Документация по ELK

# Ссылки на документацию

<https://qbox.io/blog/parsing-logs-using-logstash>

тестирование в GROK фильтров

<http://grokconstructor.appspot.com/do/match#result>

# Запуск ELK

## elasticsearch

настройка

elasticsearch.yml

network.host: art-elk

http.port: 9200

если не настроить, то будет работать по 127.0.0.1 (со внешних машин не достучаться)

Запуск elasticseacrh.bat

! elasticsearch устанавливаем на сервере с базой-хранилищем логов (sdlogs01)

## Logstash

Запуск logstash.bat -f c:\logs\myconfig.config

где myconfig.config – путь к конфигурационному файлу с описанием pipeline из файла с логом в elasticseacrh (см. ниже пример).

! Logstash устанавливаем на сервере с логами (sdecb01/ssecb01)

kibana

настройка

kibana.yml

server.host: "localhost"

elasticsearch.url: <http://ART-ELK:9200>

прописывается хост к elasticsearch

запуск kibana.bat

!? kibana устанавливаем на сервере с базой-хранилищем логов (sdlogs01)

Пример конфигурационного файла Logstash

|  |
| --- |
| **input** {  file {  # Give path to your log file  **path** => 'c:/logs/mylogfile.log'  # Grok pattern for multiline log (stacktrace etc)  **codec** => **multiline** {  **pattern** => "^%{TIMESTAMP\_ISO8601} "  **negate** => true  **what** => "previous"  }  }  }  **filter** {  **grok** {  # Log Example  #2017-11-28 23:23:14.374 ERROR 6108 --- [main] o.s.b.l.LoggingApplicationListener : Cannot set level…  #2017-11-28 23:23:14.456 INFO 6108 --- [main] r.c.c.s.SupplierApp : Starting SupplierApp o..  **match** => { "message" => "%{TIMESTAMP\_ISO8601:log-timestamp}(%{SPACE})+%{LOGLEVEL:log-level}((( EXPERTISEID=)%{DATA:log-key})\*) %{DATA:log-pid} (---) \[%{DATA:log-method}\] %{DATA:log-class} \:%{GREEDYDATA:log-message}"}  # Some specific field for each entry  **add\_field** => {"log-system"=>"ecb"}  **add\_field** => {"log-env"=>"uat"}  }  }  **output** {  **elasticsearch** {  # Elastic server IP and port  **hosts** => ["art-elk:9200"]  # index name (ecb-uat-2017.12.06)  **index** => "ecb-uat-%{+YYYY.MM.dd}"  }  } |

Наиболее часто используемые типы

TIMESTAMP\_ISO8601 – timstamp 2017-11-28 23:23:14.374

LOGLEVEL – WARN|ERROR|INFO …

NOTSPACE – Любые непустые символы

SPACE – Пробел

DATA – что-то, что ограничивается «6108 ---»

GREEDYDATA

WORD

NUMBER

INT

# Mandatory fields

Все поля лога начинаются с “log-“. Это нужно, чтобы можно было отличить их от стандартных полей

|  |  |  |
| --- | --- | --- |
| **#** | **Field name** | **Description** |
| 1 | log-timestamp | Timestamp возникновения события |
| 2 | log-level | Уровень события (INFO/WARNING/ERROR/DEBUG etc) |
| 3 | log-key | Ключ объекта по которому логируется работа (Например, код клиента или код договора)  Для DMS - Numauto |
| 4 | log-message | Сообщение лога |

Рекомендованные названия полей (для совместимости логов)

|  |  |  |
| --- | --- | --- |
| **#** | **Field name** | **Description** |
| 1 | log-method | Название метода, в котором произошло событие |
| 2 | log-class | Навзание класса |
| 3 | log-pid | Код/название потока |
| 4 | log-system | Название системы логирования |
| 5 | log-env | Название среды (dev/uat/prod) |

# Remove elasticsearch index

Узнать о текущих индексах

<http://art-elk:9200/_cat/indices?v>

удалить индекс

http: DELETE http://art-elk:9200/index\_name

curl -X DELETE http://art-elk:9200/index\_name

(допускаются \*)

В kibana: DevTools/console

DELETE / index\_name

{

"query": {

}

}

(допускаются \*)

# Index naming convention

Наименование индексов происходит по правилу

I\_ENV\_SERVER\_APP

Где

ENV- название среды DEV/UAT/PROD

SERVER – название сервера. Например SDECB01/SSECB01

APP – Название основного приложения, которое сохраняет логи. Например DMS

Пример

I\_UAT\_SDECB01\_DMS

I\_PROD\_SSECB01\_DMS

# Role management

В ELK определяются роли доступа к индексам. Из-за специфики настройки ролей, доступ к индексам может быть задан следующим образом

I\_ENV\_SERVER\_\*

I\_ENV\_ \*

Т.е. «\*» устанавливается только в хвостовой части. Это следует учитывать при планировании ролей

Пример

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **#** | **SYSTEM** | **ENV** | **SERVER** | Role1 | Role2 | .. | RoleN |
| 1 | DMS | UAT | SDECB01 | + |  |  |  |
| 2 | Cetelem.Online | UAT | SDCOAPP01 | + |  |  |  |
| 3 | DMS | PROD | SSECB01 |  | + |  |  |
| 4 | Cetelem.Online | PROD | SSCOAPP01 |  | + |  |  |

# Filebeat greater than logstash

ttps://logz.io/blog/filebeat-vs-logstash/