INSTITUTO TECNOLOGICO DE ESTUDIOS SUPERIORES DE LOS CABOS

MATERIA:

Taller de base de datos

TRABAJO:

3.1 Reporte Seguridad y tipos de usuarios en diversos SGBD

DOCENTE:

MSC. LILIA UREÑA LUGO

GRUPO:

5ISC01M

ESTUDIANTE(S):

Sanchez Arroyo Edgar

Fecha: 06/10/23

Tipos de usuarios y accesos y roles de los SGBD MySQL, Postgres, Oracle y SQL Server:

Tipos de usuario:

Primero iniciare con los tipos de usuario para el gestor de base de datos e MySQL.

Superusuario:

Este es el usuario el cual posee todos los privilegios y tiene un acceso total a todas las bases de datos y tablas del servidor MySQL en el que se encuentra, este en el sistema posee un nombre por default el cual es root.

Usuario de host especifico:

Como su nombre lo indica es un usuario que está asociado con un host en especifico y puede acceder al servidor solo si ingresa desde ese host

Usuario anónimo:

Es un usuario que no tiene un nombre y una contraseña asociadas, este generalmente es usado para conexiones temporales o par pruebas, pero generalmente no es usado en gran manera.

Usuario de privilegios en específico:

Son usuarios los cuales tienen privilegios limitados, arrancando desde un solo privilegio, o ninguno, los privilegios pueden ser tales como SELECT, INSERT, DELETE, etc., esto par bases de datos o tablas en particular.

Usuarios con privilegios de ejecución de procedimientos almacenados:

Estos son usuarios los cuales tienen permisos en especifico para ejecutar procedimientos ya almacenados en una base de datos.

Usuario de administración de base de datos:

Son usuarios con los privilegios para la creación, modificación y eliminación de bases de datos, tablas, así como también administrar su estructura.

Usuario de solo lectura:

Usuario que solo puede leer, consultar los datos existentes en una base de datos, pero este no puede modificar nada de lo que vea. Es un usuario con privilegios de SELECT.

Accesos(privilegios):

Daré mención a los privilegios u accesos mas relevantes e importantes de conocer de MySQL:

Los accesos no son mas que sentencias que permiten realizar diversas cosas en la base de datos, y estas se usan dentro de los privilegios, ya que dentro de los privilegios le indicamos al sistema que sentencias puede realizar el usuario, es decir que si tiene habilitado solo SELECT, es un usuario que solo puede consultar información, y de igual manera a los usuarios se les puede permitir varias sentencias.

INSERT:

Esta permite realizar inserciones es decir agregar nuevos registros a una tabla en específico, otorgándolo como privilegio al usuario le permitirá realizar INSERT en la tabla en la que tenga el acceso o en la base de datos en la que la tenga.

SELECT:

Esta permite realizar consultas, esto para poder obtener información o datos de una tabla en específico.

UPDATE

Esta es una sentencia la cual permite la modificación de registros ya existentes en una tabla, de igual manera aplicado como privilegio le daríamos al usuario el acceso a la modificación de registros en una tabla.

CREATE

Esta permite crear ya sea nuevas bases de datos o nuevas tablas.

ALTER

Permite el modificar la estructura de una tabla existente, ya sea que queramos agregar algo a la tabla que seria el agregar columnas o el de eliminar columnas.

DROP

Esta es la que permite el eliminar bases de datos o tablas existentes.

INDEX

Permite tanto la creación como la eliminación de índices en una tabla.

GRANT OPTION

Esta sentencia es sumamente importante conocerla ya que es la que permite otorgar los privilegios a los usuarios.

REFERENCES:

Permite la creación de claves foráneas (foreign key) en una tabla.

CREATE TEMPORARY TABLES:

Es la que permite crear tablas temporales.

LOCK TABLES:

Permite bloquear tablas para impedir que otros usuarios accedan a ellas.

CREATE VIEW:

Permite crear vistas que proporcionan una vista virtual de una o más tablas.

SHOW DATABASES:

Permite ver la lista de bases de datos disponibles o que existen dentro del servidor MySQL.

EXECUTE:

Esta es la que permite la ejecución de procedimientos almacenados y funciones definidas por un usuario.

Roles:

Básicamente los roles es algo que podemos crear dentro del sistema gestos al cual le podemos agregar diversos privilegios como a un usuario, pero con el detalle de que no es un usuario, esto sirve como su nombre lo dice para definir roles, y a estos roles ponerles diversos privilegios lo cual ahora el estar poniendo los roles a cada uno de los usuarios, en ese caso solamente se le asignaría el rol al usuario y automáticamente tiene los privilegios previamente puestos al rol.

Creación de un rol:

CREATE ROLE nombre_del_rol;

Asignación de los privilegios:

GRANT SELECT, INSERT ON base_de_datos.tabla TO nombre_del_rol;

Asignación de un rol al usuario:

GRANT nombre_del_rol TO 'usuario'@'host';

Postgres:

Tipos de usuario:

Se tiene que en este sistema gestor PostgreSQL los usuarios y los roles tomas un significado esencialmente igual, el termino rol es usado ampliamente aquí para referirse tanto a los usuarios como a los roles de grupo, estos roles pueden poseer privilegios, y se pueden agrupar otros roles para facilitar el tema de la administración de permisos.

Usuario:

Representa un usuario que puede iniciar sesión en la base de datos.

Rol de Grupo:

Un rol que no puede iniciar sesión y solo se utiliza para agrupar otros roles (usuarios o roles de grupo).

Rol de Superusuario:

Un rol especial con todos los privilegios. El cual Puede realizar cualquier operación en la base de datos.

Rol de Base de Datos:

Es un rol específico de una base de datos. Los privilegios asignados a este rol afectan a la base de datos en particular.

Rol de Conexión:

Un rol que tiene permiso para conectarse a la base de datos, pero puede tener privilegios limitados.

Rol de Creación de Base de Datos:

Este es un rol que puede crear nuevas bases de datos.

Rol de creación de roles:

Este es un rol el cual permitirá la creación de nuevos roles.

Accesos(privilegios):

Muchos de estos privilegios son realmente parecidos al de MySQL aunque en algunos hay ligeras diferencias como veremos a continuación, los que realmente son lo mismo tendrán la misma descripción:

INSERT:

Esta permite realizar inserciones es decir agregar nuevos registros a una tabla en específico, otorgándolo como privilegio al usuario le permitirá realizar INSERT en la tabla en la que tenga el acceso o en la base de datos en la que la tenga.

SELECT:

Esta permite realizar consultas, esto para poder obtener información o datos de una tabla en específico.

UPDATE

Esta es una sentencia la cual permite la modificación de registros ya existentes en una tabla, de igual manera aplicado como privilegio le daríamos al usuario el acceso a la modificación de registros en una tabla.

DELETE:

Permite la eliminación de registros existentes en una tabla.

USAGE:

Esta permite el uso de un objeto en especifico como por ejemplo secuencias, esquema, función etc.

CREATE:

Permite la creación de nuevos objetos las cuales pueden ser por ejemplo tablas, vistas, secuencias entre otras.

CONNECT:

Permite el poder conectarse a una base de datos en específico.

TEMPORARY:

Permite la creación de tablas temporales.

REFERENCES:

Permite crear una clave foránea (foreign key) en una tabla.

EXECUTE:

Permite la ejecución de una función o procedimiento almacenado.

USAGE ON SCHEMA:

Permite el poder usar objetos en un esquema.

ALL PROVILEGES:

Este Concede todos los privilegios disponibles para un objeto.

Roles:

La creación de los roles en este sistema es la siguiente:

Crear un rol:

CREATE ROLE nombre_del_rol;

Crear un rol con contraseña:

CREATE ROLE nombre_del_rol WITH LOGIN PASSWORD 'contraseña';

Asignar privilegios al rol:

GRANT SELECT, INSERT ON tabla TO nombre_del_rol;

Asignar roles al rol:

GRANT nombre_otro_rol TO nombre_del_rol;

Oracle:

Tipos de usuario:

Usuario de Aplicación:

Es un usuario creado para permitir el acceso a una aplicación específica a la base de datos Oracle.

Usuario Nombrado:

Es un usuario individual con un nombre de usuario y una contraseña únicos que pueden conectarse y trabajar en la base de datos Oracle, este es el tipo de usuario más común.

Usuario de Base de Datos:

Es un usuario que se autentica en la base de datos Oracle y puede realizar operaciones dentro de su propio esquema.

Usuario de Acceso Externo:

Es un usuario cuya autenticación y autorización están controladas por un sistema de autenticación externo.

Usuario de Proxy:

Es un usuario que puede actuar en nombre de otro usuario para poder realizar operaciones en la base de datos.

Accesos:

Estos de igual manera son bastante similares algunos a los anteriores ya vistos de los demás gestores.

SELECT:

Este permite la realización de consultas y el poder ver o leer datos de una tabla.

INSERT:

Permite el poder agregar nuevos registros a una tabla.

UPDATE:

Permite modificar registros existentes en una tabla.

DELETE:

Este permite el eliminar registros de una tabla ya existente.

CREATE:

Permite crear objetos en la base de datos, como tablas, vistas, procedimientos almacenados, etc.

ALTER:

Permite modificar la estructura de un objeto existente, como lo podría ser una tabla.

DROP:

Permite eliminar objetos de la base de datos.

GRANT:

Es el que permite otorgar privilegios a otros usuarios o roles.

REVOKE:

Permite revocar privilegios previamente otorgados.

CONNECT:

Permite establecer una conexión a la base de datos.

RESOURCE:

Un privilegio que otorga acceso total a la base de datos y control sobre todos los objetos.

EXECUTE:

Permite ejecutar procedimientos almacenados y funciones.

CREATE SESSION:

Este le permite a un usuario iniciar sesión en la base de datos.

SELECT ANY TABLE:

Este permite consultar cualquier tabla en la base de datos, incluso si el usuario no es el propietario de la tabla.

Roles:

Los roles en este sistema gestor son determinados como un conjunto de privilegios que se pueden asignar ya sea a uno o más usuarios aquí mostrare algunos de los más comunes de Oracle:

DBA:

Role que proporciona privilegios de administrador de base de datos. Incluye acceso total a la base de datos y control sobre todos los objetos.

RESOURCE:

Role que proporciona un conjunto básico de privilegios para crear ciertos tipos de objetos en la base de datos.

CONNECT:

Role que permite a los usuarios conectarse a la base de datos y crear sus propios objetos.

ALTER USER:

Role que permite a los usuarios alterar información de otros usuarios.

SELECT ANY DICTIONARY:

Role que permite a los usuarios consultar cualquier tabla del diccionario de datos.

SQL Server:

Tipos de usuario:

Aquí en los usuarios son entidades de seguridad las cuales están relacionadas, asociadas con un inicio de sesión o login, y estos tienen acceso a una base de datos en específico.

Usuario de SQL Server:

Es un usuario individual con un nombre de usuario y una contraseña únicos asociados a un inicio de sesión en SQL Server. Los usuarios de SQL Server tienen acceso a una base de datos específica y pueden realizar operaciones en ella.

Usuario de Aplicación:

Es un usuario creado para permitir el acceso a una aplicación específica a la base de datos SQL Server.

Usuario de Windows:

Es un usuario de un dominio de Windows que tiene un inicio de sesión (login) en SQL Server asociado a su cuenta de Windows.

Usuario de Base de Datos:

Es un usuario creado dentro de una base de datos específica. Los usuarios de la base de datos tienen acceso a su respectiva base de datos y pueden realizar operaciones dentro de ella.

Accesos:

SELECT:

Este permite el realizar consultas y leer datos de una tabla.

INSERT:

Permite agregar nuevos registros a una tabla.

UPDATE:

Permite modificar registros existentes en una tabla.

DELETE:

Este es el que permite el poder eliminar registros de una tabla.

CREATE TABLE:

Permite crear nuevas tablas en una base de datos.

ALTER TABLE:

Permite modificar la estructura de una tabla ya existente.

DROP TABLE:

Permite eliminar tablas de una base de datos.

CREATE DATABASE:

Permite crear nuevas bases de datos.

ALTER ANY LOGIN:

Permite modificar cualquier inicio de sesión de SQL Server.

VIEW SERVER STATE:

Permite ver el estado del servidor y las sesiones actuales.

EXECUTE:

Permite ejecutar procedimientos almacenados y funciones.

CONNECT SQL:

Permite establecer una conexión con la instancia de SQL Server.

SHUTDOWN:

Permite apagar la instancia de SQL Server.

CREATE VIEW:

Este nos permite crear nuevas vistas las cuales son creadas en base a una tabla.

Roles:

Estos son un conjunto lógico de permisos que se pueden llegar a otorgar a usuarios o grupos de estos, estos permiten simplificar el tema de la administración de permisos al asignar un conjunto de estos, en un conjunto común de usuarios.

db_owner:

Tiene todos los permisos de nivel de base de datos en la base de datos. Puede realizar cualquier operación en la base de datos.

db_datareader:

Tiene permisos para leer cualquier dato en todas las tablas de la base de datos.

db_datawriter:

Tiene permisos para agregar, modificar o eliminar cualquier dato en todas las tablas de la base de datos.

db_ddladmin:

Tiene permisos para realizar operaciones de definición de datos (DDL) en la base de datos, como crear, modificar o eliminar objetos.

db_securityadmin:

Tiene permisos para administrar roles de seguridad y permisos en la base de datos.

db_accessadmin:

Tiene permisos para agregar o quitar accesos a la base de datos para usuarios y grupos de usuarios respectivamente.

db_backupoperator:

Tiene permisos para realizar copias de seguridad de la base de datos en la que se esté trabajando.

db_creator:

Tiene permisos para crear, modificar, eliminar y restaurar cualquier base de datos en el servidor.

¿Qué es seguridad en las bases datos?

Dentro de lo que son las bases de datos, la seguridad hace una referencia al conjunto de medidas que se toman para poder proteger la integridad, confidencialidad y la disponibilidad de la información que se encuentran en las bases de datos. Esta claramente es fundamental para cualquier sistema gestor de bases de datos, esto para poder garantizar que los datos estén protegidos contra accesos no autorizados y también contra usos indebidos dentro del mismo sistema.

Entonces la seguridad en las bases de datos involucra lo que es la confidencialidad es decir el poder garantizar que las personas autorizadas que tengan acceso a la información, y el que los que no lo estén no puedan ver esta información, también la seguridad maneja aspectos de integridad, el cual es el asegurar que los datos se mantengan precisos en todo momento, durante su creación y hasta su eliminación, y otro punto es el de la disponibilidad que esta enlazado con el primero el cual es que los datos estén disponibles para aquellos usuarios que poseen permisos.

Entonces la implementación adecuada del conjunto de políticas de seguridad y el uso de tecnologías de seguridad, son esenciales para poder garantizar la integridad, confidencialidad y disponibilidad de los datos presentes en la base de datos.

¿Cuáles son las amenazas a la seguridad en las bases de datos?

Estos son básicamente potencias vulnerabilidades o ataques que pueden llegar a comprometer lo anterior mencionado, y es fundamental el comprender las amenazas para la correcta implementación de medidas de seguridad.

Dentro de las posibles amenazas podemos tener:

Acceso no autorizado:

Personas no autorizadas intentan acceder a la base de datos para robar información

Inyección de SQL:

Los atacantes insertan código SQL malicioso en las consultas de la aplicación, lo que puede permitirles acceder, modificar o eliminar datos de la base de datos.

Fuga de información:

La información confidencial se divulga inadvertidamente o de forma malintencionada a personas no autorizadas.

Ataques de fuerza bruta:

Los atacantes intentan adivinar contraseñas o claves de acceso probando diferentes combinaciones hasta que logran acceder.

Malware:

Software malicioso diseñado para dañar o acceder de forma no autorizada a la base de datos.

También dentro de las amenazas puede existir el propio error humano.

Y estas solo son algunas.

¿Cuáles son las vulnerabilidades en las bases de datos?

Estas son básicamente fallas en las medidas de seguridad tomadas, o que fueron implementadas dentro de la base de datos, las cuales pueden ser explotadas por amenazas para poder comprometer la integridad de la información al igual que la confidencialidad de esta, puede ser desde fuga de la información por factores externos como usuarios no autorizados, los excesos de privilegios a los usuarios, la ausencia de cifrado en la información, y entre otras, pero en si estas son las vulnerabilidades, un punto en nuestra seguridad que puede ser aprovechado por las amenazas siempre presentes.

Bibliografía:

AndreasWolter. (s/f). Permissions (database engine). Microsoft.com. Recuperado el 7 de octubre de 2023, de https://learn.microsoft.com/en-us/sql/relational-databases/security/permissions-database-engine?view=sql-server-ver15

Database documentation. (2017, diciembre 12). Oracle Help Center. https://docs.oracle.com/en/database/

Documentation. (s/f). Postgresql.org. Recuperado el 7 de octubre de 2023, de https://www.postgresql.org/docs/

GRANT. (2023, septiembre 14). PostgreSQL Documentation. https://www.postgresql.org/docs/current/sql-grant.html

Seguridad de la base de datos: una guía de introducción. (s/f). Ibm.com. Recuperado el 7 de octubre de 2023, de https://www.ibm.com/mx-es/topics/database-security

SQL statements: DROP TABLE to LOCK TABLE. (s/f). Recuperado el 7 de octubre de 2023, de https://docs.oracle.com/en/database/oracle/oracle-database/21/sqlrf/SQL-Statements-DROP-TABLE-to-LOCK-TABLE.html

VanMSFT. (s/f). Database-level roles - SQL Server. Microsoft.com. Recuperado el 7 de octubre de 2023, de https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/database-level-roles?view=sql-server-ver15

(S/f). Mysql.com. Recuperado el 7 de octubre de 2023, de https://dev.mysql.com/doc/refman/8.0/en/