

1. ELK Stack ??

ELK Stack?

- 它是一个开源的日志收集、存储、分析和可视化系统。 OpenSource
- Elasticsearch / Logstash / Kibana 是 ELK 堆栈的三个主要组件，fileBeat 是 ELK Stack 的一部分。

Component? ??

- **filebeat** : 它是一个轻量级的日志收集器，负责从源日志文件中收集日志并发送到 logstash。 (logstash 接收来自 filebeat 的日志数据，并将其发送到 Elasticsearch 存储和索引。)
- **Logstash** : filebeat 的日志数据，并将其发送到 Elasticsearch 存储和索引。
- **Elasticsearch** : logstash 的日志数据，并将其存储在 Elasticsearch 数据库中。
- **Kibana** : Elasticsearch 的日志数据，并将其可视化。

???? ????

C	H		
o	a		
m	r		
p	d		
o	w		
n	a		
e	r		
n	e		
t			

Elas tic se ar ch	8 C o r e	
Elas tic se ar ch	mem : 16GB : 64GB	8GB 1GB 1GB 1GB 1GB 1GB 1GB 1GB 1GB

E	d	S	*
l	i	S	
a	s	D	s
s	k	□	s
t		□	d
i			□
c			□
s			i
e			o
a			□
r			□
c			□
h			□
			d
			e
			a
			d
			l
			i
			n
			e
			□
			□
			n
			o
			o
			p
			□
			□
			□
			c
			f
			q
			:
			r
			/
			r
			,
			d
			e
			a
			d
			l
			i
			n
			e
			:

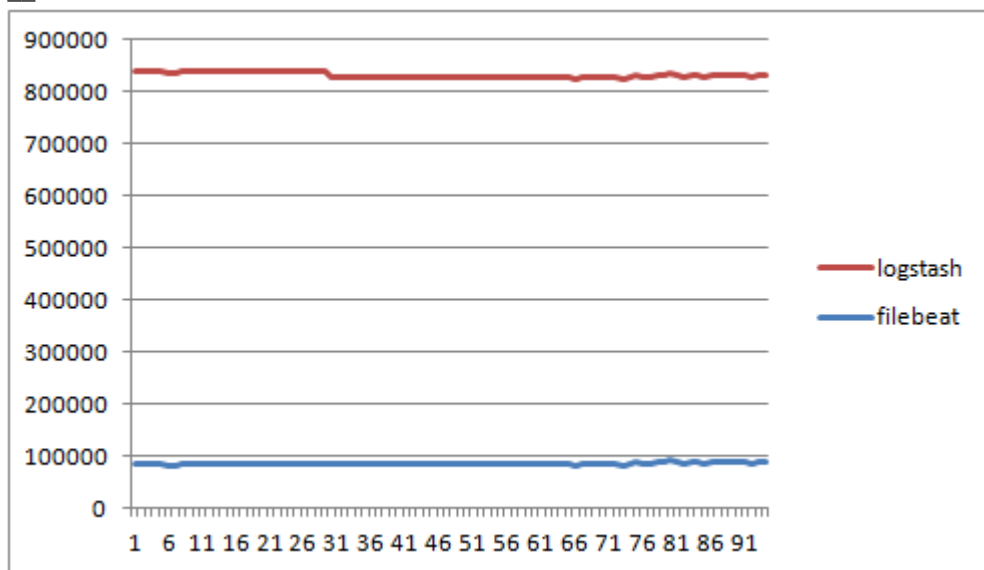
K i b a n a	c p u	8 C o r e	
K i b a n a	m e m	<div> <div></div> <div></div> <div>1</div> <div>G</div> <div>B</div> <div></div> <div>:</div> <div>4</div> <div>G</div> <div>B</div> <div></div> <div></div> </div>	
K i b a n a	d i s k	<div> <div></div> <div></div> <div></div> <div></div> </div>	
L o g s t a s h	c p u	2 C o r e	
L o g s t a s h	m e m	2 G B	

L	d		
o	i		
g	s		
s	k		
t			
a			
s			
h			

* Elasticsearch는 100GB 이하의 데이터를 저장하는 데 적합하며, 100GB 이상의 데이터를 저장하는 데는 Elasticsearch가 적합하지 않습니다.

ELK Data Flow

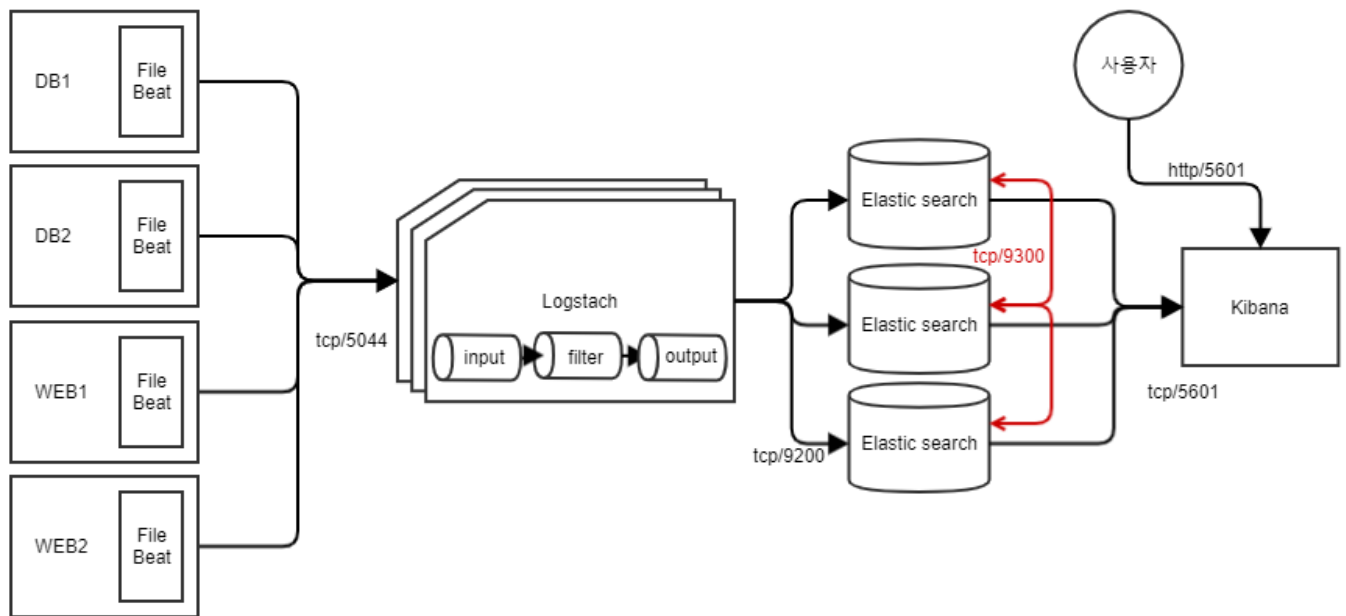
1. Node는 filebeat, logstash, Elasticsearch로 구성됩니다.
2. filebeat / logstash는 RSS를 사용하여 데이터를 수집합니다.
 - filebeat는 1MB의 데이터를 수집하여 100MB의 데이터를 수집합니다.



Elasticsearch ??

- Elasticsearch는 100GB 이하의 데이터를 저장하는 데 적합하며, 100GB 이상의 데이터를 저장하는 데는 Elasticsearch가 적합하지 않습니다.
 - **master node** : Elasticsearch는 100GB 이하의 데이터를 저장하는 데 적합하며, 100GB 이상의 데이터를 저장하는 데는 Elasticsearch가 적합하지 않습니다. master node는 100GB 이하의 데이터를 저장하는 데 적합하며, 100GB 이상의 데이터를 저장하는 데는 Elasticsearch가 적합하지 않습니다. master node는 100GB 이하의 데이터를 저장하는 데 적합하며, 100GB 이상의 데이터를 저장하는 데는 Elasticsearch가 적합하지 않습니다.

- **data node** : 1 1 1 1 1 1
- Cluster 1 1 1 1
 - 1 1 1 1 Elasticsearch 1 1 1 1 : tcp/9200
 - Elasticsearch 1 1 1 1 1 1 1 1 : tcp/9300
- 1 1 / 1 1



DBMS (like, mysql)	Elasticsearch
database	index
table	type
row	document
column	field
schema	mapping
index	index
sql	Query DSL
select	GET (Rest API 1 1)

DBMS (like, mysql)	Elasticsearch
update	PUT (Rest API 링크)
insert	POST (Rest API 링크)
delete	DELETE (Rest API 링크)

Index ?????? ?? ?? ?? : 6.7????? ?????? ??? ??

- hot : [링크](#) [링크](#) [링크](#)
- warm : [링크](#) , [링크](#) [링크](#) [링크](#)
- cold : [링크](#) [링크](#) [링크](#) , [링크](#) [링크](#) [링크](#) [링크](#)

Index ?? ??

- Create : [링크](#) [링크](#)
- close : [링크](#) [링크](#) , write [링크](#) [링크](#)
- delete : [링크](#) [링크](#)

Index ?? ??

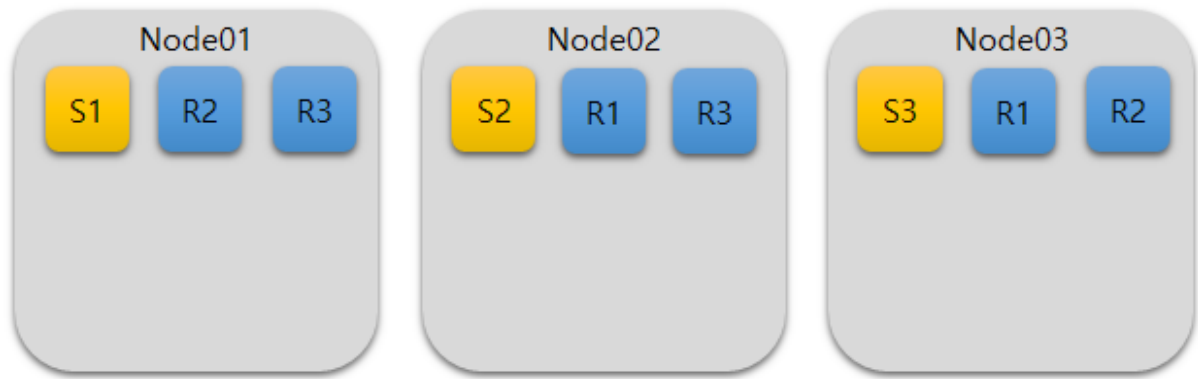
- green : [링크](#) , [링크](#) [링크](#) [링크](#) [링크](#)
- yellow : [링크](#) [링크](#) [링크](#) [링크](#) [링크](#) [링크](#)
- red : [링크](#) [링크](#) [링크](#) [링크](#) [링크](#) [링크](#) , [링크](#) [링크](#) read/write [링크](#) [링크](#)

??? ????? (??? ??? ??? ??, ????? ????? ?? ?? re-index ????? ????)

- shard :
 - Document [링크](#) [링크](#) [링크](#) (7.x [링크](#) Default [링크](#) 1 [링크](#) , 6.x [링크](#) Default [링크](#) 5)
 - [링크](#) [링크](#) [링크](#) [링크](#) [링크](#) [링크](#) . shard [링크](#) [링크](#) [링크](#) [링크](#) [링크](#) ([링크](#) [링크](#))
- replica :
 - Primary shard([링크](#)) [링크](#) [링크](#) shard(2 [링크](#)), replica(1 [링크](#)) [링크](#) [링크](#) 2x1 = 2 [링크](#) replica [링크](#) , replica [링크](#) [링크](#)

primary shard 1 2 3 4 5

◦ node = 3, shard = 2, replica = 1 2 3 4 5 6 7



Revision #6

Created 15 July 2022 16:28:00 by artop0420

Updated 30 March 2024 00:34:41 by artop0420