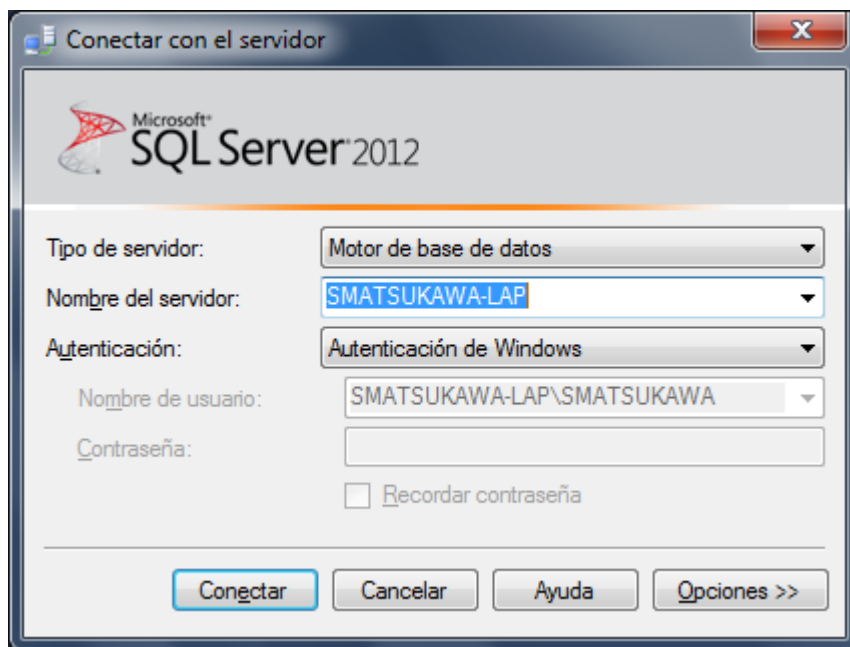


Capítulo XV

Introducción a la Seguridad en SQL Server

En este capítulo trataremos del control de acceso a SQL Server y a sus bases de datos, de los requisitos que se deben cumplir para utilizar los objetos de una base de datos y del control de las operaciones con los datos.

Cuando trabajamos con SQL Server por lo general utilizamos la aplicación cliente **SQL Server Management Studio**. Al iniciar esta aplicación se muestra la siguiente ventana de inicio de sesión



En **Tipo de servidor** seleccionamos **Motor de base de datos** si es que deseamos trabajar con el servidor de bases de datos.

En **Nombre del servidor** especificamos el nombre del servidor ó su dirección IP, ó digitamos **localhost**, la cadena **(local)** con los paréntesis incluidos, ó . (el punto) cuando el servidor de bases de datos es local.

En **Autenticación** debemos especificar con qué tipo de autenticación ingresamos al servidor de bases de datos.

Veremos a continuación el tema Autenticación.

1. TIPOS DE AUTENTICACIÓN EN SQL SERVER

El proceso de autenticación se entiende como aquél en el que el servidor verifica las credenciales de la persona ó de la aplicación que desea acceder a él.

Tenemos dos tipos de autenticación en SQL Server:

- **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

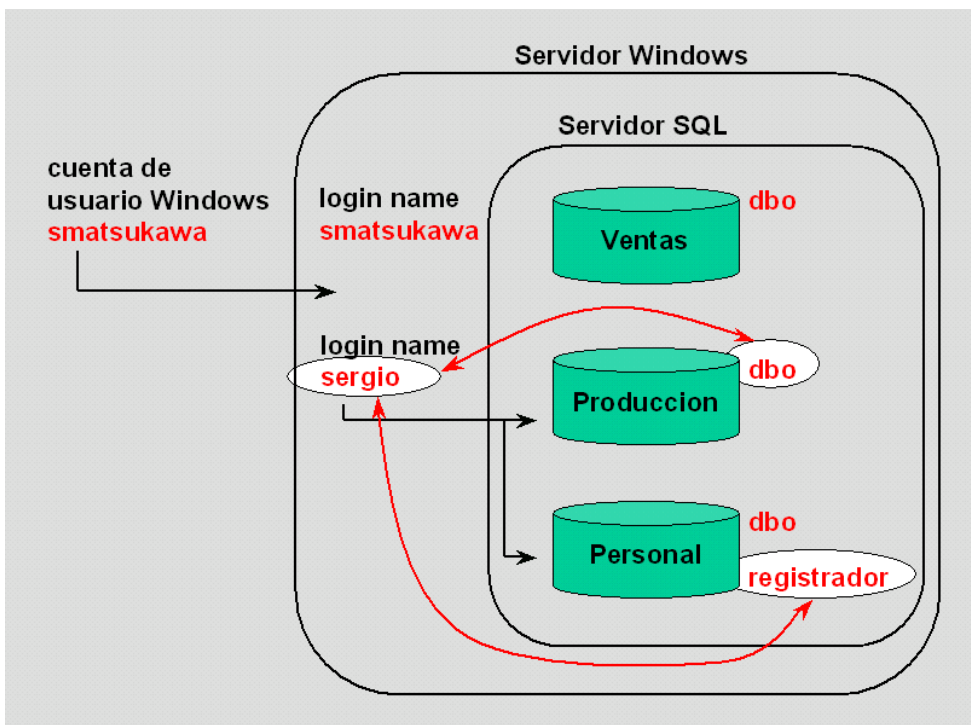
smatsukawa-lap\smatsukawa con la que ingreso a la red Windows) esté registrada también como **cuenta de inicio de sesión SQL Server** ó **login name SQL Server** en el servidor de bases de datos.

- **Autenticación SQL:** cuando después de haber accedido a Windows con la cuenta de usuario de Windows (por ejemplo, mi cuenta **smatsukawa-lap\smatsukawa**), accedemos a SQL Server utilizando una **cuenta de inicio de sesión SQL Server** ó **login name SQL Server** con un identificador distinto al de la cuenta de usuario Windows. Por ejemplo, con el login name **sa** (system administrator).

Como vemos, no importa cuál sea el tipo de autenticación que utilizamos, si no contamos con un **login name SQL Server**, 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.

2. PROCESO DE AUTENTICACIÓN EN SQL SERVER

El diagrama siguiente muestra esquemáticamente el proceso de autenticación 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**.

Cuenta de usuario Windows: es la cuenta de usuario ó de grupo que permite acceder a los recursos de la red administrada por Windows.

Login name SQL Server: es la cuenta que permite iniciar sesión en SQL Server y proporciona acceso al servidor de base de datos.

Autenticación SQL Server: se presenta cuando primero se accede a Windows con una cuenta de usuario Windows, y luego se accede a SQL Server con una cuenta propia de SQL Server (login name SQL Server).

Autenticación integrada a Windows: se presenta cuando no se necesita una cuenta propia de SQL Server, y se accede a SQL server con la cuenta de usuario Windows; para esto se requiere que la cuenta de usuario Windows esté registrada en SQL Server (login name SQL Server creado a partir de la cuenta de usuario Windows).

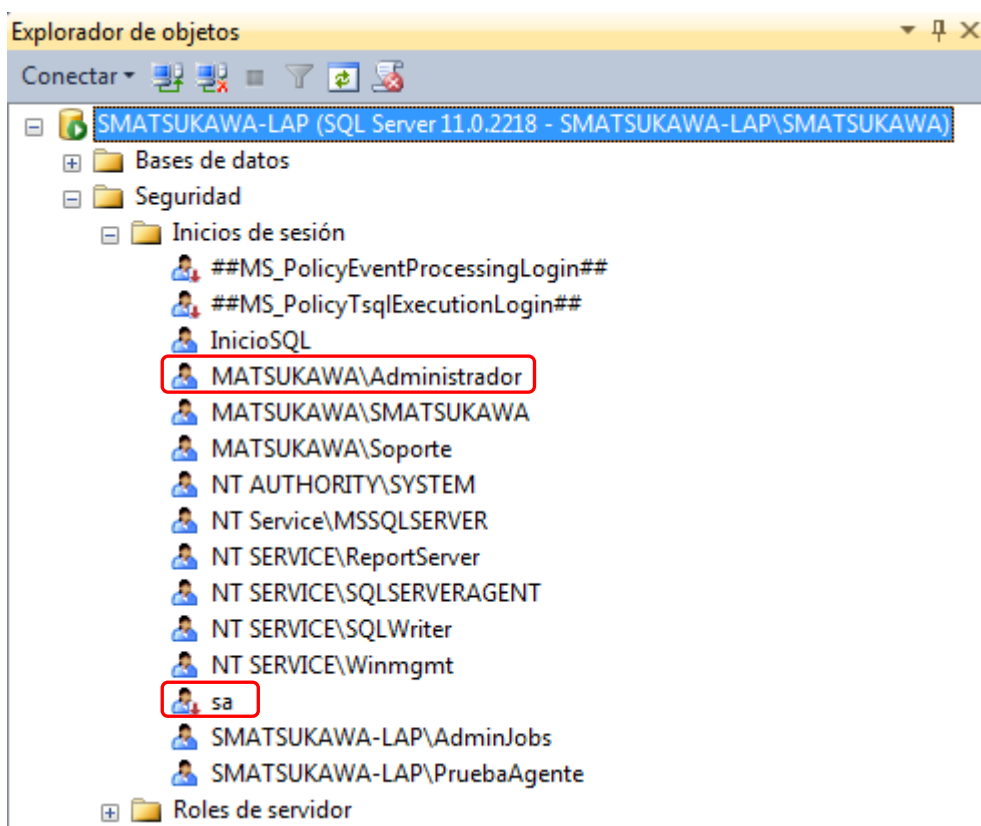
Usuario de base de datos: es la cuenta que se genera cuando a un login name SQL Server se le da acceso a una base de datos. De modo predeterminado, este acceso a la base de datos solo permite consultar la metadata de la base de datos. El usuario de base de datos es la entidad de seguridad que obtiene los permisos para utilizar los objetos de la base de datos y operar los datos.

2.1. La cuenta Administrador de Windows

Esta cuenta de Windows y la cuenta de grupo Administradores de Windows se registran de modo predeterminado como login name de SQL con privilegios de administrador de SQL Server durante la instalación de SQL Server. Es por esto que los administradores de Windows pueden acceder sin restricciones a SQL Server.

Ejercicio 15.1: Verificando la cuenta Administrador de Windows

1. Inicie una sesión **SQL Server Management Studio** y conéctese a su servidor SQL.
2. En el panel **Explorador de objetos**, expanda el nodo **Seguridad**, luego expanda el nodo **Inicios de sesión**.
3. Se muestra la entrada para la cuenta **Administrador** de Windows.



2.2. Login name estándar sa

La instalación de SQL Server crea también un login name propio de SQL Server identificado como **sa** (system administration), inicialmente deshabilitado y sin contraseña. Este login name tiene privilegios de administrador de SQL Server. Observe la imagen que se muestra arriba. El login name **sa** se muestra con una flechita apuntando hacia abajo.

3. MODOS DE AUTENTICACIÓN DE SQL SERVER

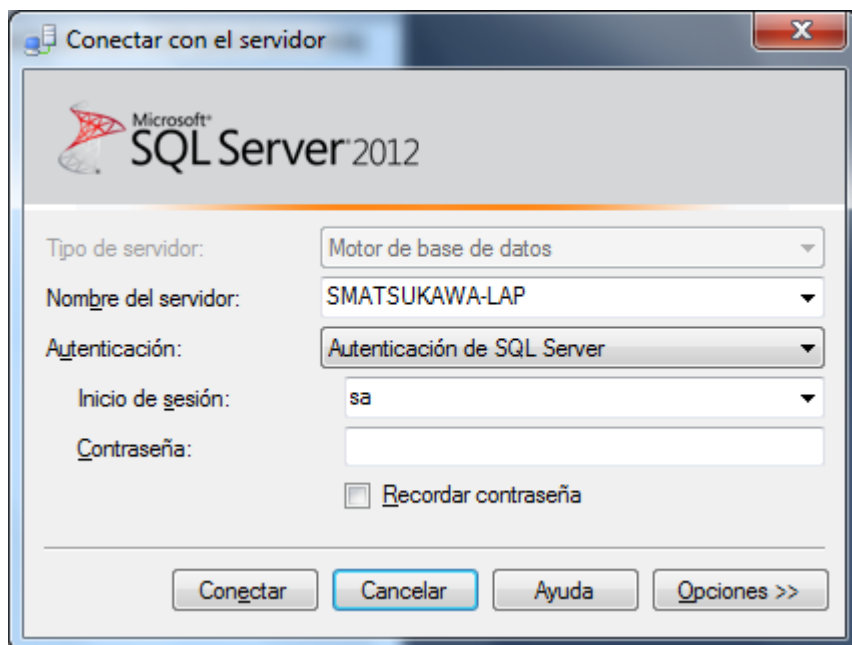
Hemos visto que SQL Server tiene dos tipos de autenticación: la **Autenticación integrada a Windows** y la **Autenticación SQL Server**.

El término "modo de autenticación" hace referencia a qué tipo de autenticación acepta nuestro servidor de base de datos. SQL Server se puede configurar en cualquiera de los siguientes dos modos de autenticación:

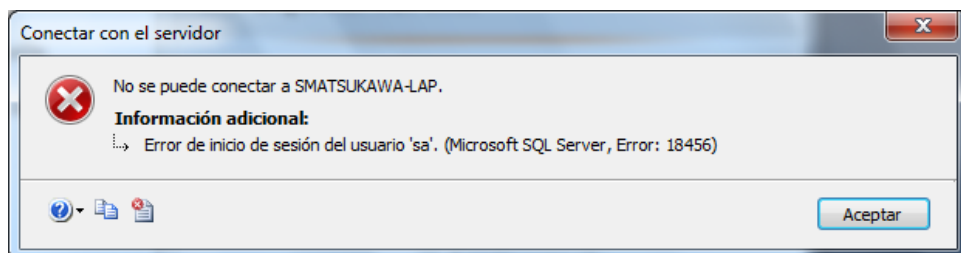
- **Modo de autenticación de Windows** (Modo Solo Windows): en este caso SQL Server solo acepta la autenticación integrada a Windows, es decir que solo podemos acceder a SQL Server con una cuenta de usuario Windows que se haya registrado como login name SQL Server.
- **Modo de autenticación de Windows y SQL Server** (Modo Mixto): si el servidor está configurado con este modo acepta los dos tipos de autenticación: la integrada a Windows y la de SQL Server.

Ejercicio 15.2: Conexión a SQL Server con autenticación SQL Server

1. En el **Explorador de objetos**, en la barra de herramientas, haga clic en el botón **Conectar**, y seleccione **Motor de base de datos**.
2. En la ventana **Conectar con el servidor**, en **Nombre del servidor** especifique su servidor SQL.
3. En **Autenticación** seleccione **Autenticación de SQL Server**.
4. En **Inicio de sesión** digite **sa**. La entrada para **Contraseña** déjela en blanco. Recuerde que si su SQL Server lo ha instalado hace poco y no le ha cambiado la configuración, la contraseña de **sa** no está definida.



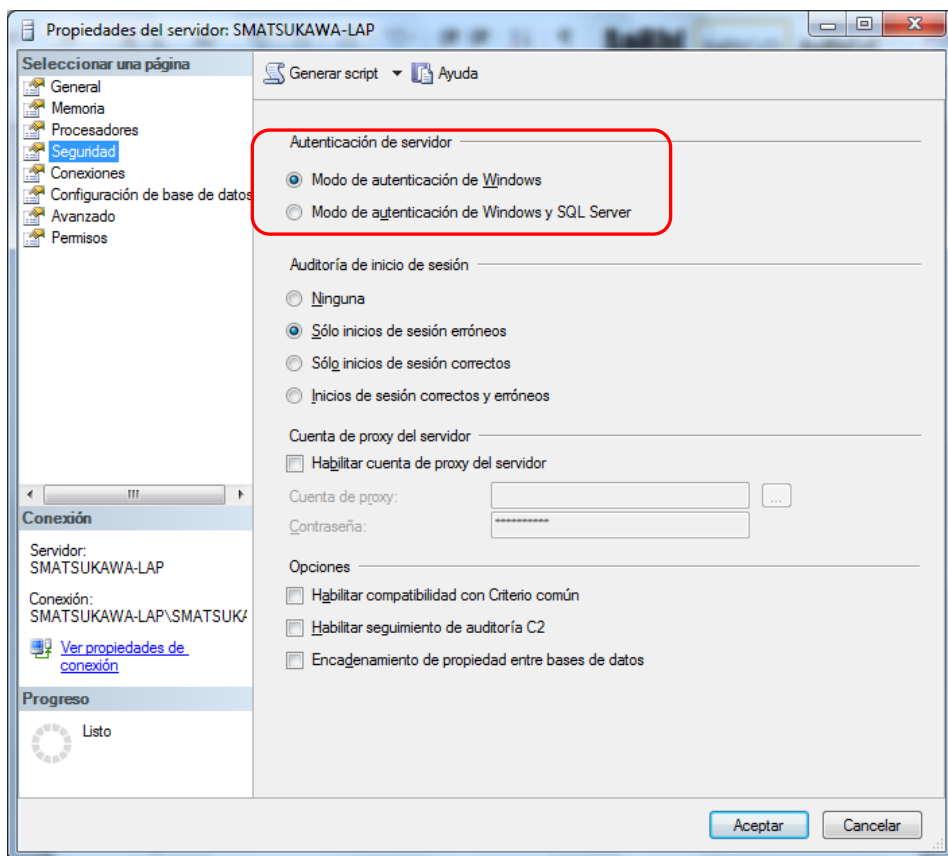
5. Haga clic en el botón **Conectar**. Si recibe el siguiente mensaje, tenemos que revisar la configuración de seguridad del servidor.



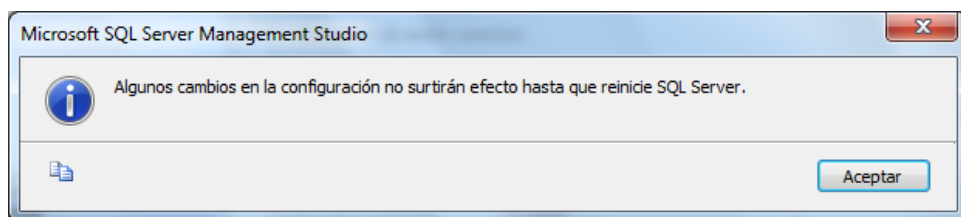
6. Haga clic en **Aceptar** para cerrar la ventana con el mensaje, y luego clic en **Cancelar** para cerrar la ventana **Conectar con el servidor**.

Ejercicio 15.3: Verificación del modo de autenticación de SQL Server

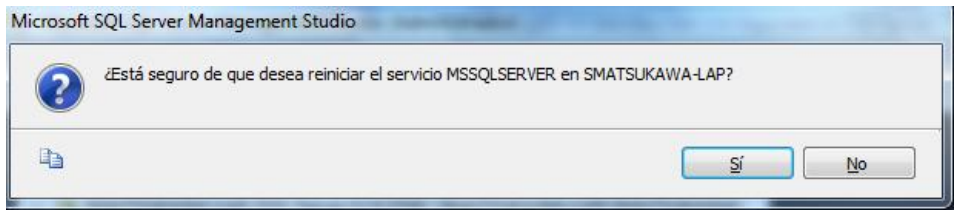
1. En **SQL Server Management Studio**, en el **Explorador de objetos**, haga clic secundario sobre su servidor SQL, y luego clic en **Propiedades**.
2. En la ventana **Propiedades del servidor** seleccione la página **Seguridad**.
3. En **Autenticación de servidor** seleccione el modo de autenticación con el que desea configurar su servidor:



4. Para que el servidor acepte la conexión del login name SQL Server **sa**, seleccione **Modo de autenticación de Windows y SQL Server** y haga clic en **Aceptar**. Recibirá el siguiente mensaje:



5. Haga clic en **Aceptar** para cerrar la ventana del mensaje.
6. Haga clic secundario en su servidor SQL, luego clic en **Reiniciar**. Se mostrará una ventana solicitando la confirmación, ya que el reinicio del servidor afectará el trabajo de las sesiones actualmente conectadas a SQL Server.

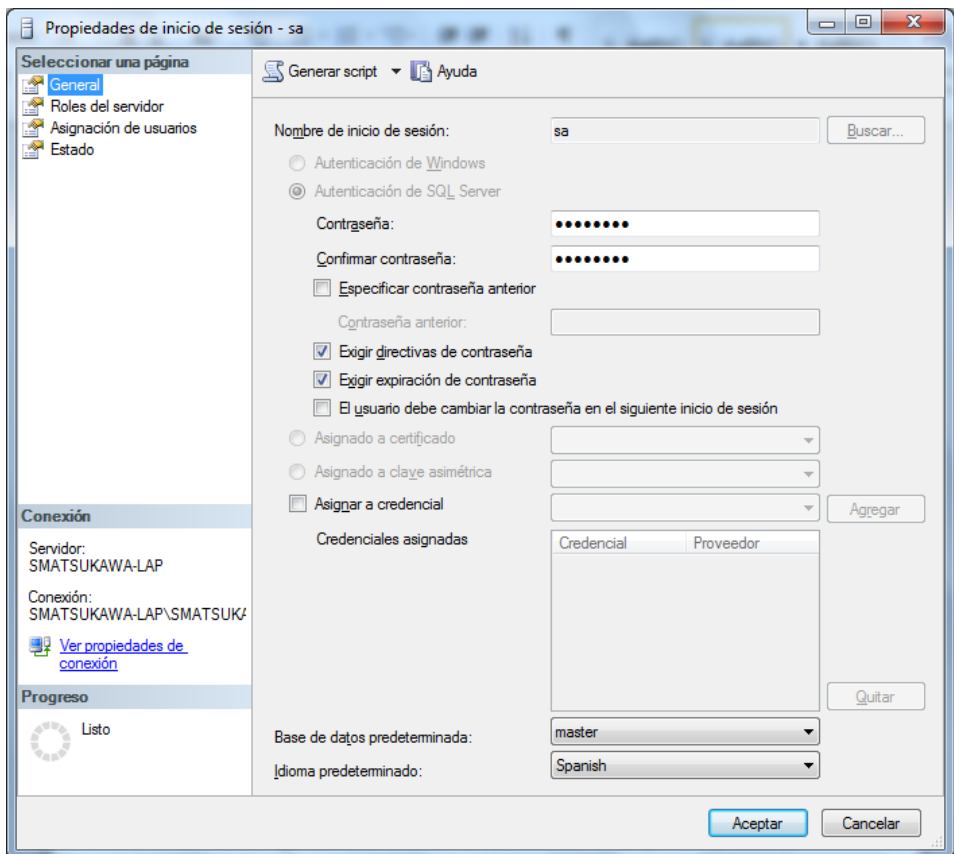


7. Haga clic en **Sí** para reiniciar el servidor.

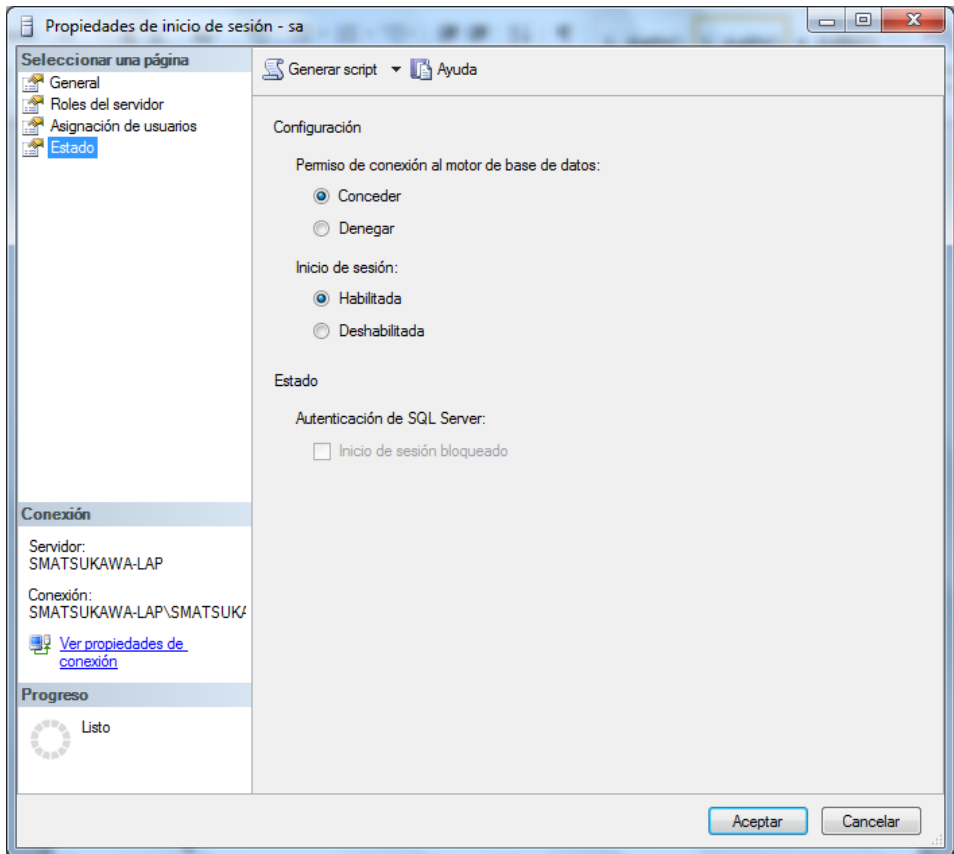
Ejercicio 15.4: Configuración del login name SQL Server sa

En una instalación nueva de SQL Server, el login name **sa** está inicialmente deshabilitado y no tiene contraseña. Procederemos a configurarlo.

1. En **SQL Server Management Studio** inicie su sesión con autenticación Windows.
2. En el **Explorador de objetos**, expanda la carpeta **Seguridad**, expanda **Inicios de sesión**, y haga doble clic sobre la cuenta **sa**.
3. En la ventana **Propiedades de inicio de sesión – sa**, en **Seleccionar una página**, seleccione la página **General**.
4. En **Contraseña**, digite la contraseña para la cuenta **sa**.
5. En **Confirmar contraseña**, digite nuevamente la contraseña.



6. En **Seleccionar una página**, seleccione la página **Estado**.
7. En **Configuración**, en **Inicio de sesión**, seleccionar la opción **Habilitada**.



8. Haga clic en **Aceptar** para finalizar la configuración de la cuenta **sa**.

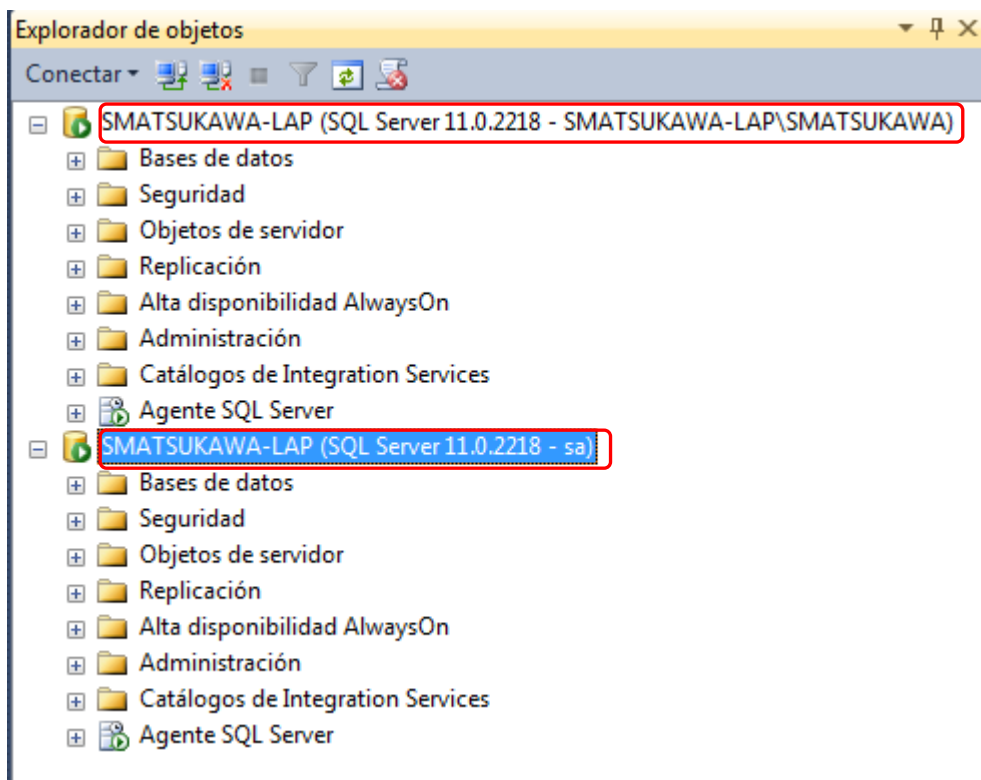
Ejercicio 15.5: Prueba de la cuenta **sa**

1. En **SQL Server Management Studio**, en el **Explorador de objetos**, clic en el botón **Conectar** de la barra de herramientas, luego clic en **Motor de base de datos**.
2. En la ventana **Conectar con el servidor**, en **Nombre del servidor**, verifique que está seleccionado el servidor deseado.
3. En **Autenticación**, seleccione **Autenticación de SQL Server**.
4. En **Inicio de sesión**, digite **sa**.
5. En **Contraseña**, digite la contraseña de la cuenta **sa**.



6. Haga clic en **Conectar**.

El panel **Explorador de objetos** que se ve muestra a continuación tiene registradas dos conexiones a SQL Server: una con autenticación integrada a Windows (cuenta de usuario Windows SMATSUKAWA-LAP\SMATSUKAWA), y la segunda con autenticación de SQL Server (cuenta **sa**).



4. DISEÑO DEL CONTROL DE ACCESO A UNA BASE DE DATOS

En un servidor de bases de datos podemos tener muchas bases de datos, cada una de ellas con sus propias tablas y objetos relacionados. Muchas personas pueden acceder a los datos:

- Unas solo pueden ver los datos, pero no pueden modificarlos.
- Otras pueden ver solo los datos de ciertas tablas.
- Algunas tienen la posibilidad de revisar los datos y modificarlos.
- Otras pueden ingresar nuevos datos.
- Muy pocas no tienen ninguna limitación en cuanto al acceso a los datos y las operaciones que pueden ejecutar.

¿Cómo controla SQL Server que cada persona solo pueda realizar aquello para lo que está autorizado?

Para explicar este tema simularemos el siguiente escenario.

4.1. Escenario

Se tiene la base de datos **Northwind** que registra la data de ventas de una empresa comercializadora de productos alimenticios gourmet. El script para instalar la base de datos y sus datos lo encontrará en el CD que acompaña al libro en la carpeta **ScriptsBD**.

Robert King es uno de los vendedores de la empresa, y como tal tiene que registrar sus ventas en la base de datos. Robert debe tener acceso a las siguientes tablas de la base de datos **Northwind** con los permisos indicados a continuación:

Tabla	Descripción	Permisos de los vendedores
Categories	Listado de las categorías de productos	Pueden leer los datos, pero no modificarlos.
Products	Listado de los productos	Pueden leer los datos y modificar solamente el contenido de la columna UnitsInStock .
Customers	Listado de los clientes	Pueden leer los datos, y registrar a un cliente nuevo. No pueden modificar los datos de clientes ya registrados. No pueden dar de baja a ningún cliente.
Orders	Listado de los pedidos	Pueden leer los datos, registrar un pedido nuevo, y modificar los datos de pedidos ya registrados. Pueden eliminar pedidos.
[Order Details]	Registro de los detalles de pedidos	Pueden leer los datos, registrar un item, modificar un item, eliminar un item.
Employees	Listado de los empleados	No tienen acceso a esta tabla.
Suppliers	Listado de los proveedores	No tienen acceso a esta tabla.
Shippers	Listado de los transportistas	No tienen acceso a esta tabla.

Se le pide diseñar el control de acceso de los vendedores de la empresa a la base de datos. Los vendedores deben acceder usando autenticación integrada a Windows.

4.2. Diseño del control de acceso

Para el diseño debemos tener en cuenta los siguientes elementos de control:

1. Creación en Windows de una cuenta de grupo denominada **VendedoresNw**.
4. Creación de una cuenta de usuario Windows para cada uno de los vendedores.
5. Agrupación de todos los vendedores en la cuenta de grupo **VendedoresNw**.
6. Registro de la cuenta de grupo **VendedoresNw** como login name SQL Server.
7. Acceso del login name SQL Server a la base de datos **Northwind**.
8. Asignación al usuario de la base de datos Northwind de los siguientes permisos en cada tabla:

Tabla	Rol	Permisos de los vendedores
Categories	Solo lectura	Pueden leer los datos, pero no modificarlos.
Products	Lectura/escritura	Pueden leer los datos y modificar solamente el contenido de la columna UnitsInStock .
Customers	Lectura/escritura	Pueden leer los datos, y registrar a un cliente nuevo. No pueden modificar los datos de clientes ya registrados. No pueden dar de baja a ningún cliente.
Orders	Lectura/escritura	Pueden leer los datos, registrar un pedido nuevo, y modificar los datos de pedidos ya registrados. Pueden eliminar pedidos.
[Order Details]	Lectura/escritura	Pueden leer los datos, registrar un item, modificar un item, eliminar un item.
Employees	Sin acceso	No tienen acceso a esta tabla.
Suppliers	Sin acceso	No tienen acceso a esta tabla.
Shippers	Sin acceso	No tienen acceso a esta tabla.

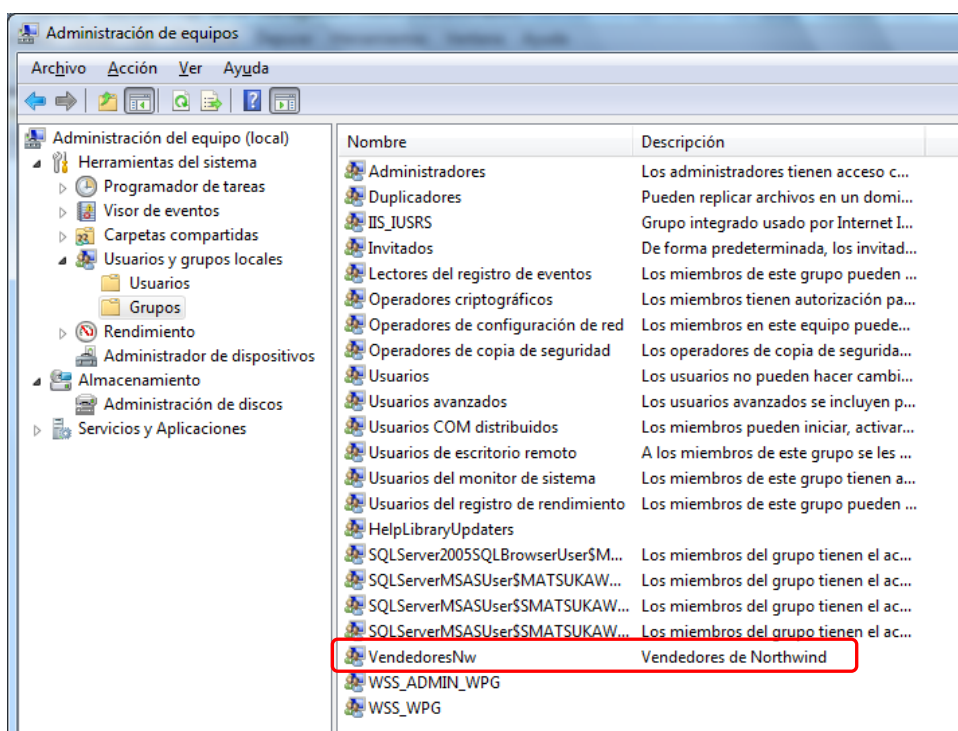
4.3. Creación de cuentas Windows

Si para controlar el acceso a SQL Server deseamos utilizar autenticación integrada a Windows, necesitamos asignarle a cada una de las personas ó grupos de personas que accederán a SQL Server, una cuenta de usuario ó una cuenta de grupo Windows.

Ejercicio 15.6: Creación de una cuenta de grupo Windows y de una cuenta de usuario Windows para el grupo

Para crear el grupo Windows **VendedoresNw** ejecute:

1. Clic secundario en el acceso directo **Equipo** de su máquina, clic en **Administrar**.
2. En la ventana **Administración de equipos**, en **Herramientas del sistema**, expanda **Usuarios y grupos locales**, clic secundario en **Grupos**, clic en **Grupo nuevo**.
3. En la ventana **Grupo nuevo**, en **Nombre de grupo**, digite **VendedoresNw**.
4. En **Descripción**, digite **Vendedores de Northwind**, clic en **Crear**, clic en **Cerrar**.



Para crear la cuenta de usuario Windows del vendedor Robert King ejecute:

1. En la ventana **Administración de equipos**, clic secundario en **Usuarios**, clic en **Nuevo usuario**.
2. En la ventana **Nuevo usuario**, en **Nombre de usuario**, digite **RKing**.
3. En **Nombre completo**, digite **Robert King**.

4. En **Descripción**, digite **Vendedor de Northwind**.
5. En **Contraseña** y **Confirmar contraseña**, especifique la contraseña inicial del usuario.

Usuario nuevo

Nombre de usuario: RKing

Nombre completo: Robert King

Descripción: Vendedor de Northwind

Contraseña:

Confirmar contraseña:

☒ El usuario debe cambiar la contraseña en el siguiente inicio de sesión

☐ El usuario no puede cambiar la contraseña

☐ La contraseña nunca expira

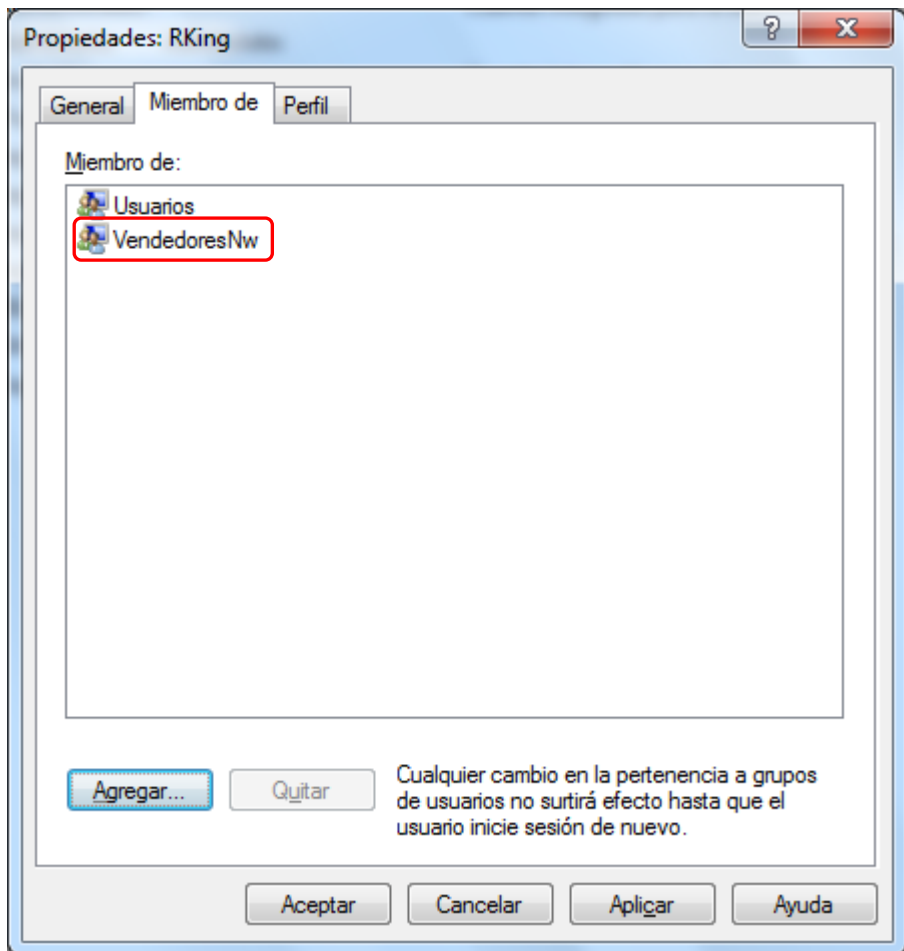
☐ La cuenta está deshabilitada

Ayuda Crear Cerrar

6. Clic en **Crear**, clic en **Cerrar**.

Para agregar al usuario **RKing** al grupo **VendedoresNw** ejecute:

1. En la ventana **Administración de equipos**, clic en **Usuarios**.
2. En el panel de detalles, doble clic en **RKing**.
3. En la ventana **Propiedades: RKing**, seleccione la ficha **Miembro de**, clic en **Agregar**, clic en **Opciones avanzadas**, clic en **Buscar ahora**.
4. En **Resultado de la búsqueda**, seleccionar **VendedoresNw**, clic en **Aceptar**, clic en **Aceptar**.



5. Clic en **Aceptar**. Cerrar la ventana **Administración de equipos**.

4.4. Registrar una cuenta Windows como login name SQL Server

Para que una cuenta Windows pueda acceder a SQL Server usando autenticación integrada a Windows se requiere que la cuenta Windows esté registrada en SQL Server como login name ó cuenta de inicio de sesión SQL.

Ejercicio 15.7: Registro de una cuenta Windows como login name SQL Server

Vamos a registrar en SQL Server a la cuenta de grupo **VendedoresNw** de Windows, de modo tal que todos los miembros de este grupo tengan acceso a SQL Server.

Para registrar la cuenta Windows en SQL Server:

1. En **SQL Server Management Studio**, en **Explorador de objetos**, en su servidor SQL, expanda **Seguridad**, clic secundario en **Inicios de sesión**, clic en **Nuevo inicio de sesión**.
2. En la ventana **Inicio de sesión**, en **Seleccionar una página**, en la página **General**, en **Nombre de inicio de sesión**, clic en **Buscar**.
3. En la ventana **Seleccionar Usuario o Grupo**, clic en **Tipos de objeto**.
4. En la ventana **Tipos de objeto**, marcar la casilla **Grupos**, clic en **Aceptar**.
5. En la ventana **Seleccionar Usuario o Grupo**, clic en **Opciones avanzadas**, clic en **Buscar ahora**.
6. En **Resultado de la búsqueda**, seleccionar **VendedoresNw**, clic en **Aceptar**, clic en **Aceptar**.
7. En la ventana **Inicio de sesión**, verifique que está seleccionada la opción **Autenticación de Windows**.
8. En **Base de datos predeterminada**, seleccione **Northwind**.

Inicio de sesión - Nuevo

Seleccionar una página

- General
- Roles del servidor
- Asignación de usuarios
- Elementos protegibles
- Estado

Conexión

Servidor: SMATSUKAWA-LAP

Conexión: SMATSUKAWA-LAP\SMATSUKAWA-LAP

Ver propiedades de conexión

Progreso

Listo

Generar script Ayuda

Nombre de inicio de sesión: SMATSUKAWA-LAP\VendedoresNw Buscar...

☒ Autenticación de Windows

☐ Autenticación de SQL Server

Contraseña:

Confirmar contraseña:

☐ Especificar contraseña anterior

Contraseña anterior:

☒ Exigir directivas de contraseña

☒ Exigir expiración de contraseña

☒ El usuario debe cambiar la contraseña en el siguiente inicio de sesión

☐ Asignado a certificado

☐ Asignado a clave asimétrica

☐ Asignar a credencial

Credenciales asignadas

Credencial	Proveedor
------------	-----------

Agregar

Quitar

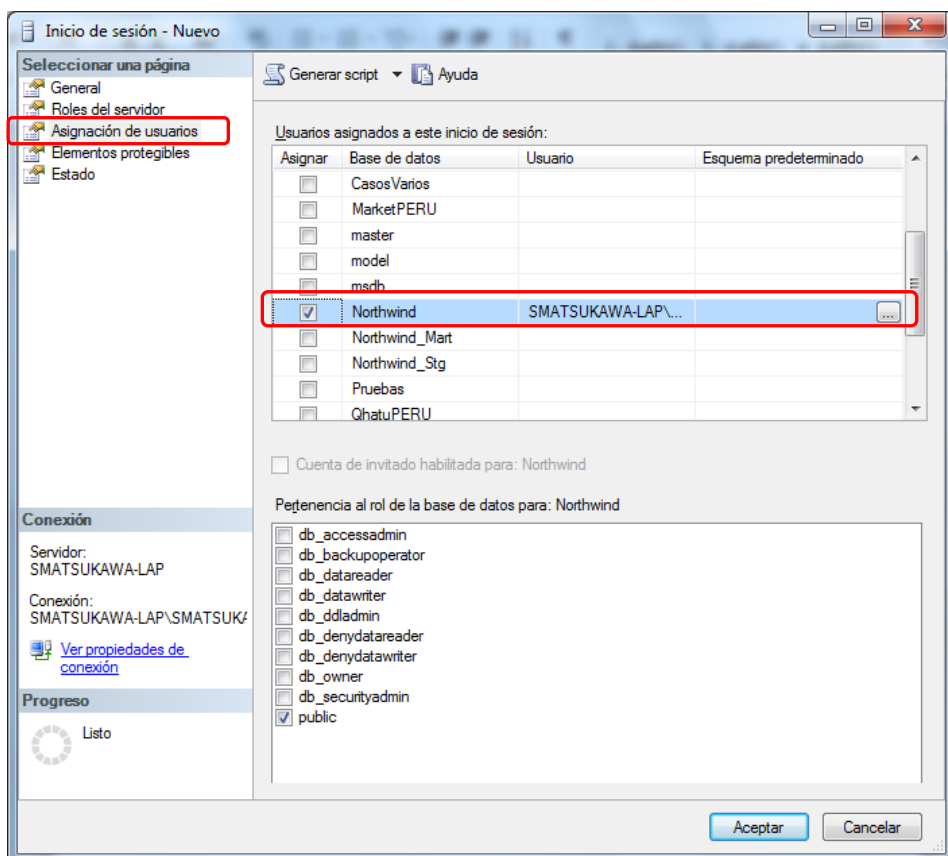
Base de datos predeterminada: Northwind

Idioma predeterminado: <predeterminado>

Aceptar Cancelar

Para darle acceso a la base de datos **Northwind** al nuevo login name SQL Server:

1. En **Seleccionar una página**, clic en la página **Asignación de usuarios**.
2. En **Usuarios asignados a este inicio de sesión**, marque la casilla de la base de datos **Northwind**. Se crea en la base de datos un usuario de base de datos que tiene el mismo identificador que el login name SQL Server.

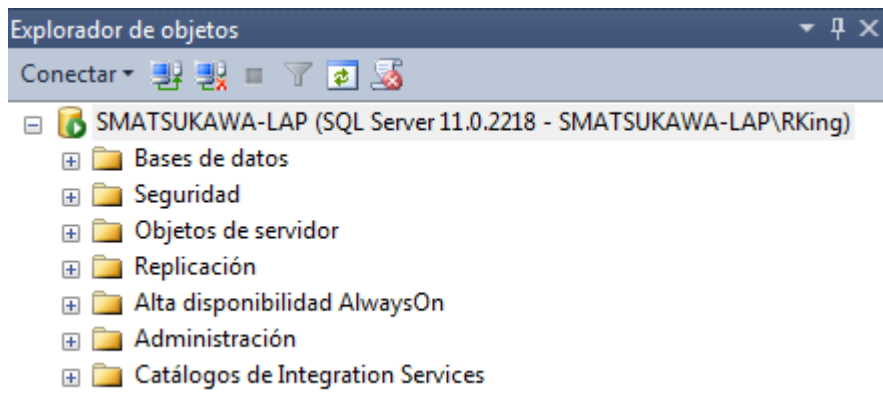


3. Clic en **Aceptar**.

Ejercicio 15.8: Iniciando una sesión SQL Server con la cuenta de usuario Windows RKing

1. Inicie una nueva sesión Windows pulsando [Ctrl]+[Alt]+[Supr].
2. Clic en **Cambiar de usuario**.
3. Inicie sesión con la cuenta de usuario Windows **RKing**.

4. Inicie **SQL Server Management Studio** con autenticación integrada a Windows. Observe que se ha conectado el login name **SMATSUKAWA-LAP\RKing**.



5. Abra una ventana de consulta. La sesión "se para" de modo predeterminado en la base de datos **Northwind**.
6. Ejecute la siguiente consulta:

```
SELECT * FROM Products
go
```

7. Recibe un mensaje de error que indica que no tiene permiso para ejecutar SELECT.
8. Regrese a su sesión habitual.

4.5. Asignación de permisos a un usuario de base de datos

La función del login name SQL Server es darle al propietario de la cuenta acceso a SQL Server, y a una ó más bases de datos a través de un usuario de la base de datos, tal como lo hemos comprobado con el login name **VendedoresNw** en el último ejercicio. Para que el poseedor del login name pueda realizar operaciones con los objetos de la base de datos se requiere que el usuario de base de datos asociado al login name tenga asignados los permisos necesarios.

Un usuario de base de datos puede obtener sus permisos de dos maneras:

- **Por su pertenencia a un rol de base de datos:** se puede establecer por ejemplo, que el usuario pertenezca al rol de base de datos **db_datareader**, lo que le permitirá ejecutar SELECT en cualquier tabla o vista de la base de datos.

- **Por habérsele asignado directamente un permiso:** se le puede conceder directamente al usuario el permiso SELECT sobre una tabla.

A continuación veremos qué es un rol de base de datos.

4.6. Roles de base de datos

Un rol de base de datos proporciona un grupo de privilegios a nivel de la base de datos. Un rol de base de datos agrupa un conjunto de permisos para determinado tipo de operaciones en la base de datos. La pertenencia de un usuario de la base de datos a uno ó más roles de base de datos determina las operaciones que el login name asociado al usuario puede llevar a cabo en la base de datos.

En una base de datos encontramos los siguientes roles:

Rol	Descripción	Permisos
public	Permisos generales	Define los permisos predeterminados mínimos 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.
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.

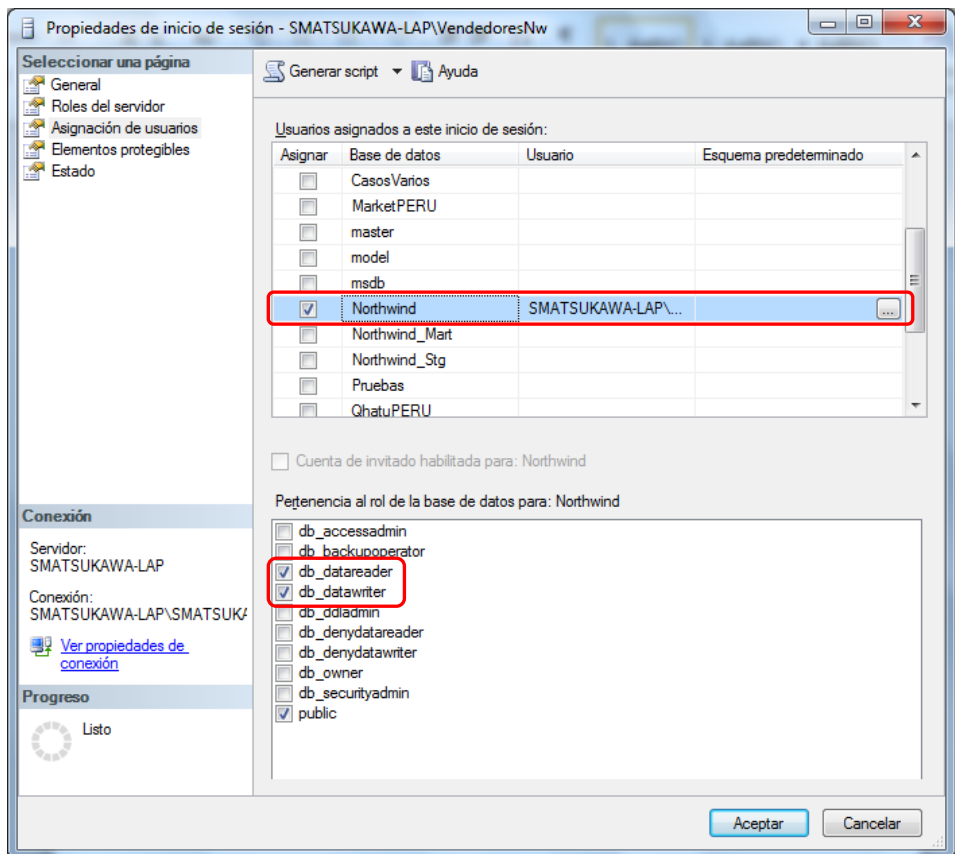
db_denydatawriter	Sin acceso de escritura	No puede modificar los datos en las tablas.
--------------------------	-------------------------	---

Ejercicio 15.9: Incluir un usuario de base de datos en un rol de base de datos

De acuerdo con las especificaciones de control de acceso a **Northwind** mencionadas arriba para el vendedor Robert King, que es miembro del grupo Windows **VendedoresNw**, áquel debe tener acceso de lectura y escritura en las tablas.

Vamos a incluir al usuario de la base de datos **Northwind** asociado al login name **VendedoresNw** en los roles de base de datos **db_datareader** y **db_datawriter**.

1. En **SQL Server Management Studio**, en **Explorador de objetos**, expanda **Seguridad**, expanda **Inicios de sesión**, doble clic en **VendedoresNw**.
2. En la ventana **Propiedades de inicio de sesión**, en **Seleccionar una página**, seleccione la página **Asignación de usuarios**.
3. En **Usuarios asignados a este inicio de sesión**, seleccione **Northwind**, verifique que la casilla de la columna **Asignar** está marcada.
4. En **Pertenencia al rol de la base de datos para: Northwind**, marque las casillas de **db_datareader** y **db_datawriter**.



5. Clic en **Aceptar** para finalizar.
6. Para probar los privilegios del login **VendedoresNw** regrese a su sesión Windows de la cuenta **RKing**.
7. En una ventana de consulta digite y ejecute el siguiente batch:

```

SELECT * FROM Categories
SELECT * FROM Products
SELECT * FROM Suppliers
SELECT * FROM Employees
SELECT * FROM Customers
SELECT * FROM Orders
SELECT * FROM [Order Details]
SELECT * FROM Shippers
go

```


8. Note que todas las consultas se ejecutan sin problemas ya que el usuario asociado al login name **VendedoresNw** pertenece al rol de base de datos **db_datareader**, por lo que puede leer todas las tablas y vistas.
9. Cierre la ventana de consulta.

4.7. Manejo de los permisos sobre los objetos de la base de datos

Por lo general, además de administrar la pertenencia de un usuario de la base de datos a uno o más roles de base de datos, se puede requerir gestionar el acceso a algunos de los objetos de la base de datos en forma individual.

En las especificaciones de control de acceso mostradas arriba para el usuario **VendedoresNw** de la base de datos **Northwind** se indica que este usuario:

- No debe escribir en la tabla **Categories**.
- En la tabla **Products** no debe insertar ni eliminar filas, pero si puede actualizar la columna **UnitsInStock**.
- En la tabla **Customers** no puede eliminar filas, ni modificar los datos de los clientes.
- No debe tener ningún tipo de acceso a las tablas **Employees**, **Suppliers** y **Shippers**.

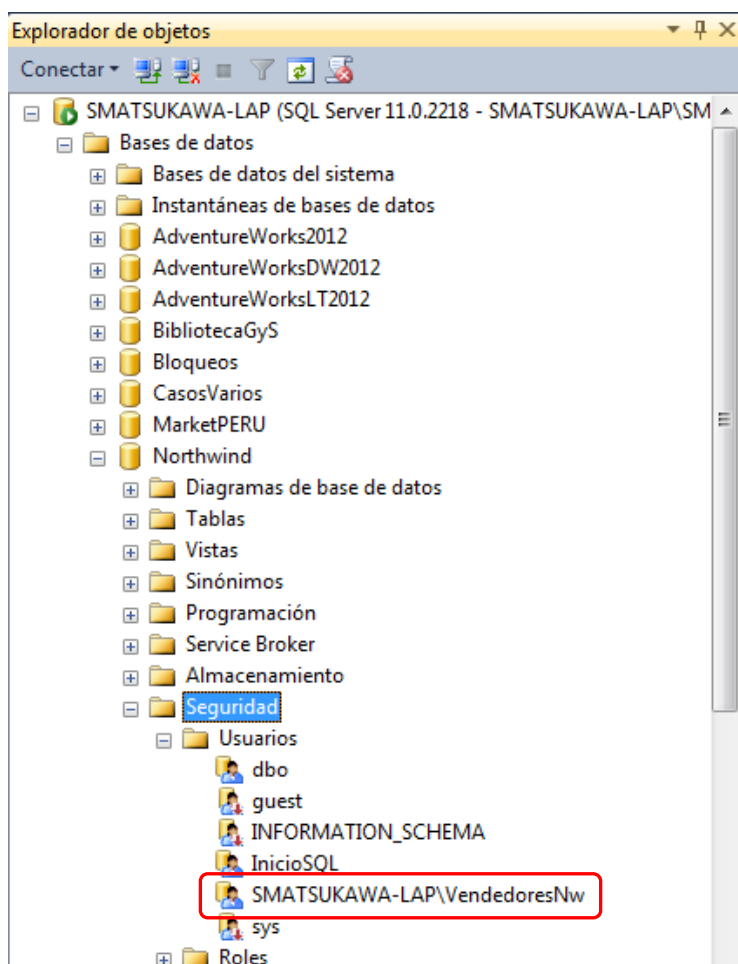
Como el usuario **VendedoresNw** pertenece al rol **db_datareader** de **Northwind**, puede ejecutar SELECT sobre cualquier tabla o vista de la base de datos. También pertenece al rol **db_datawriter**, lo que le permite ejecutar INSERT, UPDATE y DELETE en cualquier tabla o vista de la base de datos.

Para cumplir con sus especificaciones de control de acceso se debe:

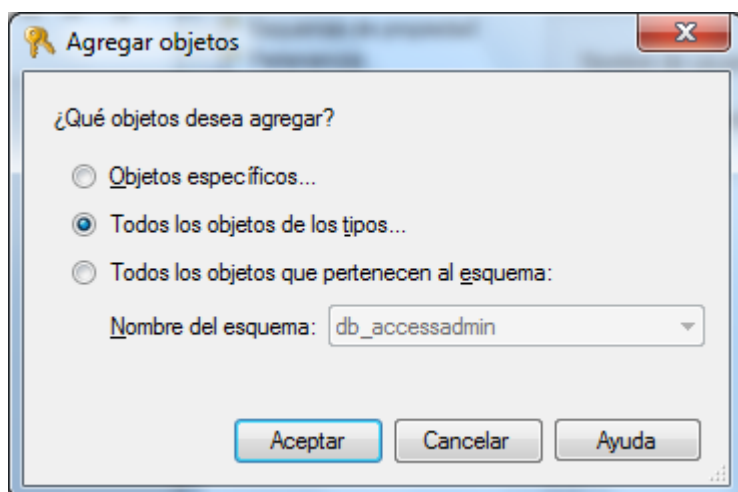
- Negarle la ejecución de INSERT, UPDATE y DELETE en la tabla **Categories**.
- Negarle la ejecución de INSERT y DELETE en la tabla **Products**. Permitirle ejecutar UPDATE, pero solo en la columna **UnitsInStock**.
- Negarle la ejecución de UPDATE y DELETE en la tabla **Customers**.
- Negarle la ejecución de SELECT, INSERT, UPDATE y DELETE en las tablas **Employees**, **Suppliers** y **Shippers**.

Ejercicio 15.10: Gestión de los permisos sobre los objetos de la base de datos

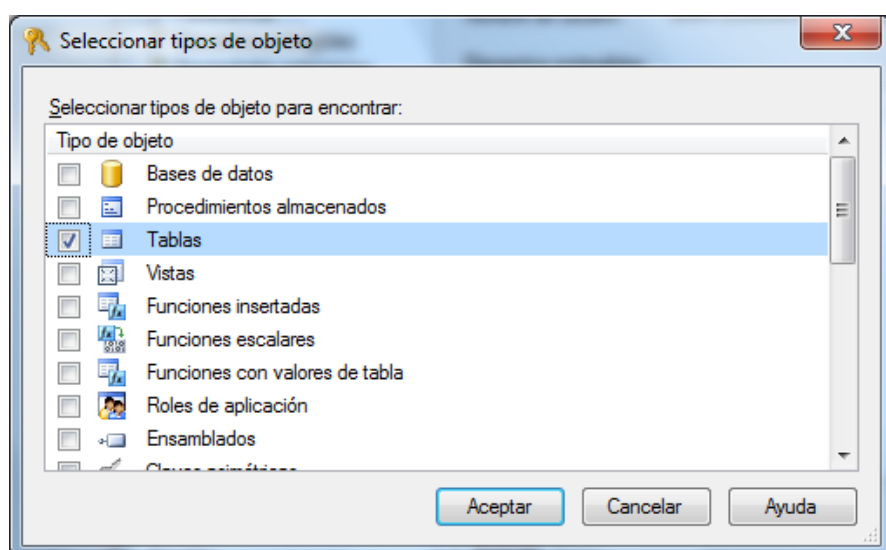
1. En **SQL Server Management Studio**, en **Explorador de objetos**, expanda **Bases de datos**, expanda **Northwind**, expanda **Seguridad**, expanda **Usuarios**, doble clic sobre **VendedoresNw**.



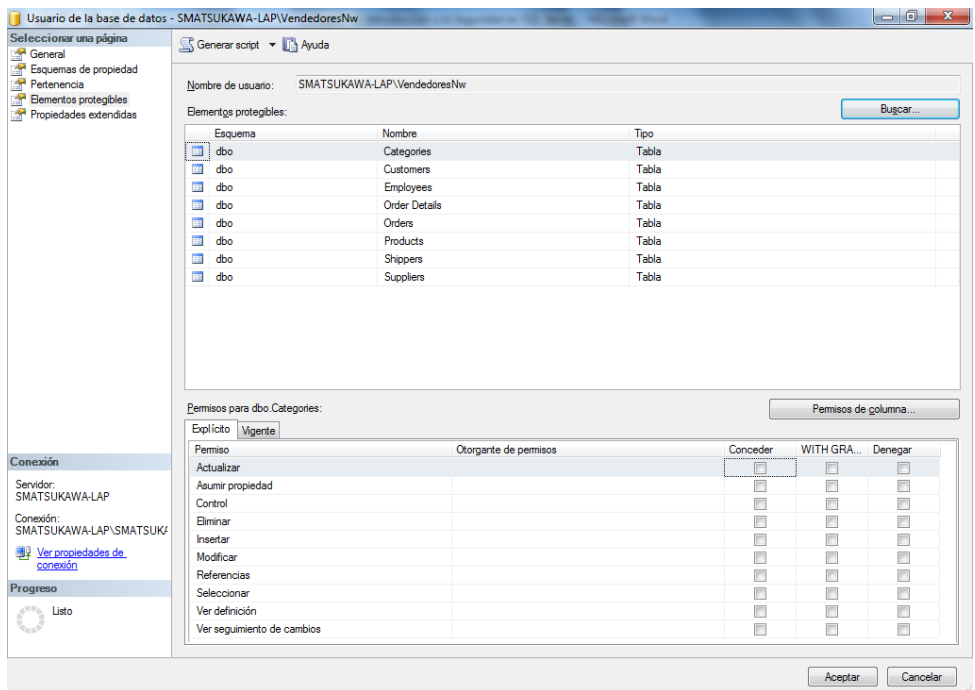
2. En la ventana **Usuario de la base de datos**, en **Seleccionar una página**, seleccione la página **Elementos protegibles**.
3. En la lista **Elementos protegibles**, clic en **Buscar**.
4. En el diálogo **Agregar objetos**, seleccione **Todos los objetos de los tipos**.



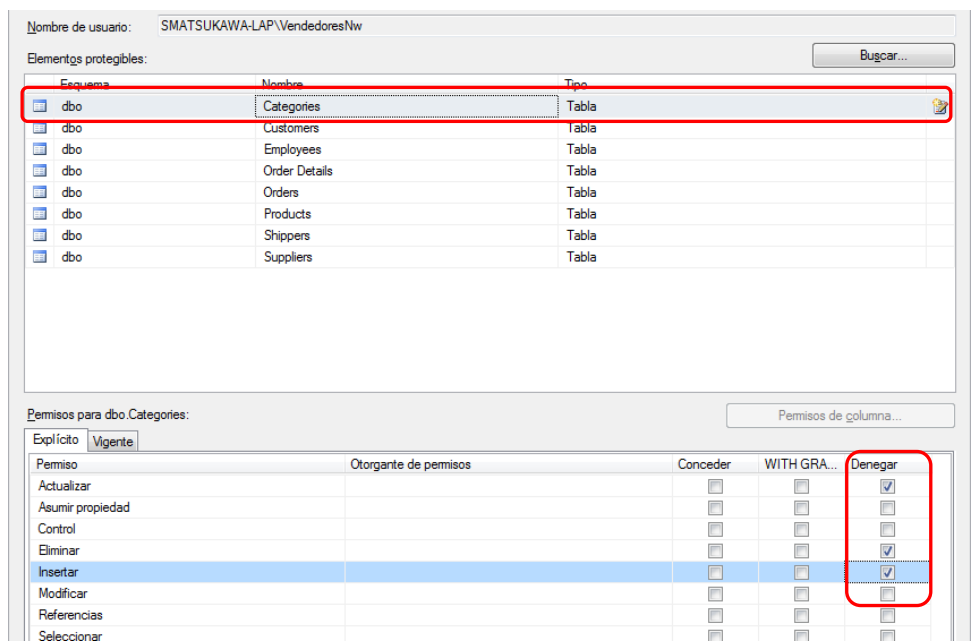
5. Clic en **Aceptar**. En el diálogo **Seleccionar tipos de objetos**, seleccione **Tablas**.



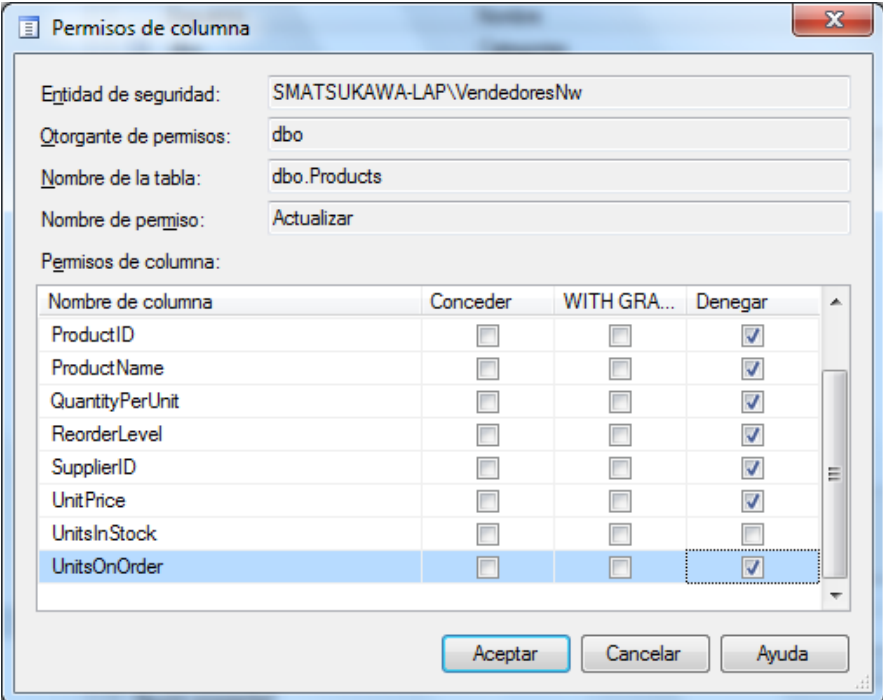
6. Clic en **Aceptar**. Se muestra la ventana **Usuario de la base de datos** con los objetos seleccionados y la lista de permisos asociada a cada objeto.



- En **Elementos protegibles**, clic en la tabla **Categories**.
- En **Permisos para Categories**, marque la casilla **Denegar** para las filas **Actualizar**, **Eliminar** e **Insertar**.



9. En **Elementos protegibles**, clic sobre la tabla **Products**.
10. En **Permisos para Products**, marque la casilla **Denegar** para las filas **Eliminar** e **Insertar**.
11. Clic en **Permisos de columna**.
12. En el diálogo **Permisos de columna**, marcar la casilla **Denegar** para todas las columnas excepto para la columna **UnitsInStock**.



Permisos de columna

Entidad de seguridad: SMATSUKAWA-LAP\VendedoresNw

Otorgante de permisos: dbo

Nombre de la tabla: dbo.Products

Nombre de permiso: Actualizar

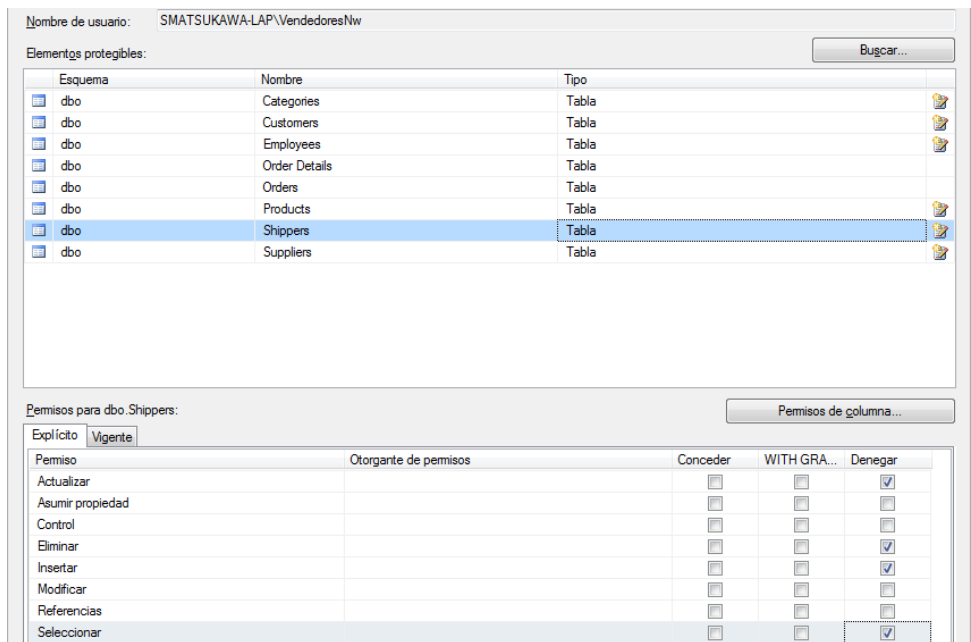
Permisos de columna:

Nombre de columna	Conceder	WITH GRA...	Denegar
ProductID	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ProductName	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
QuantityPerUnit	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ReorderLevel	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SupplierID	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
UnitPrice	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
UnitsInStock	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
UnitsOnOrder	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Aceptar Cancelar Ayuda

13. Clic en **Aceptar**.
14. En **Elementos protegibles**, clic sobre la tabla **Customers**.
15. En **Permisos para Customers**, marque la casilla **Denegar** para las filas **Actualizar** y **Eliminar**.
16. En **Elementos protegibles**, clic sobre **Employees**.
17. En **Permisos para Employees**, marque la casilla **Denegar** para las filas **Actualizar**, **Eliminar**, **Insertar** y **Seleccionar**.

18. Repita el **procedimiento seguido para Employees** sobre las tablas **Suppliers** y **Shippers**.



19. Clic en **Aceptar** para cerrar la ventana **Usuario de la base de datos**.
20. Para probar los permisos del usuario **VendedoresNw** regrese a su sesión Windows de la cuenta **RKing**.
21. En una ventana de consulta digite y ejecute las siguientes instrucciones:

```
SELECT * FROM Employees  
go
```

Se recibe el siguiente mensaje:

```
Mens. 229, Nivel 14, Estado 5, Línea 1  
Se denegó el permiso SELECT en el objeto  
'Employees', base de datos 'Northwind', esquema  
'dbo'.
```

```
UPDATE Products  
SET UnitPrice = 20  
WHERE ProductID = 1
```

go

Se genera el siguiente mensaje de error:

```
Mens. 230, Nivel 14, Estado 1, Línea 1
Se denegó el permiso UPDATE en la columna
'UnitPrice' del objeto 'Products', base de datos
'Northwind', esquema 'dbo'.
```

```
UPDATE Products
SET UnitsInStock = 50
WHERE ProductID = 1
go
```

La actualización se ejecuta sin problemas.

22. Cierre la ventana de consulta.

5. DEFINICIÓN DEL CONTROL DE ACCESO A UNA BASE DE DATOS CON TRANSACT-SQL

En este apartado veremos cómo definir el control de acceso a una base de datos usando sentencias SQL. Para poder ejecutar los ejemplos se ha creado en Windows una cuenta de usuario **JPerez**.

Ejercicio 15.11: Definición de control de acceso con Transact-SQL

5.1. Creación de un login name SQL Server a partir de una cuenta Windows

Sintaxis

```
CREATE LOGIN [hostWindows\cuentaWindows]
FROM Windows
```

Ejemplo

```
CREATE LOGIN [SMATSUKAWA-LAP\jperrez]
FROM Windows
```

5.2. Concesión de acceso a una base de datos para un login name SQL Server

Sintaxis

```
USE baseDatos  
CREATE USER nombreUsuario FOR LOGIN loginNameSQL
```

Ejemplo

```
USE Northwind  
go  
  
CREATE USER jperez  
    FOR LOGIN [smatsukawa-lap\jperez]  
go
```

5.3. Establecimiento de la base de datos predeterminada para un login name SQL Server

Sintaxis

```
ALTER LOGIN loginName  
    WITH DEFAULT_DATABASE baseDatos
```

Ejemplo

```
ALTER LOGIN [SMATSUKAWA-LAP\jperez]  
    WITH DEFAULT_DATABASE = Northwind
```

5.4. Asignación de un usuario de base de datos a un rol de base de datos

Sintaxis

```
sp_addrolemember nombreRolBD, nombreUsuarioBD
```

Ejemplo

```
sp_addrolemember db_datareader, jperez
```


5.5. Concesión de permisos sobre una tabla de una base de datos

Sintaxis

```
GRANT listaPermisosSentencia ON tabla TO usuario
```

Ejemplo

```
GRANT INSERT, UPDATE, DELETE ON Categories  
    TO jperez  
go
```

5.6. Denegación de permisos sobre una tabla de una base de datos

Sintaxis

```
DENY listaPermisosSentencia ON tabla TO usuario
```

Ejemplo

```
DENY SELECT ON Employees TO jperez  
go
```

6. ROLES DE SERVIDOR

Un rol de servidor agrupa privilegios administrativos que permiten ejecutar determinado tipo de operaciones a nivel del servidor. Para que un login name de SQL Server pueda ejecutar labores administrativas a nivel del servidor, debe pertenecer al rol de servidor adecuado.

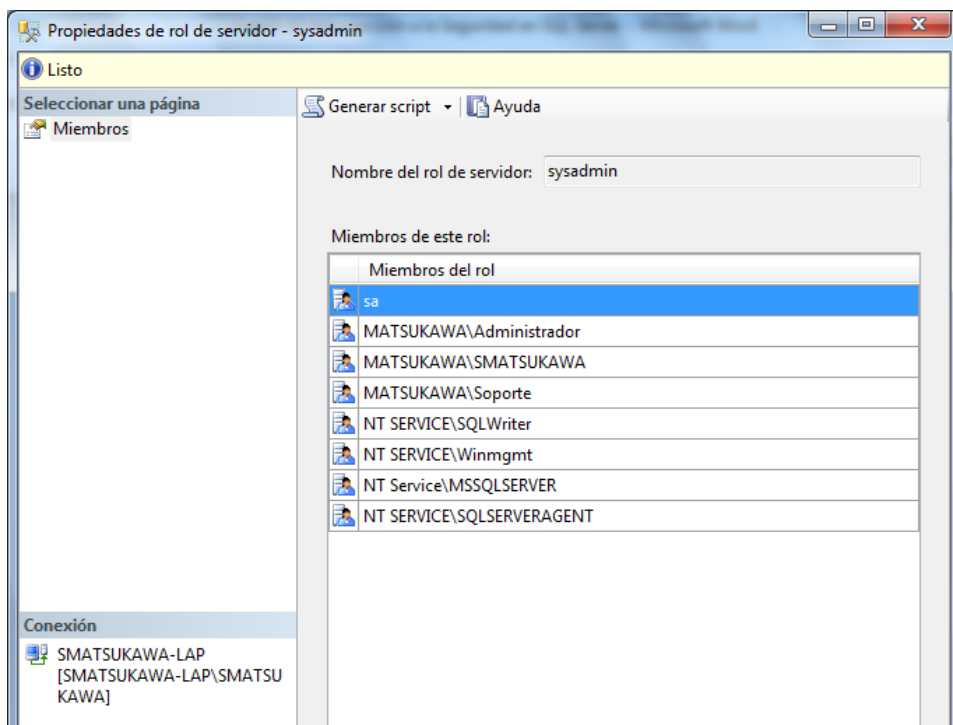
La siguiente tabla muestra los roles de servidor y sus funciones:

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.

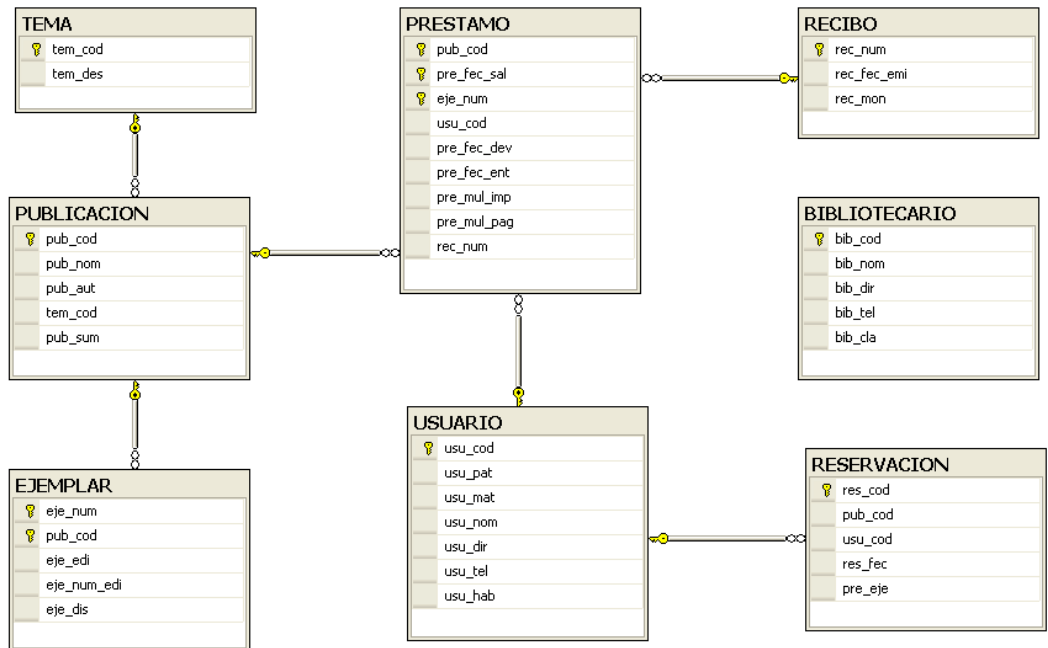
Ejercicio 15.12: Verificación de los miembros de un rol de servidor

1. En **SQL Server Management Studio**, en **Explorador de objetos**, expanda **Seguridad**, expanda **Roles de servidor**, doble clic en **sysadmin**.
2. La ventana **Propiedades de rol de servidor – sysadmin** muestra los login names SQL Server que son miembros de este rol, y por lo tanto son reconocidos como administradores de SQL Server.



7. EJERCICIO PROPUESTO

Se tiene la base de datos **BibliotecaGyS** que está formada por las siguientes tablas y relaciones (el script de creación de la base de datos lo puede ubicar en el CD que acompaña esta publicación):



Defina el diseño de la seguridad de la base de datos (con autenticación Windows) en base a las siguientes especificaciones (para aquello que no está explícitamente especificado, deberá usar su criterio):

1. Rosa Briones es la administradora de la biblioteca. Ella ejecuta las siguientes tareas:
 - Mantenimiento de los empleados (altas, bajas y actualizaciones).
 - Consultas de usuarios.
 - Consultas de publicaciones y temas.
 - Reporte de cuántos ejemplares se tiene por publicación.
2. Amanda Soria, Carlos Miranda, Juan Flores y Víctor Zavala son bibliotecarios. Sus tareas son:
 - Registrar a nuevos usuarios de la biblioteca.
 - Registrar los movimientos de los usuarios: préstamos, devoluciones, reservaciones.
 - Registrar las multas de los usuarios morosos.

3. Carlos Miranda y Víctor Zavala tienen las siguientes tareas adicionales:

- Mantenimiento de las publicaciones (altas, bajas y actualizaciones).

4. Todos los usuarios de la biblioteca pueden consultar el catálogo de la biblioteca. Usted deberá crear el catálogo.

Implemente su diseño de control de acceso a BibliotecaGyS usando Transact-SQL.