



Ministerio de Producción  
Presidencia de la Nación

Ministerio de Educación y Deportes

Subsecretaría de Servicios Tecnológicos y Productivos



Programa  
**111**  
**mil**  
VOS PODÉS  
SER UNO.

**SEGURIDAD**



# Agenda

- Seguridad en Bases de Datos
  - Amenazas
  - Autenticación y Autorización
  - Cifrado de datos
- Mecanismos de seguridad en MySQL
  - Gestión de Usuarios
  - Gestión de Permisos
  - Conexiones seguras en MySQL

# Seguridad en Bases de Datos

- La seguridad de las bases de datos se refiere a la protección frente a **accesos malintencionados**. No es posible la protección absoluta de la base de datos contra el uso malintencionado, pero se puede elevar lo suficiente el coste para quien lo comete como para disuadir la mayor parte, si no la totalidad, de los intentos de tener acceso a la base de datos sin la autorización adecuada
- Los datos guardados en la base de datos deben estar protegidos contra los accesos no autorizados, de la destrucción o alteración malintencionadas además de la introducción accidental de inconsistencias que evitan las restricciones de integridad

# Tipos de Amenazas

- **Pérdida de integridad.** La integridad de la base de datos tiene relación con el requisito a cumplir de que la información se encuentre protegida frente a modificaciones inadecuadas. La modificación de datos incluye la creación, inserción, modificación, cambio del estado de los datos y el borrado. La integridad se pierde si se realizan cambios no autorizados en los datos mediante acciones intencionadas o accidentales.
- **Pérdida de disponibilidad.** La disponibilidad de la base de datos tiene relación con que los objetos estén disponibles para un usuario humano o para un programa que tenga los derechos correspondientes. Hemos analizado técnicas de alta disponibilidad en la sección anterior relacionada con las copias de seguridad.
- **Pérdida de confidencialidad.** La confidencialidad de la base de datos tiene relación con la protección de los datos frente al acceso no autorizado. El acceso no autorizado, no previsto o no intencionado podría tener como resultado la pérdida de la confianza en la organización, el que ésta quede en entredicho o que sea objeto de acciones legales en su contra.

# Niveles de Seguridad

- **Sistema de bases de datos.** Puede que algunos usuarios del sistema de bases de datos sólo estén autorizados a tener acceso a una parte limitada de la base de datos. Puede que otros usuarios estén autorizados a formular consultas pero tengan prohibido modificar los datos. Es responsabilidad del sistema de bases de datos asegurarse de que no se violen estas restricciones de autorización.
- **Sistema operativo.** Independientemente de lo seguro que pueda ser el sistema de bases de datos, la debilidad de la seguridad del sistema operativo puede servir como medio para el acceso no autorizado a la base de datos.
- **Red.** Dado que casi todos los sistemas de bases de datos permiten el acceso remoto mediante terminales o redes, la seguridad en el nivel del software de la red es tan importante como la seguridad física, tanto en Internet como en las redes privadas de las empresas.
- **Físico.** Los sitios que contienen los sistemas informáticos deben estar protegidos físicamente contra la entrada de intrusos.
- **Humano.** Los usuarios deben ser autorizados cuidadosamente para reducir la posibilidad de que alguno de ellos dé acceso a intrusos a cambio de sobornos u otros favores

# Autenticación y Autorización

- Conceptos de suma relevancia en cuanto a seguridad informática en general
- La autenticación es el proceso por el cual se identifica un cliente (persona) como válida para posteriormente acceder a ciertos recursos definidos.
  - Relacionado con la gestión de usuarios y control de acceso al DBMS
- La autorización es el proceso sobre el cual se establecen qué tipos de recursos están permitidos o denegados para cierto usuario o grupo de usuarios concreto.
  - Relacionado con permisos (lectura, escritura) para cada usuario autenticado



# Cifrado de Datos

- El cifrado de datos se utiliza para proteger datos confidenciales como los números de las tarjetas de crédito y contraseñas.
- El cifrado se puede utilizar también para proporcionar protección adicional a partes confidenciales de la base de datos.
- Los datos se codifican utilizando algún algoritmo de codificación o cifrado.
- Un usuario no autorizado que acceda a datos codificados tendrá dificultades para descifrarlos, pero a los usuarios autorizados se les proporcionarán algoritmos de descodificación o descifrado (claves) para descifrar los datos

# Cifrado de Datos: Técnicas comunes

- Características de una buena técnica de cifrado
  - Es relativamente sencillo para los usuarios autorizados cifrar y descifrar los datos.
  - El esquema de cifrado no depende de lo poco conocido que sea el algoritmo, sino más bien de un parámetro del algoritmo denominado clave de cifrado.
  - Es extremadamente difícil para un intruso determinar la clave de cifrado.
- La norma de cifrado de datos (Data Encryption Standard, DES) realiza una sustitución de caracteres y una reordenación de los mismos en función de una clave de cifrado.
  - Para que este esquema funcione los usuarios autorizados deben proveerse de la clave de cifrado mediante un mecanismo seguro
- La norma de cifrado avanzado (Advanced Encryption Standard, AES).
  - Algoritmo Rijndael seleccionado como norma AES en 2000. Nivel significativamente más fuerte de seguridad y su facilidad relativa de implementación en los sistemas informáticos actuales, así como en dispositivos como tarjetas inteligentes





# Cifrado de Datos: Técnicas comunes

- El cifrado de clave pública es un esquema alternativo que evita parte de los problemas que se afrontan con DES. Se basa en dos claves; una clave pública y una clave privada. Cada usuario  $U_i$  tiene una clave pública  $C_i$  y una clave privada  $D_i$ . Todas las claves públicas están publicadas: cualquiera puede verlas. Cada clave privada sólo la conoce el usuario al que pertenece.
- Si el usuario  $U_1$  desea guardar datos cifrados, los cifra utilizando la clave pública  $C_1$ . Descifrarlos requiere la clave privada  $D_1$ . Como la clave de cifrado de cada usuario es pública es posible intercambiar información de manera segura utilizando este esquema. Si el usuario  $U_1$  desea compartir los datos con  $U_2$  los codifica utilizando  $E_2$ , la clave pública de  $U_2$ . Dado que sólo el usuario  $U_2$  conoce la manera de descifrar los datos, la información se transmite de manera segura.
- Para que el cifrado de clave pública funcione debe haber un esquema de cifrado que pueda hacerse público sin permitir a la gente descubrir el esquema de descifrado. En otros términos, debe ser difícil deducir la clave privada dada la clave pública.

# Mecanismos de Seguridad (MySQL)

- Administración de cuentas de usuarios
  - Creación, modificación y borrado de cuentas de usuario
- Gestión de permisos
  - Otorgamiento, Modificación y Revocación de privilegios
- Conexiones seguras
  - Tipos de conexiones y soporte para SSL

# Administración de usuarios (MySQL)

- Un usuario MySQL se define en términos de un nombre de usuario, el equipo o equipos desde los que el usuario puede conectar al servidor y una contraseña/password.
- Por defecto, el motor de base de datos crea un usuario con permisos para todas las tablas de la base de datos
  - El superusuario se denomina root
  - Se recomienda limitar su uso a la gestión del DBMS y no usarlo en aplicaciones de producción.

# Administración de usuarios (MySQL)

## Consideraciones:

- Los nombres de usuarios en MySQL pueden tener como máximo 16 caracteres de longitud.
- Las contraseñas MySQL no están relacionadas con las contraseñas para ingresar en el sistema operativo. No hay una conexión necesaria entre la contraseña que se usa para iniciar sesión en una máquina Windows o Unix y la contraseña usada para acceder al servidor MySQL en la misma computadora.
- MySQL encripta contraseñas usando su propio algoritmo. Esta encriptación es diferente de la usada durante el proceso de logueo de Unix y es la misma que la implementada en la función `PASSWORD()`.

# Creación de usuarios (MySQL)

```
CREATE USER 'nombre_usuario'@'host' IDENTIFIED BY  
'tu_contrasena';
```

- Seguido al nombre de usuario, se debe especificar la IP desde donde podrá realizar conexiones a la base de datos el usuario creado
  - 'localhost' o '127.0.0.1', desde la misma PC en la que se encuentre instalado MySQL, es decir el host local.
  - '192.168.1.100', sólo permite conexiones desde dicha IP (utilizada para identificar a un PC en un LAN)
  - '%' es un comodín que permite conexiones desde cualquier IP

# Niveles de privilegios (MySQL)

En MySQL existen cinco niveles distintos de privilegios:

- **Globales:** se aplican al conjunto de todas las bases de datos en un servidor. Es el nivel más alto de privilegio, en el sentido de que su ámbito es el más general.
- **De base de datos:** se refieren a bases de datos individuales, y por extensión, a todos los objetos que contiene cada base de datos.
- **De tabla:** se aplican a tablas individuales, y por lo tanto, a todas las columnas de esas tabla.
- **De columna:** se aplican a una columna en una tabla concreta.
- **De rutina:** se aplican a los procedimientos almacenados.

# Conceder privilegios a usuarios (MySQL)

```
GRANT [permiso] ON [nombre de bases de datos].  
[nombre de tabla] TO  
'[nombre de usuario]@'host';
```

- Tipos de Permisos

- ALL PRIVILEGES: esta opción otorga todos los permisos.
- CREATE: permite crear nuevas tablas o bases de datos.
- DROP: permite eliminar tablas o bases de datos.
- DELETE: permite eliminar registros de tablas.
- INSERT: permite insertar registros en tablas.
- SELECT: permite leer registros en las tablas.
- UPDATE: permite actualizar registros seleccionados en tablas.
- GRANT OPTION: permite otorgar o remover privilegios a otros usuarios usuarios.



# Revocar privilegios a usuarios (MySQL)

```
REVOKE [permisos] ON [nombre de base de datos]  
.[nombre de tabla] FROM '[nombre de usuario]'  
@'host';
```

Una vez que se haya finalizado con la configuración de privilegios (GRANT o REVOKE) se deben refrescar todos los con el comando:

```
FLUSH PRIVILEGES;
```



# Ejemplos de privilegios (MySQL)

```
GRANT ALL ON midb.usuarios TO 'juan'@'%'  
WITH GRANT OPTION;
```

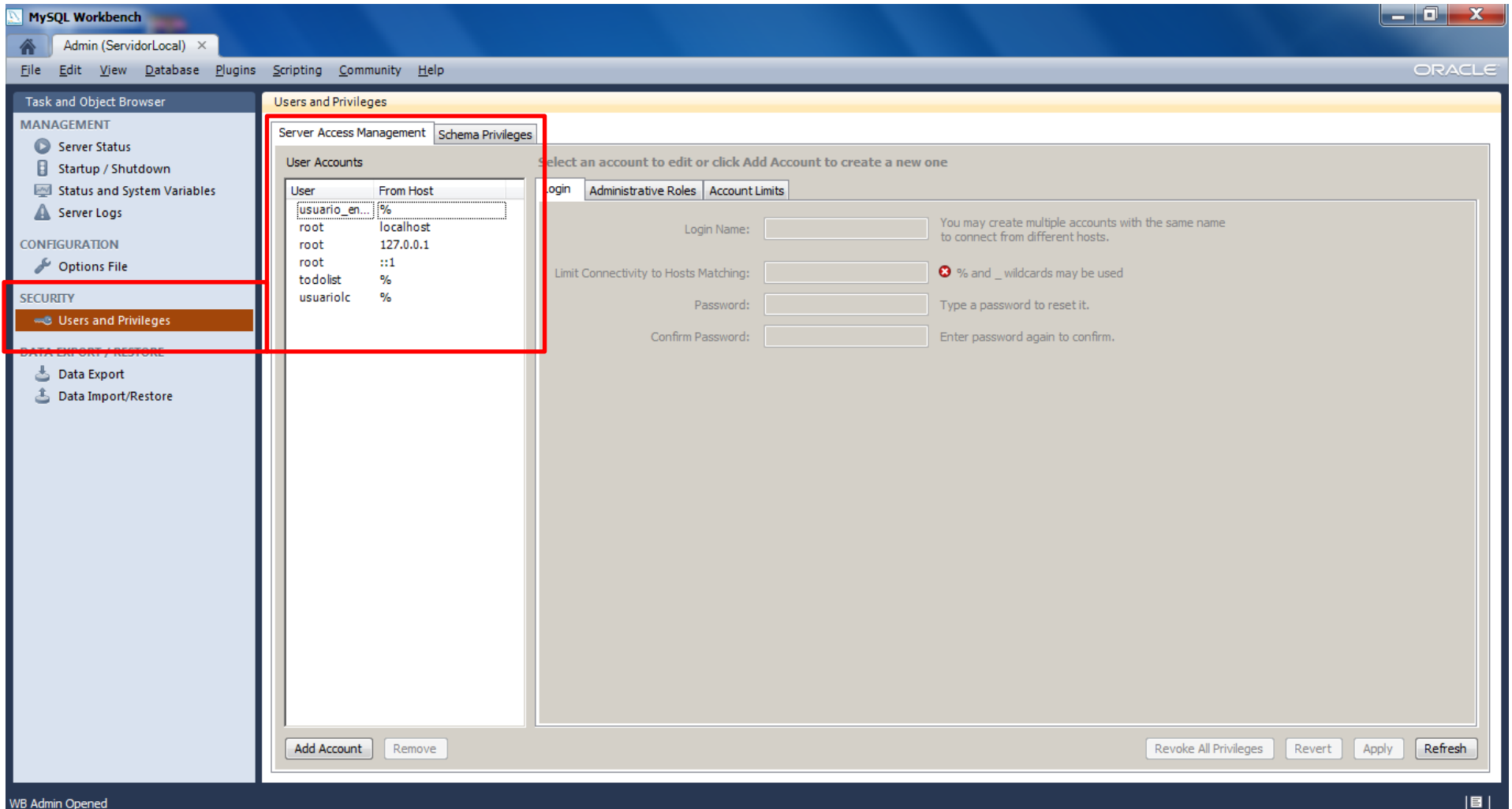
```
GRANT ALL ON midb.* TO 'admin'@'%' ;
```

```
GRANT SELECT ON midb.log TO  
'auditor'@'192.168.1.100' ;
```

```
REVOKE ALL ON midb.* TO 'admin'@'%' ;
```

```
FLUSH PRIVILEGES;
```

# Gestión de usuarios en MySQL Workbench

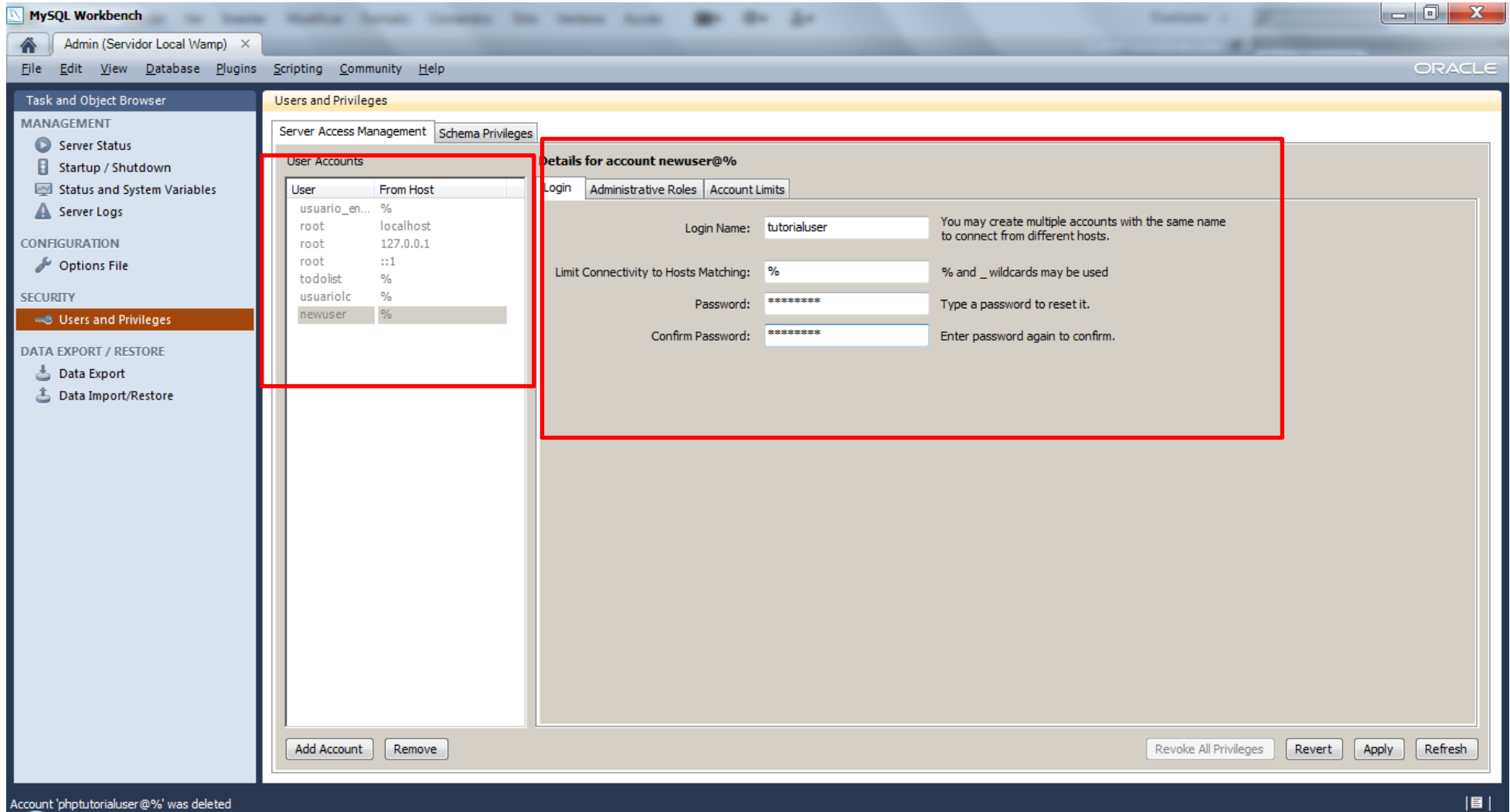


The screenshot shows the MySQL Workbench interface with the 'Users and Privileges' window open. The 'User Accounts' table is highlighted with a red box, showing the following data:

User	From Host
usuario_en...	%
root	localhost
root	127.0.0.1
root	:::1
todolist	%
usuariolc	%

The 'Users and Privileges' window also includes tabs for 'Login', 'Administrative Roles', and 'Account Limits'. The 'Login' tab is currently selected, showing fields for 'Login Name', 'Limit Connectivity to Hosts Matching', 'Password', and 'Confirm Password'. The 'Add Account' button is visible at the bottom left of the window.

# Gestión de usuarios en MySQL Workbench (2)



MySQL Workbench

Admin (Servidor Local Wamp) x

File Edit View Database Plugins Scripting Community Help

ORACLE

Task and Object Browser

MANAGEMENT

- Server Status
- Startup / Shutdown
- Status and System Variables
- Server Logs

CONFIGURATION

- Options File

SECURITY

- Users and Privileges**

DATA EXPORT / RESTORE

- Data Export
- Data Import/Restore

Users and Privileges

Server Access Management Schema Privileges

User Accounts

User	From Host
usuario_en...	%
root	localhost
root	127.0.0.1
root	:::1
todolist	%
usuariolc	%
newuser	%

Details for account newuser@%

Login Administrative Roles Account Limits

Login Name: tutorialuser You may create multiple accounts with the same name to connect from different hosts.

Limit Connectivity to Hosts Matching: % % and \_ wildcards may be used

Password: \*\*\*\*\* Type a password to reset it.

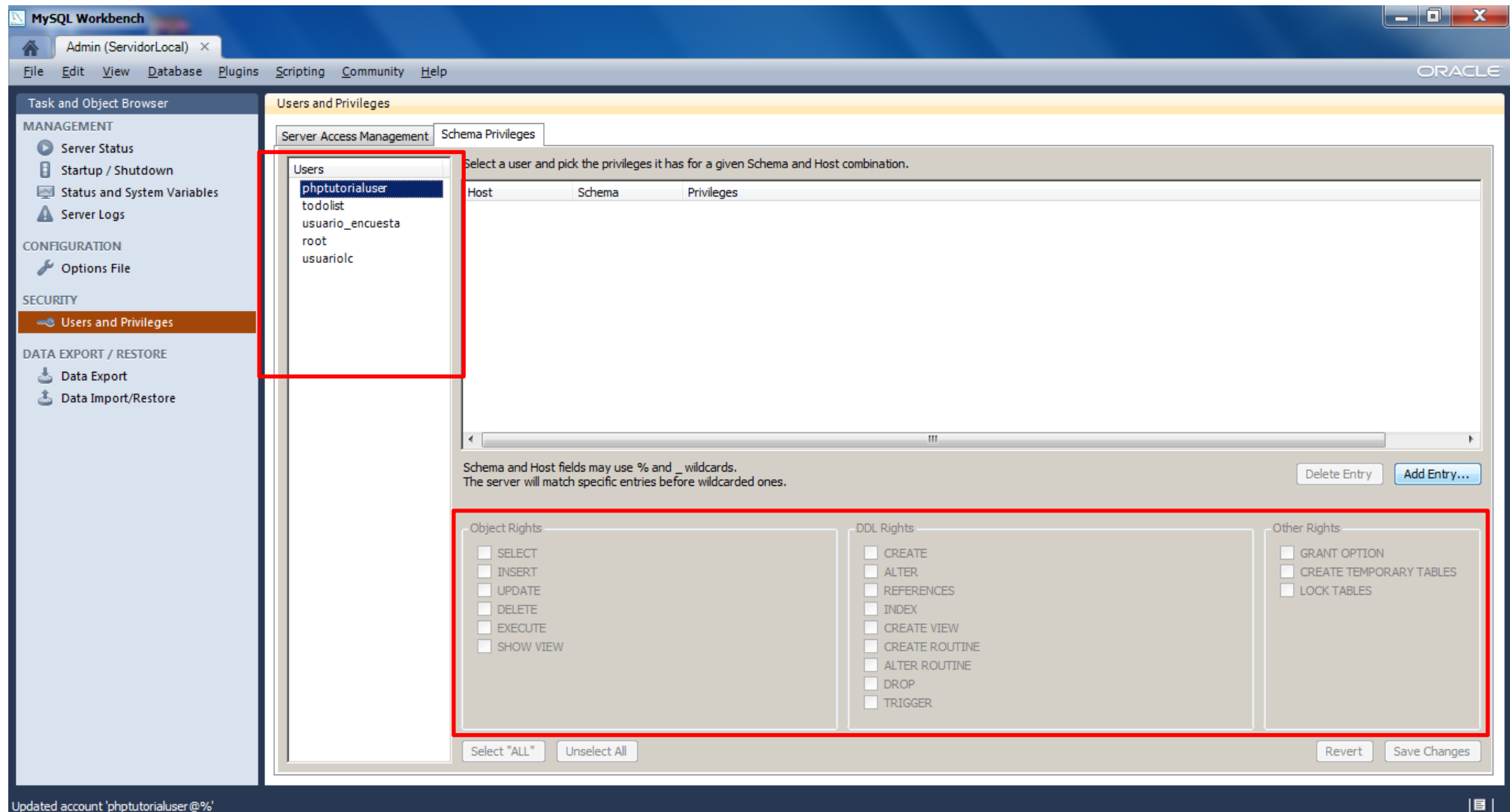
Confirm Password: \*\*\*\*\* Enter password again to confirm.

Add Account Remove

Revoke All Privileges Revert Apply Refresh

Account 'phptutorialuser@%' was deleted

# Gestión de usuarios en MySQL Workbench (3)



The screenshot shows the MySQL Workbench interface with the 'Users and Privileges' window open. The 'Server Access Management' tab is selected. In the 'Users' list on the left, 'phptutorialuser' is highlighted. The main area shows a table with columns 'Host', 'Schema', and 'Privileges'. Below the table, there are three sections for assigning rights: 'Object Rights', 'DDL Rights', and 'Other Rights'. Each section contains a list of permissions with checkboxes. The 'Object Rights' section includes SELECT, INSERT, UPDATE, DELETE, EXECUTE, and SHOW VIEW. The 'DDL Rights' section includes CREATE, ALTER, REFERENCES, INDEX, CREATE VIEW, CREATE ROUTINE, ALTER ROUTINE, DROP, and TRIGGER. The 'Other Rights' section includes GRANT OPTION, CREATE TEMPORARY TABLES, and LOCK TABLES. At the bottom, there are buttons for 'Select "ALL"', 'Unselect All', 'Revert', and 'Save Changes'.

MySQL Workbench

Admin (ServidorLocal) x

File Edit View Database Plugins Scripting Community Help

Task and Object Browser

MANAGEMENT

- Server Status
- Startup / Shutdown
- Status and System Variables
- Server Logs

CONFIGURATION

- Options File

SECURITY

- Users and Privileges**

DATA EXPORT / RESTORE

- Data Export
- Data Import/Restore

Users and Privileges

Server Access Management Schema Privileges

Select a user and pick the privileges it has for a given Schema and Host combination.

Host	Schema	Privileges
------	--------	------------

Schema and Host fields may use % and \_ wildcards.  
The server will match specific entries before wildcarded ones.

Delete Entry Add Entry...

Object Rights

- ☐ SELECT
- ☐ INSERT
- ☐ UPDATE
- ☐ DELETE
- ☐ EXECUTE
- ☐ SHOW VIEW

DDL Rights

- ☐ CREATE
- ☐ ALTER
- ☐ REFERENCES
- ☐ INDEX
- ☐ CREATE VIEW
- ☐ CREATE ROUTINE
- ☐ ALTER ROUTINE
- ☐ DROP
- ☐ TRIGGER

Other Rights

- ☐ GRANT OPTION
- ☐ CREATE TEMPORARY TABLES
- ☐ LOCK TABLES

Select "ALL" Unselect All

Revert Save Changes

Updated account 'phptutorialuser'@%'

# Conexiones Seguras (MySQL)

- Concepto de cliente - servidor
  - Servidor: unidad de proceso donde se ejecuta el servidor
  - Cliente: dispositivo desde donde se consulta al servidor
    - Línea de consola
    - Cliente como MySQL Workbench
    - Aplicación móvil / web
- Tipos de conexiones
  - Local: localhost, servidor y cliente en mismo equipo
  - LAN: red local
  - Internet/Remota: diferentes ubicaciones geográfica, es recomendable asegurar la conexión

# Conexiones Seguras: riesgos (MySQL)

- El cifrado es la forma en la que MySQL protege las conexiones de datos.
- Por defecto, MySQL no usa conexiones cifradas en pos de la rapidez de la transferencia.
  - Cifrar datos es una operación que requiere un uso intensivo de CPU
- Las conexiones inseguras/no cifradas pueden tener consecuencias graves
  - Un usuario no autorizado con acceso a la red podría ver el tráfico y los datos que están siendo enviados o recibidos, violando la privacidad.
  - Un usuario no autorizado podría cambiar los datos mientras están aún en tránsito entre el cliente y el servidor.

# Soporte para SSL (MySQL)

- SSL proporciona [autenticación](#) y [privacidad](#) de la información entre extremos sobre [Internet](#) mediante el uso de [criptografía](#)/cifrado de datos.
  - El protocolo SSL utiliza diferentes algoritmos de cifrado para asegurarse de que los datos recibidos a través de una red pública son seguros.
  - Tiene mecanismos para detectar cambios de datos, pérdidas, o reenvíos.
  - SSL también incorpora algoritmos que proveen de verificación de identidad, utilizando el X509.
- Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.
- Puede utilizarse OpenSSL para activar conexiones seguras en el servidor de MySQL