

Universidad Mariano Gálvez

Ingeniería en Sistemas

Sexto Semestre

Base de datos

Tema:

TAREA 12



Nombre:

Rudy Jaser Samuel
Castellanos López

Fecha:

10/10/2024

San Benito, Petén

INTRODUCCION

Las auditorías en SQL, especialmente en sistemas de bases de datos como Oracle, son un aspecto fundamental de la gestión de datos y la seguridad. En un entorno donde la información es cada vez más crítica y su protección es prioritaria, las auditorías no solo se convierten en una herramienta de cumplimiento normativo, sino en un medio esencial para garantizar la integridad y la confianza en los sistemas de información.

Desde mi perspectiva, la auditoría proporciona una capa adicional de seguridad que permite a las organizaciones rastrear y analizar la actividad dentro de la base de datos. Esto no solo ayuda a identificar accesos no autorizados o actividades sospechosas, sino que también permite realizar un seguimiento de los cambios en los datos y entender cómo se utilizan los recursos. En un mundo donde las brechas de seguridad y las violaciones de datos son cada vez más comunes, contar con un sistema de auditoría robusto es crucial para la protección de la información sensible.

Además, la auditoría fomenta la transparencia en las operaciones de la base de datos, lo que puede ser valioso tanto para las auditorías internas como para las externas. La capacidad de generar informes detallados sobre quién hizo qué y cuándo puede ser un recurso invaluable en la toma de decisiones y en la resolución de disputas.

AUDITORIA EN ORACLE

La auditoría le permite ver los eventos registrados por el servicio Audit. Puede ver los eventos mediante la consola, la API o los SDK. Puede utilizar datos de eventos para realizar diagnósticos, realizar un seguimiento del uso de recursos, supervisar la conformidad y recopilar eventos relacionados con la seguridad.

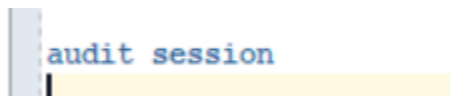
La información de log incluye:

- Hora a la que se ha producido la actividad de API
- Origen de la actividad
- Destino de la actividad
- Tipo de acción
- Tipo de respuesta
- Cambios de estado de recursos
- Mejor seguimiento de las API de larga ejecución
- Solución de problemas relacionados con la información de log

Puede visualizar los logs de auditoría en la consola. Los logs de auditoría se conservan durante 365 días. Si desea conservarlos durante más tiempo, puede exportar los logs de auditoría a un cubo de OCI Object Storage. También puede ingerir logs de auditoría en Oracle Management Cloud o en sistemas de terceros como Splunk. El registro de auditoría se puede ajustar a su estrategia de registro empresarial.

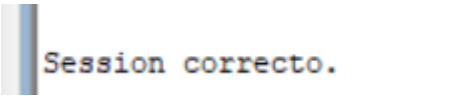
COMO USAR LAS FUNCIONES DE AUDITORIA

Primero activaremos la sesión de auditoria dentro de nuestra base, para este caso usaremos el usuario principal. Pues este tiene todos los permisos necesarios para hacer, la auditoria. En caso sea otro usuario se deberá otorgarle los permisos



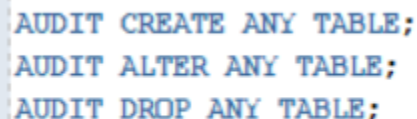
```
audit session
```

Audit Session, nos activa una Sesiones para registrar accesos



```
Session correcto.
```

Podemos de igual manera activar la auditoria para la creacion, alteracion y eliminacion de tablas, tal como se ve en la imagen de al lado.



```
AUDIT CREATE ANY TABLE;  
AUDIT ALTER ANY TABLE;  
AUDIT DROP ANY TABLE;
```

```
SQL> AUDIT SELECT ON HELP;
```

Para auditar el uso de privilegios específicos, como el privilegio de "SELECT": en la tabla HELP para el ejemplo mostrado arriba

```
SQL> SELECT * FROM DBA_AUDIT_TRAIL;
```

Si se desea consultar los servicios de auditoría, luego

de haber activado las mismas, con el comando que se ve en la izquierda se puede realizar, de modo que vera los cambios sacados de la auditoria.

Si se quiere desactivar la auditoria solo se utiliza el comando que se ve abajo:

```
SQL> NOAUDIT ALL BY system;
```

Podemos utilizar las funciones Audit, para guardarlas en trigger, de manera que la auditoria se haga cada vez que se cumpla dicha regla, tal como se ve en la expresión de abajo:

```
CREATE OR REPLACE TRIGGER audit_trigger
AFTER INSERT OR UPDATE OR DELETE ON help
FOR EACH ROW
BEGIN
    INSERT INTO audit_log (username, operation, changed_at)
    VALUES (USER, CASE
        WHEN INSERTING THEN 'INSERT'
        WHEN UPDATING THEN 'UPDATE'
        WHEN DELETING THEN 'DELETE'
    END, SYSDATE);
END;
```

Además de Audit hay otras funciones que pueden servir para auditar la base de datos tales como FGA

FGA permite auditar acciones basadas en condiciones específicas. Por ejemplo, puedes auditar solo las actualizaciones en la tabla empleados donde el salario sea mayor a un cierto valor:

```
BEGIN
    DBMS_FGA.ADD_POLICY(
        object_schema => 'tu_schema',
        object_name    => 'empleados',
        policy_name     => 'salario_policy',
        audit_condition => 'salario > 100000',
        statement_types => 'UPDATE',
        handler_schema  => NULL,
        handler_module  => NULL,
        enable          => TRUE
    );
END;
/
```