TECNICATURA UNIVERSITARIA EN PROGRAMACIÓN UTN-FRC

TUP

UTN

Facultad Regional Córdoba

TECNICATURA UNIVERSITARIA EN PROGRAMACIÓN

DISEÑO Y ADMINISTRACIÓN DE BASE DE DATOS

Unidad Temática V: Seguridad de datos y restauración

Material Teórico

2do Año – 4to Cuatrimestre

V.0.1

Índice

Seguridad de datos y restauración

SQL Server incluye varias características de seguridad configurables y de gran precisión. Estas características permiten a los administradores implementar una defensa optimizada para los riesgos de seguridad específicos de su entorno.

En la siguiente tabla se muestran temas importantes relativos a la seguridad.

Tema	Descripción
Proteger SQL Server	Proporciona información general acerca de la protección de SQL Server.
Consideraciones de seguridad para una instalación de SQL Server	Describe la preparación de la red y del servidor de Windows para una instalación de SQL Server.
Configurar cuentas de servicio de Windows	Describe los derechos mínimos de Windows y los permisos de archivo necesarios para los servicios instalados por SQL Server.
Configuración de superficie	Describe cómo minimizar el área de superficie vulnerable de una instalación de SQL Server.
Consideraciones de seguridad para bases de datos y aplicaciones de bases de datos	Describe las características de seguridad del SQL Server Database Engine (Motor de base de datos de SQL Server).
Proteger Analysis Services	Proporciona información general de la seguridad de SQL Server Analysis Services (SSAS).
Consideraciones de seguridad para Integration Services	Proporciona información general de la seguridad de SQL Server Integration Services (SSIS).
Consideraciones de seguridad para la réplica	Proporciona información general de la seguridad de la réplica.
Proteger Reporting Services	Describe las opciones para la configuración de la seguridad de SQL Server Reporting Services (SSRS).
Consideraciones de seguridad para Notification Services	Proporciona información general de la seguridad de SQL Server Notification Services.
Consideraciones de seguridad para Service Broker	Proporciona una descripción general de la seguridad de SQL Server Service Broker.
CLR Integration Security	Proporciona información general de aspectos relativos a la seguridad de Integración CLR.
Vistas de catálogo de seguridad	Muestra los metadatos relativos a la seguridad

(Transact-SQL)	visibles en vistas de catálogos optimizadas para el rendimiento y la utilidad.
Funciones de seguridad (Transact-SQL)	Muestra las funciones que incluyen información útil para la administración de la seguridad.
Funciones de cifrado (Transact-SQL)	Muestra las funciones que admiten cifrado, descifrado, firma digital y validación de firmas digitales.

Tabla 1: Elaboración propia

La protección de SQL Server implica tres áreas: la plataforma y la red, las entidades de seguridad y los asegurables, y las aplicaciones que obtienen acceso a la base de datos. Los siguientes temas le guiarán durante el proceso de creación e implementación de un plan de seguridad eficaz.

Seguridad de la plataforma y de la red

La plataforma de SQL Server incluye el hardware físico y los sistemas de redes que conectan los clientes con los servidores de base de datos, así como los archivos binarios que se utilizan para procesar solicitudes de base de datos.

Seguridad física

Las recomendaciones de seguridad física limitan de forma estricta el acceso al servidor físico y a los componentes de hardware. Por ejemplo, use salas cerradas de acceso restringido para el hardware de servidor de base de datos y los dispositivos de red. Además, limite el acceso a los medios de copia de seguridad almacenándolos en una ubicación segura fuera de las instalaciones.

Seguridad del sistema operativo

Los Service Packs y las actualizaciones del sistema operativo incluyen mejoras de seguridad importantes. Aplique todas las revisiones y actualizaciones al sistema operativo después de probarlas con las aplicaciones de base de datos.

Los firewalls también proporcionan formas eficaces de implementar la seguridad. Lógicamente, un firewall es un separador o limitador del tráfico de red, que puede configurarse para aplicar la directiva de seguridad de datos de su organización. El uso de un firewall aumenta la seguridad del sistema operativo ya que proporciona un punto de arranque en el que pueden centrarse las medidas de seguridad. En la siguiente tabla se incluye más información sobre la forma de usar un firewall con SQL Server.

La reducción de la superficie es una medida de seguridad que implica detener o deshabilitar componentes no utilizados. La reducción de la superficie ayuda a mejorar la seguridad al proporcionar menos accesos para ataques

potenciales al sistema. La clave para limitar la superficie de SQL Server consiste en ejecutar los servicios requeridos con "privilegios mínimos" mediante la concesión de los derechos necesarios únicamente a los servicios y usuarios. En el siguiente gráfico se incluye más información sobre el acceso al sistema y los servicios.

Seguridad de los archivos del sistema operativo de SQL Server

SQL Server usa archivos del sistema operativo para el funcionamiento y el almacenamiento de datos. Las recomendaciones de seguridad de archivos indican que se restrinja el acceso a estos archivos.

Los Service Packs y actualizaciones de SQL Server proporcionan una seguridad mejorada. Para determinar el último Service Pack disponible para SQL Server.

Puede usar la siguiente secuencia de comandos para determinar el Service Pack instalado en el sistema:

```
SELECT CONVERT(char(20), SERVERPROPERTY('productlevel'));
GO
```

Entidades de seguridad y seguridad de objetos de base de datos

Las entidades de seguridad son los individuos, grupos y procesos que tienen acceso a SQL Server. Los asegurables son el servidor, la base de datos y los objetos incluidos en la base de datos. Cada uno de estos elementos dispone de un conjunto de permisos que pueden configurarse para minimizar aún más la superficie de SQL Server.

Cifrado y certificados

El cifrado no resuelve los problemas de control de acceso. Sin embargo, mejora la seguridad debido a que limita la pérdida de datos, incluso en el caso poco probable de que se superen los controles de acceso. Por ejemplo, si el equipo host de base de datos no está configurado correctamente y un pirata informático obtiene datos confidenciales, como números de tarjetas de crédito, esa información robada resulta inservible si está cifrada.

Los certificados son "claves" de software que se comparten entre dos servidores que permiten las comunicaciones seguras a través de una autenticación segura. Puede crear y usar certificados en SQL Server para mejorar la seguridad de objetos y conexiones.

Funciones y vistas de catálogo de seguridad de SQL Server

El Database Engine (Motor de base de datos) expone información de seguridad en varias vistas y funciones que se optimizan en cuanto a rendimiento y

utilidad. En el siguiente gráfico se incluye más información acerca de las funciones y vistas de seguridad.

Funciones

Las siguientes funciones devuelven información útil para la administración de la seguridad.

CURRENT_USER (Transact-SQL)	SETUSER (Transact-SQL)
sys.fn_builtin_permissions (Transact-SQL)	SUSER_ID (Transact-SQL)
Has_Perms_By_Name (Transact-SQL)	SUSER_SID (Transact-SQL)
IS_MEMBER (Transact-SQL)	SUSER_SNAME (Transact-SQL)
IS_SRVROLEMEMBER (Transact-SQL)	SYSTEM_USER (Transact-SQL)
PERMISSIONS (Transact-SQL)	SUSER_NAME (Transact-SQL)
SCHEMA_ID (Transact-SQL)	USER_ID (Transact-SQL)
SCHEMA_NAME (Transact-SQL)	USER_NAME (Transact-SQL)
SESSION_USER (Transact-SQL)	

Tabla 2: Elaboración propia

Para obtener detalle sobre cada función, por favor recurrir a la documentación oficial de Microsoft.

Autenticación

Una credencial es un registro que contiene la información de autenticación (credenciales) necesaria para conectarse a un recurso situado fuera de SQL Server. Esta información es utilizada internamente por SQL Server. La mayoría de las credenciales incluyen un nombre de usuario y una contraseña de Windows.

La información almacenada en una credencial permite al usuario que se haya conectado a SQL Server mediante autenticación de SQL Server obtener acceso a recursos situados fuera de la instancia de servidor. Cuando el recurso externo es Windows, el usuario se autentica como el usuario de Windows especificado en la credencial. Se puede asignar una única credencial a varios inicios de sesión de SQL Server. Sin embargo, un inicio de sesión de SQL Server sólo se puede asignar a una credencial.

Las credenciales del sistema se crean de forma automática y se asocian a extremos específicos. Los nombres de las credenciales del sistema comienzan por dos signos de número (##).

Configurar el modo de autenticación

Si selecciona la autenticación de modo mixto durante la instalación, debe proporcionar una contraseña segura, y confirmarla después, para la cuenta de

administrador del sistema de SQL Server integrada denominada sa. La cuenta sa se conecta con la autenticación de SQL Server.

Si selecciona la autenticación de Windows durante la instalación, el programa de instalación crea la cuenta sa para la autenticación de SQL Server pero se deshabilita. Si después cambia a la autenticación de modo mixto y desea utilizar la cuenta sa, debe habilitar la cuenta.

Cualquier cuenta de SQL Server o de Windows se puede configurar como del administrador del sistema. Dado que la cuenta sa es muy conocida y a menudo es el objetivo de usuarios malintencionados, no la habilite a menos que la aplicación lo requiera. Nunca establezca una contraseña en blanco o con poca seguridad para la cuenta sa.

Conectar a través de la Autenticación de Windows

Cuando un usuario se conecta a través de una cuenta de usuario de Microsoft Windows, SQL Server valida el nombre de cuenta y la contraseña con el token de la entidad de seguridad de Windows del sistema operativo. Esto significa que Windows confirma la identidad del usuario.

SQL Server no pide la contraseña y no realiza la validación de identidad. La autenticación de Windows es el modo de autenticación predeterminado y es mucho más seguro que la autenticación de SQL Server. La autenticación de Windows usa el protocolo de seguridad de Kerberos, proporciona la aplicación de directivas de contraseñas en cuanto a la validación de la complejidad de las contraseñas seguras, ofrece compatibilidad para el bloqueo de cuentas y admite la expiración de las contraseñas. Una conexión realizada utilizando la autenticación de Windows se denomina a veces conexión de confianza, porque SQL Server confía en las credenciales proporcionadas por Windows.

Conectar a través de la Autenticación de SQL Server

Al utilizar la autenticación de SQL Server, los inicios de sesión se crean en SQL Server, que no se basa en las cuentas de usuario de Windows. El nombre de usuario y la contraseña se crean utilizando SQL Server y se almacenan en SQL Server. Los usuarios que se conectan utilizando la autenticación de SQL Server deben proporcionar sus credenciales (inicio de sesión y contraseña) cada vez que se conectan. Al utilizar la autenticación de SQL Server, debe establecer contraseñas seguras para todas las cuentas de SQL Server.

Hay tres directivas de contraseñas opcionales para los inicios de sesión de SQL Server.

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión Exige que el usuario cambie la contraseña la próxima vez que se

conecte. SQL Server Management Studio proporciona la capacidad de cambiar la contraseña. Otros programadores de software deberían proporcionar esta característica si se utiliza esta opción.

- Exigir expiración de contraseña. La directiva de vigencia máxima de la contraseña del equipo se exige para los inicios de sesión de SQL Server.
- Exigir directivas de contraseñas. Las directivas de contraseñas de Windows del equipo se exigen para los inicios de sesión de SQL Server. Esto incluye la longitud y complejidad de las contraseñas. Esta funcionalidad depende de la API NetValidatePasswordPolicy, que sólo está disponible en Windows Server 2003 y versiones posteriores.

Para determinar las directivas de las contraseñas del equipo local

- En el menú Inicio, haga clic en Ejecutar.
- En el cuadro de diálogo Ejecutar, escriba secpol.msc y, a continuación, haga clic en Aceptar.
- En la aplicación Configuración de seguridad local, expanda Configuración de seguridad, expanda Directivas de cuenta y, a continuación, haga clic en Directiva de contraseñas.

Las directivas de contraseñas se describen en el panel de resultados

Ventajas de la Autenticación de SQL Server

- Permite a SQL Server admitir las aplicaciones anteriores y las que proporcionan terceros y requieren la autenticación de SQL Server.
- Permite que SQL Server admita entornos con sistemas operativos mixtos, en los que un dominio de Windows no autentica a todos los usuarios.
- Permite a los usuarios conectarse desde dominios desconocidos o que no son de confianza. Por ejemplo, una aplicación en la que los clientes establecidos se conectan con los inicios de sesión de SQL Server asignados para recibir el estado de sus pedidos.
- Permite que SQL Server admita aplicaciones basadas en WEB en las que los usuarios crean sus propias identidades.
- Permite a los desarrolladores de software distribuir sus aplicaciones utilizando una jerarquía de permisos compleja basada en los inicios de sesión conocidos y preestablecidos de SQL Server.

Desventajas de la Autenticación de SQL Server

- Si un usuario del dominio de Windows tiene un inicio de sesión y una contraseña para Windows, aún debe proporcionar otro inicio de sesión y contraseña (SQL Server) para conectarse. Hacer el seguimiento de varios nombres y contraseñas es difícil para muchos usuarios. Tener que proporcionar las credenciales de SQL Server cada vez que se conectan a la base de datos puede resultar molesto.
- La autenticación de SQL Server no puede utilizar el protocolo de seguridad de Kerberos.
- Windows proporciona directivas de contraseñas adicionales que no están disponibles para los inicios de sesión de SQL Server.

SQL Server puede ser configurado para utilizar unos de estos modos de autenticación.

Cuándo utilizar el Modo de Autenticación de Windows

Utilice este modo en entornos de red en los cuales los usuarios son autenticados a través de cuentas de usuario de Windows.

Ventajas de la Autenticación Windows

- Permite agregar grupos de usuarios a SQL Server agregando una única cuenta de usuario.
- Permite a los usuarios acceder rápidamente a SQL Server sin tener que recordar cuenta y contraseña.

Cuándo utilizar el Modo Mixto

Utilice este modo cuando tenga que permitir conectarse a SQL Server a usuarios o aplicaciones que no tengan credenciales Windows.

Directiva de Contraseñas

Cuando SQL Server se ejecuta en Windows Server 2003 o versiones posteriores, puede utilizar mecanismos de directiva de contraseñas de Windows.
SQL Server puede aplicar las mismas directivas de complejidad y caducidad que se usan en Windows Server 2003 a las contraseñas que se usan en SQL Server. Esta funcionalidad depende de la API NetValidatePasswordPolicy, que sólo está disponible en Windows Server 2003 y versiones posteriores.

Las directivas de complejidad de contraseñas están diseñadas para impedir ataques por fuerza bruta mediante el aumento del número de contraseñas posibles.

Cuando se aplica la directiva de complejidad de contraseñas, se exige que las nuevas contraseñas cumplan las siguientes directrices:

- La contraseña no debe contener parte o todo el nombre de la cuenta del usuario. Una parte de un nombre de cuenta se define como tres o más caracteres alfanuméricos consecutivos delimitados en ambos extremos por un espacio en blanco, como un espacio, tabulación, retorno, etc., o por alguno de los siguientes caracteres: coma (,), punto (.), guión (-), carácter de subrayado (_) o signo de número (#).
- La contraseña debe tener una longitud de ocho caracteres como mínimo.
- La contraseña debe contener caracteres de tres de las siguientes categorías: o Letras en mayúsculas del alfabeto Latín (de la “A” a la “Z”) o Letras en minúsculas del alfabeto Latín (de la "a" a la "z") o Dígitos en base 10 (del 0 al 9) o Caracteres que no sean alfanuméricos, como signo de exclamación (!), signo de moneda ($), signo de número (#) o porcentaje (%).

Las contraseñas pueden tener hasta 128 caracteres. Se recomienda utilizar contraseñas lo más largas y complejas posible.

Las directivas de caducidad de contraseñas se utilizan para administrar la duración de una contraseña. Cuando SQL Server aplica la directiva de caducidad de contraseñas, se recuerda a los usuarios que cambien las contraseñas antiguas, y las cuentas con contraseñas que han caducado se deshabilitan.

Contraseñas Seguras

Las contraseñas pueden constituir el vínculo más débil de una implementación de seguridad de servidor. Debe tener siempre mucho cuidado a la hora de elegir una contraseña. Una contraseña segura presenta las siguientes características:

- Tiene una longitud de 8 caracteres como mínimo.
- Contiene una combinación de letras, números y símbolos.
- No es una palabra que pueda encontrarse en el diccionario.
- No es el nombre de un comando.
- No es el nombre de una persona.
- No es el nombre de un usuario.
- No es el nombre de un equipo.
- Se cambia con frecuencia.
- Presenta diferencias notables con respecto a contraseñas anteriores.

Las contraseñas de SQL Server pueden contener hasta 128 caracteres, entre los que se pueden incluir letras, símbolos y dígitos. Dado que los inicios de

sesión, nombres de usuario funciones y contraseñas se utilizan con frecuencia en instrucciones Transact-SQL determinados símbolos deberán estar incluidos entre comillas dobles (") o corchetes ([ ]). Utilice estos delimitadores en las instrucciones Transact-SQL cuando el inicio de sesión, usuario función o contraseña de SQL Server presente las siguientes características:

- Contiene o comienza por un carácter de espacio.
- Comienza por el carácter $ o @.

Si se utiliza en una cadena de conexión OLE DB u ODBC, el inicio de sesión o la contraseña no deben contener ninguno de los siguientes caracteres: [] {}() , ; ? * ! @. Estos caracteres se utilizan para inicializar una conexión o para separar valores de conexión.

Funciones (Roles) de Nivel de Servidor (Server Fixed Roles)

Las funciones fijas de servidor abarcan todo el ámbito del servidor. Cada miembro de una función fija de servidor puede agregar otros inicios de sesión a esa misma función.

Las funciones fijas de servidor se pueden asignar a los permisos más específicos que se incluyen en SQL Server. La siguiente tabla describe la asignación de funciones fijas de servidor a permisos.

Función fija de servidor	**Permiso en el servidor**
bulkadmin	**Se le concede: ADMINISTER BULK OPERATIONS**
dbcreator	**Se le concede: CREATE DATABASE**
diskadmin	**Se le concede: ALTER RESOURCES**
processadmin	**Se le concede: ALTER ANY CONNECTION, ALTER SERVER STATE**
securityadmin	**Se le concede: ALTER ANY LOG**
serveradmin	**Se le concede: ALTER ANY ENDPOINT, ALTER RESOURCES, ALTER SERVER STATE, ALTER SETTINGS, SHUTDOWN, VIEW SERVER STATE**
setupadmin	**Se le concede: ALTER ANY LINKED SERVER**
sysadmin	**Se le concede con la opción GRANT: CONTROL SERVER**

Tabla 3: Elaboración propia

La Función public

Además de las funciones fijas de servidor mencionadas en la tabla anterior, cada instancia de SQL contiene una función fija de servidor especial denominada public de la cual todos los inicios de sesión son miembros.

A la función public se le concede el permiso VIEW ANY DATABASE.

Funciones (Roles) en el Nivel de Base de Datos

Las funciones fijas de base de datos se definen en el nivel de base de datos y existen en cada una de ellas. Los miembros de las funciones de base de datos db_owner y db_securityadmin pueden administrar a los miembros de una función fija de base de datos; sin embargo, sólo los miembros de una función de base de datos db_owner pueden agregar miembros a la función fija de base de datos db_owner.

Las funciones fijas de base de datos se pueden asignar a permisos más detallados que se incluyen en SQL Server. La tabla siguiente describe la asignación de funciones fijas de base de datos a permisos.

Función fija de base de datos	Permiso en la base de datos	Permiso en el servidor
db_accessadmin	Concedido: ALTER ANY USER, CREATE SCHEMA	Concedido: VIEW ANY DATABASE
db_accessadmin	Concedido con la opción GRANT: CONNECT	
db_backupoperator	Concedido: BACKUP DATABASE, BACKUP LOG, CHECKPOINT	Concedido: VIEW ANY DATABASE
db_datareader	Concedido: SELECT	Concedido: VIEW ANY DATABASE
db_datawriter	Concedido: DELETE, INSERT, UPDATE	Concedido: VIEW ANY DATABASE
db_ddladmin	Concedido: ALTER ANY ASSEMBLY, ALTER ANY ASYMMETRIC KEY, ALTER ANY CERTIFICATE, ALTER ANY CONTRACT,	Concedido: VIEW ANY DATABASE

	ALTER ANY DATABASE DDL TRIGGER, ALTER ANY DATABASE EVENT, NOTIFICATION, ALTER ANY DATASPACE, ALTER ANY FULLTEXT CATALOG, ALTER ANY MESSAGE TYPE, ALTER ANY REMOTE SERVICE BINDING, ALTER ANY ROUTE, ALTER ANY SCHEMA, ALTER ANY SERVICE, ALTER ANY SYMMETRIC KEY, CHECKPOINT, CREATE AGGREGATE, CREATE DEFAULT, CREATE FUNCTION, CREATE PROCEDURE, CREATE QUEUE, CREATE RULE, CREATE SYNONYM, CREATE TABLE, CREATE TYPE, CREATE VIEW, CREATE XML SCHEMA COLLECTION, REFERENCES	
db_denydatareader	Denegado: SELECT	Concedido: VIEW ANY DATABASE
db_denydatawriter	Denegado: DELETE, INSERT, UPDATE	
db_owner	Concedido con la opción GRANT: CONTROL	Concedido: VIEW ANY DATABASE
db_securityadmin	Concedido: ALTER ANY APPLICATION ROLE, ALTER ANY ROLE, CREATE SCHEMA, VIEW DEFINITION	Concedido: VIEW ANY DATABASE

dbm_monitor	**Concedido: VIEW el estado más reciente en el Monitor de creación de reflejo de la base de datos Nota: La función fija de base de datos dbm_monitor se crea en la base de datos msdb cuando se registra la primera base de datos en el Monitor de creación de reflejo de la base de datos. La nueva función dbm_monitor no tiene miembros hasta que un administrador del sistema asigne usuarios a la función.**	**Concedido: VIEW ANY DATABASE**

Tabla 4: Elaboración propia

Jerarquía de Permisos

El Motor de base de datos de SQL Server administra un conjunto jerárquico de entidades que se pueden proteger mediante permisos. Estas entidades se conocen como asegurables.

Los asegurables más importantes son los servidores y las bases de datos, aunque se pueden establecer permisos discretos en niveles menores. SQL Server regula las acciones de las entidades de seguridad en los asegurables comprobando que se les han concedido los permisos adecuados.

Los permisos se pueden manipular con las conocidas consultas GRANT, DENY y REVOKE de Transact-SQL. La información sobre los permisos está visible en las vistas de catálogo sys.server_permisions y sys.database_permisions. También hay información sobre la compatibilidad con permisos para consultas mediante el uso de las funciones integradas.

Usuarios de SQL Server

Para crear un usuario de base de datos mediante SQL Server Management Studio.

En SQL Server Management Studio, abra el Explorador de objetos y expanda la carpeta Bases de datos. Expanda la base de datos en la que se va a crear el usuario de la misma.

Haga clic con el botón secundario en la carpeta Seguridad, seleccione Nuevo y, a continuación, haga clic en Usuario.

En la página General, escriba un nombre para el usuario en el cuadro Nombre de usuario. En el cuadro Nombre de inicio de sesión, escriba el nombre de un inicio de sesión de SQL Server para asignarlo al usuario de la base de datos.

Haga clic en Aceptar.

Para crear un usuario de bases de datos mediante Transact-SQL

```
USE <nombre_base_datos>
GO
CREATE USER <nombre usuario> FOR LOGIN <nombre login>;
GO
```

Modificación de usuarios

```
ALTER USER user_name
    WITH <set_item> [ ,...n ]
<set_item> ::=
    NAME = new_user_name
    | DEFAULT_SCHEMA = schema_name
    | LOGIN = login_name
```

En donde:

user_name

Especifica el nombre por el que se identifica al usuario en esta base de datos.

LOGIN = login_name

Reasigna un usuario a otro inicio de sesión al cambiar el identificador de seguridad del usuario (SID) para que coincida con el SID del inicio de sesión.

NAME = new_user_name

Especifica el nuevo nombre de este usuario. new_user_name no debe existir en la base de datos actual.

DEFAULT_SCHEMA = schema_name

Especifica el primer esquema donde buscará el servidor cuando resuelva los nombres de objetos de este usuario.

Sólo puede cambiar el nombre de un usuario que está asignado a un grupo o inicio de sesión de Windows cuando el SID del nuevo nombre de usuario coincide con el SID registrado en la base de datos. Esta comprobación ayuda a evitar la suplantación de inicios de sesión de Windows en la base de datos.

La cláusula WITH LOGIN permite reasignar un usuario a un inicio de sesión diferente. Con esta cláusula no se pueden reasignar los usuarios sin un inicio de sesión, los usuarios asignados a un certificado ni los usuarios asignados a una clave asimétrica. Sólo se pueden reasignar los usuarios de SQL Server y los usuarios (o grupos) de Windows. La cláusula WITH LOGIN no se puede utilizar para cambiar el tipo de usuario, como cambiar una cuenta de Windows a un inicio de sesión.

El nombre del usuario se cambiará automáticamente al nombre de inicio de sesión si se trata de un usuario de Windows, si el nombre es un nombre de Windows (contiene una barra diagonal inversa), o si no se especificó ningún nombre nuevo para él y su nombre actual es diferente del nombre de inicio de sesión. En caso contrario, no se cambiará el nombre al usuario a menos que el autor de las llamadas invoque además la cláusula NAME.

Eliminación de usuarios

DROP USER user_name

En donde:

user_name

Especifica el nombre por el que se identifica al usuario en esta base de datos.

Los usuarios que poseen elementos que pueden protegerse no pueden quitarse de la base de datos. Para poder quitar un usuario de la base de datos que posea un elemento que puede protegerse, primero debe quitar o transferir la propiedad de esos elementos.

El usuario guest no puede quitarse, pero puede deshabilitarse si revoca su permiso CONNECT; para ello, ejecute REVOKE CONNECT FROM GUEST en cualquier base de datos que no sea master o tempdb.

Usuarios especiales de SQL Server

- 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 de la función fija del servidor sysadmin se asignan automáticamente a dbo. La cuenta de usuario dbo se confunde a menudo con la función fija 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 a la función db_owner no proporciona privilegios de usuario dbo.
- Cuenta de usuario
- : 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
- 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
- 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
- de Transact-SQL.

Nota: Se debe evitar el uso de la cuenta, ya que todos los inicios de sesión que no dispongan de permisos de base de datos propios obtendrán los permisos de base de datos concedidos a esta cuenta. Si debe usar la cuenta, concédale los permisos mínimos.

Planear la estrategia de copias de seguridad y restauración

Al administrar una base de datos de SQL Server, es importante estar preparado para la recuperación de desastres potenciales. Es necesario un plan de restauración y de copia de seguridad correctamente diseñado y probado para poder

recuperar las copias de seguridad de SQL Server de las bases de datos después de un desastre.

Además, para garantizar que todos los sistemas y datos puedan recuperar rápidamente su funcionamiento normal en caso de un desastre natural, es necesario crear un plan de recuperación de desastres. Durante la elaboración de este plan es preciso tener en cuenta los escenarios de distintos tipos de desastres que pueden afectar a su negocio, incluidos los desastres naturales, como un incendio, y los desastres técnicos, como los errores en dos discos de una matriz RAID-5. Cuando cree un plan de recuperación de desastres, identifique y prepare todos los pasos necesarios para hacer frente a cada tipo de desastre. Debe realizar la comprobación práctica de los pasos de recuperación de cada escenario. Se recomienda que compruebe el plan de recuperación de desastres mediante la simulación de un desastre natural.

Durante el diseño del plan de copia de seguridad y restauración, es necesario realizar el diseño del plan de recuperación de desastres según el entorno y las necesidades del negocio.

Por ejemplo, supongamos que se produce un incendio y destruye el centro de datos disponibles 24 horas al día. ¿Está seguro de que es posible la recuperación? ¿Cuánto tiempo se puede tardar en llevar a cabo la recuperación y tener disponible el sistema? ¿Cuál es la cantidad de datos perdidos que pueden tolerar los usuarios?

Lo ideal es que el plan de recuperación de desastres indique el tiempo que durará la recuperación y el estado final de las bases de datos que los usuarios pueden esperar. Por ejemplo, puede determinar que, tras la adquisición del hardware especificado, la recuperación debe completarse en 48 horas y sólo se garantizarán los datos hasta finales de la semana previa al incidente.

Un plan de recuperación de desastres se puede estructurar de diferentes maneras y puede contener muchos tipos de información. Entre los tipos de planes de recuperación de desastres se incluyen los siguientes:

- Un plan para adquirir el hardware.
- Un plan de comunicación.
- Una lista de las personas con las que ponerse en contacto si se produce un desastre.
- Instrucciones para ponerse en contacto con las personas implicadas en la respuesta al desastre.
- Información acerca del propietario de la administración del plan.
- Una lista de comprobación de las tareas necesarias para cada escenario de recuperación. Para facilitar la revisión de la evolución de la recuperación de desastres, ponga a cada tarea una inicial a medida

que se vayan completando y anote la hora de finalización en la lista de comprobación.

Elegir el tipo de medio para la copia de seguridad

SQL Server puede generar copias en discos rígidos o cintas. Los discos locales o a través de la red son el medio mas común para guardar copias de seguridad. Cuando la copia se genera en cinta, el dispositivo debe estar instalado localmente al servidor de SQL Server.

Modelos de recuperación

Los modelos de recuperación se han diseñado para controlar el mantenimiento del registro de transacciones. Existen tres modelos de recuperación: simple (Simple), completa (Full) y por medio de registros de operaciones masivas (BULK_LOGGED). Normalmente, en las bases de datos se usa el modelo de recuperación completa o el modelo de recuperación simple.

Modelo de recuperación	Descripción	Riesgo de pérdida de trabajo	¿Recuperación hasta un momento dado?
Simple	Sin copias de seguridad de registros. Recupera automáticamente el espacio de registro para mantener al mínimo los requisitos de espacio, eliminando, en esencia, la necesidad de administrar el espacio del registro de transacciones.	Los cambios realizados después de la copia de seguridad más reciente no están protegidos. En caso de desastre, es necesario volver a realizar dichos cambios.	Sólo se puede recuperar hasta el final de una copia de seguridad.
Completa	Requiere copias de seguridad de registros. No se pierde trabajo si un archivo de datos se pierde o resulta dañado. Se puede recuperar hasta cualquier momento, por ejemplo, antes del error de aplicación o usuario.	Normalmente ninguno. Si el final del registro resulta dañado, se deben repetir los cambios realizados desde la última copia de seguridad de registros.	Se puede recuperar hasta determinado momento, siempre que las copias de seguridad se hayan completado hasta ese momento.
Por medio de registros de operaciones masivas	Requiere copias de seguridad de registros. Complemento del modelo de recuperación completa que permite operaciones de copia masiva de alto rendimiento. Reduce el uso del espacio de	Si el registro resulta dañado o se han realizado operaciones masivas desde la última copia de seguridad de registros, se pueden repetir los cambios desde esa última copia de seguridad. En caso contrario, no	Se puede recuperar hasta el final de cualquier copia de seguridad. No admite recuperaciones a un momento dado.

	registro mediante el registro masivo de la mayoría de las operaciones masivas.	se pierde el trabajo.	

Tabla 5: Elaboración propia

Recuperación simple

Utilícelo si se dan todas las condiciones siguientes:

- La recuperación al momento del error no es necesaria. Si se pierde o se daña la base de datos, no le importa perder todas las actualizaciones realizadas entre el error y la copia de seguridad anterior.
- No le importa perder algunos datos del registro.
- No desea realizar copias de seguridad del registro de transacciones ni restaurarlo, y prefiere confiar exclusivamente en las copias de seguridad completas y diferenciales.

Recuperación completa

Utilice este modelo y, opcionalmente, también el modelo de recuperación por medio de registros de operaciones masivas, si se da cualquiera de las condiciones siguientes:

- Desea poder recuperar todos los datos.
- Si la base de datos incluye varios grupos de archivos y desea realizar una restauración por etapas de los grupos de archivos secundarios de lectura y escritura, y opcionalmente, de los de sólo lectura.
- Debe poder realizar una recuperación hasta el momento del error.
- Desea poder restaurar páginas individuales.
- Le resulta aceptable incurrir en los costes administrativos de las copias de seguridad del registro de transacciones.

Tipos de copias de seguridad

- Copias de seguridad completas de bases de datos.
- Copias de Seguridad del Registro de Transacciones.
- Copias de Seguridad Diferenciales.
- Copias de Seguridad de Archivos o Grupos de Archivos.

Copias de seguridad completas de bases de datos

Una copia de seguridad completa de la base de datos crea una copia de seguridad de toda la base de datos, que incluye parte del registro de transacciones para que se pueda recuperar la copia de seguridad completa de la base de datos. Las copias de seguridad completas representan la base de datos en el momento en que finalizó la copia de seguridad.

Las copias de seguridad de bases de datos son fáciles de utilizar. Una copia de seguridad completa de una base de datos contiene todos los datos de la base de datos. Para las bases de datos pequeñas, de las que se puede hacer una copia de seguridad con rapidez, la práctica recomendada es utilizar copias de seguridad completas de la base de datos. Sin embargo, a medida que la base de datos aumenta de tamaño, las copias de seguridad completas requieren una mayor cantidad de tiempo y espacio de almacenamiento. Por ello, para una base de datos grande, puede que desee complementar las copias de seguridad completas con copias de seguridad diferenciales.

Copia de seguridad en el modelo de recuperación completa

En el modelo de recuperación completa se usan copias de seguridad de registros para evitar la pérdida de datos en la mayor parte de los casos de error y es necesario realizar copias de seguridad y restaurar el registro de transacciones (copias de seguridad de registros). La ventaja de usar las copias de seguridad de registros reside en que permite restaurar una base de datos a cualquier momento de una copia de seguridad de registros (recuperación a un momento dado). Si consideramos que se puede realizar una copia de seguridad del registro activo después de que ocurra un desastre, se podrá restaurar la base de datos al momento del error sin perder datos. Las desventajas de usar las copias de seguridad de registros son que requieren espacio de almacenamiento y aumentan la duración y la complejidad de las restauraciones.

En las bases de datos en que se usa con frecuencia el modelo de recuperación completa, se pueden optimizar algunas operaciones masivas utilizando temporalmente el modelo de recuperación por medio de registros de operaciones masivas. El modelo de recuperación por medio de registros de operaciones masivas impone varias restricciones que hacen que no sea adecuado para su uso diario.

Minimizar el riesgo de pérdida de trabajo

Una vez que finaliza la primera copia de seguridad completa de la base de datos y se inician las copias de seguridad periódicas de registros, el riesgo potencial de pérdida de trabajo se limita al tiempo transcurrido entre el momento en que se daña la base de datos y la copia de seguridad periódica de registros más reciente. Por lo tanto, recomendamos que realice copias de seguridad de registros con suficiente frecuencia para mantener el riesgo de pérdida de trabajo dentro de los límites establecidos por sus requisitos empresariales.

Cuando se produce un error, puede intentar realizar una copia de seguridad del registro después del error (el registro del que aún no se ha realizado una copia de seguridad). Si la copia de seguridad del registro después del error se realiza sin problemas, puede evitar cualquier pérdida de trabajo restaurando la base de datos hasta el momento del error. Puede utilizar una serie de copias de seguridad de registros para poner al día una base de datos hasta cualquier momento que se encuentre en una de las copias de seguridad de registros. Para minimizar el riesgo, recomendamos programar copias de seguridad de registros rutinarias. Tenga en cuenta que para minimizar el tiempo de restauración, puede complementar cada copia de seguridad completa con una serie de copias de seguridad diferenciales de los mismos datos.

Copias de Seguridad del Registro de Transacciones

En los modelos de recuperación completa y por medio de registros de operaciones masivas, es necesario realizar copias de seguridad periódicas de los registros de transacciones (copias de seguridad de registros) para recuperar datos. Gracias a las copias de seguridad de registros es posible recuperar la base de datos en el punto en que se haya producido el error o en un momento dado. Es aconsejable realizar copias de seguridad de registros suficientemente regulares para ajustarse a los requisitos de su empresa, específicamente a la tolerancia a la pérdida de trabajo que una unidad de registro dañada podría provocar. La frecuencia adecuada para realizar copias de seguridad de registros varía en función de la tolerancia al riesgo de pérdida de trabajo y, por otra parte, de la cantidad de copias de seguridad de registros que puede almacenar, administrar y, potencialmente, restaurar. Una copia de seguridad de registros cada 15 ó 30 minutos puede ser suficiente. Si su empresa necesita minimizar el riesgo de pérdida de trabajo, piense en la posibilidad de realizar copias de seguridad de registros más frecuentemente. Al realizar copias de seguridad de registros con más frecuencia tendrá la ventaja añadida de que la frecuencia del truncamiento del registro será mayor, por lo que los archivos o archivos de registro serán más pequeños.

Antes de crear la primera copia de seguridad de registros, debe crear una copia de seguridad completa, como una copia de seguridad de la base de datos o la primera de un conjunto completo de copias de seguridad de archivos. La restauración de una base de datos utilizando únicamente copias de seguridad de archivos puede llegar a ser un proceso complejo. Por lo tanto, es recomendable que comience con una copia de seguridad de la base de datos completa si es posible. Posteriormente, será necesario realizar copias de seguridad del registro de transacciones con regularidad. De esta forma, no sólo se minimiza el riesgo de pérdida de trabajo, sino que también se permite el truncamiento del registro de transacciones.

Normalmente, el registro de transacciones se trunca tras cada copia de seguridad de registros convencional.

La cadena de registros

Una secuencia continua de copias de seguridad de registros se denomina cadena de registros.

Una cadena de registros empieza con una copia de seguridad completa de la base de datos.

Por lo general, una nueva cadena de registros sólo se inicia cuando se realiza una copia de seguridad de la base de datos por primera vez o después de cambiar del modelo de recuperación simple al modelo de recuperación completa o por medio de registros de operaciones masivas.

Para restaurar una base de datos al momento del error, es preciso que la cadena de registros esté intacta. De esta forma, es necesario que una secuencia ininterrumpida de las copias de seguridad del registro de transacciones se extienda hasta el momento del error. El lugar en el que ésta secuencia de registros debe comenzar depende del tipo de copias de seguridad de datos que esté restaurando: de base de datos, parcial o de archivos. En las copias de seguridad de base de datos o parciales, la secuencia de copias de seguridad de registros debe extenderse desde el final de la copia de seguridad de base de datos o parcial. En un conjunto de copia de seguridad de archivos, la secuencia de copias de seguridad de registros debe comenzar desde el principio del conjunto completo de copias de seguridad de archivos.

Si sólo utiliza copias de seguridad de archivos, es necesario realizar una copia de seguridad del registro desde el principio de la primera copia de seguridad de archivos completa. Es posible comenzar a realizar copias de seguridad de registros inmediatamente después de la primera copia de seguridad de archivos completa. Es recomendable comenzar en ese momento, dado que la primera copia de seguridad de registros puede tardar mucho tiempo.

Mientras se realiza la copia de seguridad del registro, puede realizar copias de seguridad de otros archivos. Para restaurar la base de datos sólo con copias de seguridad de archivos, el conjunto de copias de seguridad completas de archivos debe ampliarse con una o más copias de seguridad de registros que cubran el intervalo entre la primera copia de seguridad de archivos y la última.
Nota: Para identificar la copia de seguridad con la que comienza la cadena de registros en un conjunto de copias de seguridad, consulte la columna begins_log_chain de la tabla backupset o ejecute RESTORE HEADERONLY en el dispositivo de copia de seguridad para ver la columna BeginsLogChain en el conjunto de resultados.

Copias de seguridad diferenciales

Este tema es relevante para todos los tipos de base de datos.

Una copia de seguridad diferencial se basa en la copia de seguridad completa más reciente existente. Esto se denomina base del diferencial. Una copia de seguridad diferencial incluye sólo los datos que han cambiado desde la última base diferencial.

El tamaño de una copia de seguridad diferencial depende de la cantidad de datos que han cambiado desde la base. Como regla general, cuanto más antigua sea una base, más grande será una nueva copia de seguridad diferencial. Una copia de seguridad diferencial captura el estado de las extensiones modificadas en el momento en que se crea la copia de seguridad. Si crea una serie de copias de seguridad diferenciales, es probable que una extensión actualizada con frecuencia contenga datos diferentes en cada una de las copias diferenciales. A medida que se incrementa el tamaño de las copias de seguridad diferenciales, la restauración de una copia de seguridad diferencial puede incrementar sensiblemente el tiempo necesario para restaurar una base de datos. Por ello, recomendamos que realice una copia de seguridad completa a intervalos definidos para establecer una nueva base diferencial para los datos. Por ejemplo, cada semana podría realizar una copia de seguridad completa de toda la base de datos (es decir, una copia de seguridad completa de la base de datos) seguida de una serie de copias de seguridad diferenciales de la base de datos realizadas periódicamente durante la semana.

Migración de bases de datos

A veces resulta útil copiar una base de datos de un equipo a otro. Se puede utilizar una base de datos copiada con muchos fines, como realizar pruebas, comprobaciones de coherencia, desarrollo de software, ejecución de informes, creación de una base de datos reflejada, o para que la base de datos esté disponible para operaciones con oficinas remotas.

Existen varios métodos alternativos para copiar una base de datos entre servidores:

- Usar el Asistente para copiar bases de datos
- Restaurar una copia de seguridad de una base de datos. Para copiar una base de datos completa, puede utilizar las instrucciones BACKUP y RESTORE de Transact-SQL. Normalmente, la restauración de una copia de seguridad completa de una base de datos se utiliza para copiar la base de datos de un equipo a otro por varios motivos. Para obtener información sobre el uso de la copia de seguridad y la restauración para copiar una base de datos.
- Copiar bases de datos desde Microsoft SQL Server 6.5 o anterior.

Bibliografía

Libros en pantalla SQL Server
Fundamentos de Bases de Datos - Quinta Edición, Silberschatz – Korth - Sudarshan, Mc Graw Hill.
W3Schools - SQL https://www.w3schools.com/sql/default.asp