

SimbirSoft

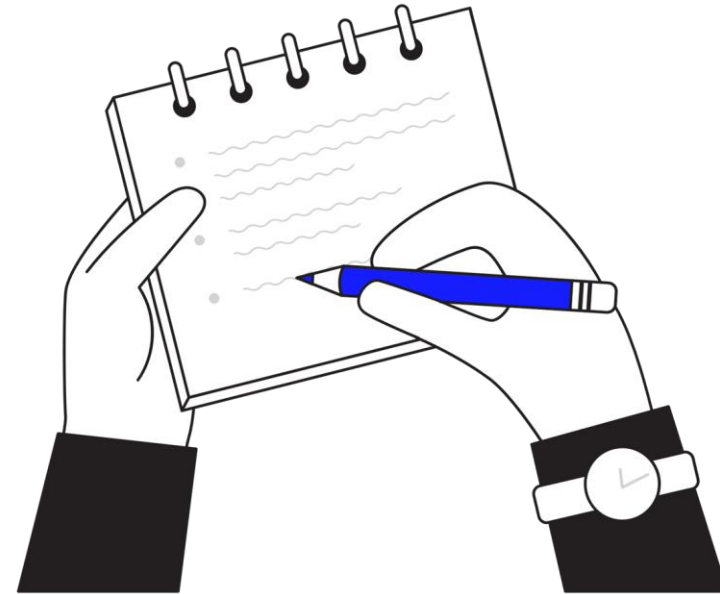
Укращение логов

Даценко В.

Краснодар, 2024

Для чего нужна система логирования?

- Единая точка хранения и доступа к логам;
- расширенные возможности для обработки, анализа и визуализации логов;
- удобное хранение и архивация логов;
- безопасность и контроль доступа.



Какие бывают системы логирования?



graylog



Open Distro



Какие бывают системы логирования?



graylog



Open Distro

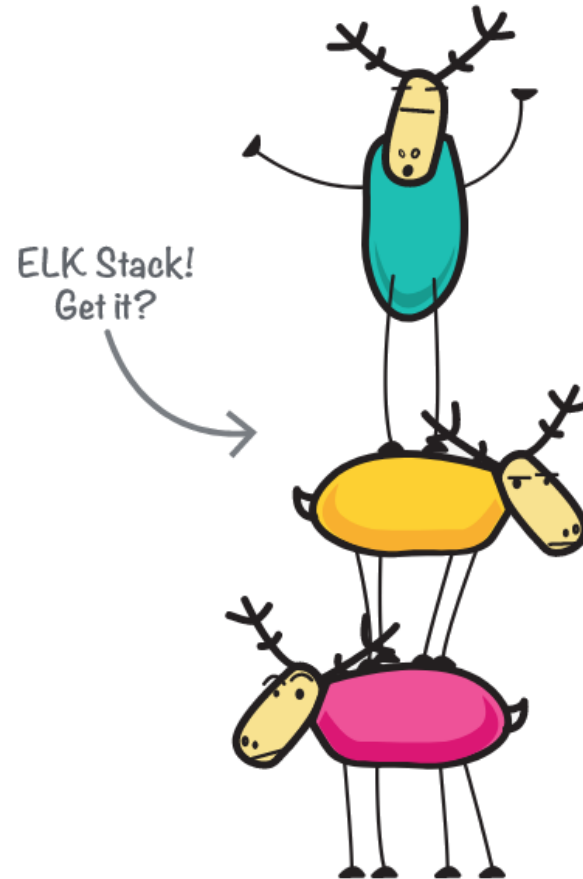


Grafana loki

ЧТО ВХОДИТ В ELK?

- Elasticsearch;
- Logstash;
- Kibana;
- Beats:
 - Filebeat;
 - Metricbeat;
 - Packetbeat;
 - ...
- X-Pack (\$)

non-Apache 2.0 license (≥ 7.11)



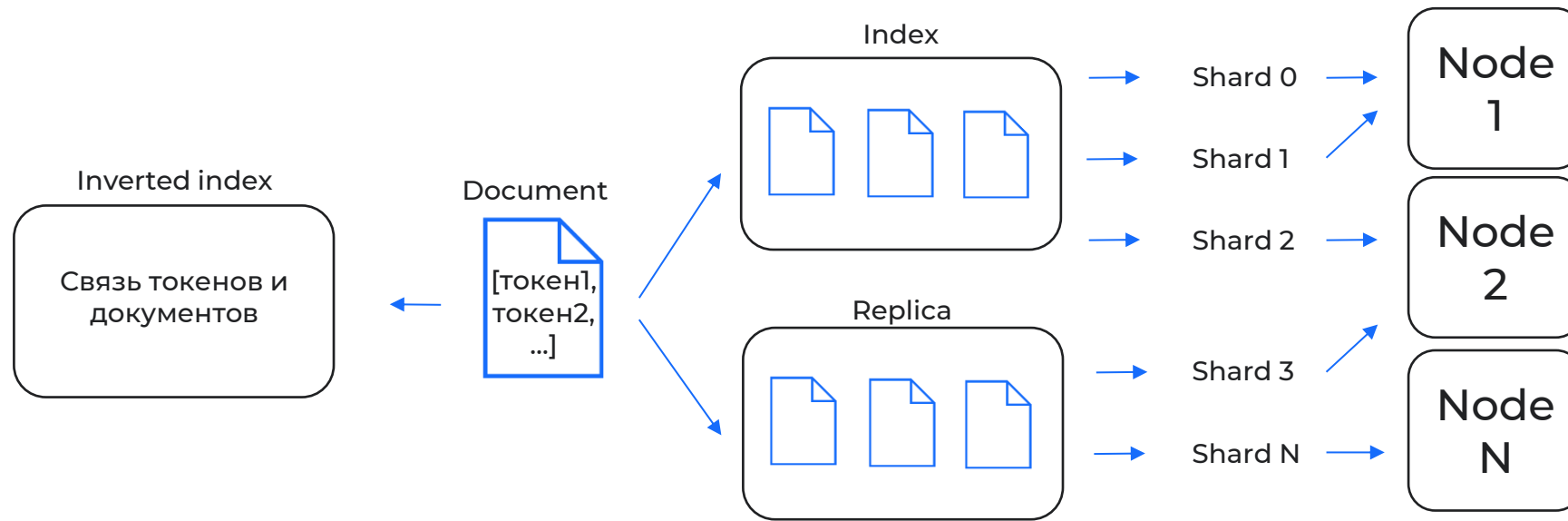
E Elasticsearch

L Logstash

K Kibana

Что такое Elasticsearch?

- NoSQL-хранилище JSON-подобных документов;
- поисковая и аналитическая система;
- обеспечивает возможность горизонтального масштабирования;
- управляет жизненным циклом данных.

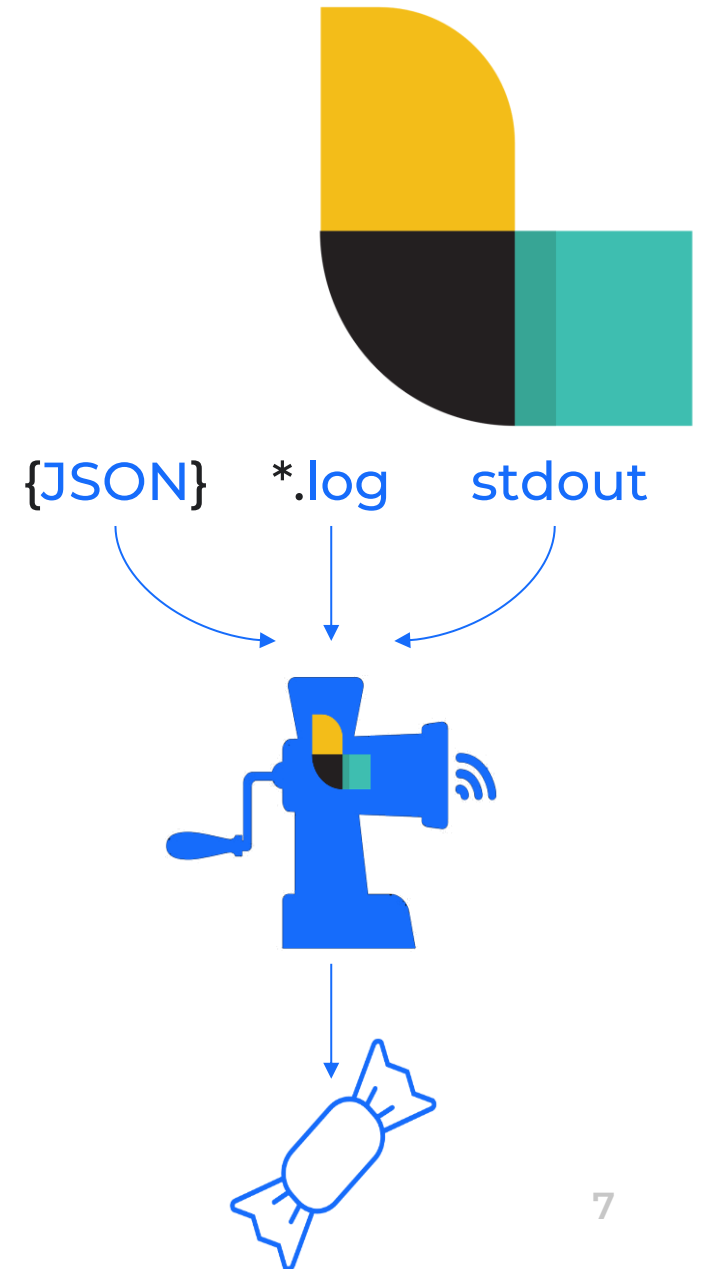


Что такое Logstash?

Конвейер по парсингу данных одновременно из множества источников, их обработки и вывода.

Фазы обработки Logstash:

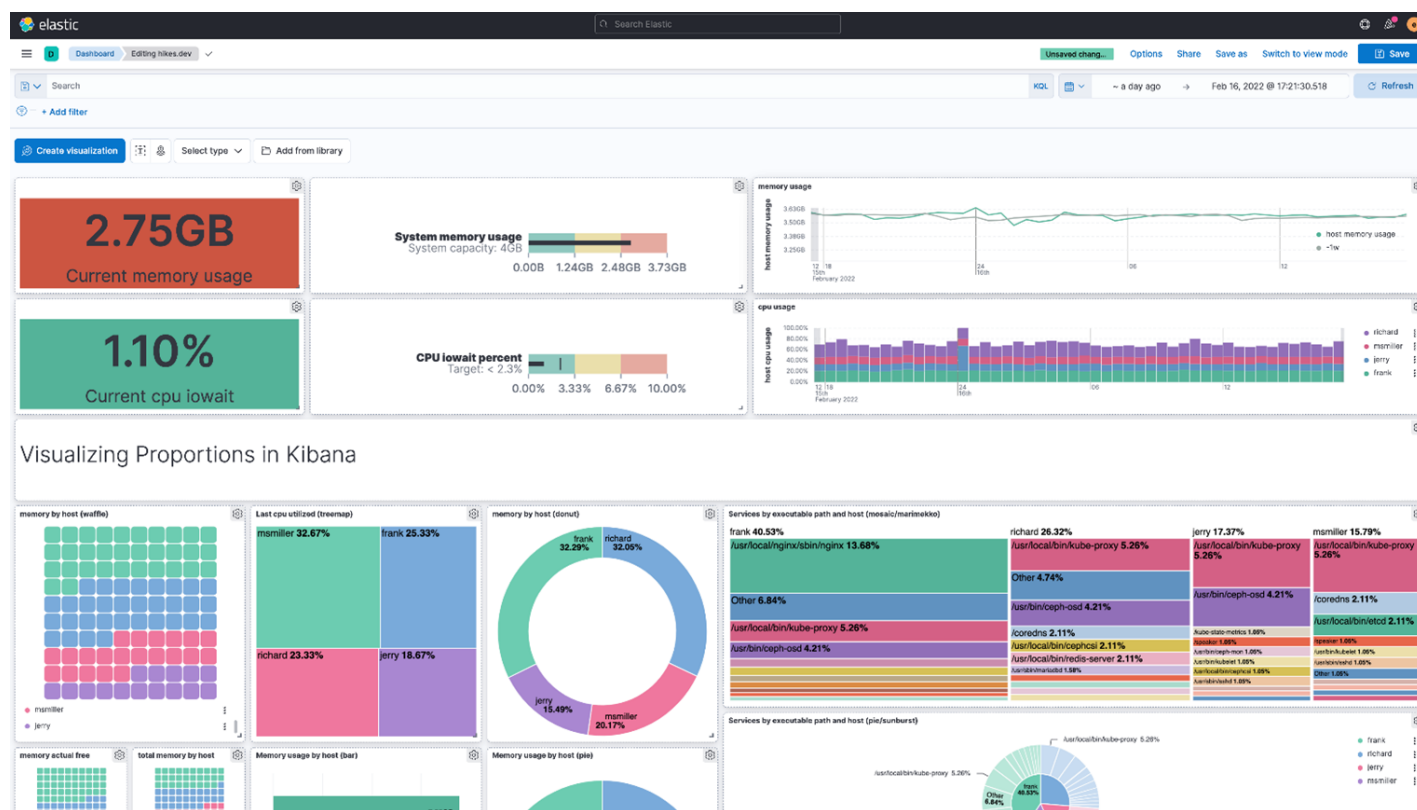
- input – откуда принимаем данные (file, port, Apache Kafka и т.д.);
- filter – преобразование данных (парсинг, дополнение, обфускация и т.д.);
- output – куда выводим данные (Elasticsearch, console, file и т.д.)



Что такое Kibana?

Инструмент визуализации и анализа данных.

Создает интерактивные дашборды, графики и отчеты из Elasticsearch.

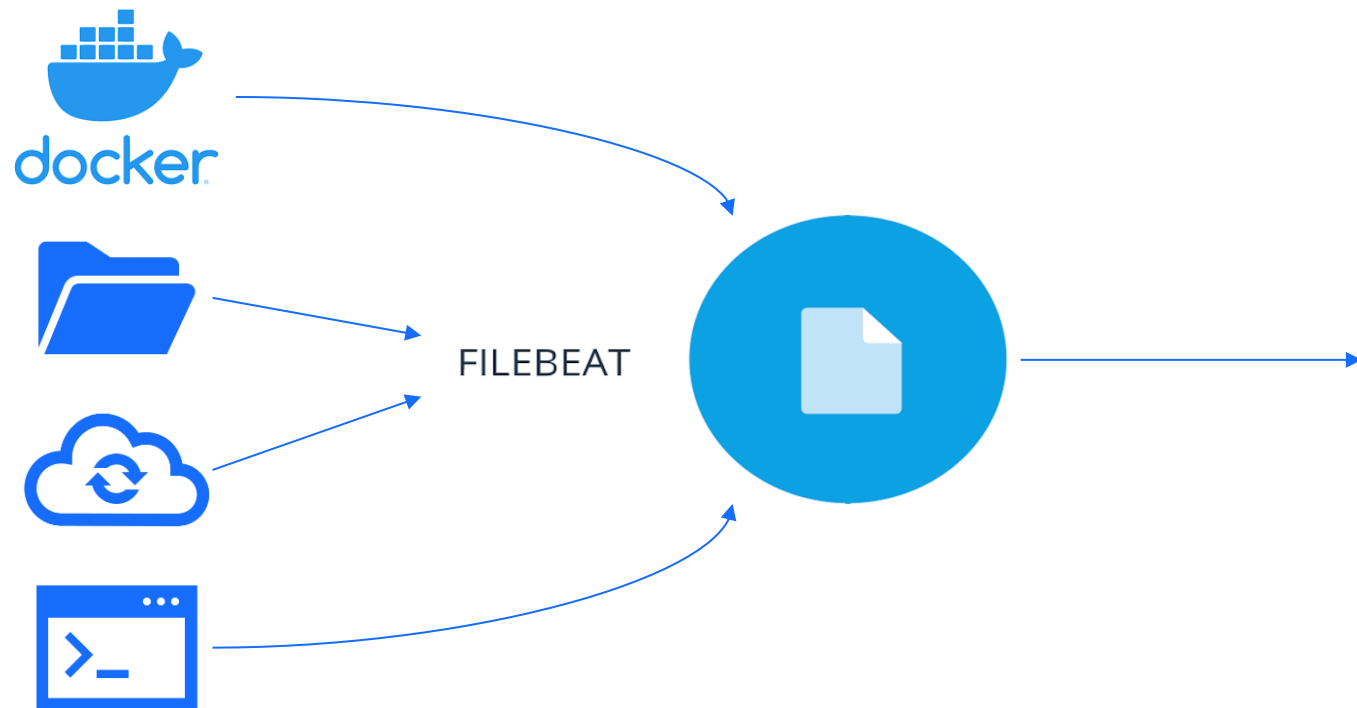


Что такое Beats?

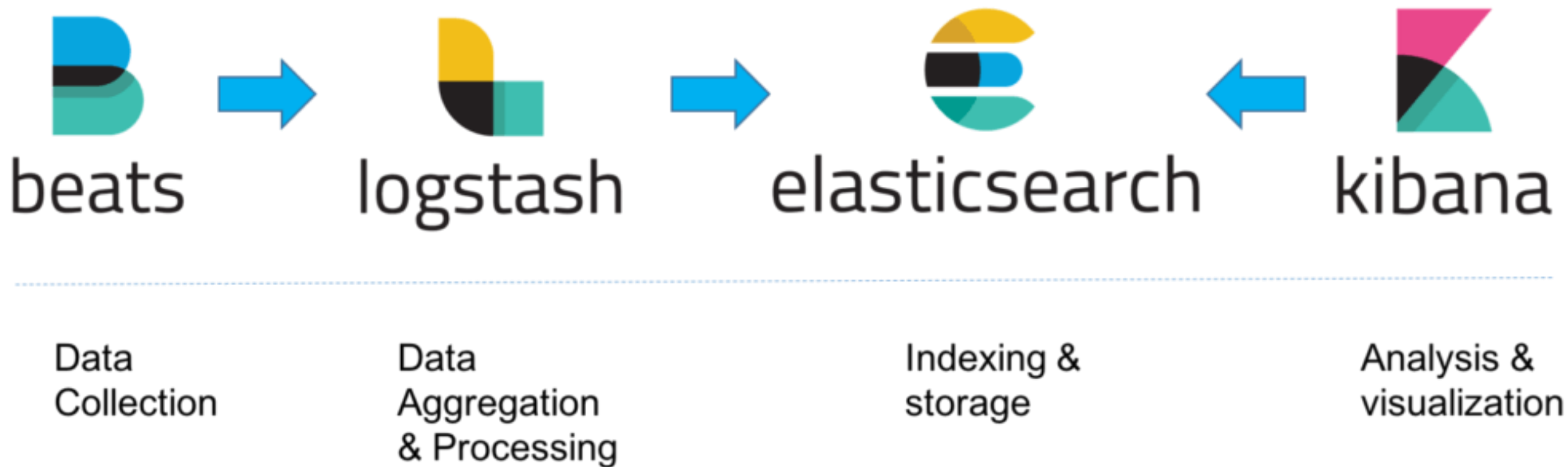
Утилиты, собирающие данные и отправляющие их по заданному адресу.

Примеры:

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



Как взаимодействует ELK?



SimbirSoft

Спасибо за внимание



[SimbirFriends](#)

Порекомендуйте друга —
получите вознаграждение!



[GitHub](#)

Материалы
презентации