

# Оглавление

Об авторах .....	13
О научном редакторе .....	15
Предисловие .....	16
Структура книги.....	16
Что вам понадобится для работы .....	18
Для кого предназначена книга .....	18
Условные обозначения.....	18
Загрузка примеров кода.....	19
Скачивание цветных изображений, использованных в книге .....	19
<b>Глава 1. Введение в Elastic Stack.....</b>	<b>20</b>
Что такое система Elasticsearch и чем она хороша .....	21
Неструктурированность и документоориентированность.....	21
Поиск.....	22
Анализ данных .....	23
Поддержка пользовательских библиотек и REST API .....	23
Легкое управление и масштабирование.....	23
Работа в псевдореальном времени.....	24
Высокая скорость работы.....	24
Устойчивость к ошибкам и сбоям.....	24
Обзор компонентов Elastic Stack.....	25
Elasticsearch.....	25
Logstash.....	25
Beats.....	26

Kibana.....	26
X-Pack .....	27
Elastic Cloud.....	28
Способы применения Elastic Stack.....	28
Анализ и безопасность логов.....	29
Поиск по продуктам.....	29
Анализ показателей.....	30
Веб-поиск и поиск по сайту.....	30
Скачивание и установка .....	31
Установка Elasticsearch.....	31
Установка Kibana.....	32
Резюме.....	32
<b>Глава 2. Начало работы с Elasticsearch .....</b>	<b>34</b>
Пользовательский интерфейс Kibana Console .....	34
Основные понятия Elasticsearch.....	36
Индекс.....	37
Тип .....	38
Документ.....	38
Узел.....	39
Кластер .....	39
Шарды и копии.....	40
Разметка и типы данных.....	42
Обратный индекс .....	47
Операции CRUD.....	48
Index API.....	48
Get API .....	50
Update API .....	50
Delete API.....	52
Создание индексов и контролирование разметки.....	52
Создание индекса.....	53
Создание разметки типов в существующем индексе .....	54
Обновление разметки.....	55
Обзор REST API.....	56
Общие правила API .....	57
Управление несколькими индексами .....	58
Резюме.....	60

<b>Глава 3. Поиск — вот что важно</b> .....	61
Основы анализа текста.....	61
Анализаторы Elasticsearch .....	62
Использование встроенных анализаторов.....	66
Добавление автозавершения в пользовательском анализаторе .....	70
Поиск по структурированным данным .....	74
Запрос диапазона .....	75
Запрос существования .....	78
Term-запрос.....	79
Полнотекстовый поиск .....	80
Запрос соответствия .....	82
Запрос соответствия фразы.....	85
Запрос нескольких соответствий .....	87
Написание составных запросов .....	88
Запрос постоянной оценки.....	88
Булев запрос .....	91
Резюме.....	94
<b>Глава 4. Анализ данных с помощью Elasticsearch</b> .....	96
Основы агрегации .....	96
Сегментарные агрегации .....	97
Метрические агрегации .....	98
Матричные агрегации .....	98
Агрегации контейнеров .....	98
Подготовка данных к анализу .....	99
Загрузка данных с помощью Logstash .....	102
Метрические агрегации .....	103
Агрегации суммы, среднего, максимального и минимального значений.....	103
Агрегации статистики и расширенной статистики.....	106
Агрегация мощности.....	108
Сегментарные агрегации .....	109
Сегментирование строковых данных.....	109
Сегментирование числовых данных .....	114
Агрегирование отфильтрованных данных.....	117
Вложенные агрегации .....	118
Сегментирование с нестандартными условиями.....	121
Сегментирование данных даты/времени .....	123
Сегментирование геопространственных данных.....	129
Агрегации контейнеров.....	132
Резюме.....	134

<b>Глава 5. Анализ журнальных данных.....</b>	<b>136</b>
Вызовы при анализе логов.....	136
Logstash.....	138
Архитектура Logstash .....	142
Обзор плагинов Logstash.....	144
Установка или обновление плагинов .....	145
Обзор плагинов.....	148
Узел поглощения данных.....	158
Определение контейнера .....	158
Ingest API.....	159
Резюме.....	162
<b>Глава 6. Разработка контейнеров данных с помощью Logstash.....</b>	<b>163</b>
Обработка и дополнение логов с помощью Logstash .....	163
Плагины фильтрации.....	164
Введение в Beats.....	171
Beats от Elastic.co .....	173
Компоненты Beats от сообщества .....	174
Logstash против Beats.....	175
Filebeat .....	176
Скачивание и установка Filebeat.....	176
Архитектура.....	178
Настройка Filebeat.....	179
Резюме.....	190
<b>Глава 7. Визуализация данных в Kibana .....</b>	<b>191</b>
Скачивание и установка Kibana.....	191
Установка в Windows.....	192
Установка в Linux.....	192
Настройка Kibana .....	194
Подготовка данных.....	195
Пользовательский интерфейс Kibana.....	196
Взаимодействие с пользователем.....	197
Настройка шаблона индекса .....	198
Исследование .....	200
Визуализация .....	213
Создание визуализации.....	216
Типы визуализаций.....	218
Визуализации в деле.....	219

Панели управления .....	226
Timelion .....	230
Использование плагинов.....	234
Установка плагинов .....	234
Удаление плагинов.....	235
Резюме.....	235
<b>Глава 8. Elastic X-Pack.....</b>	<b>236</b>
Установка X-Pack .....	236
Установка X-Pack в Elasticsearch.....	236
Установка X-Pack в Kibana .....	239
Удаление X-Pack.....	240
Настройка X-Pack.....	240
Безопасность.....	241
Пользовательская аутентификация .....	241
Авторизация пользователя.....	243
Безопасность на деле .....	245
Мониторинг Elasticsearch .....	260
Раздел Monitoring (Мониторинг) пользовательского интерфейса .....	261
Метрики Elasticsearch .....	262
Уведомления.....	267
Структура наблюдателя.....	268
Уведомления в деле .....	272
Резюме.....	279
<b>Глава 9. Запуск Elastic Stack в работу.....</b>	<b>280</b>
Размещение Elastic Stack в управляемом облаке .....	280
Настройка и запуск Elastic Cloud.....	281
Использование Kibana .....	283
Изменение настроек.....	283
Восстановление .....	284
Размещение Elastic Stack на своем хостинге.....	285
Выбор аппаратной части .....	285
Выбор операционной системы .....	286
Настройка узлов Elasticsearch.....	286
Управление Elasticsearch и ее мониторинг .....	287

Запуск в контейнерах Docker .....	287
Особенности запуска в облаке .....	288
Резервное копирование и восстановление .....	291
Настройка репозитория для снапшотов .....	291
Облако распределенных файловых систем .....	292
Создание снапшотов .....	293
Восстановление из определенного снапшота .....	293
Присвоение псевдонимов индексам .....	294
Что такое псевдонимы индексов .....	294
Чем могут помочь псевдонимы индексов .....	295
Настройка шаблонов индексов .....	295
Определение шаблона индекса .....	296
Создание индекса на ходу .....	296
Моделирование данных временного ряда .....	297
Масштабирование индекса с непредсказуемым объемом через некоторое время .....	297
Изменение разметки со временем .....	299
Автоматическое удаление более старых документов .....	299
Как временный индекс решает эти проблемы .....	300
Резюме .....	301
<b>Глава 10. Создание приложения для анализа данных с датчиков .....</b>	<b>302</b>
Введение в приложение .....	302
Создаваемые датчиками данные .....	304
Метаданные с датчиков .....	304
Окончательно сохраняемые данные .....	306
Моделирование данных в Elasticsearch .....	307
Настройка базы метаданных .....	309
Создание контейнера данных Logstash .....	310
Прием запросов JSON по сети .....	311
Дополнение JSON метаданными из нашей базы данных MySQL .....	312
Сохранение в Elasticsearch полученных в результате документов .....	315
Отправка данных в Logstash через HTTP .....	316
Визуализация данных в Kibana .....	317
Настройка шаблона индекса в Kibana .....	317
Создание визуализаций .....	318
Создание панели управления .....	324
Резюме .....	326

<b>Глава 11. Мониторинг серверной инфраструктуры.....</b>	<b>328</b>
Metricbeat.....	328
Скачивание и установка Metricbeat .....	328
Архитектура.....	330
Настройка Metricbeat .....	334
Конфигурация модуля .....	334
Общие настройки.....	336
Конфигурация вывода .....	337
Логирование .....	339
Сбор системных метрик.....	339
Запуск Metricbeat с модулем system .....	340
Указание псевдонимов.....	343
Визуализация системных метрик в Kibana .....	344
Архитектура внедрения .....	347
Резюме.....	349