

# ELK: система логирования и визуализации



# Roadmap

- 1. Создание docker-контейнера ELK
- 2. Настройка отправки syslog на iek.ru
- 3. Логирование в syslog и ES



# 1. Docker

```
docker pull sebp/elk
```

```
docker run --restart=always -p 5601:5601 -p 9200:9200  
-p 5044:5044 -e TZ=Europe/Moscow --hostname  
elk.dev.local --name elk.dev.local -d sebp/elk
```

```
vim /etc/sysctl.conf
```

```
make entry vm.max_map_count=262144
```



## 2. Настройка syslog

```
vim /etc/rsyslog.d/50-default.conf
```

```
# Log anything (except mail, auth, cron) of level info or higher.
```

```
# Don't log private authentication messages!
```

```
*.info;mail.none;authpriv.none;cron.none
```

```
/var/log/messages
```

установка filebeat для отправки файлов

# 3. Логирование в syslog и ES





# syslog: PHP

- `syslog(int $уровень, string $сообщение);`
- `syslog(LOG_ERR, "[LK 2.0][ws:order.detail.get][error][user:20881][uri:http://europes.iek.local/Plazma/hs/lk20/order_detail/0e10070b-e70b-11e8-8118-00155d049f73]: curl error Couldn't resolve host 'europes.iek.local'");`
- `syslog(LOG_INFO, "[LK 2.0][ws:order.detail.get][info:ok][user:20881][uri:http://mab.iek.local/DubrovinPlazma/hs/lk20/order_detail/591da78a-fd06-11e8-8120-00155d040154]");`



# syslog: bash, node














#!/bin/bash

- logger "[LK 2.0] Hello from bash"

- NodeJS

nodejs ~/myapp.js 2>&1 | logger &  
... или npm-пакет

# syslog: bash, node

 kibana	2019-01-23 03:46:33.000	[uri:http://mab.iek.local/DubrovinPlazma/hs/lk20/order_detail/591da78a-fd06-11e8-8120-00155d040154] [LK 2.0][ws:order.detail.get][error][user:20881] [uri:http://europes.iek.local/Plazma/hs/lk20/order_detail/0e10070b-e70b-11e8-8118-00155d049f73]: curl error Couldn't resolve host 'europes.iek.local'	09 PM
 Discover	2019-01-23 03:46:35.000	[LK 2.0][ws:order.detail.get][info:ok][user:20881] [uri:http://mab.iek.local/DubrovinPlazma/hs/lk20/order_detail/591da78a-fd06-11e8-8120-00155d040154]	
 Visualize	2019-01-23 03:48:33.000	[LK 2.0][ws:order.detail.get][error][user:20881] [uri:http://europes.iek.local/Plazma/hs/lk20/order_detail/0e10070b-e70b-11e8-8118-00155d049f73]: curl error Couldn't resolve host 'europes.iek.local'	Wed 23
 Dashboard	2019-01-23 03:48:34.000	[LK 2.0][ws:order.detail.get][info:ok][user:20881] [uri:http://mab.iek.local/DubrovinPlazma/hs/lk20/order_detail/591da78a-fd06-11e8-8120-00155d040154]	
 Timelion	2019-01-23 03:50:52.000	[LK 2.0][ws:order.detail.get][info:ok][user:20881] [uri:http://mab.iek.local/DubrovinPlazma/hs/lk20/order_detail/591da78a-fd06-11e8-8120-00155d040154]	03 AM
 Canvas	2019-01-23 03:50:53.000	[LK 2.0][ws:order.detail.get][error][user:20881] [uri:http://europes.iek.local/Plazma/hs/lk20/order_detail/0e10070b-e70b-11e8-8118-00155d049f73]: curl error Couldn't resolve host 'europes.iek.local'	
 Machine Learning	2019-01-23 03:53:02.000	[LK 2.0] Hello from bash	06 AM
 Infrastructure	2019-01-23 03:55:36.000	[LK 2.0][ws:order.detail.get][error][user:20881] [uri:http://europes.iek.local/Plazma/hs/lk20/order_detail/0e10070b-e70b-11e8-8118-00155d049f73]: curl error Couldn't resolve host 'europes.iek.local'	
 Logs	2019-01-23 03:55:38.000	[LK 2.0][ws:order.detail.get][error][user:20881] [uri:http://europes.iek.local/Plazma/hs/lk20/order_detail/0e10070b-e70b-11e8-8118-00155d049f73]: curl error Couldn't resolve host 'europes.iek.local'	09 AM
 APM			
 Dev Tools			
 Monitoring			
 Management			





# ES: кастомные логи

POST\_bulk

```
{ "index" : { "_index" : "1c-exchange-ws", "_type" : "_doc" } }  
{ "guid": "cbd40940-a92e-4374-91e6-295d46eb2cd1",  
"method": "POST", "body": "... some data ..." }
```

```
{ "index" : { "_index" : "1c-exchange-ws", "_type" : "_doc" } }  
{ "guid": "ad2f7319-12fa-4902-8e34-93934172389f", "method":  
"GET", "response": "... some data ..." }
```

# ES: кастомные логи

```
GET /1c-exchange-ws/_search
{
  "query": { "match_all": {} }
}
```

```
1 {
2   "took": 1,
3   "timed_out": false,
4   "_shards": {
5     "total": 5,
6     "successful": 5,
7     "skipped": 0,
8     "failed": 0
9   },
10  "hits": {
11    "total": 2,
12    "max_score": 1.0,
13    "hits": [
14      {
15        "_index": "1c-exchange-ws",
16        "_type": "_doc",
17        "_id": "1k1WYd2gBV2Qvaw6Udr8l",
18        "_score": 1.0,
19        "_source": {
20          "guid": "cbd40940-a92e-4374-91e6-295d46eb2cd1",
21          "method": "POST",
22          "body": "... some data ..."
23        }
24      },
25      {
26        "_index": "1c-exchange-ws",
27        "_type": "_doc",
28        "_id": "10k1WYd2gBV2Qvaw6Udr8l",
29        "_score": 1.0,
30        "_source": {
31          "guid": "ad2f7319-12fa-4902-8e34-93934172389f",
32          "method": "GET",
33          "response": "... some data ..."
34        }
35      }
36    ]
37  }
38 }
39
```

```
hostel-desktop :: ~/tmp/n-s » curl -sH 'Content-Type: application/json' -XGET
localhost:9200/1c-exchange-ws/_search' -d '{ "query": { "match_all": {} } }'
| jq ".
{
  "hits": {
    "hits": [
      {
        "_source": {
          "body": "... some data ...",
          "method": "POST",
          "guid": "cbd40940-a92e-4374-91e6-295d46eb2cd1"
        },
        "_score": 1,
        "_id": "1k1WYd2gBV2Qvaw6Udr8l",
        "_type": "_doc",
        "_index": "1c-exchange-ws"
      },
      {
        "_source": {
          "response": "... some data ...",
          "method": "GET",
          "guid": "ad2f7319-12fa-4902-8e34-93934172389f"
        },
        "_score": 1,
        "_id": "10k1WYd2gBV2Qvaw6Udr8l",
        "_type": "_doc",
        "_index": "1c-exchange-ws"
      }
    ]
  },
  "max_score": 1,
  "total": 2
},
"_shards": {
  "failed": 0,
  "skipped": 0,
  "successful": 5,
  "total": 5
},
"timed_out": false,
"took": 1
}
```

# ES: КАСТОМНЫЕ ЛОГИ

The screenshot displays the Kibana search interface. On the left is the navigation sidebar with the 'kibana' logo and menu items: Discover, Visualize, Dashboard, Timelion, Canvas, Machine Learning, Infrastructure, Logs, APM, Dev Tools, Monitoring, and Management. The main search bar contains the query `>_ guid:cbd40940-a92e-4374-91e6-295d46eb2cd1`. Below the search bar, the index is set to `1c-exchange-ws`. The search results show a single hit with the following details:

- `_source`:
  - `guid`: `cbd40940-a92e-4374-91e6-295d46eb2cd1` (highlighted)
  - `method`: `POST`
  - `body`: `.. some data ...` (highlighted)
  - `_id`: `1kWYd2gBV2Qvaw6Udr81`
  - `_type`: `_doc`
  - `_index`: `1c-exchange-ws`
  - `_score`: `1.438`

Below the search results, there are tabs for `Table` and `JSON`. The `JSON` tab is selected, showing the document structure:

```
1 {
2   "index": "1c-exchange-ws",
3   "type": "_doc",
4   "id": "1kWYd2gBV2Qvaw6Udr81",
5   "version": 1,
6   "_score": 1.4384104,
7   "_source": {
8     "guid": "cbd40940-a92e-4374-91e6-295d46eb2cd1",
9     "method": "POST",
10    "body": ".. some data ..."
11  },
12  "highlight": {
13    "guid": [
14      "@kibana-highlighted-field@cbd40940@/kibana-highlighted-field@-@kibana-highlighted-field@a92e@/kibana-highlighted-field@-@kibana-highlighted-field@4374@/kibana-highlighted-field@-@kibana-highlighted-field@91e6@/kibana-highlighted-field@-@kibana-highlighted-field@295d46eb2cd1@/kibana-highlighted-field@"
15    ]
16  }
17 }
```

# Кейсы

- Apache/Nginx log => статистика обращения к API `"/api/planresidues/"`
- «Какие данные отправились/пришли в 1С» - для дебага
- «Через какое время с момента размещения заказа партнер может подтвердить резерв пути в ЛК» (задача 193748)