

# Онлайн образование

otus.ru



Проверить, идет ли запись

# Меня хорошо видно && слышно?



Тема вебинара

# Логирование



**Лавлинский Николай**

Технический директор “Метод Лаб”

<https://www.methodlab.ru/>

<https://www.youtube.com/c/NickLavlinsky>

<https://vk.com/nick.lavlinsky>



# Преподаватель



## Лавлинский Николай

Более 15 лет в веб-разработке

Преподавал в ВУЗе более 10 лет  
Более 3 лет в онлайн-образовании

Специализация: оптимизация производительности,  
ускорение сайтов и веб-приложений

# Правила вебинара



Активно  
участвуем



Off-topic обсуждаем  
в Slack #general



Задаем вопрос  
в чат или голосом



Вопросы вижу в чате,  
могу ответить не сразу

## Условные обозначения



Индивидуально



Время, необходимое  
на активность



Пишем в чат



Говорим голосом

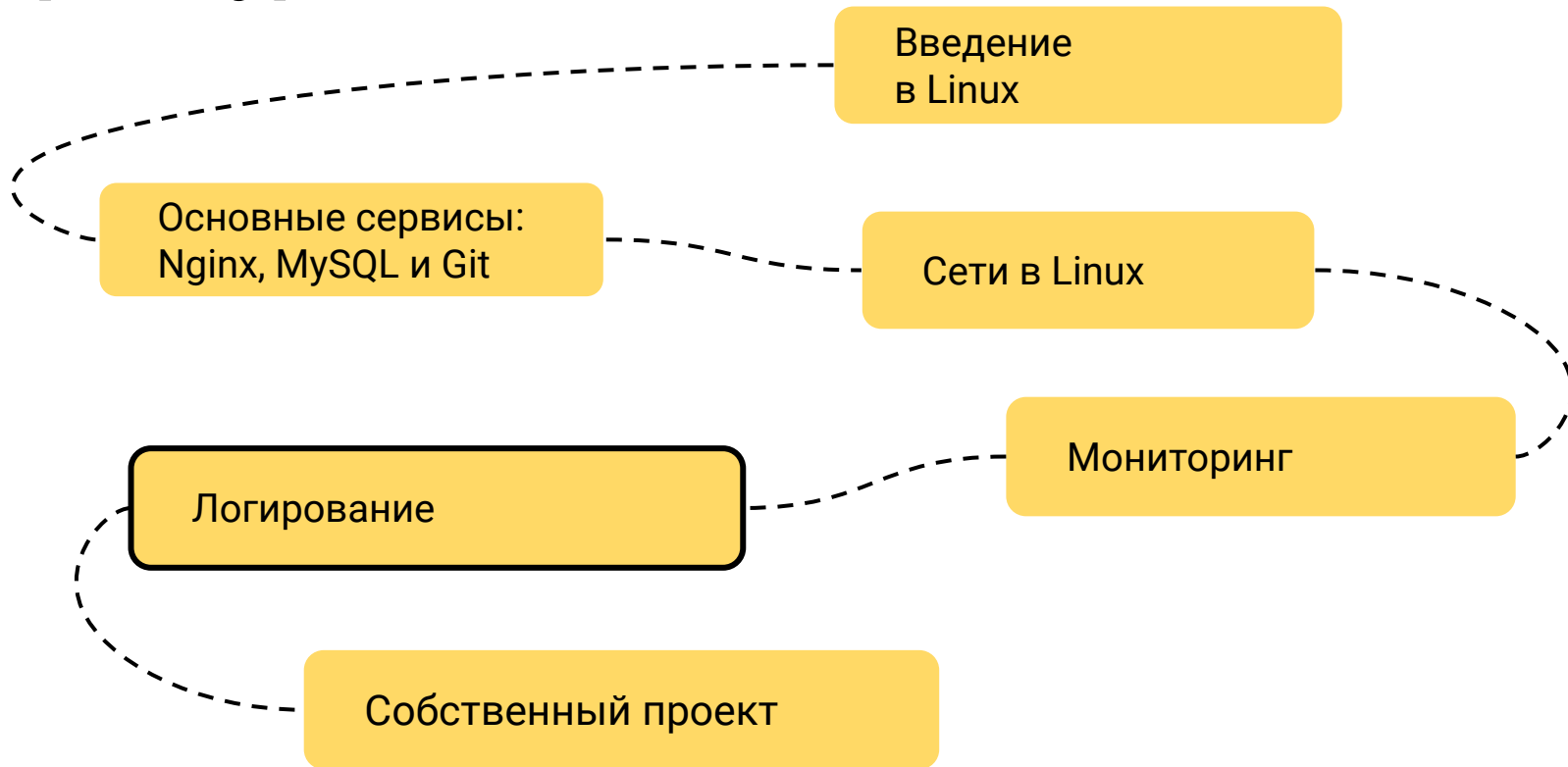


Документ



Ответьте себе или  
задайте вопрос

# Карта курса



# Маршрут вебинара



Виды логирования

Работа с текстовыми и  
бинарными логами

Настройка логирования в ELK

# Цели вебинара

После занятия вы сможете

1. Научиться находить значимые события в логах
2. Настраивать системы логирования
3. Работать с логами через стек ELK



# Смысл

Зачем вам это уметь

1. Решать проблемы функционирования системы
2. Управлять процессом логирования
3. Централизовать сбор и анализ логов

# Логирование в Linux



Что такое, зачем?

# Типы логов

- Текстовые
  - Прямой записи: `/var/log/nginx/access.log`
  - Через `rsyslogd`: `/var/log/messages`
- Бинарные (через `systemd-journald`): `/run/log/journal/`
- База данных (Elasticsearch, MySQL)

# Работа с текстовыми логами

```
Text logs  — □ ×

# Фильтрация лога
cat messages | grep err | grep -P '\d{2}:\d{2}:00'

# Последние 10 строк лога
tail -n 10 messages

# Первые 10 строк лога
head -n 10 messages

# Просмотр сообщений в реальном времени
tail -f messages
```



# Ротация логов

- Хранение истории
- Сжатие старых логов
- Конфигурация `/etc/logrotate.conf`, `/etc/logrotate.d/*`
- Часто настройки ротации создаются при установке пакета
- Скрипт запуска: `/etc/cron.daily/logrotate`

# Работа с journald

```
Journald logs

# Проверка формата времени
timedatectl status
sudo timedatectl set-timezone zone

# Логи с момента загрузки
journalctl -b

# Сохранение логов между загрузками системы
sudo mkdir -p /var/log/journal
sudo nano /etc/systemd/journald.conf

[Journal]
Storage=persistent

# Фильтрация по времени
journalctl --since "2022-01-01 17:15:00"
journalctl --since "2022-01-01 17:15:00" --until "2022-01-02 17:15:00"
journalctl --since yesterday
journalctl --since 09:00 --until "1 hour ago"

# Фильтрация по юниту
journalctl -u nginx.service

# Фильтрация по приоритету
journalctl -p err -b

# Форматирование в JSON
journalctl -b -u nginx -o json-pretty
```

# Сбор и анализ логов с помощью ELK стека



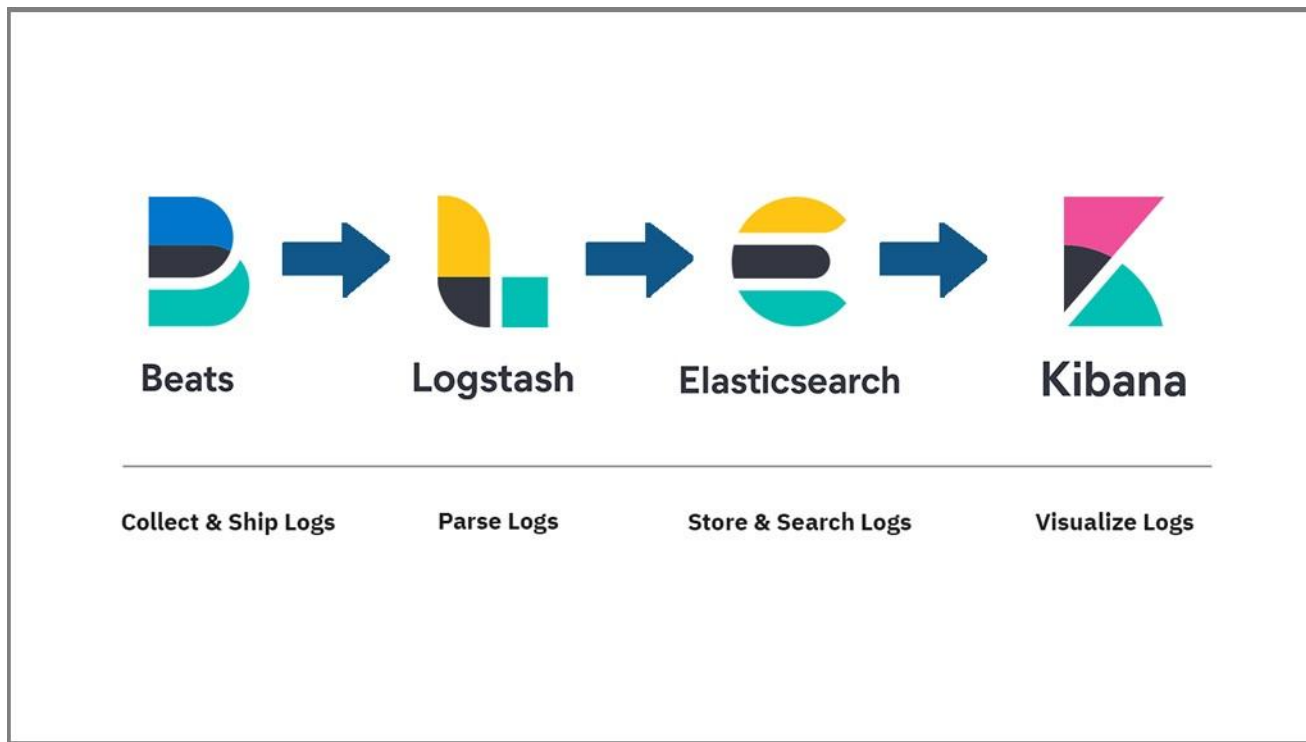
Что такое, зачем?

# Компоненты

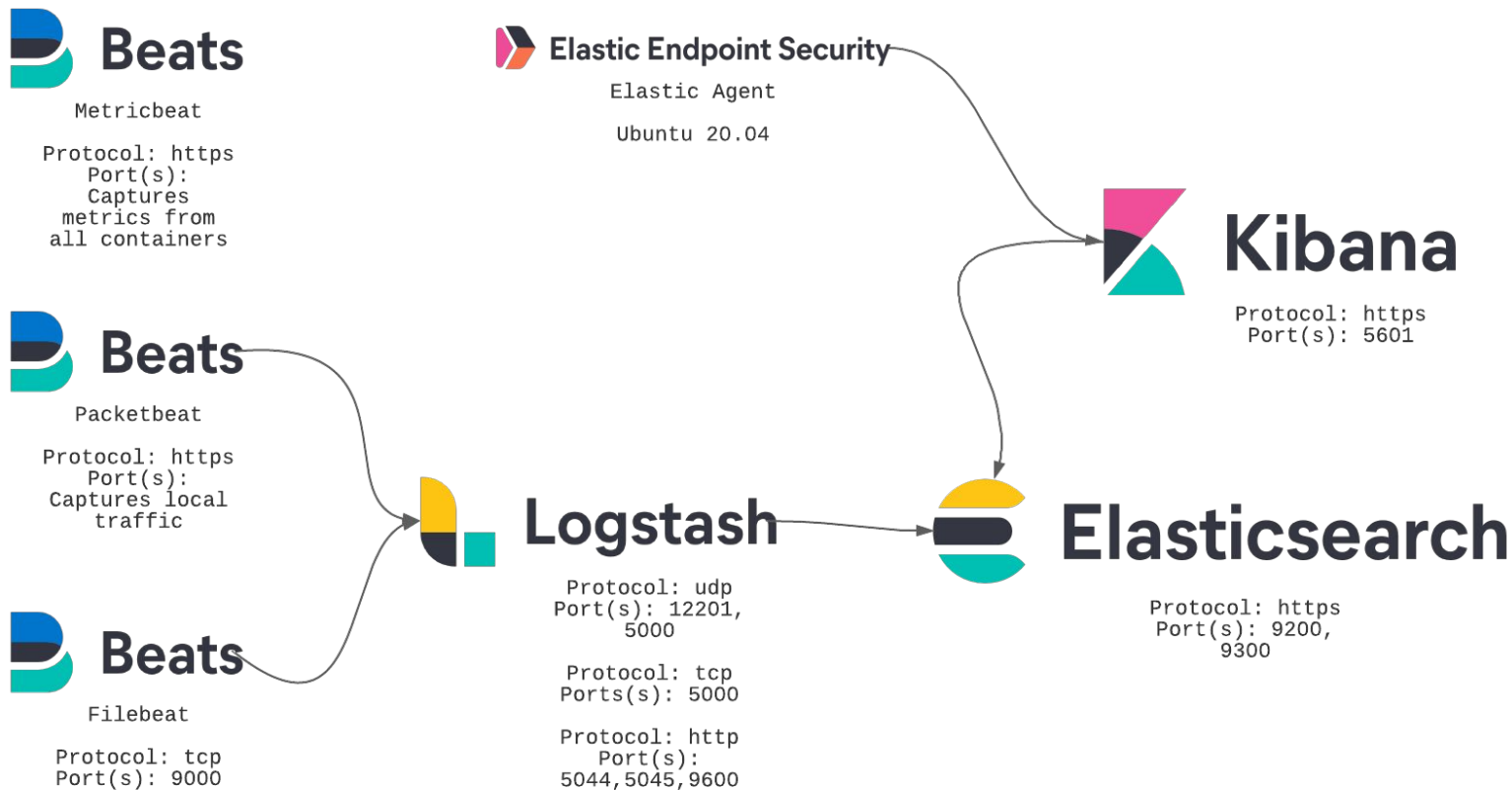
- **Elasticsearch** (база данных)
- **Logstash** (обработка данных)
- **Kibana** (визуализация – графики, диаграммы)
- **Beats** (сбор данных из логов)



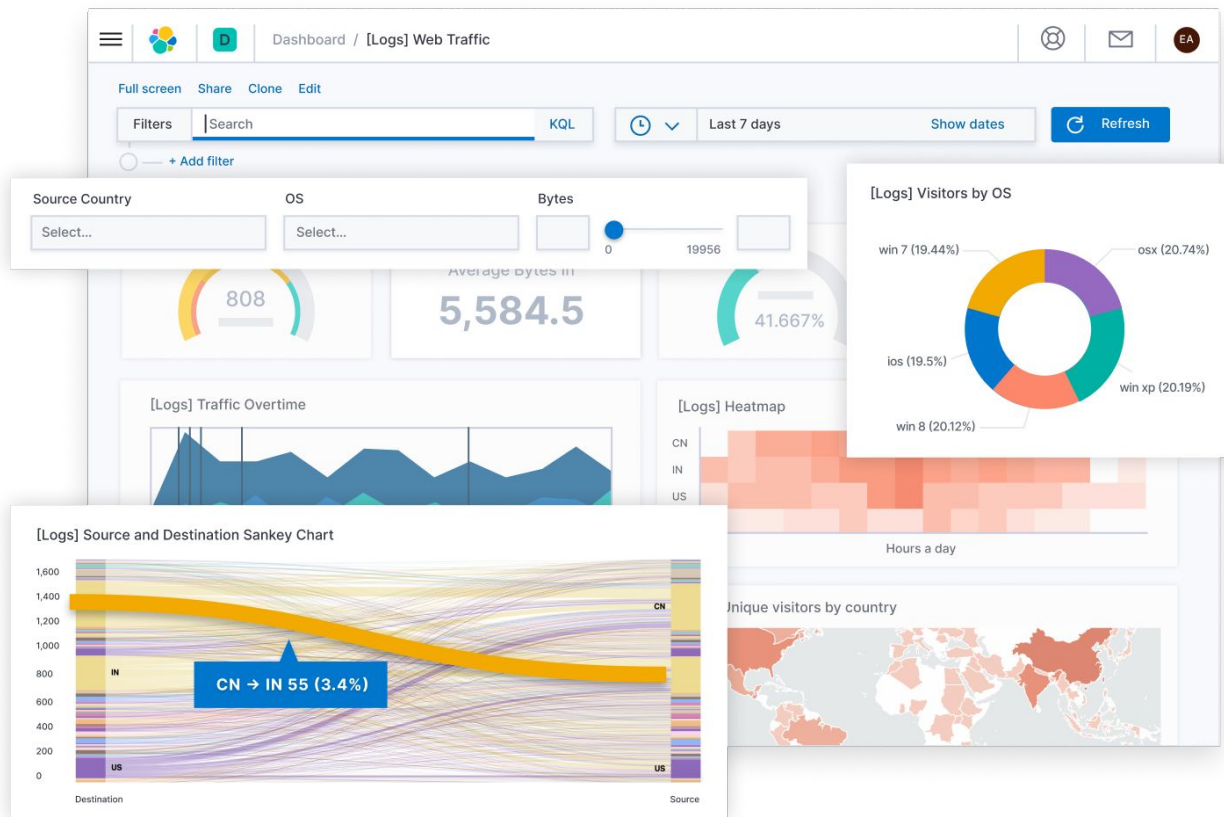
# ELK стек – назначение



# ELK стек – взаимодействие



# Пример визуализации данных



# Практика

# Домашнее задание

1. Установить все компоненты стека ELK
2. Настроить сбор логов Nginx через стек ELK
3. Настроить dashboard с несколькими метриками
4. Прислать отчет по конфигурации и скриншот dashboard'a



**Сроки выполнения: указаны в личном кабинете**



# Список материалов для изучения

1. <https://www.digitalocean.com/community/tutorials/how-to-use-journalctl-to-view-and-manipulate-systemd-logs-ru>
2. <https://max-ko.ru/33-logi-v-linux-1.html>
3. <https://www.unixmen.com/logging-journald-rhel7centos7/>
4. <https://computingforgeeks.com/how-to-install-elk-stack-on-centos-fedora/>
5. <https://sysadmins.co.za/how-to-ingest-nginx-access-logs-to-elasticsearch-using-filebeat-and-logstash/>
6. <https://pawelurbanek.com/elk-nginx-logs-setup>

# Вопросы?



Ставим "+",  
если вопросы есть



Ставим "-",  
если вопросов нет

# Рефлексия



# Рефлексия



Что было самым полезным на занятии?



Как будете применять на практике то, что узнали на вебинаре?



**Заполните, пожалуйста,  
опрос о занятии  
по ссылке в чате**

Спасибо за внимание!

# Приходите на следующие вебинары



**Лавлинский Николай**

Технический директор “Метод Лаб”

<https://www.methodlab.ru/>

<https://www.youtube.com/c/NickLavlinsky>

<https://vk.com/nick.lavlinsky>

