



Universidad Nacional del Litoral

Facultad de Ingeniería y Ciencias Hídricas

Departamento de Informática

Bases de Datos

Unidad Temática VI

Aspectos internos del RDBMS

Seguridad SQL Server

A continuación vamos a estudiar aspectos de Seguridad de SQL Server que, si bien son más bien tarea del Administrador de Base de Datos- necesitamos conocer a fin de poder llevar a cabo nuestras tareas de Desarrollo SQL.



Conceptos básicos de seguridad de la Base de Datos

SQL Server administra su seguridad a través de lo que se denomina **SQL Server security framework**.

- Lo primero que tenemos que comprender es que SQL Server administra una colección jerárquica de entidades.
- En la raíz del árbol de estas entidades está la **instancia de SQL Server** y las bases de datos en la instancia. Debajo del database level están el resto de los objetos.

Cada entidad debajo del nivel de instancia "es propiedad de" (owned) por individuos o grupos de individuos.

La SQL Server security framework controla el acceso a las entidades dentro de la instancia SQL Server.

De manera similar a cualquier resource manager, la SQL Server security framework posee dos partes: **autenticación** y **autorización**.

Autenticación

Llamamos autenticación al proceso por el cual un usuario presenta sus "credenciales" ante una instancia de SQL server a fin de solicitar acceso. SQL Server establece la identidad del usuario y decide si le otorga acceso o no.

Autorización

Llamamos autorización al proceso por el cual SQL Server decide si a una identidad dada le es permitido acceder a un recurso.

SQL Server define dos conceptos asociados a la Autenticación y Autorización:

Securable

Es una entidad o recurso sobre la cual SQL Server regula el acceso y sobre el cual pueden ser otorgados permisos.
Las bases de datos, los schemas y los objetos son **securables**.

Server Principal

Es una entidad que puede acceder a Securables.

Server Primary Principal

Es un Principal que representa a un único usuario.
Un SQL Server Login Id (que veremos a continuación) o un Windows login son Primary principals.

Server Secondary Principal

Es un Principal que representa varios usuarios.
Un role o Windows group son Secondary principals.



Métodos de Autenticación

Modos de Autenticación

Como dijimos, cualquier usuario que desee acceder a un recurso de SQL Server debe primero ser autenticado a Server level.

SQL Server proporciona dos **métodos** básicos de autenticación de Logins:

Windows Authentication

Bajo este método, la seguridad de la autenticación en SQL Server está integrada directamente a la seguridad de Windows, permitiendo que el sistema operativo autentique a los usuarios SQL Server.

SQL Server en este caso no valida el acceso del usuario, sino que "confía" en el otorgamiento de acceso llevado a cabo por Windows.

SQL Server Authentication

Bajo este método, un administrador crea **cada** SQL Server login account (llamada **Login ID**) dentro de la instancia de SQL Server, definiendo una password para el mismo, y cualquier usuario que desee conectarse a la instancia debe proporcionar un SQL Server login name (Login ID) y password válidos.

El método (o métodos) usados por SQL Server determinan su **Modo de Seguridad**. SQL Server puede ejecutarse en uno de dos modos de seguridad:

Windows Authentication Mode Seguridad "integrada"

Es el Modo de Autenticación que usa el método Windows Authentication. Históricamente a este modo se le llamó "Seguridad integrada".

Cuando conectamos a una instancia de SQL Server configurada con este modo de autenticación, no podemos proporcionar un SQL Server login name y nuestro Windows user name es el que determina nuestro nivel de acceso a SQL Server.

Mixed Mode

Este Modo de Autenticación permite usar cualquiera de los dos métodos: **Windows Authentication** o **SQL Server Authentication**, a elección del cliente. A este método también se le llama "SQL Server and Windows Authentication".



Configuración del Tipo de Seguridad durante la instalación

Recordemos cuando aprendimos a instalar SQL Server:

SQL Server



Instrucciones para trabajar con el motor de base de datos SQL Server

...en la ventana *Database Engine Configuration* elegíamos el Modo de Seguridad que deseábamos usar:

SQL Server 2008 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Setup Support Rules
Feature Selection
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Error and Usage Reporting
Installation Rules
Ready to Install
Installation Progress
Complete

Account Provisioning | Data Directories | FILESTREAM

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

☐ Windows authentication mode

☒ Mixed Mode (SQL Server authentication and Windows authentication)

Built-in SQL Server system administrator account

Enter password: [password field]

Confirm password: [password field]

Specify SQL Server administrators

SQL Server administrators have unrestricted access to the Database Engine.

Add Current User Add... Remove

< Back Next > Cancel Help



Especificar el modo de seguridad cuando nos conectamos a SQL Server

Recordemos también cuando aprendimos a conectarnos a SQL Server usando el *Microsoft SQL Server Management Studio*:

SQL Server



Instrucciones para trabajar con el motor de base de datos SQL Server

...en la ventana *Connect to Server* teníamos lo siguiente:

Durante la instalación habíamos elegido el modo de autenticación **Mixed Mode**, que permitía usar tanto **SQL Server authentication** como **Windows authentication**. Por eso en la lista Authentication (**A**) tenemos la posibilidad de elegir entre **SQL Server Authentication** y **Windows Authentication**.

En la lista Login (**B**) seleccionábamos *sa*. (el usuario administrador en SQL Server) y en la caja Password (**C**) escribíamos la password que habíamos definido durante la instalación.