

Хранение событий в базе данных системы Логикор

ПО Логикор представляет собой систему долговременного хранения и фильтрации событий информационной безопасности (далее СДХ). Основное предназначение системы — получение, обработка, сохранение и передача событий информационной безопасности. Одной из функций системы является надежное, масштабируемое хранение событий.

В данной статье описаны принципы хранения событий в системе Логикор, роль ClickHouse в архитектуре, структура основных таблиц, а также механизмы отказоустойчивости, масштабирования и управления жизненным циклом данных.

Процесс хранения событий

В Логикор хранение и передача данных, конфигураций, правил и событий в системе производится в слое хранения данных и событий, который взаимодействует со слоем обработки и маршрутизации событий.

В общем виде процесс хранения выглядит следующим образом:

1. После завершения обработки подготовленное событие передается в слой хранения данных системы Логикор и асинхронно записывается в кластер ClickHouse.
2. Запись события выполняется напрямую в локальную таблицу `messagesTable` на одном из узлов кластера ClickHouse.
3. При вставке данных ClickHouse формирует физические части таблицы (парты), которые сохраняются внутри соответствующих логических партиций.
4. ClickHouse автоматически выполняет фоновые операции объединения (`merge`) партов внутри одной партиции.
5. Для обеспечения отказоустойчивости используется репликация данных между узлами кластера и шардирование для горизонтального масштабирования.
6. Координация репликации, шардирования и состояния кластера осуществляется компонентом **ClickHouse-Keeper**.
7. После записи к данным применяются политики хранения и правила TTL (`Time To Live`), которые определяют условия recompression, перемещения между уровнями хранения и автоматического удаления устаревших событий.
8. Доступ к сохраненным событиям осуществляется через таблицу **messages** (`Distributed table`), которая выполняет распределенные запросы ко всем таблицам **messagesTable** на узлах кластера.

Более подробно рассмотрим процесс ниже.

ClickHouse в Логикор

Общие сведения

ClickHouse — это система управления базами данных с открытым исходным кодом, предназначенная для аналитической обработки больших объемов данных. В системе Логикор данная система отвечает за хранение всех событий, прошедших этап обработки и маршрутизации.

Основные таблицы базы данных `logger` в ClickHouse

Все события хранятся в базе данных `logger` в ClickHouse и распределены по различным таблицам. Основными являются следующие:

- **messagesTable** — основная таблица хранения событий. Фактическая запись данных осуществляется непосредственно в данную таблицу.
- **messages** — распределенная таблица, предназначенная для чтения данных со всех узлов кластера. Запросы на события необходимо выполнять именно в эту таблицу.
- **tagsTable** — основная таблица для хранения списка используемых тегов;
- **tags** — распределенная таблица чтения информации по тегам на всем кластере базы данных;
- **mv_tagsTable** — материализованное представление на основании таблицы `messagesTable` в таблицу `tagsTable` для сохранения используемых тегов.

Оптимизация хранения событий

Оптимизация хранения событий в системе Логикор реализуется за счет механизмов партиционирования и фонового объединения данных, встроенных в ClickHouse. Данные механизмы обеспечивают управляемость жизненного цикла информации, снижение нагрузки на файловую систему и стабильную производительность при больших объемах событий.

Логические партиции

При создании таблицы задается выражение **PARTITION BY**, определяющее способ логического разбиения данных. В типовой конфигурации Логикор используется партиционирование по дате события на основе поля `timestamp`.

Партиция является логической единицей хранения, объединяющей строки за определенный временной интервал (например, сутки).

Физические парты

Физически данные в ClickHouse хранятся в виде партов (`parts`). Парт представляет собой каталог на диске, содержащий:

- файлы колонок;
- индексы;
- служебные метаданные.

Парты формируются при операциях вставки данных. При высокой скорости поступления событий внутри одной логической партии может создаваться множество мелких парт. Избыточное количество парт увеличивает нагрузку на файловую систему и может негативно влиять на производительность чтения.

Первичный ключ и сортировка данных

В таблицах семейства **MergeTree** важную роль играет механизм сортировки данных, задаваемый выражением **ORDER BY**., которое задает порядок физической сортировки строк внутри каждого парта.

В системе Логикор используется следующая схема сортировки:

ORDER BY (timestamp, uuid)

Это означает, что данные внутри каждого парта упорядочиваются сначала по времени события (timestamp), а затем по уникальному идентификатору события (uuid).

Сортировка данных выполняет несколько важных функций:

- позволяет эффективно выполнять фильтрацию по диапазонам времени;
- повышает эффективность операций объединения парт (merge);
- улучшает степень сжатия данных.

Фоновое объединение данных (Merge)

Для оптимизации хранения ClickHouse выполняет фоновый процесс объединения (merge). В рамках одной логической партии мелкие парты автоматически объединяются в более крупные. Процесс объединения обеспечивает уменьшение количества файлов на диске, повышение степени компрессии данных, оптимизацию индексов и ускорение выполнения аналитических запросов.

Масштабирование и отказоустойчивость

Для обеспечения отказоустойчивости системы и масштабирования системы в ClickHouse используются механизмы репликации и шардирования.

Репликация — применяется для повышения отказоустойчивости и доступности данных. Данные хранятся и поддерживаются на нескольких узлах кластера одновременно. Репликация обеспечивает сохранность данных при отказе узла, автоматическое восстановление данных и возможность чтения данных с любой реплики.

Шардирование — метод горизонтального масштабирования базы данных, при котором данные разделяются на независимые части (шарды). Каждый шард содержит только часть общей информации, но вместе они образуют полную базу. Это позволяет распределять нагрузку и увеличивать производительность системы, так как запросы к данным могут выполняться параллельно на разных узлах.

За координацию репликации и состояние реплик отвечает **ClickHouse Keeper**.

Политики хранения данных

В системе Логикор используются политики хранения данных, определяющие размещение и жизненный цикл информации в ClickHouse.

В рамках одной политики могут использоваться несколько уровней (дисков) хранения данных:

- **Hot** — высокопроизводительные носители (SSD), предназначенные для наиболее актуальных данных;
- **Warm** — промежуточный уровень хранения;
- **Cold** — более медленные носители, используется для архивных данных.

Такое разделение позволяет оптимизировать использование ресурсов и снизить стоимость хранения данных.

Политики хранения определяют на каких физических носителях хранятся данные, в какие моменты они перемещаются между уровнями и при каких условиях подлежат удалению. Политика хранения привязывается к таблице **messagesTable** и применяется ко всем записываемым данным.

Жизненный цикл данных в ClickHouse управляется механизмом TTL (Time To Live). С помощью TTL могут быть заданы правила рекомпрессии данных, их перемещения между уровнями хранения и окончательного удаления.

Пример механизма:

- через 7 дней — рекомпрессия данных;
- через 10 дней — перенос на холодное хранилище;
- через 6 месяцев — удаление данных.

Как правило удаление выполняется на уровне парт.

Подробное описание настроек ClickHouse можно посмотреть [в статье Настройки ClickHouse в Логикор](#).

ID статьи: 1633

Последнее обновление: 7 мая, 2026

Обновлено от: Михалева А.

Ревизия: 1

База знаний Логикор -> Документация -> Система хранения и обработки данных «Логикор». Версия 2.6.0 -> Логикор.

Руководство разработчика -> Управление конфигурационными файлами -> Хранение событий в базе данных системы Логикор

<https://docs.axel.pro/entry/1633/>