

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	3
2. Paso 2	5
3. Paso 3	8
4. Paso 4	9

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.

Restablecer									
Seleccionar	Nombre	Ayuda	Revisiones	Valor	Comentarios	Tipo	Básico	Dinámico	Categoría
<input checked="" type="radio"/>	audit_trail	?		db		String			Seguridad y Auditoría
<input type="button" value="Actual"/> <input type="button" value="SPFile"/>									

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.

Restablecer									
Seleccionar	Nombre	Ayuda	Revisiones	Valor	Comentarios	Tipo	Básico	Dinámico	Categoría
<input checked="" type="radio"/>	audit_trail	?		DB_EXTENDED		String			Seguridad y Auditoría
<input type="button" value="Actual"/> <input type="button" value="SPFile"/>									

Figura 2: Captura del *Enterprise Manager* con la información del parámetro $AUDIT_{TRAIL}$ actualizada.

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*.

```
1 oracle@ubuntu32vb:~$ sqlplus sys as sysoper
2
3 SQL*Plus: Release 11.2.0.1.0 Production on Wed Nov 20 16:37:29 2019
4
5 Copyright (c) 1982, 2009, Oracle. All rights reserved.
6
7 Enter password:
8
9 Connected to:
10 Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
11 With the Partitioning, OLAP, Data Mining and Real Application Testing options
12
13 SQL> shutdown immediate
14 Database closed.
15 Database dismounted.
16 ORACLE instance shut down.
17 SQL> startup
18 ORACLE instance started.
19 Database mounted.
20 Database opened.
21 SQL> show parameter audit_trail;
22 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 última ejecución:

```
1 oracle@ubuntu32vb:~$ sqlplus sys as sysdba
2
3 SQL*Plus: Release 11.2.0.1.0 Production on Wed Nov 20 16:40:12 2019
4
5 Copyright (c) 1982, 2009, Oracle. All rights reserved.
6
7 Enter password:
8
9 Connected to:
10 Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
11 With the Partitioning, OLAP, Data Mining and Real Application Testing options
12
13 SQL> show parameter audit_trail;
14
15 NAME                                TYPE          VALUE
16 -----
17 audit_trail                          string        DB_EXTENDED
18 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 otorgamos el rol y los permisos requeridos en el enunciado del ejercicio:

```
1 SQL> create user sec_admin identified by sec_admin;
2
3 User created.
4
5 SQL> grant SELECT_CATALOG_ROLE to sec_admin;
6
7 Grant succeeded.
8
9 SQL> grant CREATE PROCEDURE to sec_admin;
10
11 Grant succeeded.
12
13 SQL> grant CREATE ROLE to sec_admin;
14
15 Grant succeeded.
16
17 SQL> grant CREATE SESSION to sec_admin;
18
19 Grant succeeded.
20
21 SQL> grant SELECT ANY DICTIONARY to sec_admin;
22
23 Grant succeeded.
24
25 SQL>
```

2. **En SQL*Plus, conectate como SCOTT y concede 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:

```
1 oracle@ubuntu32vb:~$ sqlplus scott
2
3 SQL*Plus: Release 11.2.0.1.0 Production on Wed Nov 20 16:50:43 2019
4
5 Copyright (c) 1982, 2009, Oracle. All rights reserved.
6
```

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

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

```
1 oracle@ubuntu32vb:~$ sqlplus sys as sysdba
2
3 SQL*Plus: Release 11.2.0.1.0 Production on Wed Nov 20 16:51:40 2019
4
5 Copyright (c) 1982, 2009, Oracle. All rights reserved.
6
7 Enter password:
8
9 Connected to:
10 Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
11 With the Partitioning, OLAP, Data Mining and Real Application Testing options
12
13 SQL> alter user scott identified by scott;
14
15 User altered.
16
17 SQL> alter user scott account unlock;
18
19 User altered.
```

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

```
1 oracle@ubuntu32vb:~$ sqlplus scott
2
3 SQL*Plus: Release 11.2.0.1.0 Production on Wed Nov 20 16:54:43 2019
4
5 Enter password:
6
7 Connected to:
8 Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
9 With the Partitioning, OLAP, Data Mining and Real Application Testing options
10
11 SQL> grant select on scott.bonus to sec_admin;
12
13 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 *Enterprise Manager* y navegamos hasta la pestaña seleccionada. En la figura 3 tenemos el resultado de este apartado.

Agregar Objeto Auditado

Seleccione el tipo de objeto que desea auditar y especifique los atributos d

Tipo de Objeto

Atributos para Tipo de Objeto: Tabla

Tabla

Sentencias Disponibles

ALTER
AUDIT
COMMENT
DELETE
FLASHBACK
GRANT
INDEX
INSERT
LOCK
RENAME
UPDATE



Mover



Mover Todo



Eliminar



Eliminar Todo

Sentencias Seleccionadas

SELECT

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.

Seleccionar	Esquema	Nombre del Objeto	Sentencia Auditada	Correcto	Fallo	Tipo de Objeto
<input type="checkbox"/>	SCOTT	BONUS	SELECT	BY SESSION	BY SESSION	TABLE

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;
```

```
1 SQL> SELECT COUNT(*) FROM SCOTT.BONUS;
2
3      COUNT(*)
4  -----
5              0
6
7 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.

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

```
4
5
6
7 USERNAME          SQL_TEXT                                TIMESTAMP
8 -----
9 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.

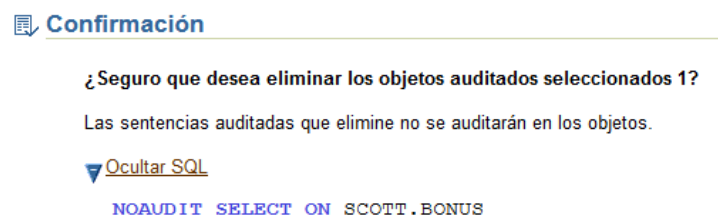


Figura 5: Captura del *Enterprise Manager* del mensaje de confirmación de borrado.

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

Mensaje de Actualización
Los cambios se han realizado correctamente. La aplicación de los cambios puede llevar algún tiempo.

Parámetros de Inicialización

Actual SPFile

Los valores de parámetros que aparecen son de SPFILE: /u01/app/oracle/product/11.2.0/dbhome_1/dbs/spfileorcl.ora

Nombre: audit_trail Básico Dinámico Categoría: Todo Todo Todo (Ir)

Filtro en un nombre o parte del nombre

☐ Aplique los cambios en modo SPFile a las instancias en ejecución actuales. Para los parámetros estáticos, debe reiniciar la base de datos.

Restablecer

Seleccionar	Nombre	Ayuda	Revisión	Valor	Comentarios	Tipo	Básico	Dinámico	Categoría
<input checked="" type="radio"/>	audit_trail		1	DB		String			Seguridad y Auditoría

Actual SPFile

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
```

```
1 SQL> oracle@ubuntu32vb:~$ sqlplus sys as sysdba
2
3 Enter password:
4
5 Connected to:
6 Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
7 With the Partitioning, OLAP, Data Mining and Real Application Testing options
8
9 SQL> shutdown immediate
10 Database closed.
11 Database dismounted.
12 ORACLE instance shut down.
13 SQL> startup
14 ORACLE instance started.
15
16 Total System Global Area 636100608 bytes
17 Fixed Size 1338392 bytes
18 Variable Size 230687720 bytes
19 Database Buffers 398458880 bytes
20 Redo Buffers 5615616 bytes
21 Database mounted.
22 Database opened.
23 SQL>
```