vi config/logstash.yml

config.reload.automatic: true

vi weblog.conf

input {

tcp {

port => 9900

}

}

output {

stdout { }

}

bin/logstash -f weblog.conf

echo 'hello world' | nc localhost 9900

2017-11-21T11:54:06.937Z 0:0:0:0:0:0:0:1 hello

vi cat weblog.conf

input {

tcp {

port => 9900

}

}

output {

stdout {

codec=>"rubydebug"

}

}

echo '14.49.42.25 - - [12/Mar/2015:01:24:44 +0000] "GET /articles/ppp-over-ssh/ HTTP/1.1" 200 18586 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2b1) Gecko/20091014 Firefox/3.6b1 GTB5"' | nc localhost 9900

{

"@version" => "1",

"host" => "0:0:0:0:0:0:0:1",

"@timestamp" => 2017-11-21T12:11:24.308Z,

"message" => "14.49.42.25 - - [12/Mar/2015:01:24:44 +0000] \"GET /articles/ppp-over-ssh/ HTTP/1.1\" 200 18586 \"-\" \"Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2b1) Gecko/20091014 Firefox/3.6b1 GTB5\"",

"port" => 45600

}

vi weblog.conf

input {

tcp {

port => 9900

}

}

filter{

grok {

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

}

}

output {

stdout {

codec=>"rubydebug"

}

}

{

"request" => "/articles/ppp-over-ssh/",

"agent" => "\"Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2b1) Gecko/20091014 Firefox/3.6b1 GTB5\"",

"auth" => "-",

"ident" => "-",

"verb" => "GET",

"message" => "14.49.42.25 - - [12/Mar/2015:01:24:44 +0000] \"GET /articles/ppp-over-ssh/ HTTP/1.1\" 200 18586 \"-\" \"Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2b1) Gecko/20091014 Firefox/3.6b1 GTB5\"",

"referrer" => "\"-\"",

"@timestamp" => 2017-11-21T12:21:44.394Z,

"port" => 46264,

"response" => "200",

"bytes" => "18586",

"clientip" => "14.49.42.25",

"@version" => "1",

"host" => "0:0:0:0:0:0:0:1",

"httpversion" => "1.1",

"timestamp" => "12/Mar/2015:01:24:44 +0000"

}

vi weblog.conf

input {

tcp {

port => 9900

}

}

filter{

grok {

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

}

geoip { source => "clientip" }

}

output {

stdout {

codec=>"rubydebug"

}

}

{

"request" => "/articles/ppp-over-ssh/",

"agent" => "\"Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2b1) Gecko/20091014 Firefox/3.6b1 GTB5\"",

"geoip" => {

"timezone" => "Asia/Seoul",

"ip" => "14.49.42.25",

"latitude" => 37.5112,

"country\_name" => "Republic of Korea",

"country\_code2" => "KR",

"continent\_code" => "AS",

"country\_code3" => "KR",

"location" => {

"lon" => 126.97409999999999,

"lat" => 37.5112

},

"longitude" => 126.97409999999999

},

"auth" => "-",

"ident" => "-",

"verb" => "GET",

"message" => "14.49.42.25 - - [12/Mar/2015:01:24:44 +0000] \"GET /articles/ppp-over-ssh/ HTTP/1.1\" 200 18586 \"-\" \"Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2b1) Gecko/20091014 Firefox/3.6b1 GTB5\"",

"referrer" => "\"-\"",

"@timestamp" => 2017-11-21T12:28:52.595Z,

"port" => 46710,

"response" => "200",

"bytes" => "18586",

"clientip" => "14.49.42.25",

"@version" => "1",

"host" => "0:0:0:0:0:0:0:1",

"httpversion" => "1.1",

"timestamp" => "12/Mar/2015:01:24:44 +0000"

}

vi weblog.conf

input {

tcp {

port => 9900

}

}

filter{

grok {

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

}

geoip { source => "clientip" }

useragent {

source => "agent"

target => "useragent"

}

}

output {

stdout {

codec=>"rubydebug"

}

}

{

"request" => "/articles/ppp-over-ssh/",

"agent" => "\"Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2b1) Gecko/20091014 Firefox/3.6b1 GTB5\"",

"geoip" => {

"timezone" => "Asia/Seoul",

"ip" => "14.49.42.25",

"latitude" => 37.5112,

"country\_name" => "Republic of Korea",

"country\_code2" => "KR",

"continent\_code" => "AS",

"country\_code3" => "KR",

"location" => {

"lon" => 126.97409999999999,

"lat" => 37.5112

},

"longitude" => 126.97409999999999

},

"auth" => "-",

"ident" => "-",

"verb" => "GET",

"useragent" => {

"patch" => "b1",

"os" => "Windows 7",

"major" => "3",

"minor" => "6",

"build" => "",

"name" => "Firefox Beta",

"os\_name" => "Windows 7",

"device" => "Other"

},

"message" => "14.49.42.25 - - [12/Mar/2015:01:24:44 +0000] \"GET /articles/ppp-over-ssh/ HTTP/1.1\" 200 18586 \"-\" \"Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2b1) Gecko/20091014 Firefox/3.6b1 GTB5\"",

"referrer" => "\"-\"",

"@timestamp" => 2017-11-21T12:41:00.484Z,

"port" => 47494,

"response" => "200",

"bytes" => "18586",

"clientip" => "14.49.42.25",

"@version" => "1",

"host" => "0:0:0:0:0:0:0:1",

"httpversion" => "1.1",

"timestamp" => "12/Mar/2015:01:24:44 +0000"

}

vi weblog.conf

input {

tcp {

port => 9900

}

}

filter{

grok {

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

}

geoip { source => "clientip" }

useragent {

source => "agent"

target => "useragent"

}

mutate {

convert => {

"bytes" => "integer"

}

}

}

output {

stdout {

codec=>"rubydebug"

}

}

{

"request" => "/articles/ppp-over-ssh/",

"agent" => "\"Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2b1) Gecko/20091014 Firefox/3.6b1 GTB5\"",

"geoip" => {

"timezone" => "Asia/Seoul",

"ip" => "14.49.42.25",

"latitude" => 37.5112,

"country\_name" => "Republic of Korea",

"country\_code2" => "KR",

"continent\_code" => "AS",

"country\_code3" => "KR",

"location" => {

"lon" => 126.97409999999999,

"lat" => 37.5112

},

"longitude" => 126.97409999999999

},

"auth" => "-",

"ident" => "-",

"verb" => "GET",

"useragent" => {

"patch" => "b1",

"os" => "Windows 7",

"major" => "3",

"minor" => "6",

"build" => "",

"name" => "Firefox Beta",

"os\_name" => "Windows 7",

"device" => "Other"

},

"message" => "14.49.42.25 - - [12/Mar/2015:01:24:44 +0000] \"GET /articles/ppp-over-ssh/ HTTP/1.1\" 200 18586 \"-\" \"Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2b1) Gecko/20091014 Firefox/3.6b1 GTB5\"",

"referrer" => "\"-\"",

"@timestamp" => 2017-11-21T12:44:15.620Z,

"port" => 47694,

"response" => "200",

"bytes" => 18586,

"clientip" => "14.49.42.25",

"@version" => "1",

"host" => "0:0:0:0:0:0:0:1",

"httpversion" => "1.1",

"timestamp" => "12/Mar/2015:01:24:44 +0000"

}

vi weblog.conf

input {

tcp {

port => 9900

}

}

filter{

grok {

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

}

geoip { source => "clientip" }

useragent {

source => "agent"

target => "useragent"

}

mutate {

convert => {

"bytes" => "integer"

}

}

date {

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

}

}

output {

stdout {

codec=>"rubydebug"

}

}

{

"request" => "/articles/ppp-over-ssh/",

"agent" => "\"Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2b1) Gecko/20091014 Firefox/3.6b1 GTB5\"",

"geoip" => {

"timezone" => "Asia/Seoul",

"ip" => "14.49.42.25",

"latitude" => 37.5112,

"country\_name" => "Republic of Korea",

"country\_code2" => "KR",

"continent\_code" => "AS",

"country\_code3" => "KR",

"location" => {

"lon" => 126.97409999999999,

"lat" => 37.5112

},

"longitude" => 126.97409999999999

},

"auth" => "-",

"ident" => "-",

"verb" => "GET",

"useragent" => {

"patch" => "b1",

"os" => "Windows 7",

"major" => "3",

"minor" => "6",

"build" => "",

"name" => "Firefox Beta",

"os\_name" => "Windows 7",

"device" => "Other"

},

"message" => "14.49.42.25 - - [12/Mar/2015:01:24:44 +0000] \"GET /articles/ppp-over-ssh/ HTTP/1.1\" 200 18586 \"-\" \"Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2b1) Gecko/20091014 Firefox/3.6b1 GTB5\"",

"referrer" => "\"-\"",

"@timestamp" => 2015-03-12T01:24:44.000Z,

"port" => 48006,

"response" => "200",

"bytes" => 18586,

"clientip" => "14.49.42.25",

"@version" => "1",

"host" => "0:0:0:0:0:0:0:1",

"httpversion" => "1.1",

"timestamp" => "12/Mar/2015:01:24:44 +0000"

}

vi weblog.conf

input {

tcp {

port => 9900

}

}

filter{

grok {

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

}

geoip { source => "clientip" }

useragent {

source => "agent"

target => "useragent"

}

mutate {

convert => {

"bytes" => "integer"

}

}

date {

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

}

}

output {

#stdout {

# codec=>"rubydebug"

# }

elasticsearch { }

}

curl -XGET 'http://localhost:9200/logstash-\*/\_search?pretty'

{

"took" : 0,

"timed\_out" : false,

"\_shards" : {

"total" : 10,

"successful" : 5,

"skipped" : 0,

"failed" : 0

},

"hits" : {

"total" : 1,

"max\_score" : 1.0,

"hits" : [

{

"\_index" : "logstash-2015.03.12",

"\_type" : "logs",

"\_id" : "AV\_epQpnjResMXBZ7b7A",

"\_score" : 1.0,

"\_source" : {

"request" : "/articles/ppp-over-ssh/",

"agent" : "\"Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2b1) Gecko/20091014 Firefox/3.6b1 GTB5\"",

"geoip" : {

"timezone" : "Asia/Seoul",

"ip" : "14.49.42.25",

"latitude" : 37.5112,

"country\_name" : "Republic of Korea",

"country\_code2" : "KR",

"continent\_code" : "AS",

"country\_code3" : "KR",

"location" : {

"lon" : 126.97409999999999,

"lat" : 37.5112

},

"longitude" : 126.97409999999999

},

"auth" : "-",

"ident" : "-",

"verb" : "GET",

"useragent" : {

"patch" : "b1",

"os" : "Windows 7",

"major" : "3",

"minor" : "6",

"build" : "",

"name" : "Firefox Beta",

"os\_name" : "Windows 7",

"device" : "Other"

},

"message" : "14.49.42.25 - - [12/Mar/2015:01:24:44 +0000] \"GET /articles/ppp-over-ssh/ HTTP/1.1\" 200 18586 \"-\" \"Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2b1) Gecko/20091014 Firefox/3.6b1 GTB5\"",

"referrer" : "\"-\"",

"@timestamp" : "2015-03-12T01:24:44.000Z",

"port" : 48372,

"response" : "200",

"bytes" : 18586,

"clientip" : "14.49.42.25",

"@version" : "1",

"host" : "0:0:0:0:0:0:0:1",

"httpversion" : "1.1",

"timestamp" : "12/Mar/2015:01:24:44 +0000"

}

}

]

}

}

cd filebeat/data

rm registry

vi filebeat.yml

paths:

# - /var/log/\*.log

- /home/choga88/download/\*.log 🡺 실제 로그파일이 있는 절대경로 지정

output.elasticsearch:

# Array of hosts to connect to.

hosts: ["localhost:9200"]

# Optional protocol and basic auth credentials.

#protocol: "https"

#username: "elastic"

#password: "changeme"

#----------------------------- Logstash output --------------------------------

#output.logstash:

# The Logstash hosts

# hosts: ["localhost:5044"]

curl -XDELETE 'http://localhost:9200/filebeat-\*'

{"acknowledged":true}

curl -XGET 'http://localhost:9200/filebeat-\*/\_search?pretty'

{

"took" : 0,

"timed\_out" : false,

"\_shards" : {

"total" : 0,

"successful" : 0,

"skipped" : 0,

"failed" : 0

},

"hits" : {

"total" : 0,

"max\_score" : 0.0,

"hits" : [ ]

}

}

./filebeat -e

curl -XGET 'http://localhost:9200/filebeat\*/\_search?pretty'

{

"took" : 4,

"timed\_out" : false,

"\_shards" : {

"total" : 5,

"successful" : 5,

"skipped" : 0,

"failed" : 0

},

"hits" : {

"total" : 162097, => data입력되면서 total수가 증가

"max\_score" : 1.0,

"hits" : [

vi filebeat.yml

#output.elasticsearch:

# Array of hosts to connect to.

# hosts: ["localhost:9200"]

# Optional protocol and basic auth credentials.

#protocol: "https"

#username: "elastic"

#password: "changeme"

#----------------------------- Logstash output --------------------------------

output.logstash:

# The Logstash hosts

hosts: ["localhost:5044"]

vi weblog.conf

input {

#tcp {

#port => 9900

#}

beats {

port => 5044

}

}

filter{

grok {

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

}

geoip { source => "clientip" }

useragent {

source => "agent"

target => "useragent"

}

mutate {

convert => {

"bytes" => "integer"

}

}

date {

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

}

}

output {

#stdout {

# codec=>"rubydebug"

# }

elasticsearch { }

}

netstat -anlp | grep 5044

tcp6 0 0 :::5044 :::\* LISTEN 22350/java

cd filebeat/data

rm registry

curl -XDELETE 'http://localhost:9200/logstash-\*'

{"acknowledged":true}

curl -XGET 'http://localhost:9200/logstash-\*/\_search?pretty'

{

"took" : 0,

"timed\_out" : false,

"\_shards" : {

"total" : 0,

"successful" : 0,

"skipped" : 0,

"failed" : 0

},

"hits" : {

"total" : 0,

"max\_score" : 0.0,

"hits" : [ ]

}

}

./filebeat -e

curl -XGET 'http://localhost:9200/logstash-\*/\_search?pretty'

{

"took" : 9,

"timed\_out" : false,

"\_shards" : {

"total" : 25,

"successful" : 25,

"skipped" : 0,

"failed" : 0

},

"hits" : {

"total" : 19000,

"max\_score" : 1.0,

"hits" : [





