Auditando el uso de la Base de Datos

1. Directrices para Realizar Auditoria 2
   1.1. Decidir si la Pistas de Auditoría es de la Base de Datos ó el Sistema Operativo 2
   1.2. Guardar La Información Auditada y Mantenerla Disponible 3
   1.3. Directrices para Auditar Actividad Sospochesa de la Base de Datos 4
   1.4. Directrices para auditar actividad normal de la base de datos 4
2. ¿Qué información esta contenida en la Pista de Auditoria? 5
   2.1. Información Almacenada en la Pista de Auditoria de la Base de Datos 5
   2.2. Información Almacenada en el Archivo del Sistema Operativo 6
3. Acciones de Auditoria por Defecto 7
4. Auditando Usuarios Administradores 8
5. Administrando la Pista de Auditoria 10
   5.1. Habilitar y deshabilitar la auditoria 10
   5.2. Establecer opciones de auditoria 12
   5.3. Desabilitar opciones de auditoria 21
6. Verificar de Información de la Pista de Auditoria 23

1. Directrices para Realizar Auditoria

1.1. Decidir si la Pistas de Auditoría es de la Base de Datos o el Sistema Operativo

El diccionario de datos de cada base de datos tiene una tabla de nombre **SYS.AUD$**, normalmente llamada **Pista de Auditoria** de la base de datos, diseñada para almacenar entradas de auditoria de instrucciones, privilegios o objetos de esquemas de la base de datos.

Podemos opcionalmente seleccionar guardar la información de auditoria en un archivo del sistema operativo. Si su sistema operativo tiene una **Pista de Auditoria** que guarda los registros de auditoría generados por el sistema operativo, y Oracle está habilitado para escribir a él, podemos optar por dirigir las entradas de auditoría de la base de datos a este archivo. Por ejemplo, el sistema operativo de Windows le permite a Oracle escribir los registros de auditoría como eventos de la aplicación del log eventos.

Considere las ventajas y desventajas de usar la pista de auditoria de la base de datos o del sistema operativo para almacenar los registros de auditoria.

La pista de auditoria de la base de datos ofrece las siguientes ventajas:

- Podemos ver porciones seleccionadas de la pista de auditoria con las vistas predefinidas del diccionario de los datos.
- Podemos usar herramientas de Oracle (como Oracle Reports) para generar reportes de auditoria.

Alternativamente, la pista de auditoría del sistema operativo puede permitirle consolidar los registros de auditoría de múltiples fuentes incluido Oracle y otras aplicaciones. Por consiguiente, examinar la actividad del sistema podría ser más eficaz porque todos los registros de auditoría están en un lugar.

1.2. Guardar La Información Auditada y Mantenerla Disponible

Aunque auditar es relativamente barato, debemos limitar el número de eventos tanto como posible. Esto minimiza el impacto de performance en la ejecución de sentencias que son auditadas, y minimiza el tamaño de la pista de auditoria.

Debemos usar las siguientes pautas cuando diseñe una estrategia de auditoria:

- Evaluar el proposito de la auditoria

  Después de tener una comprensión clara de las razones por auditar, podemos diseñar una estrategia apropiada y evitar auditorias innecesarias.

  Por ejemplo, supongamos que estamos auditando para investigar actividad sospechosa de la base de datos. Esta información por si misma no es muy específica. ¿Qué tipo de actividad sospechosa de la base de datos hemos notado? Una auditoria con un propósito más enfocado podría ser la auditoria de eliminaciones no autorizadas de cualquier tabla de la base de datos. Este propósito reduce el tipo de acción que se audita y el tipo de objeto que es afectado por la actividad sospechosa.

- Auditoria Inteligente

  Debemos auditar el número mínimo de sentencias, usuarios, u objetos requeridos para conseguir la información solicitada. Esto previene que información innecesaria de auditoria desordenar la información significante y el valioso espacio que se consume en el tablespace del SYSTEM. Debemos equilibrar la necesidad de recoger suficiente información de seguridad y la habilidad para almacenarla y procesarla.

  Por ejemplo, si estamos auditando para recoger la información sobre la actividad de la base de datos, debemos determinar exactamente qué tipos de actividades necesitamos hacerle seguimiento, debemos auditar solo las actividades de interés, y sólo auditar para la cantidad de tiempo necesario para recoger la información deseada. No auditar los objetos si sólo estamos interesados en información de I/O lógica de cada sesión.

1.3. Directrices para Auditar Actividad Sospechosa de la Base de Datos

Cuando realizamos auditoria para monitorear actividad sospechosa de la base de datos, debemos usar las siguientes directrices:

- Auditoría general, luego específica.

  Al empezar una auditoria para actividad sospechosa de la base de datos, es común que no mucha información esté disponible a usuarios u objetos específicos del esquema. Por consiguiente, debemos establecer opciones de la auditoría lo más generales al principio. Una vez que la información de auditoría preliminar se graba y se analiza, las opciones de auditoría generales deben deshabilitarse y las opciones de auditoría más específicas deben habilitarse. Este proceso debe continuar hasta que se recoja bastante evidencia para hacer las conclusiones concretas sobre el origen de la actividad sospechosa de la base de datos.

- Proteger la pista de auditoria.

  Al auditar para actividad sospechosa de la base de datos, debemos proteger la pista de auditoría para que la información de la auditoría no pueda agregarse, modificarse, eliminarse a menos que ya se encuentre auditada.

1.4. Directrices para auditar actividad normal de la base de datos

Cuando el propósito para auditar es recoger información sobre una actividad particular de la base de datos, debemos usar las siguientes directrices:

- Auditar solo acciones pertinentes.

  Evitar desordenar la información significante con registros de auditoría inútiles y reducir la cantidad de la pista de auditoría a administrar, sólo audiytar las actividades de base de datos significativa.

- Archivar los registros auditados y limpiar la pista de auditoria.

  Después de que usted ha reunido la información requerida, archive los registros auditados y purge la pista de auditoría de esta información.

2. ¿Qué información está contenida en la Pista de Auditoria?

Oracle puede escribir registros en la pista de auditoria de la base de datos, en un archivo del sistema operativo, o ambos. Esta sección describe la composición de esta información del registro de auditoría.

2.1. Información Almacenada en la Pista de Auditoria de la Base de Datos

La pista de auditoria de la base de datos, almacenada en la tabla **SYS.AUD$**, contiene diferentes tipos de información, dependiendo de los eventos auditados y las opciones de auditoria establecidas. La siguiente información siempre está incluida en cada registro de la pista de auditoria:

- El usuario del sistema operatrivo
- Usuario de Oracle
- El identificador de sesion
- El identificador del terminal
- Nombre del esquema y objeto accedido
- Operación o itento ejecutado
- Codigo de la operación
- Fecha y hora

La pista de auditoria no guarda información sobre cualquier valor de los datos que podrían ser involucrados en la sentencia auditada. Por ejemplo, los valores viejos y nuevos de las filas actualizadas no se guardan cuando una sentencia **UPDATE** es auditada. Sin embargo, este tipo de auditoria especial puede ser ejecutada usando los métodos de auditoria fina.

2.2. Información Almacenada en el Archivo del Sistema Operativo

El archivo del sistema operativo que contiene la pista de auditoría puede contener cualquier de siguiente información:

- Registros de auditoria generados por el sistema operativo
- Registros de la pista de auditoria de la base de datos
- Acciones de la base de datos que siempre se auditan
- Registros de auditoria para usuarios administradores (SYS)

Registros de la pista de auditoria escritos en la pista de auditoria del sistema operativo pueden contener información codificada, pero esta información puede ser decodificada usando tablas del diccionario de datos y mensajes de error como los siguientes:

Información Codificada	Como Decodificarla
Código de Acción	Describe la ejecución de operaciones ó intentos. La tabla del diccionario de datos **AUDIT_ACTIONS** contiene una lista de estos codigos y sus descripciones.
Uso de privilegios	Describe cualquier privilegio del sistema usado para ejecutar la operación. La tabla **SYSTEM_PRIVILEGE_MAP** contiene una lista de estos privilegios y sus descripciones.
Código ejecutado	Describe el resultado de la operación intentada. Operación satisfactoria retorna el valor caro; operación sin éxito retorna el código de error de Oracle que describe por que la operación ha fallado.

3. Acciones de Auditoria por Defecto

Sin tener en cuenta si el base de datos auditada esta habilita, Oracle siempre audita ciertas operaciones y las escribe al archivo de auditoría de sistema operativo. Estos operaciones incluye lo siguiente:

- Conexiones con privilegios de administradores

  Un registro de la auditoría se genera con el usuario del sistema operativo que se conecta a Oracle como SYSOPER o SYSDBA. Esto provee responsabilidad a los usuarios con privilegios administrativos. Una auditoria completa puede habilitarse para estos usuarios como se explicada en **Auditoria de Usuarios Administradores**.

- Inicios de la base de datos

  Un registro de auditoría se genera con el usuario del sistema operativo que inicia la instancia, el identificador del terminal del usuario, la fecha y hora, y si la base de datos auditada fue habilitada o se desactivó. Esto se guarda en la pista de auditoria del sistema operativo por que los registros de auditoría de base de datos no están disponibles hasta después de que el inicio de la base de datos se haya completado satisfactoriamente.

- Paradas de la base de datos

  Un registro de la auditoría se genera con el usuario del sistema operativo que cierra la instancia, el identificador del término del usuario, la fecha y hora.

4. Auditando Usuarios Administradores

Las sesiones para usuarios que conectan como **SYS**, esto incluye a todos los usuarios que conectan como **SYSDBA** o **SYSOPER**, puede auditarse totalmente. Debemos usar el parámetro **AUDIT_SYS_OPERATIONS** para especificar si usuario **SYS** se auditado. Por ejemplo, la siguiente sentencia especifica ese **SYS** será auditado:

```
AUDIT_SYS_OPERATIONS = TRUE
```

FALSE es el valor por defecto, y desactiva la auditoria de SYS.

Todos los registros de auditoría para SYS se graban en el archivo del sistema operativo que contiene la pista de auditoría, y no en SYS.AUD$. Todas las sentencias SQL ejecutadas por SYS se auditan indiscriminadamente y sin tener en cuenta el parámetro AUDIT_TRAIL.

Ejemplo 1

Consideremos la siguiente sesión de SYS:

```
SQL> conn / as sysdba
Connected.

SQL> alter system flush shared_pool;
System altered.

SQL> update scott.emp
  2  set sal = sal - 100;
16 rows updated.
```

Cuando la auditoria de SYS está habilitada, ambos sentencias ALTER SYSTEM y UPDATE son registradas en el archivo de auditoría de sistema operativo como sigue:

```
ACTION : 'CONNECT'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: EGCC\Administrador
CLIENT TERMINAL: EGCC
STATUS: 0

22/10/2004     10:38:00 a.m.  Oracle.sidegcc
Audit trail:
ACTION : 'commit'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: EGCC\Administrador
CLIENT TERMINAL: EGCC
STATUS: 0
```

```
22/10/2004     10:39:45 a.m.  Oracle.sidegcc
Audit trail:
ACTION : 'alter system flush shared_pool'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: EGCC\Administrador
CLIENT TERMINAL: EGCC
STATUS: 0

22/10/2004     10:41:18 a.m.  Oracle.sidegcc
Audit trail:
ACTION : 'update scott.emp set sal = sal - 100'
DATABASE USER: '/'
PRIVILEGE : SYSDBA
CLIENT USER: EGCC\Administrador
CLIENT TERMINAL: EGCC
STATUS: 0
```

Debido a los privilegios de superusuario disponible para usuarios que se conectan como SYSDBA, Oracle recomienda que DBAs raramente usen esta conexión y sólo la usen cuando necesario. El mantenimiento normal del día a día puede realizarse por usuarios que tienen el rol DBA.

5. Administrando la Pista de Auditoria

En esta sección describiremos varios aspectos de la administración de la información de la pista de auditoria, y contiene los siguientes topicos:

- Habilitar y deshabilitar la auditoria
- Establecer opciones de auditoria
- Deshabilitar opciones de auditoria

5.1. Habilitar y deshabilitar la auditoria

Cualquier usuario autorizado de la base de datos pueden establecer opciones de auditoria de sentencias, privilegios, y objetos, pero Oracle no genera registros de auditoria para la pista de auditoria a menos que la base de datos auditada esté habilitada. El administrador de seguridad es normalmente el responsable de controlar la auditoria.

5.1.1. Establecer al parámetro AUDIT_TRAIL

Los valores que puede tomar este parámetro son:

DB	Habilita la auditoria de la base de datos y dirige todos los registros de la auditoría a la pista de auditoria base de datos, salvo registros que siempre se escriben la pista de auditoría de sistema operativo,
OS	Habilita la auditoria de la base de datos y direcciona todos los registros a un archivo del sistema operativo.
NONE	Este es el valor por defecto. Deshabilita la auditoria de la base de datos.

Ejemplo 2

```
SQL> conn / as sysdba;
Connected.

SQL> alter system set audit_trail = DB scope = spfile;
System altered.

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

SQL> startup
ORACLE instance started.

Database mounted.
Database opened.
```

5.1.2. Establecer el parámetro AUDIT_FILE_DEST

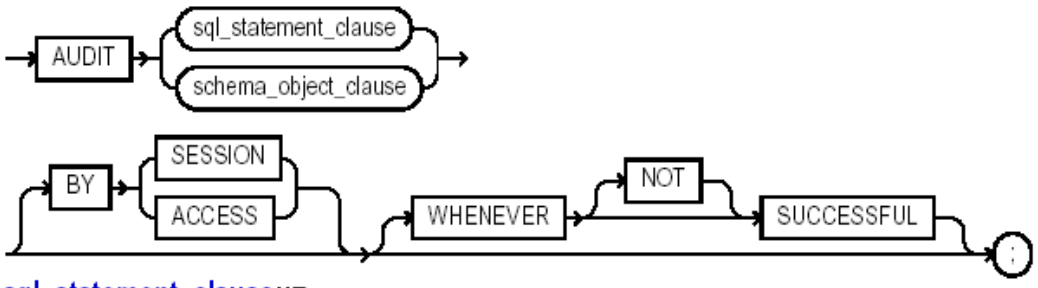
El parámetro AUDIT_FILE_DEST especifica un directorio del sistema operativo en que se grabara la pista de auditoria cuando se establece **AUDIT_TRAIL=OS**. También es la ubicación donde la pista de auditoria obligatoria será grabada y, en el caso especificó de AUDIT_SYS_OPERATIONS, los registros de auditoría para el usuario SYS.

Si el parámetro AUDIT_FILE_DEST no está especificado, el directorio por defecto es $ORACLE_HOME/rdbms/audit.

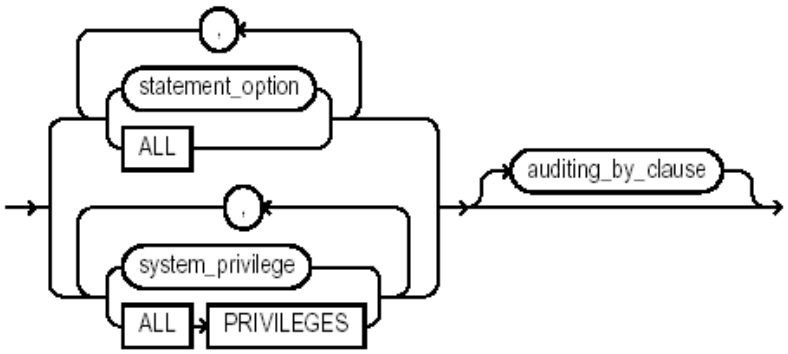
Específicamente para Windows este parámetro no está permitido.

5.2. Establecer opciones de auditoria

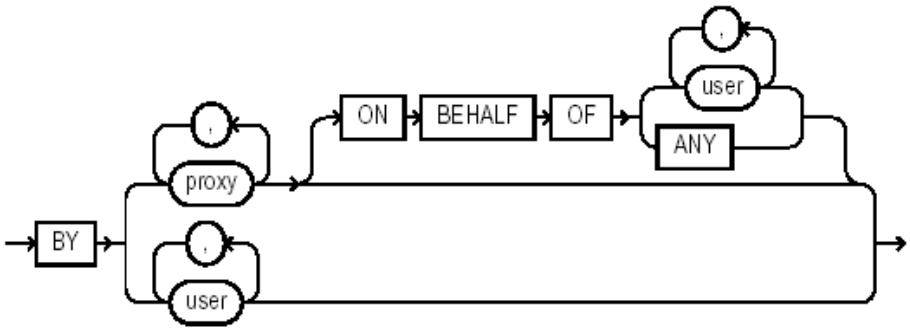
Sintaxis



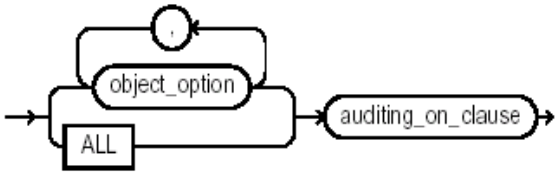
sql_statement_clause::=



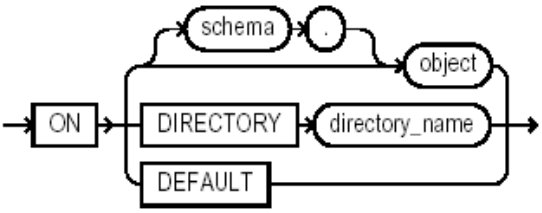
auditing_by_clause::=



schema_object_clause::=



auditing_on_clause::=



Podemos establecer opciones de auditoria con la sentencia **AUDIT**. La sentencia AUDIT permite establecer opciones de auditoria de tres niveles:

Nivel	Efecto
Sentencia	Origina que se auditen las sentencias SQL específicas o grupos de sentencias que afectan a un tipo de objeto específico. Por ejemplo, AUDIT TABLE audita las sentencias CREATE TABLE, TRUNCATE TABLE, COMMENT ON TABLE, y DELETE [FROM] TABLE.
Privilegio	Audita las sentencias SQL que son autorizadas por el privilegio del sistema específico. Por ejemplo, AUDIT CREATE ANY TRIGGER audita las sentencias ejecutadas usando el privilegio del sistema CREATE ANY TRIGGER.
Objeto	Audita sentencias específicas sobre objetos especificos, como ALTER TABLE en la tabla **emp**.

Ejemplo 3

```
SQL> conn / as sysdba
Connected.

SQL> audit select on scott.dept by access;
Audit succeeded.

SQL> conn scott/tiger
Connected.

SQL> select * from dept;

    DEPTNO DNAME          LOC
---------- -------------- -------------
        10 ACCOUNTING     NEW YORK
        20 RESEARCH       DALLAS
        30 SALES          CHICAGO
        40 OPERATIONS     BOSTON

SQL> select username,owner,obj_name,action_name,timestamp
  2  from user_audit_object
  3  where owner = 'SCOTT';

USERNAME        OWNER           OBJ_NAME        ACTION_NAME          TIMESTAM
--------------- --------------- --------------- -------------------- --------
SCOTT           SCOTT           DEPT            SELECT               22/10/04
```

Para usar la sentencia AUDIT es necesario tener el privilegio AUDIT SYSTEM. Para establecer opciones de auditoria sobre objetos, necesitamos ser dueños del objeto o tener el privilegio AUDIT ANY.

Las sentencias de auditoria que establecen opciones de auditoria para sentencias y privilegios pueden incluir la cláusula BY para especificar la lista de usuarios que limitan el alcance de las opciones de auditoria de las sentencias y privilegios.

Ejemplo 4

```
SQL> conn / as sysdba
Connected.

SQL> noaudit all privileges by sergio;
Noaudit succeeded.

SQL> noaudit all on scott.dept;
Noaudit succeeded.

SQL> revoke all on scott.emp from sergio;
Revoke succeeded.

SQL> grant select any table to sergio;
Grant succeeded.

SQL> audit select any table by sergio;
Audit succeeded.

SQL> alter system flush shared_pool;
System altered.

SQL> conn sergio/chino
Connected.

SQL> select * from scott.dept;

    DEPTNO DNAME          LOC
---------- -------------- -------------
        10 ACCOUNTING     NEW YORK
        20 RESEARCH       DALLAS
        30 SALES          CHICAGO
        40 OPERATIONS     BOSTON

SQL> conn / as sysdba
Connected.

SQL> select username,owner,obj_name,action_name,
  2  to_char(timestamp,'dd-mon-yyyy hh24:mi') as fecha
  3  from dba_audit_object
  4  where owner = 'SCOTT';

USERNAME     OWNER        OBJ_NAME     ACTION_NAME     FECHA
------------ ------------ ------------ --------------- -----------------
SERGIO       SCOTT        DEPT         SELECT          23-oct-2004 00:31
```

Cuando establecemos opciones de auditoria tambien podemos establecer las condiciones siguientes:

- BY SESSION / BY ACCESS

  BY SESSION hace que Oracle grabe un solo registro para todas las sentencias SQL del mismo que se ejecutaron en una misma sesión. BY ACCESS hace Oracle grabe un registro por cada acceso.

- WHENEVER SUCCESSFUL / WHENEVER NO SUCCESSFUL

  WHENEVER SUCCESSFUL audita solo sentencias que han tienen exito. WHENEVER NO SUCCESSFUL audita sólo sentencias que no tienen éxito ó que generan errores.

Una nueva sesión de la base de datos recoge las opciones de auditoria desde el diccionario de datos cuando se crea la sesión. Estas opciones permanecen durante todo el tiempo que dure la conexión con la base de datos. Si establecer nuevas opciones de auditoria del sistema u objetos, solo las sesiones subsecuentes podran usarlas; las sesiones existentes continuaran usando las opciones de auditoría en el momento que la sesión fue creada.

Ejemplo 5

Este ejemplo lo desarrollaremos en dos instancias de SQLPLUSW, a las que llamaremos *Instancia 1* e *Instancia 2*.

Instancia 1

```
SQL> conn / as sysdba
Connected.

SQL> noaudit all by sergio;
Noaudit succeeded.

SQL> grant select on scott.dept to sergio;
Grant succeeded.

SQL> grant select on scott.emp to sergio;
Grant succeeded.

SQL> audit select any table
  2  by sergio
  3  by access
  4  whenever successful;

Audit succeeded.
```

Instancia 2

```
SQL> conn sergio/chino
Connected.

SQL> select * from scott.dept;

    DEPTNO DNAME          LOC
---------- -------------- -------------
        10 ACCOUNTING     NEW YORK
        20 RESEARCH       DALLAS
        30 SALES          CHICAGO
        40 OPERATIONS     BOSTON
```

Instancia 1

```
SQL> select username, owner, obj_name, action_name,
  2  to_char(timestamp,'dd-mon-yyyy hh24:mi') as fecha
  3  from dba_audit_object;

USERNAME     OWNER        OBJ_NAME     ACTION_NAME  FECHA
------------ ------------ ------------ ------------ -----------------
SERGIO       SCOTT        DEPT         SELECT       22-oct-2004 17:07

SQL> noaudit all;
Noaudit succeeded.
```

Instancia 2

```
SQL> select count(*) from scott.emp;

  COUNT(*)
----------
        16
```

Instancia 1

```
SQL> select username, owner, obj_name, action_name,
  2  to_char(timestamp,'dd-mon-yyyy hh24:mi') as fecha
  3  from dba_audit_object
  4  order by fecha;

USERNAME     OWNER        OBJ_NAME     ACTION_NAME  FECHA
------------ ------------ ------------ ------------ -----------------
SERGIO       SCOTT        DEPT         SELECT       22-oct-2004 17:07
SERGIO       SCOTT        EMP          SELECT       22-oct-2004 17:25
```

5.2.1. Especificando Auditoria de sentencia

Sintaxis

```
AUDIT {statement_option | ALL}
    [BY user1, user2, … ]
    [BY ACCESS | BY SESSION]
    [WHENEVER [NOT] SUCCESSFUL]
```

Ejemplo 6

Por ejemplo, si utilizamos la opcion TABLE, estaremos auditando las instrucciones CREATE TABLE, DROP TABLE, y TRUNCATE TABLE.

```
SQL> conn / as sysdba
Connected.

SQL> noaudit all by scott;
Noaudit succeeded.

SQL> delete from aud$;
3 rows deleted.

SQL> audit table by scott by access;
Audit succeeded.

SQL> conn scott/tiger
Connected.

SQL> create table test(
  2     id number primary key,
  3     dato varchar2(30) );
Table created.

SQL> drop table test;
Table dropped.
```

Ahora verifiquemos los registros de auditoria creados.

```
SQL> conn / as sysdba
Connected.

SQL> select username, owner, obj_name, action_name,
  2  to_char(timestamp,'dd-mon-yyyy hh24:mi') as fecha
  3  from dba_audit_object
  4  where owner = 'SCOTT'
  5  order by fecha;

USERNAME     OWNER        OBJ_NAME     ACTION_NAME  FECHA
------------ ------------ ------------ ------------ ----------------
SCOTT        SCOTT        TEST         CREATE TABLE 22-oct-2004 19:39
SCOTT        SCOTT        TEST         DROP TABLE   22-oct-2004 19:40
```

Auditando conexiones y Desconexiones

La opción SESSION es única; esta opción genera un solo registro de auditoría para cada sesión creada por las conexiones a una instancia. Un registro de auditoría se inserta en la pista de auditoria en el momento que se conecta y se actualiza cuando se desconecta. La información sobre una sesión como la hora de conexión, la hora de desconexion, y más se guardan en un solo registro de auditoría que corresponde a la sesión.

Ejemplo 7

```
SQL> conn / as sysdba;
Connected.

SQL> noaudit all by scott;
Noaudit succeeded.

SQL> delete from aud$;
74 rows deleted.

SQL> audit session by scott;
Audit succeeded.

SQL> conn scott/tiger
Connected.

SQL> disconnect

SQL> conn / as sysdba;
Connected.

SQL> select username, action_name,
  2  to_char(timestamp,'dd-mon-yyyy hh24:mi') as Inicio,
  3  to_char(logoff_time, 'dd-mon-yyyy hh24:mi') as Fin
  4  from dba_audit_session
  5  where username = 'SCOTT';

USERNAME     ACTION_NAME  INICIO           FIN
------------ ------------ ---------------- ----------------
SCOTT        LOGOFF       22-oct-2004 19:56 22-oct-2004 19:59
```

Auditando sentencias que fallan por que el objeto no existe

La opcion NOT EXISTS permite auditar todas las sentencias SQL que fallan por que el objeto destino no existe.

Ejemplo 8

```
SQL> conn / as sysdba
Connected.

SQL> noaudit all by scott;
Noaudit succeeded.

SQL> delete from aud$;
12 rows deleted.

SQL> audit not exists by scott by access;
Audit succeeded.

SQL> conn scott/tiger
Connected.

SQL> select * from test;
select * from test
              *
ERROR at line 1:
ORA-00942: table or view does not exist

SQL> conn / as sysdba
Connected.

SQL> select username, owner, obj_name, action_name,
  2  to_char(timestamp,'dd-mon-yyyy hh24:mi') as fecha
  3  from dba_audit_object
  4  where owner = 'SCOTT';

USERNAME     OWNER        OBJ_NAME     ACTION_NAME  FECHA
------------ ------------ ------------ ------------ -----------------
SCOTT        SCOTT        TEST         SELECT       22-oct-2004 20:19
```

5.2.2. Especificando Auditoria de Privilegios

Las opciones de auditoría de privilegios son exactamente iguales a los privilegios del sistema. Por ejemplo, la opción para auditar el uso del privilegio DELETE ANY TABLE privilegio es DELETE ANY TABLE.

Sintaxis

```
AUDIT {system_privilege | ALL PRIVILEGES}
    [BY user1, user2, … ]
    [BY ACCESS | BY SESSION]
    [WHENEVER [NOT] SUCCESSFUL]
```

Ejemplo 9

```
SQL> conn / as sysdba;
Connected.

SQL> noaudit all privileges by sergio;
Noaudit succeeded.

SQL> noaudit all on scott.dept;
Noaudit succeeded.

SQL> revoke all on scott.dept from sergio;
Revoke succeeded.

SQL> delete from aud$;
1 row deleted.

SQL> grant insert any table to sergio;
Grant succeeded.

SQL> audit insert any table by sergio by access;
Audit succeeded.

SQL> alter system flush shared_pool;
System altered.
```

Realicemos operaciones como sergio.

```
SQL> conn sergio/chino
Connected.

SQL> insert into scott.dept values(77,'Sistemas','Lima');
1 row created.

SQL> insert into scott.emp(empno,ename)
  2  values(7777,'Maribel');
1 row created.
```

Verifiquemos la pista de auditoria.

```
SQL> conn / as sysdba
Connected.
SQL> select username, owner, obj_name, action_name,
  2  to_char(timestamp,'dd-mon-yyyy hh24:mi') as fecha
  3  from dba_audit_object
  4  where owner = 'SCOTT';

USERNAME     OWNER        OBJ_NAME     ACTION_NAME     FECHA
------------ ------------ ------------ --------------- -----------------
SERGIO       SCOTT        DEPT         INSERT          23-oct-2004 00:53
SERGIO       SCOTT        EMP          INSERT          23-oct-2004 00:54
```

5.2.3. Especificando Auditoria de Objetos

Sintaxis

```
AUDIT {object_option | ALL} ON {DEFAULT | schema.object}
   [BY ACCESS | BY SESSION ]
   [WHENEVER [NOT] SECCESSFUL];
```

Ejemplo 10

Preparemos el ambiente de prueba.

```
SQL> conn / as sysdba;
Connected.

SQL> noaudit all privileges by sergio;
Noaudit succeeded.

SQL> noaudit all on scott.dept;
Noaudit succeeded.

SQL> revoke all on scott.dept from sergio;
Revoke succeeded.

SQL> revoke insert any table from sergio;
Revoke succeeded.

SQL> delete from aud$;
2 rows deleted.

SQL> grant all on scott.dept to sergio;
Grant succeeded.

SQL> audit all on scott.dept by access;
Audit succeeded.
```

Realicemos operaciones como sergio.

```
SQL> conn sergio/chino;
Connected.

SQL> select * from scott.dept;

    DEPTNO DNAME          LOC
---------- -------------- -------------
        10 ACCOUNTING     NEW YORK
        20 RESEARCH       DALLAS
        30 SALES          CHICAGO
        40 OPERATIONS     BOSTON
        77 Sistemas       Lima

SQL> delete from scott.dept where deptno = 77;

1 row deleted.
```

Verifiquemos la pista de auditoria.

```
SQL> conn / as sysdba
Connected.

SQL> select username, owner, obj_name, action_name,
  2  to_char(timestamp,'dd-mon-yyyy hh24:mi') as fecha
  3  from dba_audit_object
  4  where owner = 'SCOTT';

USERNAME     OWNER        OBJ_NAME     ACTION_NAME     FECHA
------------ ------------ ------------ --------------- -----------------
SERGIO       SCOTT        DEPT         SELECT          23-oct-2004 01:32
SERGIO       SCOTT        DEPT         DELETE          23-oct-2004 01:32
```

5.3. Deshabilitar opciones de auditoria

La sentencia NOAUDIT permite deshabilitar las opciones de auditoria que creamos con la sentencia AUDIT.

5.3.1. Deshabilitar Auditoria de Sentencias y Privilegios

Para ejecutar estas tareas necesitamos el privilegio de sistema AUDIT SYSTEM.

Las siguientes sentencias deshabilitan las correspondientes opciones de auditoria:

```
SQL> noaudit session;
Noaudit succeeded.

SQL> noaudit session by scott;
Noaudit succeeded.

SQL> noaudit delete any table;
Noaudit succeeded.

SQL> noaudit select table, insert table, delete table, execute procedure;
Noaudit succeeded.
```

La siguiente sentencia deshabilita todas las opciones de auditoria de sentancias.

```
SQL> noaudit all;
Noaudit succeeded.
```

La siguiente sentencia deshabilita todas las opciones de auditoria de privilegios.

```
SQL> noaudit all privileges;
Noaudit succeeded.
```

5.3.2. Deshabilitar Auditoria de Objetos

Las siguientes sentencias deshabilitan las correspondientes opciones de auditoria.

```
SQL> noaudit delete on scott.emp;
Noaudit succeeded.

SQL> noaudit select, insert, delete on scott.dept;
Noaudit succeeded.
```

Si queremos deshabilitar todas las opciones de auditoria de una tabla, por ejemplo, para la tabla **emp**, debemos ejecutar la siguiente sentencia.

```
SQL> noaudit all on scott.emp;
Noaudit succeeded.
```

6. Verificar de Información de la Pista de Auditoria

Vista	Descripción
STMP_AUDIT_OPTION_MAP	Contiene información sobre tipo de codigo de opciones de auditoria. Creado por el script SQL.BSQ cuando se crea la base de datos.
AUDIT_ACTIONS	Contiene una descripcion para los tipos de codigos de la pista de auditoria.
ALL_DEF_AUDIT_OPTS	Contiene las opciones por defecto de la auditoria de objetos que serán aplicados cuando los objetos son creados.
DBA_STMT_AUDIT_OPTS	Describe las opciones de auditoria actuales del sistema a través del sistema y por usuario.
DBA_PRIV_AUDIT_OPTS	Describe privilegios del sistema actuales que se auditan por el sistema y por el usuario.
DBA_OBJ_AUDIT_OPTS USER_OBJ_AUDIT_OPTS	Describe las opciones de auditoria sobre todos los objetos.
DBA_AUDIT_TRAIL USER_AUDIR_TRAIL	Lista todas las entradas en la pista de auditoria.
DBA_AUDIT_OBJECT USER_AUDIT_OBJECT	Contiene los registros de la pista de auditoria para todos los objetos.
DBA_AUDIT_SESSION USER_AUDIT_SESSION	Lista todos los registros de la pista de auditoria concernientes a CONNECT y DISCONNECT.
DBA_AUDIT_STATEMENT USER_AUDIT_STATEMENT	Lista los registros de la pista de auditoria concernientes a las sentencias GRANT, REKOVE, AUDIT, NOAUDIT, y ALTER SYSTEM.
DBA_AUDIT_EXISTS	Lista las entradas de la pista de auditoria producidas por BY AUDIT NOT EXISTS.