Prácticas de Administración de Bases de Datos

Grado en Ingeniería Informática

PRÁCTICA 11

Seguridad en las Bases de Datos
(auditoría)

SOLUCIONES

OBJETIVOS

- Aprender a manejar la auditoría de Oracle

1. Comprobar los usuarios que tienen asignado los privilegios AUDIT SYSTEM y AUDIT ANY (vista **dba_sys_privs**)

```
select * from dba_sys_privs where privilege ='AUDIT ANY';
select * from dba_sys_privs where privilege ='AUDIT SYSTEM';
```

2. Desde el usuario **system**, activar una auditoría para registrar todas las conexiones exitosas y no exitosas

```
audit session;
```

3. Borrar toda la información de la tabla SYS.AUD$

```
delete from sys.aud$;

Si tuviéramos tantas filas y limitado el espacio de
tablas undo… de forma que no poamos ejecutar la
instrucción, hacer previamente:

alter tablespace UNDO_01 add datafile
'c:\temp\undo2.dat' size 25M autoextend on;
```

4. Realizar conexiones y desconexiones con los usuarios **admin** y **estudiante**. Realizar algunas con éxito y otras con fallo (introduciendo una contraseña errónea). Estos usuarios han sido creado en prácticas anteriores.

5. Desde el usuario **system**, visualizar las conexiones realizadas a la base de datos. ¿Cuál es el campo que indica si la conexión se ha realizado con éxito o ha fallado y cuáles son sus códigos respectivamente?
CONSEJO: no intentar ver todos los campos a la vez. Además, para poder visualizar correctamente los campos, es recomendable usar las funciones *substr* para cadenas de texto y *to_char* para campos de tipo TIMESTAMP

```
select substr(os_username,1,10) usuario_so, substr(username,1,12)
usuario, to_char(timestamp,'dd-mm-yyyy hh24:mi:ss') tiempo_conexion,
to_char(logoff_time,'dd-mm-yyyy hh24:mi:ss') tiempo_desconexion,
returncode exito
from dba_audit_session
order by username, timestamp, logoff_time;
```

USUARIO_SO	USUARIO	TIEMPO_CONEXION	TIEMPO_DESCONEXION	ÉXITO
NT AUTHORI	DBSNMP	24-05-2016 10:09:08	24-05-2016 10:09:07	0
NT AUTHORI	DBSNMP	24-05-2016 10:10:37	24-05-2016 10:10:36	0
NT AUTHORI	ESTUDIANTE	24-05-2016 10:09:49		1017
NT AUTHORI	ESTUDIANTE	24-05-2016 10:09:33	24-05-2016 10:09:48	0

```
El campo es returncode (0 = éxito; 1017 = error en la contraseña)
```

6. Desde el usuario **sys** o **system**, eliminar las entradas de la tabla de auditoría

```
delete from SYS.aud$;
```

7. Desactivar la auditoría anterior y activar sólo para que registre las sesiones fallidas

```
noaudit session;
audit session whenever not successful;
```

8. Volver a realizar conexiones con éxito y sin éxito y comprobar que sólo se registran las fallidas

9. Volver a eliminar las entradas de la tabla de auditoría

```
delete from sys.aud$;
```

10. Desactivar la auditoría anterior y activarla sólo para que registre las sesiones del usuario **admin**

```
noaudit session;
audit session by admin;
```

11. Volver a realizar conexiones con éxito y sin éxito con varios usuarios y comprobar que sólo se registran las del usuario **admin**

12. Desde al usuario **system**, otorgar al usuario **admin** el privilegio de sistema para crear usuarios

```
grant create user to admin;
```

13. Desde el usuario **system** activar una auditoría que controle las sentencias de creación de usuarios en la base de datos

```
audit create user;
```

14. Desde el usuario **admin**, crear un usuario correctamente. Después intentar crear el mismo usuario (por supuesto dará un error) y comprobar la auditoría (vista **DBA_AUDIT_OBJECT**). ¿Cuál es el código de error que indica el fallo en la creación?

```
select * from DBA_AUDIT_OBJECT where username='ADMIN';

código 1920
```

15. Desde el usuario **system**, activar una auditoría para saber quién está borrando e insertando tuplas en la tabla ESTUDIANTE (propiedad del usuario **admin**). Se debe almacenar una fila cada vez que ocurra una operación de inserción o borrado

```
AUDIT DELETE, INSERT ON admin.estudiante BY ACCESS;
```

16. Desde el usuario **estudiante**, intentar realizar borrados e inserciones en la tabla **admin.estudiante** (si no tiene permiso para ello, debéis otorgárselo). Hacer pruebas con intentos válidos e incorrectos y comprobar las auditorías

```
EN ADMIN:
 GRANT INSERT,DELETE ON ADMIN.ESTUDIANTE TO ESTUDIANTE;

En estudiante
 INSERT    INTO    ADMIN.ESTUDIANTE(NOMBRE,FECHANAC,DNI,CURSO)
VALUES ('PEPITO','01/01/1970','29','C01');
delete from admin.estudiante where nombre='pepito';
delete from admin.estudiante where nombre='PEPITO';

  select substr(username,1,12) usuario,
    to_char(timestamp,'dd-mm-yyy hh24:mi:ss')
       tiempo_conexion,
    substr(owner,1,10) propie, substr(obj_name,1,15) objeto,
    substr(action_name,1,10) accion ,returncode
  from dba_audit_object
  where username='ESTUDIANTE'
  order by os_username,timestamp,owner,obj_name,action_name;


ESTUDIANTE  24-05-010 15:11:00     ADMIN ESTUDIANTE  INSERT 0
ESTUDIANTE  24-05-010 15:11:25     ADMIN ESTUDIANTE  DELETE 0
ESTUDIANTE  24-05-010 15:11:25     ADMIN ESTUDIANTE  DELETE 0
```

17. Desde el usuario **system**, activa una auditoría para cualquier operación de consulta, inserción o borrado que se realice en la tabla PROFESOR (propiedad del usuario **admin**). En este caso sólo se desea almacenar una fila por sesión

```
AUDIT SELECT, DELETE, INSERT ON admin.profesor BY SESSION;
```

18. Desde el usuario **admin** realizar una inserción y una consulta en la tabla PROFESOR. Desde el usuario **system**, comprobar las auditorías. ¿Qué indica el campo **ses_actions**?

```
select substr(username,1,10) usuario,
     to_char(timestamp,'dd-mm-yyyy hh24:mi:ss') fecha,
     substr(owner,1,10) prop, substr(obj_name,1,15) objeto,
     ses_actions
from dba_audit_object
order by timestamp;
```

SES_ACTIONS Resumen de sesión, una cadena de 16 caracteres, uno por cada tipo de acción de la lista ordenada ALTER, AUDIT, COMMENT, DELETE, GRANT, INDEX, INSERT, LOCK, RENAME, SELECT, UPDATE, REFERENCES, y EXECUTE.

19. Consultar las opciones por defecto de auditoría de objetos (ALL_DEF_AUDIT_OPTS)

```
select * from all_def_audit_opts;

ALT AUD COM DEL GRA IND INS LOC REN SEL UPD REF EXE
--- --- --- --- --- --- --- --- --- --- --- --- ---
-/- -/- -/- -/- -/- -/- -/- -/- -/- -/- -/- -/- -/-

1 fila seleccionada.
```

20. Especificar las opciones de auditoría por defecto para los objetos creados en un futuro de forma que se registre información siempre que se produzca un “alter”, “insert”, “update” o “delete”

```
audit alter, insert, update, delete on default;

ALT AUD COM DEL GRA IND INS LOC REN SEL UPD REF EXE
--- --- --- --- --- --- --- --- --- --- --- --- ---
S/S -/- -/- S/S -/- -/- S/S -/- -/- -/- S/S -/- -/-

1 fila seleccionada.
```

El significado de cada una de las columnas es:
-/-: No auditoria por defecto.
S/-: Auditado cuando sea exitosa la operación.
-/S: Auditado cuando sea fallida la operación.

ALT ... ALTER
AUD ... AUDIT
COM ... COMMENT
DEL ... DELETE
GRA ... GRANT
IND ... INDEX
INS ... INSERT
LOC ... LOCK
REN ... RENAME
SEL ... SELECT
UPD ... UPDATE
REF ... REFERENCES
EXE ... EXECUTE

21. Comprobar a qué usuarios se les está auditando las conexiones (vista **dba_priv_audit_opts**)

```
select substr(user_name,1,12) usuario, privilege,
        success,failure
    from dba_priv_audit_opts
    where privilege = 'CREATE SESSION'
    order by user_name, privilege;
```

22. Desactivar la auditoría de las conexiones a la base de datos.

```
noaudit session;
```

23. Volver a consultar la vista **dba_priv_audit_opts**. ¿Se sigue auditando las conexiones a ciertos usuarios?

```
select substr(user_name,1,12) usuario, privilege,
        success,failure
from dba_priv_audit_opts
order by user_name,privilege;
```

24. Desactivar la auditoría de las conexiones para que afecte también a los usuarios que aún la tienen activa.

```
noaudit session by admin, estudiante;
```

25. Programar una auditoría de grano fino para que se registre una fila cada vez que se consulte la tabla PROFESOR buscando un salario mayor que 1700€

```
BEGIN
  DBMS_FGA.ADD_POLICY(object_schema => 'admin',
  object_name => 'profesor',
  policy_name => 'control',
  audit_column => 'sueldo',
  audit_condition => 'sueldo > 1700',
  statement_types => 'SELECT');
END;
```

26. Desde el usuario **admin** hacer una consulta a la tabla PROFESOR buscando profesores que ganen menos de 1700€. Comprobar si se ha registrado algo en la auditoría (vista **dba_fga_audit_trail**)

27. Volver a consultar la tabla PROFESOR pero esta vez buscando profesores que ganen más de 1700€. Comprobar si se ha registrado algo en la auditoría (vista **dba_fga_audit_trail**)