Кушнір І. В., магістрант,
Фальковський І. Г., ст. викладач,
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ СТЕКУ ПРОГРАМ ELASTIC STACK ДЛЯ ЗАБЕЗПЕЧЕННЯ ФУНКЦІЙ МОНІТОРИНГУ, АНАЛІЗУ ТА ВІЗУАЛІЗАЦІЇ ДАНИХ В МЕРЕЖІ

Щоб переконатися, що пристрої працюють надійно та надають відповідні послуги, фахівці у сфері IT аналізують різні типи даних, які генеруються програмними продуктами та пристроями. Такі дані, як логи подій чи метрики надають можливість відстежувати стан систем та оперативно виявляти та реагувати на помилки. Однак кількість пристроїв та обсяг даних невпинно зростають, тому нині є актуальним питанням впровадження централізованої системи, яка б збирали дані з усіх пристроїв в одному місці й дозволила б проводити аналіз отриманої інформації. І одним з таких популярних рішень є стек ElasticStack.

ElasticStack (раніше ELK Stack) – це набір з трьох безоплатних інструментів з відкритим вихідним кодом: Elasticsearch, Logstash та Kibana, які призвані допомогти користувачам збирати, зберігати, шукати, аналізувати та візуалізувати великі обсяги даних, зокрема журнали подій, метрик. Даний набір може бути встановлений на всіх відомих популярних ОС, як Windows, Linux, MacOS та бути розгорнутою в хмарному середовищі або в Docker-контейнері. Даний стек програм дозволяє надійно та швидко отримувати дані з будь-якого джерела у всіх форматах та опрацьовувати інформацію: здійснювати пошук за певними фільтрами, аналізувати, візуалізувати і все це в режимі реального часу. ElasticStack дозволяє зручно контролювати стан пристроїв та додатків на одному місці та швидко виявляти проблеми або розв`язувати задачі пов’язані з аналізом інформації.

Elasticsearch – високо масштабований повнотекстовий пошуковий і аналітичний двигун з відкритим вихідним кодом (заснований на Lucene) і фактично є ядром ElasticStack. Даний продукт дозволяє зберігати, шукати та аналізувати великі обсяги даних у реальному часі. Elasticsearch є документо-орієнтованою базою даних в якій інформація зберігається у вигляді серіалізованих документів JSON, що дозволяє зберігати довільні структури даних.

Logstash – засіб для обробки даних з відкритим вихідним кодом. На вході отримує сирі дані (логи) з декількох джерел і залежно від налаштувань отримана інформація оброблюється, нормалізуються, застосовуються певні фільтри і вже на виході отримуємо уніфікований формат даних, який можна надсилати до отримувача, в цьому випадку до Elasticsearch. Однак Logstash не є обов’язковою ланкою: інформацію з пристроїв можна в необробленому вигляді відправляти напряму до Elasticsearch, якщо відсутня потреба в стандартизації та фільтрації даних.

Kibana – це популярний інструмент для візуалізації даних і створення детальних звітів. Kibana дозволяє створювати різноманітні види графіків, діаграм, звітів на основі даних отриманих від Elasticsearch.

Для забезпечення передачі даних з пристроїв і додатків використовуються так звані Beats – спеціальні агенти для відправлення даних в Logstash або Elasticsearch. Відповідно до того, які дані необхідно передавати (журнали, метрики тощо) кожен з відповідних Beats необхідно встановлювати та налаштовувати індивідуально. Однак для полегшення процесу налаштування пропонується використовувати ElasticAgent, який так само, як Beat передає дані до Logstash або Elasticsearch, але встановлюється лише один раз на систему і після цього ним можна централізовано керувати з панелі Fleet в головному меню ElasticStack.

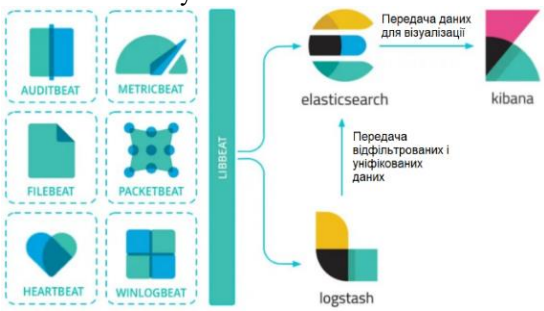

Рис. 1. Типова архітектура ElasticStack

В доповіді буде представлено використання набору програм ElasticStack для забезпечення функцій моніторингу, збору, аналізу та візуалізації даних з пристроїв локальної мережі.

Список використаних джерел

1. Що таке ElkStack? [Електронний ресурс] – Режим доступу: https://freehost.com.ua/ukr/faq/articles/chto-takoe-elk-stack/
2. ElasticStack – потужний інструмент для пошуку та аналізу даних. [Електронний ресурс] – Режим доступу: https://108.in.ua/elastic-stack-potuzhnyj-instrument-dlya-poshuku-ta-analizu-danyh