УДК 004.056.5

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ГРАФОВЫМИ БАЗАМИ ДАННЫХ GRAPHDB

Е.А. Курако
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: kea@ipu.ru

В.Л. Орлов
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: ovl@ipu.ru

Ключевые слова: безопасность, защита информации, GraphDB, пользователи, роли, управление доступом, аутентификация, авторизация, шифрование, аудит.

Аннотация: Рассмотрены основные принципы обеспечения безопасности при использовании графовых баз данных GraphDB. Доступ к базам данных осуществляется с использованием механизма разграничения прав пользователей. Каждый пользователь может иметь имя пользователя и пароль. Кроме того, каждому пользователю присваивается определенная роль из набора: администратор, менеджер репозиториев, обычный пользователь. Может проводиться аутентификация пользователя различными методами. На основе аутентификации осуществляется авторизация пользователя, то есть установление для него определенного набора разрешений. Рассматриваются вопросы шифрования и аудита. Проведено экспериментальное исследование работы в защищенном и незащищенном режиме.

1. Введение

В настоящее время существует достаточно большой перечень реально использующихся графовых баз данных. В него включаются такие базы как Neo4j, Amazon NepTune, JanusGraph, TigerGraph, Apache Cassandra и др. Эти базы не только позволяют обрабатывать большие объемы информации, но и обеспечивать защиту данных [1]. Одной из наиболее популярных является GraphDB [2], которая обеспечивает хорошее быстродействие и даже для бесплатного варианта GraphDB Free дает возможность управления большими объемами RDF-операторов на одном сервере, полной поддержки языка запросов SPARQL 1.1, использования оптимизатора запросов. В то же время бесплатная версия ограничена выполнением двух одновременных запросов, что несколько замедляет работу при использовании множественных клиентов.

При этом важно, чтобы использование таких баз данных, как GraphDB, давало бы возможность не только загружать информацию и выполнять разнообразные запросы, но и обеспечивать безопасную работу с данными. Для этого следует рассмотреть основные методы защиты информации, характерные для GraphDB и особенности их использования [3].

2. Пользователи и роли

Доступ к базам данных GraphDB осуществляется с использованием механизма разграничения прав пользователей. Каждому из пользователей присваивается определенная роль. Причем, ролей может быть только три. Это:

- роль – Администратор;
- роль – Менеджер репозиториев;
- роль – Пользователь.

Роль администратора позволяет выполнять все административные функции в GraphDB. Роль менеджера репозиториев по существу управляет базами данных, так как каждый репозиторий является независимой базой данных RDF. Менеджер репозиториев имеет доступ ко всем репозиториям. Роль пользователя позволяет сохранять запросы SPARQL, проводить визуализацию графиков, а также ему может быть предоставлена возможность управления конкретным репозиторием.

Каждый пользователь должен иметь имя пользователя и пароль. По умолчанию для администратора задается имя пользователя (login) «admin» с паролем по умолчанию «root». Но это данные только для начальной установки. Поэтому рекомендуется сразу же заменить пароль администратора на новое значение. Имя «admin» при этом остается без изменений, так как это имя считается ключевым.

Все остальные пользователи могут иметь произвольные имена. Отметим, что для отладки допускается вариант, когда механизм ролевого доступа может быть отключен. Это действие осуществляется одним переключателем в разделе настройки пользователей. В отключенном режиме все подключаются к базе без пароля и с правами администратора. Но это не означает, что в режиме эксплуатации этот вариант должен использоваться.

3. Авторизация и управление доступом

Авторизация – это установление соответствия пользователя и определенного набора разрешений. На основе этого набора разрешений осуществляется управление доступом. Каждое разрешение предоставляет право доступа к тому или иному действию.

Все разрешения группируются в совокупности иерархических ролей, которые содержат как разрешения, непосредственно относящиеся к данной роли, так и разрешения, наследуемые от родительских.

В зависимости от основных ролей (администратор, менеджер репозитория и администратор) пользователи получают также предопределенные разрешения. Например, предопределенное разрешение «доступ на запись/чтение ко всем репозиториям» имеют пользователи «администратор» и «менеджер репозиториев», но не имеет «пользователь».

4. Методы аутентификации

Рассмотрим процесс подключения клиента к GraphDB. При этом производится проверка соответствия подключаемого пользователя предварительно заданному в базе данных пользователю. При этом в случае успешной проверки считается, что создается контекст безопасности. Как только этот контекст безопасности сопоставлен конкретному пользователю, то с ним связывается перечень разрешений.

При этом используются следующие методы аутентификации:

- базовая аутентификация, когда логин и пароль отправляются в виде текста в заголовке (используется по умолчанию);
- аутентификация на основе токенов;
- с использованием протокола Kerberos;
- аутентификация с использованием цифровой подписи (с использованием сертификата X.509;
- идентификация с использованием метода единого входа OpenID.

5. Вопросы шифрования

Рекомендуется при передаче данных между клиентом и сервером осуществлять шифрование информации. При этом целесообразно для закрытия трафика использовать протокол SSL/TLS. При этом обычно используются сертификаты, выданные доверенным центром сертификации.

Нужно отметить, что данные в базах данных обычно не шифруются. Поэтому при необходимости можно использовать сторонние средства шифрования.

6. Журнал аудита

При использовании GraphDB ведется журнал аудита. Его можно включить и настроить с помощью параметров конфигурации. Обычно в журнале аудита фиксируется события несанкционированного доступа, реконфигурация и случаи предотвращения недопустимых действий.

7. Общая оценка настройки безопасности в GraphDB

GraphDB обладает достаточно большим спектром настройки и применения параметров безопасности, к тому же разработчики ведут активное исправление ошибок и добавляют новые возможности. Имеется возможность проведения аутентификации разными средствами [4]. Возможно простая аутентификация с использованием пары логин-пароль, возможно использование токенов, допускается применение цифровой подписи и других методов. На основе аутентификации обеспечивается проведение авторизации, которая для каждого пользователя может установить определенный спектр разрешений. С использованием протоколов SSL возможно проведение шифрование трафика обмена. Кроме того, для проведения дополнительного контроля предусмотрены средства аудита.

Влияние реализованных механизмов защиты на быстродействие базы минимально. Для проверки этого был проведен ряд экспериментов. В базе данных был создан репозиторий с объемом информации чуть больше 100 Мб. Были реализованы 2 запроса. Первый – это минимальный запрос, возвращающий около 50 символов. Второй запрос является по сути обычным запросом, с результатом около 4000 символов. Запросы выполнялись в цикле 100 раз и замерялось время. Такие циклы вызывались несколько раз как для открытого режима, так и для защищенного. Минимальное и максимальное время выполнения такого блока в сто вызовов приведено в таблице 1. Как можно видеть, если на минимальном запросе время выполнения чуть больше при включенной защите, то при уже обычном запросе разница практически не видна.

Таблица 1. Минимальное и максимальное время выполнения блока запросов в открытом и защищенном режимах.

	Время выполнения первого запроса (100 раз)		**Время выполнения второго запроса (100 раз)**	
	Min (сек)	**Max (сек)**	**Min (сек)**	**Max (сек)**
Открытый режим	0,87	1,04	28,57	28,96
Защищенный режим	0,98	1,08	28,85	28,97

8. Заключение

Опыт работы с системой GraphDB показал, что она обладает необходимой устойчивостью и достаточным быстродействием при работе с графовыми базами данных. Вместе с тем имеется достаточно полный набор средств, обеспечивающий безопасную обработку информации. Все это дает возможность эффективно обрабатывать данные, сформированные на основе онтологических схем.

Список литературы

1. Плаксий К.В., Никифоров А.А., Милославская Н.Г. Исследование графовых СУБД, пригодных для работы с большими данными при обнаружении дел по отмыванию доходов, полученных преступным путем, и финансированию терроризма. Безопасность информационных технологий - IT Security. 2019. Т. 26, № 3. С. 103–116.
2. Загрузки и ресурсы GraphDB (ontotext.com), https://graphdb.ontotext.com/ (дата обращения 20.11.2023).
3. Документация по GraphDB 10.4 (ontotext.com) https://graphdb.ontotext.com/documentation/10.4/ (дата обращения 20.11.2023).
4. Козлов А.Д., Орлов В.Л. Методы и средства обеспечения информационной безопасности распределенных корпоративных систем. М.: ИПУ РАН, 2017. 165 с.