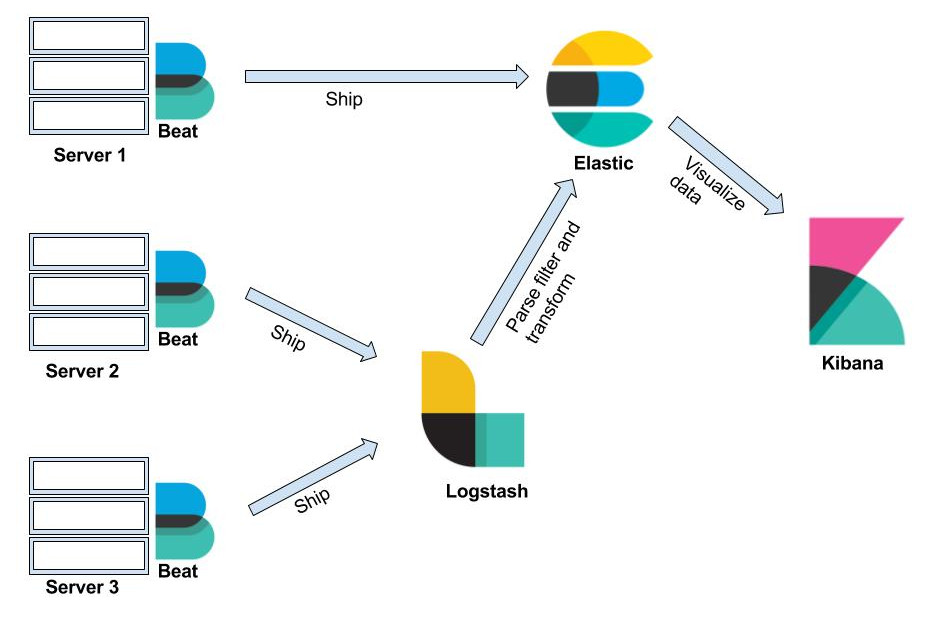
**Balluun** **Log Analytics**

With

**ELK Stack**

* ELK is natively designed to do log analysis.
* Elasticsearch engine will store the data in the JSON format
* Each log it will store in the JSON and treat it as one document.

Following diagram illustrate how data will be shipped into elasticsearch engine.



We can ship data in two ways

1. Install filebeats → give log file path.
2. Install filebeats → give log file path → In the target section give logstash configuration → remove/add unnecessary fields and dump in the elasticsearch engine.

#1 will be using file beats when we multiple patterns in the log file. #2 will be useful when we want to have necessary fields only.

As we have multiple log files and multiple patterns we have chosen file beats to ship logs into elasticsearch. Follow the below instructions to install filebeat.

1. Download and install the public signing key for Linux distributions:

sudo rpm --import https://packages.elastic.co/GPG-KEY-elasticsearch

1. Create a file with a .repo extension (for example, elastic.repo) in your /etc/yum.repos.d/directory and add the following lines:

[elastic-6.x]

name=Elastic repository for 6.x packages

baseurl=https://artifacts.elastic.co/packages/6.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1

autorefresh=1

Now install **metricbeat**

sudo yum install filebeat

1. To configure the Beat to start automatically during boot, run:

sudo chkconfig --add filebeat

This is a basic installation to install file beat, based on requirement we will change filebeat.yml file and enable modules.

Let’s see how to configure file beat for each server.

**Balluun - UI file beat configuration:**

* Login into Balluun UI server
* Follow the above steps to install file beat
* As UI hosted in elastic beanstalk, the log format will be in apache logs. So we need to enable apache2 module using the below command
  + Sudo filebeat modules enable apache2
* Open the file beat config file under **/etc/filebeat/** folder
  + Sudo vi filebeat.yml
* At line 99 add the below lines to have custom fields

fields:

hostname: balluun-ui

fields\_under\_root: true

* In line 155 rename elasticsearch IP.
* For the first time, we need to load file beat dashboards into kibana to visualize apache2 logs. Run below command to load them.
  + Sudo filebeat setup --dashboards
* This dashboard loads geo maps, response codes, end-user browser information, and error log information.

**Note:** Elastic Beanstalk is changing the apache2 application log pattern. When we run, fields cannot be indexed and visualized in kibana dashboard. We need to change the grok pattern which is being used by file beat.

**Log pattern:**

10.0.0.96 **(67.163.78.87)** - - [04/Feb/2018:05:13:32 +0000] "GET /assets/img/icons/icon-heart.svg HTTP/1.1" 304 - "https://shoptoys365.balluun.com/assets/css/style-min.css?1517391259" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36"

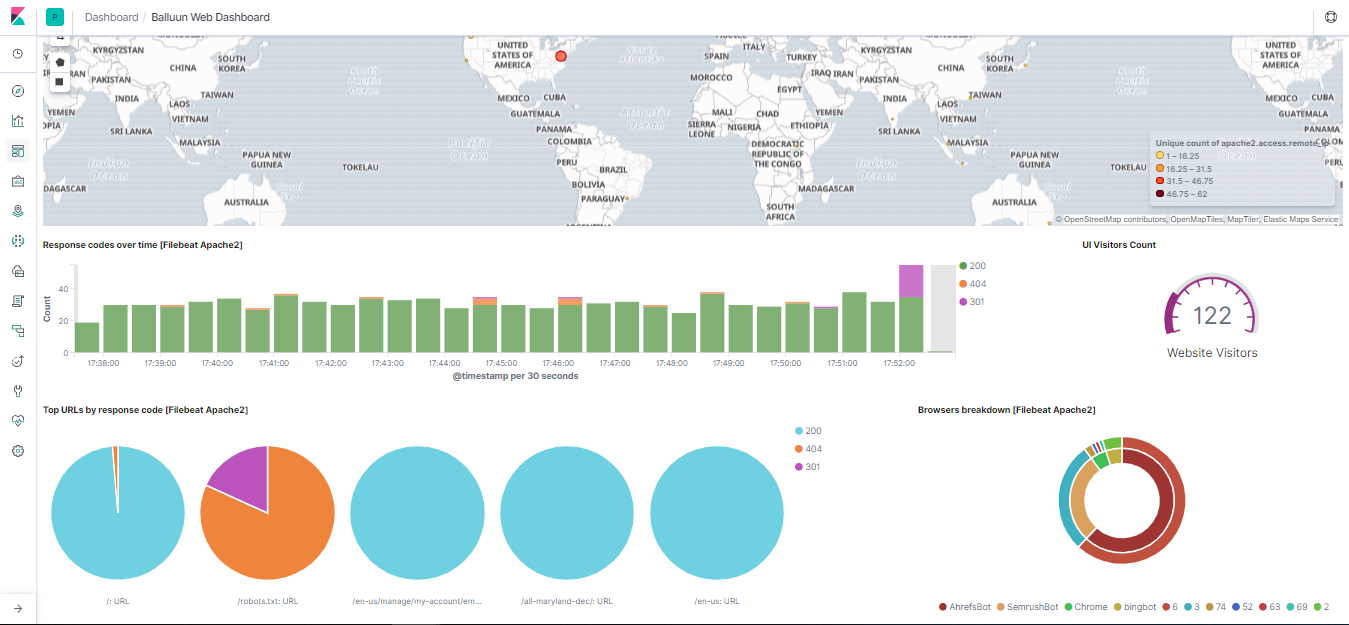
10.0.0.221 **(73.82.235.183)** - - [04/Feb/2018:05:13:32 +0000] "GET /assets/img/icons/icon-down-chevron.svg HTTP/1.1" 304 - "https://shoptoys365.balluun.com/en-us/showroom/products/manage/all" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_12\_6) AppleWebKit/604.5.6 (KHTML, like Gecko) Version/11.0.3 Safari/604.5.6"

We are getting additional IP first and required client IP was in brackets and some other fields pattern was not matching exactly. So we need to update file beat fields pattern to identify the log format and visualize in the dashboards.

Follow the below steps to update grok pattern which using by apache2 module.

* cd /usr/share/filebeat/modules/apache2/access/ingest
* Sudo vi default.json
* Update the pattern with below one in line 7 to take the effect.
  + "%{IPORHOST:http\_vhost} \\(%{IPORHOST:apache2.access.remote\_ip}\\) - %{DATA:apache2.access.user\_name} \\[%{HTTPDATE:apache2.access.time}\\] \"(?:%{WORD:apache2.access.method} %{DATA:apache2.access.url} HTTP/%{NUMBER:apache2.access.http\_version}|-)?\" %{NUMBER:apache2.access.response\_code} (?:%{NUMBER:apache2.access.body\_sent.bytes}|-) \"-\" (\"%{DATA:apache2.access.agent}\")?(\"%{DATA:apache2.access.referrer}\")?
* Save and exit.
* Run the following commands before start file beat
  + curl -XGET 10.0.3.64:9200/\_ingest/pipeline
  + curl -XDELETE:9200/\_ingest/pipeline/filebeat-7.0.1-apache-access-default
* Restart file beat
  + Sudo service filebeat restart

Now we should able to see the dashboard in kibana (Dashboards → Apache2 [filebeat])



**Balluun API file beat configuration:**

API is running inside the Nginx. So we will be having access logs and error logs in **/var/log/nginx** folder.

* Login into Balluun API server
* Follow the same steps to install file beat in the API server. (**Reference:** Page- 2)
* API hosted in normal EC2 instance and it has nginx as a reverse proxy. So whenever we access this API log will be recorded in Nginx logs and the log format will be in nginx logs. So we need to enable nginx module using the below command
  + Sudo filebeat modules enable nginx
* Open the file beat config file under **/etc/filebeat/** folder
  + Sudo vi filebeat.yml
* At line 99 add the below lines to have custom fields

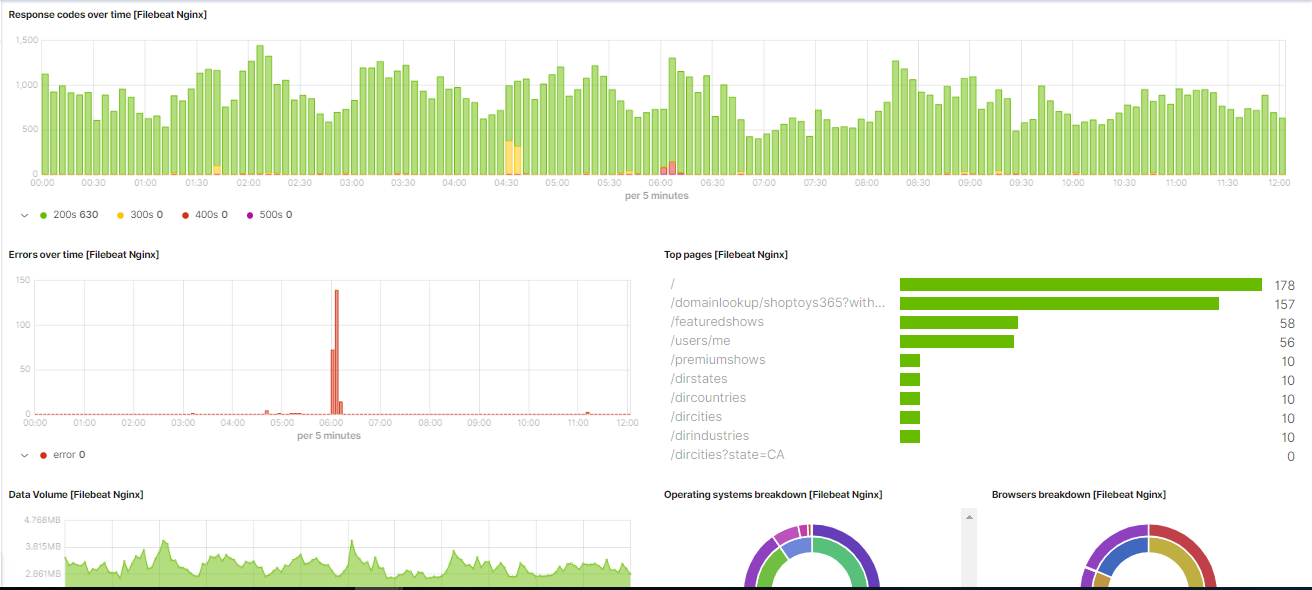
fields:

hostname: balluun-perf-api

fields\_under\_root: true

* We don’t need to load the file beat dashboards as it has done in while configuring file beat for UI.
* This dashboard loads geo maps, response codes, end-user browser information, and error log information.
* In line 155 rename elasticsearch IP.

Now we should able to see the dashboard in kibana (Dashboards → Nginx Overview [filebeat])





**Balluun worker server - file beat configuration:**

The worker is running inside EC2 machine. It has so many log files under /root/.pm2/logs folder. So give /root/.pm2/logs path to get all logs and dump into the elasticsearch engine.

* Login into Balluun worker server
* Follow the same steps to install file beat in the worker server. (**Reference:** Page- 2)
* Worker hosted in normal EC2 instance and it has a bunch of log files under the /root/.pm2/logs folder.
* Open the file beat config file under **/etc/filebeat/** folder
  + Sudo vi filebeat.yml
* In line 24
  + change **enabled: false** to **enabled: true**
* Under paths filed add below line
  + **- /root/.pm2/logs/\*.log**
* At line 99 add the below lines to have custom fields

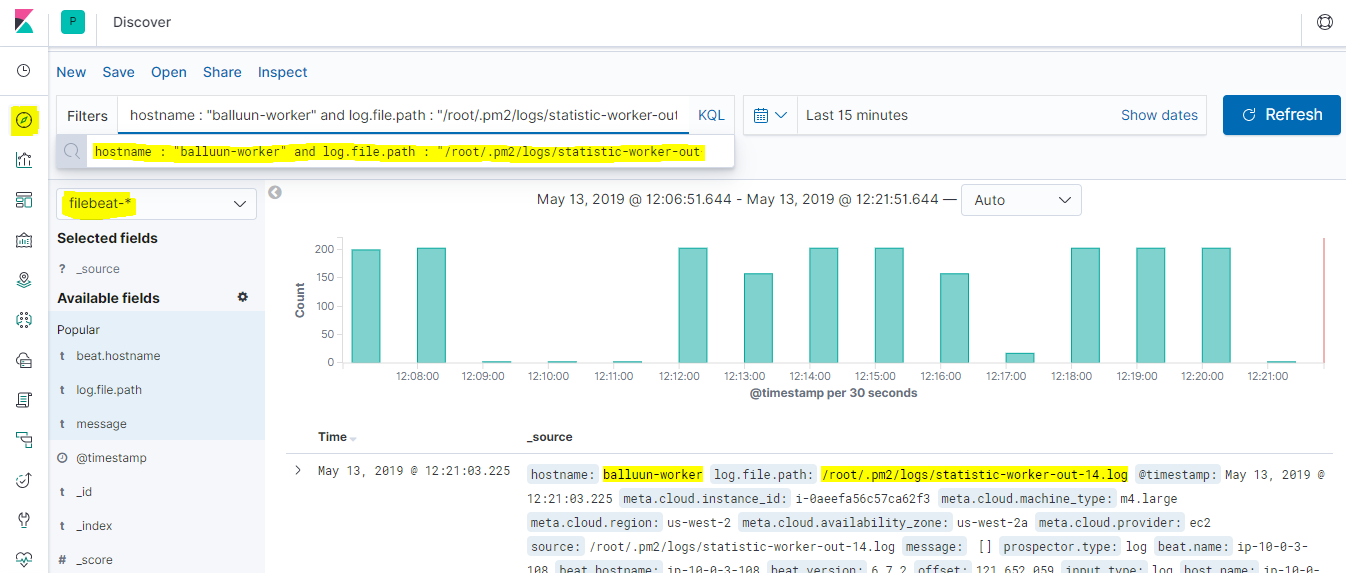
fields:

hostname: balluun-worker

fields\_under\_root: true

* In line 155 rename elasticsearch IP.

Now we should able to see the dumped logs in kibana discover section. Open kibana and search the logs like below.



**Balluun Rabbit-MQ server - file beat configuration:**

The Rabbit-MQ is running inside the EC2 machine. It has log files under /var/log/rabbitmq/ folder. So give point to the above path to get all logs and dump into the elasticsearch engine.

* Login into Balluun Rabbit-MQ server
* Follow the same steps to install file beat in the worker server. (**Reference:** Page- 2)
* Rabbit-MQ hosted in normal EC2 instance and it has log files under the */var/log/rabbitmq/* folder.
* Open the file beat config file under **/etc/filebeat/** folder
  + Sudo vi filebeat.yml
* In line 24
  + change **enabled: false** to **enabled: true**
* Under paths filed add below line
  + **- /var/log/rabbitmq**/**\*.log**
* **Note:** Rabbit-MQ logs are in multiline pattern, file beat consider each line is a log. So we need to add some additional configuration to get the multiline logs.
* Add the below two lines in 65 line
  + multiline.pattern: ^\=
  + multiline.match: before
* At line 99 add the below lines to have custom fields

fields:

hostname: balluun-mq

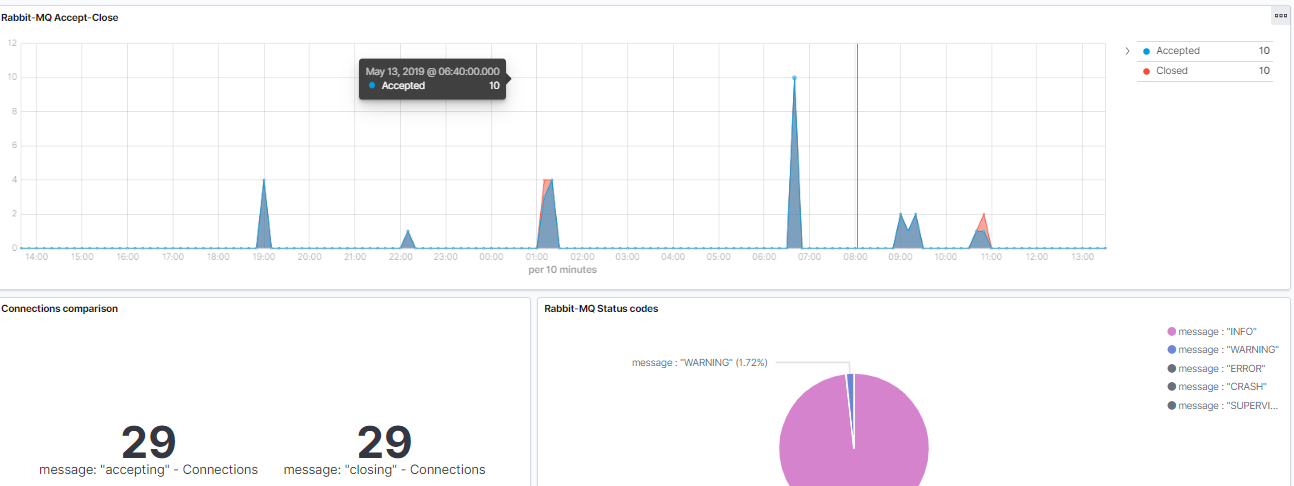
fields\_under\_root: true

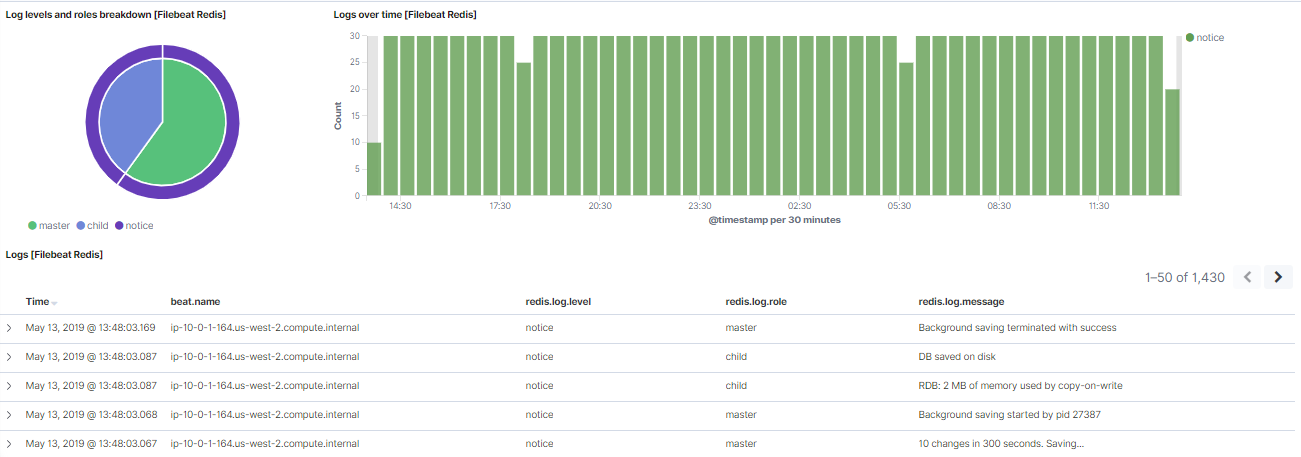
* In line 155 rename elasticsearch IP.

We have Redis logs also in the same server if we just enable Redis module it could also capture Redis server logs. Run the below command to enable Redis file beat module.

Sudo filebeat modules enable redis

* Now start filebeat to dump the redis and rabbit-mq logs into elasticsearch.
  + sudo service filebeat start

****

****