Administración de Bases de Datos

Auditoría en Oracle

En Oracle existen tres tipos de auditoría:

* Auditoría de Bases de Datos
* Auditoría de Objetos
* Auditoría de Granularidad Fina

Para que Oracle grabe los registros de auditoría, debe tener el parámetro “audit\_trail” activado. Por defecto, dicho parámetro, en el campo VALUE, tiene el valor NONE. Cuando está en NONE, la auditoría está desactivada.

Para consultar si la auditoría está activada o no, se ejecuta el siguiente comando y se revisa el valor de la columna VALUE.

SELECT \*

FROM V$PARAMETER

WHERE NAME = 'audit\_trail'

Para activar la auditoria, se ejecuta el siguiente comando:

ALTER SYSTEM SET AUDIT\_TRAIL = 'DB' SCOPE = SPFILE;

Y se debe reiniciar el servidor (shutdown / startup) para que tome efecto el cambio.

Auditoría de Bases de Datos

Vamos a consultar la tabla que tiene las pistas de auditoria.

SELECT \*

FROM SYS.AUD$;

Para mirar la auditoria de sentencias, es decir, a cuáles usuarios se van a auditar y bajo que sentencias, se puede consultar la vista DBA\_STMT\_AUDIT\_OPTS:

SELECT SUBSTR( USER\_NAME , 1 , 10 ) ,

SUBSTR( AUDIT\_OPTION , 1 , 20 ) ,

SUBSTR( SUCCESS , 1 , 10 ) ,

SUBSTR( FAILURE, 1 , 10

FROM DBA\_STMT\_AUDIT\_OPTS

ORDER BY 1;

Para hacer el ejercicio, crear el usuario llamado USER20 y darle el rol de DBA.

CREATE USER USER20 IDENTIFIED BY 123;

GRANT DBA TO USER20;

Para auditar los SELECTs e INSERTs que haga el usuario USER20, ejecutemos lo siguiente:

AUDIT SELECT TABLE , INSERT TABLE BY USER20 BY ACCESS;

Para mirar cuáles sentencias se van a auditor del usuario USER20:

SELECT SUBSTR( USER\_NAME , 1 , 10 ) ,

SUBSTR( AUDIT\_OPTION , 1 , 20 ) ,

SUBSTR( SUCCESS , 1 , 10 ) ,

SUBSTR( FAILURE, 1 , 10 )

FROM DBA\_STMT\_AUDIT\_OPTS

ORDER BY 1;

Vamos a conectarnos con el usuario USER20 y vamos a realizar un SELECT sobre una tabla de su esquema. Es decir, primero creemos una tabla, llamada EMPLEADO, en el esquema de USER20 y luego le hacemos SELECT.

Vamos a comprobar que la sentencia SELECT, hecha por USER20, haya quedado registrada en la vista DBA\_AUDIT\_TRAIL:

SELECT SUBSTR(OS\_USERNAME,1,20) USUARIO\_SO,

SUBSTR(USERNAME,1,12) USUARIO,

TO\_CHAR(TIMESTAMP,'DD-MM-YYY HH24:MI:SS') TIEMPO\_CONEXION,

SUBSTR(ACTION\_NAME,1,10) ACCION,

SUBSTR( OBJ\_NAME , 1, 15 ) OBJETO

FROM DBA\_AUDIT\_TRAIL

WHERE USERNAME = 'USER20' AND OBJ\_NAME IN (‘EMPLEADO’)

ORDER BY USERNAME,TIMESTAMP,LOGOFF\_TIME;

Se puede ver que queda grabada, en la vista de auditoria, el hecho de que el usuario USER20 hizo un SELECT sobre la table EMPLEADO.

En este tipo de auditoria no queda registrada la instrucción SQL completa que dio pie para el registro de auditoría, solamente dice que instrucción se ejecutó (INSERT, SELECT, etc.).

Con el usuario USER20, insertar dos tuplas en la table EMPLEADO. Luego, revisar de nuevo el registro de auditoria (ejecutar la misma consulta anterior).

Si queremos desactivarle al usuario USER20 la auditoria sobre la instrucción SELECT, se ejecuta la siguiente instrucción:

NOAUDIT SELECT TABLE BY USER20;

Para comprobar que ya no se le va a auditar los SELECTs al usuario USER20:

SELECT SUBSTR( USER\_NAME , 1 , 10 ) ,

SUBSTR( AUDIT\_OPTION , 1 , 20 ) ,

SUBSTR( SUCCESS , 1 , 10 ) ,

SUBSTR( FAILURE, 1 , 10 )

FROM DBA\_STMT\_AUDIT\_OPTS

ORDER BY 1;

Auditoría de Objetos

La Auditoría de objetos, registra los cambios por operaciones efectuadas por los usuarios en determinadas tablas.

Vamos a consultar las auditorías activas que existen sobre objetos de la base de datos:

SELECT \* FROM DBA\_OBJ\_AUDIT\_OPTS;

Para hacer el ejercicio, vamos a activar la auditoria relacionada con las acciones SELECT, INSERT y UPDATE, sobre el objeto USER20.EMPLEADO.

AUDIT SELECT, INSERT, DELETE, UPDATE ON USER20.EMPLEADO;

Consultemos los objetos auditados:

SELECT \*

FROM DBA\_OBJ\_AUDIT\_OPTS;

Creemos un nuevo usuario, llamado MATEO, con permisos de hacer consultas e inserciones sobre la table EMPLEADO de USER20. Luego de esto, con el usuario MATEO, inserter datos en EMPLEADO y consultarlos.

Miremos como quedó grabado el registro de auditoría sobre el objeto USER20.EMPLEADO, por parte del usuario MATEO:

SELECT SUBSTR(OS\_USERNAME,1,10) USUARIO\_SO,

SUBSTR(USERNAME,1,12) USUARIO,

TO\_CHAR(TIMESTAMP,'DD-MM-YYYHH24:MI:SS') TIEMPO\_CONEXION, SUBSTR(OWNER,1,10) PROPIE,

SUBSTR(OBJ\_NAME,1,15) OBJETO,

SUBSTR(ACTION\_NAME,1,35) ACCION

FROM DBA\_AUDIT\_OBJECT

WHERE USERNAME='MATEO' AND OBJ\_NAME LIKE '%EMPLEADO%'

ORDER BY TIMESTAMP DESC;

Para desactivar todas las opciones de auditoría que tenemos configuradas, ejecutamos:

NOAUDIT ALL ON DEFAULT;

Auditoría de Granularidad Fina

Si queremos que la auditoria hecha por Oracle grabe la instrucción SQL completa ejecutada por un usuario, utilizamos este tipo de auditoría.

En el ejemplo que vamos a desarrollar se auditan las sentencias INSERT, UPDATE, DELETE, y SELECT en la tabla “USER20.EMPLEADO”, controlando cualquier acceso a la columna “APELLIDO” pertenecientes a los empleados con apellido “GOMEZ”:

BEGIN

DBMS\_FGA.ADD\_POLICY(

OBJECT\_SCHEMA => 'USER20',

OBJECT\_NAME => 'EMPLEADO',

POLICY\_NAME => 'CHK\_HR\_EMP',

AUDIT\_CONDITION => 'APELLIDO= ''GOMEZ'' ',

AUDIT\_COLUMN => 'APELLIDO',

STATEMENT\_TYPES => 'INSERT,UPDATE,DELETE,SELECT');

END;

Ahora, desde otro usuario que tenga permisos, vamos a insertar dos nuevas tuplas en la tabla EMPLEADO, una tupla de un empleado cuyo apellido es GOMEZ, y otra tupla con un empleado de apellido LOPEZ.

Ahora consultemos los datos de la auditoría de granularidad fina:

SELECT TO\_CHAR( TIMESTAMP , 'DD/MM/YY HH24:MI') TIEMPO ,

DB\_USER , USERHOST, SUBSTR( OBJECT\_NAME , 1 , 15 ) ,

SUBSTR( OBJECT\_SCHEMA , 1 , 15 ) , POLICY\_NAME,

SQL\_TEXT

FROM DBA\_FGA\_AUDIT\_TRAIL;

Como podemos apreciar, la instrucción INSERT del empleado GOMEZ quedó registrada en la auditoria, mas el del empleado de apellido LOPEZ no quedó registrado. Y se puede observar que la instrucción INSERT complete queda registrada.

Si queremos eliminar la auditoria anterior, ejecutamos:

BEGIN

DBMS\_FGA.DROP\_POLICY( object\_schema =>'USER20' ,

object\_name => 'EMPLEADO',

policy\_name =>'CHK\_HR\_EMP');

END;