УДК 004.062
В. Василенко, Н. Стадник
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИКОРИСТАННЯ СТАКУ ELK ДЛЯ ДОСЛІДЖЕННЯ ПОДІЙ

UDC 004.062
V. Vasylenko, N. Stadnyk

USING ELK STACK TO RESEARCH OF EVENTS

Logstash – це засіб для збору, фільтрації та структуризації log-файлів (подій). Це безплатний та open source додаток, створений на базі Apache Lucene. Додаток Logstash входить до стаку ELK - Elasticsearch, Logstash і Kibana, де Elasticsearch – пошукова і аналітична система, Logstash – серверний конвеєр для обробки даних, який може отримувати дані одночасно з декількох джерел, переробляти їх та відправляти на сервер, в нашому випадку – це Elasticsearch. Kibana – засіб для візуального подання інформації, який дозволяє створювати різні діаграми та графіки з інформації, яка знаходиться в Elasticsearch.

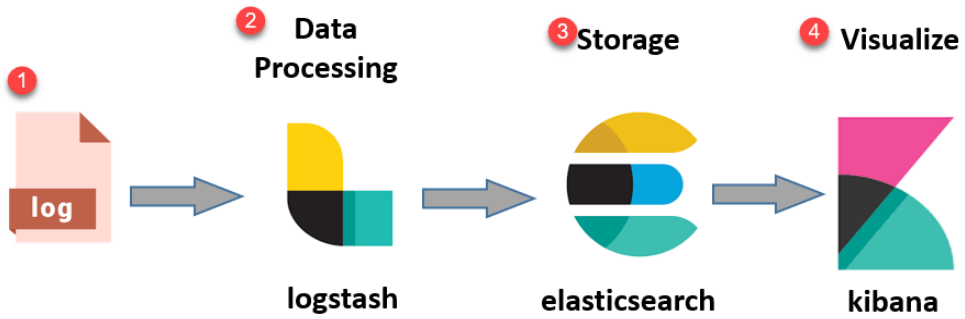

Рисунок 1. Схема роботи стаку ELK

Logstash використовує спеціальні вирази, які називаються грок патерни (grok-patterns) для розбору log-файлів. Grok – це фільтр всередині Logstash, який використовується для структуризації неструктурованих даних. Він знаходиться поверх регулярного виразу (regex), і використовує текстові шаблони для зіставлення рядків у файлах журналів. Logstash постачається з більш ніж 100 вбудованих шаблонів, які можна використати для загальних системних журналів apache, linux, haproxy, aws тощо. Також є можливість написання свого власного патерну, за яким буде розбиратись лог. Для цього можна використати спеціалізовані сервіси для написання патерну, одним з найкращих є грок дебагер «herokuapp», в якому можна знайти приклади для різних частин логу. Синтаксис шаблону патерну виглядає наступним чином – %{SYNTAX:SEMANTIC}.

Після написання патерну, який буде проходитись по всіх рядках log-файлу, потрібно відправити структуровані файли на Elasticsearch. Після цього отримані дані можна буде візуалізувати за допомогою багатьох вбудованих засобів та візуалізацій, до яких входять різноманітні графіки і таблиці.

Література

1. What is the ELK Stack? URL: https://www.elastic.co/what-is/elk-stack.
2. The complete guide to the elk stack. URL: https://logz.io/learn/complete-guide-elk-stack/.
3. ELK Stack Tutorial: What is Kibana, Logstash & Elasticsearch? URL: https://www.guru99.com/elk-stack-tutorial.html.