Universidad Complutense de Madrid
Facultad de Informática
Máster en Ingeniería Informática - Administración de Bases de Datos

Práctica 8 – Ejercicios Auditoría

20 de octubre de 2020

Daniel Bastarrica Lacalle
Jose Javier Cortés Tejada

Índice

1. Paso 1

1. **Conectate a la BD en Database Control con las credenciales:**
   - **User Name: SYS.**
   - **Password: adbd19.**
   - **Connect As: SYSDBA.**
2. **Selecciona la sección Database Configuration en Server y pulsa Initialization Parameters / SPFile.**
3. **Si no aparece, indica que la instalación no utilizo un fichero de configuración para los parámetros del servidor. Busca el parámetro AUDIT_TRAIL y pulsa IR.**

Figura 1: Captura del *Enterprise Manager* con la información del parámetro $AUDIT_TRAIL$.

4. **Introduce el valor DB_EXTENDED y pulsa APPLY. Por defecto AUDIT_TRAIL tiene valor DB, que almacena todos los registros de la auditoria en SYS.AUD$, excepto algunos que siempre se almacenan en ficheros del sistema operativo. DB_EXTENDED además almacena el texto SQL de las operaciones posibles variables.**

Figura 2: Captura del *Enterprise Manager* con la información del parámetro $AUDIT_TRAILactualizada$.

5. **Reinicia la instancia para que tengan efecto los cambios. Ejecuta los siguientes comandos:**

```
sqlplus sys as sysoper
Enter password: password
SQL> SHUTDOWN IMMEDIATE
SQL> STARTUP
SQL> SHOW PARAMETER AUDIT_TRAIL
```

A continuación se muestra el log tras ejecutar las instrucciones requeridas. La última instrucción falla al lanzarse con *sysoper*.

```
oracle@ubuntu32vb:~$ sqlplus sys as sysoper

SQL*Plus: Release 11.2.0.1.0 Production on Wed Nov 20 16:37:29 2019

Copyright (c) 1982, 2009, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> shutdown immediate
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> startup
ORACLE instance started.
Database mounted.
Database opened.
SQL> show parameter audit_trail;
ORA-00942: table or view does not exist
```

Para solventar este error hemos entrado como sysdba y a continuación se muestra el resultado de la útlima ejecución:

```
oracle@ubuntu32vb:~$ sqlplus sys as sysdba

SQL*Plus: Release 11.2.0.1.0 Production on Wed Nov 20 16:40:12 2019

Copyright (c) 1982, 2009, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> show parameter audit_trail;

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

2. Paso 2

1. **Crea el usuario sec_admin asignándole el rol SELECT_CATALOG_ROLE y los privilegios de sistema CREATE PROCEDURE, CREATE ROLE, CREATE SESSION y SELECT ANY DICTIONARY.** Creamos el usuario con una contraseña por defecto y le otrogamos el rol y los permisos requeridos en el enunciado del ejercicio:

```
SQL> create user sec_admin identified by sec_admin;

User created.

SQL> grant SELECT_CATALOG_ROLE to sec_admin;

Grant succeeded.

SQL> grant CREATE PROCEDURE to sec_admin;

Grant succeeded.

SQL> grant CREATE ROLE to sec_admin;

Grant succeeded.

SQL> grant CREATE SESSION to sec_admin;

Grant succeeded.

SQL> grant SELECT ANY DICTIONARY to sec_admin;

Grant succeeded.

SQL>
```

2. **En SQL*Plus, conectate como SCOTT y concedele a sec_admin el privilegio SELECT sobre SCOTT.BONUS table.**

   Tras intentar conectarnos como Scott obtenemos un mensaje que nos informa de un bloqueo sobre la cuenta:

```
oracle@ubuntu32vb:~$ sqlplus scott

SQL*Plus: Release 11.2.0.1.0 Production on Wed Nov 20 16:50:43 2019

Copyright (c) 1982, 2009, Oracle.  All rights reserved.

```

```
Enter password:
ERROR:
ORA-28000: the account is locked
```

Nos loggeamos como *sysdba* para modificar la contraseña de *Scott* y además marcamos la cuenta como *unlock*:

```
oracle@ubuntu32vb:~$ sqlplus sys as sysdba

SQL*Plus: Release 11.2.0.1.0 Production on Wed Nov 20 16:51:40 2019

Copyright (c) 1982, 2009, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> alter user scott identified by scott;

User altered.

SQL> alter user scott account unlock;

User altered.
```

Por último accedemos con las credenciales de *Scott* y ejecutamos el la siguiente intrucción de acuerdo al enunciado:

```
oracle@ubuntu32vb:~$ sqlplus scott

SQL*Plus: Release 11.2.0.1.0 Production on Wed Nov 20 16:54:43 2019

Enter password:

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> grant select on scott.bonus to sec_admin;

Grant succeeded.
```

3. **Conectate en Database Control a la cuenta SYS con rol SYSDBA.**

4. **Selecciona en Server la sección Security y pulsa Audit Settings. En la página Audited Objects añade la siguiente información:**

   - **Object Type: Select Table.**
   - **Table: Enter SCOTT.BONUS.**
   - **Available Statements: SELECT.**

   Accedemos con las credenciales del enunciado el *Entreprise Manager* y navegamos hasta la pestaña selecionada. En la figura 3 tenemos el resultado de este apartado.

Figura 3: Captura del *Enterprise Manager* del tipo de auditoría a realizar.

5. **Pulsa OK.**

6. **Desconéctate de Database Control.**

   En la figura 4 tenemos el resultado de este apartado.

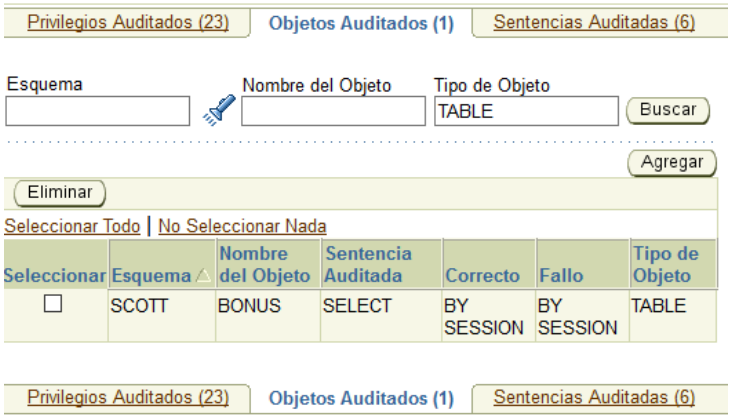

Figura 4: Captura del *Enterprise Manager* del objeto auditado.

3. Paso 3

Ya podemos auditar, y las consultas SELECT que se ejecuten sobre SCOTT.BONUS se registrarán en DBA_AUDIT_TRAIL.

1. **Conectate a SQL*Plus con la cuenta sec_admin.**

```
sqlplus sec_admin
Enter password: password
```

2. **Ejecuta la sentencia:**

```
SELECT COUNT(*) FROM SCOTT.BONUS;
```

```
SQL> SELECT COUNT(*) FROM SCOTT.BONUS;

  COUNT(*)
----------
         0

SQL>
```

3. **Comprueba en DBA_AUDIT_TRAIL la información registrada:**

```
SELECT USERNAME, SQL_TEXT, TIMESTAMP
FROM DBA_AUDIT_TRAIL
WHERE SQL_TEXT LIKE 'SELECT %';
```

El valor almacenado en la columna SQL_TEXT distingue entre mayúsculas y minúsculas, introdúcelo tal y como lo has escrito.

```
SQL> SELECT USERNAME, SQL_TEXT, TIMESTAMP
  2  FROM DBA_AUDIT_TRAIL
  3  WHERE SQL_TEXT LIKE 'SELECT %';



USERNAME           SQL_TEXT                               TIMESTAMP
------------------ -------------------------------------- ----------------------
SEC_ADMIN          SELECT COUNT(*) FROM SCOTT.BONUS       20-NOV-19
```

4. **Sal de SQL*Plus**

4. Paso 4

Dejamos todo como estaba

1. **Conéctate a Database Control con la cuenta SYS como SYSDBA.**
2. **Database Configuration en Server y pulsa Audit Settings en la sección Security. Selecciona Audited Objects y selecciona SCOTT.BONUS y elimínalo.**

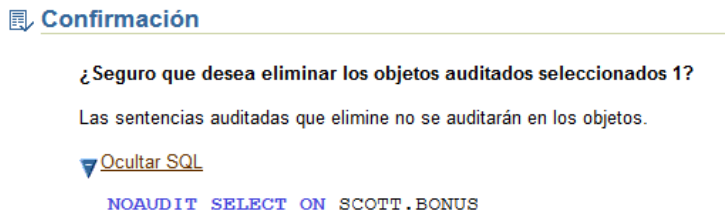

Figura 5: Captura del *Enterprise Manager* del mensaje de confirmación de borrado.

3. **Selecciona Database Configuration en Server y pulsa Initialization Parameters./SPFile. Actualiza al valor original en el parámetro AUDIT_TRAIL.**

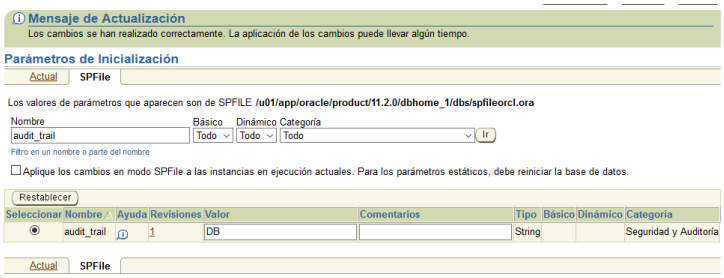

Figura 6: Captura del *Enterprise Manager* de la restauración de *AUDIT_TRAIL* al valor por defecto

4. **Reinicia la base de datos para que tengan efecto los cambios.**

```
sqlplus sys as sysoper
Enter password: password
SQL> SHUTDOWN IMMEDIATE
SQL> RESTART
```

```
SQL> oracle@ubuntu32vb:~$ sqlplus sys as sysdba

Enter password:

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> shutdown immediate
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> startup
ORACLE instance started.

Total System Global Area  636100608 bytes
Fixed Size                  1338392 bytes
Variable Size             230687720 bytes
Database Buffers          398458880 bytes
Redo Buffers                5615616 bytes
Database mounted.
Database opened.
SQL>
```