



Elasticsearch



Алексей Чепугов

Web-developer



elastic

Elasticsearch

Что это?

- является распределенной полнотекстовой поисковой системой с веб интерфейсом для решения широкого круга различных задач
- основанная на Lucene система.
- написан на Java
- разрабатывается компанией Elastic вместе со связанными проектами.
- наиболее часто используется в качестве интегрированного в стек ELK решения



Шай Банон

ELK Stack

Elasticsearch, Logstash, Kibana



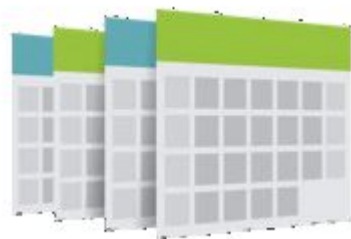
Elasticsearch - основа ELK стека. Используется для хранения и индексации данных.

Logstash - конвейер для сбора, анализа, фильтрации, нормализации данных. Позволяет обрабатывать и гибко настраивать большое число различных типов источников или потоков данных, в частности системных журналов событий.

Kibana - используется как клиент к Elasticsearch. Позволяет выполнять запросы, запрашивать, обрабатывать и визуализировать данные.

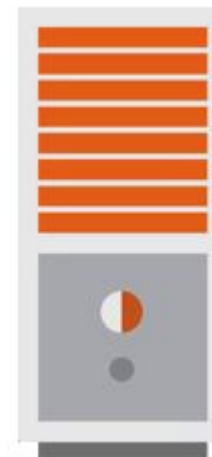
Хранение данных

Структура

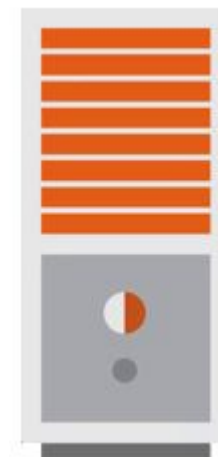


Хранение данных

Масштабирование. SQL



master



replica

Хранение данных

Elasticsearch. Фрагментирование



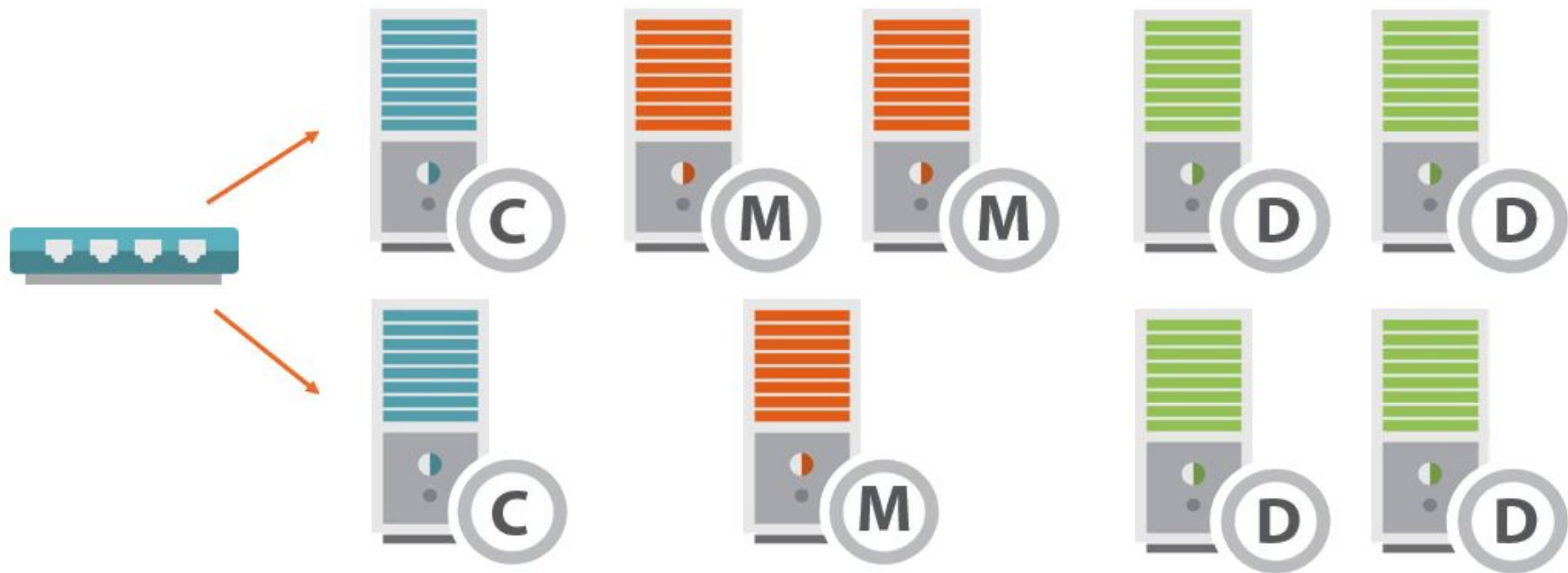
Хранение данных

Elasticsearch. Репликация



Elasticsearch

Конфигурация кластера



Elasticsearch

Кворум

auto



Elasticsearch

Elasticsearch is everywhere

Особенности

Преимущества и недостатки



- Масштабируемость разделением на фрагменты, репликация; простота их использования
- REST API
- Полнотекстовый поиск с настраиваемой системой ранжирования, подсветкой результатов
- Фильтрация документов (Percolation)



- Непривычный формат запросов
- Сложность понимания понятий "контекстов", "признаков" и "анализаторов",
- Отсутствие транзакций в обычном понимании
- Ограниченное использование объединений (JOIN`s)

```
mkdir -p /opt/elasticsearch; cd /opt/elasticsearch
# скачаем архив с официального сайта Elasticsearch и контрольную сумму
wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.1.1.tar.gz
wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.1.1.tar.gz.sha512
# проверка - проверка
shasum -a 512 -c elasticsearch-6.1.1.tar.gz.sha512
# ты умеешь запускать из архива? я - нет
tar -xzf elasticsearch-6.1.1.tar.gz

### Еще немного магии и мы закончим ###
cd /opt/elasticsearch/elasticsearch-6.1.1/
cp -R /opt/elasticsearch/elasticsearch-6.1.1/ /opt/elasticsearch/

# для отъявленных перфекционистов
useradd -M elasticsearch
usermod -L elasticsearch
mkdir -p /var/run/opt-elasticsearch/
chown -R elasticsearch:elasticsearch /var/run/opt-elasticsearch/
chown -R elasticsearch:elasticsearch /opt/elasticsearch/
```

Elasticsearch

Установка. 2



```
# я говорил, что Elasticsearch на Java?  
yum install java-1.8.0-openjdk
```

```
### Музыкальная пауза ###
```

```
# Надо больше золота памяти  
sysctl -w vm.max_map_count=262144
```

```
# Поехали!  
systemctl daemon-reload  
systemctl restart opt-elasticsearch
```

Elasticsearch

=^.^=

auto

RIA

<http://localhost:9201>

<http://localhost:9201/>

<http://localhost:9201/>

<http://localhost:9201/>

<http://localhost:9201/>

http://localhost:9201/_cat

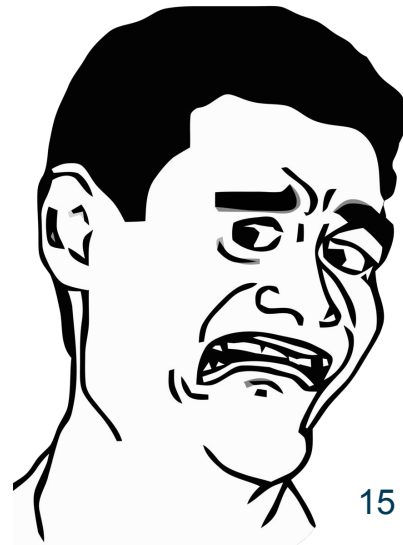


Elasticsearch

Работа с данными. Консоль



```
curl -XPOST localhost:9201/logs/logs/1 -d '{"error": {"type": 42, "message": "Я  
был слишком ленив и не придумал нормальный текст"}}' -H 'Content-Type:  
application/json'
```



**ТЫ ПРИХОДИШЬ И ПРОСИШЬ ЧТО ТО У
МЕНЯ, НО ТЫ ПРОСИШЬ БЕЗ УВАЖЕНИЯ**



Kibana

Установка



```
wget https://artifacts.elastic.co/downloads/kibana/kibana-6.1.1-linux-x86_64.tar.gz
wget https://artifacts.elastic.co/downloads/kibana/kibana-6.1.1-linux-x86_64.tar.gz.sha512
shasum -a 512 -c elasticsearch-6.1.1.tar.gz.sha512
tar -xzf kibana-6.1.1-linux-x86_64.tar.gz
cd kibana/bin
./kibana
```

Elasticsearch

Работа с данными



<https://raw.githubusercontent.com/a-chepugov/es-lesson/master/es/%D0%97%D0%B0%D0%BF%D1%80%D0%BE%D1%81%D1%8B>



e-mail:

oleksii.chepugov@ria.com

материалы:

<https://github.com/a-chepugov/es-lesson>