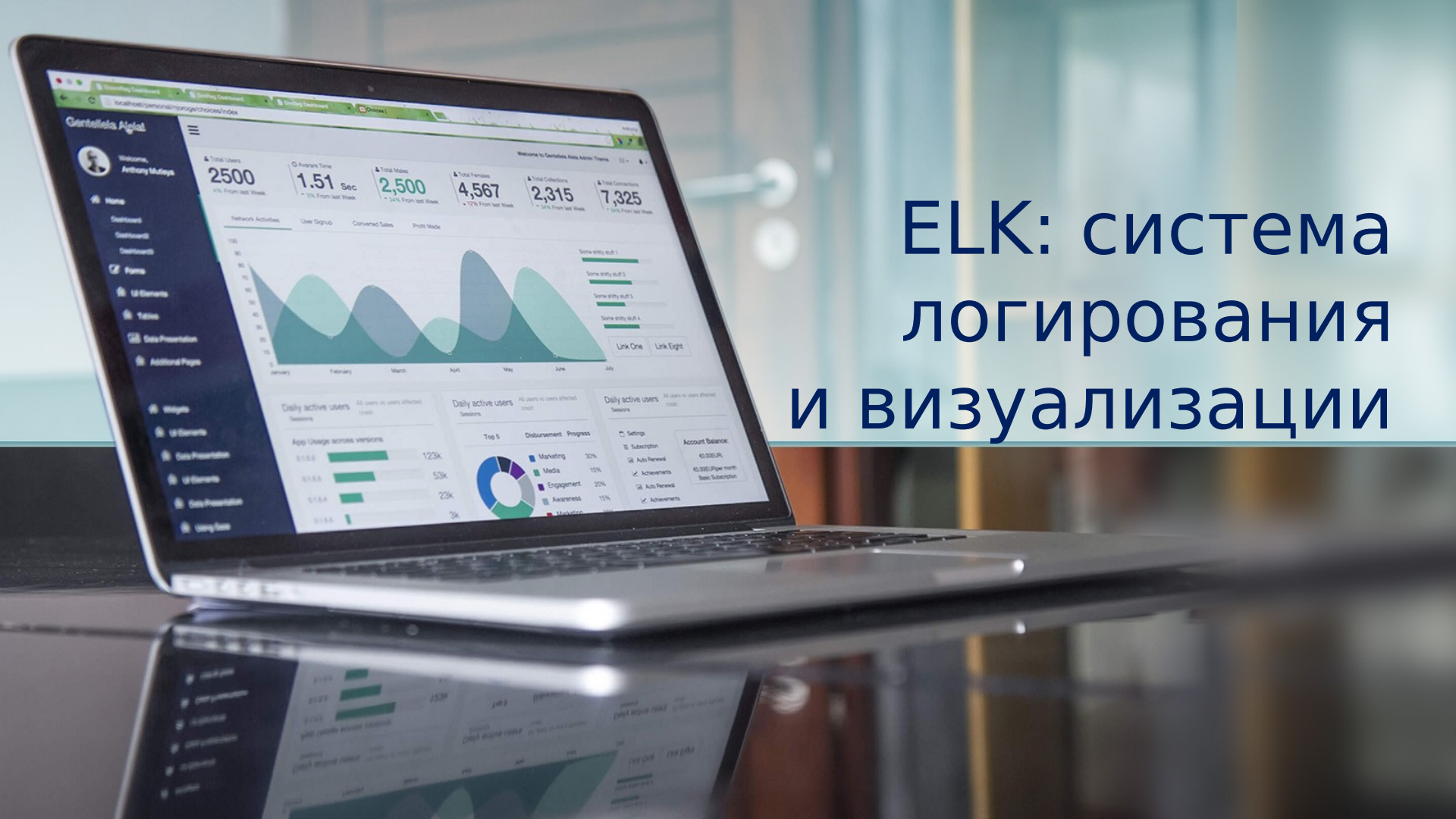
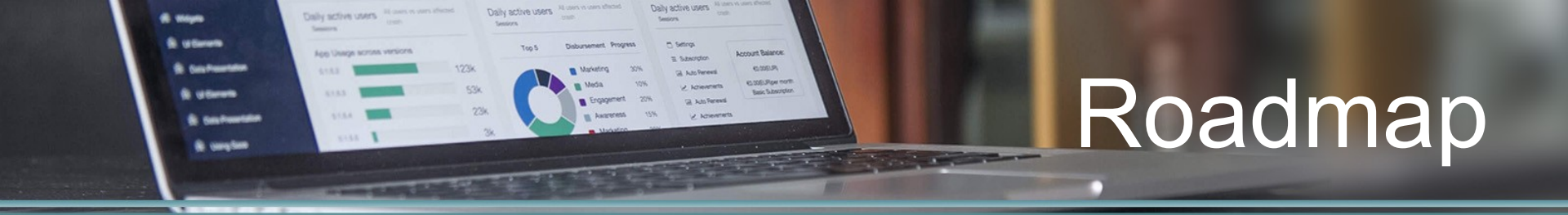
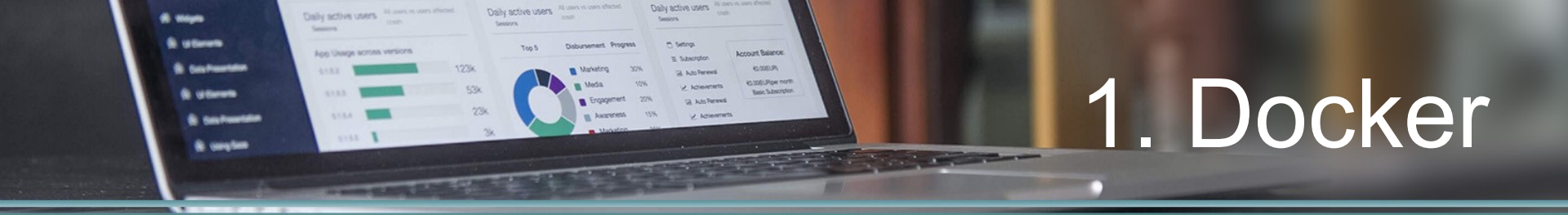

ELK: система
логирования
и визуализации



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

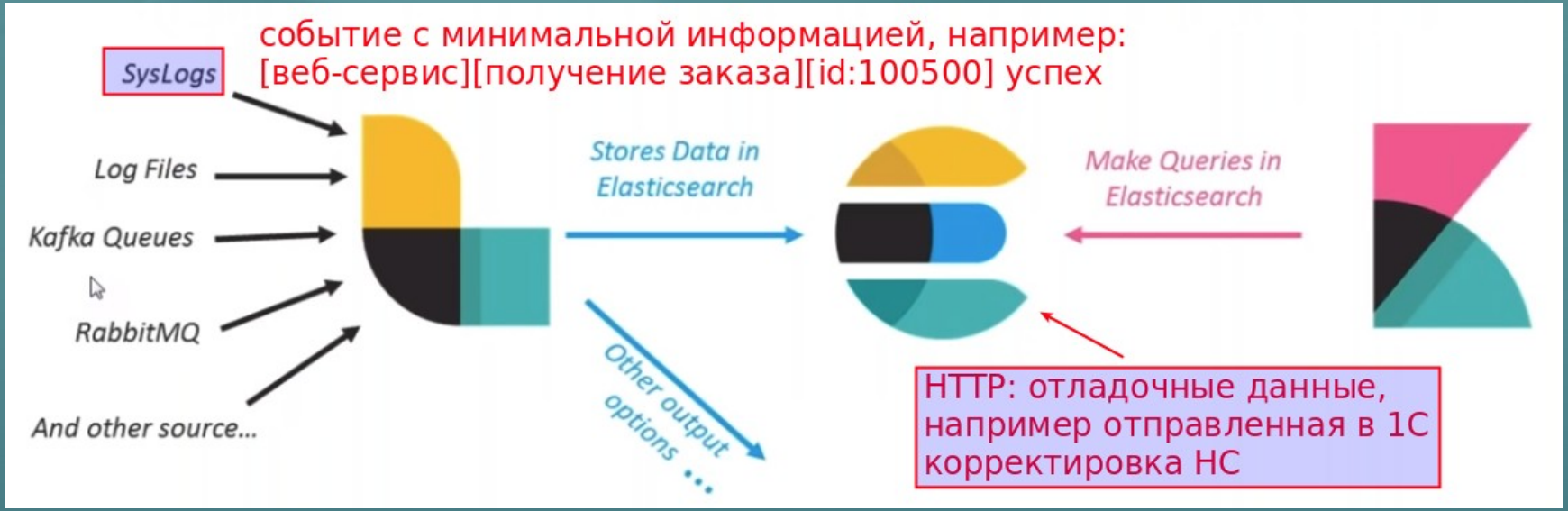
vim /etc/rsyslog.d/50-default.conf

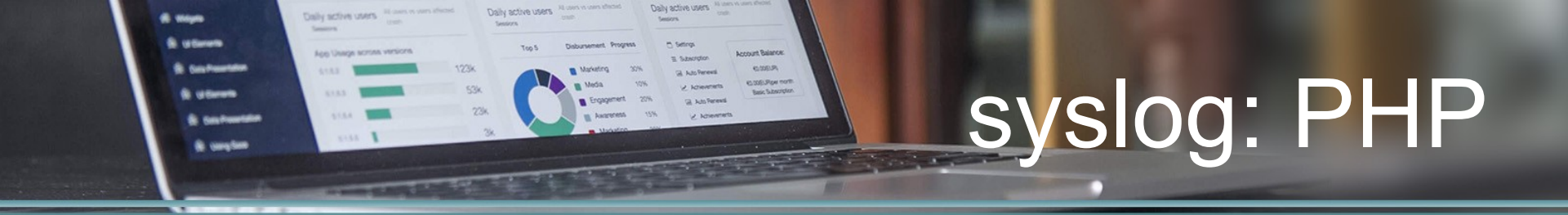
Log anything (except mail, auth, cron) of level info or higher.
Don't log private authentication messages!

*.info;mail.none;authpriv.none;cron.none
/var/log/messages

установка filebeat для отправки файлов

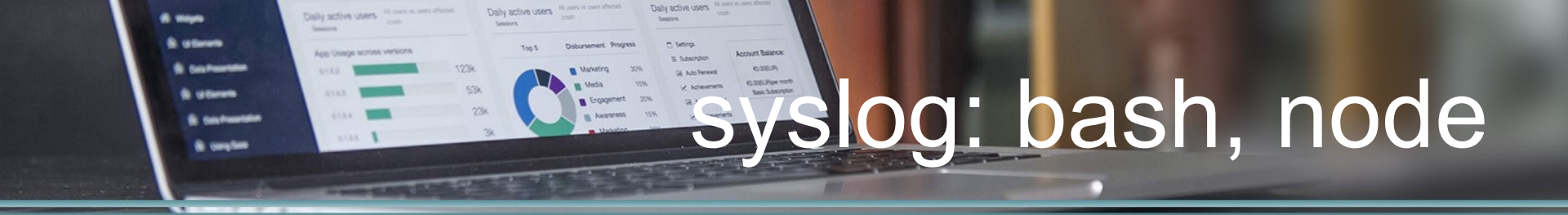
3. Логирование в syslog и ES





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]");

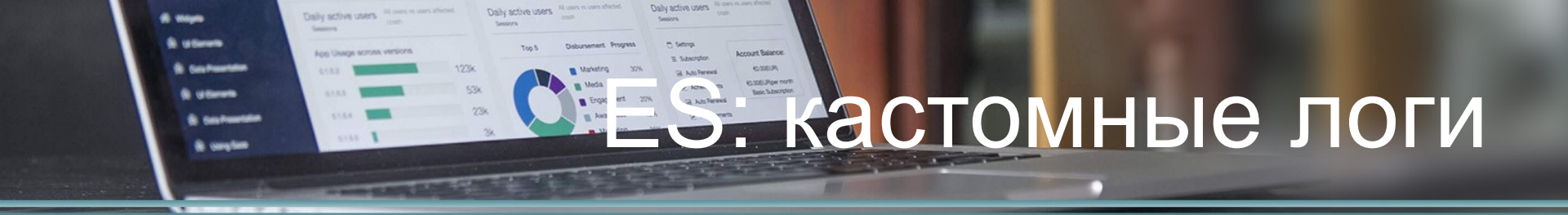


syslog: bash, node

#!/bin/bash

- logger "[LK 2.0] Hello from bash"
- NodeJS
  nodejs ~/myapp.js 2>&1 | logger &
  … или npm-пакет

syslog: bash, node



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

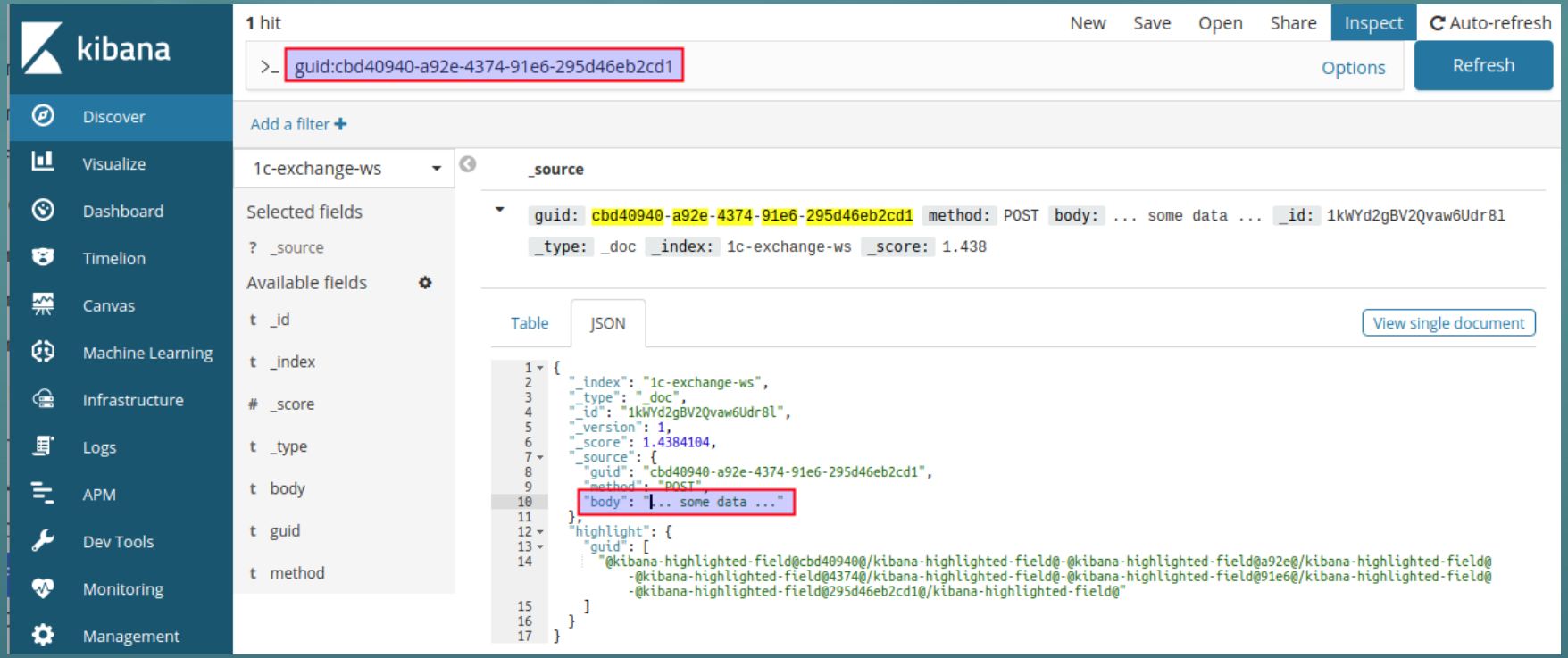
```
GET /1c-exchange-ws/_search
{
  "query": { "match_all": {} }
}
```

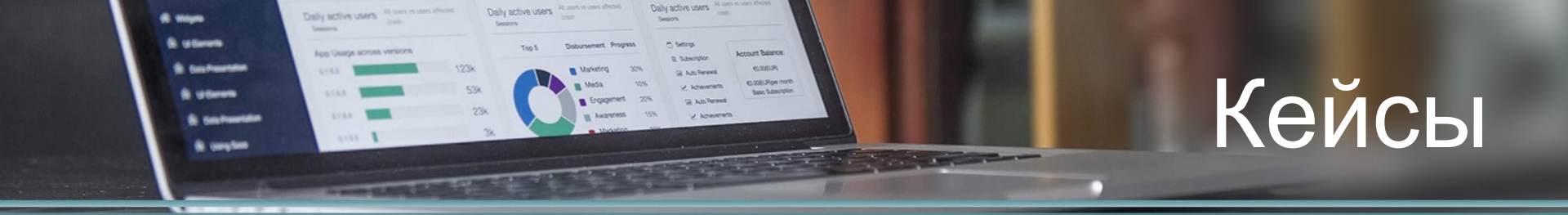

```
{
  "took" : 1,
  "timed_out" : false,
  "_shards" : {
    "total" : 5,
    "successful" : 5,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : 2,
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "1c-exchange-ws",
        "_type" : "_doc",
        "_id" : "1kWYd2gBV2Qvaw6Udr8l",
        "_score" : 1.0,
        "_source" : {
          "guid" : "cbd40940-a92e-4374-91e6-295d46eb2cd1",
          "method" : "POST",
          "body" : "... some data ..."
        }
      },
      {
        "_index" : "1c-exchange-ws",
        "_type" : "_doc",
        "_id" : "10WYd2gBV2Qvaw6Udr8l",
        "_score" : 1.0,
        "_source" : {
          "guid" : "ad2f7319-12fa-4902-8e34-93934172389f",
          "method" : "GET",
          "response" : "... some data ..."
        }
      }
    ]
  }
}
```


```
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": "1kWYd2gBV2Qvaw6Udr8l",
        "_type": "_doc",
        "_index": "1c-exchange-ws"
      },
      {
        "_source": {
          "response": "... some data ...",
          "method": "GET",
          "guid": "ad2f7319-12fa-4902-8e34-93934172389f"
        },
        "_score": 1,
        "_id": "10WYd2gBV2Qvaw6Udr8l",
        "_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





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)