1. ELK Stack ??

ELK Stack?

- □ □□□ □□□ □□□ □□□□ □□□ □□□ □□□ □□ Opensource
- Elasticsearch / Logstash / Kibana□ □□ ELK□□ □□□□ □□□ , fileBeat□ □□□□□ ELK Stack□□ □□ .

Component? ??

- **filebeat** : □□□□ □□□ □□□□□□ logstash□ □□□ □□ □□ (logstash□□ □□□□□□ , □□□□□□ json□□ □□□□ □□ □□ logstash□ □□□ □□ elasticsearch□□ □□□ □ □□ □)
- **Logstash** : filebeat□□ □□ □□ , □□□□ □□□ □□□□□□ Elasticsearch□ □□□ □□
- **Elasticsearch** : logstash□□ □□□□ □□□□ DB□ □□
- **Kibana** : Elasticsearch□□ □□□ □□□□ □□□ □□

???? ????

Component	Hardware	□ □	□
		□	
			□

Elasticsearch	cpu	8Core	
Elasticsearch	mem	建议:16GB起步，推荐:64GB以上	8GB以下的内存配置是不推荐的

Elasticsearch	disk	SSD磁盘	*ssd□□□io□□□□□□deadline□□noop□□□□cfq：r/r，deadline：

Kibana	cpu	8 Core	
Kibana	mem	□□1GB□□□:4GB□□	
Kibana	disk	□□□□	
Logstash	cpu	2 Core	
Logstash	mem	2 GB	

Logstash	disk	☐☐☐☐

* Elasticsearch☐☐ ☐☐☐ ☐☐☐ ☐☐ ☐☐ ☐☐

 (☐☐ ☐☐☐ * ☐☐☐) * ☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐ ☐☐☐☐

ELK Data Flow

1. Node☐ ☐☐☐☐ filebeat☐☐☐ logstash☐ ☐☐☐☐ ElasticSearch☐ ☐☐ ☐☐☐☐ ☐☐ .
2. filebeat / logstash☐ RSS☐☐☐ ☐☐☐ ☐☐
   - ☐☐ ☐☐☐☐ ☐☐ 1Mbyte☐ ☐☐☐☐ ☐☐ ☐☐☐☐ ☐☐ , ☐ 100☐☐☐ ☐☐☐☐ ☐☐ ☐☐
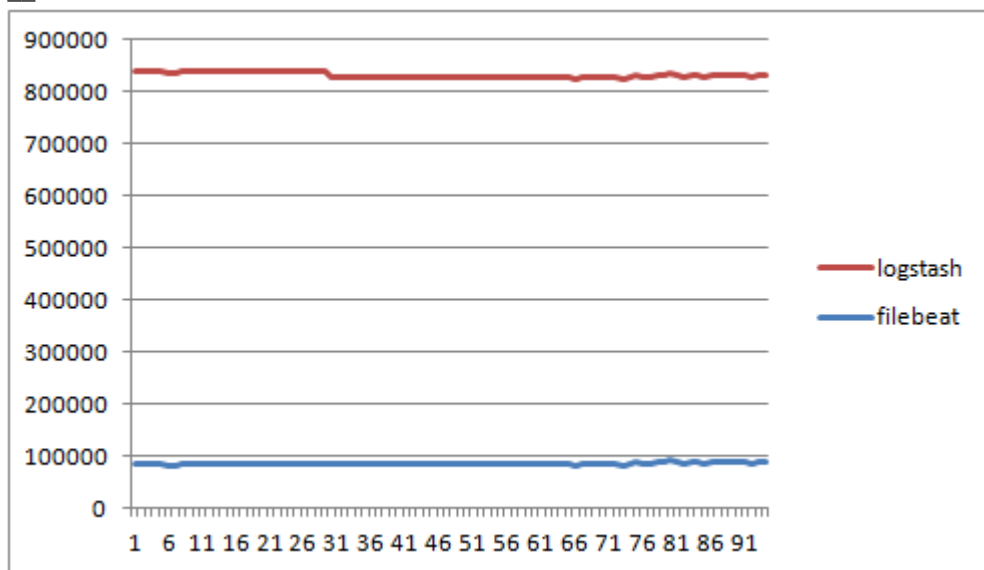
Elasticsearch ??

- Elasticsearch ☐☐ ☐☐
  - **master node** : Elasticsearch☐ ☐☐☐ ☐☐☐☐☐ , ☐☐ , ☐☐☐☐ ☐☐ ☐☐ ☐☐☐☐
    ☐☐ .. ☐☐ ☐☐☐ ☐☐☐ ☐☐ ☐☐ ☐☐☐ master☐☐☐ ☐☐☐ ☐☐
    ☐☐ ☐☐☐ ☐☐ ☐☐☐ ☐☐☐☐ 10☐☐☐ ☐☐☐ ☐☐ master/data ☐☐ ☐☐☐☐
    ☐☐☐☐☐☐ best practice

- ○ **data node** : □□ □□□□ □□□□ □□
- Cluster□□□ □□□□
  - ○ □□□□□□ Elasticsearch□□ □□□ □□ □□ : tcp/9200
  - ○ Elasticsearch□□□□ □□□ □□ □□ : tcp/9300
- □□ □□ / □□
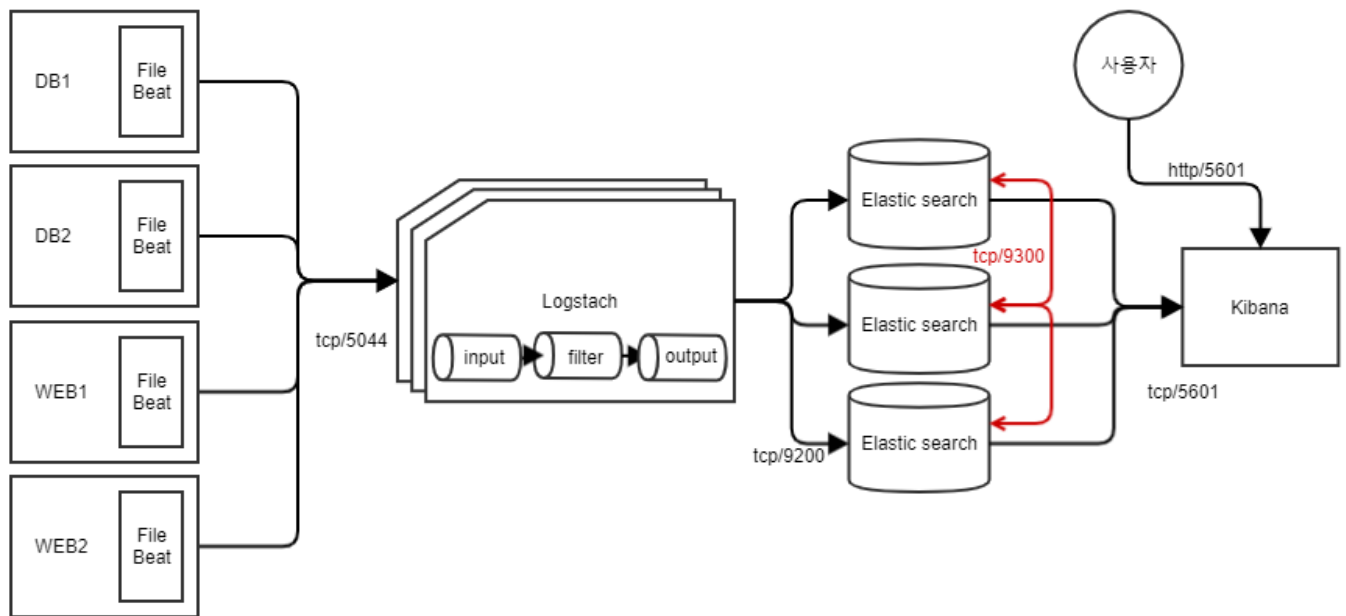
DBMS (like, mysql)	Elasticsearch
database	index
table	type
row	document
column	field
schema	mapping
index	index
sql	Query DSL
select	GET (Rest API□□)

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

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

- hot : □□□□ □□□□ □□□
- warm : □□□□□□□ , □□ □□□□ □□ □□□
- cold : □□ □□□□ □□□ , □□□ □□ □□□□ □□□

Index ?? ??

- Create : □□□ □□
- close : □□□□ □□□□ , write□ □□
- delete : □□□ □□

Index ?? ??

- green : □□ , □□□□□□ □□ □□□ □□
- yellow : □□ □□□□ □□□□□□ □□□□ □□ □□
- red : □□ □□□□ □□□ □□□□□□ □□□□ □□ □□ , □□□ □□□□ read/write□ □□□□

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

- shard :
  - Document□ □□□□ □□□□□ □□ (7.x□□ Default□ 1□ □□ , 6.x □□ Default□ 5)
  - □□□□ □□ □□□□ □□ □□□ □□ □□□ □□□ . shard□ □□□ □□□□□ □□ □□□ □□ (□□ □□)
- replica :
  - Primary shard(□□□□)□□□□ □□ shard(2□), replica(1□)□ □□□ □□ 2x1 = 2□□ replica□ □□ , replica□ □□□□

primary shard□ □□　□□□　□□　□□

- node = 3, shard = 2, replica = 1□ □□□　□□　□□□　□□□　□□　□□

Revision #6

Created 15 July 2022 16:28:00 by artop0420

Updated 30 March 2024 00:34:41 by artop0420