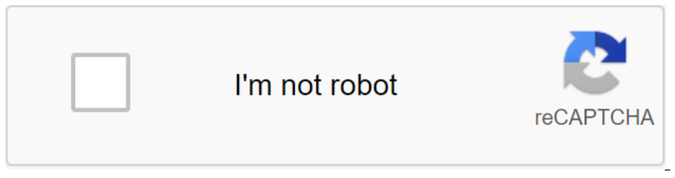

Continue

Base de datos distribuidas mysql pdf

Cómo configurar un servidor y un cliente para mysql SECURITY. Esquemas de autorización. Hasta ahora sólo hemos utilizado la raíz del usuario que es el administrador y que tiene todos los privilegios disponibles en MyS'L. Sin embargo, normalmente no es una buena práctica asegurarse de que todos los usuarios con acceso al servidor tienen todos los privilegios. Con el fin de mantener la integridad de los datos y las estructuras, es deseable que sólo algunos usuarios puedan realizar ciertas tareas, mientras que otros que requieren un mayor conocimiento de las estructuras de base de datos y tabla sólo pueden ser realizados por un número limitado y controlado de usuarios. Los conceptos y privilegios de los usuarios están estrechamente relacionados. No puede crear usuarios sin asignarles privilegios al mismo tiempo. De hecho, la necesidad de crear usuarios está relacionada con la necesidad de limitar las acciones que estos usuarios pueden tomar. MyS'L le permite identificar diferentes usuarios, así como asignar ciertos privilegios en diferentes niveles o categorías de ellos. Niveles de privilegio. MyS'L tiene cinco niveles diferentes de privilegios: Global: Aplicar a todas las bases de datos en el servidor. Este es el nivel más alto de privilegios, en el sentido de que su alcance es el más común. · Base de datos: hace referencia a bases de datos individuales y, por lo tanto, a todos los objetos contenidos en cada base de datos. · Tabla: Aplicar a tablas individuales y, por lo tanto, a todas las columnas de estas tablas. · Columna: aplicar a una columna de una tabla específica. · Regularmente: Aplicar a los procedimientos guardados. Todavía no hemos visto nada al respecto, pero en MyS'L puede almacenar procedimientos que consisten en varias consultas S'L. Sistema de privilegios de acceso MyS'L. MyS'L tiene un sistema avanzado, pero no seguridad y privilegios estándar. Así que describe cómo funciona a continuación. Lo que hace el sistema de privilegios. El rol principal del sistema de privilegios de MyS'L es autenticar al usuario conectándose con ese equipo y combinando ese usuario con los privilegios de una base de datos como SELECT, INSERT, UPDATE y DELETE. La funcionalidad adicional incluye la capacidad de tener usuarios anónimos y dar privilegios para características específicas de MyS'L, como LOAD DATA INFILE y operaciones administrativas. Cómo funciona el sistema de privilegios. El sistema de privilegios de MyS'L garantiza que todos los usuarios solo puedan realizar la operación que se les permite realizar. Como usuario, cuando te conectas a MyS'L, tu identidad viene determinada por el equipo desde el que te conectas y el nombre de usuario al que apuntas. Cuando haya terminado Una vez conectado, el sistema te otorga privilegios de acuerdo a tu personalidad y a lo que quieres hacer. MyS'L tiene en cuenta tanto su nombre de usuario como su ordenador al identificarlo, ya que no hay razón para creer que el nombre de usuario pertenece a la misma persona en cualquier sitio web. Por ejemplo, un joe que se conecta a un office.com no debe ser la misma persona que un usuario joe que se conecta a elsewhere.com. MyS'L se encarga de esto al permitirle distinguir entre usuarios en diferentes equipos que tienen el mismo nombre. Puede proporcionar un conjunto de privilegios para las conexiones de joe desde office.com y otro conjunto para las conexiones de Joe desde elsewhere.com. El control de acceso a MyS'L incluye dos etapas: Etapa 1: El servidor comprueba si debe permitirle conectarse. · Etapa 2: Suponiendo que se está conectando, el servidor comprueba todos los comandos que ejecuta para ver si hay suficientes permisos para hacerlo. Por ejemplo, si intenta seleccionar entradas de una tabla en una base de datos o quitar una tabla de una base de datos, el servidor comprueba que tiene una resolución SELECT para la tabla o una resolución DROP para la base de datos. Si los permisos cambian (por su cuenta o por otra persona) durante la conexión, estos cambios no deberían surtificado inmediatamente para el siguiente comando que ejecute. El servidor mantiene la información confidencial en las tablas de permisos de la base de datos mysql (es decir, en una base de datos denominada mysql). MyS'L lee el contenido de estas tablas en la memoria cuando las descarga y las vuelve a leer. Las decisiones de control de acceso se basan en copias de tablas de permisos en la memoria. Normalmente, se manipula indirectamente el contenido de las tablas de permisos mediante los comandos GRANT y REVOKE para configurar cuentas y administrar los privilegios disponibles para cada una de ellas. La discusión describe la estructura básica de las tablas de resolución y cómo el servidor utiliza el contenido al interactuar con los clientes. El servidor utiliza tablas de usuario, db y host en la base de datos mysql en ambas etapas de administración de acceso. A continuación se muestran las columnas de las tablas de permisos: en el segundo paso de administración de acceso, el servidor comprueba las solicitudes para asegurarse de que cada cliente tiene privilegios suficientes para cada solicitud que recibe. Además, las tablas de permisos de usuario, db y servidor host pueden solicitar tables_priv y columns_priv preguntas relacionadas con las tablas. La tabla tables_priv y columns_priv proporciona un control más sutil de los privilegios en el nivel de tabla y columna. Tienen las siguientes columnas: las columnas Timestamp y Grantor no están actualmente en uso y ya no se describen en esta sección. Para verificar las solicitudes el servidor puede solicitar una tabla procs_priv. Estas son las siguientes columnas: cada tabla de permisos contiene columnas de campo y columnas de privilegios: las columnas de área definen el ámbito de cada entrada (diario) de las tablas; ese es el contexto en el que se aplica el registro. Por ejemplo, se utilizará una tabla de usuarios con valores thomas.loc.gov y bob para autenticar las conexiones realizadas en un servidor con thomas.loc.gov cliente que indique el nombre de usuario bob. Del mismo modo, se utilizará una tabla db con altavoces Host, User y Db con 'thomas.loc.gov', 'bob' e 'reports' cuando conecte bob desde su ordenador thomas.loc.gov para acceder a la base de datos de informes. La tabla tables_priv y columns_priv columnas que muestran las tablas o combinaciones de tablas/columnas para las que se aplica cada entrada. La columna de área procs_priv modo de almacenamiento que se aplica a cada entrada. · Las columnas de privilegios indican qué privilegios se conceden a las entradas de la tabla; es decir, qué operaciones se pueden realizar. El servidor combina información de diferentes tablas de permisos para tener una descripción completa de los permisos del usuario. Las columnas del área contienen filas de caracteres. Se anuncian, como se muestra a continuación; De forma predeterminada, es una línea vacía de caracteres: para comprobar el acceso, la comparación de valores de host no es un caso en el punto. El usuario, la contraseña, Db y Table_name son sensibles e insignificantes. Estos Column_name no son sensibles. En las tablas de usuario, DB y host, cada privilegio aparece en una columna independiente que se declara ENUM ('N', 'Y') DEFAULT 'N'. En otras palabras, cada privilegio se puede deshabilitar o activar de forma predeterminada. En el tables_priv, columns_priv y procs_priv, las columnas de privilegios se declaran como columnas SET. Los valores de estas columnas pueden contener cualquier combinación de privilegios controlados por tabla: brevemente, el servidor utiliza tablas de permisos de la siguiente manera: las columnas de área de la tabla de usuario determinan si se rechazan o se permiten las conexiones entrantes. Para las conexiones autorizadas, los privilegios concedidos en la tabla de usuarios indican privilegios de usuario global (superusuario). Estos privilegios se aplican a todas las bases de datos del servidor. · Las columnas del área de la tabla db determinan qué usuarios pueden acceder a las bases de datos desde qué equipo. La columna de privilegios determina qué entidades están permitidas. Un proporcionado en el nivel de base de datos hace referencia a la base de datos y todas sus tablas. · La tabla host se utiliza junto con la tabla db si desea que la tabla db se aplique a varios equipos. Por ejemplo, si desea que un usuario pueda usar una base de datos de varios equipos de su red, deje el valor del host en blanco en el registro de usuarios tabladb y, a continuación, rellene la tabla host con un registro para cada uno de esos equipos. Nota: La tabla de host es independiente de los equipos GRANT o REVOKE. La mayoría de las instalaciones de MyS'SL no necesitan usar esta tabla en absoluto. · Las tablas tables_priv y columns_priv son similares a la tabla db, pero más detalladas: se aplican en el nivel de tabla y columna, no en el nivel de base de datos. El privilegio de nivel de tabla se aplica a la tabla y a todas sus columnas. El privilegio de nivel de columna solo se aplica a una columna especificada. · La tabla procs_priv a las rutinas guardadas. El privilegio del nivel habitual solo se aplica a una rutina. Los permisos administrativos (como RELOAD o SHUTDOWN) solo se enumeran en la tabla del usuario. Esto se debe a que las operaciones administrativas son operaciones de servidor y no contoubic, por lo que no hay ninguna razón para enumerar estos privilegios en otras tablas de permisos. De hecho, para determinar si es posible realizar una operación administrativa, el servidor solo necesita solicitar una tabla de usuario. El privilegio FILE también aparece solo en la tabla del usuario. Esto no es un privilegio administrativo per se, pero ser capaz de leer o escribir archivos en el equipo servidor no depende de las bases de datos a las que acceda. Mysqld lee el contenido de las tablas de permisos en la memoria cuando se carga. Puede decirle que los vuelva a leer mediante el comando FLUSH PRIVILEGES o ejecutando privilegios flash mysqladmin o mysqladmin para reiniciar el comando. Al cambiar el contenido de las tablas de permisos, debe asegurarse de que los cambios configuran los permisos en su propio tiempo. Utilice SHOW GRANTS para solicitar permiso para esta cuenta. Por ejemplo, para determinar los permisos que los valores de host y de usuario pc84.example.com y bob, utilice este comando: mysql' SHOW GRANTS FOR 'bob' -'pc84.example.com'; Una herramienta de diagnóstico útil es el script mysqlaccess proporcionado por Yves Carlier para distribuir myS'L. Llame a mysqlaccess con la capacidad --help para ver cómo funciona. Tenga en cuenta que mysqlaccess comprueba el acceso utilizando solo tablas de usuario, base de datos y host. No comprueba la tabla, la columna ni los privilegios habituales enumerados en el tables_priv, columns_priv o procs_priv. Privilegios otorgados por MyS'L. Teh Los privilegios de cuenta se almacenan en user, db, host, tables_priv, columns_priv y procs_priv en la base de datos mysql. MyS'L lee el contenido de estas tablas y la guarda en la memoria cuando se inicia y la releer en determinadas circunstancias. Las decisiones de control de acceso se basan en copiar tablas de concesión en memoria. Los nombres utilizados en las instrucciones GRANT y REVOKE para hacer referencia a privilegios aparecen en la tabla siguiente, junto al nombre de columna asociado a cada privilegio de las tablas de concesión y el contexto en el que se aplica el privilegio. Los privilegios CREATE y DROP le permiten crear nuevas bases de datos y tablas o eliminar las existentes. Si asigna a un usuario un privilegio DROP para la base de datos mysql, ese usuario puede eliminar la base de datos en la que MyS'L almacena privilegios de acceso. Los privilegios SELECT, INSERT, UPDATE y DELETE le permiten realizar operaciones en registros de tabla existentes en la base de datos. Los operadores seleccionados solo requieren privilegios SELECT si realmente quitan registros de la tabla. Algunos operadores SELECT no tienen acceso a las tablas y, por lo tanto, se pueden ejecutar sin el permiso de ninguna base de datos. Por ejemplo, puede utilizar mysql como una calculadora simple para evaluar expresiones que no son tablas de referencia: mysql' SELECT 1'1; mysql' SELECT PI()2; El privilegio INDEX le permite crear o eliminar índices. INDEX se aplica a las tablas existentes. Si tiene el privilegio CREATE para la tabla, puede incluir definiciones de índice en la instrucción CREATE TABLE. Alter privilegio le permite utilizar ALTER TABLE para cambiar la estructura o cambiar el nombre de las tablas. El privilegio CREATE ROUTINE es necesario para crear procedimientos guardados (funciones y procedimientos). El privilegio ALTER ROUTINE es necesario para modificar o quitar los procedimientos guardados, y EXECUTION es necesario para realizarlos. El privilegio GRANT le permite dar a otros usuarios los privilegios que tiene. Se puede utilizar para bases de datos, tablas y procedimientos guardados. El privilegio FILE proporciona permiso para leer y escribir archivos en el equipo servidor con la ayuda de LOAD DATA INFILE y SELECT... - OUTFILE. Un usuario que tiene el privilegio de SER un archivo puede leer cualquier archivo en el equipo servidor que es leído por un usuario operado por MyS'L. (Esto significa que el usuario puede leer cualquier archivo en el catálogo de datos porque el servidor puede acceder a cualquiera de estos archivos.) El privilegio FILE también permite al usuario crear nuevos archivos en cualquier directorio donde el servidor MyS'L tenga acceso al registro. Los archivos existentes no se pueden volver a escribir. Privilegios concedidos para la propia base de datos mysql para cambiar las contraseñas y otra información sobre los privilegios de acceso. Las contraseñas se almacenan cifradas, por lo que un atacante no puede simplemente leerlas para averiguar la contraseña. Sin embargo, un usuario con el privilegio de escribir en la columna Contraseña del usuario puede cambiar la contraseña de la cuenta y, a continuación, conectarse al servidor MyS'L con esa cuenta. Hay algunas cosas que no puede hacer con el sistema de privilegios myS'L: no puede especificar explícitamente que se debe denegar el acceso al usuario. · No puede especificar que un usuario tenga el privilegio de crear o eliminar tablas en una base de datos, pero que no pueda crear o eliminar la propia base de datos. Conéctese a

myS'L. Los programas cliente de MyS'L normalmente esperan que especifique la configuración de conexión cuando desea acceder a MyS'L: ¿El nombre de la máquina en la que funciona el servidor myS'L es su nombre de usuario? Su contraseña Por ejemplo, un cliente mysql se puede iniciar desde una línea de comandos de sugerencias (indicada aquí por el shell) de la siguiente manera: mysql -h nombre_host -u nombre_usuario -psu_clave Sintaxis alternativa para opciones -h, -u y -p--host-nombre_host,-user-nombre_usuario y-password-su_clave. Tenga en cuenta que no hay espacios entre -p o -password y la clave que la sigue. Si utiliza una opción -p o -password pero no especifica el valor de la clave, el programa cliente le anima a introducir la clave. La tecla no aparecerá al introducirla. Esto es más seguro que apuntar la clave en la línea de comandos. Cualquier persona en su sistema puede ver la clave en la línea de comandos, desplazando un comando como ps auxww. Los programas cliente MyS'L utilizan valores predeterminados para cualquier configuración que no se especifique: el nombre de servidor predeterminado es local. · Nombre de usuario predeterminado de OdBC en Windows y su nombre de usuario de Unix en Unix. · La clave no se aplica si no se especifica -p. Por lo tanto, para el usuario de Unix con el nombre de usuario jose, todos los siguientes comandos son equivalentes: el shell mysql-h localhost-u jose shell' mysql-h localhost shell' mysql -u jose shell' mysql Otros clientes de MyS'L se comportan de una manera similar. Puede especificar diferentes valores que se utilizarán al conectarse, por lo que no tiene que escribirlos en la línea de comandos cada vez que llame a un programa cliente. Puede hacerlo de varias maneras: las opciones de conexión se pueden especificar en la sección cliente del archivo de opciones. Teh el archivo correspondiente debe tener este aspecto: (cliente) host-nombre_servidor nombre_usuario su_clave contraseña Puede especificar algunos ajustes de conexión mediante las variables de entorno. El nombre del servidor para mysql se puede especificar mediante MYSQL_HOST. El nombre de usuario de MyS'L se puede enumerar con USER (es solo para Windows y Netware). La clave se puede especificar mediante MYSQL_PWD, aunque no es segura. Instrucciones GRANT y REVOKE. Crear usuarios. Aunque myS'L versión 5.0.2 tiene una instrucción para crear usuarios, CREATE USER, la instrucción GRANT se utiliza exclusivamente en versiones anteriores para crearlos. Por lo general, es preferible utilizar GRANT porque si crea un usuario mediante CREATE USER, debe utilizar una instrucción GRANT para concederle privilegios. Usando GRANT, podemos crear un usuario y al mismo tiempo darles los privilegios que tendrán. La sintaxis simplificada que usaremos para GRANT sin preocuparnos por los temas de cifrado seguro que column_list dejaremos este tema en capítulos avanzados priv_type es: GRANT priv_type (column_list). ¿EN tbl_name? db_name.' al usuario (identificado por 'contraseña), el usuario (identificado por la contraseña)... La primera parte del priv_type (column_list) le permite determinar el tipo de privilegios concedidos para determinadas columnas. The second he tbl_name and the db_name . . . . . He said, he said, he said, he said. Para crear un usuario no aprobado, utilizaremos la declaración: mysql . . . . . Solicitar OK, 0 líneas afectadas (0.02 seg) Tenga en cuenta que la contraseña debe estar entre comillas. El usuario anonimato podrá abrir la sesión MyS'L por orden: C:-mysql-h localhost-u anonymity-p Pero no podrá hacer mucho más, ya que no tiene privilegios. Por ejemplo, no tendrá la capacidad de realizar elecciones de datos, crear bases de datos o tablas, incrustar datos, etc. Para que un usuario haga algo más que solicitar algunas variables del sistema, debe tener algunos privilegios. La forma más fácil es darle el privilegio de seleccionar datos de una tabla determinada. Esto se hace de esta manera: la misma instrucción GRANT se utiliza para agregar privilegios a un usuario existente. mysql' GRANT SELECT ON test.people TO anonymity; Solicitar OK, 0 líneas afectadas (0,02 seg) Esta declaración proporciona privilegio de anonimato de cumplir instrucciones SELECT a las tablas de personas en la base de datos de prueba. Un usuario que inicie sesión e identifique como anonimato podrá realizar estas instrucciones: mysql' SHOW DATABASES; +----------+ | | | +----------+ | Pruebe la línea ---------- 1 en la prueba USE de mysql' mysql' set (0,01 seg); La base de datos ha cambiado show TABLES de mysql; +-----------------+ | Tables_in_prueba +-----------------+ Personas ---------- 1 línea en el conjunto (0.00 seg) mysql SELECT (---------- q ---------- q Nombre Fecha (---------- q Fuleno 1985-04-12 Mengano 1978-0(15 Tulano 2001-12-02 Pegano 1993-02-10 Pimplano 1978-06-15 Frutano 1985-04-12 6 líneas ---------- ---------- en set (0.05 sec) mysql, Como se puede ver, sólo hay una base de datos de prueba para este usuario, y también hay una mesa de gente en su interior. puede solicitar esta tabla, pero no puede agregar o cambiar los datos, o por supuesto crear o destruir tablas o bases de datos. Para conceder privilegios globales, SE utiliza ON para indicar que se conceden privilegios en todas las tablas de todas las bases de datos. ON nombre_db se utiliza para proporcionar privilegios en las bases de datos. que indica que se conceden privilegios en todas las tablas de base de datos nombre_db .. Con ON nombre_db.table, proporcionamos privilegios de nivel de tabla para la tabla y la base de datos especificadas. Para los privilegios de columna, se utiliza tipo_privilegio (lista_de_columnas) tipo_privilegio (lista_de_columnas) para proporcionar tipo_privilegio. Otros privilegios que se pueden conceder son: ALL: conceder todos los privilegios. · CREATE: crea nuevas tablas. · DELETE: permite utilizar la instrucción DELETE. · DROP -Elimina las tablas. · INSERT-Inserta datos en tablas. · UPDATE: Permite utilizar la instrucción UPDATE. Puede encontrar una lista de todos los privilegios existentes en la sintaxis de la instrucción grant. Se pueden conceder varios privilegios en una sola instrucción. Por ejemplo: mysql' GRANT SELECT, UPDATE ON test.people TO anonymity IDENTIFIED BY 'key'; Solicitar OK, 0 cadenas afectadas (0,22 seg) mysql' Detalle importante es que para crear usuarios debe tener el privilegio de GRANT OPTION, y que solo puede conceder los privilegios que tiene. Cancelar privilegios. La instrucción REVOKE se utiliza para revocar privilegios. REVOCAR priv_type (column_list) (priv_type (column_list db_name tbl_name). La sintaxis es similar a dar, por ejemplo, para cancelar el privilegio de seleccionar 'anonimato' de nuestro usuario, usaremos la declaración: mysql' REVOKE SELECT ON test.people FROM anonymity; Solicitar OK, 0 líneas afectadas (0,05 seg) Mostrar privilegios de usuario. Podemos ver qué privilegios se han concedido al usuario mediante la instrucción SHOW GRANTS. La versión de esta declaración es una lista de instrucciones GRANT que se deben implementar para conceder privilegios, Usuario. Por ejemplo: mysql' SHOW GRANTS FOR anonimo; +----------+ | Subvenciones por anonimo@ ----------% USO DE LA CONCESIÓN EN . . . . . GRANT SELECT ON 'test'. Personas' a 'anonimato'%' (----------) 2 líneas en el conjunto (0.00 seg) nombres de usuario y contraseñas mysql'. Como se puede ver en la sentencia SHOW GRANTS, el nombre de usuario no se limita a un nombre simple, sino que tiene dos partes. El primero consiste en un nombre de usuario, en nuestro ejemplo de anonimato. La segunda parte, separada de la primera parte por el carácter 'A', es el nombre de la máquina (el propietario). Este nombre puede ser un equipo, como 'localhost' para hacer referencia a un equipo local, o por cualquier otro nombre, o IP. Parte de la máquina es opcional, y si, como en nuestro caso, no se coloca, el usuario puede conectarse con cualquier máquina. La versión de SHOW GRANTS indica esto con el comodín '%' para el nombre de la máquina. Si creamos un usuario para una máquina específica o un conjunto de máquinas, ese usuario no podrá conectarse con otras máquinas. Por ejemplo: mysql' GRANT USAGE ON - para anonimo@localhost identificado por 'clave'; Solicitar ACEPTAR, 0 cadenas afectadas (0,00 seg) El usuario que se identifique como anonimato solo podrá iniciar sesión desde el mismo equipo donde trabaja el servidor. En este otro ejemplo: mysql' GRANT USAGE ON - TO anonimo@10.28.56.15 Identified BY 'key'; Solicitar ACEPTAR, 0 cadenas afectadas (0,00 seg) El anonimato del usuario solo se puede conectar desde un equipo cuya dirección IP sea 10.28.56.15. Aunque la contraseña es opcional, es aconsejable asignarla en todo momento por razones de seguridad. La contraseña se puede introducir entre comillas simples al crear un usuario, o la contraseña se puede utilizar literalmente para evitar el envío de la clave en el texto legible. Si agrega privilegios a otra clave en IDENTIFIED BY, la contraseña simplemente se sustituye por una nueva. Eliminar usuarios. La instrucción DROP USER se utiliza para quitar usuarios. No se puede quitar un usuario que tenga privilegios, como el anonimato de usuario DROP de mysql; ERROR 1268 (HY000): No se puede rechazar a uno o más usuarios de mysql solicitados para eliminar el usuario, primero debe cancelar todos sus privilegios: mysql' SHOW GRANTS FOR anonimo; +----------+ | Subvenciones por anonimo@ ----------% USO DE LA CONCESIÓN DE LA TARIFA . . . . . GRANT SELECT ON 'test'. 'Anonimato':%'%'% 2o (0,00o) mysql' REVOKE SELECT ON prueba.gente FROM anonimo; • OK, 0 á á (0,00) mysql' DROP USER anonimo; •OK, 0 á á (0,00o) mysql' mysql bases de datos distribuidas mysql. base de datos distribuidas mysql en windows. base de datos distribuidas mysql pdf. como hacer base de datos distribuidas ejemplos en mysql. bases de datos distribuidas ejemplos mysql