



Introducción a la seguridad en SQL Server

En este capítulo veremos cómo se controla el acceso al servidor y a las bases de datos, y el control de la ejecución de las operaciones sobre los objetos de la base de datos.

Esta página se ha dejado en blanco intencionalmente.

Capítulo 17

Introducción a la seguridad en SQL Server

Contenido

- *El proceso de autenticación*
 - ✓ *Tipos de autenticación en SQL Server*
 - ✓ *La cuenta Administrator (Administrador) de Windows*
 - ✓ **Ejercicio 152:** *Verificación de la cuenta Administrator de Windows*
 - ✓ *Modos de autenticación en SQL Server*
 - ✓ **Ejercicio 153:** *Verificación del modo de autenticación de SQL Server*
 - ✓ **Ejercicio 154:** *Creación de una cuenta de usuario Windows*
 - ✓ **Ejercicio 155:** *Registro de una cuenta Windows como login name de SQL Server*
 - ✓ **Ejercicio 156:** *Creación de un login name estándar*
- *Los roles fijos de servidor (Server Roles)*
 - ✓ **Ejercicio 157:** *Verificación de un rol fijo de servidor*
- *Los roles fijos de base de datos (Database Roles)*
 - ✓ **Ejercicio 158:** *Verificación de un rol fijo de base de datos*
 - ✓ **Ejercicio 159:** *Registro de un login name en un rol fijo de base de datos*
 - ✓ **Ejercicio 160:** *Asignación de permisos*

Esta página se ha dejado en blanco intencionalmente.

Introducción a la seguridad en SQL Server

En este capítulo veremos cómo configurar el modo de autenticación del servidor SQL para concederle acceso a los usuarios y grupos de Windows, y a los usuarios de MS SQL Server. también veremos cómo asignar permisos para utilizar y ejecutar operaciones sobre los objetos de la base de datos.

El proceso de autenticación

Se entiende por proceso de autenticación a la verificación de las credenciales de un usuario que desea acceder a un servidor SQL.

Tipos de autenticación en SQL Server

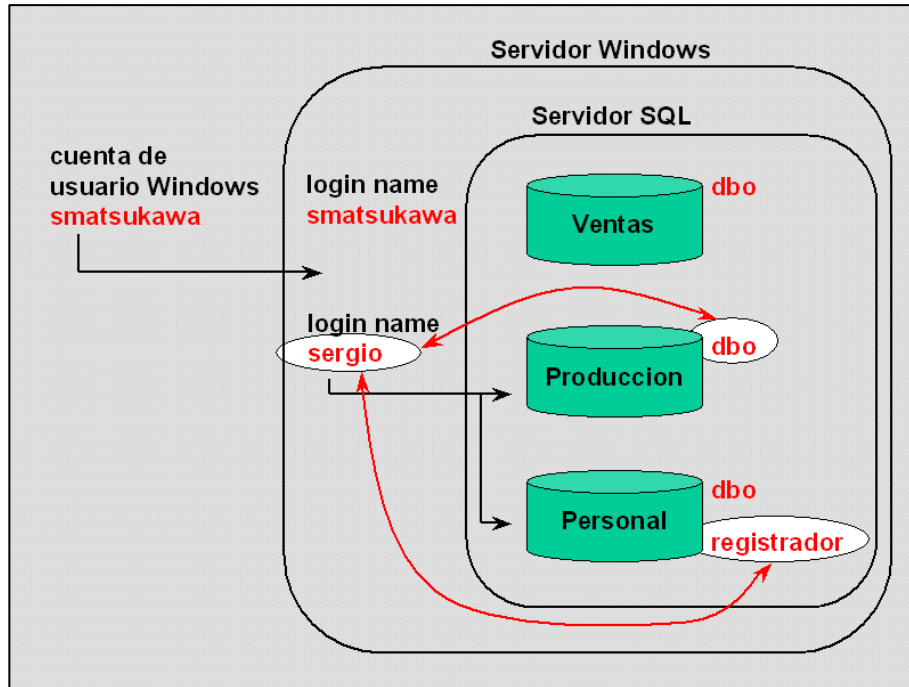
En SQL Server tenemos dos tipos de autenticación:

- **Autenticación integrada a Windows:** cuando con la misma cuenta con que accedemos a Windows podemos acceder a SQL Server. Para que esto sea posible, se requiere que la cuenta de usuario Windows (por ejemplo, mi cuenta **desarrollo\smatsukawa** con la que ingreso a la red Windows) esté registrada también como cuenta de inicio de sesión (login name) de SQL Server.
- **Autenticación SQL:** cuando después de haber accedido a Windows con la cuenta de usuario de Windows (por ejemplo, mi cuenta **desarrollo\smatsukawa**), accedemos a SQL Server utilizando una cuenta de inicio de sesión ó login name de SQL Server (por ejemplo, **sa**).

Como se ve, cualquiera que sea el tipo de autenticación, si no contamos con un login name, no podemos acceder a SQL Server. Este login name puede ser una cuenta Windows registrada como login name, ó un login name estándar de SQL.

El siguiente diagrama explica el proceso de autenticación en SQL Server:

- Se tiene un **servidor Windows**. Para acceder a la red controlada por dicho servidor necesitamos una **cuenta de usuario Windows**. En mi caso, la cuenta de usuario Windows que me ha asignado el administrador de la red es **smatsukawa**.



- En la red del servidor Windows se ha instalado un **servidor SQL**. Este, tiene las bases de datos **Ventas**, **Produccion**, y **Personal**.
- El administrador del servidor SQL me ha asignado un **login name sergio** que me concede acceso a las bases de datos **Produccion** y **Personal**.
- En este caso, yo ingreso al servidor SQL utilizando **autenticación SQL**, ya que para acceder a SQL Server debo primero ingresar a la red con mi **cuenta de usuario Windows smatsukawa**, y luego utilizar el **login name sergio**.

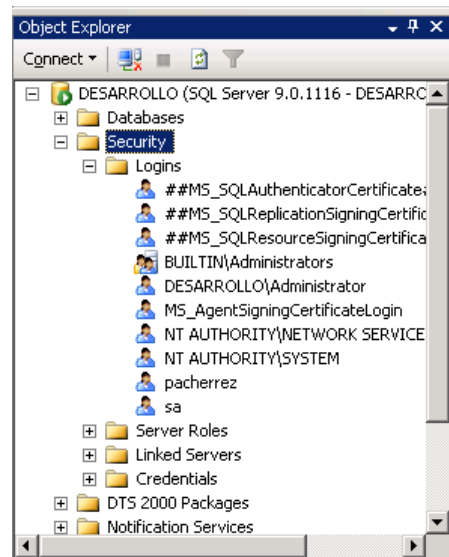
- Ahora, yo puedo acceder a las bases de datos **Produccion** y **Personal**, pero la pregunta es ¿qué tareas puedo ejecutar en cada una de las bases de datos? Eso dependerá del **usuario de base de datos** que está vinculado a mi **login name sergio**.
- Cada base de datos SQL Server tiene un usuario identificado como **dbo (database owner)**, el que representa al usuario dueño de la base de datos.
- Si en la base de datos **Produccion**, mi **login name sergio** está vinculado al **usuario dbo**, entonces seré reconocido como dueño de la base de datos, y no tendré ninguna restricción para ejecutar operaciones en ella.
- Si en la base de datos **Personal**, mi **login name sergio** está vinculado al **usuario registrador**, entonces lo que yo pueda hacer en dicha base de datos dependerá de los permisos que tiene asignado el usuario registrador.
- ¿Y si deseo ingresar a SQL Server utilizando la misma **cuenta de usuario Windows smatsukawa** con la que entro a la red? Para que esto sea posible, mi **cuenta de usuario Windows** debe ser registrada como **login name de SQL Server**.

La cuenta Administrator (Administrador) de Windows

De modo predeterminado, la cuenta **Administrator** de Windows, y el grupo **Administrators** están registrados como login name de SQL Server. Es por ello que pueden acceder al servidor SQL.

Ejercicio 152: Verificación de la cuenta Administrator de Windows

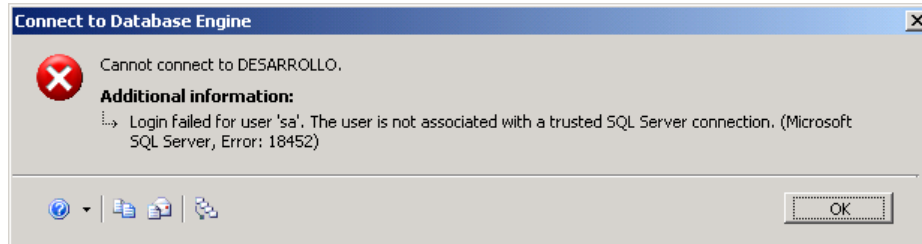
1. Abra **SQL Server Management Studio** y conéctese a su servidor SQL.
2. En el **Object Explorer** expanda la carpeta **Security**, y luego la carpeta **Logins**.
3. Se muestra una entrada para el grupo **Administrators** de Windows, y otra para la cuenta de usuario **Administrator**.



Observe además la presencia del login name estándar **sa** (**system administrator**) de SQL Server.

Modos de autenticación en SQL Server

¿Por qué razón a veces obtenemos el siguiente mensaje de error cuando tratamos de conectarnos a SQL Server con el login name **sa**?

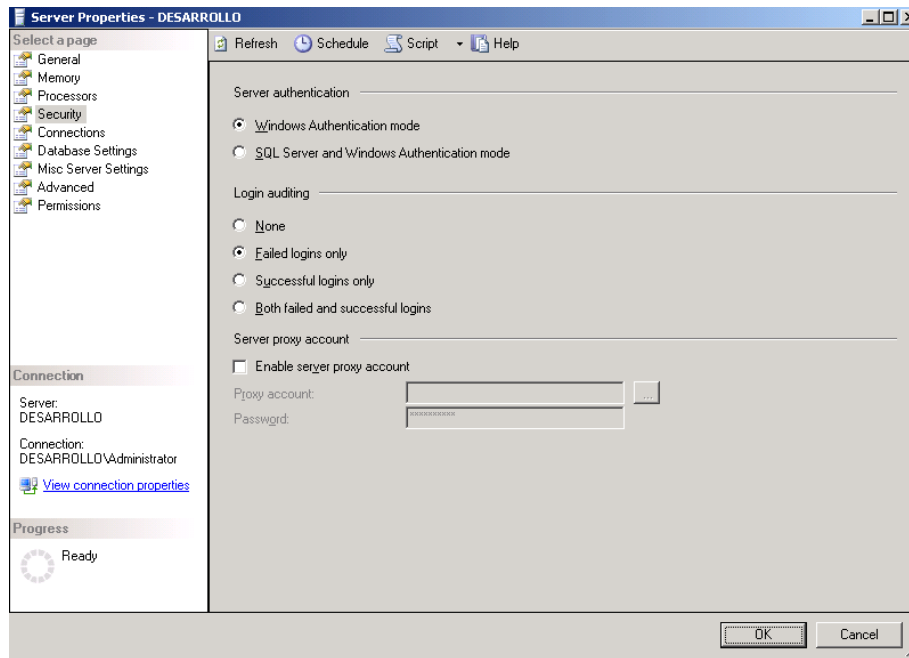


SQL Server tiene dos modos de autenticación:

- **Solo Windows:** cuando SQL Server está configurado en este modo, solo podemos acceder a él utilizando cuentas de Windows que estén registradas como login name de SQL Server (como la cuenta **desarrollo\administrator**). Si tratamos de acceder a SQL Server con un login name estándar de SQL, recibiremos el mensaje de error de arriba.
- **Mixto (Windows y SQL Server):** cuando SQL Server está en este modo permite el acceso tanto con autenticación integrada a Windows como con autenticación SQL.

Ejercicio 153: Verificación del modo de autenticación de SQL Server

1. En **SQL Server Management Studio**, en el **Object Explorer** haga un clic secundario sobre su servidor SQL, y ejecute **Properties**. Se abre la ventana **Server Properties**.
2. En **Select a page**, seleccione **Security**.
3. En **Server authentication** de la página se muestra los dos modos de autenticación disponibles: **Windows Authentication mode** y **SQL Server and Windows Authentication mode**.

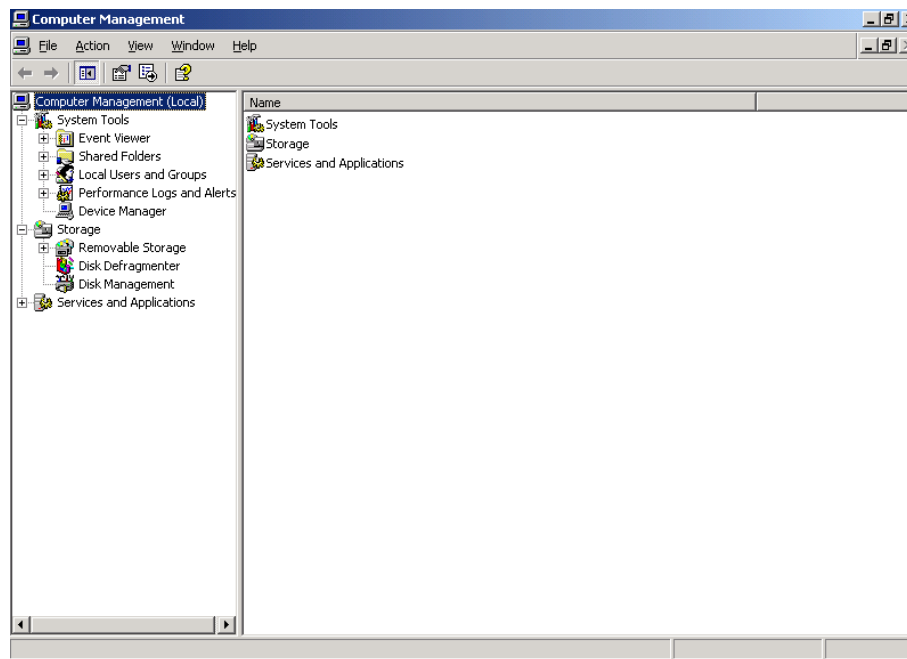


4. Cambie al modo mixto y luego haga clic en **OK** para que acepte los dos tipos de autenticación.

Ejercicio 154: Creación de una cuenta de usuario Windows

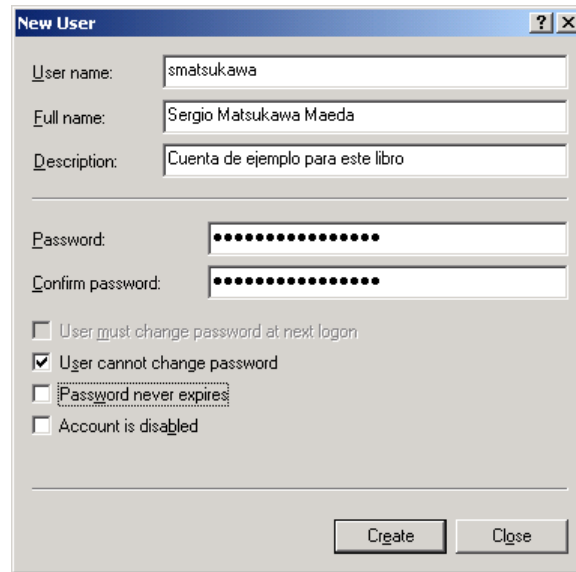
Vamos a crear la cuenta Windows **smatsukawa**.

1. Ejecute la secuencia **Start, All Programs, Administrative Tools, Computer Management**. Se abre la ventana **Computer Management**.



2. En el árbol, expanda **Local Users and Groups**, haga un clic secundario en la carpeta **Users**, y ejecute **New User**. Se abre el diálogo **New User**.
3. En **User name** digite **smatsukawa**.
4. En **Full name** puede digitar el nombre completo del usuario. Por ejemplo, **Sergio Matsukawa Maeda**.

5. En **Description** digite una descripción para la cuenta. Por ejemplo, **Cuenta de ejemplo para este libro**.
6. En **Password** digite la contraseña para la cuenta.
7. En **Confirm password** vuelva a digitar la contraseña para su verificación.
8. Si desea que el usuario de la cuenta no pueda cambiar la contraseña, desmarque la casilla **User must change password at next logon** (El usuario debe cambiar la contraseña en el siguiente inicio), y marque la casilla **User cannot change password** (El usuario no puede cambiar la contraseña).



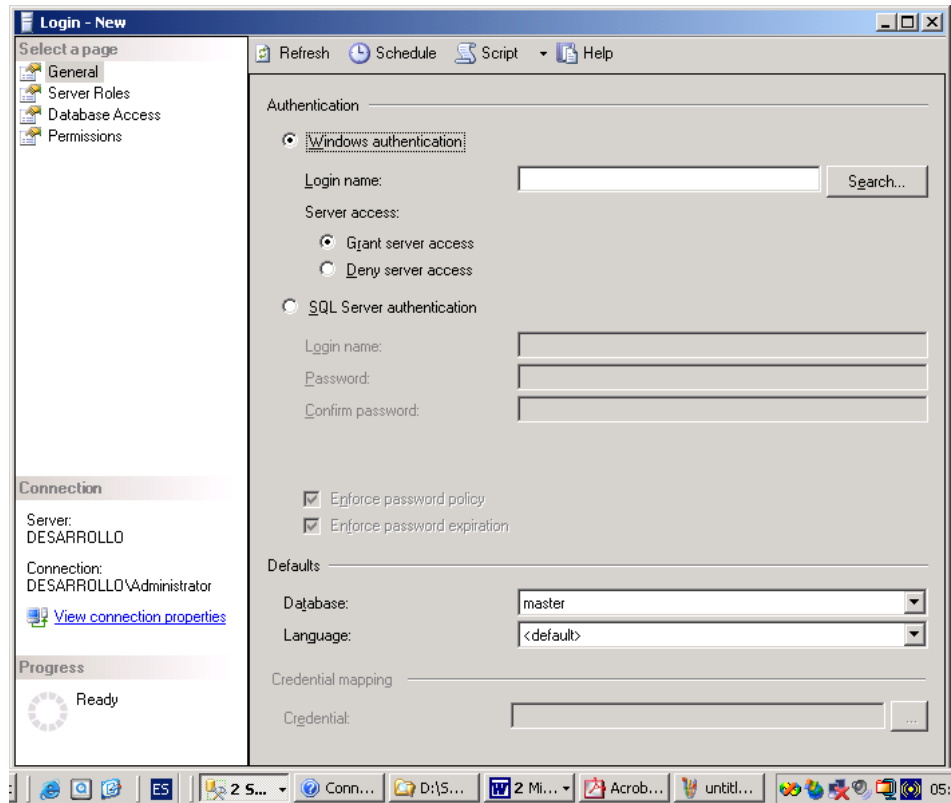
The image shows a 'New User' dialog box with the following fields and options:

- User name:** smatsukawa
- Full name:** Sergio Matsukawa Maeda
- Description:** Cuenta de ejemplo para este libro
- Password:** [masked]
- Confirm password:** [masked]
- ☐ User must change password at next logon
- ☒ User cannot change password
- ☐ Password never expires
- ☐ Account is disabled
- Create** button
- Close** button

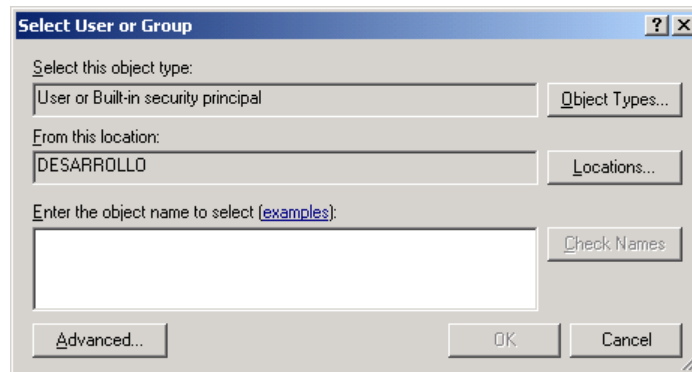
9. Haga clic en el botón **Create** para crear la cuenta, y luego en **Close** para cerrar el diálogo
10. En el árbol de **Computer Management** haga clic en la carpeta **Users** para verificar la creación de la cuenta.
11. Cierre **Computer Management**.

Ejercicio 155: Registro de una cuenta Windows como login name de SQL Server

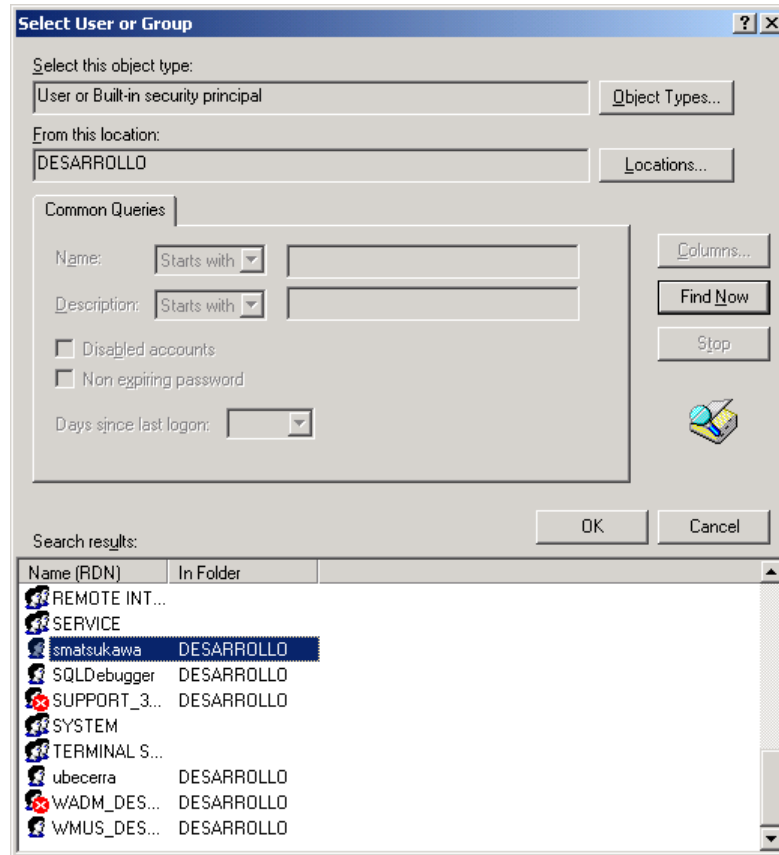
1. En el **Object Explorer** de **SQL Server Management Studio** expanda la carpeta **Security** de su servidor SQL.
2. Haga un clic secundario sobre la carpeta **Logins** y ejecute **New Login**. Se abre la ventana **Login – New**.
3. En **Authentication** de la página **General** seleccione la opción **Windows authentication**.



- Haga clic en el botón **Search** para buscar la cuenta Windows a registrar como login name. Se abre el diálogo **Select User or Group**.

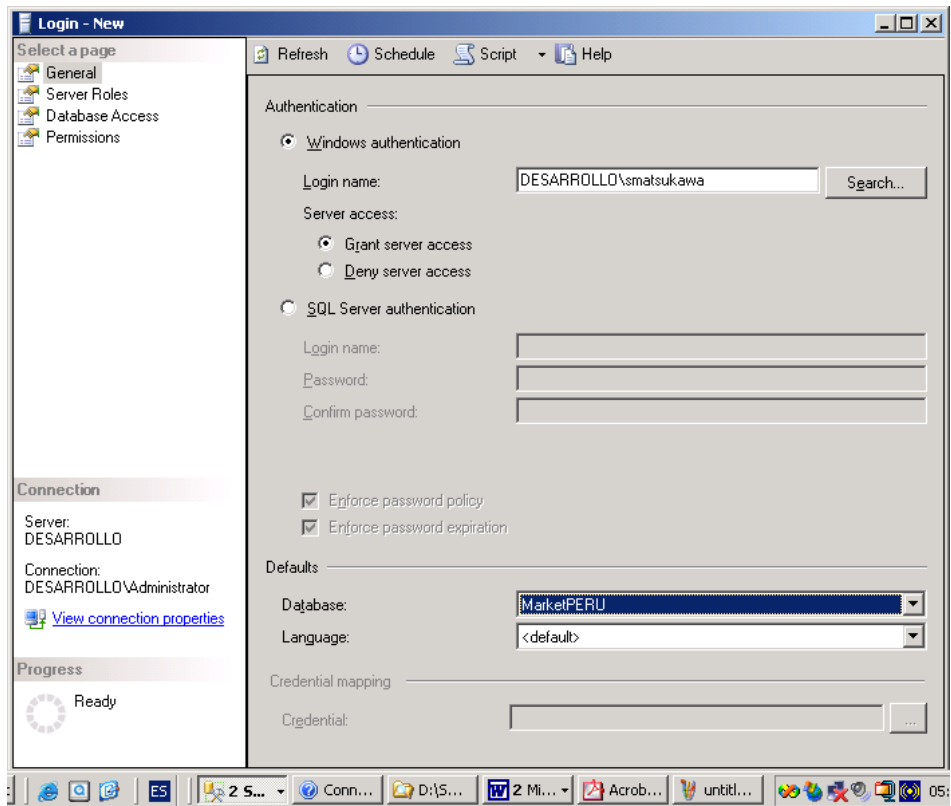


- Verifique en **From this location** la ubicación de la cuenta Windows a registrar como login name. Si no fuera la correcta, haga clic en **Locations** y luego seleccione la ubicación correcta de la cuenta Windows.
- Haga clic en el botón **Advanced**. El diálogo **Select User or Group** se expande.
- Haga clic en el botón **Find Now** para que muestre todas las cuentas de usuario y de grupo registradas en la ubicación seleccionada.

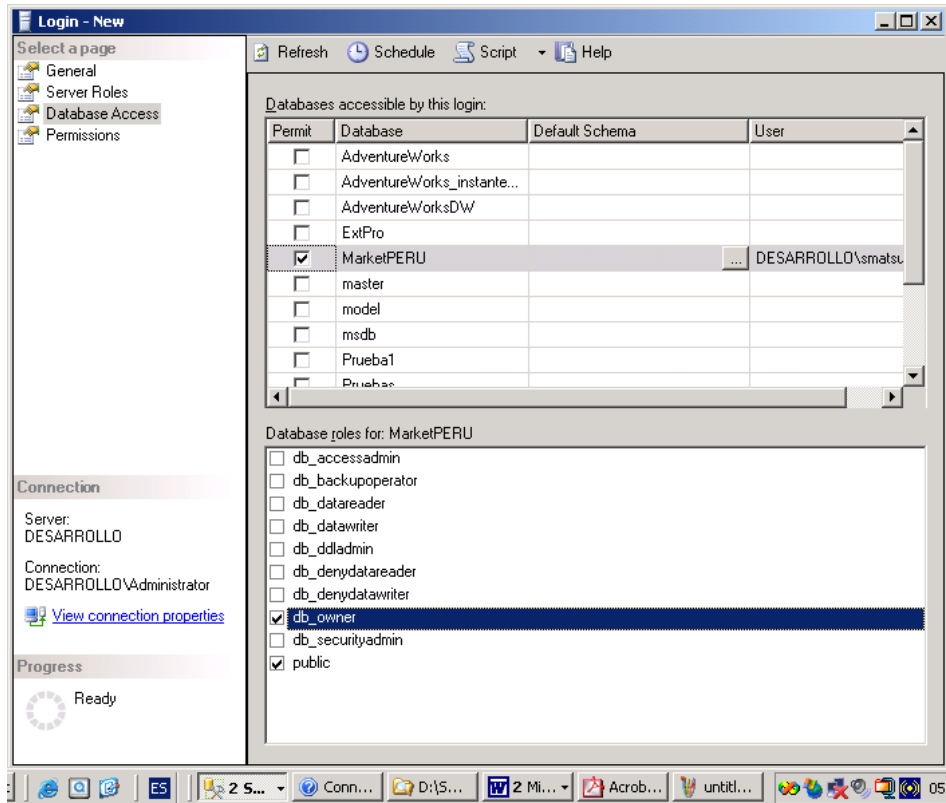


8. Seleccione la cuenta **smatsukawa** y haga clic en **OK**. La cuenta se copia en el diálogo **Select User or Group**.
9. Haga clic en **OK** para cerrar **Select User or Group**.
10. En **Server access** de la página **General** en la ventana **Login – New**, verifique que esté seleccionada la opción **Grant server access** (conceder acceso al servidor).

11. En la lista desplegable **Database** de **Defaults** seleccione la base de datos **MarketPERU**.



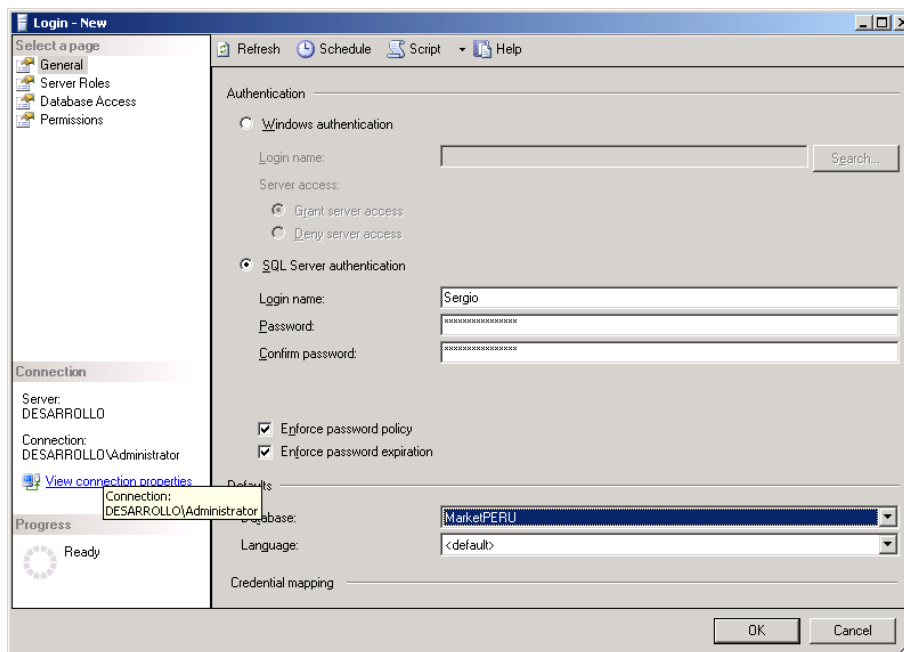
12. En **Select a page** seleccione la página **Database Access**.
13. En la lista de bases de datos disponible marque la base de datos **MarketPERU**. Se crear el usuario de base de datos **smatsukawa**.
14. En la lista **Database roles for: MarketPERU** marque el rol de base de datos **db_owner** para que la cuenta **smatsukawa** sea reconocida como dueña de la base de datos.



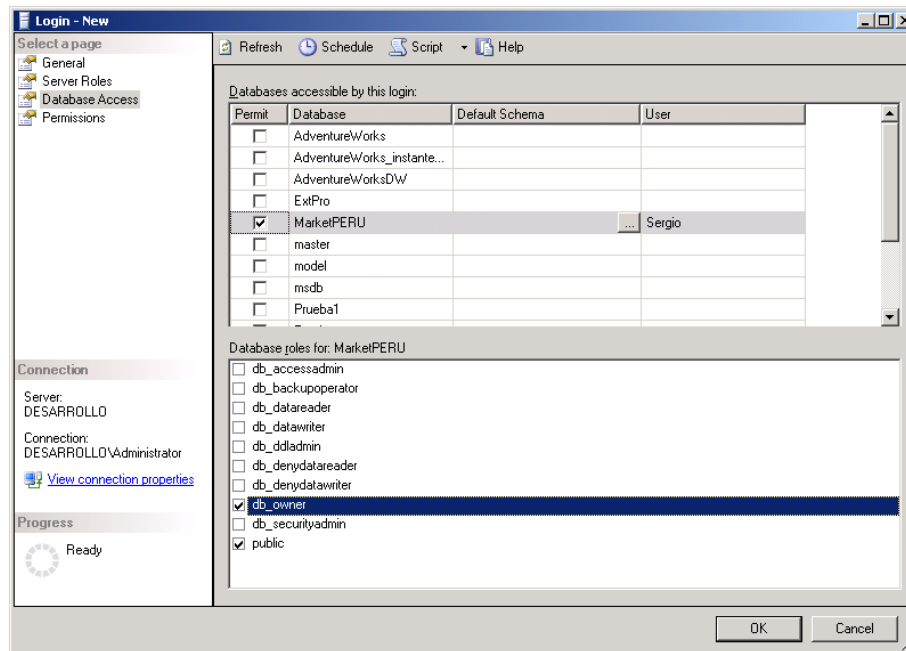
15. Haga clic en el botón **OK** para cerrar **Login – New** y registrar el login name.
16. En el **Object Explorer** expanda la carpeta **Logins**. Se debe mostrar la cuenta de usuario Windows **smatsukawa** como login name de SQL Server.
17. Para probar la cuenta, cierre todas sus aplicaciones y reinicie su Windows con la cuenta **smatsukawa**. Abra **SQL Server Management Studio**, y conéctese a su servidor utilizando **Autenticación Windows**.
18. Revise la base de datos **MarketPERU**.
19. Trate de revisar cualquier otra base de datos.

Ejercicio 156: Creación de un login name estándar

1. En el **Object Explorer** de **SQL Server Management Studio** expanda la carpeta **Security** de su servidor.
2. Haga un clic secundario sobre la carpeta **Logins** y ejecute **New Login**.
3. En **Authentication** de la página **General** seleccione la opción **SQL Server authentication**.
4. En **Login name** digite el identificador del login name. Por ejemplo, digite **Sergio**.
5. En **Password** digite la contraseña del login name.
6. En **Confirm password** vuelva a digitar la contraseña para su verificación.
7. En **Database** de **Defaults** seleccione la base de datos **MarketPERU**.



8. Seleccione la página **Database Access**.
9. Marque la base de datos **MarketPERU**.
10. En **Database roles for: MarketPERU** marque el rol **db_owner**.



11. Haga clic en **OK** para crear el login name.
12. Para probar el login name estándar, haga clic en **New Query** de la barra de herramientas, y luego en **Database Engine Query**. Se abre el diálogo **Connect to Database Engine**.
13. En **Authentication** seleccione **SQL Server Authentication**.
14. En **Login**, digite el login name que acaba de crear.
15. En **Password** digite la contraseña.



16. Haga clic en **Connect** para conectarse al servidor. Note que se conecta al servidor y por defecto "se para" en la base de datos **MarketPERU**.

17. En el **Code Editor** digite y ejecute la siguiente instrucción:

```
USE ExtPro  
go
```

18. Se produce el siguiente error:

```
Msg 916, Level 14, State 1, Line 1  
The server principal "Sergio" is not able to access the  
database "ExtPro" under the current security context.
```

El login name **Sergio** no tiene acceso a la base de datos **ExtPro**.

Los roles fijos de servidor (Server Roles)

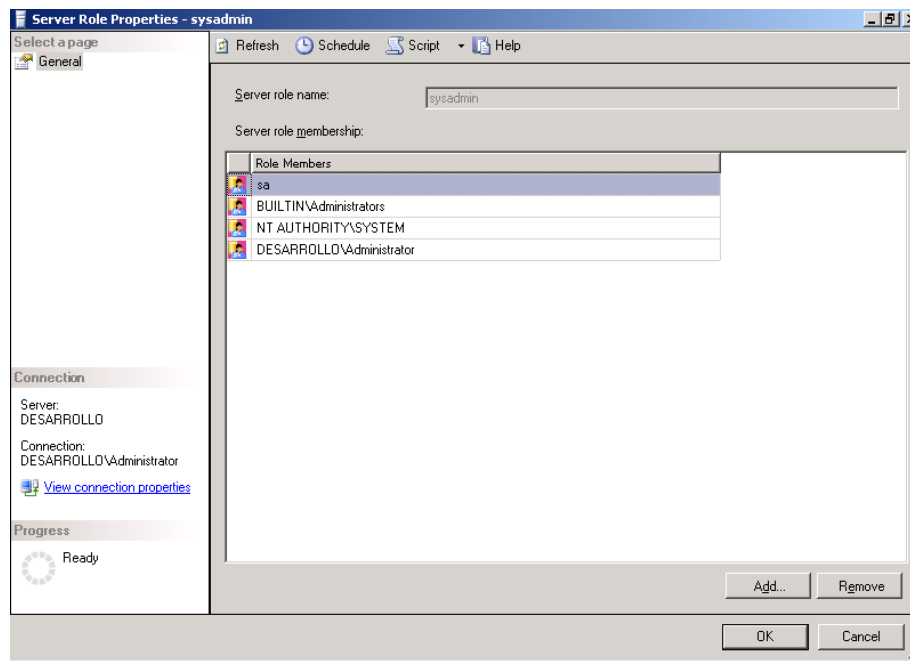
Los roles fijos de servidor proporcionan grupos de privilegios administrativos a nivel del servidor SQL. La pertenencia de un login name a uno ó más roles fijos de servidor determina el conjunto de tareas administrativas que dicho login name puede llevar a cabo a nivel del servidor.

Los roles fijos de servidor son los siguientes:

Rol	Descripción	Permisos
sysadmin	Administradores del sistema	Puede ejecutar cualquier tarea en el servidor SQL.
dbcreator	Creadores de bases de datos	Puede crear y modificar las bases de datos.
diskadmin	Administradores de archivos de disco	Puede manejar los archivos de disco.
processadmin	Administradores de procesos	Puede administrar los procesos SQL Server.
serveradmin	Administradores del servidor	Puede cambiar las opciones de configuración del servidor y "bajar" (shutdown) el servidor.
setupadmin	Administradores de configuración remota	Puede añadir y eliminar servidores vinculados, así como ejecutar algunos procedimientos almacenados del sistema.
securityadmin	Administradores de seguridad	Puede administrar los logins y los permisos CREATE DATABASE.
bulkadmin	Ejecutores de inserciones por lotes	Puede ejecutar la sentencia BULK INSERT.

Ejercicio 157: Verificación de un rol fijo de servidor

1. En el **Object Explorer** de **SQL Server Management Studio** expanda la carpeta **Security** de su servidor.
2. Expanda la carpeta **Server Roles**.
3. Para verificar un rol, haga doble sobre el rol. Por ejemplo, haga doble sobre **sysadmin**. Se abre la ventana **Server Role Properties – sysadmin**.



4. Se muestra la relación de cuentas pertenecientes al rol **sysadmin**.
5. Cierre la ventana **Server Role Properties**.

Los roles fijos de base de datos (Database Roles)

Los roles fijos de base de datos proporcionan grupos de privilegios administrativos a nivel de una base de datos. La pertenencia de un login name a uno ó más roles fijos de base de datos determina el conjunto de tareas dicho login name puede llevar a cabo en la base de datos.

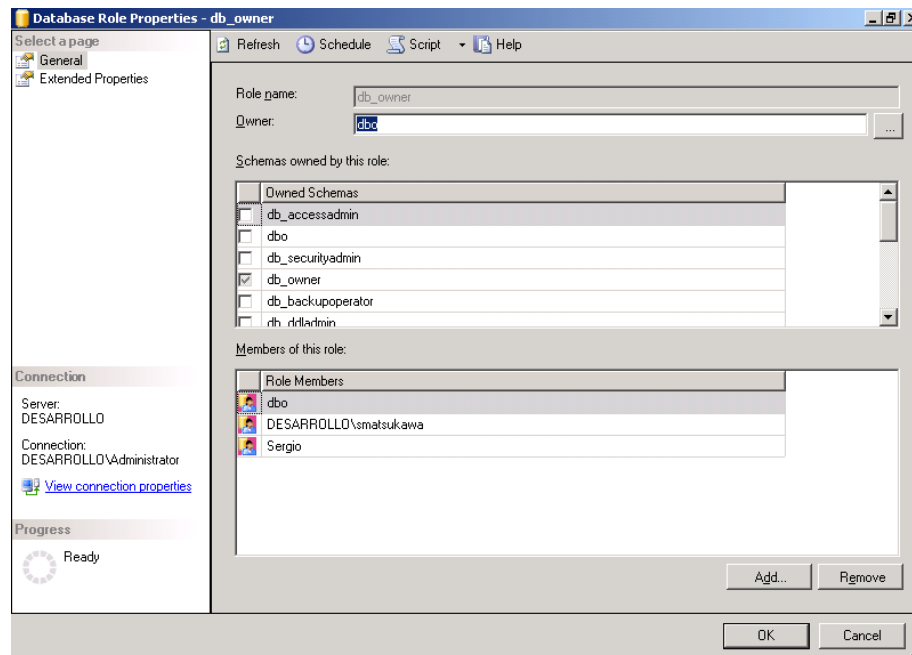
Los roles fijos de bases de datos son los siguientes:

Rol	Descripción	Permisos
public	Permisos generales	Define los permisos predeterminados para todos los login name que acceden a la base de datos.
db_owner	Dueños de la base de datos	No tiene restricciones sobre las operaciones a ejecutar en la base de datos.
db_accessadmin	Administradores de acceso	Administra el acceso a la base de datos para las cuentas y grupos Windows, y los login names de SQL Server.
db_ddladmin	Ejecutores de declaraciones DDL	Puede ejecutar cualquier declaración DDL.
db_securityadmin	Administradores de la seguridad	Puede administrar la pertenencia a los roles de base de datos y los permisos.
db_backupoperator	Ejecutores de copias de seguridad	Puede obtener copias de seguridad de la base de datos.

Rol	Descripción	Permisos
db_datareader	Lectores de datos	Puede leer el contenido de cualquier tabla ó vista.
db_datawriter	Escritores de datos	Puede modificar los datos en las tablas.
db_denydatareader	Sin acceso de lectura	No puede leer el contenido de las tablas ó vistas.
db_denydatawriter	Sin acceso de escritura	No puede modificar los datos en las tablas.

Ejercicio 158: Verificación de un rol fijo de base de datos

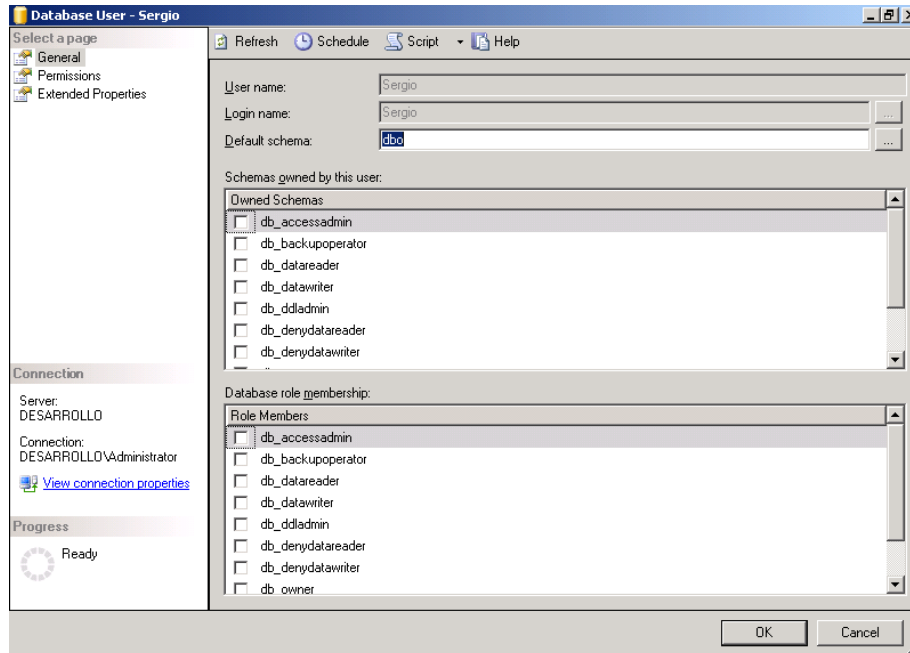
1. En el **Object Explorer** de **SQL Server Management Studio** expanda la carpeta **Databases**.
2. Expanda la base de datos cuyos roles desea verificar. Por ejemplo, expanda **MarketPERU**.
3. En **MarketPERU**, expanda la carpeta **Security**, y luego la carpeta **Roles**.
4. Expanda la carpeta **Database Roles**.
5. Haga doble clic sobre el rol a verificar. Por ejemplo, haga doble clic sobre **db_owner**. Se abre la ventana **Database Role Properties – db_owner**.



6. Se muestra la relación de miembros del rol fijo de base de datos **db_owner**.
7. Seleccione al miembro **Sergio**, y haga clic en el botón **Remove** para eliminarlo del rol.
8. Haga clic en OK para cerrar la ventana **Database Role Properties**.

Ejercicio 159: Registro de un login name en un rol fijo de base de datos

9. En el **Object Explorer** de **SQL Server Management Studio**, expanda la carpeta **Databases** de su servidor.
10. Expanda la base de datos **MarketPERU**, luego la carpeta **Security**, y finalmente la carpeta **Users**.
11. Haga doble clic sobre el usuario **Sergio** (el usuario de base de datos vinculado al login name **Sergio**). Se abre la ventana **Database User – Sergio**.



12. Observe que el usuario **Sergio** solo pertenece al rol **public** (**public** no se muestra ya que todos los usuarios pertenecen obligatoriamente a este rol). En **Database role membership**, marque la casilla del rol **db_datareader**. Esto le permite a **Sergio** leer todas las tablas y vistas de la base de datos.
13. Haga clic en **OK** para cerrar la ventana.

14. Para probar los privilegios de **Sergio**, abra el **Code Editor** conectándose al servidor con el login name **Sergio**.

15. Digite y ejecute el siguiente batch:

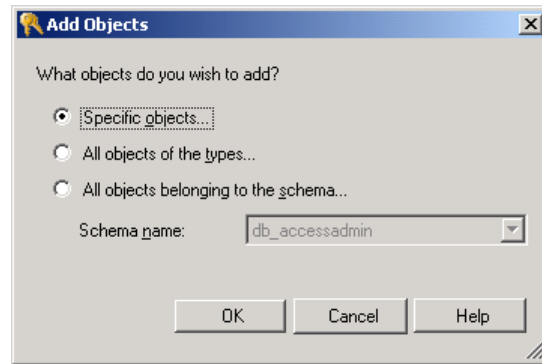
```
SELECT * FROM Categoria
SELECT * FROM Producto
SELECT * FROM Proveedor
SELECT * FROM Orden
SELECT * FROM Orden_detalle
SELECT * FROM Local
SELECT * FROM Guia
SELECT * FROM Guia_detalle
go
```

16. Observe que todas las consultas se ejecutan sin problemas. Como **Sergio** pertenece al rol **db_datareader**, él puede leer todas las tablas de la base de datos.

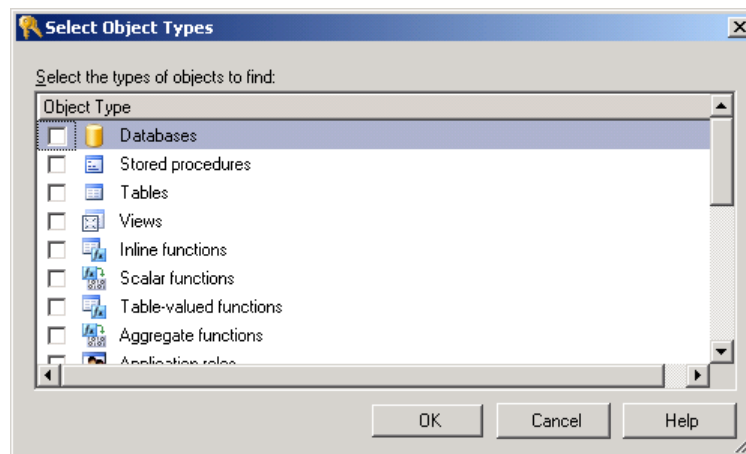
17. Cierre el **Code Editor**.

Ejercicio 160: Asignación de permisos

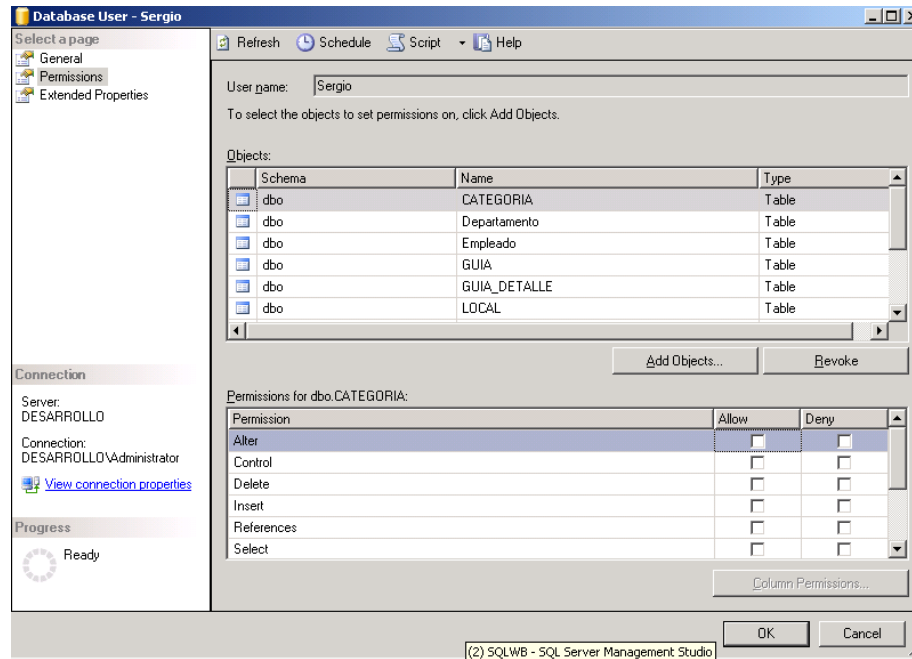
1. En el **Object Explorer** de **SQL Server Management Studio**, expanda la carpeta **Databases** de su servidor.
2. Expanda la base de datos **MarketPERU**, luego la carpeta **Security**, y finalmente la carpeta **Users**.
3. Haga doble clic sobre el usuario **Sergio** (el usuario de base de datos vinculado al login name **Sergio**). Se abre la ventana **Database User – Sergio**. Observe que pertenece al rol **db_datareader**.
4. Seleccione la página **Permissions**.
5. Haga clic en el botón **Add Objects**. Se abre el diálogo **Add Objects**.



6. Seleccione la opción **All objects of the types**, y haga clic en **OK**. Se abre el diálogo **Select Object Types**.



7. Marque la casilla **Tables**, y haga clic en **OK**. Se cargan todas las tablas de la base de datos **MarketPERU**.



8. En la lista **Objects**, seleccione la tabla **Guia**.
9. En la lista **Permissions for dbo.Guia**, seleccione la fila **Select**, y marque la casilla **Deny**.
10. Repita los pasos 8 y 9 para las tablas **Guia_detalle**, **Orden**, y **Orden_detalle**.
11. Haga clic en **OK** para cerrar la ventana.
12. Para probar los privilegios de **Sergio**, abra el **Code Editor** conectándose al servidor con el login name **Sergio**.

13. Digite y ejecute el siguiente batch:

```
SELECT * FROM Categoria
SELECT * FROM Producto
SELECT * FROM Proveedor
SELECT * FROM Orden
SELECT * FROM Orden_detalle
SELECT * FROM Local
SELECT * FROM Guia
SELECT * FROM Guia_detalle
go
```

14. Observe que todas la lectura de las tablas Guia, Guia_detalle, Orden, y Orden_detalle genera errores. Si bien **Sergio** pertenece al rol **db_datareader**, que le concede el privilegio para ejecutar SELECT sobre todas las tablas de la base de datos, le hemos denegado (DENY) el permiso SELECT sobre las tablas mencionadas.

15. Cierre el **Code Editor**.