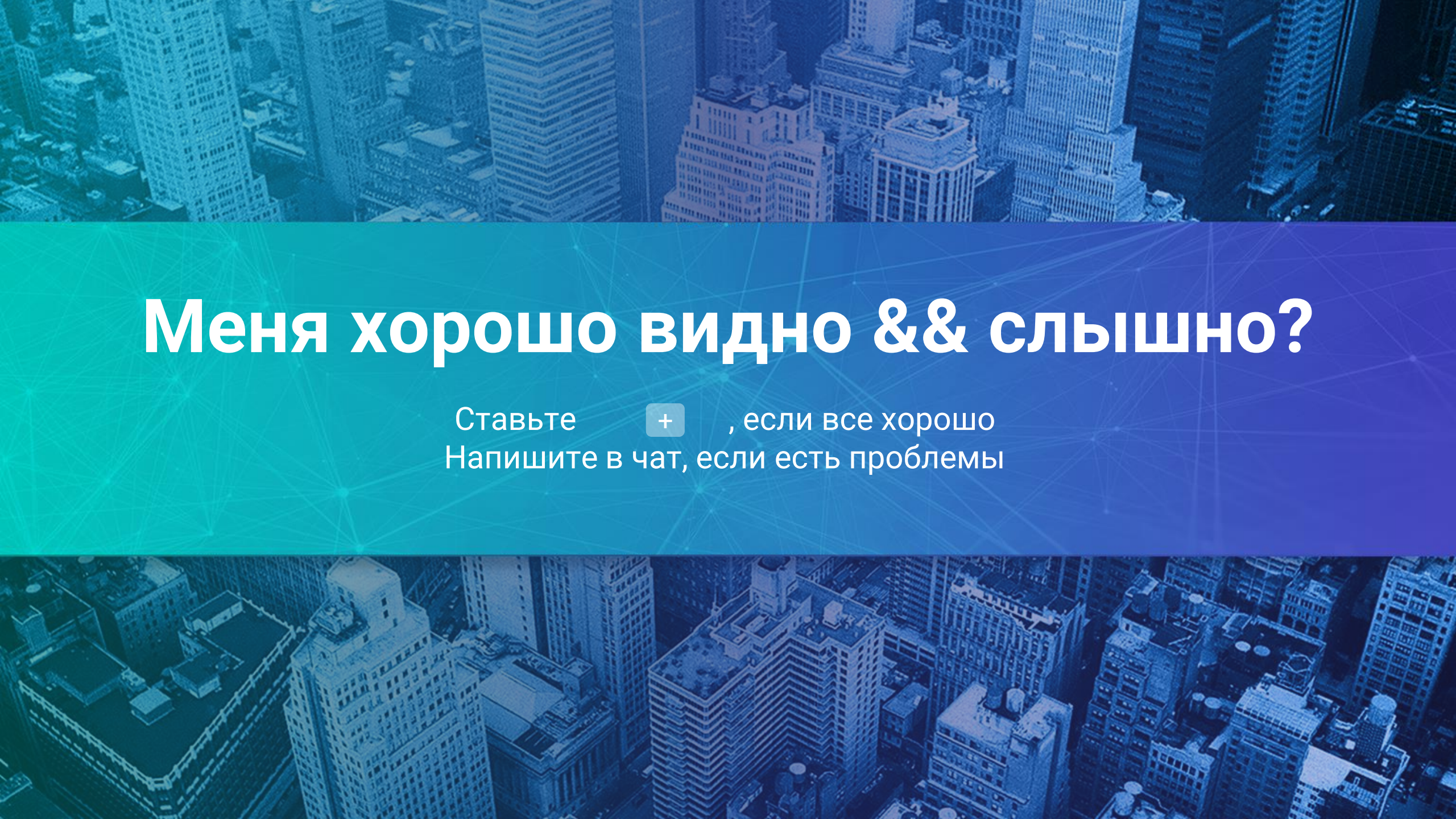

OTUS
ОНЛАЙН-ОБРАЗОВАНИЕ
Онлайн-образование

Проверить, идет ли запись!



Меня хорошо видно && слышно?

Ставьте + , если все хорошо

Напишите в чат, если есть проблемы

Logstash

Елагин Алексей

Безработный

@sh1kel

Правила вебинара

Активно участвуем

Задаем вопрос в чат или голосом

Off-topic обсуждаем в Slack #канал группы или #general

Вопросы вижу в чате, могу ответить не сразу

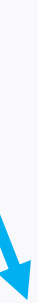
Карта курса

1 Классическое логирование в Linux

2 Системы логирования (ELK, EFK, Graylog2)

3 ELK стэк

Мы тут



4 Logstash

5 Graylog2

Маршрут вебинара

Возможности Logstash

Особенности эксплуатации

Практика

Рефлексия

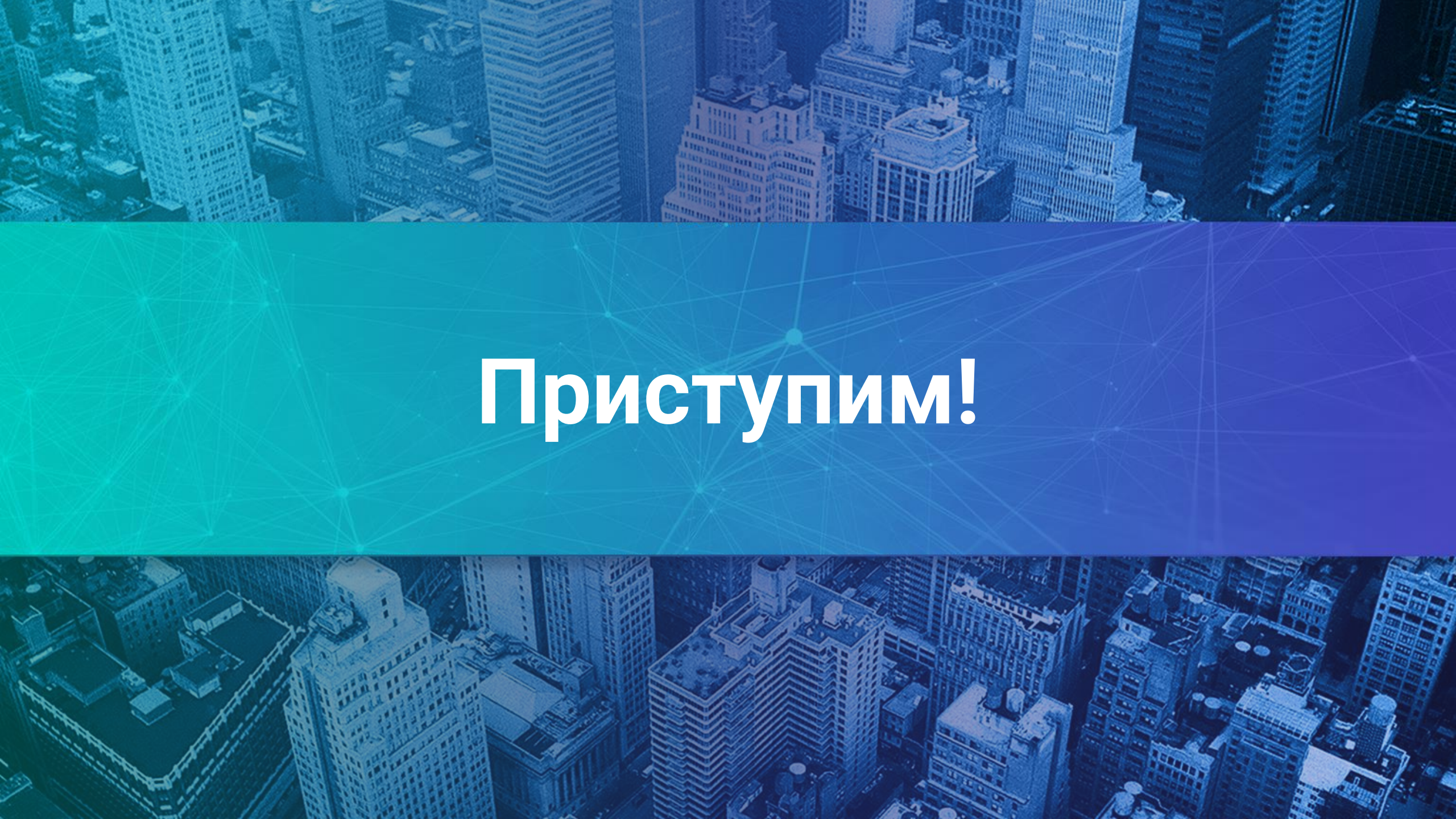
Цели вебинара | После занятия вы сможете

1. Оценить задачи, решаемые инструментом
2. Писать конфигурацию
3. Смотреть результаты в Kibana

Смысл | Зачем вам это уметь

1. Logstash – мощный инструмент по преобразованию логов, но его надо уметь конфигурировать

2. Правильный подход к выбору инструментов позволит эффективно решать задачи обработки логов


Приступим!

Кратко про Logstash

Плюсы

1. Куча regex паттернов
2. Поддерживает много разных источников данных

3. Поддерживает плагины
4. Централизованный подход
5. Поддерживает много разных баз данных и протоколов для выходных данных
6. Работает по http

Кратко про Logstash

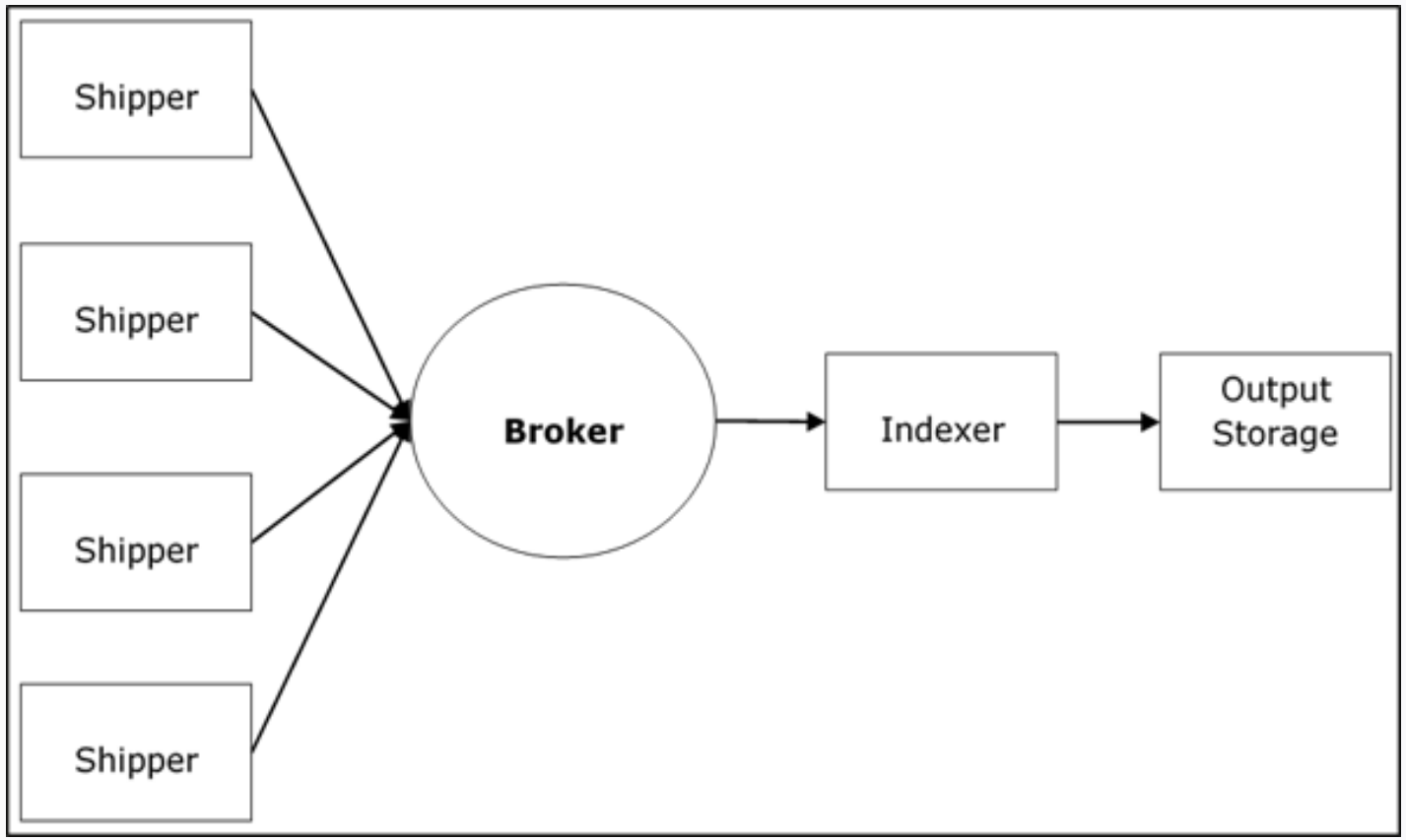
Минусы

1. Работает по http
2. Сложный и требует глубокого понимания принципов работы
3. Плагины, бывает, работают довольно странно

Архитектура

Компоненты

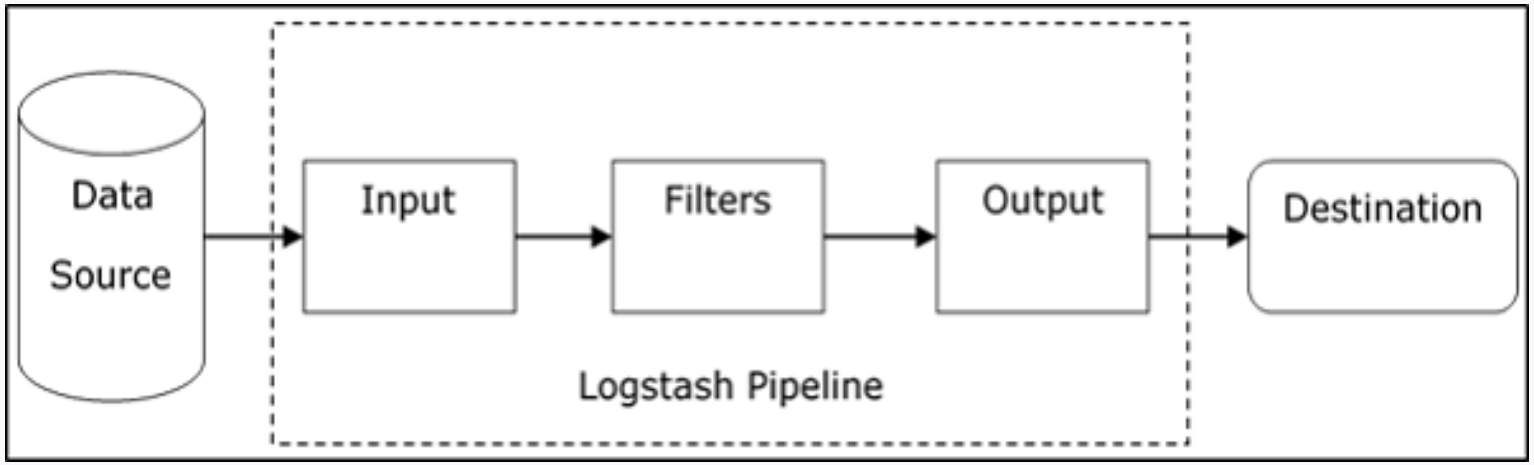
- Shipper
- Broker
- Indexer
- Output storage



Внтуреннее устройство

Пайплайн

- Data source
- Input
- Filters
- Output
- Destination



Кодеки

Кодеки отвечают за обработку формата как входных данных, так и выходных

- json_lines
- csv
- java_line
- multiline
- protopuf
- другие

Простейший пример

```
input {
    file {
        path => “/var/log/input.log”
    }
}

output {
    file {
        path => “/var/log/output.log”
    }
}
```

Базовые возможности

INPUT	FILTER	OUTPUT
file tcp udp	grok mutate date kv multiline	stdout file elasticsearch email

INPUT file

```
input {
  file {
    type => “nginx_access”
    path => [ “/var/log/nginx/*.log”, “/var/log/apache/*.log” ]
    exclude => [ “*.gz”, “*.zip”, “*.rar” ]
    start_position => “end”
    stat_interval => 1
    discover_interval => 30
  }
}
```

INPUT tcp

```
input {
  tcp {
    type => “our_tcp_service”
#codec => json
    mode => “server”            # режим сервера
    #mode => “client”           # наоборот, соединяемся по адресу
    host => “10.10.10.10“       # адрес
    port => 3337
  }
}
```

INPUT udp

```
input {
  udp {
    type => “our_udp_service”
    buffer_size => 4096
    host => “10.10.10.10”
    port => 3337
  }
}
```

FILTER grok – анализируем строку

```
filter {
  grok {
    type => “nginx_access"
    #patterns_dir => "/etc/logstash/patterns/"
    pattern => “%{IPORHOST:clientip} (?:-|(%{WORD}.%{WORD}))
%{USER:ident} \[%{HTTPDATE:timestamp}\] "(?:%{WORD:verb}
%{NOTSPACE:request}(?:
HTTP/%{NUMBER:httpversion})?|%{DATA:rawrequest})" %{NUMBER:response}
(?:%{NUMBER:bytes}|-) %{QS:referrer} %{QS:agent} %{QS:forwarder}”
  }
}
```

FILTER mutate – трансформируем строку

```
filter {
  mutate {
    type => "nginx_access"
    remove => [ "client" ]
    rename => [ "HOSTORIP", "client_ip" ]
}
}
```

FILTER date – получаем правильную дату

```
filter {
  date {
    match => [ "syslog_timestamp", "MMM  d HH:mm:ss", "MMM dd
HH:mm:ss"]
  }
}
```

FILTER multiline – многострочные логи

```
filter {
  multiline {
    type => "java_log"
    pattern => "^\s"    # знак переноса строки
    what => "previous"  # если есть, то считаем строку многострочной
  }
}
```

OUTPUT file

```
output {
  file {
    type => “syslog”
    flush_interval => 5                 # интервал записи
    gzip=> true                         # сжимать файл
    path => “/var/log/logstash/syslog.out”
  }
}
```

OUTPUT elasticsearch

```
output {
  elasticsearch {
    hosts => ["https://10.51.21.131:9200"]
    index => "local-syslog-%{+yyyy.MM.dd}"
    user => “username"
    password => “pass"
    ssl => true
    cacert => "/etc/logstash/root-ca.pem"
    ilm_enabled => false
    ssl_certificate_verification => false
  }
}
```

Списки плагинов

Input: https://www.elastic.co/guide/en/logstash/current/input-plugins.html

Output: https://www.elastic.co/guide/en/logstash/current/output-plugins.html

Codec: https://www.elastic.co/guide/en/logstash/current/codec-plugins.html


Заполните, пожалуйста,
опрос о занятии по ссылке в чате

Спасибо за внимание!
Приходите на следующие вебинары

фото

Напишите ваше ФИО

Должность
Компанию
Контакты