ELK Infrastructure

eCommerce

Exported on 04/13/2022

Table of Contents

No headings included in this document

Elk Components:

1. Filebeat
2. Topbeat
3. Logstash
4. Elasticsearch
5. Kibana

Filebeat:

Filebeat is responsible for shipping the logs from log files to logstash. Filebeat is installed in each of the server boxes from which the logs need to be shipped. Filebeat settings are controlled by two config files

Filebeat specific settings:

- name- filebeat.yml
- config path - /etc/filebeat/filebeat.yml
- code - /ecom-server-settings/filebeat/filebeat.lb.yml

This has settings related to filebeat which includes the log settings, output settings, registry file path and much more.

reference - https://www.elastic.co/guide/en/beats/filebeat/5.4/filebeat-configuration-details.html

Server specific settings:

- config path - /etc/filebeat/conf.d/<server-type>.yml
- code - /ecom-server-settings/filebeat/host-type/*.yml

This has server specific settings which includes the path of the log files, scan frequency and much more. One important setting to note is the document_type which is used to identify the log type and it should be unique within and across the servers

reference - https://www.elastic.co/guide/en/beats/filebeat/5.4/configuration-filebeat-options.html

Topbeat:

Topbeat collects the output of the top command periodically and pushes it to logstash. Similar to filebeat, it is installed in all the servers which needs to be monitored. It has a settings file which configures the output settings, interval period and much more

- name: topbeat.yml
- config path: /etc/topbeat/topbeat.yml
- code - /ecom-server-settings/topbeat/topbeat.yml

Logstash:

Logstash collects the logs from filebeat, parses it, add more details to it and finally pushes it to elasticsearch. The logstash parsing code has three parts in it

Input config:

This defines where the logs are coming from. In our case its from the filebeat. The config is defined in */ecom-server-settings/logstash-log/10-filebeat-input.conf*

Filter config:

This is where all the logic is getting applied to parse the log, filtering unwanted data and add some details to it. There are many types of filters that is available as part of logstash filter plugins. Refer to https://www.elastic.co/guide/en/logstash/5.4/filter-plugins.html for more details.

The code for the filters we have implemented are available in */ecom-server-settings/logstash-log/*.conf.*

We have grouped the filters by the type of the logs they deal with.

Output config:

This config defines where the logs should get pushed to. In our case its elasticsearch. Here we define, for each type of log, the index in elasticsearch it should go to and the elasticsearch template for it.

Refer to */ecom-server-settings/logstash-log/30-elastic5-output.conf*

Logstash node setup in AWS[1] - This has information about list of logstash nodes in production, deployment and setup steps.

Elasticsearch:

This is where logs are indexed and made available for search and analysis. We have an ES cluster of 10 data nodes, 3 master nodes and 6 client nodes. The client ES instances are installed in the same server where the logstash instances are installed so that the we dont have to worry about network latency when logstash is pushing the data to ES.

ES log cluster setup in AWS[2] - This has information about setting up an ES node in production

Kibana:

This is a web UI for viewing data stored in ES. This can be used to run complex search queries on ES data and build visualizations and reports on top of the data stored in ES.

Production kibana url - https://34.231.203.149:3321/app/kibana

username/password - kibanauser/kibblesNb1ts

Watcher:

Wather is an ES plugin which is used in our system to raise pager duty alerts based on ES search queries. Watcher plugin is installed in a seperate two node ES cluster(prod-wch-21,prod-wch-22)

Watcher Alerts[3] - This has the list of alerts currently configured in production

Code for wather alerts can be found in /ecom-server-settings/watcher/*.txt

[1] https://confluence.samsungmtv.com/display/EC/Logstash+node+setup+in+AWS
[2] https://confluence.samsungmtv.com/display/EC/ES+log+cluster+setup+in+AWS
[3] https://confluence.samsungmtv.com/display/EC/Watcher+Alerts