Auditoría de Sistemas de Información
Grado en Ingeniería Informática en Sistemas de Información - Curso 2021/2022

PRÁCTICA 2: AUDITORIA EN BBDD ORACLE II

Objetivos

- Auditoría obligatoria y de SYSDBA
- Habilitar la auditoría estándar de la base de datos
- Auditar intentos de conexiones y acceso a objetos de la base de datos
- Buenas prácticas de auditoría

Contenido

1. Auditoría obligatoria (Mandatory auditing) y Auditoría de SYSDBA

Oracle siempre audita ciertas operaciones de la base de datos y las escribe en los ficheros de auditoría del sistema operativo, independientemente de la configuración que se realice del auditado estándar. Esta auditoría obligatoria incluye registros sobre:

- **Arranque y parada de la base de datos.** Un registro de auditoría se crea indicando el usuario del SO que está arrancando/parando la instancia, el identificador terminal y la fecha/hora.
- **SYSDBA y SYSOPER logins.** Se registran todas las conexiones con `SYSDBA` y `SYSOPER`.

Además de la auditoría obligatoria, es posible auditar las operaciones de DELETE, INSERT, UPDATE y MERGE que realizan los usuarios SYS, para lo que habrá que habilitar el parámetro AUDIT_SYS_OPERATIONS. Si las operaciones SYS son auditadas, el parámetro de inicialización AUDIT_FILE_DEST controla la localización de los registros de Auditoría.

- AUDIT_FILE_DEST: especifica la localización del fichero de auditoría en el sistema operativo. Por defecto, en los sistemas Unix/Linux y Windows la ruta por defecto es $ORACLE_BASE/admin/$ORACLE_SID/adump. Además, en Windows se escribe en el visor de eventos del sistema. La ruta debería referirse a un disco local de la máquina donde está instalada la instancia de la base de datos para no perjudicar el rendimiento del sistema.
- AUDIT_SYS_OPERATIONS: habilita la auditoría de operaciones llevadas a cabo por el usuario SYS, así como la de cualquier usuario conectado con privilegios de SYSDBA, SYSOPER. La auditoría es escrita en el fichero de auditoría del sistema operativo o en el indicado en el parámetro AUDIT_FILE_DEST. Este parámetro debería estar a TRUE

Para ver los valores de estos parámetros:

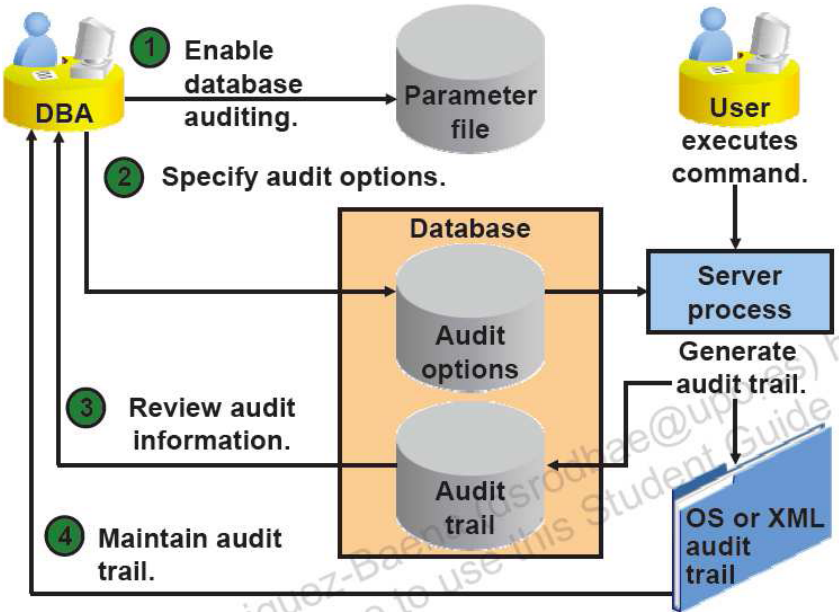
```
SHOW PARAMETER AUDIT_FILE_DEST

SHOW PARAMETER AUDIT_SYS_OPERATIONS
```

2. Auditoría estándar de base de datos Oracle

Además de la auditoría obligatoria, Oracle proporciona un mecanismo de auditoría estándar que se habilita a nivel de sistema mediante el parámetro de inicialización dinámico AUDIT_TRAIL. Este parámetro nos permite indicar el lugar donde se almacenarán los registros de auditoría.

Tras activar el auditado de la base de datos y especificar las opciones de auditado, la base de datos comienza a almacenar información de auditado. Concretamente, la auditoría estándar nos permite auditar sentencias SQL, privilegios, objetos de los distintos esquemas y actividad de la red.



Los posibles valores del parámetro AUDIT_TRAIL:

• **OS**: activa la auditoría de la base de datos, escribiendo los sucesos auditados en la pista de auditoría del sistema operativo. Por defecto, los ficheros de log del sistema operativo se encuentran en el directorio $ORACLE_BASE/admin/$ORACLE_SID/adump, tanto en Unix como en Windows. En sistemas Windows además se escribe en el visor de eventos de Windows. La ruta de estos ficheros es configurable mediante el parámetro AUDIT_FILE_DEST.
• **DB**: activa la auditoría y los datos se almacenarán en la taba SYS.AUD$ de Oracle.
• **DB, EXTENDED**: activa la auditoría y los datos se almacenarán en la taba SYS.AUD$ de Oracle. Además, se escribirán los valores correspondientes en las columnas Sql Text y Sql Bind de la tabla SYS.AUD$, con lo que se recoge la sentencia SQL ejecutada por el usuario y las variables utilizadas por la misma.
• **XML**: activa la auditoría de la base de datos, los sucesos serán escritos en ficheros XML del sistema operativo.
• **XML, EXTENDED**: activa la auditoría de la base de datos, los sucesos será escritos en el formato XML del sistema operativo, además se incluirán los valores de Sql Text y Sql Bind. La vista V$XML_AUDIT_TRAIL nos permite ver todos los ficheros XML situados en ese directorio

```
SHOW PARAMETER AUDIT_TRAIL
```

Cuando Oracle configura la auditoría de la base de datos, las sentencias SQL y privilegios más usados son auditados por defecto. Concretamente:

Privileges Audited by Default		
ALTER ANY PROCEDURE	CREATE ANY LIBRARY	GRANT ANY PRIVILEGE
ALTER ANY TABLE	CREATE ANY PROCEDURE	GRANT ANY ROLE
ALTER DATABASE	CREATE ANY TABLE	DROP ANY PROCEDURE
ALTER PROFILE	CREATE EXTERNAL JOB	DROP ANY TABLE
ALTER SYSTEM	CREATE PUBLIC DATABASE LINK	DROP PROFILE
ALTER USER	CREATE SESSION	DROP USER
AUDIT SYSTEM	CREATE USER	EXEMPT ACCESS POLICY
CREATE ANY JOB	GRANT ANY OBJECT PRIVILEGE	
Statements Audited by Default		
SYSTEM AUDIT BY ACCESS		
ROLE BY ACCESS		

Las distintas opciones de auditoría se configuran mediante el comando AUDIT. El comando NOAUDIT permite eliminar esas configuraciones de auditoría.

Comando AUDIT
El comando AUDIT permite iniciar los tipos de auditoría que a continuación se detallan. Este comando puede funcionar aunque no esté activada la auditoría de la base de datos, pero no dejará constancia hasta que la auditoría esté activada.

Sintaxis:
AUDIT
{ sql_statement_clause | schema_object_clause | NETWORK }
[BY { SESSION | ACCESS }]
[WHENEVER [NOT] SUCCESSFUL] ;

- sql_statement_clause: activa la auditoría para una sentencia SQL concreta.
- schema_object_clause: activa la auditoría para un objeto concreto de la base de datos.
- WHENEVER SUCCESSFUL: activa la auditoría sólo para operaciones e instrucciones SQL en objetos de esquema que se completen con éxito.
- WHENEVER NOT SUCCESSFUL: activa la auditoría sólo para operaciones e instrucciones SQL en objetos de esquema que originen error

.
Puede verse la sintaxis completa en:

https://docs.oracle.com/cd/B19306_01/server.102/b14200/statements_4007.htm

Comando NOAUDIT
El comando NOAUDIT se utiliza para detener la actividad de auditoría que se había activado previamente con AUDIT.

Sintaxis:
NOAUDIT
{ sql_statement_clause | schema_object_clause | NETWORK}
[WHENEVER [NOT] SUCCESSFUL] ;

- sql_statement_clause: detiene la auditoria de una sentencia SQL concreta.
- schema_object_clause: detiene la auditoría para un objeto concreto de la base de datos.
- WHENEVER SUCCESSFUL: detiene la auditoría sólo para operaciones e instrucciones SQL en objetos de esquema que se completen con éxito.
- WHENEVER NOT SUCCESSFUL: detiene la auditoría sólo para operaciones e instrucciones SQL en objetos de esquema que originen error.

Puede verse la sintaxis completa en:

https://docs.oracle.com/cd/B19306_01/server.102/b14200/statements_9017.htm

3. Especificando opciones de auditoría

Auditado de sesiones. Permite auditar todas las conexiones a la base de datos, tanto exitosas como fallidas.

SQL> AUDIT session;

También es posible auditar las sesiones de determinados usuarios:

SQL> AUDIT session by user;

O solo las exitosas o fallidas:

SQL>AUDIT session whenever successful;
SQL>AUDIT session whenever not successful;

Auditados de sentencia SQL. La sentencia mostrada a continuación permite auditar cualquier sentencia de definición de datos (DDL) que afecte a una tabla, incluyendo CREATE TABLE, DROP TABLE, TRUNCATE TABLE. El auditado de sentencias SQL puede ser filtrado por nombre de usuario y/o por éxito o fallo en su ejecución:

```
--Habilitar auditoría
SQL> AUDIT TABLE BY hr WHENEVER NOT SUCCESSFUL;

--Deshabilitar auditoría
SQL> NOAUDIT TABLE BY hr WHENEVER NOT SUCCESSFUL;
```

Auditado de privilegios de sistema. Puede ser utilizado para auditar el ejercicio de algún privilegio de sistema (tal como DROP ANY TABLE). Puede ser filtrado por nombre de usuario y/o por éxito o fallo de la ejecución de la sentencia. Por defecto, el auditado es BY ACCESS. Cada vez que un privilegio de sistema auditado es ejercido, se genera un registro de auditoría. Podemos agrupar estos registros con la cláusula BY SESSION, con lo que sólo se generará un registro por sesión (de esta forma, si un usuario ejecuta varias sentencias UPDATE sobre una tabla sólo se generará un registro por sesión).

```
--Habilitar auditoría
SQL> AUDIT DROP ANY TABLE BY hr BY SESSION;

--Deshabilitar auditoría
SQL> NOAUDIT DROP ANY TABLE BY hr BY SESSION;
```

Auditado de privilegios sobre objetos. Puede ser utilizado para auditar acciones sobre tablas, vistas, procedimientos, secuencias, directorios, y tipos de datos definidos por el usuario. Este tipo de auditoría puede ser filtrada por el éxito o fallo en la ejecución de la sentencia y agrupada por sesión o acceso. A diferencia del auditado anterior, el agrupamiento por defecto es por sesión.

```
--Habilitar auditoría
SQL> AUDIT UPDATE ON hr.employees BY ACCESS;

--Deshabilitar auditoría
SQL> NOAUDIT UPDATE ON hr.employees BY ACCESS;
```

Auditado de red. Puede ser utilizado para auditar errores inesperados en el protocolo de red o errores internos en la capa de red. Los tipos de errores descubiertos por la auditoría de red no son fallos en la conexión, pero pueden tener otras causas posibles como puede ser las relacionadas con la configuración y los procesos de encriptación de la información.

```
SQL>AUDIT network;
```

4. Visualizando la información de auditoría

Oracle proporciona una serie de vistas que contienen toda la información referente a la auditoría. Entre esas vistas podemos destacar:

- ALL_DEF_AUDIT_OPTS: contiene las opciones por defecto de la auditoría de objetos que aplica cuando estos son creados
- DBA_AUDIT_EXISTS: muestra las entradas de auditora producidas por AUDIT NOT EXISTS (esta auditoría registra todas las sentencias SQL que fallan porque el objeto no existe)
- DBA_AUDIT_OBJECT: muestra los registros de auditoría de todos los objetos de la base de datos.
- DBA_AUDIT_SESSION: muestra todos los registros de auditoría referentes a CONNECT y DISCONNECT.
- DBA_AUDIT_STATEMENT: muestra los registros de auditoría para todas las sentencias GRANT, REVOKE, AUDIT, NOAUDIT y ALTER SYSTEM de la base de datos.
- DBA_AUDIT_TRAIL: registros de auditoría estándar
- DBA_OBJ_AUDIT_OPTS: recoge las opciones de auditoría de todos los objetos.

- DBA_PRIV_AUDIT_OPTS: recoge los privilegios del sistema que son auditados actualmente por usuario.
- DBA_STMT_AUDIT_OPTS: recoge las opciones de auditoría del sistema actuales por usuario.

La descripción de las mismas se puede ver en:

http://docs.oracle.com/cd/B28359_01/server.111/b28320/index.htm

5. Buenas prácticas de auditoría

Oracle recomienda estas buenas prácticas a la hora de auditar una Base de Datos:

- Como regla general, diseña la auditoría para recoger la información que necesitas para cumplir con los requerimientos de la auditoría, poniendo el foco en las actividades que causan los mayores problemas de seguridad. Así, auditar cada tabla de la base de datos no es práctico, pero auditar las columnas de las tablas que tienen información sensible si lo es.
- Periódicamente, archiva y limpia los registros de auditoría para no penalizar el rendimiento de la base de datos.

Bibliografía

ORACLE 11GR2 Administration Workshop I Oracle University.

ORACLE DATABASE ONLINE DOCUMENTATION: https://docs.oracle.com/cd/E11882_01/index.htm

ORACLE DATABASE REFERENCE: https://docs.oracle.com/en/database/

Problemas

P1. Desde el SQL Developer usando el usuario AUDITOR, consulte los valores de los parámetros AUDIT_FILE_DEST, AUDIT_SYS_OPERATIONS y AUDIT_TRAIL. Recójalos en el Excel creado en la primera práctica junto al significado y recomendación sobre cada uno.

show parameters;

Cambie el valor de AUDIT_SYS_OPERATIONS a TRUE y el de AUDIT_TRAIL a DB en el caso de que no tengan estos valores.

Tiempo estimado: 5 minutos

P2. Acceda al enlace [ORACLE DATABASE REFERENCE] donde se explica el detalle de las vistas ALL_DEF_AUDIT_OPTS, DBA_AUDIT_EXISTS, DBA_AUDIT_OBJECT, DBA_AUDIT_SESSION, DBA_AUDIT_STATEMENT, DBA_AUDIT_TRAIL, DBA_OBJ_AUDIT_OPTS, DBA_PRIV_AUDIT_OPTS y DBA_STMT_AUDIT_OPTS, para ver la descripción de estas y entender el significado de cada campo.

Tiempo estimado: 30 minutos

P3. Desde el SQL Developer o SQL Plus, habilite la auditoría de sesión. Luego abra una nueva conexión con el usuario HR con una clave errónea. Luego, pruebe a conectarse con la clave correcta. Desde la conexión del usuario AUDITOR compruebe la auditoría de las sesiones. ¿Cómo se diferencian ambos intentos de conexión?

AYUDA: Puede utilizar las siguientes sentencias como BASE para lograr la información pedida:

```
SELECT *
FROM DBA_AUDIT_SESSION
order by timestamp desc;

SELECT *
FROM DBA_AUDIT_TRAIL
order by timestamp desc;
```

CONSEJO1: revisar los distintos campos que contienen las tablas DBA_AUDIT_SESSION y DBA_AUDIT_TRAIL y mostrar sólo aquéllos que resulten de utilidad para este apartado.

CONSEJO2: en SQLplus es posible formatear la salida. Investigar un poco sobre esta posibilidad para facilitar la comprensión de las salidas que nos den las sentencias ejecutadas.

Tiempo estimado: 10 minutos

P4. Desde el SQL Developer o SQL Plus, intente detectar todos los intentos de conexión erróneos realizados en la última semana. ¿Detecta alguna actividad sospechosa? ¿Qué debería reflejar y recomendar en un informe de auditoría al respecto?

```
SELECT *
FROM DBA_AUDIT_SESSION
WHERE ACTION_NAME ='LOGON'
AND NVL(RETURNCODE,0) != 0
AND TIMESTAMP BETWEEN (SYSTIMESTAMP - 7) AND SYSTIMESTAMP
order by timestamp desc;
```

Tiempo estimado: 10 minutos

P5. Consulte las opciones por defecto de auditoría de objetos.

select * from all_def_audit_opts;

Detenga la actividad de auditoría para “alter”, “grant”, “insert”, “update” o “delete”.

NOAUDIT alter, grant, insert, update, delete ON default;

Consulte ahora las opciones por defecto de auditoría de objetos.

Cambie esas opciones para que de ahora en adelante para los objetos creados se registre información siempre que se produzca un “alter”, “grant”, “insert”, “update” o “delete”.

Vuelva a consultar las opciones por defecto. ¿Qué cambios se han producido tras cada ejecución de NOAUDIT/AUDIT?

Tiempo estimado: 5 minutos

P6. Activamos diversas auditorias:

```
AUDIT ALTER TABLE;
AUDIT DELETE ANY TABLE;
AUDIT DROP ANY TABLE;
AUDIT AUDIT SYSTEM;
AUDIT ALL BY HR BY ACCESS;
AUDIT SELECT TABLE, UPDATE TABLE, DELETE TABLE, INSERT TABLE, EXECUTE PROCEDURE BY HR BY ACCESS;
AUDIT SELECT TABLE, DELETE TABLE, UPDATE TABLE, INSERT TABLE BY AUDITOR BY ACCESS;
AUDIT SELECT TABLE, INSERT TABLE, DELETE TABLE, EXECUTE PROCEDURE BY ACCESS WHENEVER NOT SUCCESSFUL;
```

Compruebe las opciones de auditoría activadas:

```
select user_name usuario, audit_option opcion, success, failure
from DBA_STMT_AUDIT_OPTS order by user_name;
```

Luego, desde una conexión con el usuario HR realice ciertas operaciones sobre las tablas. La sesión debe crearse de nuevo.

```
select TABLE_NAME from USER_TABLES order by TABLE_NAME;  --Vemos todas las tablas usuario HR

select * from EMPLOYEES;

select * from COUNTRIES;

insert into COUNTRIES values('ES','Espana',1);

insert into JOB_HISTORY values(114,'01-OCT-2014','10-JAN-2023','AC_MGR',70);

delete from COUNTRIES where COUNTRY_ID='ES';

CREATE TABLE prueba_auditoria
  (CODIGO varchar2(3),
  DESCRIPCION varchar2(20)); --Crear tabla

drop table prueba_auditoria; --Borrar tabla
```

Revise los registros de auditoría creados en DBA_AUDIT_OBJECT como AUDITOR:

```
select * from DBA_AUDIT_OBJECT order by timestamp desc;
```

Compruebe las opciones de auditoría de todos los objetos y los privilegios del sistema que son auditados:

```
select * from DBA_OBJ_AUDIT_OPTS;
```

select * from DBA_PRIV_AUDIT_OPTS;

Tiempo estimado: 15 minutos

P7. Active la auditoría NOT EXISTS e intente realizar una consulta sobre una tabla que no existe. Compruebe los resultados en la vista DBA_AUDIT_EXISTS.

AYUDA: Puede utilizar la siguiente sentencia como BASE para lograr la información pedida:

```
select *
from DBA_AUDIT_EXISTS
order by timestamp desc;
```

CONSEJO1: revisar los distintos campos que contienen las tablas DBA_AUDIT_EXISTS y mostrar sólo aquéllos que resulten de utilidad para este apartado. Formatear la salida para visualizarlo mejor.

Tiempo estimado: 5 minutos

P8. Compruebe el contenido de la vista DBA_AUDIT_STATEMENT. ¿Qué información proporciona?

AYUDA: Puede utilizar la siguiente sentencia como BASE para lograr la información pedida:

```
select *
from DBA_AUDIT_STATEMENT
order by timestamp desc;
```

CONSEJO1: revisar los distintos campos que contienen las tablas DBA_AUDIT_STATEMENT y mostrar sólo aquéllos que resulten de utilidad para este apartado. Formatear la salida para visualizarlo mejor.

Tiempo estimado: 5 minutos

P9. En la BD figura la fecha de comienzo de los trabajadores, así como su cargo. Han detectado que un trabajador en activo figura con un cargo que no le corresponde. ¿Podrías investigar qué ha podido pasar y cuándo? ¿Qué controles han podido fallar?

select * from EMPLOYEES;

Tiempo estimado: 10 minutos