Auditoría de Sistemas de Información
Grado en Ingeniería Informática en Sistemas de Información - Curso 2022/2023

PRÁCTICA 1: AUDITORÍA DE BBDD ORACLE I

Objetivos

- Introducción a la auditoría en un gestor de base de datos Oracle.
- Aspectos de seguridad a evaluar en una base de datos Oracle.
- Obtención de evidencias para evaluar el grado de seguridad de la base de datos Oracle.

Contenido

1. Introducción a la auditoría en un gestor de base de datos Oracle

Las bases de datos son el almacén del recurso más valioso que tienen las empresas, la información. Dentro de los distintos gestores de bases de datos existentes Oracle ocupa un lugar privilegiado como líder mundial en este mercado.

Desde el punto de vista de la auditoría, las bases de datos Oracle proporcionan un amplio conjunto de herramientas de auditoría para seguir la actividad de los usuarios e identificar las tendencias sospechosas, permitiéndonos detectar vulneraciones de la seguridad. La auditoría debe ser enfocada sólo a aquellos eventos que son de interés, ya que auditar todos los elementos y todas las acciones no tiene por qué ser necesario y afecta negativamente al desempeño del sistema.

Dentro de una base de datos Oracle podemos utilizar diversos tipos de auditoría:

- **Mandatory auditing**: todas las bases de datos de Oracle auditan ciertas acciones independientemente de la configuración de las opciones de auditado. La razón es debido a que la base de datos necesita registrar algunas actividades de la base de datos, tales como conexiones realizadas por usuarios privilegiados.

- **Standard database auditing**: se habilita a nivel de sistema mediante el parámetro de inicialización dinámico AUDIT_TRAIL. Tras habilitar el auditado, se seleccionarán los objetos y privilegios que se deseen auditar y se configurarán las opciones de auditado mediante el comando AUDIT.
    - **Value-based auditing**: extiende el auditado estándar, capturando no sólo los eventos auditados que ocurren, sino también los valores existentes antes de ser insertado, actualizado o borrado. El auditado value-based es implementado a través de triggers (disparadores) sobre los objetos de la base de datos (tablas) que permiten llevar un registro de los accesos, modificaciones de valores, eliminación de registros. El desarrollo de estas auditorías corre a cargo de los desarrolladores de las aplicaciones. Consisten fundamentalmente en triggers. Quedan por tanto a la libre elección del desarrollador, que puede apoyarse en herramientas comerciales que le facilitan esta tarea de creación de disparadores.
    - **Fine-grained auditing (FGA)**: extiende el auditado estándar de la base de datos, capturando no sólo el hecho de haber ocurrido el evento auditado, sino también, la sentencia SQL que se ejecutó.

- **Auditado de SYSDBA (y SYSOPER)**: separa las responsabilidades entre un DBA (Data Base Administrator) y un auditor o administrador de seguridad que monitoriza las actividades del DBA.

Además de las herramientas de auditoría que proporciona Oracle, el auditor de Base de datos deberá comprobar otros aspectos que garantizan una correcta implementación de la seguridad en la Base de Datos. Dentro de estos aspectos a considerar, comprobar y evaluar podemos incluir:

- Modo de operación ARCHIVELOG / NOARCHIVELOG (copiar o no copiar redo log files[1])

[1] *La estructura más crucial para las operaciones de recuperación es el redo log file, que consta de dos o más archivos preasignados que almacenan todos los cambios realizados en la base de datos a medida que ocurren.*

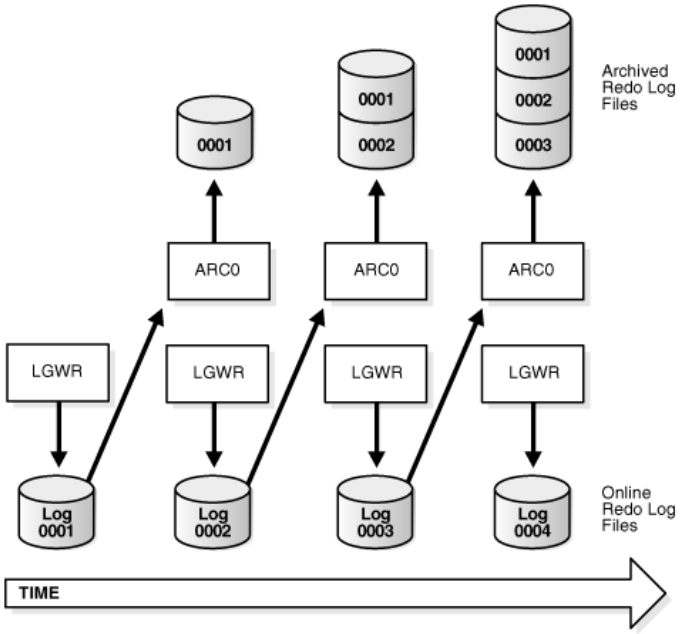
- Aplicación del Principio del Menor Privilegio
  - Protegiendo el diccionario de datos
  - Revocando privilegios PUBLIC innecesarios
  - Limitando a los usuarios con privilegio de administrador
  - Restringiendo autenticación de bases de datos remotas
- Administración de cuentas por defecto
- Implementación de seguridad en las passwords

2. Modo de operación ARCHIVELOG / NOARCHIVELOG

El modo ARCHIVELOG de Oracle es un mecanismo que protege la base de datos ante posibles fallos físicos de disco y también ante eliminaciones o modificaciones no deseadas de los datos. Con este mecanismo tendremos la opción de recuperar la base de datos en un momento específico del tiempo, es decir, se podrá recuperar el estado de la base de datos a una hora y día indicados.

El tratamiento que hace Oracle de las transacciones es el siguiente. Cuando los usuarios realizan modificaciones en la base de datos, Oracle guarda todas las transacciones que se van realizando en unos archivos denominados "archivos de redo log online". Este mecanismo permite reconstruir la información desde el último backup. La escritura en estos archivos es cíclica, de manera que se empieza a escribir en el primer archivo de redo log online, cuando se llena pasa al segundo, y así sucesivamente hasta llegar al último archivo de redo log online, momento en que se inicia un proceso en segundo plano llamado LGWR (Log Writer) que sobrescribe los contenidos del primer archivo de redo log online y así sucesivamente.

Cuando Oracle se ejecuta en modo ARCHIVELOG existe un proceso en segundo plano llamado ARC0 que hace una copia de cada archivo de redo log online una vez que el proceso LGWR termina de escribir en él, guardando dicha copia en los archivos de reconstrucción fuera de línea (redo log offline) en disco. Este proceso puede ralentizar mínimamente la base de datos y, lógicamente, requiere de más espacio en disco para alojar esos archivos.



El auditor debe comprobar si en la Base de datos está activo el modo de operación en ARCHIVELOG o NONARCHIVELOG. Si no está activo, la evidencia de ataque o cambios serán sobrescritos por un nuevo redo.

Se puede determinar realizando una sentencia SQL a la BD:

SQL> SELECT name, log_mode FROM v$database;

3. Principio de menor privilegio

Este principio parte de la premisa de que un usuario sólo debe tener los privilegios mínimos que sean necesarios para llevar a cabo las tareas que tenga asignadas. Esto permite reducir la posibilidad de que usuarios accidentalmente o intencionadamente puedan modificar o ver datos para los cuales no tienen los privilegios respectivos.

Dentro de las acciones que deben llevarse a cabo para cumplir con este principio se incluyen:

- **Proteger el diccionario de datos:** previene que usuarios con privilegio de sistemas ANY TABLE puedan acceder a tablas del diccionario de datos. Además, previene que el usuario SYS (root) se logue con un rol distinto al de SYSDBA (rol administrador BD). El valor adecuado lo indica el parámetro O7_DICTIONARY_ACCESSIBILITY:

  SQL> SELECT name, value FROM v$parameter WHERE UPPER(name)='O7_DICTIONARY_ACCESSIBILITY';

- **Revocar privilegios PUBLIC innecesarios:** eliminar todos los privilegios y roles innecesarios de la base de datos del grupo PUBLIC. La base de datos otorga permisos de ejecución sobre determinados paquetes al rol PUBLIC, lo que permite a cualquier usuario ejecutar esos paquetes. Pueden ser consultados con la siguiente SELECT:

  SQL> SELECT table_name FROM dba_tab_privs WHERE owner='SYS' AND privilege = 'EXECUTE' AND grantee='PUBLIC' and table_name like 'UTL%';

- **Limitar a los usuarios con privilegios de administrador:** los usuarios deben disponer de los mínimos privilegios necesarios para llevar a cabo sus tareas. Por ello, se debe controlar:
  - Los permisos sobre privilegios de Sistemas y Objetos
  - Conexiones privilegiadas SYS, tales como SYSDBA y SYSOPER (rol operador BD)
  - Otros privilegios de tipo DBA, tales como DROP ANY TABLE

  ```
  --Usuarios con rol DBA
  SQL> SELECT grantee FROM dba_role_privs WHERE granted_role = 'DBA'

  --Usuarios con privilegios SYSDBA y SYSOPER
  SQL> SELECT * FROM V$PWFILE_USERS;
  ```

- **Restringir la autenticación de bases de datos remotas:** cuando está habilitada la autenticación externa de usuarios de base de datos esta se delega al sistema remoto. Esto significa que la instancia confía implícitamente que los usuarios han sido autentificados adecuadamente en el cliente PC y no solicita una nueva credencial de autentificación. Los usuarios pueden conectarse a la base de datos sin proveer una password. El nombre del usuario del sistema operativo debe ser el mismo que el de la base de datos para poder ser autentificado externamente. El valor lo indica el parámetro REMOTE_OS_AUTHENT:

  SQL> SELECT name, value FROM v$parameter WHERE UPPER(name) = 'REMOTE_OS_AUTHENT';

4. Administración de cuentas por defecto

Se debe comprobar que todas las cuentas que son creadas a la hora de instalar la base de datos están bloqueadas excepto:

– SYS
– SYSTEM
– SYSMAN
– DBSNMP

El resto de las cuentas son creadas automáticamente en la instalación con las passwords por defecto. Dejarlas desbloqueadas puede permitir el logado de personas no autorizadas a la base de datos. Para obtener un listado de estas cuentas y su estado (suponiendo la fecha de instalación de la base de datos el 31/01/2006):

SQL> SELECT * FROM dba_users WHERE TRUNC(created)= '31/01/2006';

5. Implementación de seguridad de las passwords

En Oracle, la administración de password está implementada a través de los perfiles de usuarios. Estos perfiles permiten especificar ciertas características de seguridad tales como:

- **Account locking:** Habilita el bloqueo automático de cuentas cuando el usuario falla un número especificado de intentos al momento de logarse al sistema.
- **Password aging and expiration:** Habilita a la password de usuario a tener un tiempo de activación o duración, después de dicho periodo la password expira y debe ser cambiada.
- **Password history:** Chequea la nuevas password y verifica que no sean reutilizadas en un periodo de tiempo o hasta alcanzar un número específico de password nuevas.
- **Password complexity verification:** Hace un chequeo de la complejidad de la password y verifica que reúna ciertas características. El chequeo permite que las password sean lo suficientemente complejas para proporcionar mayor protección al sistema.

Parámetros a revisar:

- FAILED_LOGIN_ATTEMPTS: Número de intentos fallidos de conexión antes de bloquearse la cuenta.
- PASSWORD_LOCK_TIME: Número de días que la cuenta está bloqueada después que el número de intentos fallidos se ha superado.
- PASSWORD_LIFE_TIME: Tiempo de validez de la password en días; después de ello, la password expira.
- PASSWORD_GRACE_TIME: Periodo de gracia en días para cambiar la password después del primer intento de sesión y después que la password ha expirado.
- PASSWORD_REUSE_TIME: Especifica que el usuario no puede reusar una password hasta el número de días indicado.
- PASSWORD_REUSE_MAX: Específica el número de password modificadas antes que la password actual pueda ser reutilizada.
- PASSWORD_VERIFY_FUNCTION: Una función PL/SQL que asegura la complejidad de la password es chequeada antes de ser asignada.

Para obtener la información de los perfiles y sus características:

```
--Perfiles de los usuarios
SQL> SELECT USERNAME, PROFILE FROM dba_users ORDER BY 1;

--Carácterísticas de cada perfil
SQL> SELECT * FROM dba_profiles ORDER BY 1;
```

Los valores DEFAULT significan que Oracle usa los valores definidos en el perfil DEFAULT. Por defecto, esos valores están definidos como UNLIMITED en ese perfil.

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. Cree un documento Excel donde ir recopilando toda la información de los distintos apartados. Este documento reunirá todas las evidencias obtenidas y servirá de base para formular nuestra opinión y realizar recomendaciones en un supuesto informe de auditoría. Entre la información que debe incluir está:

- Nombre del auditor
- Datos de la empresa auditada
- Alcance de la auditoría
- Fecha de la auditoría
- Control de las revisiones
- Nombre de la base de datos
- Listado de las evidencias obtenidas

Las credenciales para acceder a la BD son:

Ubuntu:
OSBOXES: Olavide2019
root: oracle
oracle:oracleO

ORACLE SQL DEVELOPER
host: IP del ubuntu
puerto: 1521
SID: XE

usuario sys as sysdba
(pass Oracle_4U)

usuario: auditor
pass: auditor

login: hr
pass: hr

Si accedemos directamente desde Ubuntu abrimos una ventana negra:
C:\> sqlplus
login: sys as sysdba
pass: Oracle_4U

login:auditor
pass: auditor

login: hr
pass: hr

Tiempo estimado: 25 minutos

P2. Entrar en la aplicación SQL Developer usando el usuario AUDITOR. Ya dentro de la aplicación consultar el nombre y modo de operación de la base de datos. Almacenar la información en el Excel.

Tiempo estimado: 5 minutos

P3. Desde el SQL Developer compruebe la protección del diccionario de datos.

Tiempo estimado: 5 minutos

P4. Desde el SQL Developer, saque un listado de los paquetes que puede ejecutar cualquier usuario del sistema. Almacenar la información en el Excel.

Tiempo estimado: 10 minutos

P5. Desde el SQL Developer, saque un listado de los usuarios con rol DBA y con privilegios SYSDBA y SYSOPER. Almacenar la información en el Excel.

Tiempo estimado: 5 minutos

P6. Desde el SQL Developer, comprobar si la autenticación de bases de datos remota esta habilitada. Almacenar la información en el Excel.

Tiempo estimado: 5 minutos

P7. Desde el SQL Developer, compruebe si usuarios que se crearon por defecto en la instalación de la base de datos están desbloqueados. Almacenar la información en el Excel.

Tiempo estimado: 10 minutos

P8. Desde el SQL Developer, liste los distintos perfiles que están creados en la base de datos y sus características en cuanto a la seguridad de las passwords de los usuarios que tienen asignados esos perfiles. Almacenar la información en el Excel.

Tiempo estimado: 15 minutos