

Creación de Rol de Base de Datos en SQL Server

Descripción General

Este laboratorio guía a través del proceso de creación de un nuevo rol de base de datos (**role1**) en SQL Server que puede leer únicamente el contenido de la tabla **SalesLT.SalesOrderDetail** en la base de datos **db1** (AdventureWorksLT).

Entorno de Configuración

Requisitos Previos

- SQL Server Management Studio (SSMS) instalado
- Acceso a una instancia de SQL Server
- Visual Studio Code (opcional, para clonar archivos de laboratorio)

Configuración de Archivos de Laboratorio

Si su máquina virtual de laboratorio ya está configurada, debería encontrar los archivos de laboratorio en la carpeta **C:\LabFiles**. Compruébelo un momento; si los archivos ya están ahí, omita esta sección. Sin embargo, si usa su propia máquina o faltan los archivos de laboratorio, deberá clonarlos desde GitHub para continuar.

Pasos para Clonar el Repositorio

1. Desde la máquina virtual del laboratorio o su máquina local si no se proporcionó una, inicie una sesión de **Visual Studio Code**.
2. Abra la paleta de comandos (**Ctrl+Mayús+P**) y escriba **Git: Clone**. Seleccione la opción **Git: Clone**.
3. Pegue la siguiente URL en el campo URL del repositorio y seleccione **Entrar**:

```
https://github.com/MicrosoftLearning/dp-300-database-administrator.git
```

4. Guarde el repositorio en la carpeta **C:\LabFiles** en la máquina virtual del laboratorio o en su máquina local si no se proporcionó una (cree la carpeta si no existe).

Restaurar la Base de Datos

Si ya tiene la base de datos **AdventureWorksLT** restaurada, puede omitir esta sección.

Pasos para Restaurar

1. Desde la máquina virtual del laboratorio o su máquina local si no se proporcionó una, inicie una sesión de **SQL Server Management Studio (SSMS)**.

2. Al abrir SSMS, aparecerá de forma predeterminada el cuadro de diálogo **Conejar al servidor**. Elija la instancia predeterminada y seleccione **Conejar**. Es posible que deba marcar la casilla "Confiar en el certificado del servidor".

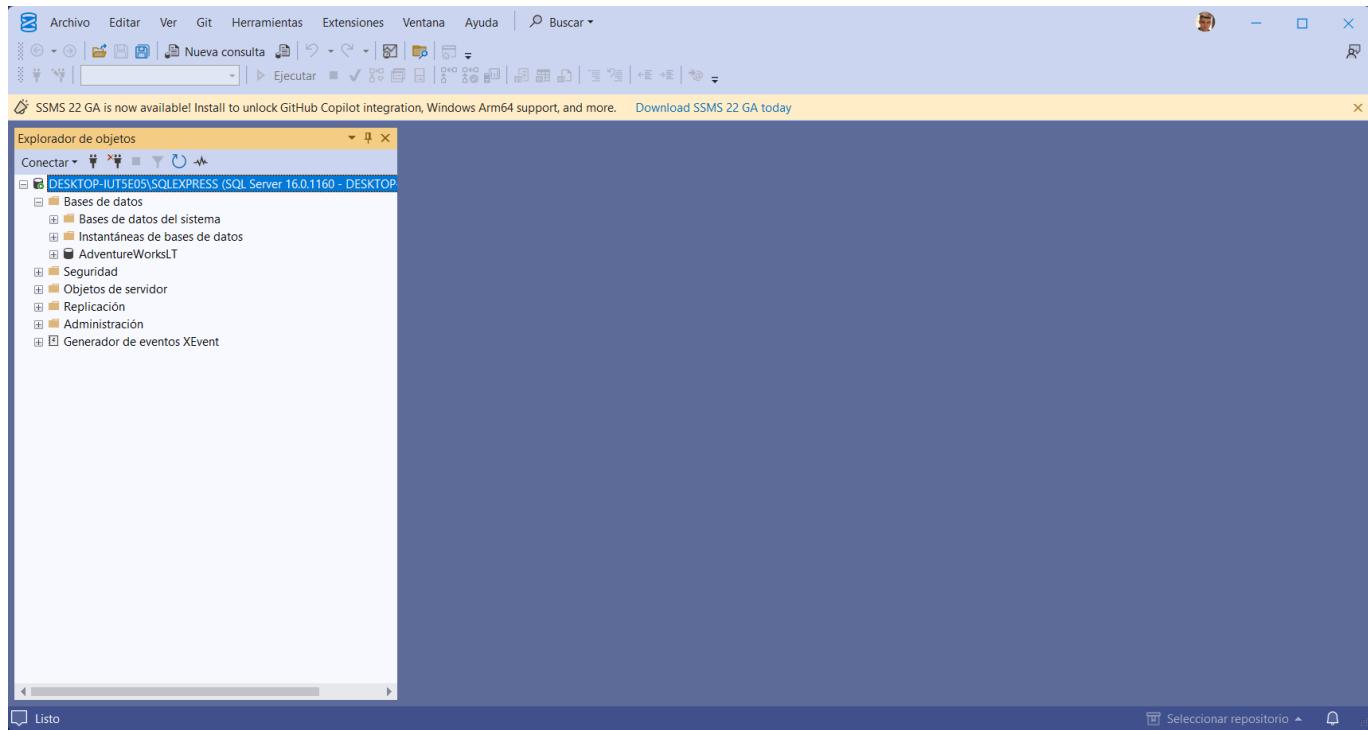
Nota: Si está utilizando su propia instancia de SQL Server, deberá conectarse a ella utilizando el nombre de instancia del servidor y las credenciales adecuadas.

3. Seleccione la carpeta **Bases de datos** y luego **Nueva consulta**.
4. Ejecute el script de restauración apropiado desde los archivos del laboratorio para restaurar la base de datos **AdventureWorksLT**.

Procedimiento de Creación del Rol

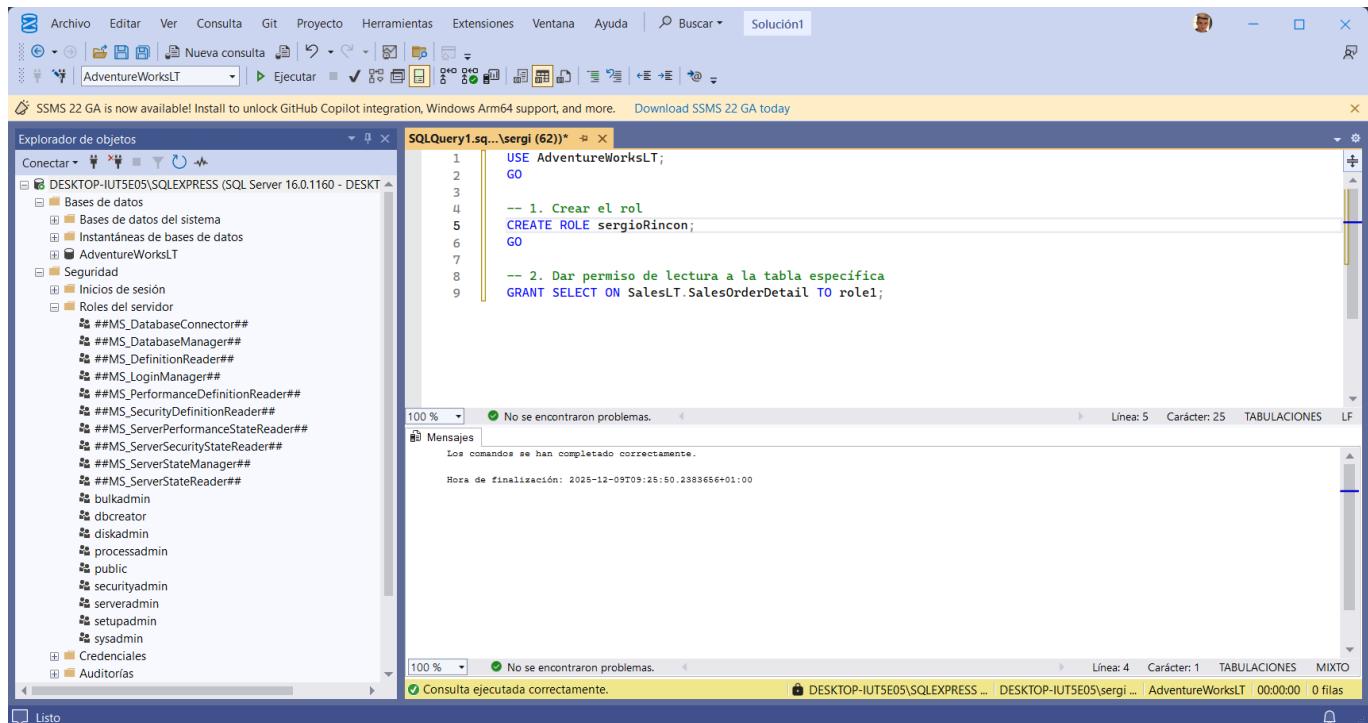
Objetivo

Crear un nuevo rol de servidor llamado **role1** que puede leer el contenido de la tabla **SalesLT.SalesOrderDetail** solo en **db1** (AdventureWorksLT).



Paso 1: Acceder a la Seguridad en Object Explorer

1. En **SQL Server Management Studio (SSMS)**, abra el **Explorador de objetos** (Object Explorer).
2. Expanda el servidor donde desea crear el nuevo rol.
3. Expanda la carpeta **Seguridad**.



Referencia: Imagen 2 - Vista inicial del Explorador de objetos con la carpeta Seguridad

Paso 2: Navegar a Roles del Servidor

1. Dentro de la carpeta **Seguridad**, localice y expanda **Roles del servidor** (Server Roles).
2. Haga clic derecho sobre **Roles del servidor** y seleccione **Nuevo rol de servidor** (New Server Role).

Paso 3: Crear el Rol en la Base de Datos

También puede crear el rol directamente usando T-SQL. Este es el método recomendado para este laboratorio:

1. Conéctese a la base de datos **AdventureWorksLT**.
2. Abra una **Nueva consulta**.
3. Ejecute el siguiente script SQL:

```

USE AdventureWorksLT;
GO

-- 1. Crear el rol
CREATE ROLE role1;
GO

-- 2. Dar permiso de lectura a la tabla específica
GRANT SELECT ON SalesLT.SalesOrderDetail TO role1;
  
```

```

USE AdventureWorksLT;
GO

-- 1. Crear el rol
CREATE ROLE sergioRincon;
GO

-- 2. Dar permiso de lectura a la tabla específica
GRANT SELECT ON SalesLT.SalesOrderDetail TO role1;
  
```

100 % No se encontraron problemas.

Mensajes Los comandos se han completado correctamente.

Hora de finalización: 2025-12-09T09:25:50.2383656+01:00

Línea: 5 Carácter: 25 TABULACIONES LF

Consulta ejecutada correctamente.

DESKTOP-IUT5E05\SQLEXPRESS ... DESKTOP-IUT5E05\sergi ... AdventureWorksLT 00:00:00 0 filas

Referencia: Imagen 2 - Vista inicial del Explorador de objetos con la carpeta Seguridad

Paso 4: Verificar la Creación del Rol

1. En el **Explorador de objetos**, navegue a:

- **Bases de datos → AdventureWorksLT → Seguridad → Roles → Roles de base de datos**

2. Verifique que **role1** aparezca en la lista de roles.

```

USE AdventureWorksLT;
GO

-- 1. Crear el rol
CREATE ROLE sergioRincon;
GO

-- 2. Dar permiso de lectura a la tabla específica
GRANT SELECT ON SalesLT.SalesOrderDetail TO role1;
  
```

100 % No se encontraron problemas.

Mensajes Los comandos se han completado correctamente.

Hora de finalización: 2025-12-09T09:25:50.2383656+01:00

Línea: 5 Carácter: 25 TABULACIONES LF

Consulta ejecutada correctamente.

DESKTOP-IUT5E05\SQLEXPRESS ... DESKTOP-IUT5E05\sergi ... AdventureWorksLT 00:00:00 0 filas

Referencia: Imagen 3 - Script SQL para crear el rol y otorgar permisos

Paso 5: Asignar el Rol a un Usuario

Una vez creado el rol **role1**, es necesario asignarlo a usuarios específicos para que puedan utilizar los permisos otorgados.

Opción A: Asignación mediante T-SQL

```
-- Asignar role1 al usuario sergioRincon
USE AdventureWorksLT;
GO

ALTER ROLE role1 ADD MEMBER [sergioRincon];
GO
```

Opción B: Asignación mediante la Interfaz Gráfica

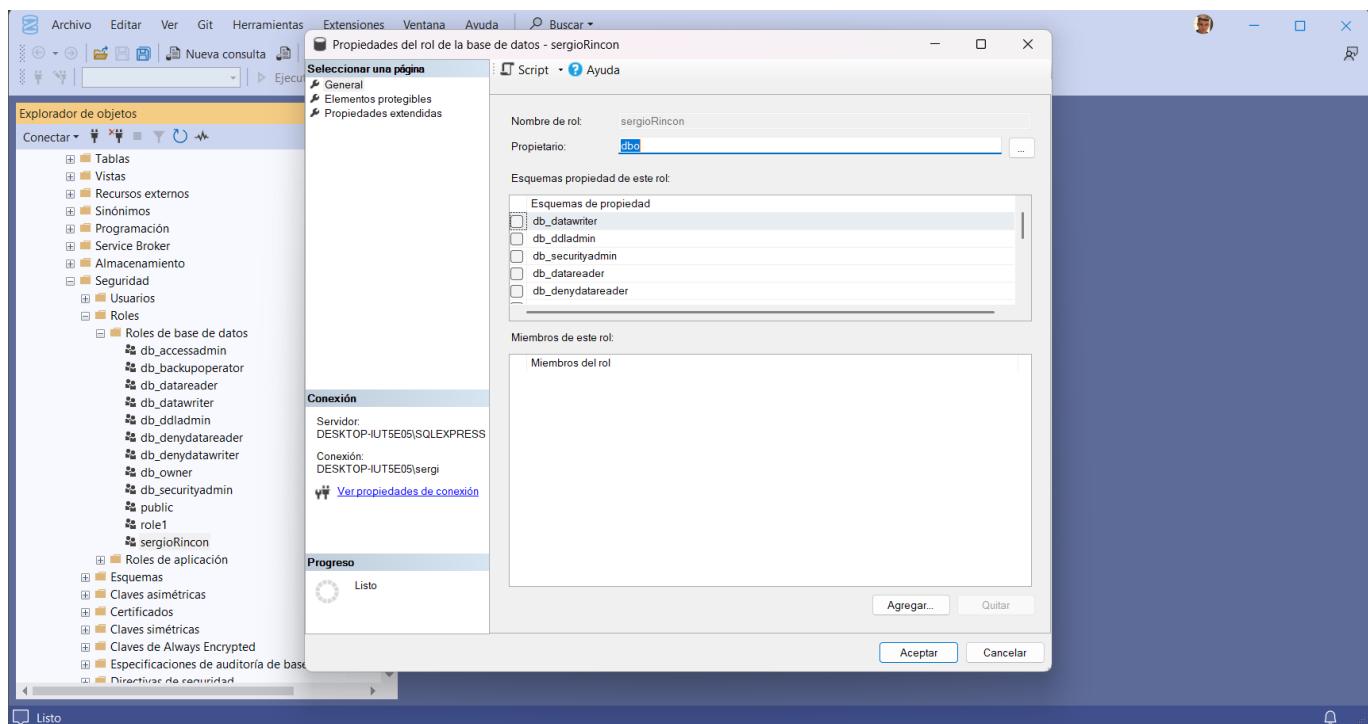
1. En el **Explorador de objetos**, navegue a:

- **Bases de datos → AdventureWorksLT → Seguridad → Roles → Roles de base de datos**

2. Haga clic derecho sobre **role1** y seleccione **Propiedades**.

3. En el cuadro de diálogo **Propiedades del rol de la base de datos - sergioRincon**:

- Seleccione la página **General** en el panel izquierdo
- En la sección **Miembros de este rol**, haga clic en el botón **Agregar...**



Referencia: Imagen 4 - Vista del Explorador de objetos mostrando **role1** en la lista de roles de base de datos

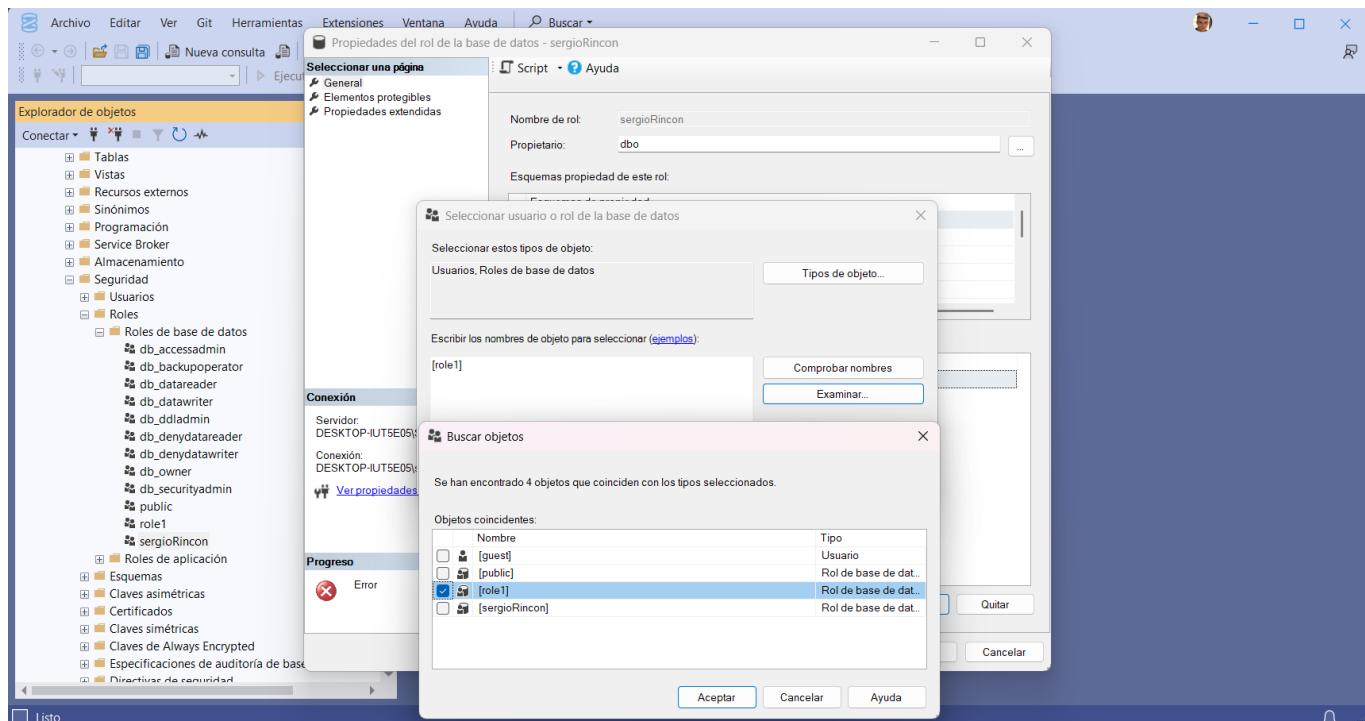
4. En el cuadro de diálogo **Seleccionar usuario o rol de la base de datos**:

- En el campo de texto, escriba **[role1]** (o el nombre del usuario que desea agregar)
- Haga clic en **Comprobar nombres** para validar
- Haga clic en **Examinar...** para buscar usuarios disponibles

5. En el cuadro de diálogo **Buscar objetos**:

- Marque la casilla junto a [role1] en la lista de objetos coincidentes
- Haga clic en **Aceptar**

6. De vuelta en la ventana de propiedades, verifique que el usuario aparece en la lista de **Miembros del rol**.

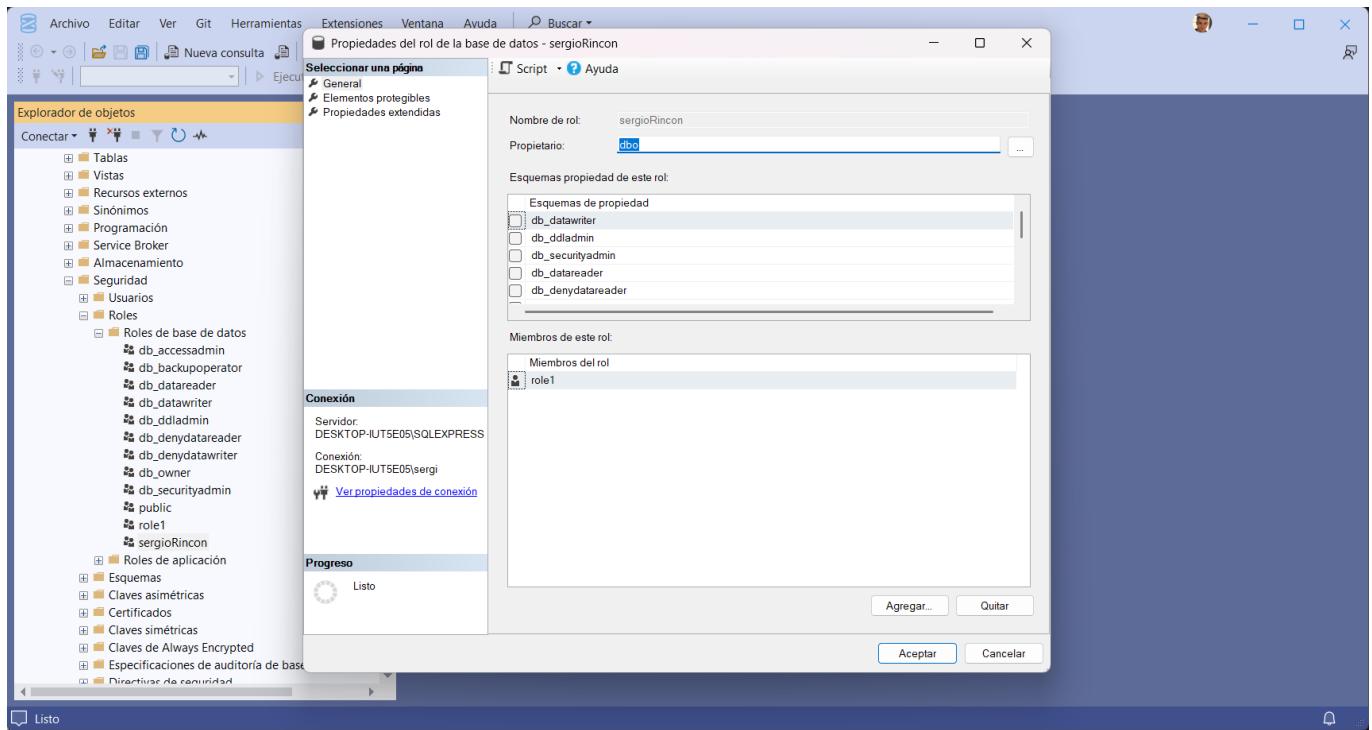


Referencia: Imagen 5 - Ventana de propiedades del rol con sección de miembros

7. Haga clic en **Aceptar** para aplicar los cambios.

8. Verifique que el usuario aparece en la lista de **Miembros del rol**.

- click derecho en el rol y seleccionar **Propiedades**
- en la sección **Miembros de este rol**, verifique que el usuario aparece en la lista de **Miembros del rol**.



Solución Correcta

Según la documentación oficial de Microsoft (imagen 1), estos son los pasos completos para crear un rol usando la interfaz gráfica:

Usando SQL Server Management Studio

Step 1: En Object Explorer, expanda el servidor donde desea crear el nuevo rol de servidor.

Step 2: Expanda la carpeta **Security** (Seguridad).

Step 3: Haga clic derecho en la carpeta **Server Roles** y seleccione **New Server Role...** (Nuevo rol de servidor).

Step 4: En el cuadro de diálogo **New Server Role** → **server_role_name**, en la página **General**, ingrese un nombre para el nuevo rol de servidor en el cuadro **Server role name** [Ingrese **role1**].

Step 5: En el cuadro **Owner**, ingrese el nombre del principal del servidor que será propietario del nuevo rol. Alternativamente, haga clic en los puntos suspensivos (...) para abrir el cuadro de diálogo **Select Server Login or Role**.

Step 6: En **Securables**, seleccione uno o más elementos asegurables de nivel de servidor [Seleccione la tabla **SalesLT.SalesOrderDetail**]. Cuando se selecciona un elemento asegurable, a este rol de servidor se le pueden otorgar o denegar permisos sobre ese elemento asegurable.

Step 7: En el cuadro **Permissions: Explicit**, marque la casilla para otorgar, otorgar con grant o denegar permiso a este rol de servidor para los elementos asegurables seleccionados [Seleccione **Read**]. Si un permiso no se puede otorgar o denegar a todos los elementos asegurables seleccionados, el permiso se representa como una selección parcial.

Step 8: En la página **Members**, use el botón **Add** para agregar inicios de sesión que representen individuos o grupos al nuevo rol de servidor. [Omitir este paso en este laboratorio]

Step 9: Un rol de servidor definido por el usuario puede ser miembro de otro rol de servidor. En la página **Memberships**, seleccione una casilla para hacer que el rol de servidor definido por el usuario actual sea miembro de un rol de servidor seleccionado. [Omitir este paso]

Step 10: Seleccione **OK**.

Referencia Oficial

Para más información, consulte la documentación oficial de Microsoft: <https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/create-a-server-role>

Referencias de Imágenes

1. **Imagen 1:** Instrucciones detalladas del ejercicio de simulación
2. **Imagen 2:** Vista inicial del Explorador de objetos en SSMS
3. **Imagen 3:** Script SQL ejecutado correctamente con mensajes de confirmación
4. **Imagen 4:** Explorador de objetos mostrando **role1** creado en la lista de roles de base de datos
5. **Imagen 5:** Ventana de propiedades del rol mostrando la configuración de propietario y esquemas
6. **Imagen 6:** Cuadro de diálogo de búsqueda de objetos con **role1** seleccionado para asignación

Notas Adicionales

- Este rol (**role1**) tiene **únicamente** permisos de **lectura (SELECT)** sobre la tabla **SalesLT.SalesOrderDetail**.
- El rol no tiene permisos sobre otras tablas de la base de datos.
- En este ejemplo, se ha asignado el rol **role1** al usuario **sergioRincon**, quien ahora puede leer datos de la tabla especificada.
- Para asignar el rol a otros usuarios, repita el proceso de asignación o use el comando T-SQL:

```
ALTER ROLE role1 ADD MEMBER [nombre_usuario];
```

- Para verificar qué usuarios son miembros de un rol:

```
SELECT DP1.name AS RoleMember
FROM sys.database_role_members AS DRM
RIGHT OUTER JOIN sys.database_principals AS DP1
    ON DRM.member_principal_id = DP1.principal_id
LEFT OUTER JOIN sys.database_principals AS DP2
    ON DRM.role_principal_id = DP2.principal_id
WHERE DP2.name = 'role1';
```

Resolución de Problemas

Error: "No se puede crear el rol"

- Verifique que tiene permisos de administrador en la base de datos.
- Asegúrese de estar conectado a la base de datos correcta (**AdventureWorksLT**).

El rol no aparece en el Explorador de objetos

- Haga clic derecho en **Roles de base de datos** y seleccione **Actualizar**.
- Verifique que está viendo la base de datos correcta.

No puedo agregar usuarios al rol

- Asegúrese de que el usuario existe en la base de datos.
- Verifique que tiene permisos suficientes para modificar roles.
- El usuario debe tener un login asociado en la instancia de SQL Server.

Error al buscar el usuario en la interfaz gráfica

- Use el botón **Comprobar nombres** para validar que el nombre del usuario es correcto.
- Si el nombre no se reconoce automáticamente, use el botón **Examinar...** para buscar en la lista de usuarios disponibles.

Conclusión

Ha completado exitosamente la creación de un rol de base de datos en SQL Server con permisos específicos de lectura sobre una tabla determinada, y ha asignado ese rol al usuario **sergioRincon**. Este es un concepto fundamental para la gestión de seguridad y control de acceso en bases de datos SQL Server.

Resumen de lo aprendido:

- Crear roles de base de datos personalizados
- Asignar permisos específicos de lectura a tablas individuales
- Agregar usuarios como miembros de roles
- Verificar la configuración mediante la interfaz gráfica y T-SQL

Con esta configuración, el usuario **sergioRincon** puede ahora consultar la tabla **SalesLT.SalesOrderDetail** sin tener acceso a otras tablas de la base de datos, implementando así el principio de privilegio mínimo en la seguridad de la base de datos.