Creación, Gestión de Usuarios y Permisos en MySQL

MySQL es uno de los sistemas de gestión de bases de datos relacionales más utilizados en el mundo. Una parte fundamental de su administración es la **gestión de usuarios y permisos**, la cual garantiza la seguridad y el control de acceso a los datos.

Creación de una Base de Datos

Antes de crear usuarios, es necesario contar con una base de datos a la cual asignarles permisos.

sql

```
CREATE DATABASE wordpress_db;
```

Nota: Es recomendable utilizar nombres descriptivos y, si es posible, seguir una convención de nomenclatura en tu organización.

Creación de Usuarios

Usuario para Conexión Local

Un usuario de conexión local solo puede conectarse desde la misma máquina donde está instalado el servidor MySQL (localhost).

sql

```
CREATE USER 'wordpress_user'@'localhost' IDENTIFIED BY 'Unicatolica2025+';
```

Explicación de los componentes:

Componente	Descripción
wordpress_user	Nombre del usuario.
@'localhost'	Restricción de host: solo permite conexiones desde la máquina local.
IDENTIFIED BY	Define la contraseña del usuario.

Usuario para Conexión Remota

Un usuario remoto puede conectarse desde cualquier dirección IP o máquina externa.

sql

```
CREATE USER 'wp_user' IDENTIFIED BY 'Unicatolica2025+';
```

Importante: Al omitir el host (@'host'), MySQL asigna por defecto @'%', lo que permite conexiones desde **cualquier host**.

Diferencia clave entre usuarios locales y remotos:

Tipo de Usuario	Sintaxis	Alcance de Conexión
Local	'usuario'@'localhost'	Solo desde el servidor local
Remoto	'usuario'@'%' o sin host	Desde cualquier dirección IP

Asignación de Privilegios (GRANT)

Privilegios para el Usuario Local

sql

GRANT ALL PRIVILEGES ON wordpress_db. TO 'wordpress_user'@'localhost';*

Explicación:

Elemento	Significado
ALL PRIVILEGES	Otorga todos los permisos disponibles (SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, etc.).
ON wordpress_db.*	Aplica los permisos a **todas las tablas** dentro de la base de datos wordpress_db.
TO 'wordpress_user'@'localhost'	Usuario destinatario de los privilegios.

Privilegios para el Usuario Remoto

sql

*GRANT ALL PRIVILEGES ON *.* TO 'wp_user'@'%';*

Explicación:

Elemento	Significado
ON *.*	Aplica los permisos a **todas las bases de datos** y **todas las tablas** del servidor.

Elemento	Significado
TO 'wp_user'@'%'	Usuario que puede conectarse desde cualquier host.

> **Advertencia de seguridad:** Otorgar ALL PRIVILEGES ON *.* a un usuario remoto representa un **riesgo de seguridad significativo**. En entornos de producción, se recomienda restringir los privilegios al mínimo necesario (principio del menor privilegio).

Aplicación de Cambios con FLUSH PRIVILEGES

sql

FLUSH PRIVILEGES;

MySQL carga los privilegios en memoria al iniciar. FLUSH PRIVILEGES fuerza a MySQL a **recargar la tabla de permisos** sin necesidad de reiniciar el servidor, asegurando que los cambios recientes se apliquen inmediatamente.

> ***Cuándo usarlo:*** *Después de cualquier operación CREATE USER, GRANT, REVOKE, ALTER USER o DROP USER.*

Verificación de Usuarios Creados

sql

SELECT user, host FROM mysql.user;

Esta consulta muestra todos los usuarios del sistema junto con sus hosts permitidos. Es útil para confirmar que:

- wordpress_user tiene el host localhost.
- wp_user tiene el host % (cualquier host).

Salida esperada:

```
+------------------+-----------+
| user             | host      |
+------------------+-----------+
| root             | localhost |
| wordpress_user   | localhost |
| wp_user          | %         |
+------------------+-----------+
```

Comandos Adicionales de Gestión de Usuarios

Revocar Privilegios

sql

```
REVOKE ALL PRIVILEGES ON wordpress_db.* FROM 'wordpress_user'@'localhost';

FLUSH PRIVILEGES;
```

Eliminar un Usuario

sql

```
DROP USER 'wp_user'@'%';

FLUSH PRIVILEGES;
```

Cambiar la Contraseña de un Usuario

sql

```
ALTER USER 'wordpress_user'@'localhost' IDENTIFIED BY
'NuevaContraseñaSegura2025!';

FLUSH PRIVILEGES;
```

Mostrar los Privilegios de un Usuario Específico

sql

```
SHOW GRANTS FOR 'wordpress_user'@'localhost';
```

Crear un Usuario con Privilegios Limitados (Ejemplo de Mejor Práctica)

sql

```
CREATE USER 'wp_readonly'@'localhost' IDENTIFIED BY 'LecturaSegura2025!';
GRANT SELECT ON wordpress_db.* TO 'wp_readonly'@'localhost';

FLUSH PRIVILEGES;
```

Este usuario solo puede **consultar** datos, no modificarlos. Ideal para reportes o dashboards de solo lectura.

Resumen del Script Completo

sql

```
-- 1. Crear la base de datos
```

```
CREATE DATABASE wordpress_db;

-- 2. Crear usuario para conexión local
CREATE USER 'wordpress_user'@'localhost' IDENTIFIED BY 'Unicatolica2025+';
GRANT ALL PRIVILEGES ON wordpress_db.* TO 'wordpress_user'@'localhost';

-- 3. Crear usuario para conexión remota
CREATE USER 'wp_user' IDENTIFIED BY 'Unicatolica2025+';
GRANT ALL PRIVILEGES ON *.* TO 'wp_user'@'%';

-- 4. Aplicar cambios
FLUSH PRIVILEGES;

-- 5. Verificar usuarios creados
SELECT user, host FROM mysql.user;

-- 6. Salir
EXIT;
```

Buenas Prácticas de Seguridad

Práctica	Descripción
🔐 Contraseñas fuertes	Usa combinaciones de mayúsculas, minúsculas, números y símbolos.
🚫 Menor privilegio	Otorga solo los permisos estrictamente necesarios.
🌐 Restringir hosts remotos	En lugar de @'%', usa IPs específicas como @'192.168.1.100'.
🔄 Rotar contraseñas	Cambia las contraseñas periódicamente.
📋 Auditar usuarios	Revisa regularmente mysql.user para detectar cuentas obsoletas.
🛡️ Firewall	Configura reglas de firewall para limitar el acceso al puerto 3306.

Niveles de Privilegios

MySQL permite asignar privilegios en **cinco niveles de granularidad**, del más amplio al más restrictivo:

- NIVEL GLOBAL → *.*
- NIVEL DE BASE DE DATOS → nombre_db.*
- NIVEL DE TABLA → nombre_db.nombre_tabla
- NIVEL DE COLUMNA → nombre_db.nombre_tabla(columna)
- NIVEL DE RUTINA → nombre_db.nombre_rutina

Sintaxis General

sql

GRANT privilegio1, privilegio2, ... ON nivel TO 'usuario'@'host';

Privilegios de Datos (DML)

Estos privilegios controlan las operaciones sobre los **datos** existentes.

SELECT

Permite leer (consultar) datos de tablas o vistas.

sql

-- Solo lectura en una base de datos específica
GRANT SELECT ON wordpress_db. TO 'lector'@'localhost';*

-- Lectura solo en tablas específicas
GRANT SELECT ON wordpress_db.wp_posts, wordpress_db.wp_users TO 'analista'@'localhost';

-- Lectura solo de columnas específicas
GRANT SELECT (ID, post_title, post_date) ON wordpress_db.wp_posts TO 'reportero'@'localhost';

Uso típico: Usuarios de reportes, dashboards, analistas de datos.

INSERT

Permite agregar nuevas filas a una tabla.

sql

-- Insertar en toda la base de datos
GRANT INSERT ON wordpress_db. TO 'editor_contenido'@'localhost';*

-- Insertar solo en una tabla específica
GRANT INSERT ON wordpress_db.wp_posts TO 'redactor'@'localhost';

```
-- Insertar solo en columnas específicas
GRANT INSERT (post_title, post_content, post_author) ON wordpress_db.wp_posts
TO 'colaborador'@'localhost';
```

UPDATE

Permite modificar datos existentes.

sql

```
-- Actualizar cualquier tabla de la base de datos
GRANT UPDATE ON wordpress_db.* TO 'moderador'@'localhost';

-- Actualizar solo una tabla
GRANT UPDATE ON wordpress_db.wp_users TO 'admin_usuarios'@'localhost';

-- Actualizar solo ciertas columnas (muy útil para seguridad)
GRANT UPDATE (display_name, user_url) ON wordpress_db.wp_users TO
'perfil_editor'@'localhost';
```

Nota de seguridad: Conceder UPDATE sobre columnas como user_pass o user_email puede ser riesgoso. Restríngelo cuando sea posible.

DELETE

Permite eliminar filas de una tabla.

sql

```
-- Eliminar en toda la base de datos
GRANT DELETE ON wordpress_db.* TO 'admin_db'@'localhost';

-- Eliminar solo en tablas de contenido (no en usuarios)
GRANT DELETE ON wordpress_db.wp_posts, wordpress_db.wp_comments TO
'moderador'@'localhost';
```

Precaución: DELETE sin WHERE elimina todas las filas. Considera no otorgarlo a usuarios junior.

Privilegios de Estructura (DDL)

Estos privilegios permiten modificar la **estructura** de la base de datos.

CREATE

Permite crear nuevas bases de datos, tablas, índices o vistas.

sql

```
-- Crear tablas dentro de una base de datos existente
GRANT CREATE ON wordpress_db.* TO 'desarrollador'@'localhost';

-- Crear bases de datos completas (nivel global)
GRANT CREATE ON *.* TO 'dba_junior'@'localhost';

-- Crear vistas dentro de una base de datos
GRANT CREATE VIEW ON wordpress_db.* TO 'analista_vistas'@'localhost';
```

DROP

Permite eliminar bases de datos, tablas o vistas.

```
sql

-- Eliminar tablas dentro de una base de datos
GRANT DROP ON wordpress_db.* TO 'admin_db'@'localhost';

-- ⚠ Nivel global: eliminar CUALQUIER base de datos
GRANT DROP ON *.* TO 'dba_senior'@'localhost';
```

Máxima precaución: DROP es destructivo e irreversible. Úsalo con extrema restricción.

ALTER

Permite modificar la estructura de tablas existentes (agregar/eliminar columnas, cambiar tipos de datos, etc.).

```
sql

-- Modificar estructura de tablas en una base de datos
GRANT ALTER ON wordpress_db.* TO 'desarrollador'@'localhost';
```

INDEX

Permite crear o eliminar índices.

```
sql

-- Gestionar índices para optimizar consultas
GRANT INDEX ON wordpress_db.* TO 'optimizador'@'localhost';
```

CREATE TEMPORARY TABLES

Permite crear tablas temporales (se eliminan al cerrar la sesión).

```
sql

-- Útil para procesos de ETL o análisis complejos
```

GRANT CREATE TEMPORARY TABLES ON wordpress_db. TO 'analista_etl'@'localhost';*

CREATE VIEW

Permite crear vistas (consultas almacenadas que funcionan como tablas virtuales).

sql

GRANT CREATE VIEW ON wordpress_db. TO 'reportes'@'localhost';*

SHOW VIEW

Permite ver la definición (código SQL) de las vistas.

sql

GRANT SHOW VIEW ON wordpress_db. TO 'auditor'@'localhost';*

TRIGGER

Permite crear y eliminar triggers (disparadores automáticos).

sql

GRANT TRIGGER ON wordpress_db. TO 'desarrollador_avanzado'@'localhost';*

EVENT

Permite crear, modificar y eliminar eventos programados (tareas automáticas).

sql

GRANT EVENT ON wordpress_db. TO 'automatizador'@'localhost';*

Privilegios Administrativos

Estos privilegios son de **nivel global** (ON *.*) y afectan todo el servidor.

ALL PRIVILEGES

Otorga **todos los privilegios disponibles** en el nivel especificado.

sql

-- Todos los privilegios sobre una base de datos específica
GRANT ALL PRIVILEGES ON wordpress_db. TO 'admin_wordpress'@'localhost';*

-- Todos los privilegios sobre TODO el servidor (¡superadmin!)
*GRANT ALL PRIVILEGES ON *.* TO 'root_backup'@'localhost';*

GRANT OPTION

Permite al usuario otorgar sus propios privilegios a otros usuarios.

sql

-- Puede dar permisos a otros usuarios sobre wordpress_db
GRANT ALL PRIVILEGES ON wordpress_db. TO 'jefe_proyecto'@'localhost' WITH GRANT OPTION;*

Nota: WITH GRANT OPTION se añade al final del comando GRANT.

4.3 SUPER

Permite realizar operaciones de administración avanzada.

sql

*GRANT SUPER ON *.* TO 'dba'@'localhost';*

Capacidades de SUPER:

- Cambiar variables globales del servidor
- Iniciar/detener replicación
- Matar procesos de otros usuarios (KILL)
- Realizar cambios incluso si read_only está activo

PROCESS

Permite ver los procesos activos de todos los usuarios.

sql

*GRANT PROCESS ON *.* TO 'monitor'@'localhost';*
sql

-- Con este privilegio puede ejecutar:
SHOW PROCESSLIST; -- Ver todas las consultas en ejecución

4.5 RELOAD

Permite recargar tablas de permisos y vaciar logs.

sql

*GRANT RELOAD ON *.* TO 'admin_mantenimiento'@'localhost';*

Comandos habilitados:

- FLUSH PRIVILEGES
- FLUSH TABLES

- FLUSH LOGS
- RESET MASTER

SHUTDOWN

Permite detener el servidor MySQL.

sql

*GRANT SHUTDOWN ON *.* TO 'admin_servidor'@'localhost';*

FILE

Permite leer y escribir archivos en el sistema de archivos del servidor.

sql

*GRANT FILE ON *.* TO 'importador'@'localhost';*

Comandos habilitados:

- LOAD DATA INFILE (importar desde archivos)
- SELECT ... INTO OUTFILE (exportar a archivos)

Riesgo de seguridad: Puede leer archivos sensibles del sistema operativo.

LOCK TABLES

Permite bloquear tablas explícitamente.

sql

GRANT LOCK TABLES ON wordpress_db. TO 'respaldo'@'localhost';*

REPLICATION SLAVE

Permite que un servidor actúe como esclavo en replicación.

sql

*GRANT REPLICATION SLAVE ON *.* TO 'replica'@'192.168.1.50';*

REPLICATION CLIENT

Permite ver información de replicación (SHOW MASTER STATUS, SHOW SLAVE STATUS).

sql

*GRANT REPLICATION CLIENT ON *.* TO 'monitoreo_replica'@'localhost';*

CREATE USER

Permite crear, renombrar y eliminar usuarios.

sql

```
GRANT CREATE USER ON *.* TO 'admin_usuarios'@'localhost';
```

CREATE ROUTINE / ALTER ROUTINE / EXECUTE

Permiten crear, modificar y ejecutar procedimientos almacenados y funciones.

sql

```
-- Crear procedimientos almacenados
GRANT CREATE ROUTINE ON wordpress_db.* TO 'desarrollador'@'localhost';

-- Modificar procedimientos existentes
GRANT ALTER ROUTINE ON wordpress_db.* TO 'desarrollador'@'localhost';

-- Ejecutar procedimientos
GRANT EXECUTE ON wordpress_db.* TO 'aplicacion'@'localhost';
```

Privilegios Especiales

USAGE

No otorga ningún privilegio real. Se usa para crear un usuario sin permisos o modificar atributos.

sql

```
-- Crear usuario sin ningún privilegio
GRANT USAGE ON *.* TO 'usuario_vacio'@'localhost' IDENTIFIED BY 'clave123';

-- Cambiar solo la contraseña sin modificar privilegios
GRANT USAGE ON *.* TO 'wordpress_user'@'localhost' IDENTIFIED BY
'NuevaClave2025!';
```

REFERENCES

Permite crear claves foráneas que referencien tablas.

sql

```
GRANT REFERENCES ON wordpress_db.* TO 'arquitecto_bd'@'localhost';
```

Tabla Resumen Completa

Privilegio	Nivel	Descripción	Riesgo
SELECT	DB/Tabla/ Columna	Leer datos	Bajo
INSERT	DB/Tabla/ Columna	Agregar datos	Medio
UPDATE	DB/Tabla/ Columna	Modificar datos	Medio-Alto
DELETE	DB/Tabla	Eliminar filas	Alto
CREATE	DB/Global	Crear tablas/bases de datos	Medio
DROP	DB/Global	Eliminar tablas/bases de datos	Muy Alto
ALTER	DB/Tabla	Modificar estructura	Medio
INDEX	DB/Tabla	Crear/eliminar índices	Medio
CREATE VIEW	DB	Crear vistas	Bajo
SHOW VIEW	DB	Ver definición de vistas	Bajo
TRIGGER	DB/Tabla	Crear triggers	Medio
EVENT	DB	Crear eventos programados	Medio
CREATE TEMPORARY TABLES	DB	Crear tablas temporales	Bajo
LOCK TABLES	DB	Bloquear tablas	Medio
ALL PRIVILEGES	Cualquiera	Todos los privilegios	Variable
GRANT OPTION	Cualquiera	Delegar permisos	Alto
SUPER	Global	Administración avanzada	Muy Alto
PROCESS	Global	Ver procesos de todos	Medio
RELOAD	Global	Recargar permisos/logs	Medio
SHUTDOWN	Global	Detener servidor	Muy Alto
FILE	Global	Leer/escribir archivos	Muy Alto
REPLICATION SLAVE	Global	Replicación como esclavo	Alto

Privilegio	Nivel	Descripción	Riesgo
REPLICATION CLIENT	Global	Ver estado de replicación	Bajo
CREATE USER	Global	Crear/eliminar usuarios	Muy Alto
CREATE ROUTINE	DB	Crear procedimientos	Medio
ALTER ROUTINE	DB	Modificar procedimientos	Medio
EXECUTE	DB	Ejecutar procedimientos	Medio
REFERENCES	DB/Tabla/ Columna	Crear claves foráneas	Bajo

Ejemplos Prácticos por Escenario

Escenario 1: Usuario de Solo Lectura (Reportero)

sql

```
CREATE USER 'reportero'@'localhost' IDENTIFIED BY 'Rep0rteS3gur0!';
GRANT SELECT ON wordpress_db.* TO 'reportero'@'localhost';

FLUSH PRIVILEGES;
```

Puede hacer:

✅ SELECT cualquier tabla

❌ No puede modificar, crear ni eliminar nada

Escenario 2: Usuario de Aplicación Web (WordPress)

sql

```
CREATE USER 'wp_app'@'localhost' IDENTIFIED BY 'WpApp#2025Secure';
GRANT SELECT, INSERT, UPDATE, DELETE ON wordpress_db.* TO
'wp_app'@'localhost';

FLUSH PRIVILEGES;
```

Puede hacer:

✅ CRUD completo sobre todas las tablas de WordPress

❌ No puede modificar la estructura de la base de datos

Escenario 3: Desarrollador Backend

sql

```
CREATE USER 'dev_backend'@'localhost' IDENTIFIED BY 'Dev#Backend99';
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, ALTER, INDEX,
    CREATE TEMPORARY TABLES, CREATE VIEW, TRIGGER, EVENT
    ON wordpress_db.* TO 'dev_backend'@'localhost';

FLUSH PRIVILEGES;
```

Puede hacer:

- ✅ Todo el CRUD de datos
- ✅ Modificar estructura de tablas
- ✅ Crear vistas, triggers, eventos, índices
- ❌ No puede eliminar la base de datos (DROP)
- ❌ No puede crear usuarios ni administrar el servidor

Escenario 4: Administrador de Base de Datos (DBA)

sql

```
CREATE USER 'dba'@'localhost' IDENTIFIED BY 'DBA#SuperSecure2025!';
GRANT ALL PRIVILEGES ON *.* TO 'dba'@'localhost' WITH GRANT OPTION;

FLUSH PRIVILEGES;
```

Puede hacer:

- ✅ Todo sobre todas las bases de datos
- ✅ Crear/eliminar usuarios
- ✅ Delegar permisos a otros

Escenario 5: Analista de Datos con Acceso Limitado

sql

```
CREATE USER 'analista'@'localhost' IDENTIFIED BY 'Anal1st#Data';

-- Solo puede leer ciertas columnas de ciertas tablas
GRANT SELECT (ID, post_title, post_date, post_status)
   ON wordpress_db.wp_posts TO 'analista'@'localhost';
```

```
GRANT SELECT (ID, user_login, user_registered)
    ON wordpress_db.wp_users TO 'analista'@'localhost';

-- Tablas temporales para análisis complejos
GRANT CREATE TEMPORARY TABLES ON wordpress_db.* TO
'analista'@'localhost';

FLUSH PRIVILEGES;
```

Puede hacer:

- ✅ Ver solo columnas específicas (no ve contraseñas ni emails)
- ✅ Crear tablas temporales para análisis
- ❌ No puede modificar datos reales

Escenario 6: Usuario de Replicación

sql

```
CREATE USER 'replica'@'192.168.1.50' IDENTIFIED BY 'Repl1ca#Binlog';
GRANT REPLICATION SLAVE ON *.* TO 'replica'@'192.168.1.50';
FLUSH PRIVILEGES;
```

Puede hacer:

- ✅ Conectarse como esclavo de replicación
- ❌ No puede leer ni modificar datos directamente

Escenario 7: Usuario de Importación/Exportación

sql

```
CREATE USER 'import_export'@'localhost' IDENTIFIED BY 'Imp0rt#Exp0rt';
GRANT FILE, SELECT, INSERT ON wordpress_db.* TO 'import_export'@'localhost';
FLUSH PRIVILEGES;
```

Puede hacer:

- ✅ LOAD DATA INFILE para importar CSV
- ✅ SELECT ... INTO OUTFILE para exportar resultados
- ✅ Insertar datos importados

Combinaciones Comunes de Privilegios

Permiso Mínimo para una Aplicación

sql

```
GRANT SELECT, INSERT, UPDATE, DELETE ON mi_app.* TO
'app_user'@'localhost';
```

Permiso para Mantenimiento (sin DROP)

sql

```
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, ALTER, INDEX
   ON mi_app.* TO 'mantenimiento'@'localhost';
```

Permiso para Auditoría (solo lectura + vistas)

sql

```
GRANT SELECT, SHOW VIEW ON mi_app.* TO 'auditor'@'localhost';
```

Permiso para Respaldo

sql

```
GRANT SELECT, LOCK TABLES, SHOW VIEW ON *.* TO 'backup_user'@'localhost';
```

Permiso para Migración de Datos

sql

```
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, ALTER, DROP, INDEX,
    CREATE TEMPORARY TABLES, LOCK TABLES, FILE
    ON *.* TO 'migrador'@'localhost';
```

Verificación de Privilegios Asignados

Ver todos los privilegios de un usuario

sql

```
SHOW GRANTS FOR 'wordpress_user'@'localhost';
```

Salida esperada:

```
+-----------------------------------------------------------------+
| Grants for wordpress_user@localhost                             |
+-----------------------------------------------------------------+
```

```
| GRANT USAGE ON *.* TO 'wordpress_user'@'localhost'                |
| GRANT ALL PRIVILEGES ON `wordpress_db`.* TO 'wordpress_user'@'localhost' |
+-------------------------------------------------------------------+
```

Ver privilegios del usuario actual

sql

```
SHOW GRANTS;
-- o
SHOW GRANTS FOR CURRENT_USER();
```

Ver qué usuarios tienen acceso a una base de datos específica

sql

```
SELECT user, host, db, select_priv, insert_priv, update_priv, delete_priv
FROM mysql.db
WHERE db = 'wordpress_db';
```

Revocación Selectiva de Privilegios

Revocar un privilegio específico

sql

```
REVOKE DELETE ON wordpress_db.* FROM 'moderador'@'localhost';
FLUSH PRIVILEGES;
```

Revocar todos los privilegios de una base de datos

sql

```
REVOKE ALL PRIVILEGES ON wordpress_db.* FROM 'desarrollador'@'localhost';
FLUSH PRIVILEGES;
```

Revocar privilegios globales

sql

```
REVOKE SUPER, PROCESS ON *.* FROM 'monitor'@'localhost';
FLUSH PRIVILEGES;
```