ПРОГРАММНОЕ СРЕДСТВО СЕРВИСНОГО ОБСЛУЖИВАНИЯ БАЗ ДАННЫХ MYSQL

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Навицкий И.П.

Ворвуль А.А. – магистр техн. наук

В настоящее время в базах данных хранятся большие объёмы информации. Базы данных могут содержать множество таблиц сложной структуры для хранения и представления различного рода данных. По мере роста и развития баз данных, всё чаще возникает необходимость системного управления и администрирования, постоянного сервисного обслуживания, контроля и диагностики. Приложение, содержащее различные сервисные функции для работы с базами данных, помогает поддерживать их в рабочем состоянии, анализировать параметры безопасности и производительности, устраняя тем самым потенциальные проблемы и сбои в работе баз данных в будущем. Поскольку в базах данных может храниться важная информация, то крайне необходимо обеспечить корректную работу баз данных и сохранность информации.

Программные средства, предназначенные для администрирования баз данных MySQL часто предоставляют оболочки над стандартными функциями MySQL в виде графического пользовательского интерфейса. Однако большинство таких программ, как правило, не имеют собственных средств анализа работы с базами данных. Разрабатываемое программное средство, помимо графической оболочки над стандартными сервисными функциями, будет иметь собственный модуль анализа безопасности, который позволит выявить как нарушения, так и возможные проблемы связанные с безопасностью баз данных.

Анализ состояния безопасности баз данных будет основан на проверке прав пользователей, а также возможности доступа с различных хостов.

Как показал анализ предметной области, в MySQL пользователи могут обладать различными глобальными привилегиями, которые дают возможность выполнять соответствующие операции над всеми базами данных в рамках одной СУБД. Эти глобальные привилегии можно разделить на 2 группы: относительно безопасные глобальные привилегии и опасные глобальные привилегии.

Пользователь, обладающий относительно безопасными глобальными привилегиями, не может выполнить какие-либо операции, которые могли бы привести к потере или искажению данных. Однако, наличие таких глобальных привилегий может привести к ухудшению работы системы управления базами данных в плане снижения производительности, а также к стремительному уменьшению дискового пространства, т.е. к «захламлению» баз данных ненужными или неактуальными данными. Эти проблемы могут возникнуть при неумелом обращении с базой данных, ошибках в запросах или при получении злоумышленником доступа к правам пользователя, обладающего относительно безопасными глобальными привилегиями.

Относительно безопасные глобальные привилегии связаны с операциями [1]: SELECT, INSERT, UPDATE, CREATE, RELOAD, FILE, REFERENCES, INDEX, SHOW_DB, CREATE_TMP_TABLE, REPL_SLAVE, REPL_CLIENT, CREATE_VIEW, SHOW_VIEW, CREATE_ROUTINE, EVENT, TRIGGER, CREATE_TABLESPACE.

Пользователь, обладающий опасными глобальными привилегиями, имеет возможность выполнить какие-либо действия, которые могут привести к искажению, потере данных, или к полному удалению баз данных. Наличие опасных глобальных привилегий у пользователей, за исключением пользователя root, является серьёзным нарушением безопасности и ставит под угрозу сохранность данных, важность которых может быть очень высока.

Опасные глобальные привилегии связаны с операциями [1]: DELETE, DROP, SHUTDOWN, GRANT, ALTER, PROCESS, SUPER, LOCK_TABLES, EXECUTE, ALTER_ROUTINE, CREATE_USER.

Таким образом, в ходе анализа безопасности баз данных выявлены как относительно безопасные глобальные привилегии, так и опасные глобальные привилегии. При обнаружении у пользователя опасных глобальных привилегий необходимо сгенерировать предупреждение о нарушении безопасности базы данных. Если у пользователя относительно безопасные глобальные привилегии, то нарушения в безопасности нет, однако генерируется соответствующее предупреждение. Для пользователя root наличие относительно безопасных глобальных привилегий и опасных глобальных привилегий нарушением безопасности не считается.

В анализ безопасности базы данных также входит проверка хостов, с которых возможен доступ каждого из пользователей. Если пользователь root доступен с других хостов, помимо localhost – то это считается нарушением безопасности. Возможность доступа ко всем остальным пользователям с хостов, не являющихся localhost, нарушением безопасности не считается, но генерируется соответствующее предупреждение.

Таким образом, в рамках данной работы будет разработано программное средство, предоставляющее как стандартные средства для сервисного обслуживания баз данных MySQL, так и собственный модуль анализа безопасности, позволяющий выявить текущие и потенциальные проблемы связанные с безопасностью баз данных.

Список использованных источников:

1. Кузнецов, М. В. MySQL 5 / М. В. Кузнецов, И. В. Симдянов. – СПб: БХВ-Петербург, 2010. – 1024 с.