А. М. Бондарь
Московский инженерно-физический институт

АУДИТ И ПРОТОКОЛИРОВАНИЕ В СУБД Oracle

Статья посвящена возможностям ведения аудита в системах управления базами данных Oracle 9i/10g, являющихся неотъемлемой частью подсистемы защиты от угроз нарушения конфиденциальности информации. Приводятся основные сведения о доступных типах аудита, настройке, а также аспекты, нюансы и рекомендации по его использованию. Данная статья будет полезна как начинающему администратору — поможет разобраться с широкими возможностями аудита, предоставляемыми Oracle, так и опытному специалисту — позволит структурировать свои знания.

Введение

Сейчас многие используемые как в коммерческих, так и государственных структурах базы данных (БД) хранят чувствительную информацию, защите которой должно быть уделено особое внимание. Защита начинается с вопроса о выборе используемой для обработки информации системы управления базами данных (СУБД). В настоящее время на рынке в этой области представлено много коммерческих проверенных временем решений, таких как Oracle Database, Microsoft SQL Server, DB2, Sybase и др., каждое из них обладает своими достоинствами и недостатками. Хорошо себя зарекомендовала СУБД Oracle Database (от Oracle Corporation), обеспечивающая хорошую производительность, масштабируемость и надежность, а также обладающая довольно широкими возможностями по защите БД. Следующим вопросом, который необходимо решить, является выбор методов обеспечения безопасности хранимой и обрабатываемой в БД информации. В данном случае, как и при построении защиты любой другой автоматизированной системы (АС), необходим комплексный подход, учитывающий по возможности все нюансы обрабатываемых данных.

Важную роль играют вопросы защиты БД от различных угроз нарушения конфиденциальности хранимой и обрабатываемой чувствительной информации, поэтому протоколирование и аудит, являющиеся неотъемлемыми частями системы защиты от реализации угроз конфиденциальности информации, требуют особого внимания со стороны администратора безопасности, лица, отвечающего за информационную безопасность БД в организации. Они и будут рассмотрены в данной статье применительно к использованию в СУБД Oracle версий 9i/10g.

Oracle предоставляет администратору мощный и гибкий инструмент ведения аудита и протоколирования различных событий в системе. Плохо настроенный аудит, в свою очередь, может не только не усилить общую защищенность БД в целом, но и подорвать ее, создав дополнительную брешь для утечки информации, или даже нарушить доступность БД. И потому так важно четко представлять тонкости использования аудита и возможности его настройки.

Аудит и протоколирование

Протоколирование — это сбор и накопление информации обо всех событиях, имеющих отношение к вопросам безопасности. В свою очередь, аудит — это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически с целью своевременного выявления и предотвращения нарушений режима информационной безопасности.

Oracle предоставляет возможности аудита различных событий и действий пользователей системы на уровне сервера БД. Соответственно, администратор безопасности должен определить политики ведения аудита для каждой БД АС, учитывающие степень детализации аудита и другие его аспекты. Ведь использование аудита является естественным дополнением механизма контроля доступа к АС.

Аудит в Oracle активируется и деактивируется путем задания параметра инициализации AUDIT_TRAIL в файле init.ora в соответствующее значение, определяющее тип аудита (по умолчанию протоколирование не ведется). Информация о произошедших в АС событиях регистрируется в *журнале аудита*, который может находиться как в БД в специальной таблице AUD$ в схеме SYS, так и в специальных файлах операционной системы (ОС). После активации аудита на уровне запущенного экземпляра БД администратор безопасности задает протоколирование соответствующих системных событий (действий пользователей) с помощью команд AUDIT <…>. Администратор безопасности должен проводить все действия под профилем пользователя БД, обладающего привилегиями AUDIT ANY и/или AUDIT SYSTEM (как правило, это пользователь SYS).

В зависимости от типов системных событий, подлежащих протоколированию, степени детализации аудита, способа хранения журнала аудита и других факторов предлагается следующую классификацию аудита в Oracle:

1. По объектам аудита

а) операторы языка SQL. Выборочный аудит соответствующих групп операторов, относящихся к определенному типу структур БД или объектов схемы. Под понятие SQL-операторов в данном случае попадают:

· операторы ЯМД (язык манипулирования данными). Например, команда AUDIT SELECT TABLE будет протоколировать попытки запросить данные из любой таблицы (представления, построенного с участием этой таблицы);

· операторы ЯОД (язык определения данных). Например, команда AUDIT TABLE будет протоколировать все операции по созданию (CREATE), удалению (DROP) таблиц.

Интересно заметить, что под данный тип аудита попадает протоколирование успешных и неуспешных установлений сессий БД (AUDIT SESSION), а также SQL-операторов, вызывающих ошибку несуществования объекта в схеме (AUDIT NOT EXISTS);

б) объекты схемы БД. Протоколирование действий (операторов ЯМД) с объектами БД определенной схемы пользователя. Например, оператор AUDIT DELETE ON Scheme1.Table1 включит протоколирование всех операций удаления строк из таблицы Table1 схемы Scheme1.

В данном случае возможны ситуации, когда одно действие пользователя будет служить причиной нескольких схожих записей в журнале аудита. Например, если задан аудит оператора SELECT для таблицы и представления, построенного с ее использованием.

Также стоит отметить, что протоколирование объектов БД активируется сразу же после соответствующей команды AUDIT и не требует в отличие от других типов аудита перезапуска сессии пользователя;

в) привилегии пользователей. Аудиту подвергается использование привилегий пользователем при выполнении каких-либо действий. Причем, если ведется протоколирование привилегии и соответствующего ей оператора SQL (например, если протоколируется привилегия командой AUDIT SELECT ANY TABLE и оператор SELECT), то в журнал аудита заносится только одна запись;

г) операции над отдельными строками/столбцами объектов БД. Данная разновидность аудита доступна при *тщательном аудите данных* (Fine-Grained Auditing), позволяющем протоколировать использование операторов SQL не на уровне объекта БД, а на уровне определенного столбца и строки таблицы/представления. Например, можно настроить аудит так, чтобы протоколировались только операции по изменению конкретного столбца таблицы на значение, превышающее заданный предел;

д) сеть. Данный узкий класс аудита позволяет протоколировать ошибки, связанные с неверным заданием настроек шифрования данных при их передаче по сети.

2. По типу аудита

а) аудит по умолчанию. К этому классу аудита относится выполняющийся всегда так называемый *обязательный* аудит, включающий протоколирование в журнал аудита ОС следующих связанных с функционированием БД операций:

· открытие сессии с правами администратора (привилегия SYSDBA или SYSOPER),

· запуск экземпляра БД,

· остановка экземпляра БД.

Активируется при любом задании параметра инициализации AUDIT_TRAIL, отличном от NONE;

б) стандартный аудит. Стандартный аудит подразумевает протоколирование различных системных событий и действий пользователей БД.

Активируется при задании параметра инициализации AUDIT_TRAIL в значения DB, XML или OS;

в) системный аудит. Аудит пользователя SYS и пользователей, обладающих привилегиями SYSDBA или SYSOPER. Для активации данного типа аудита необходимо задать параметр инициализации AUDIT_SYS_OPERATIONS=TRUE (по умолчанию FALSE). При этом производится протоколирование всех без разбора действий пользователя SYS и только в файлы журнала аудита на уровне ОС независимо от значения параметра инициализации AUDIT_TRAIL;

г) расширенный аудит. Расширенный аудит отличается от стандартного большей степенью детализации записей журнала аудита, включающих дополнительную информацию о значениях связанных переменных (bind) и текст выполненного оператора языка SQL.

Активируется при задании параметра инициализации AUDIT_TRAIL в значения либо DB,EXTENDED, либо XML,EXTENDED;

д) тщательный аудит. Тщательный аудит данных отличается от стандартного аудита возможностью протоколирования более детальных событий. О данном типе аудита будет подробнее рассказано далее.

3. По месту хранения журнала аудита

а) таблица БД. Журнал аудита находится в БД в специальной таблице AUD$ схемы SYS. Администратору безопасности (администратору базы данных) легко запрашивать данные из журнала аудита, используя обычные операторы языка SQL.

При хранении журнала аудита в БД данные защищаются резервным копированием этой базы и не требуют дополнительного инструментария для своей интерпретации;

б) файлы ОС. Журнал аудита хранится в специальных файлах ОС, местоположение которых задается параметром инициализации AUDIT_FILE_DEST (для WINDOWS значение по умолчанию $ORACLE_BASE\admin\$DB_UNIQUE_NAME\adump, где $ORACLE_BASE – домашний каталог сервера Oracle, $DB_UNIQUE_NAME – имя БД).

При данном способе хранения журнала аудита в него не попадают такие данные, как системный номер изменения, идентификатор транзакции, номер инстанса и др.

Преимуществом использования журнала аудита, хранимого в ОС, является его доступность, даже если сервер СУБД не работает. Некоторое неудобство такого журнала состоит в необходимости использования при его интерпретации инструментария, подходящего для данной ОС и форматов файлов.

4. По формату записей журнала аудита

а) формат XML. При задании параметра инициализации AUDIT_TRAIL в значения XML либо XML,EXTENDED протоколирование производится в файлы ОС в формате языка XML (eXtensible Markup Language — расширяемый язык разметки). При этом заданная опция EXTENDED предоставляет дополнительную информацию о значениях связанных переменных и текст выполненного SQL-оператора. О данном типе аудита будет подробнее рассказано далее;

б) обычный формат. Журнал аудита представляет собой обычный текстовый файл.

5. По типу протоколируемых событий

а) успешные. Протоколированию подлежат только события (действия), завершившиеся успешно. Например, AUDIT SELECT ON Scheme1.Table1 WHENEVER SUCCESSFUL;

б) неуспешные. Протоколированию подлежат только события (действия), завершившиеся неуспешно. Например, AUDIT SELECT ON Scheme1.Table1 WHENEVER NOT SUCCESSFUL. При этом протоколируются действия пользователя, если они были неуспешны, например, из-за недостатка привилегий либо отсутствия объекта в схеме, то есть попытки выполнения синтаксически неверных операторов SQL не заносятся в журнал аудита;

в) успешные и неуспешные (по умолчанию). Протоколированию подлежат все события (действия), независимо от успешности их завершения. При этом ключевые слова WHENEVER ... SUCCESSFUL не указываются.

6. По области действия протоколирования

а) по сессии. Если протоколируемое событие имеет место несколько раз в рамках сессии, то в данном случае в журнале аудита появится только одна запись. Это достигается использованием спецификатора BY SESSION. Например, AUDIT SELECT VIEW BY SESSION;

б) по срабатыванию. Если протоколируемое событие имеет место несколько раз в рамках сессии, то в данном случае соответствующее количество записей появится в журнале аудита. Это достигается использованием спецификатора BY ACCESS (значение по умолчанию). Например, AUDIT INSERT TABLE BY ACCESS.

7. По пользователю

а) аудит действий одного пользователя. Указание спецификатора BY позволяет проводить протоколирование действий определенного пользователя. Например, AUDIT SELECT TABLE BY User1;

б) аудит действий группы пользователей. Список пользователей указывается после BY через запятую. Например, AUDIT UPDATE TABLE BY User1, User2, User3;

в) аудит действий всех пользователей. Используется по умолчанию и не требует указания спецификатора BY.

Теперь, когда представлена классификация, демонстрирующая возможности протоколирования в Oracle, можно подробнее остановиться на наиболее интересных особенностях аудита.

Стандартный аудит

Для того чтобы активировать протоколирование, первым шагом должна быть, как уже было сказано ранее, установка параметра инициализации AUDIT_TRAIL, с этого момента начинает работать обязательный аудит. Для протоколирования других событий необходимо явно использовать команду AUDIT <...>. При этом журнал аудита может храниться как в БД в таблице SYS.AUD$, так и в специальных файлах ОС.

Каждый пользователь может беспрепятственно активировать и деактивировать протоколирование в своей схеме. Пользователь SYS обладает привилегиями AUDIT SYSTEM и AUDIT ANY, позволяющими активировать протоколирование объектов БД, операторов SQL и привилегий в любой схеме БД. Такими привилегиями должен обладать только администратор безопасности. При задании протоколирования можно ограничивать область его действия с помощью спецификаторов (см. классификацию аудита):

· BY — ограничение действия протоколирования на определенных пользователей;

· BY SESSION/BY ACCESS — ограничение по частоте протоколирования в журнал аудита;

· WHENEVER SUCCESSFUL/WHENEVER NOT SUCCESSFUL - протоколирование только успешно/неуспешно завершенных операций.

Деактивировать протоколирование полностью или выборочно можно командой NOAUDIT <…>. При этом допускается использование тех же спецификаторов за исключением BY SESSION/BY ACCESS.

Для просмотра журнала аудита можно не напрямую обращаться к SYS.AUD$, а использовать удобные представления DBA_OBJ_AUDIT_OPTS, DBA_AUDIT_TRAIL, DBA_AUDIT_OBJECT, DBA_AUDIT_SESSION или их USER_% аналоги. Если журнал аудита хранится в файлах ОС, то их можно анализировать при возможности, например, средствами ОС (в MS Windows это журнал безопасности).

В журнале аудита хранится полезная информация о произошедшем событии: код завершения операции, имя пользователя БД, дата и время операции, название схемы объекта, идентификатор сессии и др. При этом в зависимости от места хранения журнала аудита некоторая информация может отсутствовать в случае использования файлов ОС. Использование расширенного аудита в данном случае добавляет протоколирование информации о значениях связанных переменных и тексте выполненного оператора языка SQL, что может оказаться крайне полезным, так как дает представление о совершенном пользователем действии. Интересным может также оказаться столбец с системным номером изменения (СНИ, SCN — System Change Number), который в дополнение ко всему может дать информацию о состоянии БД на момент времени перед свершением события. С помощью ретроспективных запросов (Flashback Queries), появившихся в версии Oracle Database 10g Release 1, можно получить данные на момент времени, указанный значением СНИ (тут есть ограничения, связанные с использованием сегмента отката UNDO в ретроспективных запросах и не позволяющие использовать «старые» СНИ).

Тщательный аудит данных

Тщательный аудит данных (ТАД) появился в версии Oracle Database 9i и позволяет вести мониторинг действий на основе содержимого БД. Этот встроенный механизм аудита исключает возможность его обхода пользователями. ТАД является гибким независимым расширением возможностей стандартного и расширенного аудита ЯМД-операций над таблицами и представлениями.

В некоторых случаях протоколирование ЯМД-операторов может быть избыточным и дорогим в плане производительности. Иногда в таких случаях принимается решение использовать «самодельный» аудит, основанный на использовании триггеров БД, который заносит в собственный журнал аудита только выборочные данные. Появление ТАД позволяет отказаться в большинстве случаев от таких решений, так как он гораздо эффективнее в плане производительности, работает на уровне ядра Oracle (потому его сложно обойти), универсален и гибко настраивается, не требует поддержки со стороны разработчиков. К тому же не требуется установка параметра инициализации AUDIT_TRAIL и других параметров для ведения стандартного и системного протоколирования.

ТАД основан на использовании *политик аудита*, неких правил протоколирования для каждого конкретного случая. Используя этот пакет, администратор безопасности создает политику для объекта БД, которая содержит предикат — SQL-выражение, при срабатывании которого событие протоколируется. Таким образом, при срабатывании каждой политики добавляется одна запись в журнал аудита. Для работы с политиками и настройками ТАД применяется пакет DBMS_FGA, содержащий необходимый программный интерфейс: создание политики (ADD_POLICY), деактивация политики (DISABLE_POLICY), активация политики (ENABLE_POLICY), удаление политики (DROP_POLICY). Например, можно настроить аудит так, чтобы протоколировалась только операция INSERT, нацеленная на таблицу EMP при вставке строки со столбцом Salary > 100 (в данном случае выражение «Salary > 100» будет предикатом).

Одной из особенностей ТАД является возможность для администратора безопасности опционально определять обработчик событий, например, высылающий ему при срабатывании уведомление.

При создании политики можно указывать специфику аудита (параметр audit_trail метода DBMS_FGA.ADD_POLICY):

· Запись журнала аудита в БД (DBMS_FGA.DB). Журнал аудита хранится в системной таблице SYS.FGA_LOG$.

· Аудит в формате XML (DBMS_FGA.XML). Журнал аудита хранится в специальных файлах ОС (аналогично стандартному аудиту на уровне ОС).

· Расширенный аудит (DBMS_FGA.DB + DBMS_FGA.EXTENDED или DBMS_FGA.XML + DBMS_FGA.EXTENDED). Журнал аудита дополнительно содержит информацию о выполненном SQL-операторе и значения связанных переменных.

Анализ журнала ТАД можно проводить на основе как таблицы SYS.FGA_LOG$, так и представления V$XML_AUDIT_TRAIL, помимо этого, представление DBA_COMMON_AUDIT_TRAIL содержит данные для всех журналов аудита, что может быть очень удобно.

Аудит в формате XML

В версии Oracle Database 10g Release 2 появляется функциональная возможность протоколирования на уровне ОС в формате XML. Журнал аудита в этом случае состоит из множества XML-документов, которые легко распознаваемы, к тому же существует много инструментов (работающих во многих ОС) для чтения и форматирования этих документов.

Задание параметра AUDIT_TRAIL=XML активирует протоколирование в XML-формате. Файлы журнала аудита сохраняются в том же каталоге, как и в случае обычного аудита на уровне ОС. При этом параметр инициализации AUDIT_FILE_DEST, задающий их местоположение, может быть переопределен: ALTER SYSTEM SET AUDIT_FILE_DEST = '/новый каталог' DEFERRED.

Значительным преимуществом аудита в формате XML перед стандартным аудитом на уровне ОС является возможность анализа журнала аудита через SQL-интерфейс. Это избавляет от необходимости использования специализированного инструментария для анализа журнала аудита: представление V$XML_AUDIT_TRAIL отражает содержимое XML-файлов журнала. XML-файлы имеют определенную структуру и, по сути, содержат ту же информацию, что и обычные записи аудита. Задание параметра AUDIT_TRAIL=XML,EXTENDED позволяет использовать расширенный аудит в формате XML — каждая запись аудита теперь содержит дополнительную информацию о выполненном SQL-операторе и значения связанных переменных.

Защита журнала аудита

Администратор безопасности должен учитывать в политике ведения аудита различные аспекты его использования и уделять внимание проблемам защиты журнала аудита.

· Привилегиями AUDIT SYSTEM и AUDIT ANY должен обладать только администратор безопасности. При этом нельзя забывать, что каждый пользователь может активировать и деактивировать протоколирование для объектов, владельцем которых он является. Избежать последней неприятной особенности (сделать так, чтобы только администратор безопасности контролировал аудит объектов БД) можно двумя способами:

- Все протоколируемые объекты хранятся в схеме администратора безопасности, и только он обладает привилегией AUDIT ANY.
- Все протоколируемые объекты хранятся в схемах, в которых ни один пользователь не имеет привилегии CREATE SESSION, и только администратор безопасности имеет привилегию AUDIT ANY.

· Журнал аудита в среде ОС принадлежит владельцу программного обеспечения сервера Oracle, поэтому его хранение в специальных файлах ОС дает возможность разграничивать к ним доступ со

стороны ОС. В этом случае рекомендуется использовать отдельные учетные записи ОС для администраторов базы данных, которые позволяют им администрировать базу данных (даже с наличием привилегии SYSDBA), но не разрешают удалять или изменять файлы журнала аудита. Использование файлов журнала аудита в файловой системе может обеспечивать достаточный для многих организаций уровень защищенности системы при аккуратном разграничении доступа на уровне ОС и БД.

· Если по каким-либо причинам необходимо предоставить некоторым пользователям доступ к SYS.AUD$, то можно активировать протоколирование действий над этой таблицей. Например, AUDIT SELECT ON sys.aud$ BY ACCESS. Заметим, что операции INSERT, UPDATE, DELETE и MERGE всегда протоколируются и соответствующие записи не могут быть удалены из SYS.AUD$.

· Со временем журнал аудита может переполниться, в результате чего ни одна протоколируемая операция не сможет завершиться успешно, пока журнал аудита не будет очищен. В некоторых случаях это может привести к нарушению доступности БД, например, если установлено протоколирование сессий CREATE SESSION (пользователь не сможет установить соединение с БД). Максимальный размер таблицы SYS.AUD$ ограничен размерами табличного пространства SYSTEM. В связи с этим в обязанности администратора безопасности должен входить контроль роста и переполнения журнала аудита. Журнал аудита можно периодически архивировать и/или чистить, удаляя старые записи, что может делать пользователь SYS, пользователь с привилегиями DELETE на эту таблицу либо с привилегией DELETE ANY TABLE. Очевидно, что использование указанных привилегий должно четко регламентироваться политикой безопасности.

· Любой пользователь, имеющий системную привилегию выполнения поставляемого пакета UTL_FILE, может удалить файлы журнала аудита из файловой системы ОС (с помощью процедуры FREMOVE). Для того чтобы снизить этот риск, администратору безопасности необходимо:

- аннулировать эту привилегию у группы пользователей PUBLIC (с пакетом UTL_FILE нельзя будет работать данной группе);
- аннулировать системную привилегию CREATE DIRECTORY у группы пользователей PUBLIC (группа не сможет самостоятельно создавать каталоги).

· При необходимости может быть активировано протоколирование действий пользователей с привилегиями SYSDBA или SYSOPER, что осуществляется путем задания параметра инициализации AUDIT_SYS_OPERATIONS=TRUE. Это позволит протоколировать действия пользователей, обладающих административными привилегиями.

СПИСОК ЛИТЕРАТУРЫ

1. Oracle Database Security Guide.
2. Oracle Database Concepts.
3. Oracle Database Reference.
4. Oracle Database SQL Reference.
5. Аудит в XML-формате, Арап Нанда. http://www.oracle.com/technology/oramag/oracle/06-jan/o16security.html.