УДК 004.415.5
А.О. Волоха; Л.П. Дмитроца, к.т.н
(Тернопільський національний технічний університет імені Івана Пулюя)

РЕЗУЛЬТАТИ МОНІТОРИНГУ ТА АВТОМАТИЗАЦІЇ КЕРУВАННЯ СЕРВЕРАМИ В ВИСОКОНАВАНТАЖЕНИХ СИСТЕМАХ

UDC 004.415.5
A. Volokha, L. Dmytrotsa, Ph.D

RESULTS OF MONITORING AND AUTOMATION OF SERVER CONTROL IN HIGHLY LOADED SYSTEMS

Щодня створюється величезна кількість файлів журналів під час роботи серверів в компаніях, об'єм яких може сягати від декількох гігабайтів до сотень гігабайтів в день. Данні файли дуже великі та непридатні для аналізу людиною на наявність проблем чи аномалій. Стек Elastic, далі ELK, покращив чотири області:

1. Повторення розслідувань. Автоматизуючи виявлення нових випадків відомих проблем, було зменшено кількість дубльованих досліджень, тим самим підвищено ефективність діагностики. Це здійснюється шляхом створення запитів Elasticsearch, які визначають конкретну проблему та подання їх у інформаційну панель Kibana. Інформаційна панель, що показує випадки, що відбулися за останні 24 години відображається на великому екрані перед інженером підтримки. Таким чином, призначена особа може одним поглядом знати, що сталася відома проблема, і за допомогою повідомленої мітки часу, пов'яже це з проблемою, що нещодавно повідомлялася.
2. Висока мінливість. Навіть якщо ELK не може безпосередньо допомогти контролювати велику мінливість кількості виготовлених квитків, це ефективно допомагає швидко ідентифікувати квитки у відставанні: як тільки проблема виявляється за допомогою elasitcsearch пошукового запиту, запит виконується з пошуком екземплярів за попередні тижні або місяці. Тоді екземпляри можуть бути пов'язані зі старою, не дослідженою проблемою, про яку повідомлялося, за часом виникнення та опису.
3. Управління журналами. ELK забезпечує швидкий та універсальний спосіб пошуку та фільтрації журналів, завдяки підтримці Lucene API від Elasticsearch та зручному інтерфейсу користувача, наданому Kibana. Поточна архітектура дозволяє нам виконувати швидкі пошуки та фільтри протягом 6 місяців журналів, еквівалентних 6 ТБ, включаючи реплікацію. Однією з переваг цього є отримання за лічені секунди відповіді на запитання типу «Скільки разів ця проблема траплялася за останні місяці?»
4. Відсутність статистики та тенденційної інформації. У Кібані було створено кілька інформаційних панелей, які надають корисну інформацію: чітке уявлення про те, наскільки стабільною була попередній день, скільки спостережень було виконано, яке обладнання було використано; показує кількість журналів, вироблених програмними компонентами. Ненормальна кількість журналів, вироблених компонентом, є гарним показником проблеми. Він також відображає, скільки сигналів тривало в певні години.

Очікується в перспективі підключити стек ELK до Hadoop, Spark та інших рішень для великих даних для повного використання інформації, що міститься в журналах програмного забезпечення, для масштабованості та аналізу тенденцій, а також для характеристики бажаної та небажаної поведінки програмного забезпечення.

Література.

1. Gormley, C. and Tong, Z., [Elasticsearch: The Definitive Guide], " O'Reilly Media, Inc." (2015).
2. Avarias, J. A., Lpez, J. S., Maureira, C., Sommer, H., and Chiozzi, G., "Introducing high performance distributed logging service for acs," Proc. SPIE 7740, 77403G–77403G–10 (2010).

3. Bagnasco, S., Berzano, D., Guarise, A., Lusso, S., Masera, M., and Vallero, S., “Towards monitoring-as-a- service for scientific computing cloud applications using the elasticsearch ecosystem,” in [Journal of Physics: Conference Series], 664(2), 022040, IOP Publishing (2015).
4. RFC 5424 The Syslog Protocol [Електронний ресурс] / Internet Engineering Task Force, March 2009. URL: https: // tools. ietf.org/html/rfc5424
5. Adiscon LogAnalyzer - syslog web viewer, analysis and reporting tool [Електронний ресурс] / Adiscon GmbH. URL: http: // loganalyzer. adiscon.com
6. MonitorWare Knowledge Base [Електронний ресурс] / Adiscon GmbH. URL: http: // kb. monitorware.com/
7. Операційна аналітика, управління журналами, управління додатками, забезпечення безпеки підприємства та відповідності вимогам | Splunk [Електронний ресурс] / Splunk Inc. URL: http://www.splunk.com/ru_ru
8. IBM BigInsights for Apache Hadoop [Електронний ресурс] / IBM Corporation. URL: http: // www-03. ibm.com/software/products/ru/ibm-biginsights-for-apache-hadoop
9. Welcome to Apache ™ Hadoop®! [Електронний ресурс] / The Apache Software Foundation, останнє оновлення 13.02.2016 10: 31: 55. URL: http: // hadoop. apache.org/
10. Fluentd | Open Source Data Collector [Електронний ресурс] / Fluentd Project, Treasure Data, Inc. URL: http://www.fluentd.org/