1> filbeat-> elasticsearch -> kibana 구조

[filebeat설치]

* rpm --import <https://artifacts.elastic.co/GPG-KEY-elasticsearch>
* wget https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-5.5.2-x86\_64.rpm
* rpm -ivh filebeat-5.5.2-x86\_64.rpm
* vi filebeat.yml

filebeat.prospectors:

- input\_type: log

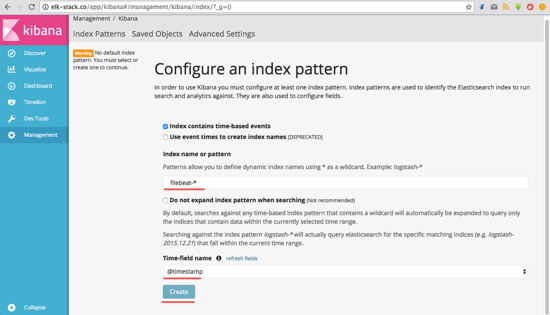
paths:

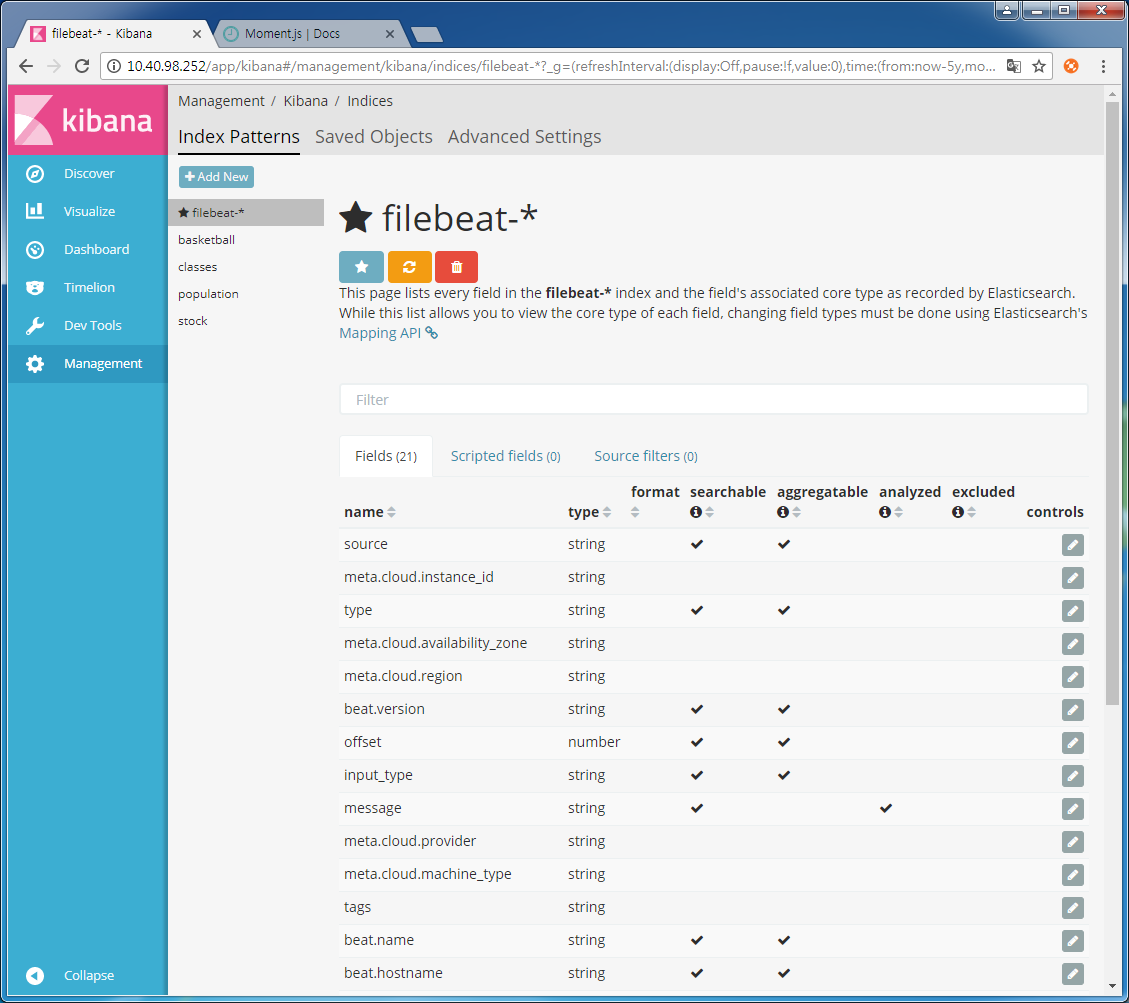
- /var/log/\*.log

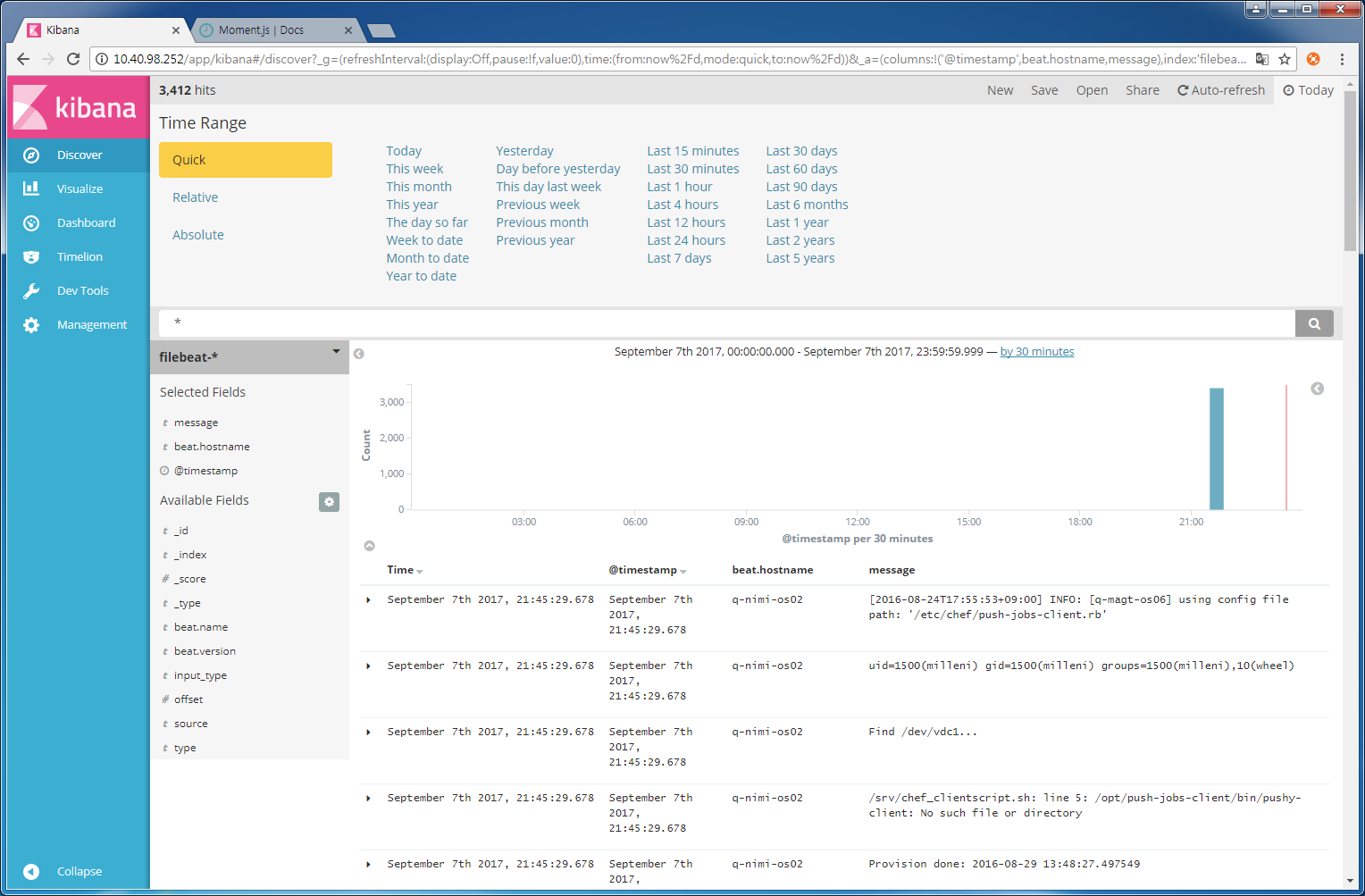
output.elasticsearch:

hosts: ["localhost:9200"]

* systemctl restart filebeat
* systemctl restart elasticsearch







2> filbeat-> logstash -> elasticsearch -> kibana 구조 [일반로그 연동설정]

[filebeat설정]

**vi /etc/filebeat/filebeat.yml**

filebeat.prospectors:

- input\_type: log

paths:

- /var/log/\*.log

output.logstash:

hosts: ["localhost:5044"]

**systemctl restart filebeat**

[logstash설정]

**vi /etc/logstash/conf.d/logstash.conf**

input {

beats {

port => 5044

}

}

# The filter part of this file is commented out to indicate that it is

# optional.

# filter {

#

# }

output {

elasticsearch {

hosts => "localhost:9200"

manage\_template => false

index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"

document\_type => "%{[@metadata][type]}"

}

}

3> filbeat-> logstash -> elasticsearch -> kibana 구조 [특정파일 연동설정]

[logstash설정]

**vi /etc/logstash/conf.d/first-pipeline.conf**

input {

beats {

port => 5043

}

}

# The filter part of this file is commented out to indicate that it is

# optional.

# filter {

#

# }

output {

stdout { codec => rubydebug }

}

**/usr/share/logstash/bin/logstash -f first-pipeline.conf --config.reload.automatic**

[filebeat설정]

**vi filebeat.yml**

filebeat.prospectors:

- input\_type: log

paths:

- /root/logstash-tutorial.log -> 사전에 파일다운로드

output.logstash:

hosts: ["localhost: 5043”]

**/usr/share/filebeat/bin/filebeat -e -c /etc/filebeat/filebeat.yml -d "publish"**

[결과값 양식]

{

"@timestamp" => 2017-09-15T08:12:22.218Z,

"offset" => 24464,

"@version" => "1",

"input\_type" => "log",

"beat" => {

"hostname" => "q-nimi-os01.novalocal",

"name" => "q-nimi-os01.novalocal",

"version" => "5.5.2"

},

"host" => "q-nimi-os01.novalocal",

"source" => "/root/logstash-tutorial.log",

"message" => "86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] \"GET /style2.css HTTP/1.1\" 200 4877 \"http://www.semicomplete.com/projects/xdotool/\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0\"",

"type" => "log",

"tags" => [

[0] "beats\_input\_codec\_plain\_applied"

]

}

4> filbeat-> logstash -> elasticsearch -> kibana 구조 [특정파일 연동 logstash grok filter설정]

[logstash설정]

cd /etc/logstash/conf.d

**vi first-pipeline.conf**

input {

beats {

port => 5043

}

}

# The filter part of this file is commented out to indicate that it is

# optional.

filter {

grok {

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

}

}

output {

stdout { codec => rubydebug }

}

**/usr/share/logstash/bin/logstash -f first-pipeline.conf --config.reload.automatic**

[filebeat설정]

**rm /var/lib/filebeat/data/registry**

**/usr/share/filebeat/bin/filebeat -e -c /etc/filebeat/filebeat.yml -d "publish"**

[결과값 양식]

{

"request" => "/style2.css",

"agent" => "\"Mozilla/5.0 (X11; Linux x86\_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0\"",

"offset" => 24464,

"auth" => "-",

"ident" => "-",

"input\_type" => "log",

"verb" => "GET",

"source" => "/root/logstash-tutorial.log",

"message" => "86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] \"GET /style2.css HTTP/1.1\" 200 4877 \"http://www.semicomplete.com/projects/xdotool/\" \"Mozilla/5.0 (X11; Linux x86\_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0\"",

"type" => "log",

"tags" => [

[0] "beats\_input\_codec\_plain\_applied"

],

"referrer" => "\"http://www.semicomplete.com/projects/xdotool/\"",

"@timestamp" => 2017-09-15T08:18:41.010Z,

"response" => "200",

"bytes" => "4877",

"clientip" => "86.1.76.62",

"@version" => "1",

"beat" => {

"hostname" => "q-nimi-os01.novalocal",

"name" => "q-nimi-os01.novalocal",

"version" => "5.5.2"

},

"host" => "q-nimi-os01.novalocal",

"httpversion" => "1.1",

"timestamp" => "04/Jan/2015:05:30:37 +0000"

5> filbeat-> logstash -> elasticsearch -> kibana 구조 [일반로그 연동설정]

[logstash설정]

**vi first-pipeline.conf**

input {

beats {

port => "5043"

}

}

filter {

grok {

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

}

geoip {

source => "clientip"

}

}

output {

elasticsearch {

hosts => [ "localhost:9200" ]

}

}

**systemctl restart logstash**

[filebeat설정]

**rm /var/lib/filebeat/data/registry**

**/usr/share/filebeat/bin/filebeat -e -c /etc/filebeat/filebeat.yml -d "publish"**

[root@q-nimi-os01 conf.d]# **curl 'localhost:9200/\_cat/indices?v'**

health status index uuid pri rep docs.count docs.deleted store.size pri.store.size

yellow open bank 23WVaGqvSvKuuBotIyRWKg 5 1 1000 0 640.8kb 640.8kb

yellow open logstash-2015.05.19 QffynWhVTySf0me6QE5l9w 5 1 4624 0 29.5mb 29.5mb

yellow open logstash-2015.05.20 o\_qOYWG6SbmOrovtd\_ugPQ 5 1 4750 0 27.4mb 27.4mb

yellow open **logstash-2017.09.15** QJeGXEVMT\_u6W0SSvm6laQ 5 1 100 0 267.2kb 267.2kb

yellow open shakespeare dhCpsdY2Rcy5DmUoYfmZqw 5 1 111396 0 28mb 28mb

yellow open .kibana inLneHTvSfO8A48xdqWm2g 1 1 10 1 53.6kb 53.6kb

yellow open logstash-2015.05.18 Dd-7kO8KSQKdkN4s0UEPEA 5 1 4631 0 28.9mb 28.9mb

yellow open filebeat-2017.09.15 kcPRDOSNQW6hHltfs0sh7A 5 1 100 0 218.1kb 218.1kb

yellow open filebeat-2017.09.10 GLi9sshOQrCFFKVOnPO4jg 5 1 171 0 78.2kb 78.2kb

**curl -XGET 'localhost:9200/logstash-2017.09.15/\_search?pretty&q=response=200' 결과 확인**

**index 패턴을 logstash-2017.09\* 로 Create**

