

Capítulo 7

Protección de los datos

Al finalizar el capítulo, el alumno podrá:

- Identificar las diferentes áreas expuestas que deben ser aseguradas.
- Asegurar datos a nivel granular.
- Asegurar bases de datos a nivel global.
- Minimizar el riesgo de accesos no autorizados.
- Minimizar el riesgo de fugas de información.

Temas

1. Integración con políticas de seguridad de Windows Server
2. Seguridad de los servicios
3. Encriptado de datos
4. Implementando encriptación a nivel de celda
5. Encriptado transparente de datos (TDE)
6. Enmascarado dinámico de datos

1. Integración con políticas de seguridad de Windows Server

Integración con políticas de seguridad de Windows Server

Integración de políticas de seguridad de Windows Server con SQL Server.

La directiva de grupo define los requisitos de contraseña de Windows:


- Longitud.
- Complejidad.
- Expiración.
- Repetición.

SQL Server aplica la directiva de contraseña solo a los inicios de sesión de SQL.

Requiere SQL Server 2005 o superior, y Windows Server 2003 o superior.

7 - 4

Copyright © Todos los Derechos Reservados - Cibertec Perú S.A.C.



En Windows Server se pueden usar las directivas de grupo para definir las configuraciones de usuarios y equipos para grupos de usuarios y equipos.

Así, se puede usar la directiva de grupo para configurar muchas opciones, incluidas las directivas de cuentas. Las directivas de contraseñas son útiles para garantizar que todas las contraseñas sean lo suficientemente complejas y que se cambien periódicamente para maximizar la seguridad y evitar el acceso no autorizado.

En SQL Server las directivas de cuentas locales o de dominio se pueden aplicar a inicios de sesión de SQL, así como, a los inicios de sesión de Windows, cuando SQL Server se instala en equipos que usan Windows Server 2008 o posterior.

1.1 Directivas de complejidad de contraseña

Las directivas de complejidad de contraseñas están diseñadas para disuadir los ataques de fuerza bruta por medio del aumento del número de contraseñas posibles. Cuando se aplica la directiva de complejidad de contraseñas, las nuevas contraseñas deben cumplir los requisitos de directiva establecidos por la directiva de contraseñas de Windows. Un ejemplo de este tipo de directiva sería:

- La contraseña no contiene todo o parte del nombre de 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 (espacio, tabulación, retorno, etc.) o por cualquiera de los caracteres siguientes: , . - _ #
- La contraseña debe tener una longitud de siete caracteres como mínimo.
- La contraseña contiene caracteres de tres de las cuatro categorías siguientes:
 - Abecedario inglés en mayúsculas (de la A a la Z).
 - Abecedario inglés en minúsculas (de la a a la z).
 - Dígitos en base decimal (del 0 al 9).
 - Caracteres no alfanuméricos (por ejemplo: !, \$, #, o %).

2. Seguridad de los servicios

Seguridad de los servicios

- Un servicio de SQL Server es un proceso independiente que interactúa con el sistema operativo para ejecutar tareas del motor de base de datos, de servicios de análisis integración, reportes, etc.
- La interacción implica autenticación de una cuenta, llamada cuenta del servicio.
- Aislar los servicios reduce el riesgo de que un servicio comprometido pueda afectar a los demás servicios.
- Para aislar servicios considere ejecutar cada servicio SQL Server usando cuentas separadas de Windows.
- Usar cuentas de dominio de Windows o locales con bajos privilegios.

7 - 7

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



El SQL Server Configuration Manager es una herramienta usada para administrar los servicios asociados a SQL Server, configurar los protocolos de red que usa SQL Server y administrar la configuración de la conectividad de red de los equipos cliente de SQL Server.

2.1 Servicios de SQL Server

Un servicio de SQL Server es un proceso independiente que interactúa con el sistema operativo para ejecutar tareas del motor de base de datos, de servicios de análisis integración, reportes, etc.

Para poder interactuar con el sistema operativo, el servicio de SQL Server debe autenticarse. Esta autenticación implica la definición de una cuenta de usuario que debe ser reconocida por Windows Server, conocida como cuenta del servicio.

Configurar la seguridad de manera particular para cada servicio permite aislar los servicios. Aislar los servicios reduce el riesgo de que un servicio comprometido con un riesgo de seguridad pueda afectar a los demás servicios y crear una brecha aún mayor. Para aislar servicios se considera ejecutar cada servicio SQL Server usando cuentas separadas de Windows.

Para configurar las cuentas de los servicios se pueden utilizar cuentas del sistema, pero para un mejor control de los niveles de seguridad se recomienda

usar cuentas de dominio de Windows o cuentas de servidor local. Cualquiera que tipo de cuenta que sea utilizada se deben contemplar lo más bajos privilegios posibles.

Al momento de instalar SQL Server 2016, dependiendo de las características seleccionadas, se pueden instalar los siguientes servicios:

- SQL Server Database
- SQL Server Agent
- Analysis Services
- Reporting Services
- Integration Services
- SQL Server Browser
- Full-text search
- SQL Writer
- SQL Server Distributed Replay Controller
- SQL Server Distributed Replay Client

Se debe usar SQL Server Configuration Manager para iniciar, pausar, detener o reiniciar los servicios de Windows asociados a SQL Server. Además, se debe configurar los servicios para controlar los modos de inicio y las cuentas de servicio, así como, las propiedades avanzadas como parámetros de inicio.

**Nota**

Se recomienda cambiar las cuentas de servicio usando SQL Server Configuration Manager en lugar de la consola de Servicios de Windows, ya que el Administrador aplica automáticamente los permisos de registro necesarios para la cuenta especificada.

3. Encriptado de datos

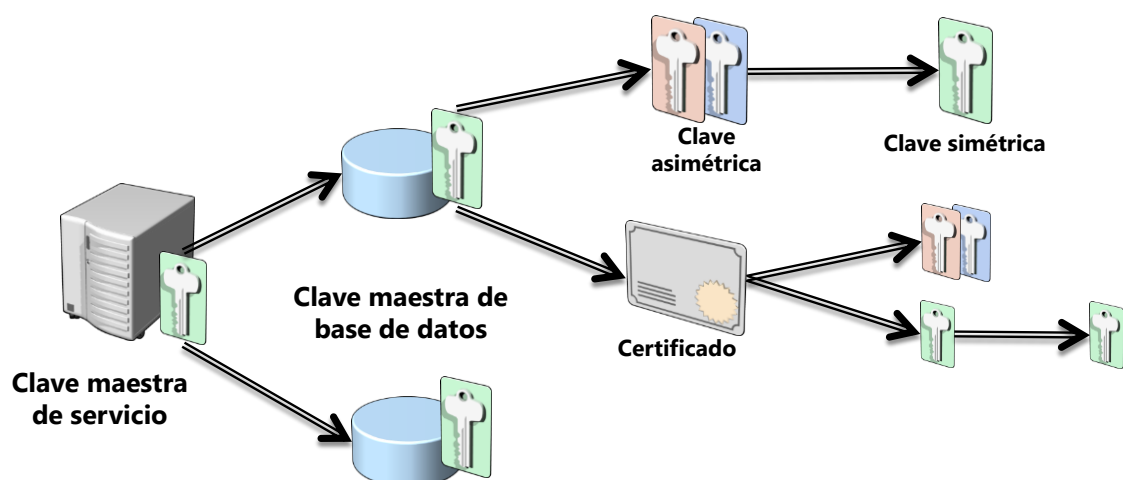
Encriptado de datos

- El encriptado de datos eleva la seguridad de la información de SQL Server
- Motivos para encriptar datos:
 - Privacidad.
 - Cumplimiento de regulaciones.
- El encriptado se produce a través de algoritmos.
- El algoritmo define la transformación de los datos.
- Dicha transformación no puede ser fácilmente revertida por usuarios no autorizados.

7 - 12 Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.

SQL Server usa una jerarquía de claves y certificados para implementar la funcionalidad de encriptado. Cada nivel de la jerarquía se usa para proteger los elementos del nivel, inmediatamente inferior.

3.1 Arquitectura de criptografía de SQL Server



Clave maestra del servicio

Es una clave triple DES en la base de la jerarquía de cifrado de SQL Server. Esta clave se genera automáticamente, cuando se necesita por primera vez, y está protegida por la protección de datos de Windows API (DPAPI).

**Nota**

Realizar una copia de seguridad de la clave principal de servicio y guardarla en una ubicación externa segura.

Clave maestra de base de datos

Es una clave simétrica triple DES que se puede usar para proteger las claves privadas de certificados y claves asimétricas de una base de datos. Cuando se crea una clave principal de base de datos, se cifra mediante el uso del algoritmo Triple DES y una contraseña proporcionada por el usuario. Para habilitar el descifrado automático de la clave principal, una copia de la clave se cifra mediante el uso de la clave principal de servicio, tanto en la misma base de datos como en la base de datos máster.

**Nota**

Realiza una copia de seguridad de cada clave maestra de base de datos y guardarla en una ubicación externa segura.

Claves y certificados de base de datos

La creación de claves y certificados en una base de datos permite cifrar los datos confidenciales o implementar una autenticación y autorización basadas en certificados. Las claves privadas en una base de datos se pueden proteger mediante la clave principal de base de datos o mediante una contraseña.

3.2 Claves

Una clave o llave es un valor que se puede aplicar a una función de encriptado para cifrar o descifrar un valor de datos seguro. El algoritmo para encriptar que se usa para crear la clave y la longitud de la clave, determinan su complejidad. Las claves son la base fundamental para todo el encriptado y se pueden implementar en dos formas: simétrica y asimétrica.

Claves simétrica

Una clave simétrica es un valor que se usa tanto para cifrar como para descifrar datos. Cuando se usa una clave simétrica, deben compartirla tanto la persona o sistema que cifra los datos como la persona o sistema que los descifra. SQL Server admite claves simétricas para la encriptación de datos.

Se puede crear una clave simétrica en SQL Server mediante la ejecución de la instrucción `CREATE SYMMETRIC KEY`, como se muestra en el ejemplo de código siguiente:

```
CREATE SYMMETRIC KEY DBLClaveSim  
WITH ALGORITHM = AES_256  
ENCRYPTION BY PASSWORD = 'BLe@rnerSecVreSimetr1cPa$$w0rd'
```

Se debe tener en cuenta que se debe cifrar la clave simétrica para mantenerla en secreto. En el ejemplo anterior, se usa una contraseña para cifrar la clave simétrica. Las opciones alternativas para cifrar una clave simétrica son usar un certificado, una clave asimétrica u otra clave simétrica.

Claves asimétricas

Las claves asimétricas están compuestas de un par de valores que pueden usarse en una función aritmética unidireccional, de manera que los datos puedan cifrarse con un valor y descifrarse con el otro. Los pares de claves asimétricas están compuestos de una clave pública, que puede compartirse públicamente, y una privada, que el propietario de la clave debe mantener en secreto. Los datos cifrados con la clave pública sólo pueden descifrarse con la clave privada. Además, la clave pública puede usarse para comprobar que una parte de los datos ha sido cifrada por la clave privada (aunque no puede usarse para descifrar los datos). Este enfoque se usa para crear una firma digital que puede usarse para autenticar el origen de los datos.

Se pueden crear claves asimétricas en SQL Server mediante la ejecución de la instrucción `CREATE ASYMMETRIC KEY`, como se muestra en el ejemplo siguiente:

```
CREATE ASYMMETRIC KEY DBLClaveAsim  
WITH ALGORITHM = RSA_2048  
ENCRYPTION BY PASSWORD = 'DBLe@rnerSecVreAsimetr1cPa$$w0rd'
```

Se debe tener en cuenta que la clave privada de una clave asimétrica, se cifra con una contraseña. Si se omite la cláusula `ENCRYPTION BY PASSWORD`, SQL Server cifra la clave privada con la clave de base de datos para la base de datos en la que se crea la clave.

3.2 Certificados

Los certificados son instrucciones firmadas digitalmente que asocian una clave pública a la identidad de la persona o sistema que posee la clave privada correspondiente. Una entidad emisora de certificados de confianza puede emitir los certificados y usarlos para autenticar un gran número de usuarios sin necesidad de mantener una contraseña para cada usuario.

Un certificado suele contener la siguiente información:

- La clave pública del sujeto (la persona o sistema al que se emitió el certificado).
- La información identificativa del sujeto, como el nombre y la dirección de correo electrónico.

- El período de validez (tiempo durante el cual, el certificado se considera válido).
- Información identificadora y firma digital del emisor.

SQL Server admite certificados para la autenticación, autorización y encriptado. También, proporciona la funcionalidad para crear, exportar e importar certificados, como se muestra en el ejemplo de código siguiente:

Crear un nuevo certificado:

```
CREATE CERTIFICATE CERT_DBLDatosSuscriptores  
ENCRYPTION BY PASSWORD = 'DBLe@rnerSecVreCertPa$$w0rd'  
WITH SUBJECT = 'Certificado para cifrar suscriptores',  
EXPIRY_DATE = '31/12/2015'
```

Exportar o respaldar el certificado:

```
BACKUP CERTIFICATE CERT_DBLDatosSuscriptores  
TO FILE = 'D:\SQLBackups\DBLSuscriptoresCERT.cer'
```

Importar un certificado o crearlo desde un respaldo:

```
CREATE CERTIFICATE CERT_DBLConexions  
FROM FILE = 'D:\SQLBackups\CERTConexions.cer'
```

4. Implementando encriptación a nivel de celda


Implementando encriptación a nivel de celda

Pasos para implementar encriptado a nivel de celda

- 1 Crear una llave maestra
- 2 Crear u obtener un certificado, protegido por la llave maestra
- 3 Crear una llave de encriptado de base de datos protegida por el certificado, para un usuario
- 4 Implementar rutinas de encriptado y desencriptado

7 - 19

Copyright © Todos los Derechos Reservados - Cibertec Perú S.A.C.



Los datos de replicación se organizan en artículos y publicaciones. Las publicaciones contienen uno o varios artículos y son las unidades de suscripción y sincronización de los datos. Los suscriptores pueden recibir suscripciones o suscribirse por sí mismos. Los agentes de replicación administran todo el proceso de replicación, incluido el movimiento de los datos entre publicadores y suscriptores.

4.1 Artículos

Un artículo puede ser toda una tabla u objeto de base de datos, o una parte. Se puede filtrar horizontalmente, restringiendo las filas que contiene, o verticalmente, restringiendo las columnas que tiene.

4.2 Publicaciones

Una publicación puede contener uno o varios artículos. Se pueden tener artículos de la misma base de datos, aunque puede haber muchas publicaciones en una base de datos. Es tanto la unidad de suscripción como la unidad de replicación.

4.3 **Suscripciones**

Una suscripción se crea en relación con una publicación; no se puede crear directamente en relación con un artículo.

Se pueden crear suscripciones de inserción o de extracción. Las suscripciones de inserción se crean en el publicador y se pueden crear al mismo tiempo que la publicación en muchos suscriptores. Dado que las suscripciones se crean de manera centralizada, este método es más seguro, pero es necesario que los suscriptores se conecten cuando la replicación tiene lugar.

Las suscripciones de extracción se crean en el suscriptor. En primer lugar, el publicador debe haber habilitado este tipo de suscripciones y haber registrado al suscriptor o bien haber permitido las suscripciones anónimas. Por lo general, este sistema es menos seguro, pero permite al suscriptor controlar cuándo se reciben las actualizaciones, haciéndolo más adecuado para aquellos sitios que se conectan con poca frecuencia.

Puede tener una suscripción de extracción en una publicación y una de inserción en otra.

4.4 **Agente de replicación**

Los agentes de replicación controlan todo el proceso de replicación. Estos agentes se configuran cuando se define la solución de replicación. Al implementar la replicación, debe especificar en qué instancias de SQL Server se ejecutarán los agentes de replicación.

SQL Server proporciona los siguientes agentes de replicación:

- Agente SQL Server
- Agente de instantáneas
- Agente de registro del LOG
- Agente de lectura de cola
- Agente de distribución
- Agente de mezcla

5. Encriptado transparente de datos (TDE)

Encriptado transparente de datos

- Cifrado completo de la base de datos.
- Ejecuta cifrado de entrada y salida (I/O) en tiempo real, tanto en los archivos de datos con los de registro de transacciones.
- Su implementación es transparente a los usuarios y a las aplicaciones.
- Si se mueven los archivos a otra instancia, estos no se pueden adjuntar.
- No se puede restaurar una copia de seguridad en otra instancia.
- Si se desea mover o restaurar en otra instancia, se deben implementar los mismos objetos de seguridad (Certificados y llaves) de la instancia original.

7 - 26

Copyright © Todos los Derechos Reservados - Cibertec Perú S.A.C.



Los distintos sistemas tendrán requisitos diferentes (y con frecuencia, en conflicto los unos con los otros) para la replicación. SQL Server proporciona tres métodos de replicación, aunque cada uno proporciona un conjunto diferente de ventajas y tiene distintas configuraciones opcionales.

Todos los métodos de replicación permiten especificar la frecuencia de sincronización.

5.1 Replicación de instantáneas (Snapshot)

La replicación de instantáneas envía todos los datos de una publicación cada vez que esta se sincroniza. De esta forma se elimina la necesidad de supervisar las modificaciones de datos, aunque podría producir un aumento del volumen de datos que se están replicando. Se replicarán todos los datos aun cuando no se haya modificado ninguno.

Normalmente, la replicación de instantáneas se usa en escenarios en los que una gran cantidad de datos cambia entre cada sincronización. Con la replicación de instantáneas, los suscriptores pueden actualizar los datos en el publicador. La actualización puede ocurrir inmediatamente o ponerse en cola hasta que se produzca la siguiente sincronización.

5.2 **Replicación transaccional**

La replicación transaccional solo envía modificaciones de los datos cuando tiene lugar la sincronización. Esto puede reducir el volumen de los datos que se están replicando, sobre todo si el número de modificaciones de datos es bajo o si la replicación es frecuente.

Debido a la disminución de volúmenes de datos, se puede usar la replicación transaccional cuando sean necesarias, actualizaciones frecuentes.

La replicación transaccional se inicia normalmente con una replicación de instantáneas de los objetos y datos para proporcionar una línea de base.

A continuación, se enviarán partes del registro de transacciones a los suscriptores cuando se produzca la replicación.

Con la replicación transaccional estándar, los suscriptores pueden actualizar datos en el publicador. La actualización puede ocurrir inmediatamente o ponerse en cola hasta que se produzca la siguiente sincronización.

La replicación transaccional punto a punto (PEER-TO-PEER) también está disponible. En este método, cada nodo es a la vez publicador y suscriptor de los mismos datos. No hay ninguna jerarquía de publicadores y suscriptores. Se utiliza este método cuando cada punto trabaja con una parte concreta de los datos. Si todos los puntos realizan cambios en los mismos datos y es posible que se produzcan conflictos, se debería usar la replicación de mezcla.

5.3 **Replicación de mezcla (Merge)**

La replicación de mezcla permite las modificaciones tanto en el publicador como en los suscriptores. Cuando se produce la sincronización, se mezclarán las modificaciones en el publicador y en el suscriptor.

En otras formas de replicación, todas las modificaciones aparecen en el publicador, con lo que se evitan conflictos, pero se reduce la autonomía. En la replicación de mezcla, pueden producirse conflictos y será necesario resolverlos. La solución de conflictos puede ser controlada, automáticamente, dando prioridad a los distintos suscriptores o usando una resolución basada en Modelo de objetos componentes (COM). Puede escribir su propia resolución basada en COM o usar una estándar incluida con SQL Server. Los conflictos también se pueden resolver interactivamente durante la sincronización mediante el componente de resolución interactiva de Microsoft. Este componente está disponible, a través del Administrador de sincronización Windows Server.

La replicación de mezcla se inicia con una replicación de instantáneas de los objetos y datos para proporcionar una línea de base. Las modificaciones subsiguientes se mezclan cuando la replicación tiene lugar.

5.4 Replicación heterogénea

Se pueden replicar los datos de SQL Server en otros productos de bases de datos, como IBM DB2, Oracle y Sybase. SQL Server también puede actuar como suscriptor de la versión 8 o posterior de Oracle. Después podrá generar y mantener la suscripción con un conocimiento mínimo de este programa. Se pueden usar replicación de instantáneas y transaccionales, si se suscribe a una base de datos de Oracle.