Capítulo 4
Gestión de la seguridad del acceso

1. Introducción

El control de acceso representa una operación importante en la gestión de la seguridad sobre un servidor de bases de datos. La seguridad de los datos requiere una organización de los objetos de manera independiente de los usuarios, y esto es posible gracias a los esquemas. La seguridad pasa también por un mejor control de las autorizaciones y la posibilidad de asignar los privilegios necesarios a cada usuario para que puedan trabajar de manera autónoma.

Para la organización de esta política de seguridad, es necesario tener en cuenta la organización jerárquica de los elementos de seguridad, de manera que la gestión de los derechos de acceso sea simple y eficaz.

SQL Server se apoya sobre tres elementos claves, que son:

– Las entidades de seguridad.

– Los objetos asegurables.

– Las autorizaciones.

Las entidades de seguridad son las cuentas de seguridad que disponen de un acceso al servidor SQL.

Los objetos asegurables representan los objetos gestionados por el servidor. Aquí, un objeto puede ser una tabla, un esquema o una base de datos, por ejemplo.

Las autorizaciones se conceden a las entidades de seguridad para que puedan trabajar con los objetos asegurables.

La organización jerárquica permite asignar una autorización (por ejemplo, SELECT) a un objeto asegurable de nivel elevado (por ejemplo, el esquema) para permitir a la entidad de seguridad que recibe la autorización ejecutar la instrucción SELECT sobre todas las tablas contenidas en el esquema.

Las vistas del catálogo de sistema permiten obtener un informe completo y detallado sobre las conexiones existentes, los usuarios de base de datos definidos y los privilegios asignados. Algunas de estas vistas se presentan a continuación:

- sys.server_permissions: lista de permisos de nivel servidor y sus beneficiarios.
- sys.sql_logins: lista de las conexiones.
- sys.server_principals: entidad de seguridad definida en el servidor.
- sys.server_role_members: lista de los beneficiarios de un rol de servidor.
- sys.database_permissions: lista de permisos y sus beneficiarios en la base de datos.
- sys.database_principals: entidad de seguridad a nivel de la base de datos.
- sys.database_role_members: lista de los beneficiarios de un rol de base de datos.

Para simplificar la gestión de los derechos de acceso, es posible utilizar tres tipos de roles. Los **roles de servidor** agrupan las autorizaciones a nivel del servidor. Estas autorizaciones son válidas para todas las bases de datos instaladas. Los **roles de base de datos** agrupan los derechos a nivel de la base de datos sobre la que se definen. Por último, los **roles de aplicaciones**, definidos sobre las bases de datos de usuario, permiten agrupar los derechos necesarios para la correcta ejecución de una aplicación cliente.

2. Gestión de los accesos al servidor

Antes de poder trabajar con los datos gestionados por las bases de datos, es necesario en primer lugar conectarse al servidor SQL. Esta etapa permite hacerse identificar por el servidor SQL y utilizar posteriormente todos los derechos que se asignan a la conexión. En SQL existen dos modos de gestión de los accesos al servidor de base de datos.

Atención: en esta sección únicamente se aborda la parte de conexión al servidor. Es importante distinguir bien la conexión al servidor de la utilización de bases de datos. La conexión al servidor permite hacerse identificar por el servidor SQL como un usuario válido para utilizar, posteriormente, una base de datos: los datos y los objetos. El conjunto de estos derechos se definirá más adelante. Estos derechos se asocian a un usuario de base de datos al que corresponde una conexión.

Observación

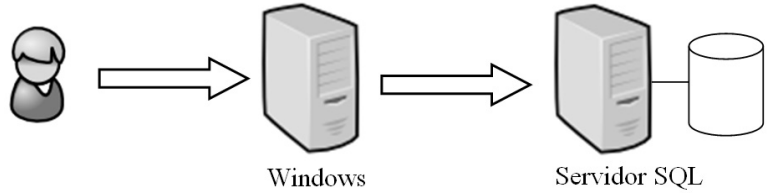
Hablaremos de conexión al servidor o de login.

2.1 Modo de seguridad de Windows

Este tipo de gestión de seguridad permite apoyarse sobre los usuarios y los grupos de Windows para el dominio y el puesto local. SQL Server utiliza la gestión de los usuarios de Windows (gestión de las contraseñas...) y recupera únicamente los nombres para crear conexiones al servidor.

Una funcionalidad muy importante de SQL Server es poder autorizar a los grupos de Windows a conectarse. La gestión de grupos simplifica enormemente la gestión del acceso a los recursos. Por lo tanto, se pueden utilizar los mismos grupos de Windows para dar acceso a archivos o a objetos de base de datos de SQL Server.

Con este método de funcionamiento, como un usuario de Windows puede pertenecer a varios grupos, puede tener varios derechos de conexión a SQL Server.



Autenticación de Windows

En modo de seguridad de Windows, solo se almacenan los nombres de usuario. La gestión de las contraseñas y la pertenencia a diferentes grupos se deja a Windows. Este modo de funcionamiento permite separar las tareas que son responsabilidad de cada uno y especializar a SQL Server en la gestión de los datos, dejando a Windows la gestión de la autenticación de los usuarios, que sabe hacerla bien. Además, con este esquema de funcionamiento, es posible aplicar la política siguiente: un usuario = una contraseña. El acceso al servidor SQL es transparente para los usuarios aprobados por Windows.

Observación

SQL Server se apoya sobre los grupos a los que pertenece el usuario en el momento de la conexión al servidor. Si se efectúan modificaciones de pertenencia a los grupos desde Windows, estas modificaciones no se tomarán en cuenta hasta la próxima conexión del usuario al servidor SQL.

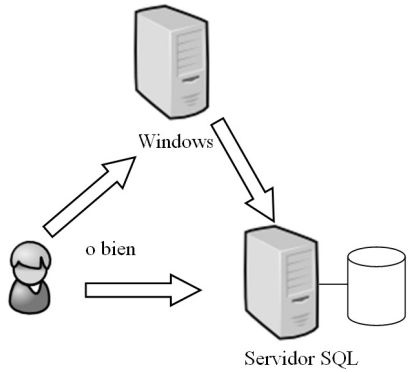
Observación

SQL Server se basa en el SID de Windows para identificar el grupo. Si un grupo se elimina y posteriormente se vuelve a crear en Windows, es importante realizar la misma operación en lo que se refiere a la conexión del grupo en SQL Server.

2.2 Modo de seguridad mixta

El modo de seguridad mixta se basa en una autenticación de Windows y posteriormente en una autenticación de SQL Server. Este modo de autenticación es el que se va a detallar aquí.

En este modo de funcionamiento, es SQL Server quien se encarga de verificar que el usuario que solicita conectarse está bien definido y posteriormente se encarga también de verificar la contraseña.

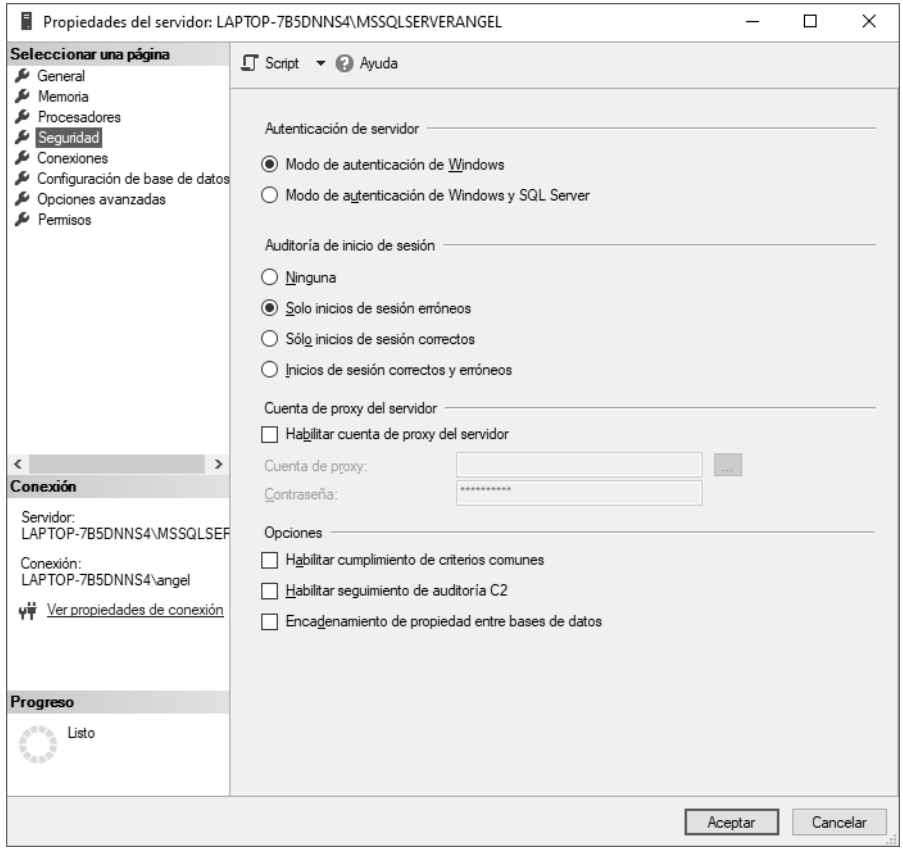


Modo de seguridad mixta

Todos los usuarios son completamente gestionados por SQL Server (nombre y contraseña). Este tipo de gestión de las conexiones se adapta bien a los clientes que no se pueden identificar.

2.3 ¿Cómo elegir un modo de seguridad?

Es posible modificar el modo de seguridad utilizado por el servidor SQL directamente desde SQL Server Management Studio modificando las propiedades de la instancia, como se muestra a continuación.



En el momento de instalar el servidor SQL, se crean conexiones de administrador SQL (**sysadmins**). En modo Windows, en la que se puede autorizar al grupo local de los Administradores a conectarse, y otra en modo de seguridad SQL Server, en la que el usuario ya está creado, solo se configura una contraseña.

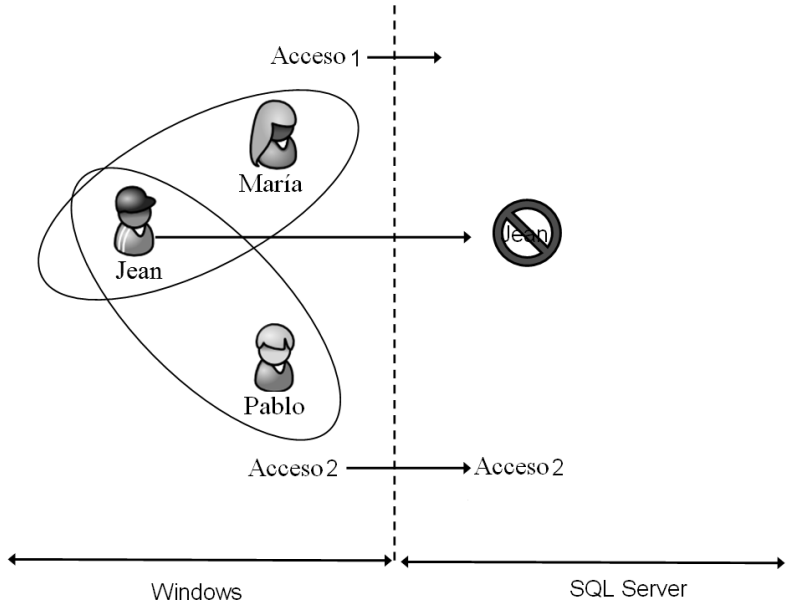
Observación

Se recomienda utilizar la seguridad de Windows, que ofrece una mayor flexibilidad para la gestión de los usuarios.

Los cambios de modo entre el modo mixto y el modo Windows, no se tienen en cuenta hasta que se reinicia el servicio SQL Server.

2.4 Administrar una conexión en SQL Server

Teniendo en cuenta que un usuario de Windows puede pertenecer a varios grupos, se le puede asignar varias veces el permiso de conexión al servidor SQL. Esto puede presentar un problema cuando un usuario o un grupo de usuarios no deben tener nunca la capacidad de conectarse al servidor SQL. Para remediar esta situación, Microsoft proporciona, dentro del conjunto de órdenes Transact SQL para la gestión de las conexiones, la orden DENY, que permite denegar explícitamente la conexión a un usuario o un grupo de Windows. DENY constituye un rechazo explícito y es prioritario frente a los permisos de conexión.



Creación de una conexión

En el esquema anterior, hay tres usuarios de Windows y dos grupos. Se ha establecido una conexión SQL para el grupo Acceso 2, el grupo Acceso 1 no tiene conexión, pero para que el usuario Jean tenga prohibido el acceso SQL Server, se ha creado una conexión en SQL Server con la propiedad DENY.

Observación

*Es necesario tener un permiso de administrador (**sysadm**) o un permiso de gestor de seguridad (**securityadmin**) para poder realizar las diferentes operaciones relativas a la gestión de las conexiones.*

Las conexiones que sean de tipo SQL Server o bien Windows se deben definir en la instancia de SQL Server para permitir a los usuarios la conexión. Se almacenan en la base de datos de sistema **Master**.

La gestión de las conexiones se puede realizar de manera gráfica con el explorador de objetos desde SQL Server Management Studio o con scripts Transact SQL. Todas las operaciones de gestión de las conexiones se realizan en Transact SQL con las instrucciones CREATE LOGIN, ALTER LOGIN y DROP LOGIN. Cada solución tiene sus ventajas y sus inconvenientes.

Observación

Los procedimientos sp_addlogin y sp_grantlogin no se deben utilizar más. Todavía están presentes en SQL Server para asegurar la compatibilidad de los scripts.

2.4.1 En modo de seguridad de Windows

Los nombres de los grupos o de los usuarios deben corresponder a los que se definen en Windows.

SQL Server Management Studio

Es posible crear conexiones desde la interfaz gráfica de SQL Server Management Studio, procediendo de la siguiente manera:

– Desde el explorador de objetos, situarse sobre el nodo **Seguridad - Inicios de sesión**.

– Desde el menú contextual asociado al nodo conexión, seleccionar **Nuevo inicio de sesión**.