implementation

Note: Prepare the system by running (this may take a few minutes)

bash -c "apt-get update && apt-get -y upgrade && apt-get -y autoremove && apt-get -y clean"

Elasticsearch

1. Install Java and Set JAVA_HOME environment variable.
2. wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
3. sudo apt -y install apt-transport-https
4. echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list
5. sudo apt update && sudo apt -y install elasticsearch
6. Open the Elasticsearch configuration file at: /etc/elasticsearch/elasticsearch.yml, and change the following values:
    a. cluster.name: my-application
    b. network.host: "localhost"
7. sudo systemctl enable elasticsearch.service && sudo systemctl restart elasticsearch.service
8. sudo curl http://localhost:9200
9. In order to make the service start on boot run:

        sudo update-rc.d elasticsearch defaults 95 10

> Pro Tip: DO NOT open any other ports, like 9200, to the world! There are many bots that search for 9200 and execute groovy scripts to overtake machines. DO NOT bind Elasticsearch to a public IP.

Fluent-bit

Fluent Bit is an open source log shipper and processor, that collects data from multiple sources and forwards it to different destinations. Fluent Bit is written in C and can be used on servers and containers alike.

Sounds pretty similar to Fluentd, right?

The main difference between the two is performance. While Fluentd requires about 40MB and can be expensive, especially if you're running tens or hundreds of instances, all Fluent Bit requires is...wait for it...450KB! This compactness allows it to be installed on small systems such as IoT devices. Fluent Bit also requires no dependencies to run whereas Fluentd requires Ruby gems. While both are pluggable by design, with various input, filter and output plugins available, Fluentd naturally has more plugins than Fluent Bit, being the older tool.

1. wget -qO - http://packages.fluentbit.io/fluentbit.key | sudo apt-key add -
2. echo "deb http://packages.fluentbit.io/ubuntu xenial main" | sudo tee -a /etc/apt/sources.list
3. sudo apt-get update && sudo apt-get install td-agent-bit
4. sudo service td-agent-bit start && sudo service td-agent-bit status
5. Fluent Bit's default configuration collects CPU stats from the host and sends it to stdout. Take a look via your /var/log/syslog file

While Fluend Bit can be configured via the command line, the best way is via the configuration file located (on Debian), at:

/etc/td-agent-bit/td-agent-bit.conf

There are four types of sections that can be defined: service, input, filter and output:

1. Service: This section defines global configuration settings such as the logging verbosity level, the path of a parsers file (used for filtering and parsing data), and more.
2. Input: This section defines the input source for data collected by Fluent Bit, and will include the name of the input plugin to use.
3. Filter: This section defines which filter plugin to use for filtering the data.
4. Output: This section defines the output destination for the data, and will include the name of the output plugin to use.

Procedure to start fluent-bit

1. Stop Fluent Bit, and edit the configuration file:
    a. sudo service td-agent-bit stop
    b. sudo vim /etc/td-agent-bit/td-agent-bit.conf
2. Fire up Fluent Bit again:
    a. sudo service td-agent-bit start
3. Within a few seconds, you should see a new Fluent Bit index created in Elasticsearch:
    a. curl -XGET 'localhost:9200/_cat/indices?v&pretty'

Kibana

Kibana is an open-source data visualization plugin for Elasticsearch. It provides visualization capabilities on top of the content indexed on an Elasticsearch cluster. Users can create bar, line, and scatter plots; pie charts; and maps on top of large volumes of data. Kibana makes working with logs easy. Its graphical web interface even lets beginning users execute powerful log searches.

1. sudo apt-get install kibana
2. sudo vim /etc/kibana/kibana.yml
3. sudo service kibana start
4. Point your browser to http://localhost:5601 after Kibana is started.

Sample Configurations

/etc/elasticsearch/elasticsearch.yml

```
network.host: "localhost"
http.port: 9200
```

/etc/td-agent-bit/td-agent-bit.conf

```
[SERVICE]
```

```
    Flush        5
    Daemon       Off
    Log_Level    info
    HTTP_Server  Off
    HTTP_Listen  0.0.0.0
    HTTP_Port    2020
[INPUT]
    Name cpu
    Tag  cpu.local
    Interval_Sec 2
[OUTPUT]
    Name  es
    Match *
    Host 127.0.0.1
    Port 9200
    Index fluent_bit
    Type cpu_metrics
```

/etc/kibana/kibana.yml

```
server.port: 5601
server.host: "localhost"
elasticsearch.url: ["http://localhost:9200"]
```

Compiled By: Nitish Tiwari