Швейкин Владислав Витальевич

студент

ФГАОУ ВО «Самарский национальный исследовательский университет им. академика С.П. Королева»

г. Самара, Самарская область

АУДИТ БАЗ ДАННЫХ ORACLE

Аннотация: *в данной статье автором рассматриваются базовые понятия аудита в базах данных, а также некоторые особенности при использовании службы аудита.*

Ключевые слова: *базы данных, аудит, безопасность, событие, информационная система.*

Введём некоторые определения, которые будут использованы в работе.

1. СУБД (система управления базами данных) – программно-аппаратный комплекс, позволяющий управлять и манипулировать базами данных.

2. Информационная система – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы, которые обеспечивают и распространяют информацию.

Одной из важных составляющих процесса обеспечения безопасности информационной системы является проведение качественного аудита. Несмотря на то, что подготовка и проведение аудита безопасности информационной системы требует существенных затрат ресурсов, зачастую подобные затраты являются оправданными. На основании исследований можно убедиться, что существует устойчивая тенденция роста числа нарушений нормальной работы ИС и финансовых потерь, связанных с различными нештатными ситуациями.

В качестве причин подобной сложившейся ситуации можно выделить:

Возрастающая роль информационных технологий в современном мире и, как следствие, применение повышенных требований к защищённости ИС.

Увеличение сложности ИС и их подсистем обеспечения безопасности.

Проведение качественного независимого аудита помогает своевременно выявить существующие недостатки в безопасности информационной системы и оценить соответствие параметров, которые характеризую режим обеспечения безопасности, требуемому решаемыми задачами уровню.

В центре построения информационной системы предприятия находится СУБД промышленного уровня, которая должна обладать средствами автоматического ведения протоколов действий пользователей системы.

В СУБД средство ведения аудита может быть представлено в виде независимой утилиты или возможностей, управляемых языковыми средствами системы. Для каждого экземпляра сервера баз данных может быть запущен собственный файл аудита.

Средства аудита позволяют выполнять фиксацию действий пользователей системы в словаре данных или журнале аудита. Информация о настройках системы аудита находится в специальном конфигурационном файле, который вместе с командами активизации аудита определяет перечень отслеживаемых системой аудита событий.

Перечень действий, которые может выполнять пользователь со средствами аудита при наличии необходимых полномочий:

– запуск и остановка средства аудита;

– просмотр состояния конфигурации средств аудита и настройка средств аудита на отслеживание определённых событий;

– запись файлов аудита во внешние файлы операционной системы для проведения независимого анализа.

В СУБД Oracle для настройки системы аудита используется оператор AUDIT. Изменения перечня событий, фиксируемых в журнале аудита, сразу вступают в силу. Так же по каждой группе событий возможна фиксация как успешно, так и неуспешно выполненных операций.

Для автоматической фиксации событий в системе при помощи соответствующих записей в журнал аудита, необходимо активизировать службу аудита и

определить перечень фиксируемых событий. Значения параметров, определяющих работу сервера баз данных находятся в файле специальной структуры spfile, который расположен в каталоге $ORACLE_HOME/dbs/spfile<SID_name>.ora. Для внесения изменений в этот файл необходимо выполнить специальную команду SQL, требующую привилегированного варианта регистрации «AS SYSDBA ‘.

Значение параметра audit_trail указывает на то, куда записываются данные аудита. При audit_trail = DB запись производится в словарь данных, при audit_trail = XML – в файл операционной системы в формате XML, а при audit_trail = NONE – аудит находится по умолчанию в выключенном состоянии. Для вступления изменённых параметров активизации аудита в силу требуется перезапустить сервер.

Перечень фиксируемых событий может быть модифицирован в любое время, при наличии привилегии AUDIT SYSTEM (аудит системных событий) или AUDIT ANY (аудит событий, которые связаны с доступом к объекту системы). Стоит отметить, что перечень отслеживаемых событий может быть изменён и в период, когда служба аудита не активна. В таком случае запись событий начнётся только после активизации службы.

Список литературы

1. Смирнов С.Н. Безопасность систем баз данных. – М.: Гелиос АРВ, 2007. – 352 с.