УДК 004.75

МЕТОД АНАЛИЗА СОБЫТИЙ В РАСПРЕДЕЛЕННОЙ БАЗЕ ЖУРНАЛОВ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Надршина А.Д. (Университет ИТМО)
Научный руководитель – к. т. н. Быковский С. В.
(Университет ИТМО)

В работе рассматривается метод анализа событий в распределенной базе журналов в телекоммуникационных системах. Метод включает в себя проектирование инструмента, способного выполнять распределенный поиск данных в журналах событий. Данный подход позволяет создавать запрос на одном управляющем узле, затем собирать информацию с нескольких узлов и выводить результат на управляющий узел. Это позволяет уменьшить время поиска ошибок и исполнения запросов пользователя. Также увеличивает скорость диагностики при возникновении аварий и сбоев системы.

Введение. Текущие методы анализа журналов событий пока недостаточно широко используются обществом, несмотря на то, что существует множество доступных систем для поддержки выполнения таких процессов, такие как: Grafana, Graylog, ProM и т.д. У каждой компании есть свои необходимые нужды, и система должна быть достаточно гибкой и удобной для использования. Процессы являются неотъемлемой частью современного мира, управляя услугами и внутренними функциями в компаниях, государственных органах и организациях, поэтому очень важно разрабатывать систему, подходящую под потребности определенной организации.

Основная часть. Проектирование инструмента для поиска по распределенной базе журналов событий предполагает решение следующих задач:

- Создание архитектуры инструмента. Есть один управляющий узел и некоторое количество узлов, на которых хранятся журналы событий. С помощью управляющего узла происходит взаимодействие и с пользователем, и с узлами с журналами событий;
- Составление архитектуры инструмента в графическом виде при помощи сервиса для формирования диаграмм, описание ее особенностей и взаимодействия с пользователем;
- Определение алгоритмов поиска по распределенной базе данных журналов событий: Process Mining – альфа-алгоритм для анализа процессов, регулярные выражения утилиты командной строки grep, синхронизация времени и т.д.;
- Определение критериев поиска по распределенной базе, например, по типу запросов: мониторинг и пользовательские инциденты; по коду ошибки; по региону страны, на котором возникла проблема, по авторизации абонентов, по звонковой части; по методу, на котором возникла ошибка;
- Выбор инструментов для работы с журналами событий: Graylog, Grafana, Splunk, ELK, Loggly, Pravega, ProM;

Выводы. В ходе работы была проанализирована предметная область по анализу событий в распределенной базе журналов в телекоммуникационных системах. Выявлено, что разработанная методика поиска по распределенной базе является более удобной для пользователя, анализирующего журналы событий, потому что нет необходимости осуществлять поиск на всех узах по очереди. Запрос поступает только на управляющий узел, после чего он передается для выборки данных одновременно ко всем узлам с журналами событий. Далее результат поиска возвращается на управляющий узел и пользователь получает необходимый вывод, что уменьшает время поиска.

Надршина А.Д. (автор) Подпись

Быковский С. В. (научный руководитель) Подпись