



UNIVERSIDAD VERACRUZANA
FACULTAD DE ESTADÍSTICA E INFORMÁTICA

Tema:

Primeros pasos en la instalación de un servidor de Bases de Datos

Experiencia Educativa:

Administración de Base de Datos

Alumno(a):

Vanessa Michelle Grapain Aldana
Samuel Ruíz Castillo
Daniel Sebastián Sánchez Medina

Carrera:

Redes y Servicios de Cómputo

Docente:

JUAN CARLOS PÉREZ ARRIAGA,

Fecha:

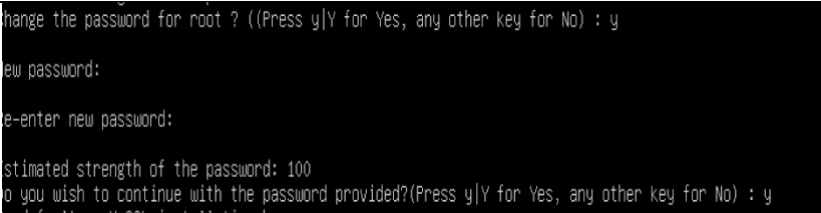
26/02/2023

Ciudad

Xalapa, Veracruz

<u>Criterio</u>	<u>Descripción</u>	<u>Ejemplo</u>	<u>Verificación</u>
Descarga de la última versión estable de MySQL	<p>Descargar la última versión estable de MySQL probablemente incluye correcciones de errores y mejoras de rendimiento que pueden mejorar el rendimiento de la base de datos. Por lo tanto, es una buena práctica mantener actualizado el software de la base de datos para garantizar su seguridad y eficacia.</p>	<pre> dbunix@dbunix:~\$ sudo apt show mysql-server Package: mysql-server Version: 8.0.32-0ubuntu0.22.04.2 </pre>	

Instalación del paquete de MySQL	Se debe realizar la instalación y verificar que la instalación se haya realizado correctamente	<pre>Press y Y for Yes, any other key for No: y Here are three levels of password validation policy: LOW Length >= 8 MEDIUM Length >= 8, numeric, mixed case, and special characters STRONG Length >= 8, numeric, mixed case, special characters and dictionary file Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2 Using existing password for root.</pre>	
Configuración de contraseñas seguras	Configurar el nivel de contraseñas STRONG para contraseñas solo sean aceptadas si contienen números, mayúsculas y minúsculas y caracteres especiales	<pre>Press y Y for Yes, any other key for No: y Here are three levels of password validation policy: LOW Length >= 8 MEDIUM Length >= 8, numeric, mixed case, and special characters STRONG Length >= 8, numeric, mixed case, special characters and dictionary file Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2 Using existing password for root.</pre>	

<p>Cambiar la contraseña del usuario root, por una contraseña segura y fácil de recordar</p>	<p>Es importante para proteger los datos almacenados en la base de datos, cumplir con las políticas de seguridad, evitar ataques de hackers y facilitar el acceso a la base de datos. Es una práctica recomendada desde el punto de vista de la seguridad de la información y puede ayudar a garantizar la integridad y confidencialidad de los datos almacenados.</p> <p>Configurar que solo se permitan contraseñas con mínimo 8 caracteres, patrones seguros, incluir mayúsculas, caracteres especiales y números en combinación</p>	 A terminal window with a black background and white text. The text shows the process of changing the root password: 'change the password for root ? ((Press y Y for Yes, any other key for No) : y', 'new password:', 're-enter new password:', 'estimated strength of the password: 100', and 'do you wish to continue with the password provided?(Press y Y for Yes, any other key for No) : y'. <pre>change the password for root ? ((Press y Y for Yes, any other key for No) : y new password: re-enter new password: estimated strength of the password: 100 do you wish to continue with the password provided?(Press y Y for Yes, any other key for No) : y</pre>		
--	---	---	--	--

Remover los accesos de usuarios anónimos a la base de datos		<pre>Remove anonymous users? (Press y Y for Yes, any other key for No) : y Success.</pre>	
Deshabilitar el acceso root remoto		<pre>Disallow root login remotely? (Press y Y for Yes, any other key for No) : y Success.</pre>	
Remover las bases de datos de test y el acceso a ellas		<pre>Remove test database and access to it? (Press y Y for Yes, any other key for No) : y - Dropping test database... Success.</pre>	
Crear usuarios dedicados para las tareas designadas	Es importante crear usuarios dedicados a cada persona con solo los permisos necesarios para ese usuario	<pre>mysql> CREATE USER 'vanessa'@'localhost' IDENTIFIED BY 'vanessaCAMBIAESTO-1'; Query OK, 0 rows affected (0,01 sec) mysql> CREATE USER 'sebastian'@'localhost' IDENTIFIED BY 'sebastianCAMBIAESTO-1'; Query OK, 0 rows affected (0,02 sec) mysql> CREATE USER 'samuel'@'localhost' IDENTIFIED BY 'samuelCAMBIAESTO-1'; Query OK, 0 rows affected (0,02 sec)</pre>	
Revisar regularmente la lista de usuarios y sus permisos	Siempre es recomendable revisar regularmente la lista de usuarios y sus permisos en el servidor de base de datos para garantizar la seguridad y el correcto funcionamiento del servidor de base de datos.		

Revocar los permisos de usuarios que ya no los necesiten	Después de realizar la revisión de usuarios, se necesita revocar los permisos a los usuarios que ya no necesitan estos o eliminar usuarios que ya no existan	Revoke permisos from usuario@localhost;	
Permitir el acceso solo a IPs autorizadas	Configurar la base de datos para que solo permita el acceso al usuario desde IPs autorizadas.	Sudo nano /etc/mysql/mysql.d.cnf y en la parte de bind_address agregar las ips autorizadas a entrar	
Evitar que se puedan realizar demasiados intentos de inicio de sesión	Configurar un límite de inicio de sesión a las cuentas de los usuarios, para evitar ataques de fuerza bruta	Al momento de crear un usuario colocar MAX_CONECCTIONS_PER_HOUR=100	
Probar que el servidor funcione correctamente y todas las configuraciones se hayan realizado de manera correcta	Es esencial para garantizar que el servidor esté listo para su uso. Las pruebas pueden ayudar a verificar la configuración, detectar problemas temprano, mejorar el rendimiento, garantizar la disponibilidad y cumplir con los requisitos del negocio.	Ejecutar mysqladmin -verbose -help para comprobar que todo esta instalado correctamente	

Realizar copias de seguridad regularmente	Es importante establecer una programación regular para la realización de copias de seguridad y almacenar las copias de seguridad en un lugar seguro y accesible en caso de emergencia.		
Monitorear la actividad de la base de datos para detectar actividades sospechosas	Monitorear la actividad de la base de datos para detectar actividades sospechosas	A través del comando show processlist; para ver las conexiones a la base de datos y que están trabajando	
Deshabilitar el acceso remoto a la base de datos, en caso de no ser necesario	Si el acceso remoto no es necesario para la aplicación o el sistema en cuestión, es recomendable deshabilitarlo para mejorar la seguridad del servidor de base de datos.	Sudo nano /etc/mysql/mysqld.cnf y en la parte de bind_address solo dejar 127.0.0.0 para solo permitir conexiones locales	

