

ELK - ElasticSearch, LogStash, Kibana

Testings

Object	Comment / Link	Status
ELK Stack	An excellent Guide for Ubuntu 14.04 is at https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-ubuntu-14-04	TESTED
TopBeat	https://www.digitalocean.com/community/tutorials/how-to-gather-infrastructure-metrics-with-topbeat-and-elk-on-ubuntu-14-04	TESTED
PacketBe at	https://z0z0.me/monitor-your-servers-with-elasticsearch-2-x-and-beats-and-display-it-in-kibana/	TESTET
GeolP Support	https://www.digitalocean.com/community/tutorials/how-to-map-user-location-with-geoip-and-elk-elasticsearch-logstash-and-kibana	TESTED Gave some field mapping challenges, and I had to delete the filebeat index values. The Great Mapping Refactoring
Tomcat Log Parsing	https://blog.lanyonm.org/articles/2014/01/12/logstash-multiline-tomcat-log-parsing.html	NOT TESTED
Shield (Security)	https://www.elastic.co/guide/en/shield/current/kibana.html#using-kibana4-with-shield	NOT TESTED

Tips



Make sure the server time is correct for all servers 😊 as in use [NTP](#).

I have divided stuff a bit, please read:

[Logstash - Tips and Troubleshooting](#)

[Elasticsearch - Tips and Troubleshooting](#)

Sample filebeat.yml config for my Confluence Server

```

paths:
  - /var/log/auth.log
  - /var/log/syslog
document_type: syslog
input_type: log
-
paths:
  - /var/log/apache2/www.mos-eisley.dk-*.log
document_type: apache
input_type: log
-
paths:
  - /data/www/Fordor.log
  - /data/www/Baghus.log
document_type: camfileslog
input_type: log

```

Sample filebeat.yml config for my Alfresco Server

```

paths:
  - /var/log/auth.log
  - /var/log/syslog
document_type: syslog
input_type: log
-
paths:
  - /var/log/apache2/alfresco.mos-eisley.dk-*.log
  - /var/log/apache2/elk.mos-eisley.dk-*.log
document_type: apache
input_type: log
-
paths:
  - /var/log/pingkaf.txt
document_type: pinglog
input_type: log

```

Other Stuff:

http://www.slideshare.net/aca_it/monitor-your-atlassian-stack-like-the-nsa

[Elasticsearch CRUD](#)

[The Great Mapping Refactoring](#)

[Embedding Visualisations](#)

[A bit of logstash cooking](#)

[ELK - 3 THINGS I WISH I'D KNOWN](#)

[Little Logstash Lessons - Part I: Using grok and mutate to type your data](#)

[5 Logstash Pitfalls You Need to Avoid](#)