

<https://www.elastic.co/downloads/kibana>

<https://www.elastic.co/downloads/elasticsearch>

<https://www.elastic.co/downloads/logstash>

search for package in repro:

apt-cache search <package>

On the client side install filebeat.

<http://ict.renevdmark.nl/2016/07/05/elastic-beats-on-raspberry-pi/>

But use as output in the yml file instead of direct connecting to elasticsearch, connect to logstash:

output:

logstash:

hosts: ["192.168.178.7:5044"]

index: "filebeat"

On server side install java8, logstash, elasticsearch and Kibana.exit

sudo apt-get install oracle-java8-jdk

sudo wget <https://artifacts.elastic.co/downloads/kibana/kibana-5.4.1-linux-x86_64.tar.gz>

sudo wget <https://artifacts.elastic.co/downloads/logstash/logstash-5.4.1.tar.gz>

mkdir /opt/elasticsearch

chmod 777 /opt/elasticsearch

useradd -d "/opt/elasticsearch" -M -s /bin/bash -U elasticsearch

su – elasticsearch

wget <https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-5.4.1.tar.gz>

tar zxvf elasticsearch-5.4.1.tar.gz

sudo mkdir -p /etc/elasticsearch/conf.d

mv elasticsearch-5.4.1/\* .

Update following items in /opt/elasticsearch/config/elasticsearch.yml

cluster.name: logstash

network.host: 192.168.178.7 -> 127.0.0.1

ln -s /opt/elasticsearch/config/elasticsearch.yml /etc/elasticsearch/conf.d/

Change JVM heap size to lower values because of memory raspberrypi.

/opt/elasticsearch/config/jvm.options

-Xms2g

-Xmx2g

-Xms128m

-Xmx512m

sysctl vm.max\_map\_count=262144

./bin/elasticsearch &

root@raspiweb:/opt/kibana# more config/kibana.yml | grep -v ^#

server.host: "127.0.0.1"

elasticsearch.url: <http://127.0.0.1:9200>

mkdir elastic

cd elastic

wget https://artifacts.elastic.co/downloads/logstash/logstash-5.4.2.tar.gz

wget https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-5.4.2-linux-x86\_64.tar.gz

wget https://artifacts.elastic.co/downloads/kibana/kibana-5.4.2-linux-x86\_64.tar.gz

wget <https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-5.4.2.tar.gz>

tar -xvf elasticsearch-5.4.2.tar.gz

cd elasticsearch-5.4.2/config

vi jvm.options

-Xms256m

-Xmx512m

sysctl vm.max\_map\_count

vm.max\_map\_count = 65530

sysctl vm.max\_map\_count=262144

vm.max\_map\_count = 262144

cd ..

./bin/elasticsearch

curl <http://127.0.0.1:9200>

{

"name" : "abGGuN6",

"cluster\_name" : "elasticsearch",

"cluster\_uuid" : "Xf3z2kjtSyyLTwNnAlDmYw",

"version" : {

"number" : "5.4.2",

"build\_hash" : "929b078",

"build\_date" : "2017-06-15T02:29:28.122Z",

"build\_snapshot" : false,

"lucene\_version" : "6.5.1"

},

"tagline" : "You Know, for Search"

}

Kill (CTRL-C) the elasticsearch binary.

cd ~/elastic

mv elasticsearch-5.4.2 /usr/share/elasticsearch

cd /usr/share/elasticsearch/config/

modify elasticsearch.yml:

cluster.name: (Whatever name you want)

network.host: 127.0.0.1

http.port: 9200

cd ~/elastic

tar xvzf logstash-5.4.2.tar.gz

mv logstash-5.4.2 /opt/logstash-5.4.2

mkdir -p /etc/logstash/conf.d

vi /opt/logstash-5.4.2/config/logstash.yml

http.host: "192.168.178.8"

USE\_JRUBY=1 LS\_HEAP\_SIZE=64m /opt/logstash-5.4.2/bin/logstash -f /opt/logstash-5.4.2/config/logstash.yml

java.lang.UnsatisfiedLinkError: /opt/logstash-5.4.2/vendor/jruby/lib/jni/arm-Linux/libjffi-1.2.so: /opt/logstash-5.4.2/vendor/jruby/lib/jni/arm-Linux/libjffi-1.2.so: cannot open shared object file: No such file or directory

apt-get update

apt-get install git

cd ~/ elastic

git clone <https://github.com/jnr/jffi.git>

cd jffi/

apt-get install -y ant

ant jar

mv /opt/logstash-5.4.2/vendor/jruby/lib/jni/arm-Linux/libjffi-1.2.so /opt/logstash-5.4.2/vendor/jruby/lib/jni/arm-Linux/libjffi-1.2.so.org

cp build/jni/libjffi-1.2.so /opt/logstash-5.4.2/vendor/jruby/lib/jni/arm-Linux/libjffi-1.2.so

apt-get install zip

zip -g jruby.jar jni/arm-Linux/libjffi-1.2.so

updating: jni/arm-Linux/libjffi-1.2.so

zip warning: Local Entry CRC does not match CD: jni/arm-Linux/libjffi-1.2.so

(deflated 62%)

root@elasticpi:/opt/logstash-5.4.2/config# more /opt/logstash-5.4.2/config/logstash.conf

input {

beats {

port => 5044

}

}

filter {

grok {

match => { "message" => "%{COMBINEDAPACHELOG}" }

}

date {

match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ]

}

}

output {

elasticsearch {

hosts => ["127.0.0.1:9200"]

}

}

SE\_JRUBY=1 LS\_HEAP\_SIZE=64m /opt/logstash-5.4.2/bin/logstash -f /opt/logstash-5.4.2/config/logstash.conf