|  |  |
| --- | --- |
| МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ | |
| ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА» | |
|  | |
|  | |
| Лабораторная работа №22 | |
|  | |
|  | Выполнил:  Стерпу Е.К., гр. 6411  Проверил:  Додонов М.В. | |
|  | |
| Самара 2018 | |

Цель: обучение методам и средствам обеспечения регистрации событий в СУБД Oracle.

#### Последовательность действий обучаемого

1. Активировать службу аудита с параметром DB. Перезагрузить БД.

sterpu> conn sys/1 as sysdba

Connected.

sterpu> alter system set audit\_trail=true scope=spfile;

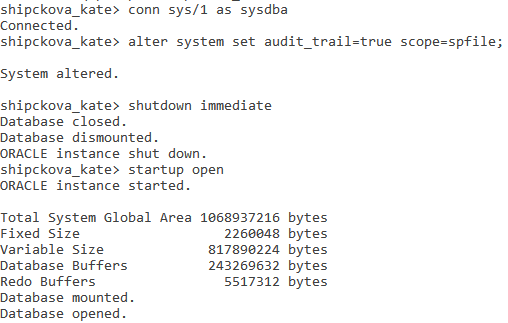
System altered.

sterpu>shutdown immediate

Database closed.

Database dismounted.

ORACLE instance shut down.



1. Подключиться к БД как пользователь, имеющий привилегии AUDIT SYSTEM и AUDIT ANY (т.е. под пользователем, создаваемым через веб-интерфейс и наделенным правами роли DBA). Далее под данным пользователем будет пониматься youUser. Создать таблицу emp с единственным столбцом типа NUMBER. Включить регистрацию неуспешных попыток вставки в таблицу emp. Через представление DBA\_STMT\_AUDIT\_OPTS убедится о включении данной опции аудита.

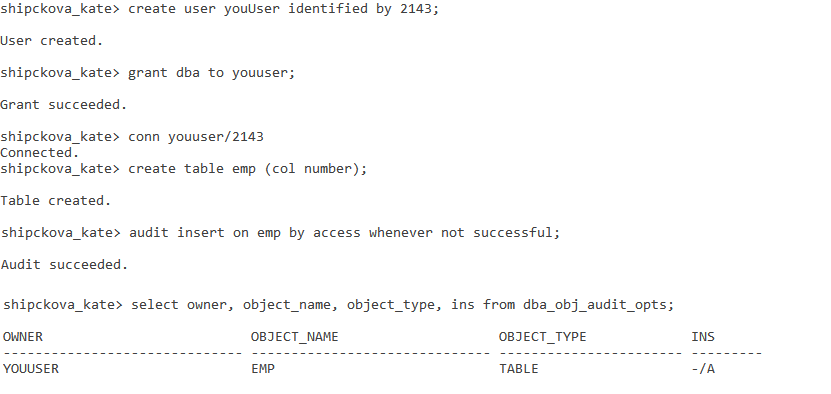
sterpu>create user youuser identified by u;

sterpu>grant dba to youuser;

sterpu>create table emp (al number);

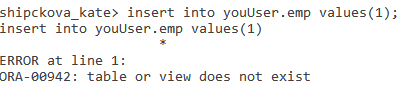
sterpu>audit insert on emp by access whenever not successful;

sterpu>select owner, object\_name,object\_type,ins from dba\_obj\_audit\_opts;



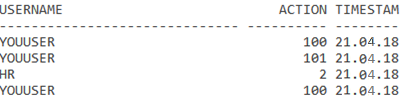
1. Подключиться к БД как hr (пользователь должен быть разблокирован через веб-интерфейс), попытаться вставить в таблицу youUser.emp строку.

sterpu> insert into youuser.emp values(1);



1. Подключиться к БД как youUser и проверить журнал аудита через представление USER\_AUDIT\_TRAIL (выбрать столбцы username, action, timestamp)

sterpu>select username, action, timestamp from user\_audit\_trail;



1. Выключить регистрацию неуспешных попыток вставки в таблицу emp. Через представление DBA\_STMT\_AUDIT\_OPTS (выбрать все столбцы) убедится что данная опция была выключена.

sterpu>noaudit insert on emp by access whenever not successful;

noaudit succeeded.

sterpu> select owner, object\_name, object\_type, ins from dba\_obj\_audit\_opts;

no rows selected

1. Включить аудит успешных и неудачных подключений и отключений от СУБД для всех пользователей. Подключиться к БД под любым пользователем. Подключиться к БД под пользователем youUser. Отключить данный аудит.

sterpu>audit create session by access;

Audit succeeded.

sterpu> connect hr/hr

Connected.

sterpu> connect youuser/123

Connected.

sterpu> noaudit create session;

Noaudit succeeded.

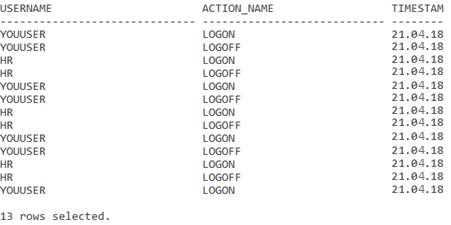
1. Включить аудит успешных и неудачных подключений и отключений от СУБД только для пользователей youUser и hr. Подключиться под пользователем hr. Подключиться под пользователем youUser. Через представление DBA\_AUDIT\_TRAIL (выбрать столбцы username, action\_name, timestamp) проверить журнал аудита.

sterpu>audit create session by youuser, hr by access ;

Audit succeeded.

sterpu>select username, action\_name, timestamp from dba\_audit\_trail where

2 (username='HR' or username='YOUUSER’) and (action\_name='LOGON' or action\_name='LOGOFF');



1. Включить аудит неуспешных применений системной привилегии DELETE ANY TABLE для всех пользователей СУБД с созданием записи в журнале аудита для каждого такого применения.

sterpu> audit delete any table by access whenever not successful;

Audit succeeded.

1. Включить аудит удачных и неудачных попыток применения системной привилегии DELETE ANY TABLE всеми пользователями.

sterpu> audit delete any table by access;

Audit succeeded.

1. Проверить, возможно, ли указать в одной команде включение аудита на выполнение операторов DML (SELECT, INSERT, UPDATE и DELETE) и использование системной привилегии (EXECUTE PROCEDURE). Вставить строку в таблицу emp, вывести все содержимое таблицы emp, удалить строки из таблицы emp. Через представление DBA\_AUDIT\_TRAIL (выбрать столбцы username, timestamp, returncode) проверить журнал аудита.

sterpu>audit select, insert, update, execute procedure;

sterpu>audit select, insert, update, execute procedure

ERROR at line 1:

ORA-00981: cannot mix table and system auditing options

sterpu> insert into emp values(1);

1 row created.

sterpu> select \* from emp;

AL

----------

1

sterpu> delete from emp;

1 row deleted.

sterpu>select username, timestamp, returncode from dba\_audit\_trail where username=

'YOUUSER';

USERNAME TIMESTAM RETURNCODE

----------------------------- -------- ----------

YOUUSER 21.04.18 0

YOUUSER 21.04.18 0

YOUUSER 21.04.18 0

YOUUSER 21.04.18 0

YOUUSER 21.04.18 0

YOUUSER 21.04.18 0

YOUUSER 21.04.18 0

YOUUSER 21.04.18 0

YOUUSER 21.04.18 0

YOUUSER 21.04.18 0

YOUUSER 21.04.18 0

YOUUSER 21.04.18 0

YOUUSER 21.04.18 0

13 rows selected

1. Отключить ранее включенный аудит использования системной привилегии и операторов DML.

sterpu> noaudit delete any tabble;

Noaudit succeeded.

sterpu> noaudit select, insert, update, delete on emp;

Noaudit succeeded.

sterpu>noaudit execute procedure;

Noaudit succeeded.

1. Отключить аудит на все операторы:

sterpu> noaudit delete any table whenever not successful;

Noaudit succeeded.

1. Отключить аудит на использование всех привилегий:

sterpu> noaudit create session by youuser, hr;

Noaudit succeeded.

1. Через представление DBA\_STMT\_AUDIT\_OPTS убедится все ранее включенные правила аудита были отключены.

sterpu> select \* from dba\_stmt\_audit\_opts where audit\_option='DELETE ANY TABLE' or audit\_option='CREATE SESSION';

no rows selected

1. Создать таблицу с двумя столбцами (varchar2(50) и NUMBER). Создать триггер, отслеживающий вставку строк в таблицу emp и заносящий информацию о пользователе производящем операцию и вставляемом значении. Вставить данные в таблицу. Вывести содержимое созданной таблицы в данном пункте и тем самым убедиться в работе триггера.

sterpu> create table extable (username varchar2(50), val number);

Table created.

sterpu> create or replace trigger insert\_emp

2 after insert on emp

3 for each row

4 begin

5 insert into extable values(USER, :new.al);

6 end;

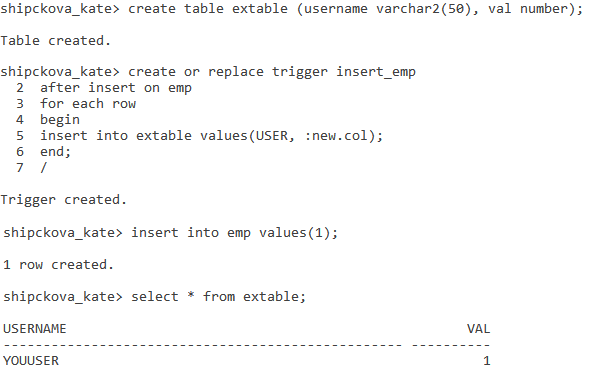
7 /

Trigger created.

sterpu>insert into emp values(1);

1 row created.

sterpu>select \* from extable;



1. Удалить созданный триггер, последнюю созданную таблицу, таблицу emp.

sterpu>drop trigger insert\_emp;

Trigger dropped.

sterpu>drop table extable;

Table dropped.

sterpu>drop table emp;

Table dropped.

1. Удалить все записи в таблице sys.aud$

sterpu>delete from sys.aud$;

22_17

1. Выключить службу аудита.

sterpu>alter system set audit\_trail=false scope=spfile;

System altered.