



# Beats



Filebeat



Packetbeat



Metricbeat



Winlogbeat



Logstash



Elasticsearch



Kibana

# Installing ElasticSearch

- Lunch the ubuntu 16 Server with 4gb ram,EIP.
- `#apt-get update`
- `#apt-get install openjdk-8-jre-headless)`

`# wget`

<https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-5.6.3.deb>

`#dpkg -i elasticsearch-5.6.3.deb`

- Change the vi /etc/elasticsearch/elasticsearch.yml

cluster.name : globo-clustering

Node.name : public DNS of Elasticsearch (in production only  
private DNS)

Network.host : private ip of elasticsearch / public ip

```
# Please see the documentation for further information on configuration options
# <http://www.elastic.co/guide/en/elasticsearch/reference/current/setup-configuration.html>
#
# ----- Cluster -----
#
# Use a descriptive name for your cluster:
#
cluster.name: globo-monitoring
#
# ----- Node -----
#
# Use a descriptive name for the node:
#
node.name: ec2-34-211-224-134.us-west-2.compute.amazonaws.com
#
```

- Increase the memory map count by ,  
`# sysctl -w vm.max_map_count=262144`

- Restart services

`# service elasticsearch start`

- Test by executing

`http://<ipaddress>:9200`

SG allow All traffic

By default elasticsearch runs on port 9200

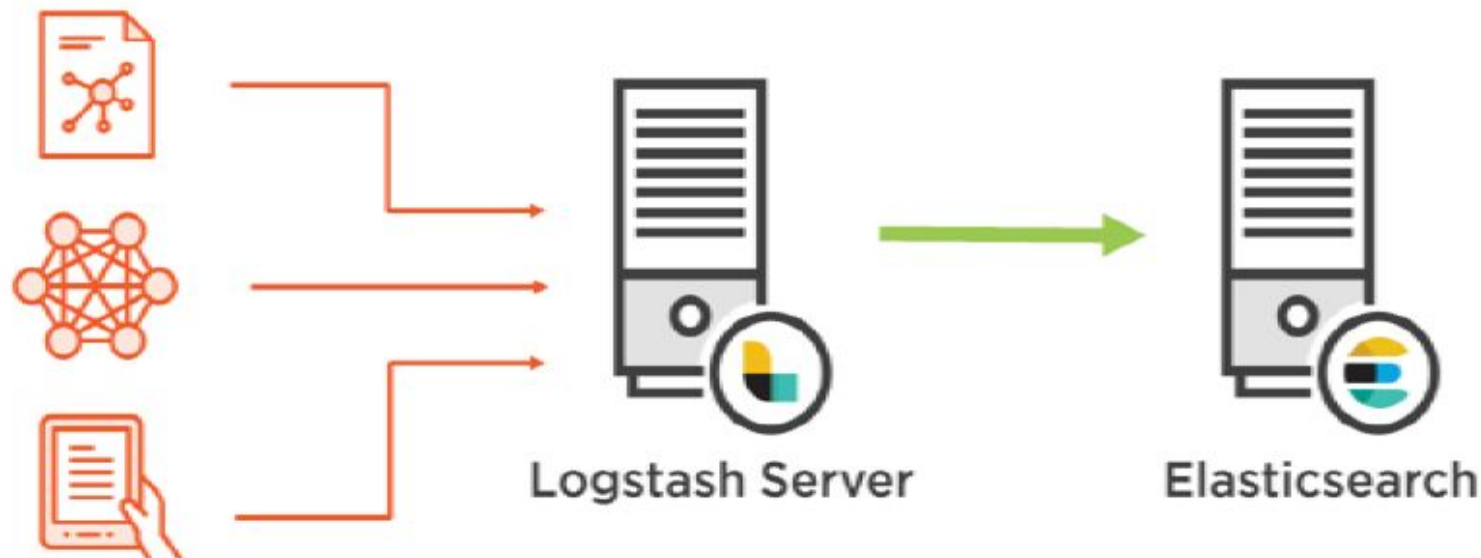
Install Logstash:

# Logstash Is a Data Collection Engine

1. Ingest

2. Enhance or modify

3. Forward



# Logstash Configuration

```
input {  
}
```



Where is data coming from?  
Logs? Beats?

```
filter {  
}
```



How should we parse the  
data? Ignore some? Modify  
any?

```
output {  
}
```



Where should we store the  
logs? Back end?  
Elasticsearch?

# Logstash Plugins



Out of the box can read apache logs, log4j files, Windows Event log, and more...

Included filters can read raw text, parse csv, or look up geo/location information by IP address, or reading json

Dozens of filters are included by default




- Lunch instant of Ubuntu 16.04 4gb ram
- `#apt-get update`
- Install java `#apt-get install openjdk-8-jre-headless`
- `#wget -qO - https://packages.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -`
- `#echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elasticsearch-5.x.list`
- Execute `#apt-get update && apt-get install logstash`
- Logstash is stored in `# /usr/share/logstash` and move to this directory using `cd`
- Now execute this command `#bin/logstash -e "input { stdin {} } output { stdout {} }"` enter some value.

# Logstash Filters

grok filter

geoip filter

93.114.45.13 - - [04/Jan/2015:05:14:33 +0000] "GET /images/web..."



Logtash:

```
# service logstash status
```

```
#cd /etc/logstash/conf.d
```

```
#vi beats.conf
```

```
input {
```

```
  beats {
```

```
    port => "5044"
```

```
  }
```

```
}
```

```
output {
```

```
  elasticsearch {
```

```
    hosts => [ "54.255.170.251:9200" ]
```

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

```
# service logstash start
```

```
#cd /usr/share/logstash
```

```
#bin/logstash -f /etc/logstash/conf.d/
```

Kibana

# Almost Complete



Elasticsearch



Logstash



Kibana



General graphing and visualization tool  
written in Node.js

Free, works great with Elasticsearch,  
includes a ton of visualization options and  
widgets

Easy to create useful dashboards and share  
them with coworkers

## Sample Map



## Events Per Day



## Windows Log



Windows Event Log Level



- Lunch instance of Ubuntu 16.04 2gb ram
- `#apt-get update`  
`#wget -qO - https://packages.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -`
- `# echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elasticsearch-5.x.list`
- `#apt-get update`
- `#apt-get install kibana`

```
#vi /etc/kibana/kibana.yml
```

```
server.host: private <ipaddress> of kibana
```

```
server.name: private <hostname> of kibana
```

```
elasticsearch.url: <elasticsearchurl> of electric search of public ip
```

```
#service kibana start
```

<http://kinbapublicip:5601>

# Instrumenting Windows Servers



File Hosting

Web Server

Email Server



RAM



CPU



Disk



Event Log

Beats

# A Complete Picture



## Winlogbeat

Windows Event Log

- Reading
- Filtering
- Enhancing
- Forwarding



## Metricbeat

All-purpose system & statistics

Broken into modules

- Apache
- HAProxy
- MongoDB
- MySQL
- NginX
- PostgreSQL
- Redis
- Zookeeper
- System logs

Install  
winlogbeat on  
windows

- [https://artifacts.elastic.co/downloads/beats/winlogbeat/winlogbeat-5.6.3-windows-x86\\_64.zip](https://artifacts.elastic.co/downloads/beats/winlogbeat/winlogbeat-5.6.3-windows-x86_64.zip)
- <https://artifacts.elastic.co/downloads/beats/winlogbeat/winlogbeat-6.3.2-windows-x86.zip>
- Extract
- Rename to [winlogbeat](#), then copy paste in c://program files
- open vi [winlogbeat](#).yml

tags: ["ap-southeast-1"]

fields:

global\_environment: production

Comment the elasticsearch

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

- From powershell install winlogbeat template by using following command
- `Cd /program files/winlogbeat`
- `Invoke-WebRequest -Method Put -InFile winlogbeat.template.json -Uri http://54.255.170.251:9200/_template/winlogbeat?pretty -ContentType application/json`
- From Powershell install winlogbeat service using following command  
`\install-service-winlogbeat.ps1`
- Start service using `start-service winlogbeat`



Service and restart the Winlogbeat on windows

service kibana start

<http://54.169.238.188:5601>

winlogbeat-\*

timestap@

Create

Discover

Visualization

save

54.255.170.251:920

EC2 Management

My Drive - Google

ELK Installation - Go

ELKZONE/beats.com

Parsing Logs with L

Kibana

maha

54.169.238.188:5601/app/kibana#/discover?\_g=()&\_a=(columns:!(\_source),index:AV\_aol1w3rb6XUZsnssy,interval:auto,query:(match\_all:()),sort:!(('@timestamp','desc'))

AppsNR DigitalEC2 Management CoWhatsApp Web

kibana

Discover

Visualize

Dashboard

Timelion

Dev Tools

Management

Collapse

12 hits

NewSaveOpenShareLast 15 minutes

Search... (e.g. status:200 AND extension:PHP)Uses lucene query syntax

Add a filter

winlogbeat-\*

Selected Fields

? \_source

Available Fields

@timestamp

@version

\_id

\_index

# \_score

\_type

beat.hostname

beat.name

beat.version

computer\_name

event\_data.Binary

November 20th 2017, 23:31:17.466 - November 20th 2017, 23:46:17.466Auto

Count

4

3

2

1

0

23:32:00

23:33:00

23:34:00

23:35:00

23:36:00

23:37:00

23:38:00

23:39:00

23:40:00

23:41:00

23:42:00

23:43:00

23:44:00

23:45:00

@timestamp per 30 seconds

Time\_source

November 20th 2017, 23:40:11.000

computer\_name: MAHA-PC keywords: Classic log\_name: Application level: Information record\_number: 6883 event\_data.param1: 3170 event\_data.param2: 0 message: Content successfully updated. Major Version: 3170 Minor Version: 0 type: wineventlog tags: ap-southeast-1, beats\_input\_codec\_plain\_applied @timestamp: November 20th 2017, 23:40:11.000 event\_id: 5,008 @version: 1 beat.name: MAHA-PC beat.hostname: MAHA-PC beat.version: 5.6.3

November 20th 2017, 23:40:11.000

computer\_name: MAHA-PC keywords: Classic log\_name: Application level: Information record\_number: 6884 event\_data.param1: 3170 event\_data.param2: 0 message: McShield successfully started. Major Version: 3170 Minor Version: 0 type: wineventlog tags: ap-southeast-1, beats\_input\_codec\_plain\_applied @timestamp: November 20th 2017, 23:40:11.000 event\_id: 5,000 @version: 1 beat.name: MAHA-PC beat.hostname: MAHA-PC beat.version: 5.6.3

Windows Taskbar

11:46 PM 11/20/2017

# Install

## Metricbeat on windows

[https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.2.4-windows-x86\\_64.zip](https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-6.2.4-windows-x86_64.zip)

Extract

Rename to metricbeat, then copy paste in c://program files

metricbeats.yml

tags: ["ap-southeast-1"]

fields:

global\_environment: production

Comment the elasticsearch

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

output.logstash:

# The Logstash hosts

hosts: ["13.229.50.243:5044"]

Winpcap download install

```
Ps > C:/programfiles/metricsbeats> Invoke-WebRequest -Method Put  
-InFile metricbeat.template.json -Uri  
http://54.255.170.251:9200/_template/metricbeat?pretty -ContentType  
application/json
```

Install-service-metricbeat.ps1

Services Start the metricbeats

# Install

## Filebeat on redhat:



**Filebeat**

Built for consuming and shipping text-based logs and data

Outputs to Elasticsearch or Logstash

Most Linux logs are text-based so it's a good fit for monitoring

Lunch redhat instance

```
#curl -L -O
```

```
https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-5.6.4-x86\_64  
.rpm
```

```
#sudo rpm -vi filebeat-5.6.4-x86_64.rpm
```

```
#cd /etc/filebeat/
```



Vi filebeat.yml

tags: ["ap-southeast-1"]

fields:

globo\_environment: production

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

output.logstash:

# The Logstash hosts

hosts: ["13.229.50.243:5044"]

```
curl -H 'Content-Type: application/json' -XPUT  
'http://52.221.196.45:9200/_template/filebeat'  
-d@/etc/filebeat/filebeat.template.json
```

```
sudo /etc/init.d/filebeat start
```

Open kibana and create pattern