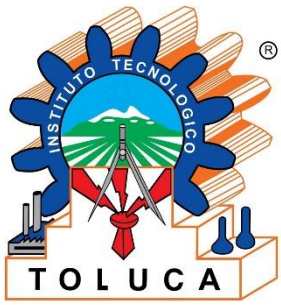

SEP **TECNM**

INSTITUTO TECNOLÓGICO DE TOLUCA

Departamento: Sistemas Computacionales

Profesor: Javier Gómez Lugo

Materia: Administración de base de datos

Reporte prácticas tema 6

Por:

Jiménez Estrada Arturo 18280133

TECNOLÓGICO NACIONAL DE MÉXICO
CAMPUS TOLUCA

LISTA COTEJO REPORTE DE LABORATORIO

NOMBRE DEL PROFESOR:	**Javier Gómez Lugo**
NOMBRE DEL ESTUDIANTE:	**Arturo Jiménez Estrada**
TEMA:	**6**
TOTAL DE PRÁCTICAS:	**5**
INSTRUCCIONES: Evaluar de acuerdo al cumplimiento colocando SI CUMPLE O NO, cada requisito tiene un valor de 4 puntos, Si no cumple mínimo con 4 de los requisitos la calificación es cero. **%CALIF=** Sumatoria del valor de los puntos.	

	REQUISITO	CUMPLE
1.	Resumen	❑
2.	Procedimientos	❑
3.	Dibujos y diagramas	❑
4.	Apariencia – Organización	❑
5.	Ortografía, Puntuación y gramática.	❑

Resumen

En este reporte vimos todo lo que son auditorias, se agregan auditorias de varios tipos, como de instrucción, al igual que auditoria de inicio de sesión, también activar los privilegios de auditoria para otro usuario. Gracias a las auditorias podemos tener un mejor control de que es lo que se hizo por cada usuario, por ejemplo, en el caso del error de inicio de sesión, en el cual si un usuario ingresa mal nos guarda el error que se cometió.

También vimos un poco de diferentes vistas dentro de la base de datos, esto nos ayuda a tener un mejor monitoreo de la base de datos.

Contenido

Consulte las diferentes vistas para el monitoreo de la BD. 4

Consulte los parámetros de la BD para determinar si se encuentra Activa la auditoría de la BD. . 5

Active la auditoría de Instrucciones de la BD sobre la BD y muestre los registros creados en la auditoría. 5

Active la auditoría de acceso a la BD..... 7

Active la auditoría de privilegios sobre el usuario SCOTT por sesión y muestre los registros generados en la auditoría. 8

Active la auditoría para objetos con el comando INSERT en la tabla HR.emp y muestre los registros generados en la auditoría. 10

Consulte las diferentes vistas para el monitoreo de la BD.

A continuación, mostramos distintas consultas dentro de la base de datos.

Vista que muestra si la base de datos está abierta.

SELECT STATUS FROM V$INSTANCE;

```
SQL> select status from v$instance;

STATUS
------------
OPEN
```

Vista que nos muestra los nombres de archivos datafile.

SELECT FILE_NAME FROM DBA_DATA_FILES;

```
SQL> select file_name from dba_data_files;

FILE_NAME
-----------------------------------------------
----------------------
/u01/app/oracle/oradata/cdb1/system01.dbf
/u01/app/oracle/oradata/cdb1/sysaux01.dbf
/u01/app/oracle/oradata/cdb1/example01.dbf
/u01/app/oracle/oradata/cdb1/users01.dbf
/u01/app/oracle/oradata/cdb1/undotbs01.dbf
```

La siguiente instrucción nos sirve para complementar la consulta anterior la cual nos va a sacar los nombres de los tablespace.

SELECT TABLESPACE_NAME FROM DBA_DATA_FILES;

```
SQL> SELECT  TABLESPACE_NAME FROM DBA_DATA_FILES;

TABLESPACE_NAME
------------------------------
SYSTEM
SYSAUX
EXAMPLE
USERS
UNDOTBS1

SQL>
```

El siguiente comando a ejecutar nos servirá para saber cuál es el espacio libre que tiene cada tablespace.

SELECT TABLESPACE_NAME, SUM(BYTES) FROM DBA_FREE_SPACE GROUP BY TABLESPACE_NAME;

```
SQL> SELECT TABLESPACE_NAME, SUM(BYTES) FROM DBA_FREE_SPAC
E GROUP BY TABLESPACE_NAME;

TABLESPACE_NAME                SUM(BYTES)
------------------------------ ----------
SYSAUX                           37486592
UNDOTBS1                          8912896
USERS                             3407872
SYSTEM                            7405568
EXAMPLE                          64159744

SQL>
```

Consulte los parámetros de la BD para determinar si se encuentra Activa la auditoría de la BD.

En esta parte ingresaremos la siguiente instrucción en la cual veremos si esta activa:

SHOW PARAMEYERS AUDIT_TRAIL;

```
SQL> SHOW PARAMETERS AUDIT_TRAIL;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_trail                          string      DB
SQL>
```

Active la auditoría de Instrucciones de la BD sobre la BD y muestre los registros creados en la auditoría.

Empezamos creando la auditoria de tablas para el usuario Scott con el siguiente comando.

Audit table by SCOTT;

```
SQL> audit table by SCOTT;

Audit succeeded.

SQL>
```

Ingresamos al usuario SCOTT para crear una tabla dentro del usuario. En lo personal le agregue solo un campo a la tabla, pero esto no importa en el ejercicio.

```
SQL> conn scott
Enter password:
Connected.
SQL> create table hola (id number(3));

Table created.
```

Regresamos a nuestro usuario “sysdba” y pondremos la siguiente consulta, esto para ver los cambios de tablas dentro del usuario Scott.

Select username, TO_CHAR(TIMESTAMP, ‘DD/MM/YYYY’) TIMESTAMP, OBJ_NAME, ACTION_NAME,SQL_TEXT FROM DBA_AUDIT_TRAIL WHERE USERNAME=’SCOTT’;

```
SQL> Select username, TO_CHAR(TIMESTAMP, 'DD/MM/YYYY') TIM
ESTAM , OBJ_NAME, ACTION_NAME,SQL_TEXT FROM DBA_AUDIT_TRAI
L WHERE USERNAME='SCOTT';
```

```
USERNAME
--------------------------------------------------------------
----------------------
TIMESTAM   OBJ_NAME        ACTION_NAME          SQL_TEXT
---------- --------------- -------------------- ----------
```

```
SCOTT
01/07/2021 HOLA            CREATE TABLE


```

Las capturas están de esta forma ya que tenía activada otra auditoria dentro del usuario SCOTT.

Ahora borramos nuestra tabla dentro del usuario SCOTT.

```
SQL> drop table HOLA;

Table dropped.

SQL>
```

Ingresamos de nuevo como sysdba para ver los cambios que se han hecho en la auditoria

Select username, TO_CHAR(TIMESTAMP, 'DD/MM/YYYY') TIMESTAM, OBJ_NAME, ACTION_NAME,SQL_TEXT FROM DBA_AUDIT_TRAIL WHERE USERNAME='SCOTT';

```
SCOTT
01/07/2021 HOLA            DROP TABLE
```

Esto seria una parte de la auditoria de instrucciones ya que no se nos especifica si todas o solo una en específico.

Active la auditoría de acceso a la BD.

Como primer paso habilitamos la auditoria de inicio de sesión, usamos los siguientes comandos:

Audit session whenever successful;

Audit session whenever no successful;

```
SQL>  audit session whenever successful;

Audit succeeded.

SQL>  audit session whenever not successful;

Audit succeeded.
```

Tratamos de acceder al usuario Scott, pero con una contraseña incorrecta para que eso nos almacene un error. Y continuamos, pero con la contraseña correcta.

```
SQL> conn scott
Enter password:
ERROR:
ORA-01017: invalid username/password; logon denied
```

```
SQL> conn scott
Enter password:
Connected.
```

En este punto regresamos a sysdba, para poder ejecutar el siguiente comando y poder ver los inicios de sesión que se han realizado después de activar la auditoria.

Select username, TO_CHAR(TIMESTAMP, ‘DD/MM/YYYY’) TIMESTAMP, OBJ_NAME, RETURNCODE, ACTION_NAME,SQL_TEXT FROM DBA_AUDIT_TRAIL WHERE ACTION_NAME IN (‘LOGON’,’LOGOFF’) ORDER BY TIMESTAMP DESC;

```
SQL> select username, TO_CHAR(TIMESTAMP,'DD/MM/YYYY') TIMESTAMP,OBJ_NAME,RETURNCODE,ACTION_NAME,SQL_TEXT
  2   FROM DBA_AUDIT_TRAIL
  3   WHERE ACTION_NAME IN ('LOGON','LOGOFF')
  4  ORDER BY TIMESTAMP DESC;

USERNAME
--------------------------------------------------------------------------------
TIMESTAMP  OBJ_NAME        RETURNCODE ACTION_NAME          SQL_TEXT
---------- --------------- ---------- -------------------- ----------
SCOTT
01/07/2021                      28000 LOGON

SCOTT
01/07/2021                          0 LOGOFF

SCOTT
01/07/2021                          0 LOGON


USERNAME
--------------------------------------------------------------------------------
TIMESTAMP  OBJ_NAME        RETURNCODE ACTION_NAME          SQL_TEXT
---------- --------------- ---------- -------------------- ----------
SCOTT
01/07/2021                       1017 LOGON


SQL>
```

Esto seria lo ultimo por esta práctica, podemos ver que si nos muestra los errores en la columna “returncode”.

Active la auditoría de privilegios sobre el usuario SCOTT por sesión y muestre los registros generados en la auditoría.

Dentro de nuestro usuario “sysdba” le damos privilegios de “dba” a nuestro usuario Scott. Utilizar el siguiente comando:

Grant dba to Scott;

```
SQL> grant dba to scott;

Grant succeeded.

SQL>
```

Creamos dentro del usuario “sysdba” la auditoria “créate table”. Utilizamos el siguiente comando para poder crearlo:

Audit create table by access whenever successful;

```
SQL> audit create table by access whenever successful;

Audit succeeded.

SQL>
```

Entramos al usuario Scott para crear una tabla.

```
SQL> conn scott
Enter password:
Connected.
SQL> create table prueba2(id number (2));

Table created.

SQL>
```

Dentro del usuario ponemos la siguiente instrucción para ver lo que nos arroja nuestra auditoria.

select username, TO_CHAR(TIMESTAMP,'DD/MM/YYYY') TIMESTAMP, RETURNCODE,ACTION_NAME FROM DBA_AUDIT_TRAIL WHERE USERNAME='SCOTT';

```
SQL> select username, TO_CHAR(TIMESTAMP,'DD/MM/YYYY') TIME
STAMP, RETURNCODE,ACTION_NAME FROM DBA_AUDIT_TRAIL
  2  WHERE USERNAME='SCOTT';

USERNAME
------------------------------------------------------------
----------------------
TIMESTAMP  RETURNCODE ACTION_NAME
---------- ---------- --------------------
SCOTT
01/07/2021      28000 LOGON

SCOTT
01/07/2021       1017 LOGON
```

```
SCOTT
01/07/2021          0 CREATE TABLE
```

Como podemos notar ahora podemos las auditorias dentro del usuario Scott,

Active la auditoría para objetos con el comando INSERT en la tabla HR.emp y muestre los registros generados en la auditoría.

Necesitamos tener creada la tabla “emp” dentro del usuario hr, en mi caso ya la tenía creada con dos campos.

```
SQL> desc emp;
 Name                                      Null?    Type
 ----------------------------------------- -------- ------
----------------------
 ID                                                 NUMBER
(3)
 NOMBRE                                             VARCHA
R2(20)
```

A continuación, dentro del usuario sysdba, vamos a crear una auditoria “insert” para el usuario hr para la tabla emp. Utilizamos el siguiente comando.

AUDIT INSERT ON HR.EMP BY ACCESS WHENEVER SUCCESSFUL;

```
SQL> conn /as sysdba
Connected.
SQL> AUDIT INSERT ON HR.EMP BY ACCESS WHENEVER SUCCESSFUL;

Audit succeeded.
```

Hacemos una inserción desde el usuario sysdba hacia la tabla emp de hr, para esto solo tenemos que especificar hacia donde es la inserción, utilizamos la siguiente instrucción.

INSERT INTO HR.EMP (ID,NOMBRE) VALUES (1,’ARTURO’);

```
SQL> insert into hr.emp (id,nombre) values (1,'Arturo');

1 row created.

SQL>
```

Ejecutamos el siguiente comando para ver las auditorias del usuario hr, y notamos que aparece nuestro insert.

SELECT USERNAME, TO_CHAR(TIMESTAMP, 'DD/MM/YYYY') TIMESTAM, OBJ_NAME, ACTION_NAME,SQL_TEXT FROM DBA_AUDIT_TRAIL WHERE USERNAME=’HR’;

```
SQL> Select username, TO_CHAR(TIMESTAMP, 'DD/MM/YYYY') TIM
ESTAM, OBJ_NAME, ACTION_NAME,SQL_TEXT FROM DBA_AUDIT_TRAIL
 WHERE USERNAME='HR';

USERNAME
------------------------------------------------------------
--------------------
TIMESTAM   OBJ_NAME        ACTION_NAME          SQL_TEXT
---------- --------------- -------------------- -----------
HR
01/07/2021 EMP             INSERT

HR
01/07/2021                 LOGON

HR
01/07/2021                 LOGOFF


SQL>
```