OTUS

Administrator Linux.Basic

Логирование

otus.ru

Проверить, идет ли запись

Меня хорошо видно && слышно?

Преподаватель

Лавлинский Николай

Технический директор «Метод Лаб»

Более 15 лет в веб-разработке

Преподавал в ВУЗе более 10 лет
Более 4 лет в онлайн-образовании

Специализация: оптимизация производительности, ускорение сайтов и веб-приложений
https://t.me/methodlab_tg
https://www.methodlab.ru/
https://www.youtube.com/c/NickLavlinsky
https://www.youtube.com/@site_support
https://vk.com/nick.lavlinsky

Правила вебинара

Активно
участвуем

Off-topic обсуждаем
в Телеграм-чате

Задаем вопрос
в чат или голосом

Вопросы вижу в чате,
могу ответить не сразу

Условные обозначения

Индивидуально

Время, необходимое
на активность

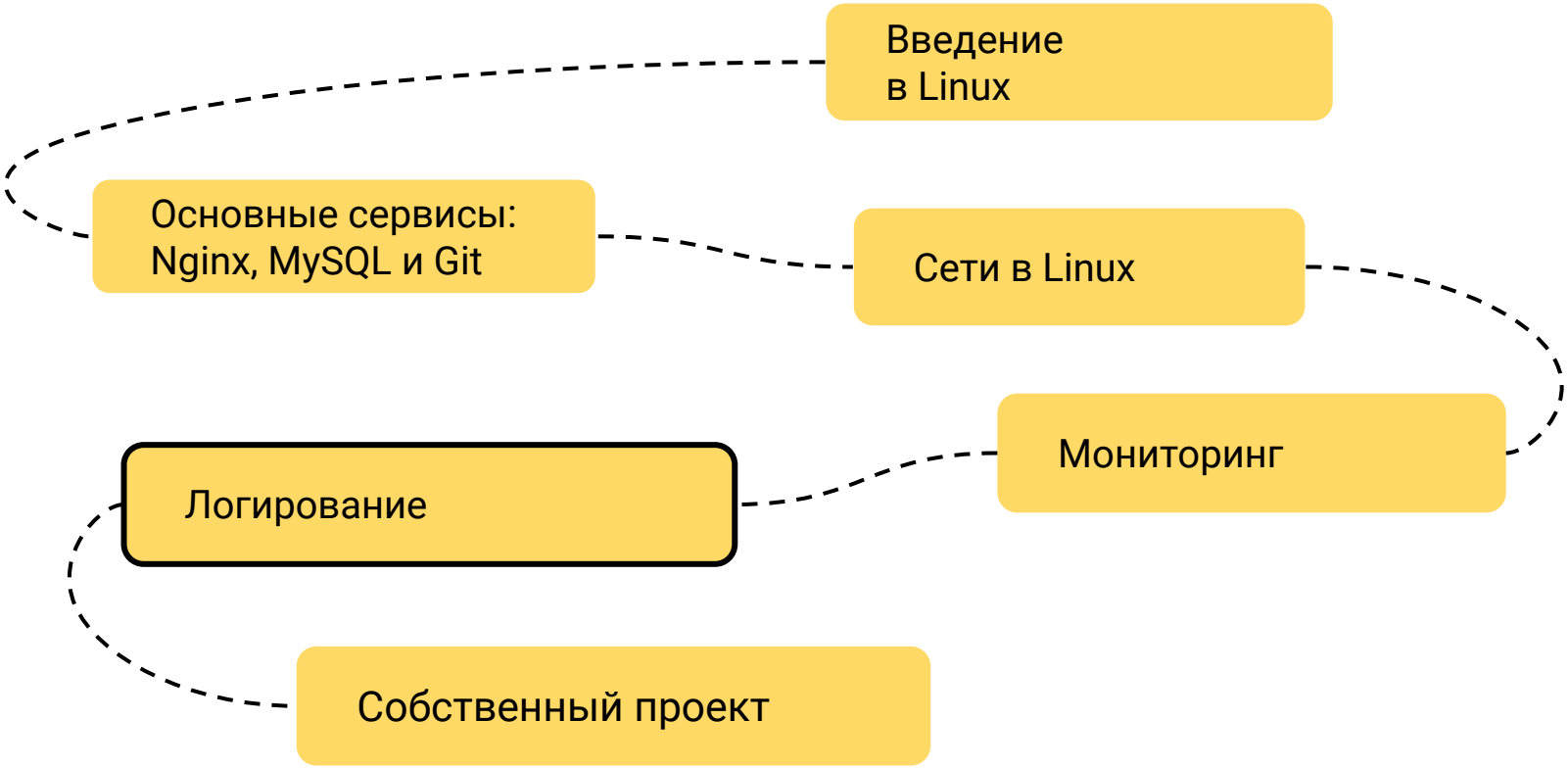
Пишем в чат

Говорим голосом

Документ

Ответьте себе или
задайте вопрос

Карта курса


Введение
в Linux
Основные сервисы:
Nginx, MySQL и Git
Сети в Linux
Мониторинг
Логирование
Собственный проект

Маршрут вебинара

- Виды логирования
- Работа с текстовыми и бинарными логами
- Архитектура ELK-стека
- 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/syslog`
- Бинарные (через `systemd-journald): /var/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?

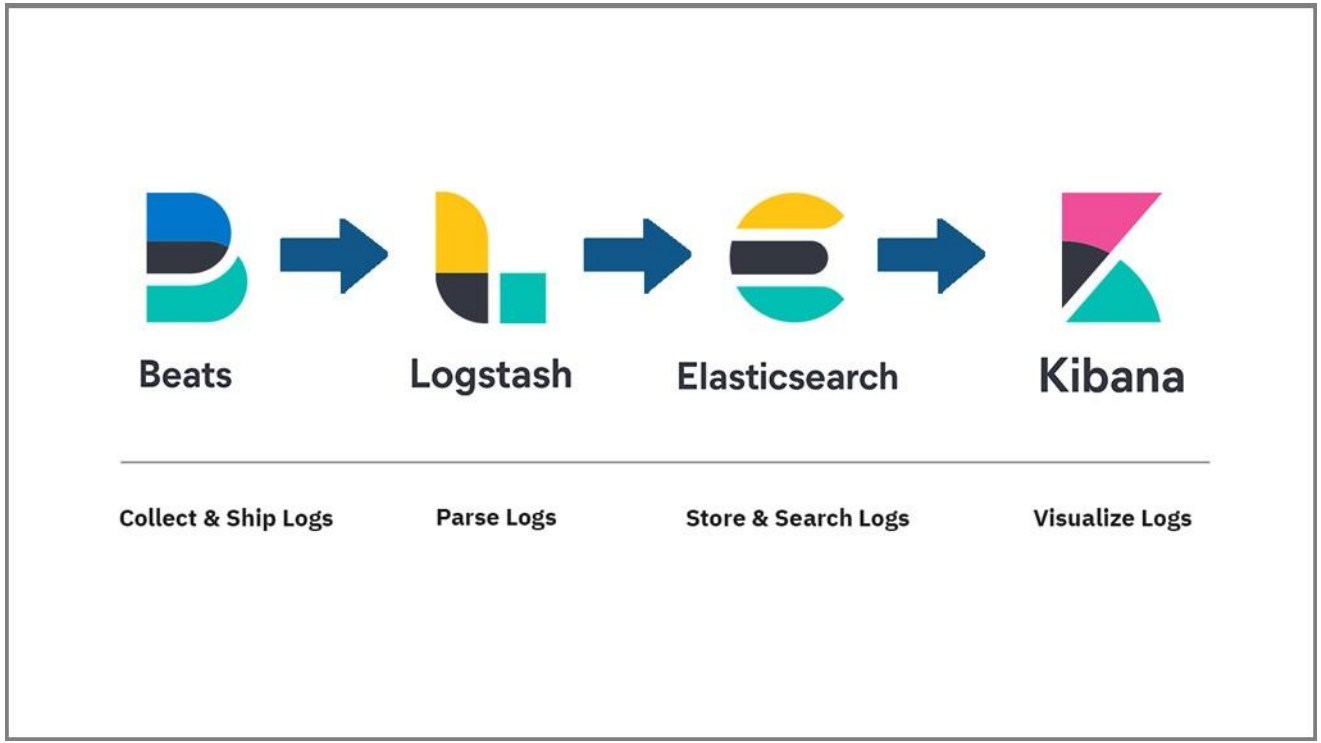
Компоненты

- **E**lasticsearch — база данных для надёжного хранения документов
- **L**ogstash — обработка данных из логов
- **K**ibana — визуализация данных из Elasticsearch (дашборды)
- Beats — сбор данных для сохранения в ELK-стеке
- Компоненты могут быть требовательными к оперативной памяти, полный стек — 4 GB минимум

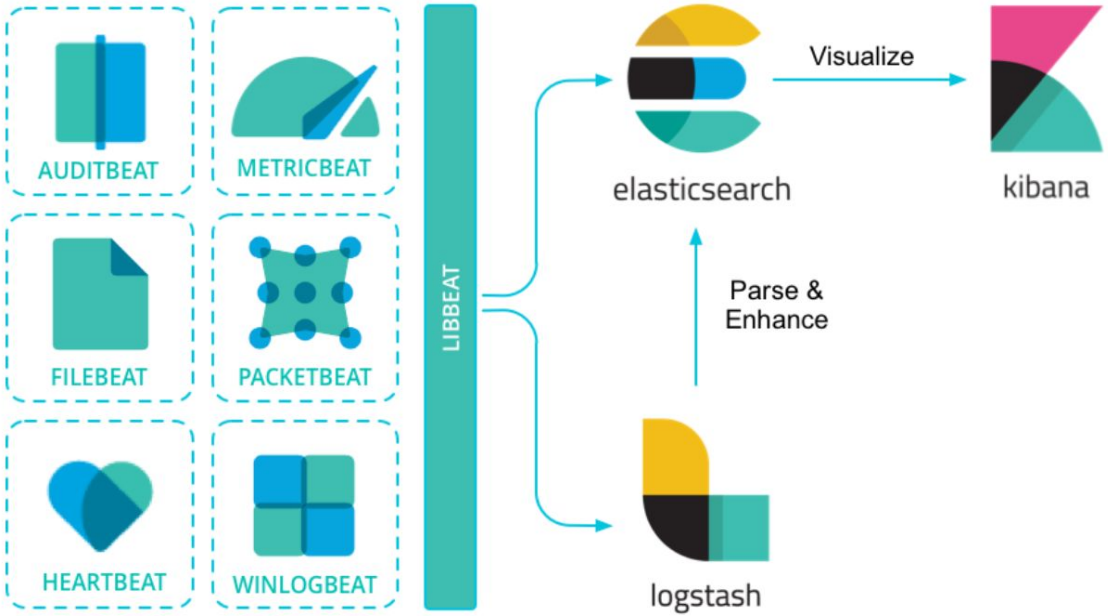
Beats

- Filebeat — основной поставщик данных в ELK
- Heartbeat — проверка сервисов
- Auditbeat — события auditd (безопасность)
- Metricbeat — метрики для мониторинга системы

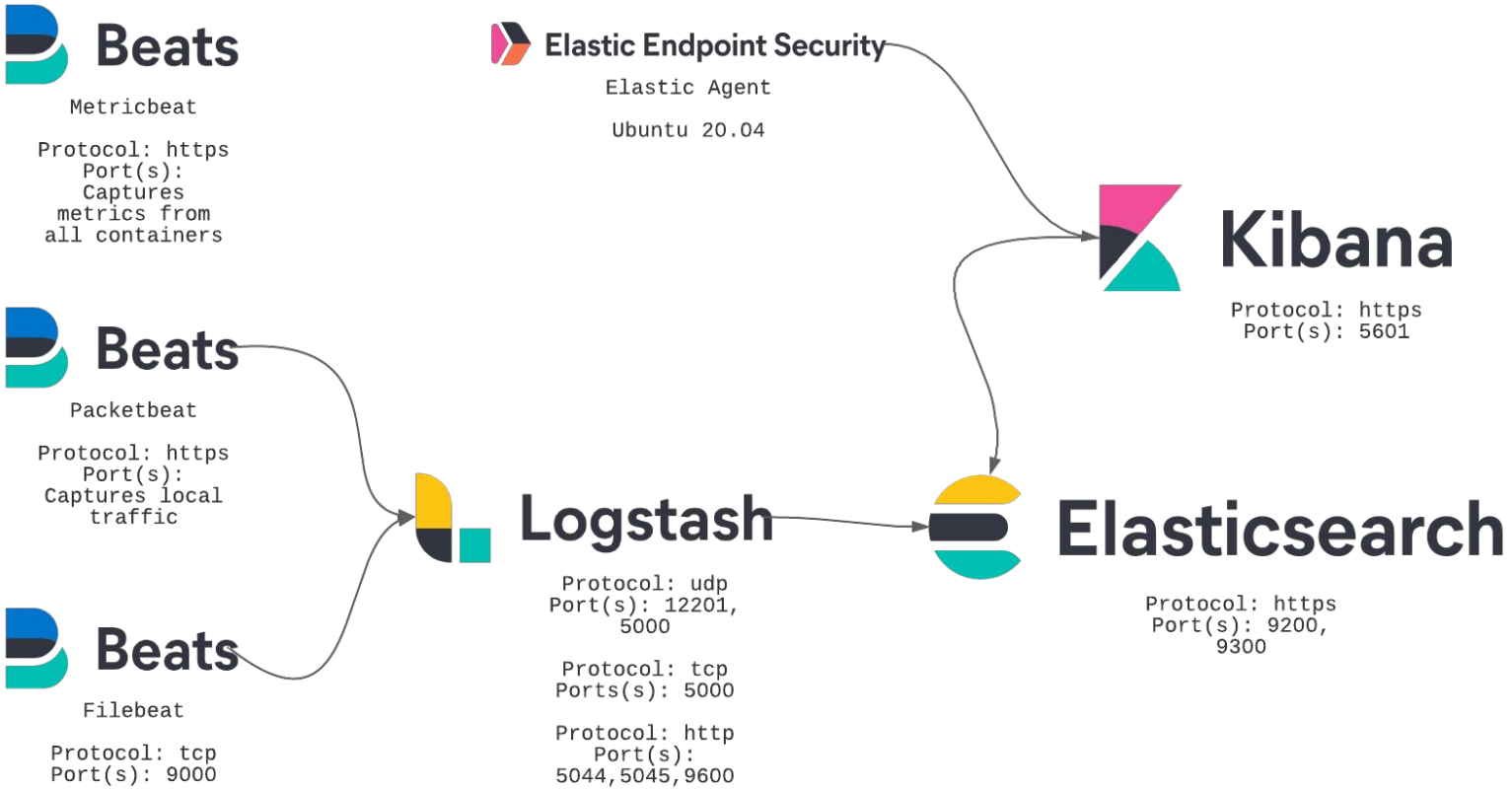
ELK стек – движение данных



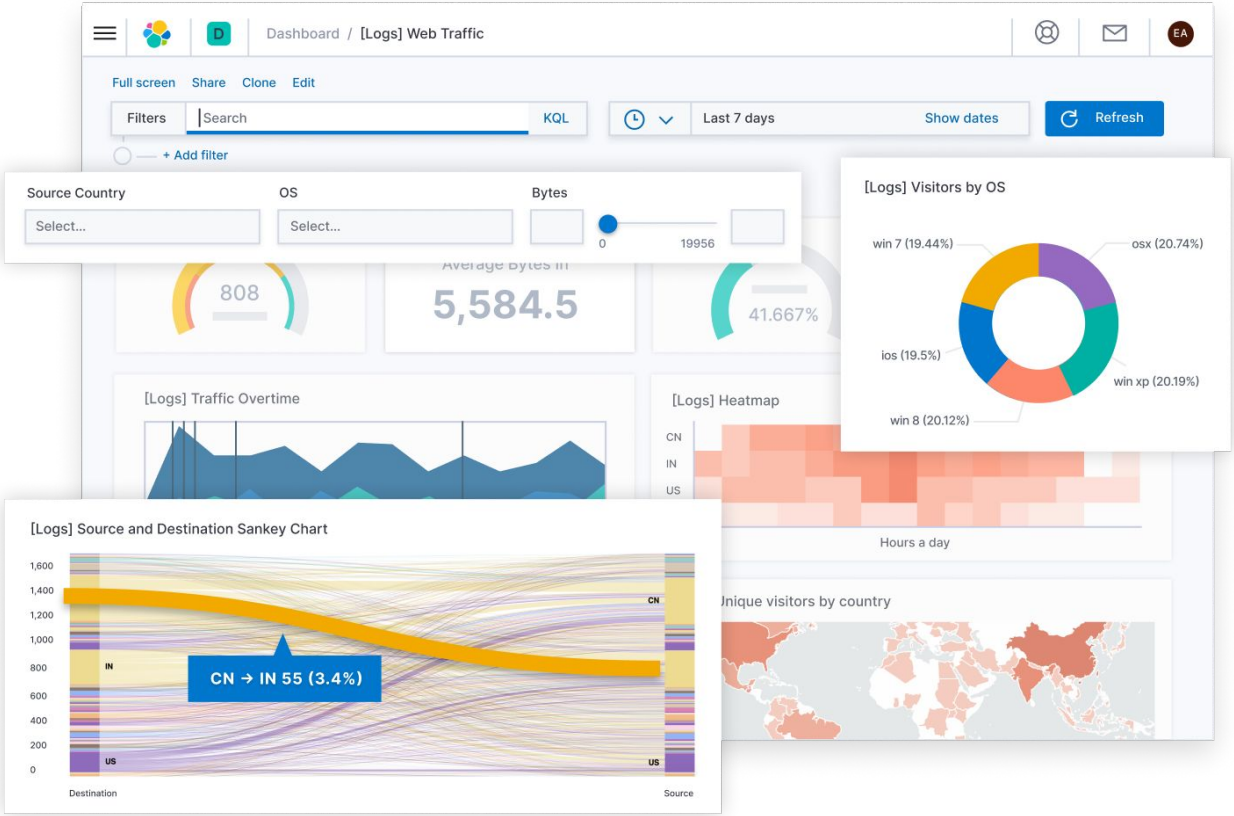
ELK стек – движение данных 2



ELK стек – взаимодействие



Визуализация данных (Kibana)



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.elastic.co/guide/en/kibana/current/install.html
2. https://www.elastic.co/guide/en/elasticsearch/reference/current/install-elasticsearch.html
3. https://www.digitalocean.com/community/tutorials/how-to-use-journalctl-to-view-and-manipulate-systemd-logs-ru
4. https://max-ko.ru/33-logi-v-linux-1.html
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
7. https://grokdebugger.com/
8. https://github.com/cjslack/grok-debugger/tree/master/public/patterns

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://t.me/methodlab_tg
https://www.methodlab.ru/
https://www.youtube.com/c/NickLavlinsky
https://www.youtube.com/@site_support
https://vk.com/nick.lavlinsky