SEGURIDAD SQL SERVER

Roles de nivel de servidor

SQL Server proporciona roles de nivel de servidor para ayudarle a administrar los permisos de un servidor. Estos roles son entidades de seguridad que agrupan otras entidades de seguridad. Los roles de nivel de servidor se aplican a todo el servidor en lo que respecta a su ámbito de permisos. (Los roles son como los grupos del sistema operativo Windows.)

Los roles fijos de servidor se proporcionan por comodidad y compatibilidad con versiones anteriores. Siempre que sea posible, asigne permisos más específicos.

SQL Server proporciona nueve roles fijos de servidor. Los permisos que se conceden a los roles fijos de servidor no se pueden modificar. A partir de SQL Server 2012, puede crear roles de servidor definidos por el usuario y agregarles permisos de nivel de servidor.

Puede agregar entidades de seguridad a nivel de servidor (inicios de sesión de SQL Server, cuentas de Windows y grupos de Windows) a los roles de nivel de servidor. Cada miembro de un rol fijo de servidor puede agregar otros inicios de sesión a ese mismo rol. Los miembros de roles de servidor definidos por el usuario no pueden agregar otras entidades de seguridad de servidor al rol.

Roles fijos de nivel de servidor

En la tabla siguiente se muestran los roles fijos de nivel de servidor y sus capacidades.

Rol fijo de nivel de servidor	Descripción
sysadmin	Los miembros del rol fijo de servidor sysadmin pueden realizar cualquier actividad en el servidor.
serveradmin	Los miembros del rol fijo de servidor serveradmin pueden cambiar las opciones de configuración del servidor y apagarlo.
securityadmin	Los miembros del rol fijo de servidor securityadmin administran los inicios de sesión y sus propiedades. Administran los permisos de servidor GRANT, DENY y REVOKE. También pueden administrar los permisos de nivel de base de datos GRANT, DENY y REVOKE si tienen acceso a una base de datos. Asimismo, pueden restablecer las contraseñas para los inicios de sesión de SQL Server. Nota de seguridad La capacidad de conceder acceso a Motor de base de datos y configurar los permisos de usuario permite que el administrador de

	seguridad asigne la mayoría de los permisos de servidor. El rol securityadmin se debe tratar como equivalente al rol sysadmin.
processadmin	Los miembros del rol fijo de servidor processadmin pueden finalizar los procesos que se ejecuten en una instancia de SQL Server.
setupadmin	Los miembros del rol fijo de servidor setupadmin pueden agregar y quitar servidores vinculados mediante instrucciones de Transact-SQL. (Es necesaria la pertenencia a sysadmin cuando se utiliza Management Studio).
bulkadmin	Los miembros del rol fijo de servidor bulkadmin pueden ejecutar la instrucción BULK INSERT.
diskadmin	El rol fijo de servidor diskadmin se usa para administrar archivos de disco.
dbcreator	Los miembros del rol fijo de servidor dbcreator pueden crear, modificar, quitar y restaurar cualquier base de datos.
public	Cada inicio de sesión de SQL Server pertenece al rol de servidor public. Cuando a una entidad de seguridad de servidor no se le han concedido ni denegado permisos específicos para un objeto protegible, el usuario hereda los permisos concedidos al rol public para ese objeto. Solo asigne permisos públicos en cualquier objeto cuando desee que el objeto esté disponible para todos los usuarios. No puede cambiar la pertenencia en public. Nota public se implementa de manera diferente que otros roles. Sin embargo, se pueden conceder, denegar o revocar permisos desde public.

Trabajar con roles de nivel de servidor

En la tabla siguiente se explican los comandos, las vistas y las funciones que se pueden utilizar para trabajar con roles de nivel de servidor.

Característica	Tipo	Descripción
sp_helpsrvrole (Transact-SQL)	Metadatos	Devuelve una lista de roles de nivel de servidor.
sp_helpsrvrolemember (Transact-SQL)	Metadatos	Devuelve información acerca de los miembros de un rol de nivel de servidor.
sp_srvrolepermission (Transact-SQL)	Metadatos	Muestra los permisos de un rol de nivel de servidor.
IS_SRVROLEMEMBER (Transact-SQL)	Metadatos	Indica si un inicio de sesión de SQL Server es miembro del rol de nivel de servidor especificado.
sys.server_role_members (Transact-SQL)	Metadatos	Devuelve una fila por cada miembro de cada rol de nivel de servidor.
sp_addsrvrolemember (Transact-SQL)	Comando	Agrega un inicio de sesión como miembro de un rol de nivel de servidor. Desusado. Utilice ALTER SERVER ROLE en su lugar.
sp_dropsrvrolemember (Transact-SQL)	Comando	Quita un inicio de sesión de SQL Server o un usuario o grupo de Windows de un rol de nivel de servidor. Desusado. Utilice ALTER SERVER ROLE en su lugar.
CREATE SERVER ROLE (Transact-SQL)	Comando	Crea un rol de servidor definido por el usuario.
ALTER SERVER ROLE (Transact-SQL)	Comando	Cambia la pertenencia de un rol de servidor o cambia el nombre de un rol de servidor definido por el usuario.
DROP SERVER ROLE (Transact-SQL)	Comando	Quita un rol de servidor definido por el usuario.
IS_SRVROLEMEMBER (Transact-SQL)	Función	Determina la pertenencia del rol de servidor.

Roles fijos de base de datos

Para administrar con facilidad los permisos en las bases de datos, SQL Server proporciona varios roles, que son las entidades de seguridad que agrupan a otras entidades de seguridad. Son como los ***grupos*** del sistema operativo Microsoft Windows. Los roles de nivel de base de datos se aplican a toda la base de datos en lo que respecta a su ámbito de permisos.

Existen dos tipos de roles de nivel de base de datos en SQL Server: los roles fijos de base de datos, que están predefinidos en la base de datos, y los roles flexibles de base de datos, que pueden crearse.

Los roles fijos de base de datos se definen en el nivel de base de datos y existen en cada una de ellas. Los miembros de los roles de base de datos **db_owner** y **db_securityadmin** pueden administrar la pertenencia a roles fijos de base de datos. Sin embargo, solo los miembros del rol de base de datos **db_owner** pueden agregar miembros al rol fijo de base de datos **db_owner**. También hay algunos roles fijos de base de datos con fines especiales en la base de datos msdb.

Puede agregar cualquier cuenta de la base de datos y otros roles de SQL Server a los roles de nivel de base de datos. Cada miembro de un rol fijo de base de datos puede agregar otros inicios de sesión a ese mismo rol.

En la tabla siguiente se muestran los roles fijos de nivel de base de datos y sus capacidades. Estos roles existen en todas las bases de datos.

Nombre de rol de nivel de base de datos	Descripción
db_owner	Los miembros del rol fijo de base de datos db_owner pueden realizar todas las actividades de configuración y mantenimiento en la base de datos y también pueden eliminar la base de datos.
db_securityadmin	Los miembros del rol fijo de base de datos db_securityadmin pueden modificar la pertenencia a roles y administrar permisos. Si se agregan entidades de seguridad a este rol, podría habilitarse un aumento de privilegios no deseado.
db_accessadmin	Los miembros del rol fijo de base de datos db_accessadmin pueden agregar o quitar el acceso a la base de datos para inicios de sesión de Windows, grupos de Windows e inicios de sesión de SQL Server.
db_backupoperator	Los miembros del rol fijo de base de datos db_backupoperator pueden crear copias de seguridad de la base de datos.
db_ddladmin	Los miembros del rol fijo de base de datos db_ddladmin pueden ejecutar cualquier comando del lenguaje de definición de datos (DDL) en una base de datos.

db_datawriter	Los miembros del rol fijo de base de datos db_datawriter pueden agregar, eliminar o cambiar datos en todas las tablas de usuario.
db_datareader	Los miembros del rol fijo de base de datos db_datareader pueden leer todos los datos de todas las tablas de usuario.
db_denydatawriter	Los miembros del rol fijo de base de datos db_denydatawriter no pueden agregar, modificar ni eliminar datos de tablas de usuario de una base de datos.
db_denydatareader	Los miembros del rol fijo de base de datos db_denydatareader no pueden leer datos de las tablas de usuario dentro de una base de datos.

Trabajar con roles de nivel de base de datos

En la tabla siguiente se explican los comandos, las vistas y las funciones que se usan para trabajar con los roles de nivel de base de datos.

Característica	Tipo	Descripción
sp_helpdbfixedrole (Transact-SQL)	Metadatos	Devuelve la lista de los roles fijos de base de datos.
sp_dbfixedrolepermission (Transact-SQL)	Metadatos	Muestra los permisos de un rol fijo de base de datos.
sp_helprole (Transact-SQL)	Metadatos	Devuelve información acerca de los roles de la base de datos actual.
sp_helprolemember (Transact-SQL)	Metadatos	Devuelve información acerca de los miembros de un rol de la base de datos actual.
sys.database_role_members (Transact-SQL)	Metadatos	Devuelve una fila por cada miembro de cada rol de base de datos.
IS_MEMBER (Transact-SQL)	Metadatos	Indica si el usuario actual es miembro del grupo de Microsoft Windows o del rol de base de datos de SQL Server especificados.
CREATE ROLE (Transact-SQL)	Comando	Crea un nuevo rol de base de datos en la base de datos actual.
ALTER ROLE (Transact-SQL)	Comando	Cambia el nombre de un rol de base de datos.

DROP ROLE (Transact-SQL)	Comando	Quita un rol de la base de datos.
sp_addrole (Transact-SQL)	Comando	Crea un nuevo rol de base de datos en la base de datos actual.
sp_droprole (Transact-SQL)	Comando	Quita un rol de base de datos de la base de datos actual.
sp_addrolemember (Transact-SQL)	Comando	Agrega un usuario de base de datos, un rol de base de datos, un inicio de sesión de Windows o un grupo de Windows a un rol de base de datos en la base de datos actual.
sp_droprolemember (Transact-SQL)	Comando	Quita una cuenta de seguridad de un rol de SQL Server de la base de datos actual.

Rol de base de datos public

Todos los usuarios de una base de datos pertenecen al rol de base de datos publics. Cuando a un usuario no se le han concedido ni denegado permisos específicos para un objeto protegible, el usuario hereda los permisos concedidos a la función pública para ese objeto.

Rol public

El rol **public** está contenido en todas las bases de datos, incluidas las bases de datos del sistema.No se puede eliminar y no se pueden agregar ni quitar usuarios de ella.Todos los usuarios y los demás roles heredan los permisos concedidos al rol **public**, ya que pertenecen de forma predeterminada al rol **public**.Por tanto, solo debe conceder al rol **public** los permisos que desee que tengan todos los usuarios.

Cuenta de usuario dbo

dbo, o propietario de base de datos, es una cuenta de usuario con permisos implícitos para realizar todas las actividades en la base de datos.Los miembros del rol fijo del servidor **sysadmin** se asignan automáticamente a **dbo**.

La cuenta de usuario **dbo** se confunde a menudo con el rol fijo de base de datos **db_owner**.El ámbito de **db_owner** es una base de datos y el ámbito de **sysadmin** es el servidor completo.La pertenencia al rol **db_owner** no proporciona privilegios de usuario **dbo**.

Cuenta de usuario guest

Después de que un usuario se haya autenticado y se le haya permitido iniciar sesión en una instancia de SQL Server, debe existir una cuenta de usuario independiente en cada base de datos a la que tenga acceso el usuario.Si se exige una cuenta de usuario en cada base de datos, se impide que los usuarios se conecten a una instancia de SQL Server y puedan tener acceso a todas las bases de datos de un servidor.La existencia de una cuenta de usuario **guest** en la base de datos

evita este requisito, ya que permite que un inicio de sesión sin cuenta de usuario de base de datos tenga acceso a una base de datos.

La cuenta **guest** es una cuenta integrada en todas las versiones de SQL Server.De forma predeterminada, está deshabilitada en las bases de datos nuevas.Si está habilitada, se puede deshabilitar mediante la revocación de su permiso CONNECT, que se lleva a cabo con la ejecución de la instrucción REVOKE CONNECT FROM GUEST de Transact-SQL.