

## ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ КОМПЛЕКСА ПРОГРАММ ELK STACK

Лябах А.С. Хачиров Е.Ф.

Научный руководитель – доц., к.т.н. Токарь Л.А. Харьковский национальный университет радиоэлектроники (61166, Харьков, пр. Науки, 14, кафедра инфокоммуникационной инженерии им. В.В. Поповского, тел.

The complex of ELK Stack software products has been analyzed. It is shown that this is an excellent solution for fast troubleshooting in the code, and a very convenient tool for developers, as well as for creating or implementing individual elements in large projects. It has been brought to the attention of ELK functionality that allows it to be used as a central repository of logs, an event aggregator with convenient navigation, as well as an analytical system with a machine learning algorithm.

Деятельность любой организации, предоставляющей определенные ресурсы, направлена на получение дохода. В связи с чем, при предоставлении любой услуги, например видео, аудио, хостинга, IP-телефонии, необходимо рассчитать их стоимость, а также провести расчеты с конечными пользователями. Таким образом, устанавливается своя мера, их характеризующая ресурсы: время, мегабайты и т.д. Поэтому возникает вопрос биллинга, что и определяет актуальность данной работы.

Основная проблема заключается в том, что для биллинга не так уж много готовых инструментов. Кроме того, они все являются платными.

Одним из решений данного вопроса предложено использовать комплекс программ ELK Stack, который является бесплатным, отвечает широким потребностям, предоставляет удобную и гибкую статистику, которая необходима для работы.

ELK расшифровывается как elasticsearch, logstash и kibana. Ранее это были три самостоятельных продукта, но позже стали принадлежать одной компании и развиваться в одном направлении. Каждый из этих инструментов (с небольшими примечаниями) является полноценным независимым open source продуктом, а вместе они составляют мощное решение для широкого спектра задач сбора, хранения и анализа данных.

Logstash – это утилита для сборки, фильтрации и последующего перенаправления в конечное хранилище данных. Ее другое название fluentd – logstash, но данная утилита решает ту же самую задачу и написана на jruby и более совместима с elasticsearch.

Elasticsearch – это решение для полнотекстового поиска, построенное поверх Apache Lucene, но с дополнительными удобствами в виде легкого масштабирования, репликации и прочих преимуществ, которые сделали elasticsearch очень удобным и хорошим решением для высоконагруженных проектов с большими объемами данных. Особенно привлекает в elasticsearch его простота и работоспособность сразу после установки. Конфигурация по-умолчанию работает для проектов средней и относительно высокой нагрузки. При этом вокруг ES сложилось отличное сообщество, которое всегда подскажет, как правильно настроить ваш ES-кластер для конкретной задачи.

Kibana, позволяет брать\искать данные по elasticsearch и строить множество интересных графиков. Это очень удобный интерфейс, позволяющий пользователю компании построить интерактивную панель для вывода аналитики того, что logstash отправил в elasticsearch.

ELK Stack позволяет проводить мониторинг большого количества данных, фильтровать их, и при необходимости производить быстрый поиск. Таким образом, это мощный инструмент, для сбора и фильтрации логов, что позволит использовать stack для биллинга во многих системах, а также значительно сократить расходы. Еще одним преимуществом является простота установки, однако для этого потребуются определенные навыки для настройки фильтров.

В результате адекватного выбора предложенного комплекса программ ELK Stack можно получить мощную CMS систему, которая способна обрабатывать огромное количество данных в секунду, предоставлять подробные отчеты, а также позволит сторонним разработчикам модифицировать систему.

Список источников:

1. Elastic Stack and Product Documentation [Электронный ресурс], Режим доступа: <https://www.elastic.co/guide/index.html>. - 2019.
2. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Интеллектуальные сети. — М.: Радио и связь, 2000.