УДК 004.3
О. Гуменюк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНАЛІЗ РОБОТИ ІНСТРУМЕНТУ ДЛЯ УПРАВЛІННЯ ТА АНАЛІЗУ ЖУРНАЛІВ GRAYLOG

UDC 004.3
O. Humeniuk

PERFORMANCE ANALYSIS OF THE GRAYLOG LOG MANAGEMENT AND ANALYSIS TOOL

Graylog – це потужна платформа, яка дозволяє легко керувати записами структурованих та неструктурованих даних разом із налагодженням додатків. Він заснований на Elasticsearch, MongoDB і Scala.

Він має головний сервер, який приймає дані від своїх клієнтів, встановлених на різних серверах, та веб-інтерфейс, який відображає дані та дозволяє працювати із записами, доданими основним сервером.

Graylog ефективний під час роботи з необробленими рядками (наприклад, із системним журналом) – інструмент аналізує та переробляє їх у потрібні нам структуровані дані. Він також забезпечує розширений налаштований пошук записів з використанням структурованих запитів. Іншими словами, при правильній інтеграції з веб-програмою, Graylog допомагає інженерам аналізувати поведінку системи майже в кожному рядку коду.

Основною перевагою Graylog є те, що він надає єдиний ідеальний екземпляр збору записів журналів для всієї системи. Це корисно, якщо системна інфраструктура велика та складна. Записи можна було розповсюджувати в кількох місцях, через кілька різних сервісів, і не всі члени команди могли мати негайний доступ до всіх його компонентів, чи ділитися ними. З Graylog ми вирішуємо ці проблеми та гарантуємо швидке реагування на інциденти.

У Logicify його можна використовувати як для додатків, що у розробці, так тих, які вже були опубліковані. В обох випадках деякі режими Graylog унікальні, а інші перетинаються.

Складається Graylog із трьох компонентів:

- graylog-webui – web-інтерфейс на Rails,
- graylog-server – Java TCP/UDP лог-колектор,
- mongodb для зберігання власне логів та налаштувань всієї системи в цілому.

Graylog-server дозволяє за протоколами TCP/UDP, як і за допомогою звичайного syslog, приймати звідусіль логи, mongodb здійснює зберігання, rails забезпечує візуально-красиве відображення даних та графіків.

Що стосується явних переваг системи, то окрім звичайних для syslog-server функцій хочеться відзначити також такі цікаві моменти в роботі системи:

- Агрегація повідомлень у потоки. За ключовим словом об'єднуємо потік логів з кількох хостів, на один потік «stream», можна створити сповіщення про події і зробити так, щоб ці сповіщення приходили комусь на пошту чи в месенджер Telegram.
- Агрегація хостів у групи. Можна об'єднати потоки з різних хостів до однієї групи.
- Вибірки з усього масиву за допомогою regexp, за часом, за важливістю, по об’єктах тощо. Можна знайти все, що завгодно і коли завгодно.
- Blacklists для логів. За допомогою регулярних виразів можна фільтрувати логи. Все, що ми заборонимо, до бази не потрапить.

- Авторотація логів. Не потрібно дбати про очищення старих записів, mongodb сама зробить всю роботу за допомогою механізму capped collections.

- Можливість використання GELF – graylog extended log format, таким чином розширюючи стандартну довжину syslog повідомлення в 1024 байти. За допомогою GELF можна моніторити не тільки системні повідомлення, але й логіку роботи коду, посилаючи розгорнуті повідомлення прямо з програми.

Література

1. Syslog Message Format. 2020. URL: https://techdocs.audiocodes.com/session-border-controllersbc/mediant-software-sbc/user-manual/version740/content/um/Syslog%20Message%20Format.htm.
2. What is graylog URL: https://www.graylog.org/.
3. HOW TO USE GRAYLOG AS A SYSLOG SERVER. 2018. URL: https://www.graylog.org/post/how-to-use-graylog-as-a-syslog-server/.