Министерство общего и профессионального образования
Российской Федерации

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЯДЕРНЫЙ
УНИВЕРСИТЕТ “МИФИ”

Факультет Кибернетики и информационной безопасности
Кафедра Информационные технологии в социальных системах

К защите допустить:
Заведующий кафедрой
_____ М. В. Сергиевский

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к курсовому проекту
на тему:

РАЗРАБОТКА АЛГОРИТМА ДЛЯ ВЫДЕЛЕНИЯ ЧАСТОВСТРЕЧАЮЩИХСЯ ШАБЛОНОВ ОШИБОК ИЗ ФАЙЛОВ ЖУРНАЛОВ ПРИЛОЖЕНИЙ

Студент: А. Г. Тропин

Научный руководитель:
к.т.н, доцент М. В. Сергиевский

Москва 2015

РЕФЕРАТ

Пояснительная записка к учебно-исследовательской работе содержит 14 страниц.

Ключевые слова: mapreduce, logs, распределенные вычисления, python, надежность, отказоустойчивость, функциональное программирование, регулярные выражения.

Цель работы — разработка алгоритма для выделения частовстречающихся шаблонов ошибок из файлов журналов приложений.

В процессе работы осуществлялась разработка алгоритма, реализация алгоритма на языке python. И внедрение в производство с использованием MapRedcue-системы Yandex Tables.

В результате работы был разработан алгоритм, реализованы 2 приложения на языке python и 2 вспомогательные утилиты на языке bash.

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей пояснительной записке к учебно-исследовательской работе использованы ссылки на следующие стандарты.

ГОСТ 7.32-2001 Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления.

ГОСТ 7.9-95 Система стандартов по информации, библиотечному издательскому делу. Реферат и аннотация. Общие требования.

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ВВЕДЕНИЕ

Большинство программных систем, имеющих сложную структуру и состоящих из нескольких сотен различных компонент, обладают рядом схожих проблем. Например веб-поиск содержит следующие компоненты: балансеры, верхние, средние метапоиски, промежуточные и базовые поиски, колдунщики, антироботы, свежесть, региональные поиск, несколько десятков параллельных поисков.

Определение 1 (Экземпляр)**.** приложение, запущенное в контейнере и описываемое парой host:port.

Всего единовременно запущено несколько ******** тысяч экземпляров приложений. Каждый экземпляр генерирует множество ошибок и записывает каждую из них в файл журнала ошибок.

Некоторые приложения, близкие по функционалу, пишут в один и тот же файл. Файлы журналов ротируются согласно определённому алгоритму. Тем не менее объем файла журнала для одного экземпляра может достигать нескольких сотен мегабайт, что препятствует быстрому ручному анализу в случае инцидента и инженеры вынуждены тратить ценные секунды на просмотр сотен тысяч строк файла в поисках сообщения с описанием элемента, вызвавшего сбой работы системы.

Начальным требованием к системе для эффективного использования алгоритма является наличие сопоставимого с количеством поисковых экземпляров приложений количества узлов на которых может быть запущена программа, реализующая алгоритм.

В организации, в которой выполнялась учебно-исследовательская работа, развёрнута большая поисковая инфраструктура, которая не лишена недостатков и существует вероятность поломки некоторой её части. Существует множество средств мониторинга состояния веб-поиска и противодействия инцидентам, но в некоторых случаях инженерам их недостаточно и приходится вручную анализировать файлы журналов отдельных экземпляров приложений на отдельных серверах, что, в свою очередь, замедляет скорость реакции на непредвиденную ситуацию. Но даже автоматизация процесса анализа файла журнала одного экземпляра не решает проблему полностью, поэтому необходима возможность быстрого анализа файлов журналов сразу множества экземпляров.

Определение 2 (Шаблон)**.** Специально подготовленное регулярное выбражение с экранированными спецсимволами.

Таким образом, целью этой учебно-исследовательской работы является разработка алгоритма, позволяющего собирать статистику по ошибкам, встречающимся в файлах журналов экземпляров поисковых приложений на основе существующих шаблонов и выделять новые шаблоны.

1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1 Представление задачи в терминах MapReduce

Для параллельного запуска приложений была выбрана модель распределённых вычислений MapReduce по ряду причин. Основные понятия:

Определение 3 (MapReduce)**.** Модель распределённых вычислений, представленная компанией Google, используемая для параллельных вычислений над очень большими, несколько петабайт, наборами данных в компьютерных кластерах.

Определение 4 (Map)**.** map(f, list) — функция высшего порядка двух аргументов, применяет к каждому элементу списка list, функцию f(x), в качестве результата возвращает список полученных значений.

Определение 5 (Reduce)**.** reduce(f, list, init=None) — функция высшего порядка, последовательно применяет f(x, y) к элементу списка и значению от предыдущего выполнения функции.

Пример. map(lambda x: x**3, [1, 2, 3]) вернёт список [1, 8, 27].

Пример. map(lambda x, y: x + y, [1, 2, 3]) вернёт 6(сумма всех элементов). 6 = sum(sum(1, 2), 3).

Как оказалось задача без особых сложностей выражается в терминах чистых функций flat map и flat reduce, так как основная структура, используемая в алгоритме — это пара(шаблон, количество совпадений) и благодаря этому однопоточный код легко запускается на множестве узлов MapReduce-кластера. Это обстоятельство освобождает от реализации сложного механизма сетевого взаимодействия.

В качестве реализации модели MapReduce была выбрана реализация Yandex Tables, обладающая рядом отличий и нововведений:

- Колоночное хранение и range-операции
- Дерево метаинформации
- Единая операция Map-Reduce
- Расширенная поддержка транзакций, включая вложенность
- Настраиваемый коэффициент репликации и алгоритмы сжатия данных
- Хранение файлов в системе и их раздача исполняемым задачам
- Разные форматы стриминга (yamr, dsv)
- Надёжность и производительность
  - Отказоустойчивый мультимастер
  - Отказоустойчивый реплицированный планировщик
  - Минорные обновления проходят без заметного эффекта для конечных пользователей
- Гибкие слоты (заказ CPU, RAM)

– Существенные обновления не требуют пересборки C++ клиентов (так как все работает через HTTP API и стриминг клиент)

Не смотря на существенные отличия от модели, описанной в документе от компании Google, код программы, реализующий алгоритм легко переносится на другие реализации данной модели распределённых вычислений.

1.2 Выбор языка программирования и средств разработки

В качестве среды разработки было решено использовать удалённую виртуальную машину с конфигурацией и окружением идентичными конфигурации и окружению MapReduce узла. Были выбраны следующие программные продукты:

– В качестве операционной системы использовался дистрибутив GNU/Linux Ubuntu 12.04 LTS с модифицированным ядром и дополнительными пакетами.
– Vim — один из немногих настоящих текстовых редакторов, обладающих массой встроенных возможностей и практически безграничным потенциалом к расширению за счёт встроенного интерпретируемого языка программирования VimL и поддержкой возможности написания расширений на таких языках, как python, ruby, perl.
– Сохранение состояние рабочего окружения осуществлялось с помощью терминального мультиплексора tmux, имеющего клиент-серверную архитектуру и позволяющего отсоединятся от текущей сессии, оставляя её работать в фоновом режиме с последующей возможностью переподключения. tmux — свободная консольная утилита-мультиплексор, предоставляющая пользователю доступ к нескольким терминалам в рамках одного экрана. tmux может быть отключён от экрана: в этом случае он продолжит исполняться в фоновом режиме; имеется возможность вновь подключиться к tmux, находящемуся в фоне. tmux является штатным мультиплексором терминалов операционной системы OpenBSD. Программа tmux задумывалась как замена программы GNU Screen.
– Удалённое подключение осуществлялось средствами защищённого протокола ssh
(беспарольная аутентификация с использованием ключа) и технологии cauth. SSH (англ. Secure Shell — “безопасная оболочка”]) — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов). Схож по функциональности с протоколами Telnet и rlogin, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования. SSH-клиенты и SSH-серверы доступны для большинства сетевых операционных систем.

– Для управления версиями исходных кодов использовалась децентрализованная система управления версиями git, в качестве сервиса для хранения репозитория был использован сервис github.

В качестве языка программирования был выбран python2.7. Так как:

– Он предустановлен в большинстве современных дистрибутивах операционных систем.
– Выразителен. Аналогичные программы на таких языках как Java, C++ имеют в разы большие объёмы исходных кодов.
– Обладает высокой производительностью.
– Имеет множество библиотек, в том числе библиотеки для работы с регулярными выражениями, обёртки для MapReduce.

1.3 Структура данных

В качестве входных данных использовался агрегированный файл журнала с нерегулярной структурой, содержащий сообщения об ошибках в различных форматах, как многострочные, так и однострочные.

Первая часть алгоритма, позволяет осуществить сбор статистики и возвращает список пар (шаблон, количество совпадений), так же существует возможность получить часть текста не удовлетворяющую известным шаблонам, для последующего анализа с помощью второй части алгоритма, позволяющей выделить новые предполагаемые шаблоны и с помощью первой части алгоритма получить статистику, подтверждающую или опровергающую предположение.

1.4 Стадии выполнения задачи

1.4.1 Подготовка репозитория

Был создан git-репозиторий на сервисе github, сделана его локальная копия. Была выбрана следующая структура проекта и правила именования файлов:

– В корневом каталоге лежат файлы README.md, LICENSE, .gitignore.
– В каталоге doc/ хранится документация. Исходные тексты в LaTeXи скомпилированная версия в PDF.
– В каталоге direlog/ хранятся исходные коды с расширением .py и тесты, имеющие префикс test_
– В каталоге direlog/example/ хранятся примеры файлов журналов и вспомогательные скрипты на языке bash.

1.4.2 Выбор хранилища для шаблонов

В качестве хранилища для паттернов было решено использовать обычный файл на языке python, названный patterns.py и содержащий в себе два списка паттернов prepare_patterns и main_patterns, используемых на подготовительном этапе и на этапе сбора статистики соответственно, и хранить его под контролем версий в этом же репозитории. Причин на это несколько: во-первых простота модификации файла с помощью скриптов, во-вторых возможность просмотра истории изменений и откат к предыдущим версиям, в-третьих возможность ручного редактирования.

1.4.3 Написание программного кода

Написание программного кода было разделено на несколько этапов.

1 Написание утилиты для предварительной обработки исходного файла журнала. Утилита получила название prepare.py и позволила подготовить сырой файл журнала для последующей обработки, путём замены уникальных токенов, таких как UUID, timestamp, версии, номера строк, пути, содержащие версии, на строковые константы.
2 Формирование prepare_patterns на основе ручного анализа файлов журналов.
3 Написание функциональных тестов для prepare.py.
4 Реализация алгоритма для сбора статистики с использованием main_patterns. Утилита получила название direlog.py. И позволяет на выходе получить список пар (шаблон, количество совпадений) или текст, не подходящий под известные шаблон.
5 Добавление поддержки буферизации входного потока и поддержки многострочных шаблонов.
6 Написание функциональных тестов для direlog.py.
7 Добавление функции, позволяющей запускать алгоритм на MapRedcue-кластере.

2 ИМПЛЕМЕНТАЦИЯ ЗАДАЧИ

2.1 Диаграмма компонентов

2.2 Описание способов запуска

2.3 Анализ полученных результатов

3 ДАЛЬНЕЙШЕЕ РАЗВИТИЕ

ЗАКЛЮЧЕНИЕ

4 СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

5 ПРИЛОЖЕНИЯ