Воронцова Дарина Павловна,
студентка ФФ и ПИ,
ФГБОУ ВО ЮЗГУ, г. Курск

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ REDIS

Аннотация: В статье определены основные проблемы использования системы управления базами данных Redis и предложены способы повышения информационной безопасности системы в целях расширения возможностей ее применения.

Ключевые слова: информационная безопасность, нереляционные базы данных, система управления базами данных Redis, несанкционированный доступ, уязвимость приложения.

В современном мире в каждом веб-приложении используются базы данных, включающие не только необходимую для работы приложения информацию, но и данные пользователей, которые могут удаляться или изменяться. Данных очень много, а признать их «большими» помогает характеристика, данная компанией «Gartner»: «Большие данные» характеризуются объемом, разнообразием и скоростью, с которой структурированные и неструктурированные данные поступают по сетям передачи в процессоры и хранилища, наряду с процессами преобразования этих данных в ценную для бизнеса информацию» [1].

С увеличением объемов информации появились проблемы хранения и обработки, с которыми классическая реляционная архитектура не справляется и потребовались новые решения. В свою очередь нереляционные базы данных или, как их еще называют, NoSQL решают эту проблему. Во многих современных системах пользуются популярностью NoSQL-базы, хранящие ключ-значение. Чаще всего они хранят информацию в кэше, что значительно увеличивает скорость обработки запросов. Например, с такой целью используется система управления базами данных (далее – СУБД) Redis. На практике в ней хранятся самые востребованные пользователями данные, что значительно ускоряет их обработку [2].

Redis (от англ. remote dictionary server) – резидентная система управления базами данных класса NoSQL с открытым исходным кодом, работающая со структурами данных типа «ключ – значение». Используется как для баз данных, так и для реализации кэшей, брокеров сообщений. Ориентирована на достижение максимальной производительности на атомарных операциях (заявляется о приблизительно 100 тыс. SET- и GET-запросов в секунду на Linux-сервере начального уровня). Написана на Си, интерфейсы доступа созданы для большинства основных языков программирования. В период 2010–2013 годов разработка системы спонсировалась компанией VMware, с мая 2013 года, после реорганизаций в федерации EMC – VMware, проект передан в Pivotal. С июня 2015 года основной спонсор проекта – компания Redis Labs, специально основанная для коммерциализации Redis, в неё же перешёл основной разработчик продукта – Сальваторе Санфилиппо [3].

Redis – это одна из самых популярных баз данных типа key-value. Одним из основных преимуществ Redis является высокая скорость работы благодаря ин-memory хранению данных. Популярность СУБД Redis обусловлена широким спектром вариантов использования. Ее можно использовать для кеширования данных, что повышает производительность системы в несколько раз за счет того, что данные хранятся в оперативной памяти. Это позволяет снизить нагрузку на реляционную СУБД и перенести часто запрашиваемые данные в Redis, а также повысить скорость обработки запросов. Помимо этого, Redis располагает инструментарием для лёгкого масштабирования в зависимости от текущих нужд сервиса [4].

Также Redis зачастую используют и для хранения сессий, это очень удобно за счет хранения вида ключ-значение. Большинство современных веб-приложений стараются переносить все данные о сессиях в кеш, с чем Redis отлично справляется. За счет этого повышается скорость обработки запросов пользователей к серверу. Помимо этого, в данной СУБД удобно хранить данные для потоковой передачи в режиме реального времени. Например, при передаче геопространственных данных, видео, аудио и изображений.

Также можно хранить метаданные, истории просмотров пользователей, токены и данные аутентификации пользователей. За счет скорости записи и чтения, обеспечиваемой СУБД Redis, подобные операции занимают минимальное количество времени, что позволяет оптимизировать нагрузку на сервер и повысить общую производительность системы.

Несмотря на то, что многие выбирают эту СУБД, она подходит далеко не всегда. Во-первых, Redis является более узконаправленной базой данных, чем SQL, что может привести к проблемам с масштабированием при росте объемов данных. Более того, некоторые функции Redis могут быть медленными при работе с большими объемами данных. Еще одним функциональным неудобством является необходимость писать код для выполнения некоторых операций, которые в других базах данных встроены в язык запросов.

Но главной проблемой является уязвимость данных в СУБД Redis. База данных Redis не обеспечивает надежную защиту данных, и, при допущении ошибок в настройках безопасности, данные могут быть легко украдены или скомпрометированы злоумышленниками. Кроме того, Redis подвержен потенциальным опасностям, таким как DDoS-атаки или атаки на уязвимость приложения и сервера. В случае, если сервер Redis окажется в руках злоумышленника, он сможет получить доступ к данным, хранящимся в нем.

Вышесказанное определяет ситуации, в которых лучше использовать другой вариант хранения и обработки информации:

- критические бизнес-данные: обычно хранятся в более традиционных базах данных, а не в Redis;
- сложные запросы данных: доступ к данным в хранилище «ключ-значение» возможен только по ключу;
- реляционные данные: СУБД Redis, как и другие базы данных NoSQL, не предназначена для управления реляционными данными;
- большой объем данных: не подходит для хранения очень больших наборов данных и в случаях, когда их количество резко растёт [5].

Несмотря на проблемы информационной безопасности (уязвимость для DDos-атак, отсутствие механизмов мониторинга безопасности, возможность внедрения зловредного кода, структуры данных и логические операции в потоки данных), СУБД Redis является одной из самых популярных систем управления базами данных в мире. В качестве способов повышения защищенности СУБД Redis возможно рекомендовать:

- шифрование данных – затрудняет доступ к ним злоумышленникам в случае кражи или утечки данных. Redis поддерживает шифрование данных на различных уровнях, начиная от защиты паролем и заканчивая использованием SSL-шифрования;
- управление доступом – возможность создавать различные уровни доступа для разных пользователей, хранить пароли в зашифрованном виде и просматривать логи доступа, чтобы отслеживать, кто, когда и с какого устройства получал доступ к базе данных;
- ограничение запросов и сетевых соединений может помочь предотвратить атаки, связанные с чрезмерным использованием CPU и памяти базы данных. Redis позволяет установить ограничения на количество запросов и сетевых соединений в единицу времени, а также управлять процессами репликации, чтобы избежать перегрузки системы;

- резервное копирование и восстановление Redis направлены на защиту данных от непредвиденных сбоев и катастроф, таких как отказ жесткого диска или злоумышленный доступ. Redis поддерживает возможность создания точек восстановления, а также резервное копирование базы данных на удаленный сервер;

- обновление системы Redis является необходимым для предотвращения уязвимостей и ошибок безопасности. Redis регулярно выпускает патчи безопасности и обновления функциональности, которые рекомендуется устанавливать как можно скорее;

- аутентификация Redis – реализация протокола REST для распределенных систем. Для аутентификации используется сервер приложений, если он установлен на компьютере, на котором установлена служба Redis. В противном случае используется сервис LDAP, используемый по умолчанию, для аутентификации пользователей;

- блокировка сетевого доступа Redis является важной мерой безопасности, которая помогает защитить сервер от атаки, в которой злоумышленник пытается получить доступ к вашему серверу с помощью специально созданного файла;

- мониторинг Redis и проверка наличия сбоев может помочь в определении атак на ваш Redis-кластер. Мониторинг: Монитор Redis-сервера может помочь вам определить, работает ли ваша система в соответствии с вашими ожиданиями;

- аудит действий пользователей и проверка авторизации и аутентификации.

Таким образом, СУБД Redis является одной из самых популярных и мощных систем управления базами данных в мире. Однако, как и любая другая технология, Redis не застрахован от угроз безопасности. Одной из основных угроз безопасности Redis является несанкционированный доступ к базам данных. Эта угроза возникает, когда злоумышленники могут получить доступ к базе данных Redis и взломать ее. Это может произойти, если Redis не защищен должным образом. Для обеспечения безопасности Redis необходимо применять меры защиты, такие как использование паролей и настройка доступа к базе данных только для авторизованных пользователей. Кроме того, можно использовать такие инструменты, как защита от атак DDoS, мониторинг безопасности и аудит безопасности.

Еще одной угрозой безопасности Redis является утечка конфиденциальной информации. В результате этой утечки злоумышленники могут получить доступ к такой информации, как пароли, логины, данные кредитных карт и другие личные данные пользователей. Для защиты от таких утечек важно использовать шифрование данных и надежные методы хранения и передачи информации.

В целом, обеспечение безопасности Redis является важным вопросом для любого предприятия, которое хранит конфиденциальные данные. Но с помощью правильных мер защиты, которые могут быть установлены совместно с Redis, можно обеспечить высокий уровень безопасности и предотвратить угрозы безопасности.

*Список литературы***:**

1. Tom White. Hadoop: The Definitive Guide, 3rd Edition. O'Reilly Media, 2012, 688 p

2. Костенко И.П., Ступина М.В. Повышение производительности WEB-приложений Ссредствами СУБД REDIS // Молодой исследователь Дона, 2022. № 4 (37). С. 29-32.

3. Redis – Википедия // Материал из Википедии – свободной энциклопедии [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/Redis. Дата обращения 05.05.2023.

4. Шарипова Н.Н. Об использовании NoSQL-хранилищ данных // Wschodnioeuropejskie Czasopismo Naukowe (East European Scientific Journal), 2016. № 9, С. 73-76 [Электронный ресурс] – Режим доступа: https://cyberleninka.ru/article/n/ob-ispolzovanii-nosql-hranilisch-dannyh. Дата обращения 05.05.2023.

5. Redis – особенности и область применения | Cloud4Y. Олег (/blog/authors/oleg-wr/) опубликовано: 05.12.2022 [Электронный ресурс] – Режим доступа: https://www.cloud4y.ru/blog/what-is-redis/ Дата обращения 05.05.2023.