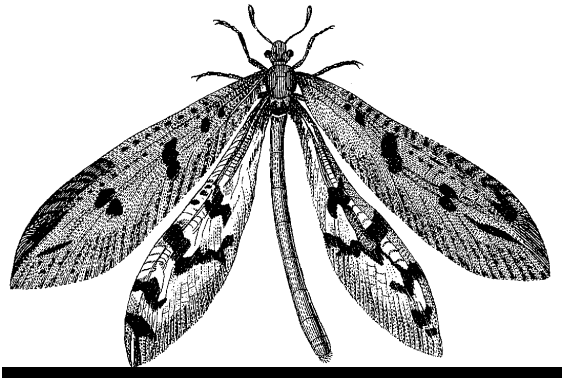
Охватывает все версии Oracle вплоть до Oracle9i

ORACLE

СПРАВОЧНИК

Символ®
O'REILLY®

Рик Гринвальд и Дэвид К. Крейнс



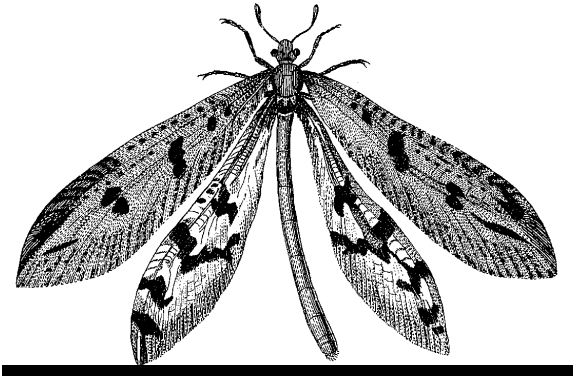
ORACLE

IN A NUTSHELL

A Desktop Quick Reference

Rick Greenwald & David C. Kreines

O'REILLY®



ORACLE

СПРАВОЧНИК

Рик Гринвальд и Дэвид К. Крейнс

Санкт-Петербург — Москва
2005

Рик Гринвальд и Дэвид Крейнс

Oracle. Справочник

Перевод П. Шера

Главный редактор	*А. Галунов*
Зав. редакцией	*Н. Макарова*
Научный редактор	*А. Королев*
Редактор	*В. Овчинников*
Корректор	*О. Макарова*
Верстка	*Н. Гриценко*

Гринвальд Р., Крейнс Д.
Oracle. Справочник. – Пер. с англ. – СПб: Символ-Плюс, 2005. – 976 с., ил.
ISBN 5-93286-064-2

Oracle появилась четверть века назад и по сей день остается ведущей СУБД масштаба предприятия. Oracle – сложная система, предлагающая несметное множество продуктов, языков и инструментов. Следующие один за другим обновления, релизы и выпуски делают все более сложной задачу пользователя, стремящегося справиться с могучим потоком часто меняющейся информации об этой СУБД и ее возможностях. Задача «Oracle. Справочник» – объединить наиболее важную информацию по архитектуре, синтаксису и пользовательским интерфейсам Oracle. Синтез формы и содержания этой книги от O'Reilly дает лаконичный и очень доступный настольный справочник, содержащий важнейшие команды, конструкции языка, параметры и форматы файлов Oracle.

«Oracle. Справочник» – это кладезь информации, необходимой администраторам БД, разработчикам на PL/SQL и Java, системным и сетевым администраторам, а также специалистам по безопасности, имеющим дело с БД Oracle. Эта книга не раз поможет программистам, использующим как Oracle9*i* версии 2, так и более ранние продукты, при написании кода, работающего с данными Oracle.

ISBN 5-93286-064-2
ISBN 0-596-00336-6 (англ)

Издательство «Символ-Плюс». 199034, Санкт-Петербург, 16 линия, 7,
тел. (812) 324-5353, edit@symbol.ru. Лицензия ЛП N 000054 от 25.12.98.
Налоговая льгота – общероссийский классификатор продукции
ОК 005-93, том 2; 953000 – книги и брошюры.

Подписано в печать 04.04.2005. Формат 70x100 1/16 . Печать офсетная.
Объем 61 печ. л. Тираж 2000 экз. Заказ N
Отпечатано с диапозитивов в ГУП «Типографии «Наука»
199034, Санкт-Петербург, 9 линия, 12.

Моему отцу, Роберту Гринвальду.

– Рик Гринвальд

Сюзанне, главной хранительнице единства.

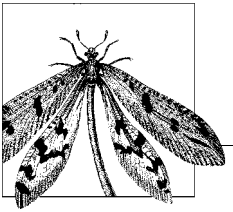
– Дэвид К. Крейнс

Оглавление

Часть II. Языки

Часть III. Инструменты и утилиты

Часть IV. Приложения



Предисловие

Появившись четверть века назад, Oracle остается мировым лидером среди реляционных систем управления базами данных (РСУБД) уровня предприятия. Oracle – это сложная система, предлагающая огромное количество продуктов, языков и инструментов. Регулярно выходят обновления, появляются новые решения и версии, и пользователям нелегко справляться с большим объемом постоянно меняющейся информации по Oracle. Помочь разобраться в ситуации призвано великое множество книг, статей и веб-сайтов. Нужна ли еще одна такая книга?

Цель издания «Oracle. Справочник» в том, чтобы предоставить вам действительно необходимые знания об Oracle в книге, содержимое и формат которой выбраны так, чтобы полезная информация всегда была у вас под рукой. Эта книга – удобный справочник по командам и параметрам основных языков и инструментов Oracle. Мы постарались собрать воедино (и представить по возможности кратко) те сведения, которые необходимы администраторам и разработчикам баз данных для управления СУБД Oracle и создания программного кода.

Как и вся серия «In a Nutshell» издательства O'Reilly, эта книга предназначена тем, кто знает, что хочет сделать, но не может вспомнить нужную команду или значение по умолчанию, соответствующий параметр или диапазон значений, правильный формат заголовка пакета или тип данных. Предполагается, что читатель уже хотя бы немного знаком с обсуждаемыми языками и инструментами. Если вам необходимо руководство, подробное описание применения или особые тонкости, можно обратиться к документации по Oracle и другим более специализированным книгам (большой список книг и других дополнительных ресурсов необходимой информации по вопросам, охваченным в нашей книге, приведен в приложении E). Но хотелось бы думать, что ответы на большинство вопросов вы сможете найти в нашей книге. Надеемся, что она станет бесценным настольным справочником для всех пользователей Oracle.

Несколько слов о том, чем является эта книга и чем не является. Это краткий справочник, необходимый практически всем пользователям Oracle. Здесь есть сведения для администраторов БД, разработчиков, использующих PL/SQL и Java, системных и сетевых инженеров, а также для специалистов по безопасности. Многие главы по большей части состоят из краткой справочной информации (например, перечень параметров инициализации; синтаксис команд SQL и PL/SQL, вызовы функций, заголовки процедур и функций встроенных пакетов; команды и параметры SQL*Plus, SQL*Loader, Import/Export и RMAN; представления словаря данных; интерфейсы и классы Oracle/Java; рекомендации по оптимизации). Но для того чтобы не делать книгу совсем

громоздкой (название серии «In a Nutshell» – «в двух словах» и так уже похоже на насмешку!), решено было не углубляться в другие интересные технические вопросы.

Основная из стоявших перед нами задач оказалась и самой сложной: как создать хороший справочник по Oracle и при этом не сделать его неподъемным? Решено было руководствоваться несколькими правилами:

1. Мы пытались следовать правилу 90/10. Аналогично правилу 80/20 оно гласит, что можно предоставить 90% наиболее важной информации об Oracle на 10% страниц. Данная книга содержит экстракт из 13 000 страниц документации Oracle (для Oracle9*i*), поэтому надеемся, что эта цель достигнута.
2. Мы хотели, чтобы несмотря на отсутствие излишних подробностей, предлагаемая информация не теряла смысла и оставалась полезной. Результат можно увидеть, например, в главе 10: для каждого из множества вызовов встроенных пакетов PL/SQL приведен заголовок и краткое описание, но ничего больше. Если потребуется изучить какой-то конкретный пакет более тщательно, обратитесь за информацией к документации Oracle, но для применения данной функциональности достаточно сведений, приведенных в главе 10.
3. Скрепя сердце, мы оставили лишь минимальное количество примеров. Если приводить пример для каждой команды, оператора и параметра, объем книги возрастет до невозможности. Наиболее заметно отсутствие примеров в главе по SQL (и без того очень длинной). При этом, как уже говорилось, мы надеемся, что книга структурно и содержательно организована так, что те, кому понадобятся какие-то дополнительные сведения, всегда будут знать, где их найти.
4. Везде, где это представлялось возможным, мы старались организовать форму и содержание так, чтобы максимально облегчить восприятие информации. В качестве примера можно рассмотреть параметры инициализации в главе 2, которые приведены не просто как список, упорядоченный по алфавиту, а разбиты на смысловые группы. Как показывает наш опыт, родственные параметры обычно используются вместе, поэтому глава была организована именно так. Кроме того, надеемся, что благодаря такой структуре читатель, обратившись за одним описанием, откроет для себя неизвестные ранее связанные параметры.
5. Наконец, было решено ограничиться только теми вопросами, которые важны для основной массы пользователей Oracle. Поэтому, хоть и неохотно, мы опускаем обсуждение Advanced Queuing, Streams, Advanced Security и множества других узкоспециализированных возможностей. Если бы мы попытались включить в повествование даже самое поверхностное их описание, наша основная цель никогда не была бы достигнута.

Надеемся, что мы приняли правильное решение. Если не согласны – ждем ваших комментариев, но, пожалуйста, будьте великодушны!

Платформа и версия

Oracle может работать на огромном количестве аппаратных и программных платформ. Большая часть информации, представленной к книге, применима к любой платформе. Если какие-то команды или параметры особым образом ведут себя в среде Windows, Linux или какой-то другой, это будет отмечено в тексте.

К моменту выхода этой книги последней версией была СУБД Oracle9*i* Release 2. Версия Oracle9*i* появилась сравнительно недавно, поэтому мы хорошо помним, какие новые возможности в ней появились, а какие исчезли. Во многих разделах будут при-

сутствовать такие комментарии, как «появилось в Oracle9*i*» и «не поддерживается после Oracle8*i*». Надеемся, что эти замечания пригодятся пользователям, работающим со старыми версиями Oracle. О системах более ранних, чем Oracle8, речь не идет.

Структура книги

Справочник состоит из четырех частей:

Часть I «Основы»

Первая часть содержит базовые сведения о СУБД Oracle, которые не зависят от используемых вами языка и инструментов.

- Глава 1 «Архитектура и комплект поставки» предлагает обзор архитектуры и основных компонентов СУБД Oracle и рассказывает о различных решениях Oracle.
- Глава 2 «Конфигурирование» описывает параметры инициализации (параметры в *INIT.ORA* и/или *SPFILE*), отвечающие за настройку вашей базы данных Oracle.
- Глава 3 «Конкурентный доступ» рассказывает о принятой в Oracle многоверсионной модели согласованности по чтению (Multiversion Read Consistency – MVRC) и обсуждает транзакции, блокировки и другие принципы конкурентного доступа к данным.
- Глава 4 «Безопасность» кратко рассказывает об аутентификации пользователей, профилях, привилегиях, ролях и аудите, а также приводит синтаксис команд управления безопасностью СУБД Oracle.
- Глава 5 «Работа в сети» описывает основы сетевых возможностей Oracle и приводит синтаксис необходимых конфигурационных файлов, а именно *TNSNAMES.ORA*, *SQLNET.ORA*, *LISTENER.ORA*, *LDAP.ORA*, *NAMES.ORA* и *CMAN.ORA*.
- Глава 6 «Словарь данных» описывает представления словаря данных Oracle, которые хранят информацию об объектах и пользователях СУБД Oracle; она охватывает как статические представления, так и динамические представления производительности.

Часть II «Языки»

Вторая часть книги посвящена синтаксису команд и функций SQL, программ PL/SQL и Java-интерфейсов для Oracle.

- В главе 7 «SQL» описывается синтаксис Oracle-версии структурированного языка запросов (SQL – Structured Query Language).
- Глава 8 «Функции» приводит синтаксис функций, которые могут быть вызваны из SQL и PL/SQL.
- В главе 9 «PL/SQL» кратко рассмотрены возможности процедурного языка Oracle и описан формат всех его операторов.
- Глава 10 «Пакеты PL/SQL» приводит перечень спецификаций заголовков всех процедур и функций встроенных пакетов Oracle, а также описания параметров.
- В главе 11 «Java и Oracle» рассказывается о Java-интерфейсах к СУБД Oracle, в том числе о драйверах Java для Oracle, о сопоставлении типов данных Java и Oracle и о синтаксисе интерфейсов SQLJ и JDBC.

Часть III «Инструменты и утилиты»

В третьей части представлены команды и спецификации файлов для различных инструментов и утилит, применяемых для управления СУБД Oracle и взаимодействия с ней.

- Глава 12 «SQL*Plus» содержит описание команд и элементов форматирования, доступных пользователю в SQL*Plus – интерфейсе командной строки для Oracle, который предназначен для ввода команд SQL, кода PL/SQL, а также для выполнения файлов сценариев.
- Глава 13 «Экспорт и импорт» содержит перечень команд, предлагаемых утилитами Export (копирование данных из базы данных в двоичный файл) и Import (импорт данных из двоичного файла в базу данных Oracle). Эти утилиты позволяют получать сведения о структуре и содержимом базы данных Oracle.
- В главе 14 «SQL*Loader» описываются команды утилиты SQL*Loader, предназначенной для загрузки данных в стандартных файловых форматах операционной системы в базу данных Oracle и выполнения различных преобразований данных в процессе загрузки.
- Глава 15 «Резервное копирование и восстановление» кратко описывает принципы резервного копирования и восстановления данных Oracle и шаблоны процедур, обеспечивающих управляемое пользователем копирование и восстановление. Приводится перечень команд специальной утилиты Oracle RMAN (Recovery Manager).
- Глава 16 «Enterprise Manager» описывает возможности Enterprise Manager – консоли с графическим интерфейсом пользователя, которая позволяет управлять сервером Oracle.
- Глава 17 «Производительность» рассматривает основные инструменты Oracle, с помощью которых можно оценить и улучшить производительность. Описываются оптимизаторы и подсказки для них в SQL. Приводится синтаксис применения таких средств оптимизации, как Explain Plan, TKPROF, AUTOTRACE, UTLBSTAT, UTLESTAT и Statspack.

Часть IV «Приложения»

В этой части книги содержится сводная и справочная информация.

- Приложение A «Типы данных» содержит перечень типов данных Oracle и правила их преобразования.
- Приложение B «Выражения, операторы и условия» предлагает список разрешенных выражений, операторов и условий, которые можно включать в команды SQL, PL/SQL и SQL*Plus.
- Приложение C «Числовые форматы» приводит форматы чисел, поддерживаемые в командах SQL, PL/SQL и SQL*Plus.
- Приложение D «Форматы даты» приводит форматы дат, поддерживаемые в командах SQL, PL/SQL и SQL*Plus.
- Приложение E «Дополнительные ресурсы» содержит перечень книг и сетевых ресурсов, предлагающих дополнительные сведения по вопросам, изучаемым в данной книге.

Соглашения, принятые в этой книге

Мы будем придерживаться следующих типографских соглашений:

Курсив

Применяется к именам файлов, каталогов, адресов URL, при первом упоминании терминов, иногда для выделения важных понятий.

`Моноширинный шрифт`

Применяется при описании синтаксических конструкций и в примерах кода.

Моноширинный курсив

В синтаксических конструкциях обозначает изменяемый элемент (например, имя файла).

Моноширинный полужирный

Применяется при описании работы пользователя с утилитами (такими как SQL*Plus, RMAN); вводимые пользователем команды выделены полужирным шрифтом, а выводимые данные набираются обычным шрифтом. Также полужирным шрифтом выделены значения, принятые по умолчанию.

ВЕРХНИЙ РЕГИСТР

Употребляется для обозначения ключевых слов при описании синтаксических конструкций.

Нижний регистр

В описании синтаксических конструкций обозначает вводимые пользователем термы, такие как переменные и параметры.

[ ]

В синтаксических конструкциях в квадратные скобки заключены необязательные элементы.

{ }

В синтаксических конструкциях в фигурные скобки помещается список элементов, из которых должен быть выбран только один.

|

В синтаксических конструкциях вертикальная черта разделяет элементы, помещенные в фигурные скобки, например {VARCHAR2 | DATE | NUMBER}.

Таким форматированием выделены советы, предложения и примечания общего характера. Например, указано, что некоторая версия имеет определенные особенности.

Так выделены предупреждения и предостережения. Например, о том, что некоторая операция может иметь нежелательные последствия.

Комментарии и вопросы

Мы протестировали и проверили информацию, содержащуюся в этой книге и в исходных текстах настолько хорошо, насколько это было возможно, но, учитывая то, о каком количестве средств мы рассказываем, и как быстро все меняется, вы можете обнаружить, что некоторые свойства могли измениться, или мы могли допустить ошибки. Обнаружив, сообщите нам, написав по адресу:

O'Reilly & Associates

1005 Gravenstein Highway

Sebastopol, CA 95472

800-998-9938 (для США или Канады)

707-829-0515 (международный или внутренний)

707-829-0104 (факс)

Также вы можете послать сообщение по электронной почте. Чтобы быть занесенным в список рассылки или получить каталог изданий, напишите письмо по адресу:

info@oreilly.com

Чтобы задать технические вопросы или дать комментарии к книге, пишите по адресу:

bookquestions@oreilly.com

У этой книги есть веб-сайт, где вы можете найти примеры программ и список опечаток (найденные ошибки и исправления доступны для просмотра). Адрес этой страницы:

http://www.oreilly.com/catalog/oraclenut

Дополнительная информация об этой и других книгах находится на веб-сайте O'Reilly:

http://www.oreilly.com

Благодарности

Как и следовало ожидать, эта книга появилась на свет благодаря помощи огромного количества людей. Мы очень благодарны всем им.

Во-первых, большое спасибо тем, чьи книги были исходным материалом для построения глав этой книги: Джонатан Генник (Jonathan Gennick), Стивен Фейерштейн (Steven Feuerstein), Билл Прибыл (Bill Pribyl), Чип Дэйвс (Chip Dawes), Брайан Лески (Brian Laskey), Дон Бэйлс (Don Bales), Дарл Кун (Darl Kuhn) и Скотт Шульце (Scott Schulze). Отдельную благодарность хотелось бы высказать Стивену Фейерштейну, нашему другу и герою; Чипу Дэйвсу, который вовремя предоставил нам массу точных данных; и Дону Бэйлсу, чьи терпение и мягкая настойчивость очень помогли в создании разделов, посвященных Java.

Мы также очень признательны нашим рецензентам: Джонатану Геннику (Jonathan Gennick), Санжею Мишра (Sanjay Mishra), Дарлу Куну (Darl Kuhn) и Алану Бьюли (Alan Beaulieu). Они всесторонне и досконально изучили книгу, согласившись при этом работать в бешеном темпе. Берем назад все проклятья, которые мы тихо посылали в их адрес в последние дни подготовки, пытаясь исправить все ошибки, найденные ими, и внести все предложенные ими изменения.

Кроме того, особая благодарность нашему редактору, Деби Рассел (Debby Russell), которая, как всегда, выступала нашим советчиком и безжалостным судебным исполнителем в одном лице; без ее усилий эта книга никогда бы не была опубликована. Спасибо всей выпускающей команде O'Reilly за то, что они превратили эту кучу страниц, синтаксических диаграмм и таблиц в замечательно оформленное единое целое.

Все ошибки и опечатки, которые остались в книге, несмотря на всеобщую помощь, остаются целиком и полностью на совести авторов.

От Рика

Создание книги – это тяжелая и утомительная работа. Чтобы дойти до конца, вам необходима поддержка всех тех многочисленных людей, о которых уже сказали выше. Но, что еще важнее, вам необходима помощь ваших близких. Для меня самые близ-

кие – это ЛуЭнн (LuAnn), Элеанора (Elinor) и Жозефина (Josephine) Гринвальд (Greenwald). ЛуЭнн подарила мне жизнь, полную счастья. Элли и Джози еще не могут даже написать слово Oracle (и не понимают, почему папочка не может поиграть с ними подольше), но в сущности, все, что я делаю, я делаю для них.

На всем протяжении этой большой работы я трудился с полной отдачей. Этот проект помог мне осознать и оценить ту трудовую этику, без которой я себя не мыслю. За это я благодарю моего отца, скончавшегося, когда я работал над этой книгой. Спасибо, папа.

От Дейва

Когда мне впервые пришла в голову мысль о создании справочника по Oracle для серии «in a Nutshell», я обсудил это кое с кем и в волнении отправил заявку Деби Рассел, редактору моих книг, уже вышедших в издательстве O'Reilly. К сожалению, оказалось, что Рик Гринуолд уже представил на рассмотрение макет такой же книги. Но мое разочарование было недолгим, поскольку Рик пригласил меня быть его соавтором. После всех беспокойств и огорчений, которых я причинил Рику в связи с соблюдением сроков, форматированием, содержанием и всем остальным, за что отвечает главный автор, он, может быть, уже пожалел о своем решении! И я хотел бы воспользоваться возможностью и поблагодарить Рика за то, что он включил меня в этот проект. Работы было очень много, и я многому научился. Спасибо, Рик! Я постараюсь компенсировать хотя бы некоторые из этих бессонных ночей!

Мою работу с Oracle поддерживали и поощряли многие друзья и знакомые, а именно Джон Бересневич (John Beresniewicz), Баф Эмсли (Buff Emslie), Стивен Фернстайн, Джонатан Генник, Стив Хейзелдайн (Steve Hazeldine), Кен Якобс (Ken Jacobs), Брайан Лески, Рич Ниемик (Rich Niemiec), Мэтт Рейган (Matt Reagan) и Марлен Терьо (Marlene Theriault). Особая благодарность моим коллегам из Rhodia: Клоду Коэну (Claude Cohen), Деб Ирвин (Deb Irwin), Дейву Флуду (Dave Flood), Рафаэлю Хевиа (Raphael Hevia), Хоакину Лусеро (Joaquin Lucero), Полю Марсу (Paul Mars), Брайану Мак-Мэхону (Brian McMahon), Бин Пэну (Bin Pan) и Кристиану Тайбергену (Christian Tiberghien). Конечно, я упомянул не всех, но те, кто помогал мне, знают, что они это делали.

Наконец, я хотел бы еще раз поблагодарить мою семью за то, что они мирились с тем, что я забросил их ради поисков, сочинительства, проверок и редактирования.

Основы

Первая часть содержит базовые сведения о СУБД Oracle, которые не зависят от используемых вами языка и инструментов.

Глава 1 «Архитектура и комплект поставки» предлагает обзор архитектуры и основных компонентов СУБД Oracle и рассказывает о различных решениях Oracle.

Глава 2 «Конфигурирование» описывает параметры инициализации (параметры в *INIT.ORA* и/или *SPFILE*), отвечающие за настройку вашей базы данных Oracle.

Глава 3 «Конкурентный доступ» рассказывает о принятой в Oracle многоверсионной модели согласованности по чтению (Multiversion Read Consistency – MVRC) и обсуждает транзакции, блокировки и другие принципы конкурентного доступа к данным.

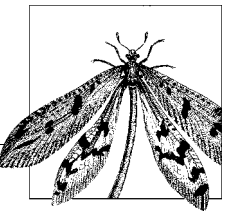
Глава 4 «Безопасность» кратко рассказывает об аутентификации пользователей, профилях, привилегиях, ролях и аудите, а также приводит синтаксис команд управления безопасностью СУБД Oracle.

Глава 5 «Работа в сети» описывает основы сетевых возможностей Oracle и приводит синтаксис необходимых конфигурационных файлов, а именно *TNSNAMES.ORA*, *SQLNET.ORA*, *LISTENER.ORA*, *LDAP.ORA*, *NAMES.ORA* и *CMAN.ORA*.

Глава 6 «Словарь данных» описывает представления словаря данных Oracle, которые хранят информацию об объектах и пользователях СУБД Oracle; в ней рассмотрены как статические представления, так и динамические представления производительности.

4

Безопасность



Oracle предлагает большой набор возможностей, позволяющих исключить несанкционированный доступ к базе данных и помогающих защитить данные от просмотра и изменения неавторизованными пользователями. Эта глава посвящена основным концепциям Oracle, связанным с безопасностью, таким как аутентификация, профили, привилегии, роли и аудит и описывает синтаксис команд управления безопасностью базы данных.

Кроме того, здесь кратко обсуждаются и некоторые из более развитых возможностей обеспечения безопасности в Oracle. Подробное описание этих специализированных и/или поставляемых отдельно компонентов выходит за рамки данной книги. Если ваша организация приобрела компоненты Advanced Security или Label Security, информацию о них можно почерпнуть из документации Oracle.

Аутентификация

Аутентификацией называется процесс распознавания авторизованных пользователей. По существу, процедура аутентификации позволяет системе убедиться, что пользователь действительно является тем, за кого себя выдает. В основе безопасности Oracle лежит концепция индивидуальной авторизации пользователей.

Системные пользователи

При установке Oracle всегда создаются два пользователя базы данных:

SYS

Схема SYS содержит базовые таблицы и представления словаря данных. Ни при каких обстоятельствах не следует их изменять. Пользователь SYS получает роль DBA. (Роли обсуждаются в соответствующем разделе далее в этой главе.) По умолчанию пользователю SYS назначается пароль CHANGE_ON_INSTALL.

SYSTEM

Пользователь SYSTEM нужен для создания дополнительных таблиц и представлений, содержащих административную информацию. Этот пользователь также получает роль DBA. По умолчанию ему назначается пароль MANAGER.

Для ограничения доступа к обширным возможностям этих пользователей можно при создании базы данных Oracle командой CREATE DATABASE применять инструкции USER SYS IDENTIFIED BY *пароль* и USER SYSTEM IDENTIFIED BY *пароль*.

Создание пользователей

Новые пользователи создаются командой CREATE USER. Свойства существующих пользователей можно изменить командой ALTER USER.

CREATE USER

```
CREATE USER имя_пользователя
 IDENTIFIED {BY пароль | EXTERNALLY | GLOBALLY AS 'внешнее_имя'}
 [DEFAULT TABLESPACE имя_табличного_пространства]
 [TEMPORARY TABLESPACE имя_табличного_пространства]
 [QUOTA {целое_число (K | M) | UNLIMITED} ON имя_табличного_пространства]
  [QUOTA {целое_число (K | M) | UNLIMITED} ON имя_табличного_пространства …]
 [PROFILE имя_профиля]
 [PASSWORD EXPIRE]
 [ACCOUNT LOCK | UNLOCK]
```

Создает пользователя и определяет его основные характеристики.

Ключевые слова

IDENTIFIED BY

Определяет способ аутентификации пользователя. Имеются три способа аутентификации:

PASSWORD

Пользователь идентифицируется с помощью хранимого локально пароля. Пароль должен состоять из однобайтовых символов, принадлежащих набору символов базы данных.

EXTERNALLY

Пользователь идентифицируется внешней службой, в частности, операционной системой. Если пользователь должен получать доступ согласно его учетной записи в операционной системе, его имя должно начинаться значением параметра OS_AUTHENT_PREFIX.

GLOBALLY AS 'внешнее_имя'

Пользователь идентифицируется службой каталогов предприятия. Значение *внешнее_имя* может содержать характерное имя (Distinguished Name), имеющееся в каталоге или пустую строку, означающую, что каталог отобразит пользователя на соответствующую схему базы данных.

DEFAULT TABLESPACE

Указывает табличное пространство, в которое по умолчанию помещаются объекты, создаваемые пользователем. По умолчанию это табличное пространство SYSTEM.

TEMPORARY TABLESPACE

Указывает табличное пространство, отведенное для хранения временных сегментов пользователя. По умолчанию это табличное пространство SYSTEM.

QUOTA

Указывает размер области, доступной пользователю в указанном табличном пространстве. Можно указывать несколько инструкций QUOTA для нескольких табличных пространств. Допускается указание в килобайтах (K) или в мегабайтах (M). Значение UNLIMITED снимает ограничения по расходованию пространства пользователем.

PROFILE

Указывает профиль, назначенный пользователю. Подробности изложены ниже в разделе «Профили».

PASSWORD EXPIRE

Указывает на то, что пользователю или администратору БД необходимо изменить пароль, прежде чем пользователь сможет получить доступ к базе данных.

ACCOUNT LOCK | UNLOCK

Разрешает и запрещает доступ для данной учетной записи.

ALTER USER

```
ALTER USER имя_пользователя
 [IDENTIFIED {BY пароль [REPLACE старый_пароль]
  EXTERNALLY | GLOBALLY AS 'внешнее_имя'}]
 [DEFAULT TABLESPACE имя_табличного_пространства]
 [TEMPORARY TABLESPACE имя_табличного_пространства]
 [QUOTA {целое_число [K | M] | UNLIMITED} ON имя_табличного_пространства]
  [QUOTA {целое_число [K | M] | UNLIMITED} ON имя_табличного_пространства]
 [PROFILE имя_профиля]
 [DEFAULT ROLE {[имя_роли[,имя_роли . . .] |
  ALL {EXCEPT [имя_роли[,имя_роли . . .]} | NONE
 [PASSWORD EXPIRE]
 [ACCOUNT LOCK | UNLOCK]
 [имя_пользователя [,имя_пользователя . . .] инструкция_прокси-сервера]
```

Изменяет характеристики пользователя.

Ключевые слова

Большинство ключевых слов в команде ALTER USER имеют то же значение, что и в команде CREATE USER. Следующие ключевые слова применяются только в команде ALTER USER:

REPLACE старый_пароль

Если включена функция проверки сложности пароля, то при изменении пароля командой ALTER USER необходимо указывать его старое значение.

DEFAULT ROLE

Механизм ролей позволяет управлять группами привилегий для групп пользователей. Можно выдать пользователю несколько ролей, все роли (ALL), все кроме перечисленных (ALL EXCEPT) или не выдать ни одной. Более подробно роли описаны ниже в соответствующем разделе.

инструкция_прокси-сервера

Инструкция может относиться к нескольким именам пользователей. Такая возможность появилась в Oracle8*i*, где пользователь может быть идентифицирован прокси-сервером, который и передает пароль серверу БД для повторной аутентификации. В Oracle9*i* информация о личности пользователя в виде характерного имени (Distinguished Name) или полного сертификата X.509 может быть передана серверу БД для идентификации без повторной аутентификации.

Инструкция прокси-сервера имеет такой синтаксис:

```
{GRANT | REVOKE} CONNECT THROUGH прокси-сервер
 [WITH {ROLE [имя_роли[,имя_роли. . .]] |
  ALL [EXCEPT] [имя_роли [,имя_роли. . .]] |
```

```
  NO ROLES}]
 AUTHENTICATED USING {PASSWORD | DISTINGUISHED NAME |
  CERTIFICATE [TYPE имя_типа][VERSION 'имя_версии']}
```

GRANT | REVOKE

Разрешает или запрещает соединение через прокси.

CONNECT THROUGH прокси-сервер

Указывает прокси-сервер, через который устанавливается соединение с Oracle. Подробная информация о прокси-серверах содержится в разделе «Другие возможности обеспечения безопасности» в конце главы.

WITH ROLE

Назначает роль прокси-пользователю. Синтаксис аналогичен синтаксису ключевого слова DEFAULT ROLE.

AUTHENTICATED USING

Указывает, будет ли аутентификация прокси-сервера производиться источником, отличным от прокси-сервера. DISTINGUISHED NAME и CERTIFICATE указывают, что прокси-сервер действует от имени глобального пользователя базы данных.

Профили

Для того чтобы ограничить доступ пользователя к ресурсам или указать условие обработки паролей пользователя, можно сопоставить ему *профиль* (*profile*). Ограничив объем вычислительных ресурсов, доступных пользователю, вы предотвратите их перерасход и нанесение ущерба работе других пользователей. (Печально известен так называемый *отказ в обслуживании* (*denial of service*)). Налагая ограничения на администрирование паролей, вы способствуете защите процесса аутентификации в вашей БД Oracle.

Для того чтобы использовать профили, следует разрешить динамические ограничения ресурсов при помощи параметра инициализации RESOURCE_LIMIT или же команды ALTER SYSTEM SET. Определив профиль командой CREATE PROFILE, вы можете назначить его пользователю посредством команды CREATE USER или ALTER USER.

CREATE PROFILE

```
CREATE PROFILE имя_профиля LIMIT {параметр_ресурса | параметр_пароля}
```

Позволяет создать профиль и назначить для этого профиля различные типы ограничений на расходование ресурсов. Для роли может быть указано несколько параметров.

Ключевые слова для всех параметров

Приведенные ниже значения могут быть заданы как в параметрах ресурсов, так и в параметрах пароля, если они не были ранее заданы в описаниях параметров.

UNLIMITED

Указывает, что для данного параметра нет ограничений.

DEFAULT

Указывает, что параметр принимает значение, заданное для профиля DEFAULT. Изначально все значения профиля DEFAULT устанавливаются в UNLIMITED.

Значения для профиля DEFAULT можно изменить при помощи команды ALTER PROFILE.

параметр_ресурса | *параметр_пароля*

Значения параметров ресурсов задаются целыми числами. Значение параметра пароля задается выражением.

Ключевые слова для параметров ресурсов

За исключением специально описанных случаев, если пользователь пытается выполнить операцию, выходящую за пределы установленных ограничений, сервер Oracle прерывает операцию, откатывает текущую команду и оставляет транзакцию нетронутой.

SESSIONS_PER_USER

Ограничивает количество одновременных сеансов пользователя.

CPU_PER_SESSION

Ограничивает время процессора для пользовательского сеанса (в сотых долях секунды).

CPU_PER_CALL

Ограничивает время процессора для отдельного пользовательского вызова (в сотых долях секунды).

CONNECT_TIME

Ограничивает общую фактическую продолжительность сеанса (в минутах). Если пользователь превышает значение этого параметра, сервер Oracle откатывает текущую транзакцию и завершает сеанс. Следующий вызов, сделанный пользователем, возвращает ошибку.

IDLE_TIME

Ограничивает время непрерывного ожидания пользователя (в минутах). Ограничение времени ожидания не применяется для длительных запросов и других подобных операций. Если пользователь превышает значение этого параметра, сервер Oracle откатывает текущую транзакцию и завершает сеанс. Следующий вызов, сделанный пользователем, возвращает ошибку.

LOGICAL_READS_PER_SESSION

Ограничивает количество логических блоков данных, считываемых в пользовательском сеансе как из памяти, так и с диска.

LOGICAL_READS_PER_CALL

Ограничивает количество логических блоков данных, считываемых в каждом пользовательском вызове как из памяти, так и с диска.

COMPOSITE_LIMIT

Ограничивает общую *стоимость ресурсов* (*resource cost*) сеанса (в сервисных единицах). Oracle вычисляет сервисные единицы как взвешенную сумму следующих параметров инициализации: CPU_PER_SESSION, CONNECT_TIME, LOGICAL_READS_PER_SESSION и PRIVATE_SGA. Вес каждого из ресурсов можно изменить при помощи команды ALTER RESOURCE COST.

PRIVATE_SGA (integer (K | M)| UNLIMITED | DEFAULT)

Ограничивает объем закрытого пространства, которое пользовательский сеанс может выделить из разделяемого пула SGA (в килобайтах (K) или мегабайтах (M)).

Ключевые слова для параметров пароля

FAILED_LOGIN_ATTEMPTS

Ограничивает количество неудачных попыток регистрации пользователя, предшествующих блокировке его учетной записи.

PASSWORD_LIFE_TIME

Устанавливает ограничение максимального срока действия одного пароля (в днях) для пользователя. По истечении этого срока пароль теряет силу.

PASSWORD_REUSE_TIME

Указывает, сколько дней должно пройти, прежде чем пароль можно будет задать повторно. Если для параметра задано целочисленное значение, то необходимо установить PASSWORD_REUSE_MAX в UNLIMITED.

PASSWORD_REUSE_MAX

Указывает, сколько раз необходимо изменить пароль, прежде чем будет разрешено задать его повторно. Если для параметра задано целочисленное значение, то необходимо установить PASSWORD_REUSE_TIME в UNLIMITED.

PASSWORD_LOCK_TIME

Указывает количество дней, на которое будет заблокирована учетная запись пользователя в случае превышения количества попыток неудачной регистрации.

PASSWORD_GRACE_TIME

Указывает, за какое количество дней до истечения срока действия пароля выдается предупреждение.

PASSWORD_VERIFY_FUNCTION функция | NULL | DEFAULT

Разрешает применение функции PL/SQL для проверки сложности пароля.

ALTER PROFILE

```
ALTER PROFILE имя_профиля LIMIT {параметр_ресурса | параметр_пароля}
```

Изменяет ограничения на расходование ресурсов или ограничения пароля для существующего профиля.

Ключевые слова

В команде ALTER PROFILE применяются те же ключевые слова и значения, что и в CREATE PROFILE.

DROP PROFILE

```
DROP PROFILE имя_профиля (CASCADE)
```

Удаляет существующий профиль.

Ключевые слова

CASCADE

Указывает, что назначение профиля для всех активных пользователей должно быть отменено, а их профили необходимо заменить на DEFAULT. Данную инструкцию следует применять при удалении профиля текущего активного пользователя.

Привилегии

Привилегии – это права, назначаемые отдельным пользователям или ролям. Привилегии делятся на два основных вида:

Системные привилегии

Дают пользователю или роли возможность выполнять определенные системные операции.

Объектные привилегии

Дают пользователю или роли права доступа к отдельным объектам схемы.

Системные привилегии относятся к экземпляру Oracle в целом, например есть привилегия для всех объектов одного типа (скажем, для всех таблиц). Объектные же привилегии связаны с конкретным объектом схемы внутри базы данных Oracle (например, с конкретной таблицей).

Системные привилегии

В этом разделе изложена общая информация обо всех системных привилегиях Oracle. Некоторые разновидности системных привилегий могут применяться к различным типам привилегий:

ANY

Дает привилегию на выполнение операции над объектами любой схемы. В отсутствие такого ключевого слова привилегия выдается только на объекты в рамках схемы пользователя. По умолчанию ключевое слово ANY дает пользователю привилегию на все объекты всех схем, включая SYS. Для того чтобы запретить привилегии ANY на доступ к схеме SYS, можно установить параметр инициализации O7_DICTIONARY_ACCESSIBILITY в FALSE.

ALTER

Дает привилегию на изменение объекта некоторого типа.

CREATE

Дает привилегию на создание объекта данного типа.

DROP

Дает привилегию на удаление объекта данного типа.

EXECUTE

Дает привилегию на исполнение объекта данного типа или обращение к нему.

SELECT ANY

Дает привилегию на доступ к объектам. Пользователи всегда имеют возможность доступа к объектам своей собственной схемы, поэтому данная разновидность привилегий применяется только с ключевым словом ANY.

Каждая из представленных разновидностей привилегий может применяться со многими типами системных привилегий, описанных далее.

В описании каждой привилегии указаны привилегии двух категорий: общие (перечисленные в предыдущем разделе, применяемые для различных типов привилегий) и уникальные (присущие только данному конкретному типу привилегий).

AUDIT

Разрешает функции аудита.

Уникальные привилегии

AUDIT SYSTEM Дает привилегию на выдачу команд AUDIT в SQL.

Общие привилегии ANY.

CLUSTER

Предоставляет возможность работы с кластерами.

Уникальные привилегии Нет.

Общие привилегии CREATE [ANY], ALTER ANY, DROP ANY.

CONTEXT

Предоставляет возможность работы с контекстами. Появилась в Oracle8*i*.

Уникальные привилегии Нет.

Общие привилегии CREATE ANY, DROP ANY.

DATABASE

Предоставляет возможность выполнения команды ALTER DATABASE.

Уникальные привилегии Нет.

Общие привилегии ALTER.

DATABASE LINKS

Предоставляет возможность работы со связями БД (*database links*).

Уникальные привилегии

CREATE PUBLIC Дает привилегию на создание открытых связей БД.

DROP PUBLIC Дает привилегию на удаление открытых связей БД.

Общие привилегии CREATE.

DEBUG

Предоставляет возможность работы с отладчиком. Появилась в Oracle9*i*.

Уникальные привилегии

DEBUG CONNECT SESSION

Дает привилегию на подключение текущего сеанса к отладчику, который использует протокол Java Debug Wire Protocol.

DEBUG ANY PROCEDURE

Дает привилегию на отладку любого PL/SQL- и Java-кода для любого объекта БД, а также отображение всех команд SQL, выполняемых приложением.

Общие привилегии Нет.

DIMENSION

Предоставляет возможность работы с измерениями. Появилась в Oracle8*i*.

Уникальные привилегии Нет.

Общие привилегии CREATE [ANY], ALTER ANY, DROP ANY.

DIRECTORY

Предоставляет возможность работы с каталогами.

Уникальные привилегии Нет.

Общие привилегии CREATE ANY, DROP ANY.

INDEX

Предоставляет возможность работы с индексами.

Уникальные привилегии Обратитесь к информации о привилегии [GLOBAL] QUERY REWRITE в разделе «Различные привилегии» далее в этой главе.

Общие привилегии CREATE ANY, ALTER ANY, DROP ANY.

INDEXTYPE

Предоставляет возможность работы с объектами типа INDEXTYPE, созданными пользователем. Появилась в Oracle8*i*.

Уникальные привилегии Нет.

Общие привилегии CREATE [ANY], ALTER ANY (появилась в Oracle9*i*), DROP ANY, EXECUTE ANY.

LIBRARY

Предоставляет возможность работы с библиотеками.

Уникальные привилегии Нет.

Общие привилегии CREATE [ANY], DROP ANY.

MATERIALIZED VIEW

Предоставляет возможность работы с *материализованными представлениями* (*materialized views*). Привилегии MATERIALIZED VIEW в версиях, предшествующих Oracle8*i*, назывались SNAPSHOT.

Уникальные привилегии

ON COMMIT REFRESH

Дает привилегию на создание материализованного представления с обновлением при выполнении COMMIT. Появилась в Oracle8*i*.

См. также информацию о [GLOBAL] QUERY REWRITE и FLASHBACK ANY TABLE в разделе «Различные привилегии».

Общие привилегии CREATE [ANY], ALTER ANY, DROP ANY.

OPERATOR

Предоставляет возможность работы с определяемыми пользователем операторами. Появилась в Oracle8*i*.

Уникальные привилегии Нет.

Общие привилегии CREATE [ANY], DROP, EXECUTE.

OUTLINE

Предоставляет возможность работы с хранимыми планами выполнения (*stored outlines*). Появилась в Oracle8*i*.

Уникальные привилегии

SELECT ANY

Несмотря на общее ключевое слово для объектов, в данном случае речь идет о предоставлении привилегии на создание закрытого плана выполнения из открытого. Появилась в Oracle9*i*.

Общие привилегии CREATE ANY, ALTER ANY, DROP ANY.

PROCEDURE

Предоставляет возможность работы с процедурами.

Уникальные привилегии Нет.

Общие привилегии CREATE [ANY], ALTER ANY, DROP ANY, EXECUTE ANY.

PROFILE

Предоставляет возможность работы с профилями.

Уникальные привилегии Нет.

Общие привилегии CREATE, ALTER, DROP.

RESOURCE COST

Предоставляет возможность присваивания стоимостей ресурсам.

Уникальные привилегии Нет.

Общие привилегии ALTER.

ROLE

Предоставляет возможность работы с ролями.

Уникальные привилегии

GRANT ANY Дает привилегию на предоставление любых ролей в БД.

Общие привилегии CREATE, ALTER ANY, DROP ANY.

ROLLBACK SEGMENT

Предоставляет возможность работы с сегментами отката.

Уникальные привилегии Нет.

Общие привилегии CREATE, ALTER, DROP.

SEQUENCE

Предоставляет возможность работы с последовательностями.

Уникальные привилегии Нет.

Общие привилегии CREATE [ANY], ALTER ANY, DROP ANY, SELECT ANY.

SESSION

Предоставляет возможность работы с сеансами.

Уникальные привилегии

ALTER RESOURCE COST

Дает привилегию на задание стоимостей ресурсов сеанса.

RESTRICTED SESSION

Дает привилегию на вход в систему после того, как экземпляр Oracle запущен командой STARTUP RESTRICT.

Общие привилегии CREATE, ALTER.

SNAPSHOT

В версии Oracle9*i* ключевое слово *SNAPSHOT заменено* на MATERIALIZED VIEW. В версии Oracle8*i* ключевые слова SNAPSHOT и MATERIALIZED VIEW были взаимозаменяемыми.

SYNONYM

Предоставляет возможность работы с синонимами.

Уникальные привилегии Нет.

Общие привилегии CREATE [ANY] [PUBLIC], DROP ANY, DROP PUBLIC.

SYSTEM

Предоставляет возможность изменения параметров системы.

Уникальные привилегии Нет.

Общие привилегии ALTER.

TABLE

Предоставляет возможность работы с таблицами.

Уникальные привилегии

BACKUP ANY

Дает привилегию на использование утилиты Export для объектов в схемах других пользователей.

COMMENT ANY

Дает привилегию на комментирование любых таблиц, столбцов и представлений в любой схеме.

INSERT ANY

Дает привилегию на вставку строк в таблицы в схемах других пользователей.

LOCK ANY

Дает привилегию на блокировку таблиц и представлений в схемах других пользователей.

FLASHBACK ANY

Дает возможность выдавать ретроспективные запросы SQL (*flashback query*) для любой таблицы или материализованного представления в схемах других пользователей. Вы можете, как и ранее, использовать встроенные процедуры пакета DBMS_FLASHBACK, не имея такой привилегии. Появилась в Oracle9*i*.

UPDATE ANY

Дает привилегию на обновление строк таблиц и представлений в схемах других пользователей.

Дополнительная информация по FLASHBACK ANY TABLE приведена в разделе «Различные привилегии».

Общие привилегии

CREATE [ANY] (CREATE поддерживается только в Oracle8 и более ранних версиях), ALTER ANY, DELETE ANY, DROP ANY, SELECT ANY.

TABLESPACES

Предоставляет возможность работы с табличными пространствами

Уникальные привилегии

MANAGE

Дает привилегию на перевод табличных пространств в автономный и оперативный режимы, а также на запуск и завершение резервного копирования табличных пространств.

UNLIMITED TABLESPACE

Дает привилегию на перекрытие любых назначенных квот для конкретных табличных пространств. Если привилегия отзывается, пользователь может выделить дополнительное табличное пространство только в рамках существующих квот. Привилегия не может быть выдана роли (то есть назначается только пользователям).

Общие привилегии CREATE, ALTER, DROP.

TRIGGER

Предоставляет возможность работы с триггерами.

Уникальные привилегии

ADMINISTER DATABASE

Дает привилегию на создание триггера для базы данных. Для получения данной привилегии пользователь или роль должен обладать привилегией CREATE [ANY] TRIGGER. Появилась в Oracle8*i*.

Общие привилегии CREATE [ANY], ALTER ANY, DROP.

TYPES

Предоставляет возможность работы с определяемыми пользователем типами.

Уникальные привилегии

UNDER ANY

Дает привилегию на создание подтипов для всех типов, которые не определены как терминальные (*final*). Появилась в Oracle9*i*.

Общие привилегии CREATE [ANY], ALTER ANY, DROP ANY, EXECUTE ANY.

USER

Предоставляет возможность работы с пользователями базы данных.

Уникальные привилегии

BECOME

Дает возможность стать другим пользователем, что необходимо для выполнения полного импорта базы данных.

Общие привилегии CREATE, ALTER, DROP.

VIEWS

Предоставляет возможность работы с представлениями.

Уникальные привилегии

UNDER ANY

Дает привилегию на создание дочерних представлений для любого объекта представления. Появилась в Oracle9*i*.

Обратитесь также к информации о FLASHBACK ANY TABLE в разделе «Различные привилегии».

Общие привилегии CREATE [ANY], DROP.

Различные привилегии

В этом разделе собраны привилегии, не попадающие ни в одну из вышеуказанных категорий.

ANALYZE ANY

Предоставляет привилегию на проведение анализа любой таблицы, кластера или индекса в любой схеме.

EXEMPT ANY

Предоставляет привилегию на игнорирование политики безопасности, проводимой приложением. Появилась в Oracle9*i*.

FLASHBACK ANY TABLE

Предоставляет привилегию на выдачу ретроспективного запроса SQL (*flashback query*) для любой таблицы, представления или материализованного представления в любой схеме. Вы можете, как и ранее, использовать встроенные процедуры пакета DBMS_FLASHBACK, не имея такой привилегии. Появилась в Oracle9*i*.

FORCE TRANSACTION

Предоставляет привилегию на принудительную фиксацию или откат любой из распределенных транзакций пользователя в локальной базе данных.

FORCE ANY TRANSACTION

Предоставляет привилегию на принудительную фиксацию или откат любой распределенной транзакции в локальной базе данных или на вызов сбоя распределенной транзакции.

GRANT ANY PRIVILEGE

Предоставляет привилегию на выдачу любых системных привилегий.

GRANT ANY OBJECT PRIVILEGE

Предоставляет привилегию на выдачу любых привилегий доступа к объектам. Появилась в Oracle9*i*.

[GLOBAL] QUERY REWRITE

Предоставляет привилегию разрешения перезаписи запроса с использованием материализованного представления или создания индекса на основе функции. Ключевое слово GLOBAL действует как ANY. Появилась в Oracle8*i*.

RESUMABLE

Предоставляет привилегию разрешения возобновляемого выделения пространства. Появилась в Oracle9*i*.

SELECT ANY DICTIONARY

Предоставляет привилегию на запрос любого объекта словаря данных в схеме SYS, что дает пользователю избирательную возможность перекрытия значения параметра инициализации O7_DICTIONARY_ACCESSIBILITY. Появилась в Oracle9*i*.

Особые системные привилегии

Описанные в разделе системные привилегии предназначены для предоставления пользователю возможности выполнения всего набора операций. Это особые привилегии, поскольку одна привилегия предоставляет пользователю набор базовых полномочий.

SYSDBA

Дает пользователю все права, необходимые для запуска и остановки базы данных Oracle. Включает в себя привилегию RESTRICTED SESSION, а также следующие полномочия:

ALTER DATABASE

CREATE DATABASE

ARCHIVELOG и RECOVERY

CREATE SPFILE (появилась в Oracle9*i*)

SYSOPER

Предоставляет пользователю чуть более ограниченный набор прав, предназначенный для оператора системы. Включает в себя привилегию RESTRICTED SESSION, а также следующие полномочия:

ALTER DATABASE OPEN | MOUNT | BACKUP

ARCHIVELOG и RECOVERY

CREATE SPFILE (появилась в Oracle9*i*)

Привилегии доступа к объектам схемы

Существует несколько разновидностей привилегий доступа к объектам схемы. Они могут применяться к различным типам объектов схемы, как описано в последующих разделах.

Разновидности привилегий доступа к объектам схемы

ALTER

Изменяет определение объекта.

DEBUG

Обращается к PL/SQL-коду или информации о командах SQL, которые обращаются к объекту напрямую через отладчик. Появилась в Oracle9*i*.

DELETE

Удаляет строки из объекта.

EXECUTE

Компилирует или исполняет процедуру или функцию объекта, или же обращается к программному объекту, объявленному в объекте.

FLASHBACK

Выполняет ретроспективный запрос к объекту. Появилась в Oracle9*i*.

INSERT

Добавляет в объект новые строки.

REFERENCES

Создает *ограничение* (*constraint*), ссылающееся на объект.

SELECT

Запрашивает объект.

UNDER

Создает дочерний объект ниже уровня объекта. Появилась в Oracle9*i*.

UPDATE

Изменяет существующие данные объекта.

Объекты схемы и их привилегии

В разделе приведены все типы объектов схемы, при этом для каждого из них указаны общие и уникальные разновидности привилегий.

Каталоги

Предоставляет привилегии на выполнение операций над каталогами.

Уникальные привилегии

READ

Читать файлы каталога.

WRITE

Писать в файлы каталога, за исключением *BFILE*. Применяется к внешним таблицам каталога. Появилась в Oracle9*i*.

Общие привилегии Нет.

Внешние таблицы

Предоставляет привилегии на выполнение операций над внешними таблицами.

Уникальные привилегии Нет.

Общие привилегии ALTER, SELECT.

Indextypes

Предоставляет привилегии на выполнение операций над объектами INDEXTYPE (пользовательские индексы, которые появились в Oracle8*i*).

Уникальные привилегии Нет.

Общие привилегии EXECUTE.

Библиотеки

Предоставляет привилегии на выполнение операций над библиотеками.

Уникальные привилегии Нет.

Общие привилегии EXECUTE.

Материализованные представления

Предоставляет привилегии на выполнение операций над материализованными представлениями. Материализованные представления – это предварительно агрегированные сводные данные, участвующие в операциях бизнес-интеллекта. Материализованные представления появились в Oracle8*i*. В Oracle8*i* привилегии могли предоставляться как для материализованных представлений, так и для *моментальных копий данных* (*snapshots*). В Oracle8 и более ранних версиях привилегии предоставлялись только для моментальных копий данных.

Уникальные привилегии Нет.

Общие привилегии

DELETE, FLASHBACK, INSERT, SELECT, UPDATE. Привилегии DELETE, INSERT и UPDATE могут быть предоставлены только для обновляемых материализованных представлений.

Операторы

Предоставляет привилегии на выполнение операций над операторами, т. е. пользовательскими операторами для определенных видов сравнений. Операторы появились в Oracle8*i*.

Уникальные привилегии Нет.

Общие привилегии EXECUTE.

Процедуры, функции и пакеты

Предоставляет привилегии на выполнение операций над тремя типами программных единиц: процедурами, функциями и пакетами.

Уникальные привилегии Нет.

Общие привилегии DEBUG, EXECUTE.

Последовательности

Предоставляет привилегии на выполнение операций над последовательностями.

Уникальные привилегии Нет.

Общие привилегии ALTER, SELECT.

Таблицы

Предоставляет привилегии на выполнение операций над таблицами.

Уникальные привилегии

INDEX

Создать индекс для таблицы.

ON COMMIT REFRESH

Создать материализованное представление, обновляемое при выполнении операции COMMIT. Появилась в Oracle9*i*.

QUERY REWRITE

Создать материализованное представление для перезаписи запроса в определенную таблицу.

Общие привилегии ALTER, DELETE, DEBUG, FLASHBACK, INSERT, REFERENCES, SELECT, UPDATE.

Пользовательские типы

Предоставляет привилегии на выполнение операций над пользовательскими типами. Пользовательские типы – это уникальные типы данных, создаваемые пользователем. Они появились в Oracle8*i*.

Уникальные привилегии Нет.

Общие привилегии DEBUG, EXECUTE, UNDER.

Представления

Предоставляет привилегии на выполнение операций над представлениями. Для того чтобы выдать привилегию на представление, необходимо обладать данной привилегией с указанием GRANT OPTION для всех таблиц, являющихся основой представления.

Уникальные привилегии Нет.

Общие привилегии DEBUG, DELETE, FLASHBACK, INSERT, REFERENCES, SELECT, UNDER.

Привилегии и пользователи

Для назначения привилегий пользователю или роли применяется команда GRANT. Команда REVOKE позволяет лишить пользователя или роль привилегии.

Общие ключевые слова и инструкции

В разделе собраны ключевые слова и инструкции, которые могут применяться как в команде GRANT, так и в REVOKE:

системная_привилегия

Системная привилегия (см. раздел «Системные привилегии» ранее в этой же главе).

роль

Существующая роль.

ALL PRIVILEGES

Предоставляет или отбирает все системные привилегии, за исключением SELECT ANY DICTIONARY. Для объектов предоставляет все привилегии, имеющиеся для данного объекта, ключевое слово PRIVILEGES является необязательным.

получатель

Один или несколько пользователей, одна или несколько ролей или ключевое слово PUBLIC, которое предоставляет или отбирает привилегии у всех пользователей

базы данных. Если указывается несколько получателей, их следует разделить запятыми.

объектная_привилегия

Привилегия доступа к объектам, описываемая ранее в этой главе.

имя_столбца

Один или несколько столбцов, для которых предоставляется или отбирается привилегия доступа к объектам INSERT, REFERENCES или UPDATE. Если имя столбца не указано, то привилегия *предоставляется* на все столбцы таблицы или представления.

схема.объект

Указывает имя объекта, на который выдается или отбирается привилегия. Если схема не задана, то сервер Oracle считает, что объект находится в собственной схеме пользователя.

DIRECTORY имя_каталога

Указывает имя каталога, на который выдается или отбирается привилегия.

GRANT

Для предоставления системных привилегий или ролей:

```
GRANT {системная_привилегия | роль | ALL PRIVILEGES} TO получатель
   [IDENTIFIED BY пароль] [WITH ADMIN OPTION]
```

Для предоставления привилегий доступа к объектам схемы:

```
GRANT {объектная_привилегия | ALL [PRIVILEGES]}
        [имя_столбца [,имя_столбца . . .]]
   ON {схема.объект | DIRECTORY имя_каталога |
        JAVA (SOURCE | RESOURCE) [схема.]объект}
   TO получатель [WITH GRANT OPTION] [WITH HIERARCHY OPTION]
```

Предоставляет пользователю или роли привилегии или роли. Для того чтобы предоставить привилегию, пользователь должен предварительно получить привилегию или роль с указанием WITH ADMIN OPTION (см. далее раздел «Ключевые слова»). Вы также можете предоставлять привилегии, если обладаете привилегией GRANT ANY PRIVILEGE (для системных привилегий), GRANT ANY ROLE (для ролей), GRANT OPTION (для объектов схемы) или являетесь владельцем объекта.

Системные привилегии и привилегии доступа к объектам схемы не могут быть предоставлены в одной команде GRANT.

Ключевые слова

IDENTIFIED BY пароль

Может применяться для идентификации существующего пользователя по паролю или для создания нового пользователя с указанным паролем. Появилась в Oracle9*i*.

ALL PRIVILEGES

Предоставляет пользователю или роли все привилегии, за исключением SELECT ANY DICTIONARY. Появилась в Oracle9*i*.

WITH ADMIN OPTION

Позволяет пользователю выдавать или отбирать системную привилегию или роль, а также изменять и удалять роль.

WITH GRANT OPTION

Подобно WITH ADMIN OPTION позволяет пользователю или роли выдавать или отбирать привилегию доступа к объектам у других пользователей или ролей.

JAVA SOURCE | RESOURCE

Разрешает доступ к исходным текстам Java или Java-ресурсу. Появилась в Oracle8*i*.

WITH HIERARCHY OPTION

Позволяет получателю получить привилегии на все дочерние объекты указанного объекта схемы. Появилась в Oracle9*i*.

REVOKE

Для изъятия системных привилегий или ролей:

```
REVOKE {системная_привилегия | роль | ALL PRIVILEGES} FROM получатель
```

Для изъятия привилегий доступа к объектам:

```
REVOKE {объектная_привилегия | ALL [PRIVILEGES]}
        [имя_столбца [,имя_столбца . . .]]
    ON {схема.объект | DIRECTORY имя_каталога |
        JAVA [SOURCE | RESOURCE] [схема.]объект}
    FROM получатель [CASCADE CONSTRAINTS] [FORCE]
```

Аннулирует привилегии, ранее выданные пользователю или роли. Эта команда может аннулировать только те привилегии, которые были ранее выданы командой GRANT. Если вы отзываете роль у клиента, который использует ее в текущий момент, то роль остается, но уже не будет доступна клиенту после того, как он перестанет ей пользоваться.

Если несколько обладателей привилегии выдали ее пользователю (или в случае PUBLIC), то для того чтобы привилегия стала недоступна пользователю, она должна быть аннулирована всеми выдавшими.

Ключевые слова

ALL PRIVILEGES

Аннулирует все существующие системные привилегии для пользователя или роли. Появилась в Oracle9*i*.

JAVA SOURCE | RESOURCE

Аннулирует доступ к исходным текстам Java и к Java-ресурсу. Появилась в Oracle8*i*.

CASCADE CONSTRAINTS

Применяется только при отзыве привилегии REFERENCES или привилегий доступа к объектам ALL. Удаляет все ограничения, которые пользователь, лишаемый привилегий, определил для объекта.

FORCE

Применяется при отзыве привилегии доступа к объектам EXECUTE для объектов пользовательских типов, имеющих зависимости от таблиц или типов. Приводит к тому, что все зависимые объекты помечаются как INVALID, запрещает доступ к данным зависимых таблиц, помечает все зависимые *функциональные индексы* (*function-based*) как UNUSABLE.

Роли

Предоставление отдельных привилегий отдельным пользователям может существенно усложнить работу, особенно в корпоративных системах с большим количеством пользователей. Роли предназначены для того, чтобы упростить управление привилегиями.

Привилегии можно выдавать ролям, а затем назначать роли пользователям. Ведение привилегий осуществляется на уровне ролей и затрагивает всех пользователей, которым назначены такие роли. Кроме того, в зависимости от контекста роли могут избирательно разрешаться и запрещаться для пользователей. То есть посредством ролей можно объединять наборы привилегий и предоставлять их как единое целое. Например, у вас может существовать роль ADMIN, наделяющая администратора соответствующими полномочиями.

Роль может выдаваться другой роли. Если вы назначаете пользователю родительскую роль, он по умолчанию получает и все роли, выданные родительской роли.

Пользователю можно назначить несколько ролей. Количество одновременно выдаваемых ролей ограничено параметром инициализации MAX_ENABLED_ROLES. Несколько ролей дают возможность одному пользователю в разные моменты времени применять разные наборы привилегий. Если роли выданы другие роли, то применение родительской роли подразумевает применение всех дочерних.

Команда ALTER USER позволяет задать одну или несколько ролей по умолчанию. Роли, назначенные по умолчанию, действуют, когда пользователь регистрируется в базе данных Oracle.

Системные роли

СУБД Oracle предлагает ряд предопределенных системных ролей:

CONNECT

Включает в себя системные привилегии ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE и CREATE VIEW. Согласно информации корпорации Oracle, эта роль предоставляется для обеспечения совместимости с ранними версиями Oracle и может не поддерживаться в версиях выше Oracle9*i*.

RESOURCE

Включает в себя системные привилегии CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE и CREATE TYPE. Согласно информации корпорации Oracle, эта роль предоставляется для обеспечения совместимости с ранними версиями Oracle и может не поддерживаться в версиях выше Oracle9*i*.

DBA

Включает в себя все системные привилегии с указанием WITH ADMIN OPTION. Согласно информации корпорации Oracle, эта роль предоставляется для обеспечения совместимости с ранними версиями Oracle и может не поддерживаться в версиях выше Oracle9*i*.

CREATE TYPE

Включает в себя привилегии CREATE TYPE, EXECUTE, EXECUTE ANY TYPE, ADMIN OPTION и GRANT OPTION. Роль удалена в версиях выше Oracle8.

EXP_FULL_DATABASE

Предназначена для предоставления всех привилегий, необходимых для выполнения полного и инкрементного экспорта базы данных. Включает в себя привилегии SELECT ANY TABLE, BACKUP ANY TABLE, EXECUTE ANY PROCEDURE, EXECUTE ANY TYPE, ADMINISTER RESOURCE MANAGER, а также привилегии INSERT, DELETE и UPDATE для таблиц SYS.INCVID, SYS.INCFIL и SYS.INCEXP. Кроме того, включает в себя роли EXECUTE_CATALOG_ROLE и SELECT_CATALOG_ROLE.

IMP_FULL_DATABASE

Предназначена для предоставления всех привилегий, необходимых для выполнения полного импорта базы данных. Включает в себя множество системных привилегий, а также роли EXECUTE_CATALOG_ ROLE и SELECT_CATALOG_ROLE.

DELETE_CATALOG_ROLE

Содержит в себе привилегию DELETE для таблицы аудита системы (AUD$).

EXECUTE_CATALOG_ROLE

Включает в себя привилегию EXECUTE для таблицы аудита системы (AUD$) и роль HS_ADMIN_ROLE.

SELECT_CATALOG_ROLE

Включает в себя привилегию SELECT для таблицы аудита системы (AUD$) и роль HS_ADMIN_ROLE.

RECOVERY_CATALOG_OWNER

Предназначена для предоставления всех привилегий, необходимых владельцу каталога восстановления. Включает в себя системные привилегии CREATE SESSION, ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE PROCEDURE, CREATE SEQUENCE, CREATE SYNONYM, CREATE TABLE, CREATE TRIGGER и CREATE VIEW.

HS_ADMIN_ROLE

Предназначена для защиты пакетов и представлений словарей данных гетерогенных сервисов (Heterogeneous Services – HS).

AQ_USER_ROLE

Предоставляет привилегию EXECUTE для встроенных пакетов механизма улучшенной организации очередей (Advanced Queuing): DBMS_AQ и DBMS_AQIN. Устарела в Oracle9*i*.

AQ_ADMINISTRATOR_ROLE

Предназначена для предоставления всех привилегий, необходимых для администрирования механизма улучшенной организации очередей. Включает в себя привилегии ENQUEUE ANY QUEUE, DEQUEUE ANY QUEUE, MANAGE ANY QUEUE, SELECT для таблиц механизма улучшенной организации очередей и привилегию EXECUTE для пакетов механизма улучшенной организации очередей.

SNMPAGENT

Используется Enterprise Manager Intelligent Agent и включает в себя привилегии ANALYZE ANY и SELECT для различных представлений.

Определение ролей

Описанные в последующих разделах команды позволяют создавать, изменять и удалять роли.

Команда ALTER USER позволяет определить одну или несколько ролей по умолчанию. Роли, назначенные по умолчанию, действуют, когда пользователь регистрируется в базе данных Oracle.

CREATE ROLE

```
CREATE ROLE имя_роли {NOT IDENTIFIED | IDENTIFIED
    {EXTERNALLY | GLOBALLY |
    BY пароль |
    USING [схема.]пакет}}
```

Создает роль. Когда пользователь создает роль, она автоматически выдается ему как роль по умолчанию.

Ключевые слова

NOT IDENTIFIED

Указывает, что для роли не требуется пароль.

IDENTIFIED

Определяет, каким способом пользователь будет аутентифицирован, прежде чем ему будет разрешено активировать роль или назначить ее ролью по умолчанию. Возможны следующие варианты:

BY пароль

Локальный пользователь должен предоставить пароль для активирования роли.

USING (схема.)пакет

Проверку пользователя осуществит пакет. Применяется для ролей приложений. Если имя схемы не указано, то считается, что пакет находится в собственной схеме пользователя. Появилась в Oracle9*i*.

EXTERNALLY

Внешний пользователь авторизуется сторонней службой, такой как операционная система.

GLOBALLY

Пользователь авторизуется службой каталогов предприятия.

ALTER ROLE

```
ALTER ROLE имя_роли {NOT IDENTIFIED | IDENTIFIED
     {EXTERNALLY | GLOBALLY |
     BY пароль |
     USING [схема.]пакет}}
```

Изменяет способ аутентификации пользователя роли.

Ключевые слова

Ключевые слова совпадают с ключевыми словами, приведенными для команды CREATE ROLE.

DROP ROLE

```
DROP ROLE имя_роли
```

Удаляет роль из базы данных. Если роль используется в данный момент, то ничего не произойдет, но заново использовать роль пользователь уже не сможет.

SET ROLE

```
SET ROLE {роль [IDENTIFIED BY пароль [,роль [IDENTIFIED BY PASSWORD_ ._ ._ ._ ]] |
    ALL [EXCEPT роль[, роль_ ._ ._ ._ ]]
    NONE}
```

Разрешает пользователю применение одной или нескольких ролей или запрещает применение всех ролей.

Ключевые слова

ALL

Разрешает применение всех ролей, предоставленных пользователю.

EXCEPT

Применяется для исключения некоторых ролей из списка разрешенных при помощи ключевого слова ALL.

NONE

Запрещает применение всех ролей пользователя.

Аудит

Подобно тому, как мониторинг расходования ресурсов способствует решению проблем производительности, аудит применяется как способ отслеживания использования базы данных и предупреждения о возможных проблемах с безопасностью.

Раньше в Oracle был разрешен аудит трех различных типов:

Аудит команд

Аудит команд, направленных базе данных отдельными пользователями или всеми пользователями.

Аудит привилегий

Аудит использования системных привилегий отдельными пользователями или всеми пользователями.

Аудит объектов схемы

Аудит определенного набора команд SQL для конкретного объекта схемы.

Oracle9*i* вводит четвертый тип аудита, который получил название *детальный аудит* (*fine-grained auditing*). О нем мы поговорим в завершающем разделе главы.

Для всех типов аудита Oracle вносит записи в журнал аудита базы данных или таблицу SYS.FGA_LOG$ или же в файл операционной системы (в двоичном формате). Записи журнала аудита содержат различную информацию в зависимости от типа аудита и установленных параметров выполнения аудита.

Аудит системных действий

Вне зависимости от того, включен ли аудит для вашей базы данных, следующие действия всегда формируют записи в журнале аудита операционной системы:

- Запуск экземпляра
- Остановка экземпляра
- Доступ пользователей с привилегиями администратора

Применение аудита

Включать и выключать аудит можно при помощи команд AUDIT и NOAUDIT.

AUDIT

```
AUDIT инструкция_для_команд_sql | инструкция_для_объектов_схемы
   [BY SESSION | ACCESS]
   [WHENEVER [NOT] SUCCESSFUL]
```

Включает аудит для БД Oracle.

Инструкции

инструкция_для_команд_sql

Инструкция применяется для включения аудита команд или системных привилегий и имеет такой формат:

```
{[параметр_команды | ALL][, ...]} |
 {[системная_привилегия | ALL PRIVILEGES] [, ...]}
 BY {прокси-сервер(, прокси-сервер ...,] ON BEHALF OF [{пользователь [,пользователь ...]} | ANY |
 { пользователь[,пользователь ...]}
```

инструкция_для_объектов_схемы

Инструкция применяется для включения аудита объектов схемы и имеет такой формат:

```
{параметр_объекта[, параметр_объекта ...] | ALL }
 ON {[схема.]объект | DIRECTORY имя_каталога | DEFAULT }
```

Ключевые слова

BY SESSION | ACCESS

Определяет, должны ли данные аудита записываться один раз за сеанс или же при каждой попытке определенного типа доступа. Аудит для всех команд и всех привилегий для команд DDL может задаваться только как BY ACCESS.

WHENEVER [NOT] SUCCESSFUL

Указывает, следует ли проверять только успешные или неудавшиеся команды SQL. Единственные неудавшиеся команды, отслеживаемые при помощи ключевого слова NOT, – это команды, которые не удается выполнить, или приводящие к возникновению ошибок из-за недостаточных привилегий или отсутствия объекта, на который приведена ссылка. По умолчанию проверяются все команды вне зависимости от того, выполнились они успешно или же не удались по упомянутым причинам.

BY пользователь

Задает аудит по одному или нескольким именам пользователей.

BY прокси-сервер ON BEHALF OF

Задает аудит действий, выполняемых прокси-сервером от имени пользователя. Появилась в Oracle8*i*.

параметр_команды

Включает аудит отдельных команд SQL. Перечисляются значения ключевого слова (параметры команд) и команды, которые будет отслеживать каждое из значений для указанного типа объекта. В первой части списка приведены команды, которые будут проверяться, если указать ключевое слово ALL.

CLUSTER

CREATE, AUDIT, DROP, TRUNCATE.

CONTEXT

CREATE, DROP. Появилась в Oracle8*i*.

[PUBLIC] DATABASE LINK

CREATE, DROP.

DIMENSION

CREATE, ALTER, DROP. Появилась в Oracle8*i*.

DIRECTORY

CREATE, DROP.

INDEX

CREATE, ALTER, DROP.

NOT EXISTS

Все команды, которые не удается выполнить из-за того, что объект не существует.

PROCEDURE

CREATE FUNCTION, CREATE LIBRARY, CREATE PACKAGE, CREATE PACKAGE BODY, CREATE PROCEDURE, DROP FUNCTION, DROP LIBRARY, DROP PACKAGE, DROP PROCEDURE.

PROFILE

CREATE, ALTER, DROP.

ROLE

CREATE, ALTER, DROP, SET.

ROLLBACK SEGMENT

CREATE, ALTER, DROP.

SEQUENCE

CREATE, DROP.

SESSION

Начало сеанса.

[PUBLIC] SYNONYM

CREATE, DROP.

SYSTEM AUDIT

AUDIT *системные_привилегии_и_роли*; NOAUDIT *системные_привилегии_и_роли*.

SYSTEM GRANT

GRANT системные_привилегии_и_роли; REVOKE системные_привилегии_и_роли.

TABLE

CREATE, DROP, TRUNCATE.

TABLESPACE

CREATE, ALTER, DROP.

TRIGGER

CREATE, ALTER с инструкциями ENABLE или DISABLE, DROP, ALTER TABLE с инструкциями ENABLE или DISABLE.

TYPE

CREATE, CREATE TYPE BODY, ALTER, DROP, DROP TYPE BODY.

USER

CREATE, ALTER, DROP.

VIEW

CREATE, DROP.

Далее приведены ключевые слова, которые могут применяться для включения аудита команд, но не проверяются при задании ключевого слова ALL. Если специально не указано иное, такие дополнительные ключевые слова включают только аудит соответствующей команды.

ALTER SEQUENCE

ALTER TABLE

COMMENT TABLE

Аудит команды COMMENT для таблицы, представления, материализованного представления или столбцов каждого из таких объектов.

DELETE TABLE

EXECUTE PROCEDURE

Аудит CALL.

GRANT DIRECTORY

GRANT и REVOKE для каталога

GRANT PROCEDURE

GRANT и REVOKE для процедуры.

GRANT SEQUENCE

GRANT и REVOKE для последовательности.

GRANT TABLE

GRANT и REVOKE для таблицы, представления или материализованного представления.

GRANT TYPE

GRANT и REVOKE для типа.

INSERT TABLE

INSERT INTO для таблицы или представления.

LOCK TABLE

LOCK для таблицы или представления.

SELECT SEQUENCE

Любая команда, содержащая CURRVAL или NEXTVAL, для последовательности.

SELECT TABLE

SELECT FROM для таблицы, представления или материализованного представления.

UPDATE TABLE

UPDATE для таблицы или обновляемого представления.

ALL (параметр_команды)

См. приведенный выше в описании *параметра_команды* список команд, которые будет отслеживать ALL.

системная_привилегия

Указывает системные привилегии, для которых будет проводиться аудит. Можно указать роли CONNECT, RESOURCE или DBA для отслеживания всех системных привилегий, включенных в роль.

ALL PRIVILEGES

Отслеживание всех системных привилегий.

прокси-сервер

Указывает, следует ли отслеживать все действия прокси-сервера или же только выполненные от имени определенного пользователя.

пользователь

Пользователи, действия которых отслеживаются.

параметр_объекта

Для каждого объекта можно отслеживать один или несколько способов доступа к нему. Приведем список объектов и возможностей выполнения аудита для них:

Контекст

GRANT. Этот вид аудита появился в Oracle8*i*.

Каталог

AUDIT, GRANT, READ.

Библиотека

GRANT, READ.

Материализованное представление

ALTER, AUDIT, COMMENT, DELETE, INDEX, INSERT, LOCK, RENAME, SELECT, UPDATE. В Oracle8 и более ранних версиях эти параметры объектов существовали под именем объекта «моментальная копия данных». Начиная с Oracle8*i* они могут использоваться как для материализованных представлений, так и для моментальных копий данных.

Объектный тип

ALTER, AUDIT, GRANT. Этот вид аудита появился в Oracle8*i*.

Процедура, функция, пакет

AUDIT, EXECUTE, GRANT, RENAME. Этот вид аудита доступен для PL/SQL или Java в версии Oracle8*i* и выше.

Последовательность

ALTER, AUDIT, GRANT, SELECT.

Таблица

ALTER, AUDIT, COMMENT, DELETE, GRANT, INDEX, INSERT, LOCK, RENAME, SELECT, UPDATE.

Представление

AUDIT, COMMENT, DELETE, GRANT, INSERT, LOCK, RENAME, SELECT, UPDATE.

[схема.]объект

Объект, аудит которого будет проводиться. Если имя схемы не указано, то сервер Oracle считает, что объект находится в схеме текущего пользователя.

имя_каталога

Имя каталога, для которого будет проводиться аудит.

DEFAULT

Указывает параметры проведения аудита по умолчанию для всех объектов, созданных после выполнения данной команды.

NOAUDIT

```
NOAUDIT инструкция_для_команды_sql | инструкция_для_объекта_схемы
    [BY SESSION | ACCESS]
```

Выключает все ранее включенные виды аудита.

Ключевые слова

Ключевые слова и инструкции NOAUDIT имеют те же значения, что и для команды AUDIT.

Другие возможности обеспечения безопасности

Описанные далее возможности обеспечения безопасности по большей части относятся к администраторам баз данных Oracle или специалистам, отвечающим за безопасность. Приведем лишь краткий обзор таких функций, подробную же информацию можно найти в документации Oracle.

Представления и хранимые процедуры

Помимо способов обеспечения безопасности данных БД Oracle, рассмотренных ранее, существуют и другие возможности. До выхода версии Oracle8*i* самым распро-

страненным способом ограничения доступа к данным в зависимости от их значений было использование представлений и хранимых процедур.

Представления

Вы определяете подмножество данных таблицы и предоставляете пользователю доступ только к представлению. Начиная с Oracle8*i* вы можете добиться такого же уровня безопасности при помощи детального контроля доступа, описанного в следующем разделе.

Хранимые процедуры

Вы можете ввести аналогичное ограничение на доступ к таблице используя хранимую процедуру или пакет, выдав пользователям привилегии на хранимую процедуру или пакет. Код хранимой процедуры может содержать собственный набор правил подтверждения правильности.

В последующих разделах поговорим о дополнительных способах контроля доступа.

Детальный контроль доступа и политика безопасности

Детальный контроль доступа (*fine-grained access control*) предлагает способ контекстного обеспечения безопасности, который может быть реализован в коде приложения или в представлениях. Благодаря тому что детальный контроль доступа реализуется на уровне базы данных, он единообразно действует для всех приложений.

Детальный контроль доступа появился в версии Oracle8*i*. Он реализуется специальными правилами для таблиц, регламентирующими права доступа к этим таблицам. *Политика безопасности* (*security policy*) реализуется программным модулем, который может предоставлять доступ на основе логического условия любого вида. Для всех команд SQL, выполняемых на базе данных, создается предикат (условие, добавляемое в инструкцию WHERE и ограничивающее доступ к данным), который автоматически может применяться для обеспечения безопасности на основе содержимого таблицы.

Виртуальные частные базы данных

Механизм контекстных мер безопасности позволяет создавать виртуальные частные базы данных (VPD, Virtual Private Database). Благодаря применению VPD сразу несколько пользователей могут видеть свои собственные представления одной или нескольких таблиц базы данных. Ранее говорилось о том, что подобные меры безопасности можно обеспечить за счет создания и поддержания представлений, но применение VPD избавляет от забот по созданию представлений и разграничению доступа к ним для отдельных пользователей и групп пользователей.

Метки безопасности и управление ими

Метки безопасности появились в Oracle9*i*. Они представляют собой расширение VPD; различие в том, что программные модули для поддержки VPD уже написаны и действуют для значений единственного столбца, содержащего метки. Поэтому для реализации меток безопасности не требуется специального программирования. Метки безопасности относятся к дополнительным компонентам Oracle9*i* Enterprise Edition.

Policy Manager, инструмент администрирования с графическим интерфейсом пользователя, входящий в состав Enterprise Manager, также появился в версии Oracle9*i*. Он реализует управление метками безопасности.

Контекст приложения

Контекст приложения (*application context*), введенный в Oracle8*i*, позволяет установить для пользователя некоторые атрибуты, которые будут действовать в течение всего пользовательского сеанса. Применяя такие атрибуты для предоставления доступа, можно создать роль для конкретного приложения, которая продолжает существовать в базе данных на всем протяжении работы приложения. Контекст приложения может использоваться для реализации детального контроля доступа.

Детальный аудит

Детальный аудит (*fine-grained auditing*) появился в Oracle9*i*. Как и детальный контроль доступа, детальный аудит реализуется за счет определения предиката, вводящего ограничение для команд SQL, которые будут подвергнуты аудиту. Проводя такую политику аудита, вы можете сконцентрироваться на отслеживании действий с небольшим объемом жизненно важных данных. Уменьшение общего количества записей аудита облегчает выявление потенциальных проблем с безопасностью.

LogMiner

LogMiner – это инструментальное средство, позволяющее применять команды SQL для анализа событий в журнале базы данных. LogMiner позволяет отслеживать транзакции по мере их обработки или выявлять, какие конкретно функции вызвали изменение данных. Утилита LogMiner появилась в Oracle8*i*.

С помощью LogMiner (наряду с журналами аудита) можно определить, что происходило с вашей базой данных Oracle. В версии Oracle9*i* LogMiner включен в Enterprise Manager.

Исследование возможностей LogMiner лежит за пределами нашей книги. Подробную информацию можно найти в документации по Oracle.

Oracle Advanced Security

Продукт Oracle Advanced Security, который ранее назывался Secure Network Services, а затем Advanced Network Services, – это пакет расширения, предлагающий мощные средства шифрования данных. Oracle Advanced Security обеспечивает дополнительные возможности по обеспечению безопасности в трех областях:

Сетевая безопасность

Шифрование сообщений, передаваемых службами Oracle Net Services, реализация SSL-шифрования (Secure Sockets Layer – протокола защищенных сокетов) и поддержка RADIUS, Kerberos, смарт-карт, карточек-идентификаторов (token cards) и биометрической аутентификации.

Безопасность пользователей предприятия

Включает применение разнообразных сторонних средств поддержки каталогов, таких как LDAP-каталоги, с помощью которых можно реализовать возможность однократной регистрации. Oracle Advanced Security включает в себя сервис каталогов Oracle Internet Directory (OID), описанный в следующем разделе.

Безопасность инфраструктуры открытых ключей

Включает поддержку стандартных сертификатов X.509 версии 3. Oracle работает с основными поставщиками сервисов инфраструктуры открытых ключей (Public

Key Infrastructure – PKI), такими как Baltimore Technologies и VeriSign, для обеспечения координации с их доверенными корневыми сертификатами.

Oracle Advanced Security внедряет эти сервисы на уровне Oracle Net Services, который реализует взаимодействие между сервером и клиентом, о чем говорится в главе 5. Кроме того, Oracle Advanced Security можно использовать с драйвером Thin JDBC, не содержащим Oracle Net Services.

Oracle Advanced Security включает в себя Oracle Enterprise Security Manager, графический интерфейс пользователя для управления доменами и пользователями предприятия.

В Oracle9*i* можно шифровать данные на сервере с помощью пакета DBMS_OBFUSCATION_TOOLKIT (без участия Oracle Advanced Security). Дополнительная информация о пакете приведена в главе 10.

Интернет-каталог Oracle

В данной главе несколько раз упоминались внешние каталоги. *Внешний каталог* (*external directory*) – это средство для хранения информации о базе данных, такой как имена пользователей и полномочия. Внешний каталог может быть связан с несколькими экземплярами Oracle внутри предприятия. Oracle предлагает свой собственный внешний каталог – интернет-каталог Oracle (Oracle Internet Directory – OID). OID отвечает стандартам упрощенного протокола доступа к сетевым каталогам (Lightweight Directory Access Protocol – LDAP), разработанного в Мичиганском университете.

С помощью OID или других каталогов LDAP можно создать способ аутентификации, который будет охватывать несколько баз данных. Можно применять внешние каталоги и в других целях в глобальной IT-структуре предприятия. OID поддерживает три вида аутентификации: анонимная, основанная на пароле и основанная на сертификате.

В состав OID входит сервер репликации каталогов Oracle и инструмент администрирования с графическим интерфейсом пользователя.

Права вызывающего

До версии Oracle8*i* хранимая процедура обладала собственным набором привилегий. Каждый, кто использовал некоторую хранимую процедуру для доступа к данным, использовал привилегии, выданные процедуре, вне зависимости от того, какими привилегиями обладал сам пользователь.

Начиная с Oracle8*i* при создании функции, процедуры, пакета, объектного типа или Java-кода пользователь может указать инструкцию для полномочий вызывающего объект пользователя. Если такая инструкция присутствует, то объект будет выполняться с привилегиями пользователя, а не самого объекта.