OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

Онлайн-образование

Не забыл включить запись

Меня хорошо видно && слышно?

Ставьте плюсы, если все хорошо

Напишите в чат, если есть проблемы

Правила вебинара

- Активно участвуем
- Задаем вопросы в чат или голосом
- Off-topic обсуждаем в Slack #канал группы или #general
- Вопросы вижу в чате, могу ответить не сразу

Сбор и анализ логов - 2: ELK

Маршрут вебинара

- Стек ELK
- Beats: Data shippers
- Logstash
- Elasticsearch
- Kibana

Цели занятия

После занятия вы сможете:

1. Понять основные принципы работы компонентов стека ELK
2. Установить и настроить компоненты стека ELK
3. Познакомиться со стеком ELK

Смысл

Зачем вам это уметь:

1. Чтобы понимать основные особенности работы со стеком ELK
2. Чтобы наиболее эффективно использовать стек ELK для сбора информации и анализа событий в инфраструктуре

Стек ELK

Стек ELK

Вопрос к аудитории: "Вы уже знакомы с ELK?"

Стек ELK

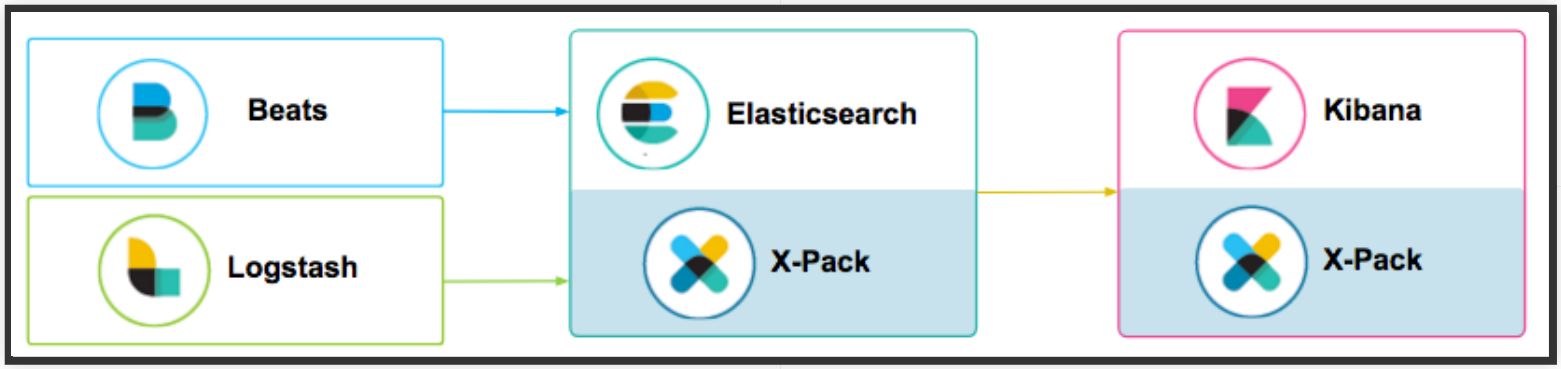
ELK - это аббревиатура из названий продуктов, которые входят в стек:

Elasticsearch - NoSQL база данных

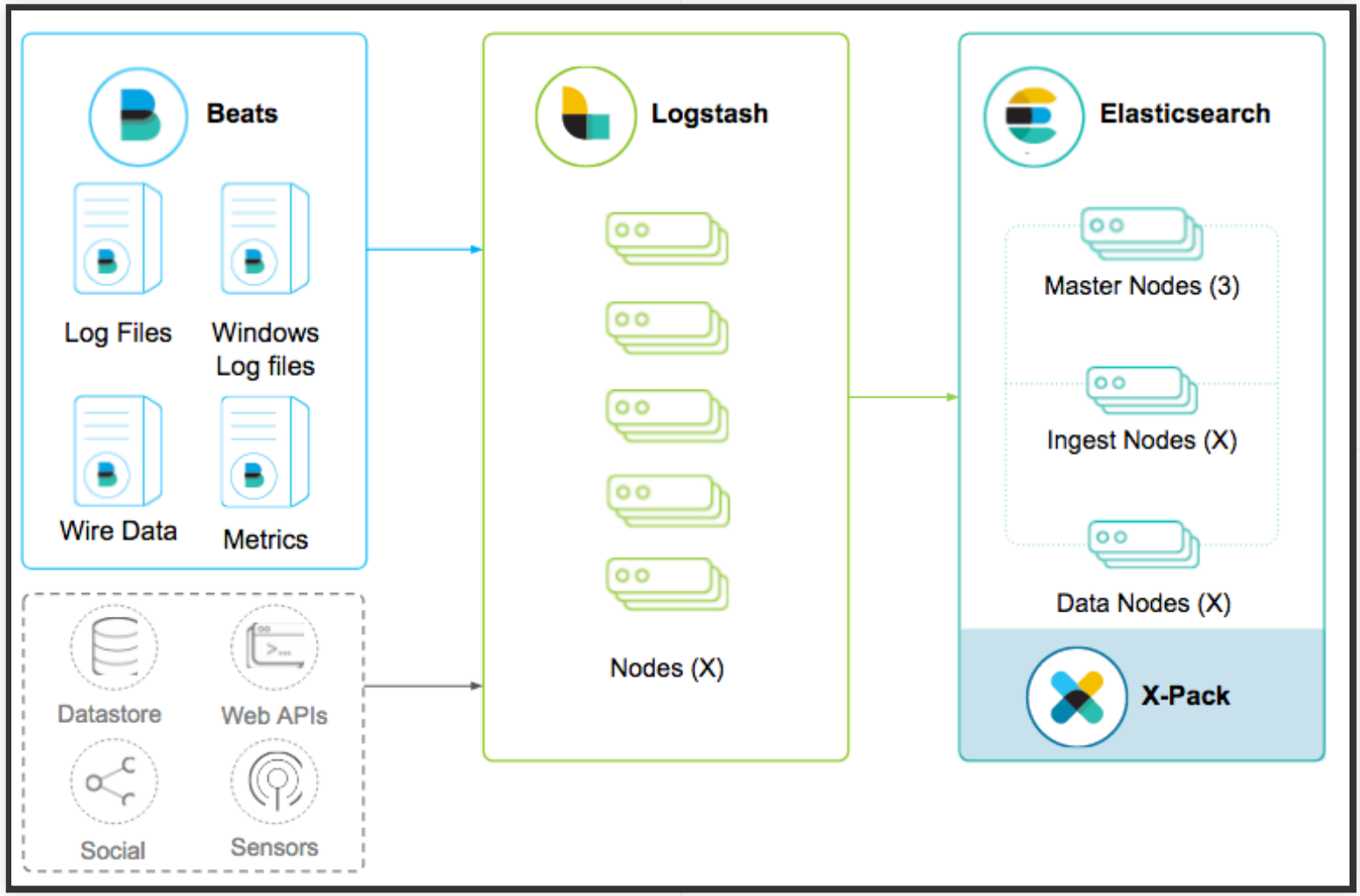
Logstash - приложение для сбора и обработки данных с возможностью конвейерной обработки

Kibana - графический интерфейс для удобства работы с базой Elasticsearch

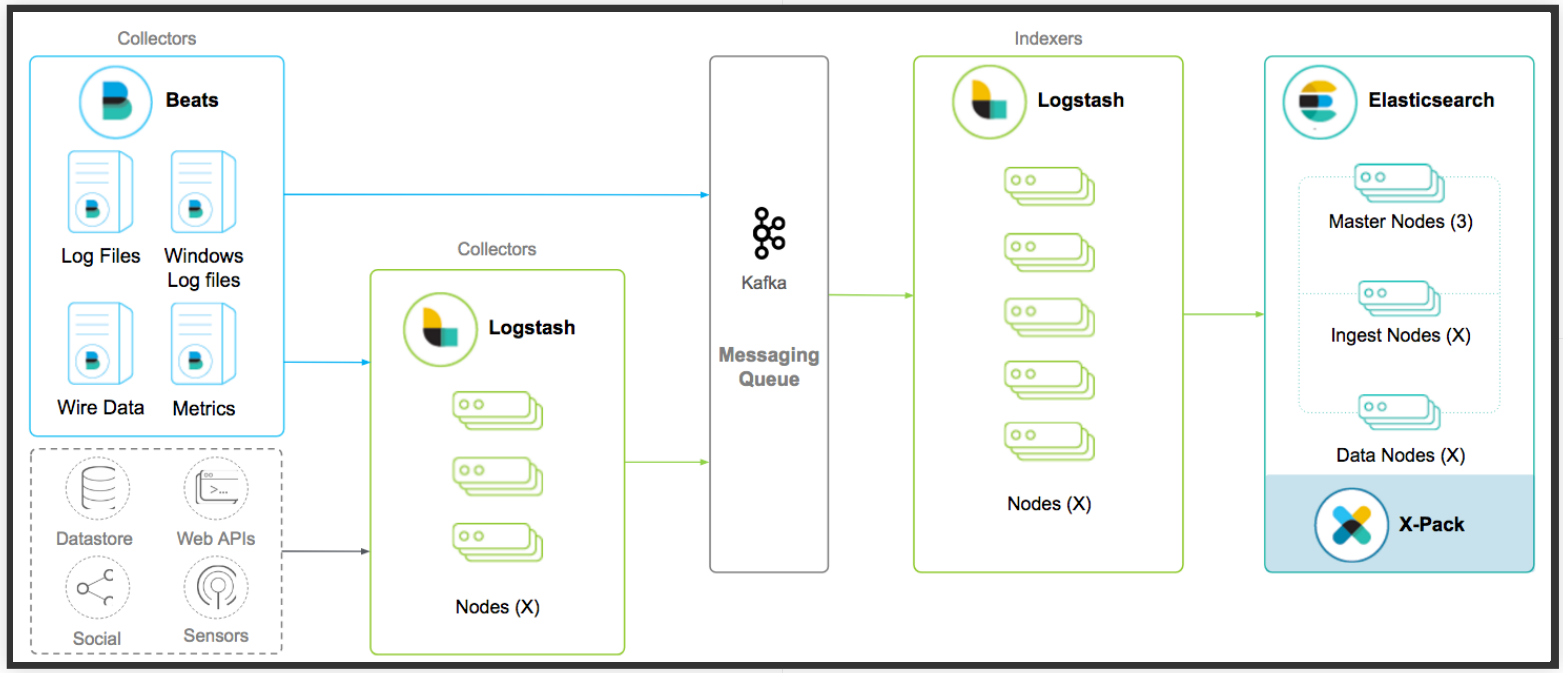
ELK: простая инсталляция



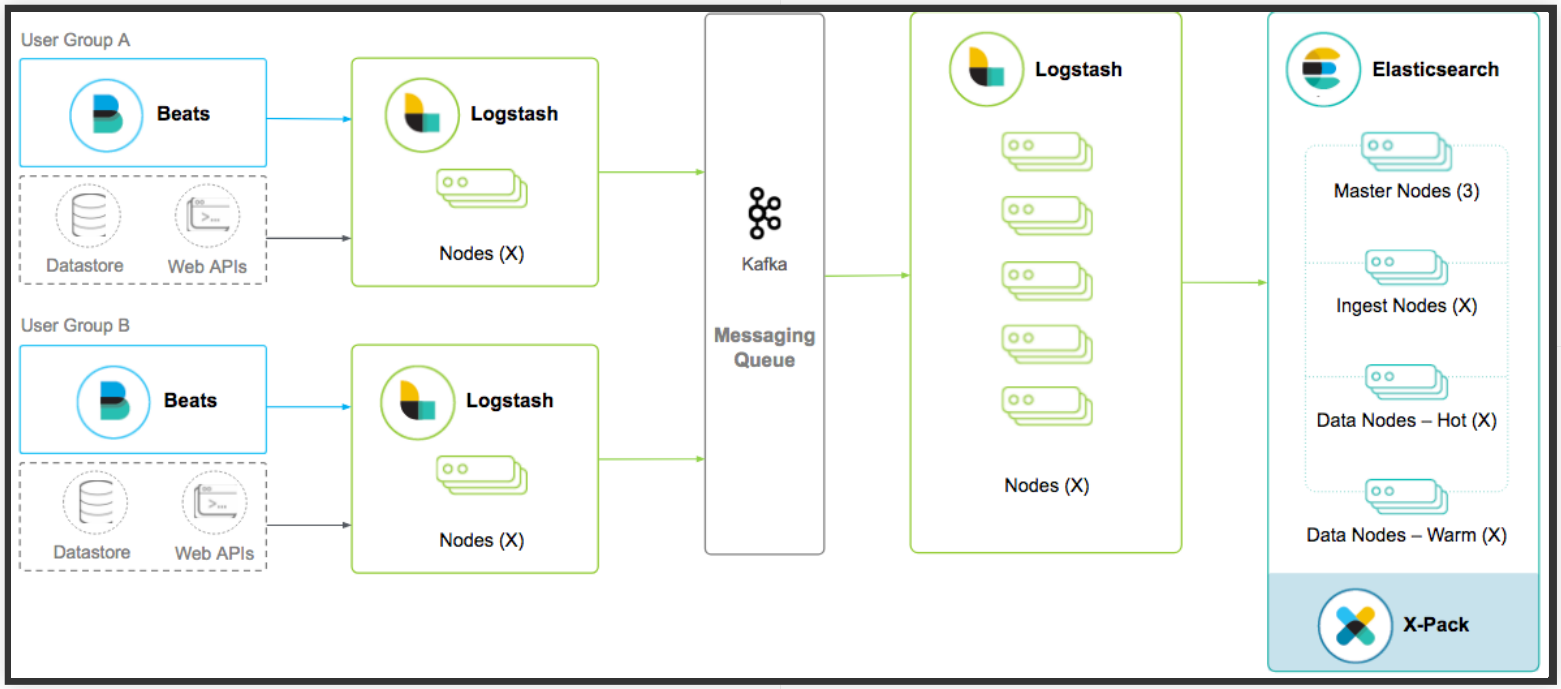
ELK: безопасное масштабирование



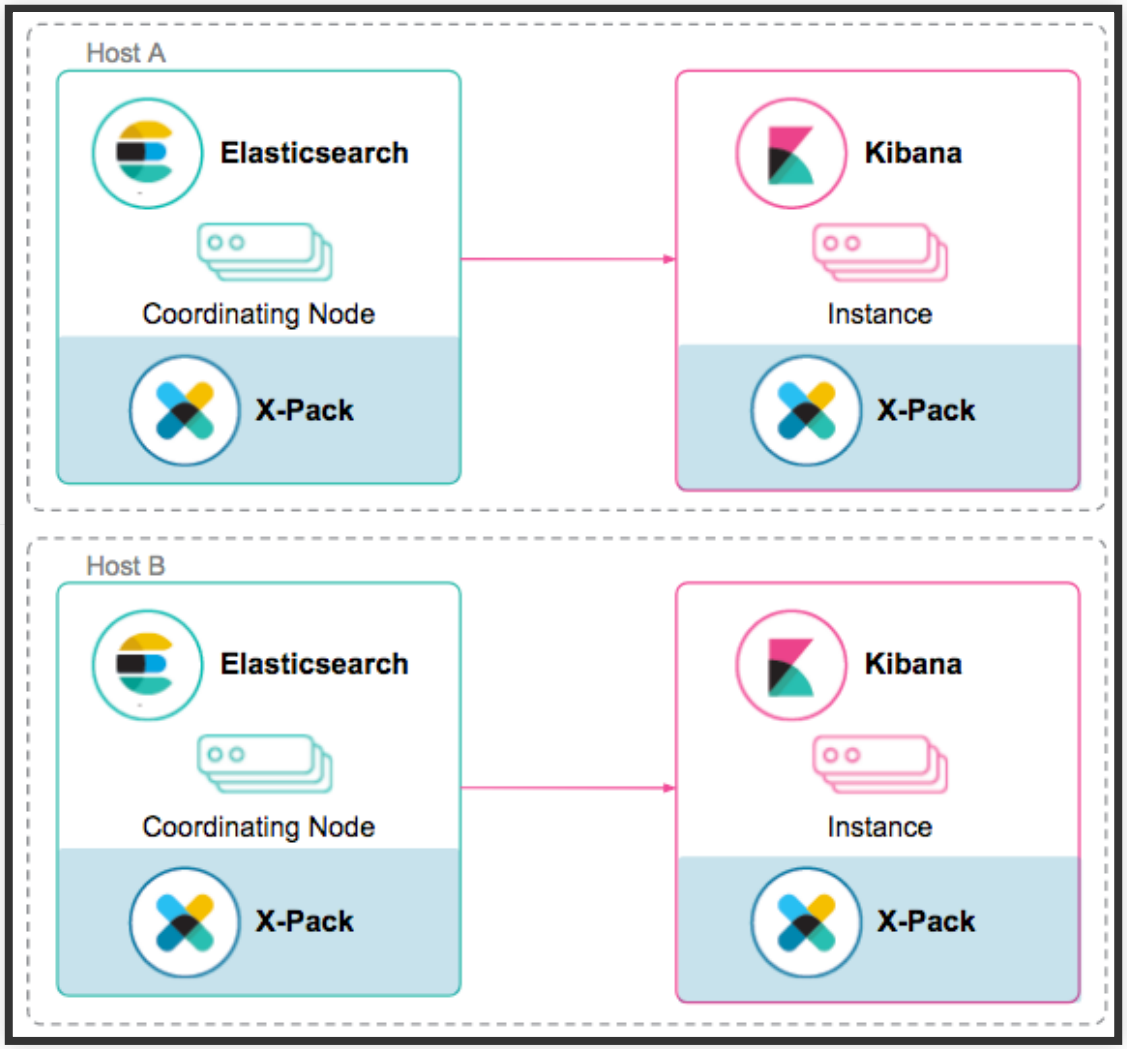
ELK: использование очереди



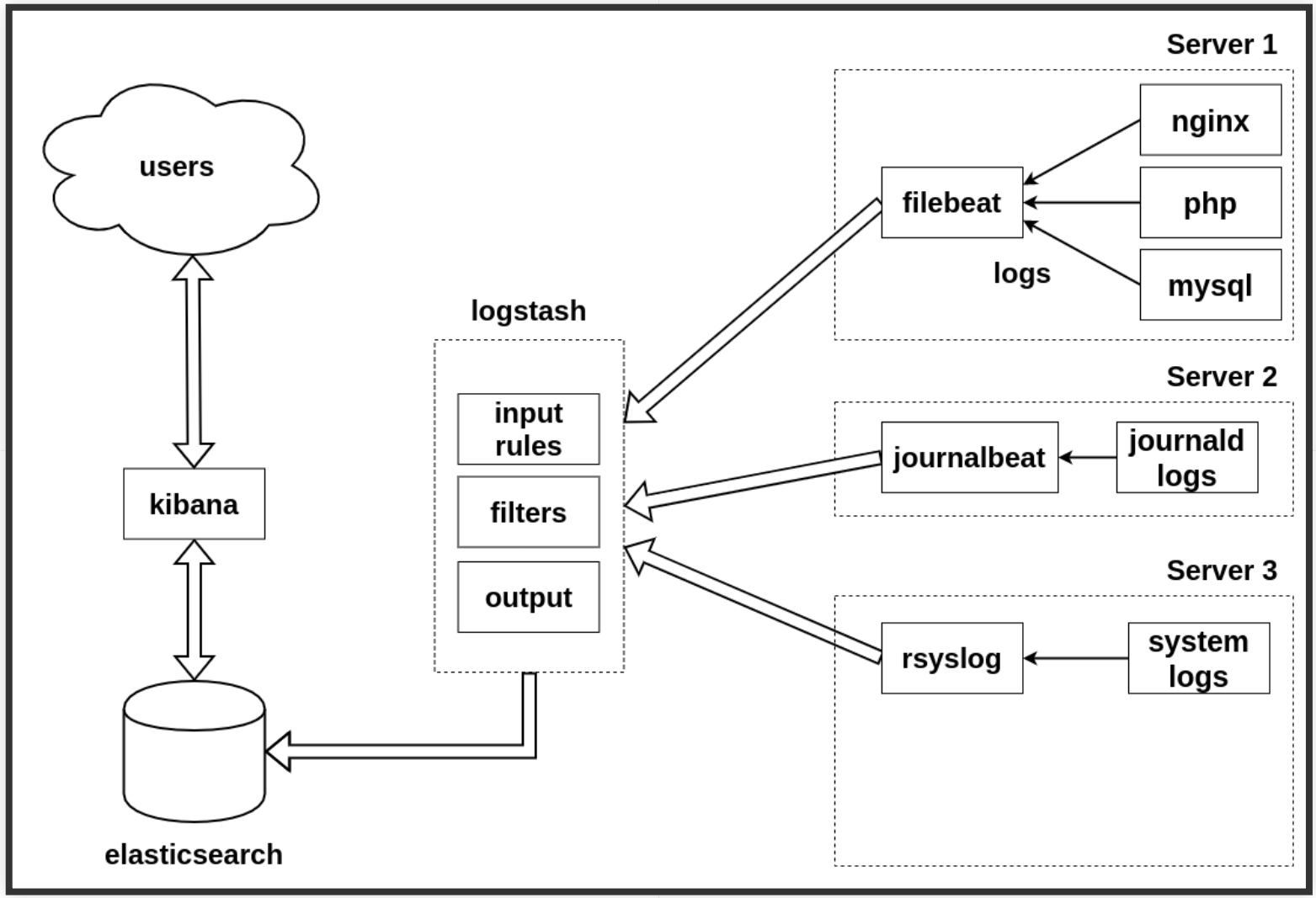
ELK: препроцессинг сообщений



ELK: Kibana high availability



ELK: схема тестового стенда



Маршрут вебинара

- Стек ELK
- Beats: Data shippers
- Logstash
- Elasticsearch
- Kibana

Beats: Data shippers

Beats: Data shippers

Beats - это поставщики данных для обработки в стеке ELK

Основные поставщики:

- Filebeat
- Metricbeat
- Packetbeat
- Winlogbeat
- Auditbeat
- Heartbeat
- Functionbeat

https://www.elastic.co/beats/

Beats: Filebeat

Filebeat - основной поставщик данных в ELK

Особенности:

- Большое количество вариантов ввода данных (files, syslog, stdin, docker, json, MQTT, netflow)
- Возможность базовой фильтрации и модификации сообщений
- Возможность вывода в Logstash или в базу Elasticsearch напрямую

Установка filebeat

Добавляем ключ репозитория:

```
rpm --import https://packages.elastic.co/GPG-KEY-elasticsearch
```

Добавляем репозиторий:

```
cat /etc/yum.repos.d/elastic.repo
[elastic-7.x]
name=Elastic repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

Установка filebeat

Устанавливаем filebeat:

```
yum install -y filebeat
```

Пример конфигурации filebeat:

```
cat /etc/filebeat/filebeat.yml
- type: log
  enabled: true
  paths:
      - /var/log/nginx/access.log
  fields:
    service: nginx_access
  fields_under_root: true
  scan_frequency: 5s
```

Пример конфигурации filebeat

Конфигурация вывода и передачи сообщений:

```
#output.elasticsearch:
#  hosts: ["localhost:9200"]

  #protocol: "https"
  #username: "elastic"
  #password: "changeme"

output.logstash:
  hosts: ["logstash_host:5044"]
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]
  #ssl.certificate: "/etc/pki/client/cert.pem"
  #ssl.key: "/etc/pki/client/cert.key"
```

Проверка конфигурации filebeat:

```
filebeat test config
```

Маршрут вебинара

- Стек ELK
- Beats: Data shippers
- Logstash
- Elasticsearch
- Kibana

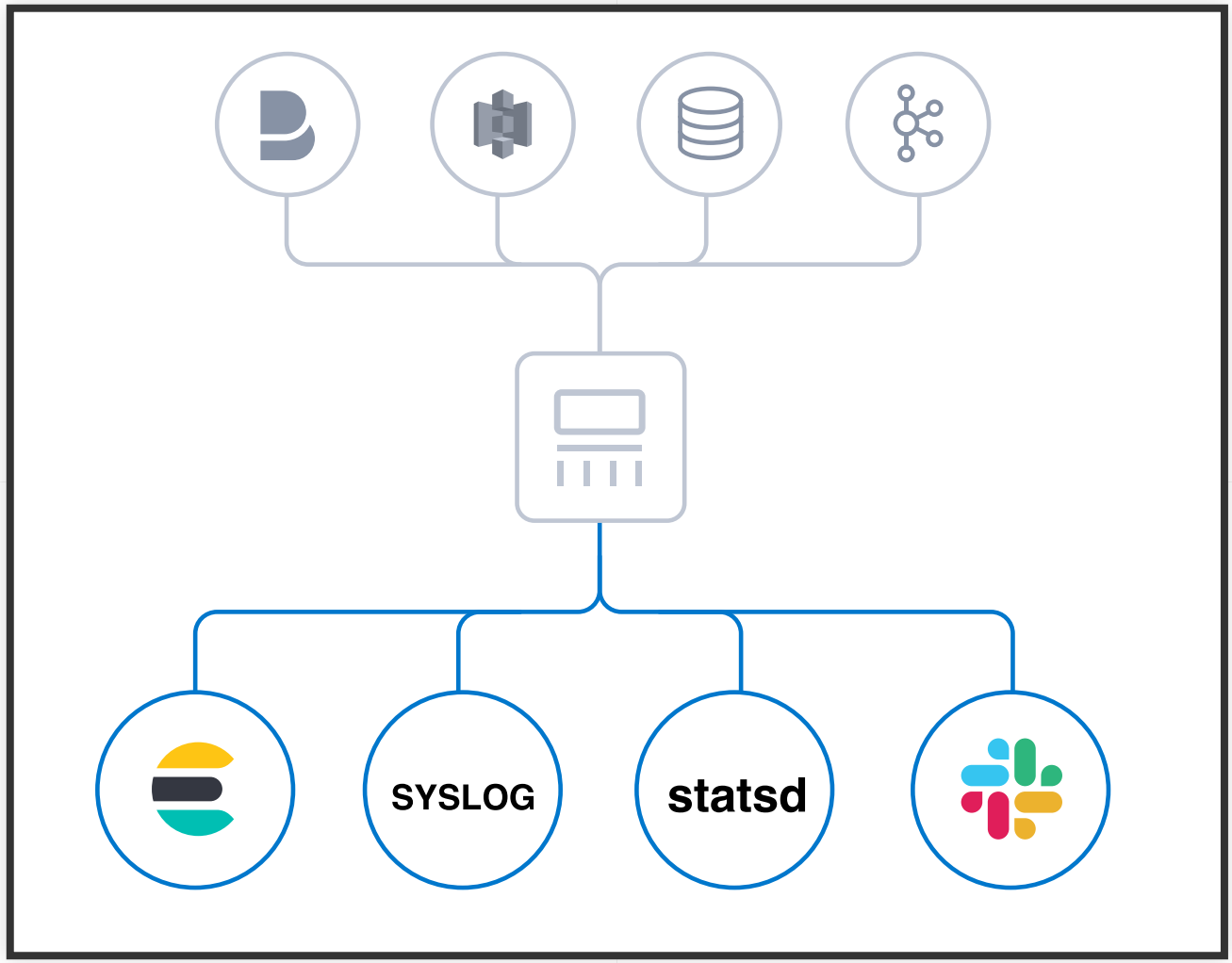
Logstash

Приложение для сбора и обработки данных с возможностью конвейерной обработки

Особенности:

- Большой выбор входящих источников данных
- Большой выбор исходящих потоков данных
- Кастомные фильтры в формате JSON

Logstash



Установка Logstash

Установка logstash:

```
yum install -y logstash
```

Конфигурация входных данных logstash:

```
cat /etc/logstash/conf.d/02-beats-input.conf
input {
    beats {
    port => 5044
    congestion_threshold => 25
    }
}
```

Конфигурация Logstash

Конфигурация фильтра обработки логов syslog выходного потока logstash:

```
cat /etc/logstash/conf.d/10-syslog-filter.conf
filter {
    if [fields][service] == "syslog" {
    grok {
    match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp} 
    add_field => [ "received_at", "%{@timestamp}" ]
    add_field => [ "received_from", "%{host}" ]
    }
    syslog_pri { }
        date {
    match => [ "syslog_timestamp", "MMM  d HH:mm:ss", "MMM dd HH:
        }
    }
}
```

Конфигурация Logstash

Конфигурация выходного потока logstash:

```
cat /etc/logstash/conf.d/20-output.conf
output {
    if [fields][service] == "syslog" {
        elasticsearch {
        hosts => ["http://1.1.1.1:9200"]
        index => "syslog-%{+YYYY.MM.dd}"
        document_type => "%{[@metadata][type]}"
        }
    }
}
```

Конфигурация Logstash

Проверка синтаксиса конфигов logstash:

```
/usr/share/logstash/bin/logstash -t -f /etc/logstash/conf.d/
```

Автоматический релоад конфигурации logstash без рестарта сервиса:

```
cat /etc/logstash/logstash.yml
...
# Periodically check if the configuration has changed and reload
# This can also be triggered manually through the SIGHUP signal
#
config.reload.automatic: true
...
```

Конфигурация Logstash

Возможные варианты плагинов вывода данных logstash: https://www.elastic.co/guide/en/logstash/current/output-plugins.html

Маршрут вебинара

- Стек ELK
- Beats: Data shippers
- Logstash
- Elasticsearch
- Kibana

Elasticsearch

База данных, построенная на движке Apache Lucene, изначально адаптированная под полнотекстовый поиск

Особенности:

- Быстрая индексация
- Производительный полнотекстовый поиск
- Масштабируемая
- Удобная репликация и шардирование

Установка Elasticsearch

Установка Java:

```
yum install java-1.8.0-openjdk
```

Добавляем репозиторий:

```
[elasticsearch-7.x]
name=Elasticsearch repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

Установка базы Elasticsearch

```
yum -y install elasticsearch
```

Установка ELK

Конфигурация Elasticsearch:

```
cat /etc/elasticsearch/elasticsearch.yml
network.host: 127.0.0.1
```

Настройка выделения памяти для работы базы:

```
cat /etc/elasticsearch/jvm.options
-Xms32g
-Xmx32g
```

Проверка работы базы данных:

```
curl -GET localhost:9200/_cat/health?v
```

Установка ELK

Просмотр индексов в базе:

```
curl -GET localhost:9200/_cat/indices?v
```

Задание общего шаблона для индексов с указанием параметра numbers_of_replicas:

```
curl -XPUT "localhost:9200/_template/all" -H 'Content-Type: appli
{
  "template": "*",
  "settings": {
    "number_of_replicas": 0
  }
}'
```

Маршрут вебинара

- Стек ELK
- Beats: Data shippers
- Logstash
- Elasticsearch
- Kibana

Kibana

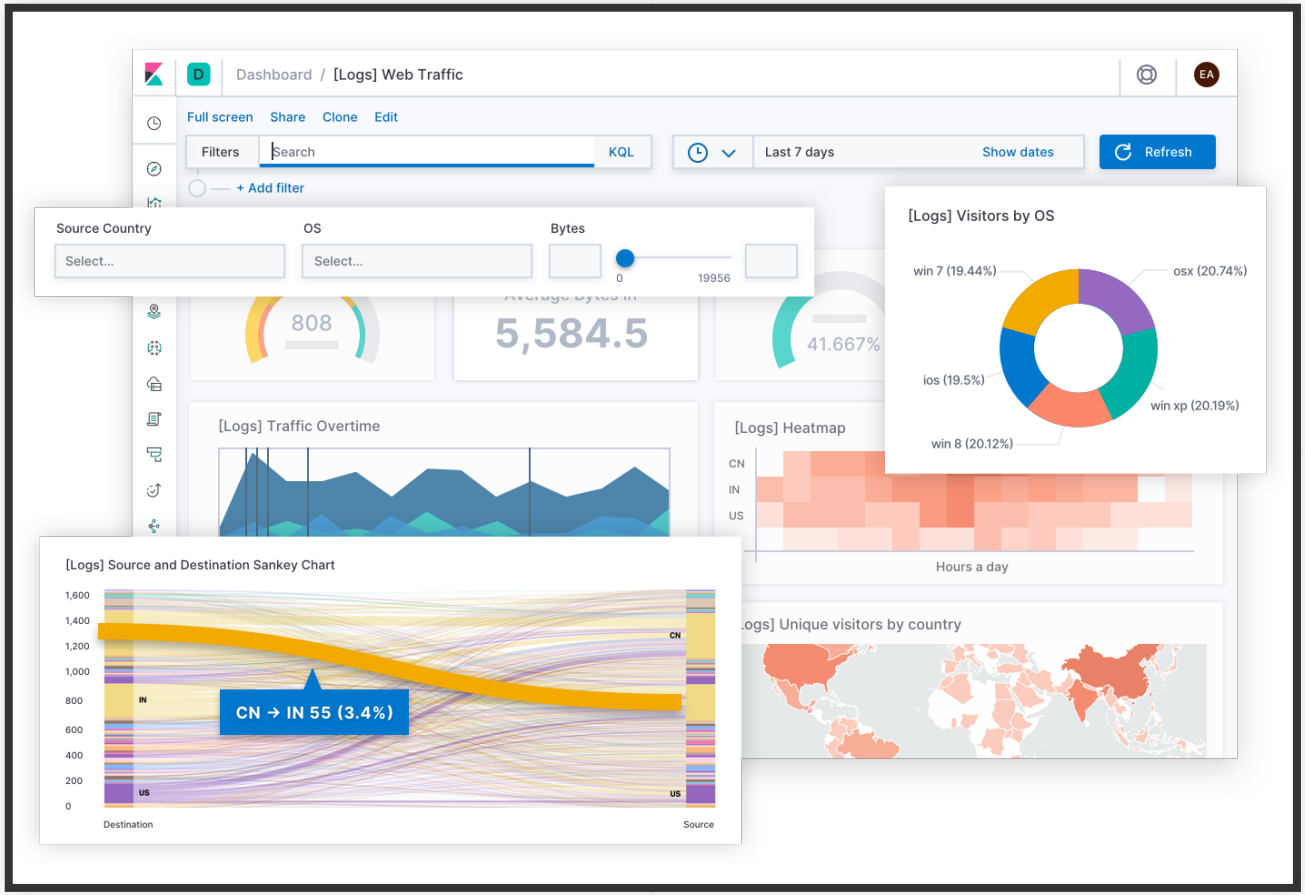
Графический интерфейс для удобства работы с базой Elasticsearch

Особенности:

- Анализ данных в индексах Elasticsearch
- Гибкое отображение данных с помощью фильтров
- Широкие возможности визуализации данных (графики, дашборды)
- Мониторинг
- Управление индексами

Установка интерфейса Kibana

Внешний вид интерфейса Kibana



Установка интерфейса Kibana

Установка интерфейса Kibana

```
yum install -y kibana
```

Заполните, пожалуйста, опрос о занятии по ссылке в чате

Приходите на следующие вебинары

Спасибо за внимание!