УДК 004:621.391

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СТЕКУ ПРОГРАМ ELASTIC STACK В ОБОЛОНЦІ UNIX-ПОДІБНОЇ СИСТЕМИ

Муха Р.В.
Науковий керівник – к.т.н., доц. Токар Л.О.
Харківський національний університет радіоелектроніки,
кафедра ІКІ ім В.В. Поповського,
м. Харків, Україна
тел. +38(099) 556-76-02

The problems when working with logs were analyzed, the main points that hinder the quality analysis of log files were identified. General provisions on the open source product - the Elastic Stack (ELK) program stack, which is proposed to be used for transparent analysis of log files in real time, are provided. The purpose and method of using ELK when working with Unix-like systems are given. The possibilities and features of using rsyslog in combination with ELK to improve data monitoring and analysis have been revealed.

Адміністраторам різних сфер діяльності необхідно переглядати лог-файли. Це може стосуватися різних галузей, таких як інформаційна безпека, IT-інфраструктура, розробка програмного забезпечення, аналіз трафіку та веб-аналітика, фінансова аналітика, медицина, енергетика, телекомунікації, IoT, автоматизоване виробництво. Перегляд лог-файлів дозволить вирішити проблеми виявлення помилок, захищення від зловмисної активності та збір статистики відвідувань й аналізу подій. Для досягнення максимальної гнучкості та ефективності в роботі використано стек програм Elastic Stack на Unix-подібній системі.

Аналіз лог-файлів у інфокомунікаціях створює ряд проблем, що ускладнюється через велику кількість різноманітних журналів. У кожного додатку різні формати, що робить процес читання лог-файлу досить складним, незручним, монотонним заняттям. Відсутність централізованого збірника інформації призводить до виникнення проблеми знаходження місця зберігання лог-файлів, необхідного застосунку, а також визначення формату. Крім того, слід відмітити, що для кожного окремого застосунку існують різні програми для обробки лог-файлів.

Це й робить використання комплексного інструменту – стеку програм ELK (Elasticsearch, Logstash, Kibana) доцільним.

Використання Elastic Stack дозволить не тільки подолати вказані проблеми, а ще й принести додаткову користь, що полягає в використанні єдиного додатку для всіх лог-файлів, любого текстового формату та можливості зберігання в єдиному місці – сховищі лог-файлів. Крім того, можливість розробити свої аналізатори дозволить прискорити роботу в пошуках в декілька разів. Візуалізація дозволить значно спростити аналіз даних. Інформацію можна представляти наглядно у формі графіків,

кругових та стовпчикових діаграм. Веб-додатки надають можливість виконувати різноманітні дії з любого пристрою, на любій операційній системі. Оскільки стек ELK є open source програмним забезпеченням, то це є важливою перевагою для перегляду, використання та модифікацій тощо.

Стек програм Elastic Stack встановлюється на різних операційних системах (Windows, MacOS, Linux), що вимагає деяких попередніх налаштувань, наприклад, встановлення віртуальної машини Java. Однак, ELK Stack першочергово розроблено для роботи з Unix-подібними операційними системами, таким чином встановлення його на Ubuntu може бути більш природнім та оптимальним.

Для покращення моніторингу та аналізу даних в роботі запропоновано використати інструмент збору логів даних rsyslog. Він стандартно встановлюється на дистрибутивах Linux і може збирати дані з різних джерел та пересилати їх на централізований сервер логування. В поєднанні з Elastic Stack rsyslog може збирати дані та передавати їх у форматі JSON, необхідному для Elasticsearch. При цьому налаштовується сервер для використання шаблону JSON та створення нового конфігураційного файлу на rsyslog-server, який буде форматувати лог-файли в JSON перед їх передачею до інструментів Logstash та Elasticsearch.

Архітектуру Elastic Stack для Unix-подібних систем наведено на рис. 1.

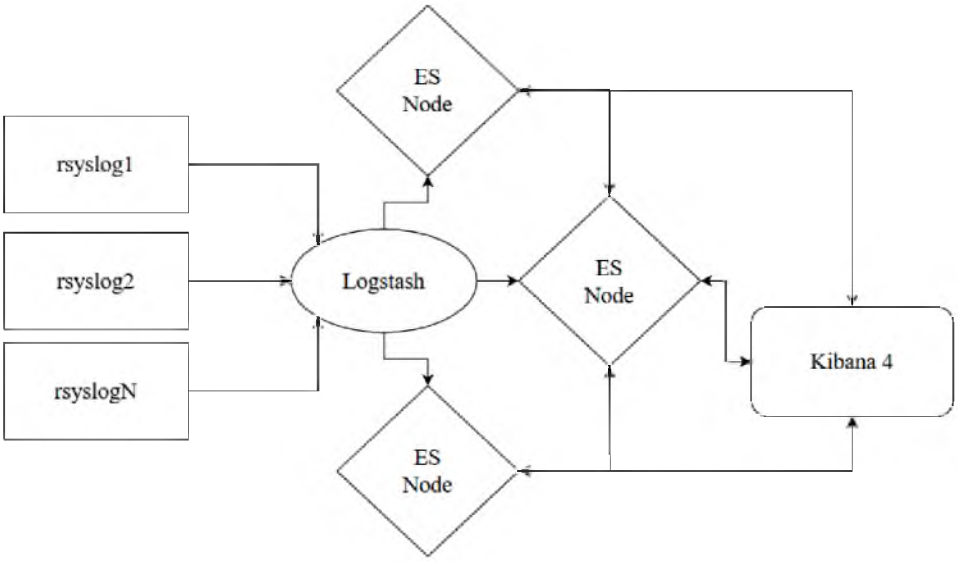

Рисунок 1 – Архітектура Elastic Stack для Unix-подібних систем

Текстові дані у вигляді лог-файлу надходять до програми-сервісу rsyslog, в свою чергу rsyslog надсилають дані в програму Logstash, яка може фільтрувати вхідні дані й розподіляти їх по іншим вузлам, де встановлено Elasticsearch. Після цього отримані результати можна переглянути за допомогою графічного інтерфейсу програми Kibana.