



ІТМО

Разработка системы онлайн- антифрода для сервиса Новостей

Докладчик: Гуммель Никита
Научный руководитель: Койнов Руслан
Компания: ООО “Дзен.Платформа”

Описание предметной области

Фрод – это любое действие, противоречащее правилам пользования платформой или совершенное ненастоящим пользователем, то есть роботом



Антифрод - комплекс мер, направленных на мониторинг и борьбу с фродом.

Одно из основных направлений антифрода - поиск фрода в событиях сервисов.

Выявление фрода в логах делится на два вида:

- Оффлайн-антифрод - поиск фродовых пользователей.
- Онлайн-антифрод - потоковая разметка событий логов на наличие фрода.

В августе 2022 года, платформы Дзен и Новости перешли от Яндекса к VK Group.

В связи с этим у сервиса Новости пропал доступ к онлайн-антифроду, который ранее совершался на стороне Яндекса.

Также сервис Новости начал пользоваться принятым в Дзене logfeller для сбора и поставки логов событий.



Цели: разработка системы онлайн-антифрода, поставляющая таблицы с добавлением колонки rules, содержащей идентификаторы правил, обнаруживших фрод в событии, с организацией директорий таблиц, соответствующей формату поставки logfeller.



Задачи:

- Применить правила онлайн-антифрода Дзена к логам сервиса Новостей
- Выявление требований к времени поставки таблиц и используемым вычислительным квотам
- Проектирование системы, выделение квоты и подготовка архитектуры данных
- Реализовать асинхронное исполнение графов вычислений

Функциональные требования

- Данные необходимо читать из stream директории logfeller;
- Поставка таблиц должна осуществляться в том же формате, что и у logfeller;
- SLA поставки таблиц - не более 4 часов;
- Настроены мониторинги времени поставки таблиц и работы отдельных компонентов;
- Должны быть настроены алерты об упавших процессах и задержке поставки таблиц;
- В поставляемых таблицах должна присутствовать колонка rules, содержащая идентификаторы правил, разметивших данное событие как фрод.



- Чтение должно происходить по батчам таблиц для асинхронной работы;
- Процессы должны быть независимы друг от друга с целью асинхронности выполнения различных компонентов системы;
- Процессы не должны работать одновременно с чувствительными данными во избежание нарушения консистентности данных;
- Все табличные данные должны хранить на YT;
- В процессе разработки необходимо использовать YQL, Nirvana, Hitman и Datalens
- Должна быть настроены разграничения доступов.



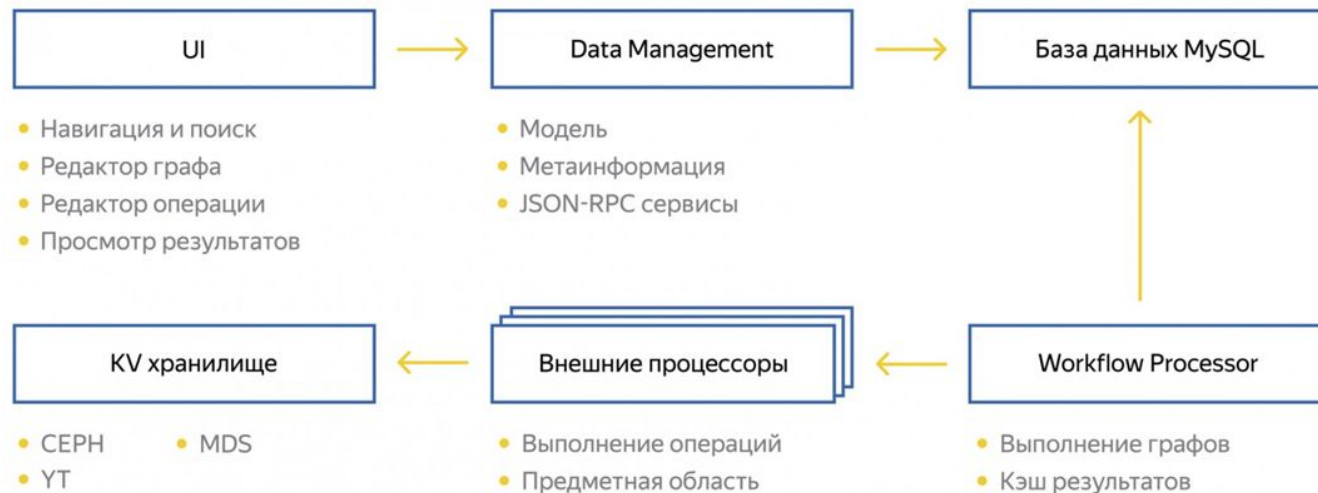
Используемые технологии: YQL, Nirvana, YT, Hitman, Groovy, DataLens, TelegramApi.



Внутренние технологии:

- YQL (Yandex Query Language, SQL диалект от Яндекса с пакетом дополнительных библиотек Яндекса)
- YT (Yandex Tables, сервис распределенного хранения и обработки данных с поддержкой модели MapReduce, распределенной файловой системой и NoSQL key-value базой данных)
- Hitman (платформа для автоматизации запусков продакшн-процессов)
- DataLens (инструмент визуализации данных)

облачная платформа для управления процессами, которые оформлены в виде ациклических графов.



Используемые технологии находятся в одном серверном окружении Яндекса.



Используемые компоненты системы:

- Сервис Hitman для регулярного запуска Nirvana-графов, мониторинга всего проекта и отдельных процессов в нем
- Сервис Nirvana для составления графов исполнения
- Все табличные данные находятся в хранилище данных YT
- Запускаемые YQL-операции разбиваются на map-reduce операции на YT

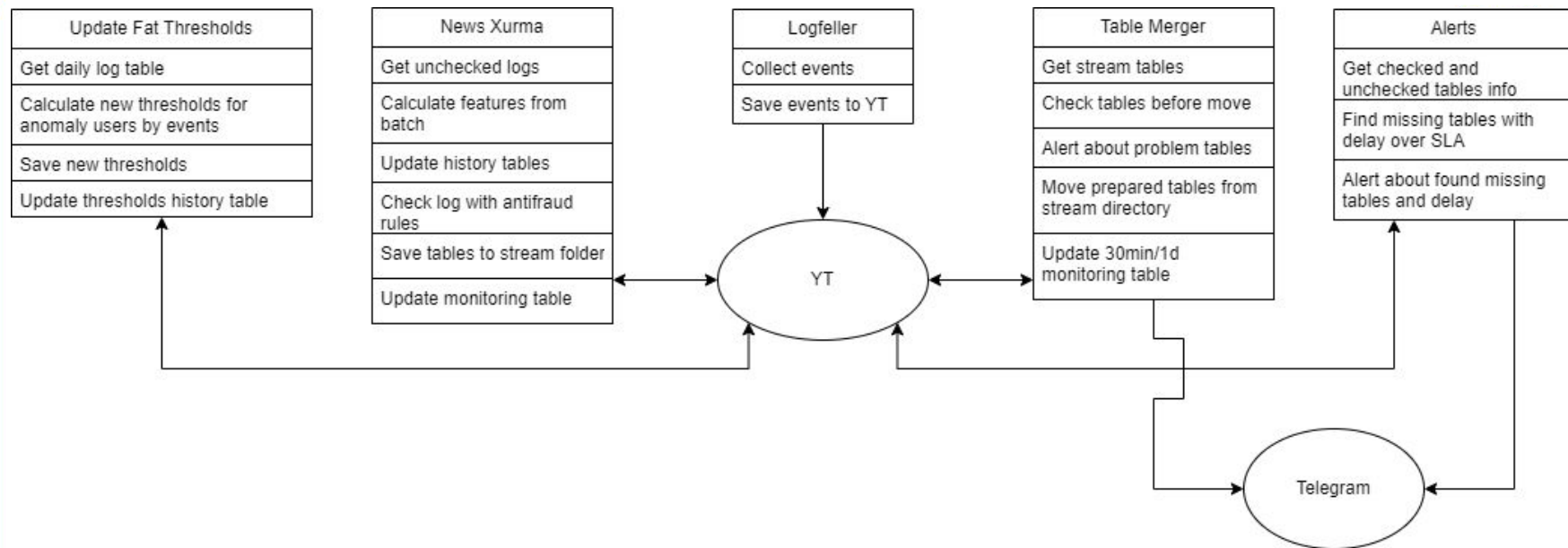
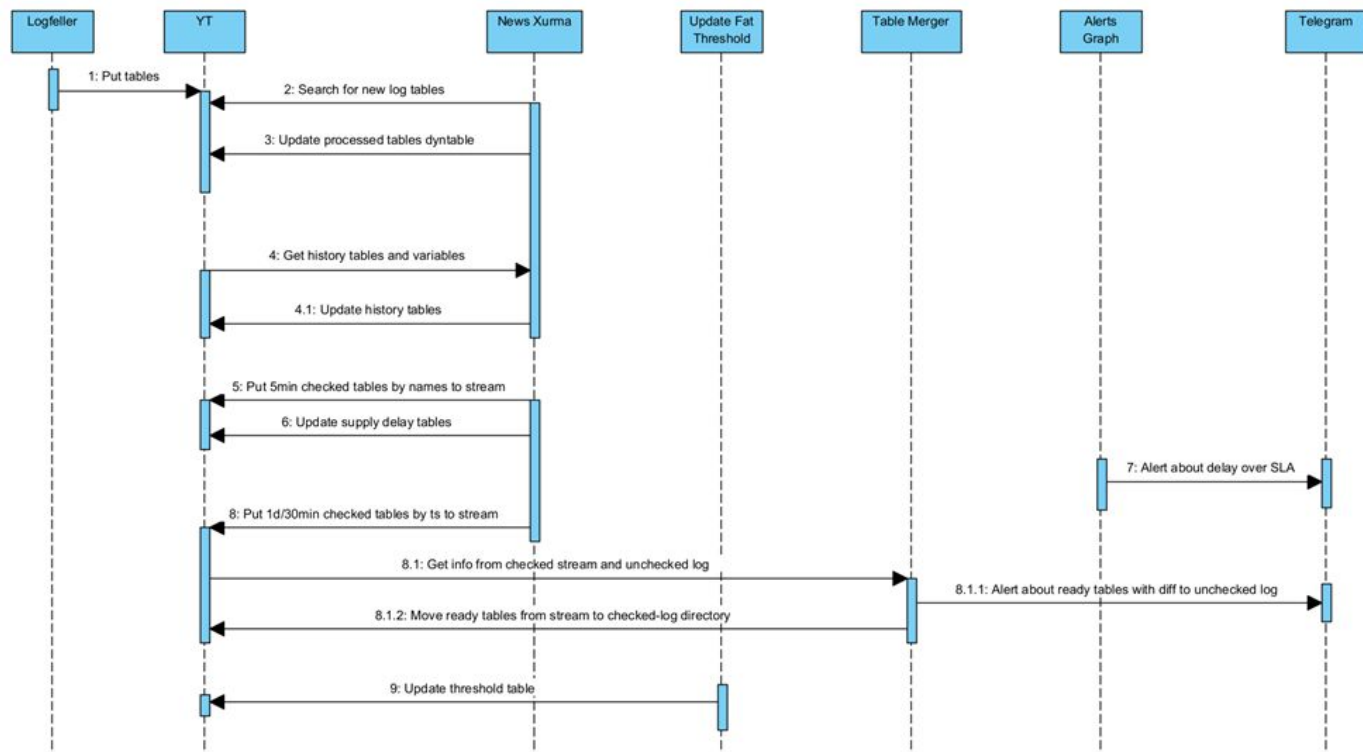


Диаграмма классов для отображения функционала графов и их взаимодействия

Программная архитектура

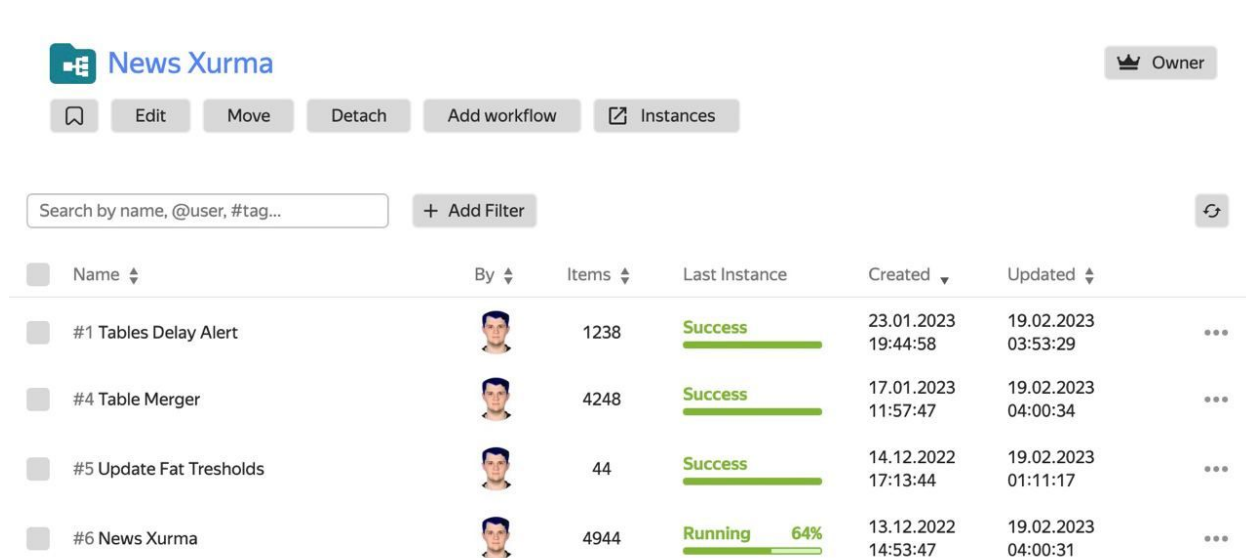
Диаграмма
последовательности
взаимодействия
компонентов



Используемые данные



Визуализация используемых таблиц с разбиением по функциональным группам



The screenshot displays the Nirvana interface for a project named 'News Xurma'. At the top, there are navigation buttons: 'Edit', 'Move', 'Detach', 'Add workflow', and 'Instances'. A search bar is located below these buttons, with the placeholder text 'Search by name, @user, #tag...'. To the right of the search bar is an 'Add Filter' button. The main content area is a table listing workflows. The table has columns for 'Name', 'By', 'Items', 'Last Instance', 'Created', and 'Updated'. Each row represents a workflow, with a status bar indicating the progress of the last instance. The workflows listed are: '#1 Tables Delay Alert', '#4 Table Merger', '#5 Update Fat Thresholds', and '#6 News Xurma'. The status for the first three is 'Success', and for the last one, it is 'Running' with a 64% progress bar.

| Name | By | Items | Last Instance | Created | Updated |
|--------------------------|----|-------|---------------|---------------------|---------------------|
| #1 Tables Delay Alert | | 1238 | Success | 23.01.2023 19:44:58 | 19.02.2023 03:53:29 |
| #4 Table Merger | | 4248 | Success | 17.01.2023 11:57:47 | 19.02.2023 04:00:34 |
| #5 Update Fat Thresholds | | 44 | Success | 14.12.2022 17:13:44 | 19.02.2023 01:11:17 |
| #6 News Xurma | | 4944 | Running 64% | 13.12.2022 14:53:47 | 19.02.2023 04:00:31 |

Реализованные графы в интерфейсе Nirvana

Zen Fraud Alerts

ЧТО-ТО СЛОМАЛОСЬ В НОВОСТНОЙ ХУРМЕ

Поставка checked-log на arnold задерживается больше, чем на 4 час(а/ов))

| table | creation_time_utc |
|---------------------------|---------------------|
| 30min/2023-02-28T18:00:00 | 2023-02-28T16:05:49 |
| ... | ... |
| 30min/2023-02-28T19:00:00 | 2023-02-28T16:41:59 |

[DEBUG]

4 P.I. Bot, 23:54

Прокомментировать

>

Алерт о задержке поставки таблиц

Zen Fraud Alerts

В НОВОСТНОЙ ХУРМЕ РАЗЛАДКИ ПО ЧИСЛУ СТРОК

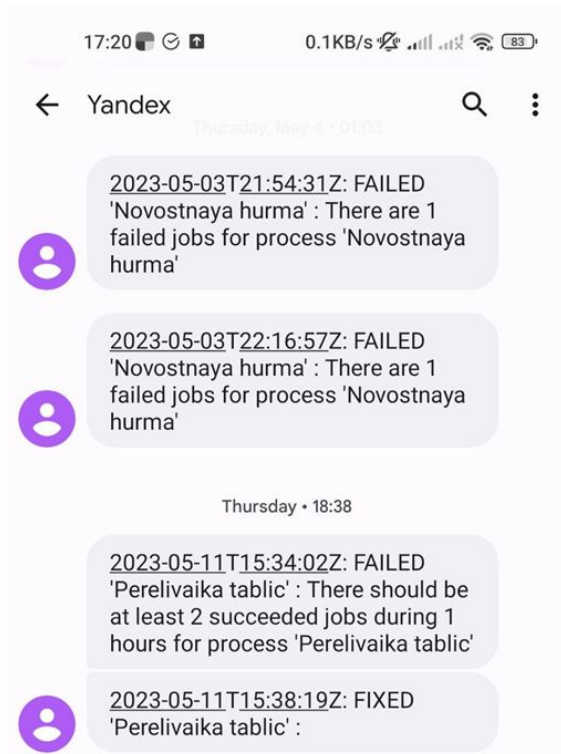
Stream таблицы не перелились из-за потенциальных разладок
 $diff=(checkedRows+streamRows)/eventsRows-1.0$

| table | diff |
|---------------------|-------------|
| 2023-05-23T09:30:00 | -0.45854013 |
| 2023-05-23T06:30:00 | -0.30341926 |
| 2023-05-23T07:00:00 | -0.37976485 |

[DEBUG]

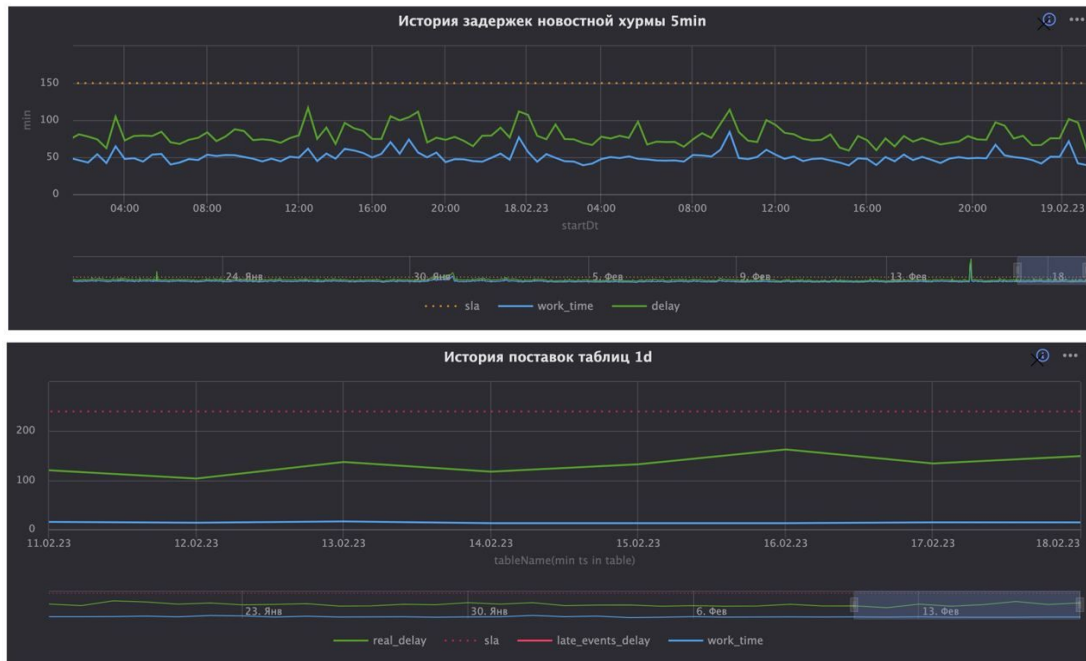
4 P.I. Bot, 14:01

Алерт о задержке поставки событий
в stream директорию



Примеры SMS-алертов от Hitman

Мониторинги поставки таблиц



Разработка данной системы с использованием выбранных технологий позволила сначала проверить все потенциальные проблемы с асинхронным исполнением. Система была протестирована с помощью ручного тестирования, качество системы оценивается с помощью грамотно настроенных алертов и мониторингов Hitman.



Поставляемые таблицы активно используются:



- В построении продуктовых метрик и дашбордов
- ML командой для обучения ранжирующих формул
- В A/B-тестах для очистки данных от фрода
- Используется в команде антифрода для построения новых процессов

**Спасибо
за внимание!**

it'sMO *re than a*
UNIVERSITY