Специальность 10.05.01 «Компьютерная безопасность»,
Специализация «Математические методы защиты информации»
Уровень высшего образования – специалитет

Дисциплина: Основы построения защищенных баз данных.

Лабораторная работа №3.
Администрирование Oracle. Контроль использования ресурсов пользователями, стандартные возможности парольной безопасности.

1. Учебные цели:

- Отработать вопросы управления экземпляром Oracle в части реализации стандартных возможностей парольной безопасности и контроля использования ресурсов пользователями.
- Освоить приемы создание и сопровождения профилей.

2. Требования к результатам обучения основной образовательной программы, достигаемые при проведении лабораторной работы:

- Уметь использовать возможности современных систем для решения задач администрирования и защиты баз данных.
- Владеть средствами приложений СУБД Oracle в части реализации стандартных возможностей парольной безопасности и контроля использования ресурсов пользователями.

3. Перечень материально-технического обеспечения

ПЭВМ с проигрывателем виртуальных машин, виртуальная машина с установленной СУБД Oracle.

4. Краткие теоритические сведения и задания на исследование. Задания выделены рамками и синим шрифтом. Результаты лабораторной работы представляются в виде файла, содержащего копии экрана, показывающие этапы выполнения заданий.

Используемые термины:

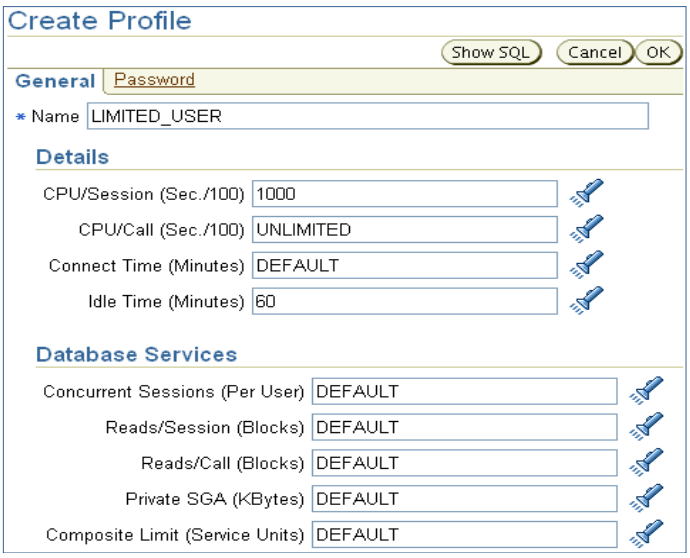
- ***Профиль (profile)*** – именованный набор ограничений на использование базы данных и ресурсов экземпляра.
- ***Квота (quota)*** – ограничение на общее пространство, которое может быть предоставлено в данном табличном пространстве. Это один из способов контроля использования ресурсов пользователями.

Профили

Профили накладывают именованный набор ограничений на использование ресурсов базы данных и экземпляра, а также ограничения на пароли пользователей (длина, срок действия пароля и его истечение и т.д.). Каждому пользователю назначается профиль и только один профиль может быть назначен пользователю в текущий момент. Изменения, внесенные в профиль, начинают действовать в будущих сеансах пользователей и не распространяются на их текущие сеансы.

На параметры стандартного профиля `DEFAULT` можно ссылаться в других профилях. Как видно на слайде, ограничения могут быть указаны либо явно (`CPU/Session`), либо как `unlimited` (`CPU/Call`), либо в виде ссылки на значение в профиле `DEFAULT` (`Connect Time`).

Профили не вызывают проверки ресурсных ограничений до тех пор, пока не будет установлено значение TRUE для параметра инициализации RESOURCE_LIMIT. Если значение этого параметра FALSE, ресурсные ограничения игнорируются.



Профили позволяют администратору контролировать следующие системные ресурсы:

- CPU. Ограничение на использование ресурсов центрального процессора (CPU) может быть наложено на уровне сеанса или на уровне отдельного вызова. Значение 1000 для ограничения CPU/session означает, что, если в любом сеансе, использующем этот профиль, потребляется более 10 секунд процессорного времени (ограничение на время CPU задается в сотых долях секунды), тогда выдается следующее сообщение об ошибке и происходит отсоединение этого сеанса: «ORA-02392: exceeded session limit on CPU usage, you are being logged off».
  Ограничение на уровне вызова осуществляет подобную проверку для каждой отдельной команды, предотвращая потребление слишком большого времени центрального процессора. Если параметр CPU/Call ограничен и пользователь превысил установленное значение, тогда выполнение команды прерывается и пользователь получает сообщение об ошибке: «ORA-02393: exceeded call limit on CPU usage»
- **Сеть/память**: каждый сеанс потребляет ресурсы системной памяти, а также сетевые ресурсы (если пользователь не установил соединение локально с того же компьютера, на котором выполняется сервер БД).
  - Connect Time: определяет, сколько минут пользователь может быть соединен с БД перед тем, как будет автоматически отсоединен.
  - Idle Time: сколько минут сеанс пользователя может простаивать перед тем, как будет автоматически отсоединен. *Время простоя* (*idle time*) подсчитывается только для серверного процесса. Действия, выполняемые приложением, не принимаются во внимание. Ограничение IDLE_TIME не действует на длительно выполняемые запросы и другие операции.
  - Concurrent Sessions: сколько одновременных сеансов может быть установлено с использованием одной и той же учетной записи пользователя БД.
  - Private SGA: ограничение на размер пространства, потребляемого внутри SGA для сортировки, слияния битовых матриц и т.д. Это ограничение действует только, когда используется разделяемый сервер (разделяемые серверные процессы рассматриваются в уроке “Конфигурирование сетевой среды Oracle”).
  - Дисковый ввод-вывод: задаются ограничения на размер информации, которую пользователь может прочитать в течении всего сеанса либо за один вызов команды. Параметры Reads/Session и Reads/Call определяют ограничения на общее

число чтений из оперативной памяти и с диска. Они позволяет исключить появление команд с интенсивным вводом-выводом, которые при этом потребляют память и ограничивают доступ к диску.

Профили также предоставляют *сводное ограничение* (`composite limit`). Это – взвешенная сумма параметров профиля: CPU/Session, Reads/Session, Connect Time и Private SGA. Использование сводного ограничения подробно рассматриваются в документе *Oracle Database Security Guide*.

Создание профиля:

Для создания профиля выберите Administration > Schema > Users & Privileges > Profiles, а затем щелкните на кнопке Create.

Примечание. Подобные ограничения можно также установить с помощью ресурсного менеджера. Дополнительные сведения о ресурсном менеджере см. в документе *Oracle Database Administrator's Guide*.

Средствами Enterprise Manager создайте профиль с именем HRPROFILE, который не допускает простоя сессии более 15 минут. Остальные параметры профиля = Default.
Измените значение параметра RESOURCE_LIMIT на TRUE (от имени администратора выполните команду ALTER SYSTEM SET resource_limit = TRUE SCOPE=SPFILE или средствами Enterprise Manager>Database Configuration>Initialization Parameters).

Пример. Процедура нецелевого расходования вычислительных ресурсов сервера и решение проблемы с помощью профилей, SQL Plus.

```
CONNECT "/AS SYSDBA"

SQL> CREATE PROFILE beat_greedy LIMIT PRIVATE_SGA 10K CPU PER
SESSION 3000;

Профиль создан.

SQL> ALTER USER u1 PROFILE beat_greedy;
Пользователь изменен.

SQL>connect u1/ulpsw
Соединено.

SQL> CREATE OR REPLACE PROCEDURE greedy_c IS
  i number;
    BEGIN
      LOOP
      i := 1;
      EXIT WHEN i > 2;
  END LOOP;
  END;
Процедура создана.

SQL> exec greedy_c  BEGIN greedy_c; END;
*
ошибка в строке 1:
```

ORA-02392: превышен предел сеанса на использование CPU, вы в процессе выхода из системы

Использование возможностей безопасности для сопровождения паролей

Сопровождение паролей в Oracle реализовано с помощью профилей пользователей.

Примечание: не используйте профили, приводящие к истечению срока действия пароля и блокированию пользователей SYS, SYSMAN и DBSNMP.

Профили позволяют использовать многие стандартные возможности обеспечения безопасности.

а) Блокирование входа пользователей в систему. Включает автоматическое блокирование входа пользователя в систему в течение установленного времени после того, как при входе в систему делается заданное число ошибочных попыток.

- Параметр FAILED_LOGIN_ATTEMPTS задает количество неудачных попыток входа в систему перед блокированием пользователя.
- Параметр PASSWORD_LOCK_TIME задает период блокирования пароля в днях после определенного количества неудачных попыток входа в систему.

б) Срок действия паролей и его истечение. Возможность определения максимального срока действия пароля, после истечения которого пароль должен быть изменен.

- Параметр PASSWORD_LIFE_TIME задает максимальный срок действия пароля в днях, после чего учетная запись пользователя получает статус expired.
- Параметр PASSWORD_GRACE_TIME задает период отсрочки в днях изменения пароля, начинающийся после первой попытки соединения, предпринимаемой после того, как истек срок действия пароля.

Примечание. Истечение срока действия пароля и блокирование пользователей SYS, SYSMAN и DBSNMP приводит к нарушению функционирования Enterprise Manager. Приложения должны перехватить предупреждающее сообщение “password expired” и выполнить изменение пароля; иначе после истечения времени, заданного параметром PASSWORD_GRACE_TIME, пользователь блокируется без уведомления.

в) Хронология паролей. При изменении пароля гарантируется, что новый пароль не повторяет старый, пока не пройдет заданный период времени или же не будет использовано установленное количество других паролей после действия старого пароля. Эти проверки реализуются с помощью задания одного из следующих двух параметров.

- Параметр PASSWORD_REUSE_TIME запрещает повторное использование пароля в течение указанного количества дней;
- Параметр PASSWORD_REUSE_MAX задает количество изменений текущего пароля до его возможного повторного использования

Это два взаимоисключающих параметра. Если один из этих параметров не имеет значение UNLIMITED (или DEFAULT; при этом в профиле DEFAULT значение данного параметра отлично от UNLIMITED), тогда другой должен быть установлен в UNLIMITED.

г) Проверка сложности паролей. Выполняется проверка сложности нового пароля на основе установленных правил. Эта проверка должна гарантировать, что пароль достаточно сложен для угадывания взломщиком, пытающимся проникнуть в систему.

В параметре PASSWORD_VERIFY_FUNCTION указывается функция PL/SQL, выполняющая проверку сложности пароля перед тем, как он может быть назначен. Функция проверки пароля должна принадлежать пользователю SYS и возвращать булево значение (true или false).

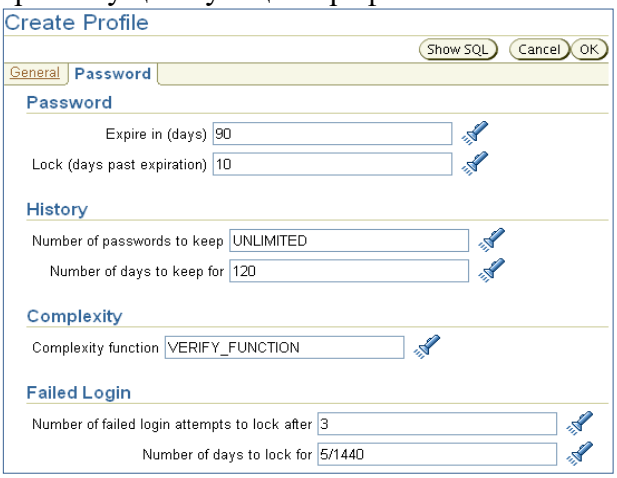
Создание профиля для проверки парольных ограничений

В Enterprise Manager перейдите следующим образом: Server> Security > Profiles. После этого щелкните на кнопке Create.

Для каждого параметра профиля можно выбрать значение из списка предлагаемых общих значений (для этого щелкните на пиктограмму “фонарик”) или ввести свою величину.

Все временные периоды выражаются в днях или долях дня. В сутках 1440 минут, поэтому 5/1440 – это 5 минут.

Enterprise Manager может также использоваться для редактирования парольных параметров в существующем профиле.



Удаление профиля

В Enterprise Manager нельзя удалить профиль, назначенный пользователям. Однако это можно сделать SQL-командой, используя опцию CASCADE. При удалении профиля всем пользователям, которым он был назначен, автоматически выделяется профиль default.

Для определения текущего профиля пользователя, выполните запрос (нужны соответствующие привилегии на чтение представления DBA_USERS):

```
SELECT USERNAME, PROFILE FROM DBA_USERS;
```

VERIFY_FUNCTION_11G – поставляемая функция проверки пароля

Oracle предоставляет функцию проверки сложности пароля, которая создается как стандартная функция PL/SQL с именем VERIFY_FUNCTION_11G в результате выполнения в схеме SYS командного файла <oracle_home>/rdbms/admin/utlpwdmg.sql.

На учебной виртуальной машине
<oracle_home> = «C:\app\IEUser\product\11.2.0\dbhome_1\»

Эта функция может быть использована в качестве шаблона для создания собственной функции проверки пароля.

При выполнении скрипта utlpwdmg.sql создается функция VERIFY_FUNCTION_11G, а также изменяет профиль DEFAULT с помощью следующей команды ALTER PROFILE:

```
ALTER PROFILE default LIMIT
PASSWORD_LIFE_TIME 180
PASSWORD_GRACE_TIME 7
PASSWORD_REUSE_TIME UNLIMITED
PASSWORD_REUSE_MAX UNLIMITED
FAILED_LOGIN_ATTEMPTS 10
```

```
PASSWORD_LOCK_TIME 1
PASSWORD_VERIFY_FUNCTION verify_function_11G;
```

В поставляемой функции `verify_function_11G` проверяются ограничения:

- Минимальная длина пароля – 8 символов
- Пароль не должен совпадать с именем пользователя (в прямом или обратном чтении) в верхнем или нижнем регистре)
- Будут отклонены простые пароли, например oracle
- Пароль должен содержать по крайней мере одну букву, одну цифру и один специальный символ
- Пароль должен отличаться от предыдущего, по крайней мере, на 3 символа.

При создании пользователя ему назначается профиль `DEFAULT`, если не указан другой профиль.

Для определения текущего профиля пользователя, выполните запрос:

```
SELECT USERNAME, PROFILE FROM DBA_USERS
```

Подсказка: используйте эту функцию в качестве шаблона для создания собственной функции проверки пароля.

1. Войти в EM как SYS или System
2. Создать профиль Profile_KB с параметрами:
   -количество сеансов на одного пользователя (количество входов в системы под одним логином) - 1.
   -время подключения в минутах, по истечении которого сеанс принудительно завершается - 10
   -время простоя в минутах, по истечении которого простаивающий сеанс будет принудительно завершен - 3
   -количество неудачных попыток входа – 4
   -количество дней, на которое блокируется учетная запись, при превышении количества неудачных попыток регистрации - 1
   -количество дней до истечения срока действия пароля - 30
   -количество дней до истечения срока действия пароля, когда будет напоминаться о необходимости его смены - 7
   -количество раз повторного использования пароля - 1
   -функция для проверки пароля на соответствие требованиям - verify_function_11G. Для начала использования функция должна быть создана администратором СУБД и всем (PUBLIC) должна быть предоставлена привилегия на ее выполнение.
3. Проверьте, что значение параметра RESOURCE_LIMIT в SPFILE установлено в TRUE (Enterprise Manager>Database Configuration>Initialization Parameters).
4. Назначить профиль Profile_KB пользователю ora1 и пользователю Jenny (создать пользователя средствами SQL Developer как копию пользователя HR с паролем «J_ora23»).
5. Запустить SQL Plus, войти под учетной записью ora1\Kb2023 и далее ничего не делать, проверить, что сеанс будет прерван через 3 минуты.
6. При входе (в SQL Plus или SQL Developer) с учетной записью Jenny ввести пароль 5 раз неправильно.
7. В EM отобразить статус учетной записи Jenny.
8. В EM изменить статус учетной записи Jenny на Open.
9. Открыть несколько сеансов (окон) SQL Plus с учетной записью Jenny (Сколько параллельных сеансов открылось?)

10. Войти под пользователем Jenny в SQL Plus или SQL Developer. Командой Password сменить пароль пользователя Jenny. Попробовать простые пароли (цифровой пароль, пароль = имени пользователя, имени с цифрой, oracle и т.п.).

11. Изменить verify_function_11G, чтобы в паролях анализировались также специальные символы !@#$%^&*()-_=+ и их наличие в пароле было обязательным.

12. Проверить, что функция изменена корректно.

Выделение квот пользователям

Квота (*quota*) – это ограничение на использование пространства в данном табличном пространстве. По умолчанию пользователь не имеет квот ни на какое табличное пространство. Имеется три различных варианта предоставления пользовательских квот.

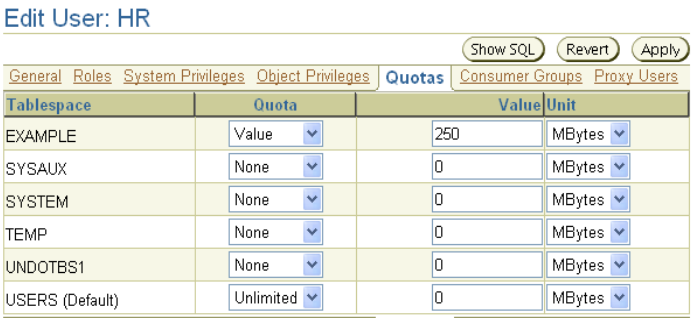
- **Unlimited**; разрешение пользователю использовать столько пространства, сколько доступно в табличном пространстве.
- **Конкретное значение** в килобайтах или мегабайтах, задающее размер пространства, которое может быть занято пользователем. Это не гарантирует, что пространство специально зарезервировано для пользователя. Значение может быть больше или меньше, чем текущий размер памяти, доступной в табличном пространстве.
- **Системная привилегия UNLIMITED TABLESPACE**. Эта привилегия имеет приоритет над всеми отдельными квотами и предоставляет пользователю неограниченную квоту на все табличные пространства, в том числе, SYSTEM и SYSAUX. Следует осторожно выдавать эту привилегию.

Примечание: следует иметь в виду, что при выделении роли RESOURCE одновременно предоставляется системная привилегия UNLIMITED TABLESPACE.

Обычно только пользователи SYS и SYSTEM должны иметь возможность создавать объекты в табличных пространствах SYSTEM и SYSAUX . Другим пользователям не следует давать квоты на эти табличные пространства.

Для использования временных табличных пространств и табличных пространств типа UNDO квоты не нужны.

Квоты на табличные пространства можно задать во вкладке Quotas страницы Edit User.



Вопросы и ответы.

- Когда экземпляр Oracle использует квоту? - Квоты используются, когда пользователь создает или расширяет сегмент.
- На какие операции не влияют квоты? - Операции, которым не требуется место в выделенном табличном пространстве, например, создание представлений или использование временного табличного пространства.
- Когда увеличивается доступное пространство в рамках квоты? - Это происходит, когда объекты, принадлежащие пользователю, удаляются с фразой PURGE или когда корзина автоматически очищается.

Время на выполнение лабораторной работы – 2 часа.