Audit.sys

audit\_trail: Guarda toda la información de todos los usuarios (Absolutamente todo: update, select, delete, insert)



Poner auditoría:

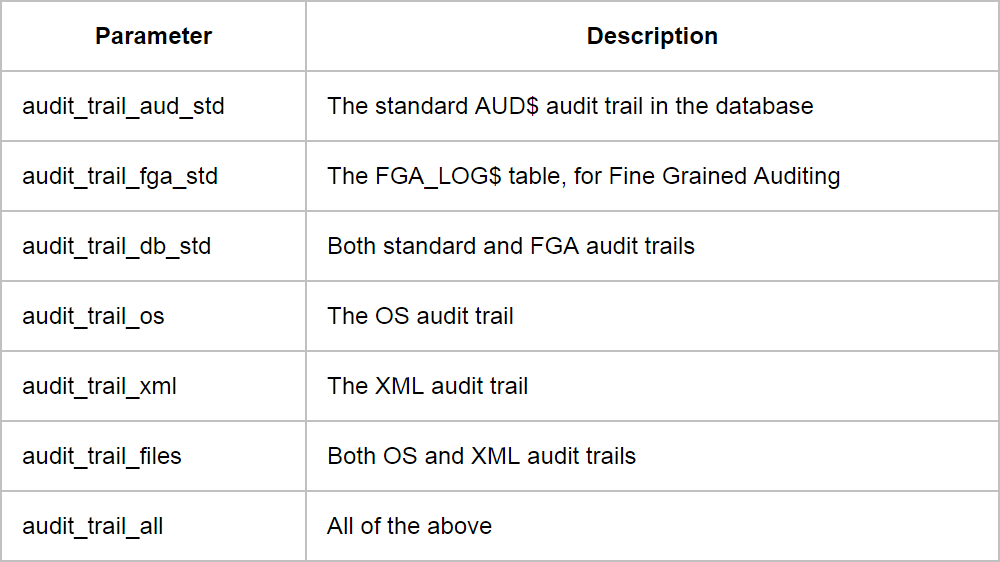
1. Establecer que se desea auditar
2. Actividades de usuarios
3. Sobre esquemas(tablas)
4. Sesiones
5. Granularidad de la información a auditar (más espacio)
6. Poner en auditoría
7. Cambiar el parámetro de auditoria
8. Iniciarla auditoría con sus opiniones
   1. DB, DB extend, OS, XML, …

C.Iniciar el tipo de auditoria

Produce retraso por constante guardado de datos, con el tiempo con datos datos puede sobrepasar la base de datos. Por este motivo se dan cierta cantidad de tablas para este proceso. Cuando se termina hay que limpiar las tablas.

Las bitácoras no guarda selects.

Hacer una aplicación entre a la base cree la auditoría sacar la información de la tabla y con la información generar un reporte, puede enviarlo por pantalla o correo, va a permitir iniciar, parar un auditoria.



Comandos:

show parameters

show parameters audit\_sys\_operations

ALTER SYSTEM SET audit\_sys\_operations=true SCOPE=spfile;

alter system set AUDIT\_TRAIL=db, extended scope=spfile;

SHUTDOWN IMMEDIATE

STARTUP

Que significa auditoria db, OS, db\_extend, XML, XML\_extend, audit\_all?

Cuales son las vistas que se obtienen del audit trail?

SELECT view\_name  
FROM dba\_views  
WHERE view\_name LIKE 'DBA%AUDIT%'  
ORDER BY view\_name;  
  
VIEW\_NAME  
------------------------------  
DBA\_AUDIT\_EXISTS  
DBA\_AUDIT\_OBJECT  
DBA\_AUDIT\_POLICIES  
DBA\_AUDIT\_POLICY\_COLUMNS  
DBA\_AUDIT\_SESSION  
DBA\_AUDIT\_STATEMENT  
DBA\_AUDIT\_TRAIL  
DBA\_COMMON\_AUDIT\_TRAIL  
DBA\_FGA\_AUDIT\_TRAIL  
DBA\_OBJ\_AUDIT\_OPTS  
DBA\_PRIV\_AUDIT\_OPTS  
DBA\_REPAUDIT\_ATTRIBUTE  
DBA\_REPAUDIT\_COLUMN  
DBA\_STMT\_AUDIT\_OPTS

Cómo auditar una sentencia concreta(Juan)?

Cómo auditar las acciones de un usuario?

Practica

1. Establecer el servidor
2. Establecer conexiones al servidor
3. Establecer usuario de auditoria
4. Montar escenario de fraude
   1. T1(a,b,c,d)
   2. U1,U2,U3,U4
   3. Rolet1(select on t1)
   4. U1 <- rolet1
   5. Insert t1 (1,2,3,4)(5,6,7,8)(9,10,11,12)
5. Poner la base en DB extend
6. Iniciar auditoria DML
7. DBA -> update on t1 U3
8. Conectar como U1, hacer consultas
9. Conectar como U3, hacer (7 -> 3)

Quien, que hizo, como lo hizo y si tuvo ayuda

IP: 172.17.112.178