CCN
centro criptológico nacional

Guía de Seguridad de las TIC

IMPLEMENTACIÓN DE SEGURIDAD EN MICROSOFT SQL SERVER 2016 SOBRE MICROSOFT WINDOWS SERVER 2016

MAYO 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES

NIPO: 083-19-179-3

Fecha de Edición: mayo de 2019
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

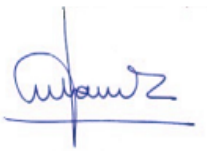
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

mayo de 2019



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. INTRODUCCIÓN

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en los productos y sistemas operativos de Microsoft (CCN STIC 500), siendo de aplicación para la Administración pública en el cumplimiento del Esquema Nacional de Seguridad (ENS) y de obligado cumplimiento para los sistemas que manejen información clasificada nacional.

La serie CCN STIC 500 se ha diseñado de manera incremental. Así, dependiendo del sistema, se aplicarán consecutivamente varias de estas guías. En este sentido se deberán aplicar las guías correspondientes dependiendo del entorno que se esté asegurando.

Por ejemplo, en el caso de un entorno que le sea de aplicación el ENS, para un servidor miembro de un dominio con Microsoft Windows Server 2016, en el que se instale Microsoft Exchange Server 2013, deberán aplicarse las siguientes guías:

a) Guía CCN-STIC-870A en el servidor miembro con Windows Server 2012 R2.

b) Guía CCN-STIC-873 Internet Information Services (IIS) 8.5.

c) Guía CCN-STIC-880 Microsoft Exchange Server 2013 en Windows 2012 R2.

Por ejemplo, en el caso de un entorno de red clasificada, para un servidor con Microsoft Windows Server 2016, en el que se instale Microsoft Exchange Server 2013, deberán aplicarse las siguientes guías:

a) Guía CCN-STIC-560A en el servidor miembro con Windows Server 2012 R2.

b) Guía CCN-STIC-563 Internet Information Services (IIS) 8.5.

c) Guía CCN-STIC-552 Microsoft Exchange Server 2013 en Windows 2012 R2.

Nota: Estas guías están pensadas y diseñadas para entornos de máxima seguridad donde no existirá conexión con redes no seguras como puede ser Internet.

3. OBJETO

El propósito de este documento consiste en proporcionar los procedimientos para la implementación, establecer la configuración y realizar tareas de administración maximizando las condiciones de seguridad del servicio Microsoft SQL Server 2016 en su versión Standard, Enterprise o Datacenter en un servidor miembro de una infraestructura de dominio.

La instalación, así como los procesos de administración, se han diseñado para que la implementación sea lo más restrictiva posible. Es factible que determinadas funcionalidades de Microsoft SQL Server 2016 requieran modificar las configuraciones que se plantean con la presente guía.

Esta guía asume que el servicio de Microsoft SQL Server 2016 se va a implementar sobre dos equipos con Windows Server 2016 y en donde se han seguido los procesos definidos en la guía CCN STIC 570A Anexo B.

4. ALCANCE

La guía se ha elaborado para proporcionar información específica para realizar una implementación de la solución de Microsoft SQL Server 2016 Standard, Enterprise o Datacenter en una configuración restrictiva de seguridad. Se plantean también las posibles operaciones de administración y aquellas acciones que deben ser llevadas a cabo para el adecuado mantenimiento de la solución.

El escenario en el cual está basada la presente guía tiene las siguientes características técnicas:

a) Un único bosque de Directorio Activo.

b) Un único dominio dentro del bosque de Directorio Activo.

c) Nivel funcional del bosque y del domino en Windows Server 2016.

d) Un controlador de dominio basado en Windows Server 2016.

e) Un servidor miembro del dominio basados en Windows Server 2016 Standard.

f) La instalación de SQL Server 2016 se realiza en modo limpio, es decir no se contemplan procedimientos de migración desde versiones anteriores.

g) No se contemplan mecanismos de alta disponibilidad ni balanceo de carga en el escenario planteado.

Este documento incluye:

a) **Mecanismos para la implementación de la solución.** Se incorporan mecanismos para la implementación de la solución de forma automatizada.

b) **Mecanismos para la aplicación de configuraciones**. Se incorporan mecanismos para la implementación de forma automática de las configuraciones de seguridad susceptibles de ello.

c) **Descripción de la seguridad en Microsoft SQL Server 2016.** Completa descripción de los mecanismos de seguridad, autenticación y autorización utilizados en Microsoft SQL Server 2016, así como las medidas para reforzar dicha seguridad.

d) **Guía paso a paso**. Permite implementar y establecer las configuraciones de seguridad necesarias en una arquitectura de un servidor Microsoft SQL Server 2016.

e) **Guía de administración.** Proporciona el método para realizar las tareas de administración más comunes en el entorno de seguridad establecido.

f) **Lista de comprobación.** Ayuda a verificar el grado de cumplimiento de un servidor con respecto a las condiciones de seguridad que se establecen en esta guía.

g) **Consideraciones en implantaciones con firewall.** Se ha creado un anexo específico en donde se detallan las consideraciones y recomendaciones a tener en cuenta cuando se implanta Microsoft SQL Server 2016 en escenarios en donde existen sistemas de control de tráfico entre los servidores SQL Server.

5. DESCRIPCIÓN DEL USO DE ESTA GUIA

Para entender esta guía de seguridad es conveniente explicar el proceso de refuerzo de la seguridad que describe y los recursos que proporciona. Este procedimiento constará de los siguientes pasos:

a) Antes de iniciar la instalación de SQL Server, debe asegurarse que dispone de un servidor controlador de dominio de Directorio Activo basado en Windows Server 2016, implementado de forma segura, habiendo hecho uso de la guía codificada como CCN-STIC-570A Anexo B.

b) Debe haberse configurado un servidor miembro del dominio con Windows Server 2016, siguiendo los pasos indicados en la guía codificada como CCN-STIC-570A Anexo B.

c) Al aplicar el procedimiento de instalación que se indica en esta guía, deberá también tenerse en cuenta que es recomendable que el servidor cuente con al menos dos particiones o volúmenes diferentes. Uno para el sistema operativo y otro para la instalación y el almacenamiento de las bases de datos de Microsoft SQL Server 2016.

5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

Los contenidos de esta guía son de aplicación para servidores con Sistemas Operativos Microsoft Windows Server 2016, en castellano, con el objetivo de reducir la superficie de exposición a ataques posibles con una instalación por defecto, manteniendo los principios de máxima seguridad, mínima exposición y servicios y mínimos privilegios que emanan de la CCN-STIC-301. En el caso de llevar a cabo la aplicación de esta guía sobre el Sistema Operativo con una configuración de idioma diferente al castellano, es posible que deba incorporar nuevos recursos y/o realizar ciertas modificaciones sobre los recursos que se adjuntan con este documento para permitir la correcta aplicación y uso del documento.

La guía ha sido probada y verificada con la versión de SQL Server 2016 sobre el sistema operativo Windows Server 2016 Standard aplicando la guía CCN-STIC 570A Anexo B. No se ha verificado en otros tipos de instalaciones como pudiera ser Windows Server 2016 Datacenter. No obstante, y teniendo en consideración las funcionalidades de ambas versiones de sistema operativo servidor podría llegar a implementarse la siguiente guía sobre la versión Datacenter. No se ha verificado en otros tipos de instalaciones como pudiera ser la de tipo OEM.

Esta guía se ha diseñado para reducir la superficie de exposición de los equipos servidores que cuenten con una implementación de Microsoft SQL Server 2016 en un entorno de dominio de Directorio Activo.

La guía de seguridad ha sido elaborada utilizando un laboratorio basado en una plataforma de virtualización tipo Hyper-V de Windows Server 2016 con las siguientes características técnicas:

a) Servidor Dell PowerEdge™ T320:

   i. Intel Pentium Xeon CPU ES 2430 2.20 GHz.

   ii. HDD 1 TB.

   iii. 64 GB de RAM.

   iv. Interfaz de Red 1 GB.

Esta guía de seguridad no funcionará con hardware que no cumpla con los requisitos de seguridad mínimos de Windows Server 2016. Esto quiere decir que se requieren equipos con procesadores Intel o AMD de 64 bits (x64), con más de 2 GB de memoria RAM.

Así mismo, hay que tener en cuenta que Microsoft SQL Server 2016 requiere, para un entorno de producción, un mínimo de 4 GB de memora RAM, aunque este valor debe aumentar a medida que el tamaño de las bases de datos gestionadas aumente, para asegurar un óptimo rendimiento.

Además, para cumplir con los requisitos establecidos en las guías de seguridad CCN-STIC-500, se debe instalar SQL Server 2016 en un volumen con el formato NTFS o en cualquiera que permita la aplicación de ACL's.

Esta guía ha sido desarrollada con el objetivo de dotar a la infraestructura los máximos niveles de seguridad. Es por ello que, es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y por lo tanto pueda ser necesario aplicar acciones adicionales para habilitar servicios o características deseadas tanto en Microsoft SQL Server 2016 como en Microsoft Windows Server 2016.

Para garantizar la seguridad de los servidores, deberán instalarse las actualizaciones recomendadas por el fabricante, disponibles a través del servicio de Windows Update. Las actualizaciones por lo general se liberan los segundos martes de cada mes, no obstante, hay que tener presente que determinadas actualizaciones por su criticidad pueden ser liberadas en cualquier momento. Se deberá tener en cuenta la implementación de las actualizaciones tanto para el sistema operativo como para los diferentes servicios requeridos, como pueden ser NET Framework 4.7.1 (según actualizaciones).

Dependiendo de la naturaleza de estas actualizaciones, el lector podrá encontrarse con algunas diferencias respecto a lo descrito en esta guía. Esto viene motivado por los cambios que en ocasiones se realizan para las distintas actualizaciones de seguridad.

Antes de aplicar esta guía en producción, deberá asegurarse de haber probado el proceso de instalación en un entorno aislado y controlado donde se han aplicado los test y los cambios en la configuración para que se ajusten a los criterios específicos de cada organización.

El espíritu de estas guías no está dirigido a remplazar políticas consolidadas y probadas de las organizaciones, sino servir como la línea base de seguridad que deberá ser adaptada a las necesidades propias de cada organización.

5.2 ESTRUCTURA DE LA GUÍA

Esta guía dispone de una estructura que diferencia la implementación del sistema Microsoft Windows Server 2016 dependiendo del entorno sobre el que vaya a ser aplicado.

La guía dispone de las siguientes configuraciones divididas en dos grandes anexos, los cuales se definen a continuación:

a) **Anexo A:** En este anexo se define la configuración necesaria para adaptar los sistemas Microsoft Windows Server 2016 en su versión Standard con el rol de Exchange Server 2016 a las necesidades requeridas por el Esquema Nacional de Seguridad (ENS).

b) **Anexo B:** En este anexo se define la configuración necesaria para adaptar los sistemas Microsoft Windows Server 2016 en su versión Standard con el rol de SQL Server 2016 a las necesidades requeridas en los entornos clasificados.

Cabe remarcar que en sus respectivos anexos se dotará de la información necesaria y concreta para cada tipo de implementación.

De manera adicional, en cada una de las carpetas "Scripts" que se adjuntan a los documentos, existe un directorio que almacena un informe en formato HTML con cada objeto de directiva de grupo (GPO) o directiva de grupo local (GPL) que se aplica durante el paso a paso de la guía.

6. EDICIONES Y COMPONENTES DE SQL SERVER 2016

SQL Server 2016 se encuentra solo disponible en versión de 64 bits, la instalación de 32 bits está discontinuada, y a su vez, se compone de las ediciones Business Intelligence, Enterprise, Standard, Express y Developer, aunque, como ya se ha indicado anteriormente, a lo largo de esta guía se hará uso de la edición Enterprise.

Las ediciones Business Intelligence, Enterprise, Standard son las únicas ediciones que permiten la agrupación en clústeres de conmutación por error, estando la edición Standard y Business Intelligence limitada a 2 nodos, mientras que la edición Entrerprise solo se encuentra limitada por el número de nodos del sistema operativo sobre el que se instale.

Internamente, el producto Microsoft SQL Server 2016 consta de varios componentes, como son, SQL Server Database Engine (motor de la base de datos de SQL Server), Analysis Services (servicios de análisis), Reporting Services (servicios de informes), Integration Services (servicios de integración) y Master Data Services (servicios de datos maestros).

SQL Server Database Engine (motor de la base de datos de SQL Server). Constituye el servicio principal para almacenar, procesar y proteger los datos. Además, incluye las funcionalidades de replicación, búsqueda de texto completo y herramientas para administrar datos XML y relacionales, siendo este componente el objeto de implementación de esta guía.

Analysis Services (servicios de análisis). Los servicios de análisis permiten crear y administrar aplicaciones de procesamiento analítico en línea (OLAP) y de minería de datos, formando parte fundamental de las herramientas de inteligencia de negocios de las que puede disponer una organización.

Reporting Services (servicios de informes). Los servicios de informes incluyen componentes de servidor y cliente para crear, administrar e implementar informes tabulares, matriciales, gráficos y de forma libre. Además, es posible extender esta plataforma para desarrollar aplicaciones de informes adaptadas a las necesidades de cualquier organización.

Integration Services (servicios de integración). Los servicios de integración se componen de un conjunto de herramientas gráficas y objetos programables que permiten y facilitan las tareas de mover, copiar y transformar datos entre diferentes orígenes de datos heterogéneos.

Master Data Services (servicios de datos maestros). Los servicios de datos maestros es la solución que se incluye en SQL Server para la administración de datos maestros de organización. MDM o Master Data Management permite a las organizaciones detectar y definir listas no transaccionales de datos con el objetivo de compilar listas maestras que se puedan mantener y cuyo resultado es la existencia de datos confiables y centralizados que se pueden analizar para tomar mejores decisiones corporativas.

7. NOVEDADES MICROSOFT SQL SERVER 2016

Como sucede con todas las versiones nuevas de cada producto de Microsoft, SQL Server 2016 incorpora un conjunto de importantes novedades y mejoras orientadas a proporcionar mejores niveles de rendimiento en entornos de misión crítica, elevar la seguridad de los datos y facilitar las tareas de administración y mantenimiento de toda la solución.

Algunas de estas novedades se pueden resumir en la siguiente lista:

a) Mejoras de características del motor de base de datos.

   i. Se pueden configurar varios archivos de base de datos tempDB durante la instalación y configuración de SQL Server.

   ii. El nuevo Almacén de consultas almacena los textos de las consultas, los planes de ejecución y las métricas de rendimiento dentro de la base de datos, lo que permite supervisar y solucionar los problemas de rendimiento con facilidad. Las consultas que consumen más tiempo, memoria o recursos de CPU se muestran en un panel.

   iii. Mejoras de optimización en las tablas temporales de historial de la base de datos tempdb.

   iv. La nueva compatibilidad de JSON integrada en SQL Server admite importaciones, exportaciones, análisis y almacenamiento de JSON.

   v. El nuevo motor de consultas de PolyBase integra SQL Server con datos externos en Hadoop o Azure Blob Storage. Puede importar y exportar datos, así como ejecutar consultas.

   vi. La nueva característica Stretch Database permite archivar datos de forma dinámica y segura desde una base de datos de SQL Server local a una instancia de Azure SQL Database en la nube. SQL Server consulta automáticamente los datos locales y remotos en las bases de datos vinculadas.

b) Mejoras de OLTP en memoria:

   i. Ahora admite las restricciones FOREIGN KEY, UNIQUE y CHECK, los procedimientos almacenados compilados nativos OR, NOT, SELECT DISTINCT y OUTER JOIN, así como las subconsultas en SELECT.

   ii. Admite tablas de hasta 2 TB (a partir de 256 GB).

   iii. Presenta mejoras del índice de almacenamiento de columnas para la ordenación, así como compatibilidad para el grupo de disponibilidad AlwaysOn.

c) Nuevas características de seguridad:

   i. Always Encrypted: cuando se habilita, solo la aplicación que tiene la clave de cifrado puede acceder a la información confidencial cifrada en la base de datos de SQL Server 2016. La clave nunca se pasa a SQL Server.

   ii. Enmascaramiento dinámico de datos: si se especifica en la definición de tabla, los datos enmascarados están ocultos para la mayoría de los usuarios, por lo que solo aquellos que dispongan del permiso UNMASK pueden ver la información completa.

   iii. Nuevas restricciones de acceso a datos a nivel de fila, columna y tabla para cada usuario.

Nota: Se puede encontrar el detalle técnico de estas y otras novedades en la siguiente dirección Web: https://docs.microsoft.com/es-es/sql/sql-server/what-s-new-in-sql-server-2016?view=sql-server-2016

Hay varias mejoras en los archivos de base de datos TempDB. Las marcas de seguimiento 1117 y 1118 ya no son necesarias para tempdb. Si hay varios archivos de base de datos tempdb, todos crecerán al mismo tiempo en función de la configuración de crecimiento. Además, todas las asignaciones de tempdb usarán extensiones uniformes. De manera predeterminada, la configuración agrega archivos tempdb según el valor que sea más bajo, ya sea 8 o la cantidad de CPU.

Durante la configuración, puede configurar la cantidad de archivos de base de datos tempdb, el tamaño inicial, el crecimiento automático y la colocación de directorio a través del nuevo control de entrada de IU en la sección Configuración del motor de base de datos → TempDB del Asistente para la instalación de SQL Server. El tamaño inicial predeterminado es de 8 MB y el crecimiento automático predeterminado es de 64 MB.

Puede especificar varios volúmenes para los archivos de base de datos tempdb. Si se especifican varios directorios, los archivos de datos tempdb se distribuirán por turnos entre los directorios.

El Almacén de consultas es una característica nueva que ofrece a los administradores de base de datos los conocimientos sobre el rendimiento y la elección del plan de consulta. Esta característica simplifica la solución de problemas de rendimiento al permitirle encontrar rápidamente diferencias de rendimiento provocadas por cambios en los planes de consulta. Captura automáticamente un historial de consultas, planes y estadísticas en tiempo de ejecución, y los conserva para su revisión. Separa los datos por ventanas de tiempo, lo que permite ver patrones de uso la base de datos y comprender cuándo se produjeron cambios del plan de consultas en el servidor. El Almacén de consultas presenta la información mediante un cuadro de diálogo de Management Studio y le permite forzar la consulta a uno de los planes de consultas seleccionados.

Nota: Se requiere como mínimo la versión 16 de Management Studio. No se puede habilitar el almacén de consultas para la base de datos master o tempdb.

SQL Server 2016 ahora es compatible con las tablas temporales con versiones del sistema. Una tabla temporal con versión de sistema es un tipo de tabla nuevo que brinda información correcta sobre los hechos almacenados en cualquier momento determinado. Cada tabla temporal con versión de sistema consta, en realidad, de dos tablas, una para los datos actuales y otra, para los históricos. El sistema garantiza que, cuando cambian los datos de la tabla con los datos actuales, los valores anteriores se almacenan en la tabla de datos históricos. Se proporcionan construcciones de consultas para que los usuarios no sepan de esta complejidad.

SQL Server 2016 agrega compatibilidad integrada para la importación y exportación de JSON y el funcionamiento con cadenas JSON. Esta compatibilidad integrada incluye las siguientes instrucciones y funciones.

a) Para aplicar el formato JSON a los resultados de la consulta, o exportar JSON, agregue la cláusula FOR JSON a una instrucción SELECT. Use la cláusula FOR JSON, por ejemplo, para delegar en SQL Server la aplicación de formato a los resultados de JSON procedentes de aplicaciones cliente.

b) Convertir datos JSON en filas y columnas, o importar JSON, mediante una llamada a la función de proveedor del conjunto de filas OPENJSON. Use OPENJSON para importar datos JSON a SQL Server o convertir datos JSON en filas y columnas para una aplicación o servicio que en este momento no puede usar directamente JSON.

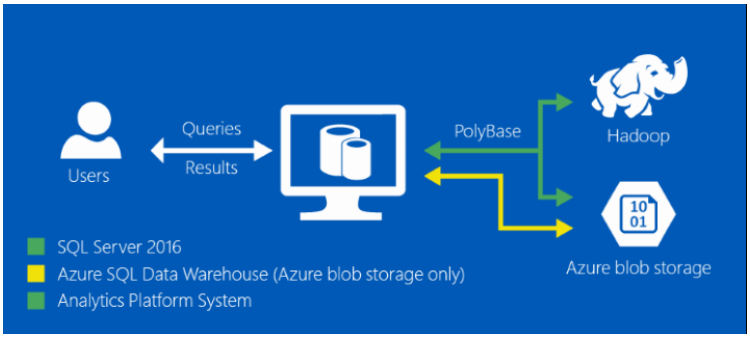
c) La función ISJSON prueba si una cadena contiene un valor JSON válido.

d) La función JSON_VALUE extrae un valor escalar de una cadena JSON.

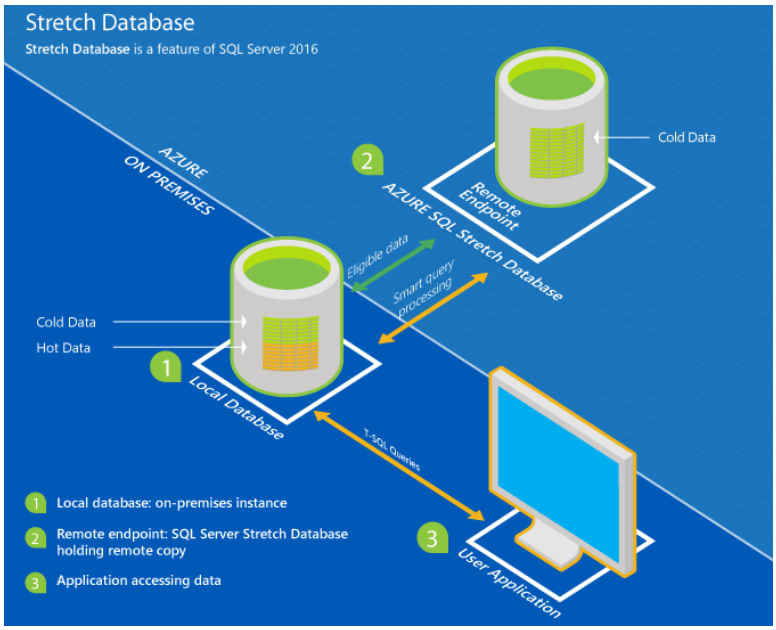
e) La función JSON_QUERY extrae un objeto o una matriz de una cadena JSON.

f) La función JSON_MODIFY actualiza el valor de una propiedad en una cadena JSON y devuelve la cadena JSON actualizada.

g) PolyBase le permite usar instrucciones T-SQL para tener acceso a los datos almacenados en Hadoop o en Almacenamiento de blobs de Azure y consultarlos de manera ad hoc. También le permite consultar datos semiestructurados y combinar los resultados con los conjuntos de datos relacionales almacenados en SQL Server. PolyBase está optimizado para las cargas de trabajo de almacenamiento de datos y está dirigido a los escenarios de consultas de análisis.



Stretch Database es una nueva característica de SQL Server 2016 que migra los datos históricos de forma clara y segura a la nube de Microsoft Azure. Puede tener acceso a los datos de SQL Server sin problemas, independientemente de si están almacenados localmente o extendidos a la nube. Solo tiene que establecer la directiva que defina dónde se almacenan los datos y SQL Server se encargará del movimiento de datos en segundo plano. La tabla entera estará siempre en línea y lista para consultarse. Además, Stretch Database no requiere ningún cambio en las consultas o aplicaciones existentes: la ubicación de los datos es completamente clara para la aplicación.



En SQL Server 2016 se mejora la funcionalidad OLTP en memoria. Hay varios elementos de Transact-SQL que no se admitían para las tablas con optimización para memoria en SQL Server 2014, que ahora se admiten en SQL Server 2016:

a) Se admiten índices y restricciones UNIQUE.

b) Se admiten referencias FOREIGN KEY entre tablas con optimización para memoria.

   i. Estas claves externas solo pueden hacer referencia a una clave principal y no pueden hacer referencia a una clave única.

c) Se admiten las restricciones CHECK.

d) Un índice que no sea único puede permitir valores NULL en su clave.

e) Los desencadenadores se admiten en las tablas con optimización para memoria.

   i. Solo se admiten desencadenadores AFTER. No se admiten desencadenadores INSTEADOF.

   ii. Cualquier desencadenador de una tabla con optimización para memoria debe usar WITH NATIVE_COMPILATION.

f) Compatibilidad total para todas las intercalaciones y páginas de códigos de SQL Server con índices y otros artefactos en tablas con optimización para memoria y módulos T-SQL compilados de forma nativa.

g) Compatibilidad con Modificar tablas con optimización para memoria:

   i. Índices ADD y DROP. Cambiar bucket_count de índices hash.

   ii. Realizar cambios de esquema: agregar, quitar o modificar columnas; agregar o quitar restricción.

h) Una tabla con optimización para memoria ahora puede tener varias columnas cuyas longitudes combinadas son superiores a la longitud de la página de 8060 bytes. Un ejemplo es una tabla con tres columnas de tipo nvarchar(4000). En estos ejemplos, algunas columnas ahora se almacenan de manera no consecutiva. Las consultas ignoran completamente si una columna se encuentra de manera consecutiva o no consecutiva.

i) Tipos de LOB (objeto grande) varbinary(max), nvarchar(max) y varchar(max) ahora se admiten en tablas con optimización para memoria.

A partir de SQL Server 2016 no existe límite en el tamaño de las tablas optimizadas para memoria, aunque estas deben adaptarse a la memoria. El tamaño de una tabla optimizada para memoria corresponde al tamaño de los datos más alguna sobrecarga de los encabezados de fila.

SQL Server 2016 Standard Edition ahora admite los grupos de disponibilidad básica AlwaysOn. Los grupos de disponibilidad básica brindan compatibilidad con una réplica principal y una réplica secundaria. Esta funcionalidad reemplaza la tecnología obsoleta de Creación de reflejo de la base de datos para lograr una alta disponibilidad.

En cuanto a la seguridad, con Always Encrypted, SQL Server puede realizar operaciones sobre datos cifrados, debido a que la clave de cifrado reside con la aplicación dentro del entorno de confianza del cliente y no en el servidor. Always Encrypted protege los datos de cliente para que los administradores de base de datos no tengan acceso a los datos de texto sin formato. El cifrado y descifrado de datos se produce sin problemas en el nivel de controlador, lo que minimiza los cambios que se deben realizar en las aplicaciones existentes.

El enmascaramiento dinámico de datos limita la exposición de información confidencial ocultándolos a los usuarios sin privilegios. El enmascaramiento dinámico de datos evita el acceso no autorizado a información confidencial permitiendo que los clientes designen la cantidad de información confidencial que se debe revelar, con un impacto mínimo en la capa de aplicación. Se trata de una característica de protección de datos que oculta la información confidencial del conjunto de resultados de una consulta de campos designados de una base de datos, sin modificar los datos de esta última.

La seguridad de nivel de fila presenta el control de acceso basado en predicados. Ofrece una evaluación flexible, centralizada y basada en predicados que puede tener en cuenta metadatos (como etiquetas) o cualquier otro criterio que el administrador determine como apropiado. El predicado se usa como un criterio para determinar si el usuario tiene o no el acceso adecuado a los datos según los atributos del usuario. El control de acceso basado en etiquetas se puede implementar con el control de acceso basado en predicados.

8. SEGURIDAD EN SQL SERVER 2016

A partir de la versión SQL Server 2005 se implementaron una serie de cambios significativos con el objetivo de conseguir un servicio SQL Server muchos más seguro que las versiones anteriores. En la versión SQL Server 2016, Microsoft continúa por este camino, implementando una serie de mejoras adicionales en los componentes de servidor y de base de datos.

Estos cambios están orientados a disminuir el área expuesta y la superficie de ataque de SQL Server y sus bases de datos, siguiendo para ello el principio del "mínimo nivel de privilegios" y aumentando la separación entre los administradores de Windows y los administradores de SQL Server.

SQL Server 2016 está desarrollado siguiendo la iniciativa Microsoft Trustworthy Computing, donde los cuatro componentes principales son: seguro por diseño, seguro por defecto, seguro en despliegue y seguro en comunicaciones

8.1 CONFIGURACIÓN DE PERMISOS Y CUENTAS DE SERVICIO

Existen consideraciones de seguridad previas a la instalación de SQL Server, tales como la seguridad física, el uso de firewalls o el uso de un sistema de archivos seguro, que deben ser establecidos siguiendo los criterios y normativas aplicables a su organización.

SQL Server 2016 cuenta con herramientas de instalación que permiten comprobar la configuración del sistema operativo para detectar posibles anomalías.

Además, el instalador activa por defecto únicamente los elementos básicos esenciales, teniendo que añadir manualmente el resto de funciones y características necesarias. De este modo se reduce la superficie de ataque, ya que los sistemas en producción disponen únicamente de los componentes y características necesarias, estando muchas de estas funciones (integración CLR, depuración, service bróker, etc.) instaladas, pero que deben ser activadas en caso de ser necesario.

Una de las tareas más importantes durante la instalación de SQL Server es la configuración de las cuentas de los servicios utilizadas por los diferentes componentes de SQL Server. A continuación, se muestra una tabla con los diferentes servicios que instala SQL Server 2016 y su descripción.

Servicio	Descripción
Servicio de base de datos de SQL Server	Servicio principal del motor de base de datos de SQL Server.
Agente SQL Server	Servicio para la ejecución de trabajos, supervisión de SQL Server, activación de alertas y automatización de algunas tareas administrativas.
SQL Server Browser	Servicio de resolución de nombres que proporciona información de conexión de SQL Server a los equipos cliente.
Búsqueda de texto completo	Servicio que se encarga de crear índices de texto completo del contenido y de las propiedades de los datos estructurados y semiestructurados para permitir el filtrado de documentos y la separación de palabras clave.
Analysis Services	Servicio que proporciona funciones de procesamiento analítico en línea (OLAP) y minería de datos para aplicaciones inteligencia de negocios.
Objeto de escritura de SQL	Este servicio permite que las aplicaciones de copias de seguridad y restauración funcionen en el marco del servicio de instantáneas de volumen (VSS).
Reporting Services	Servicio que permite administrar, ejecutar, crear, programar y enviar informes de negocio.
Integration Services	Servicio que proporciona compatibilidad de administración para el almacenamiento y la ejecución de paquetes de Integration Services.
SQL Server Distributed Replay Controller	Proporciona la orquestación de la reproducción de seguimiento en varios equipos cliente de Distributed Replay.
SQL Server Distributed Replay Client	Simula cargas de trabajo simultáneas en una instancia del motor de base de datos de SQL Server.
SQL Server Trusted Launchpad	Servicio de confianza que hospeda archivos ejecutables externos que proporciona Microsoft, como el runtime de R instalado como parte de R Services (en bases de datos).

Nota: Esta guía tiene como objetivo fundamental la implementación segura del servicio de motor de base de datos, por lo que en el anexo paso a paso no se hará referencia ni se instalarán el resto de servicios descritos en la tabla anterior, salvo aquellos estrictamente necesarios.

Para que los servicios anteriormente indicados puedan iniciarse y ejecutarse, deben tener una cuenta de servicio. Estas cuentas pueden ser de los siguientes tipos: cuentas de usuario de dominio, cuentas de usuario local, cuenta de servicio local, cuenta de servicio de red, cuenta del sistema local, cuenta de servicio administrado y cuenta virtual.

Cuando se seleccionen cuentas de servicio, debe prevalecer el principio de menor nivel de privilegios, así como el aislamiento de las cuentas, es decir, no solo las cuentas deben ser únicas para cada servicio, sino que no se deben utilizar en otros ámbitos dentro del mismo servidor.

Las cuentas virtuales y las cuentas de servicios administrados garantizan este aislamiento que se indica. Además, el aprovisionamiento, la gestión de contraseñas y la configuración de registros SPN se simplifican con este tipo de cuentas.

Una cuenta de servicio administrada es un tipo especial de cuenta de dominio que puede ser signada a un único equipo. El administrador del dominio debe aprovisionar este tipo de cuentas y no pueden ser utilizadas para iniciar sesión en equipos o servidores.

Nota: LaunchPad no puede crear las cuentas que utiliza si instala SQL Server en un equipo que también se utiliza como controlador de dominio.

Además, proporciona una gestión automática de contraseñas y registros SPN.

Por otro lado, las cuentas virtuales son cuentas administradas localmente que se aprovisionan automáticamente.

Las cuentas virtuales pueden acceder la red y habitualmente tienen un nombre conocido, con el formato "NT SERVICE\<NOMBRE_DEL_SERVICIO>". Estas cuentas se introdujeron por primera vez con Windows Server 2008 R2.

El uso de cuentas de dominio tradicionales puede ser también una buena opción si el servidor SQL forma parte de un dominio de Directorio Activo y requiere disponer de acceso a otros recursos del mismo como recursos compartidos o conexiones con servidores vinculados que ejecutan SQL Server.

Si el servidor no forma parte de un dominio o no necesita acceder a recursos del dominio, es preferible hacer uso de cuentas virtuales. Es por ello que, para incrementar el nivel de seguridad en los servicios de SQL Server en esta guía, se hace uso de cuentas virtuales durante el paso a paso de instalación.

A continuación, se muestra una tabla con los tipos de cuentas recomendados para cada servicio y el estado de inicio de cada uno de ellos en una instalación de SQL Server 2016 sobre Windows Server 2016.

Servicio	Tipo de cuenta	Inicio	Estado
Base de datos SQL Server	Cuenta virtual	Automático	Iniciado
Agente SQL Server	Cuenta virtual	Deshabilitado	Detenido
Explorador de SQL Server	Servicio local	Deshabilitado	Detenido
Búsqueda de texto completo	Cuenta virtual	Automático	Iniciado
Analysis Services	Cuenta virtual	Automático	Iniciado
Objeto de escritura de SQL	Sistema local	Manual	Detenido
Reporting Services	Cuenta virtual	Automático	Iniciado
Integration Services	Cuenta virtual	Automático	Iniciado
SQL Server Distributed Replay Controller	Cuenta virtual	Automático	Iniciado
SQL Server Distributed Replay Client	Cuenta virtual	Automático	Iniciado

Nota: No todos los servicios que se muestran en esta tabla van a ser instalados en el paso a paso de instalación de SQL Server de esta guía. Las cuentas virtuales no pueden ser utilizadas para instancias en clúster de SQL Server porque no tendrían el mismo SID en cada nodo del clúster, ni tampoco de admiten como cuentas de servicio en instalaciones sobre Controladores de Dominio.

En caso de hacer uso de cuentas de dominio, se recomienda utilizar una cuenta de dominio diferente para cada servicio, con el mínimo nivel de privilegios, en vez de utilizar una cuenta compartida para todos los servicios.

No es recomendable asignar permisos adicionales a las cuentas de servicio ni a los grupos de servicios de SQL Server. Los permisos se concederán a través de la pertenencia a un grupo o directamente a un SID de servicio si se admite su uso.

Durante el proceso de instalación se crean una serie de grupos de usuarios a los que se conceden una serie de derechos y privilegios. A continuación, se muestra una tabla con esta información.

Servicio	Grupo de usuarios	Permisos concedidos
Motor de base de datos de SQL Server	Todos los derechos se conceden al SID por servicio. Instancia predeterminada: **NT SERVICE\MSSQLSERVER**. Instancia con nombre: **NT SERVICE\MSSQL$**Nombre_de_instancia.	Iniciar sesión como servicio (SeServiceLogonRight) Reemplazar un token de nivel de proceso (SeAssignPrimaryTokenPrivilege) Omitir comprobación de recorrido (SeChangeNotifyPrivilege) Ajustar las cuotas de la memoria para un proceso (SeIncreaseQuotaPrivilege) Permiso para iniciar el objeto de escritura de SQL Permiso para leer el servicio Registro de eventos Permiso para leer el servicio Llamada a procedimiento remoto
Agente de SQL Server	Todos los derechos se conceden al SID por servicio. Instancia predeterminada: **NT Service\SQLSERVERAGENT**. Instancia con nombre: **NT Service\SQLAGENT$***Nombre_de_instancia*.	Iniciar sesión como servicio (SeServiceLogonRight) Reemplazar un token de nivel de proceso (SeAssignPrimaryTokenPrivilege) Omitir comprobación de recorrido (SeChangeNotifyPrivilege) Ajustar las cuotas de la memoria para un proceso (SeIncreaseQuotaPrivilege)
SSAS	Todos los derechos se conceden a un grupo local de Windows. Instancia predeterminada: **SQLServerMSASUser$***Nombre_de_equipo***$MSSQLSERVER**. Instancia con nombre: **SQLServerMSASUser$***Nombre_de_equipo***$***Nombre_de_instancia*. PowerPivot para SharePoint: **SQLServerMSASUser$***Nombre_de_equipo***$***PowerPivot*	Iniciar sesión como servicio (SeServiceLogonRight) Solo para modo tabular: Aumentar el espacio de trabajo de un proceso (SeIncreaseWorkingSetPrivilege) Ajustar las cuotas de la memoria para un proceso (SeIncreaseQuotaSizePrivilege) Bloquear páginas en la memoria (SeLockMemoryPrivilege): solo es necesario cuando la paginación está completamente desactivada. Solo para la instalación de clústeres de conmutación por error: Aumentar prioridad de programación (SeIncreaseBasePriorityPrivilege)

Servicio	Grupo de usuarios	Permisos concedidos
SSRS	Todos los derechos se conceden al SID por servicio. Instancia predeterminada: **NT SERVICE\ReportServer**. Instancia con nombre: **NT SERVICE\$***Nombre_de_instancia*	Iniciar sesión como servicio (SeServiceLogonRight)
SSIS	Todos los derechos se conceden al SID por servicio. Instancia predeterminada e instancia con nombre: **NT SERVICE\MsDtsServer130**. Integration Services no tiene un proceso independiente para una instancia con nombre	Iniciar sesión como servicio (SeServiceLogonRight Permiso para escribir en el registro de eventos de la aplicación Omitir comprobación de recorrido (SeChangeNotifyPrivilege) Suplantar a un cliente tras la autenticación (SeImpersonatePrivilege)
Búsqueda de texto completo	Todos los derechos se conceden al SID por servicio Instancia predeterminada: **NT Service\MSSQLFDLauncher**. Instancia con nombre: **NT Service\ MSSQLFDLauncher$***Nombre_de_ instancia*	Iniciar sesión como servicio (SeServiceLogonRight) Ajustar las cuotas de la memoria para un proceso (SeIncreaseQuotaPrivilege) Omitir comprobación de recorrido (SeChangeNotifyPrivilege)
SQL Server Browser	Todos los derechos se conceden a un grupo local de Windows. Instancia predeterminada o con nombre: **SQLServer2005SQLBrowserUser$***Nombre_de_equipo*. SQL Server Browser no tiene un proceso independiente para una instancia con nombre).	Iniciar sesión como servicio (SeServiceLogonRight)
SQL Server Objeto de escritura de VSS	Todos los derechos se conceden al SID por servicio. Instancia predeterminada o con nombre: **NT Service\SQLWriter**. SQL Server VSS Writer no tiene un proceso independiente para una instancia con nombre).	El servicio SQLWriter se ejecuta en la cuenta de sistema local que tiene todos los permisos necesarios. SQL Server no comprueba ni concede permisos para este servicio.
SQL Server Controlador de reproducción distribuida		Iniciar sesión como servicio (SeServiceLogonRight)
SQL Server Distributed Replay Client		Iniciar sesión como servicio (SeServiceLogonRight)
Launchpad		Iniciar sesión como servicio (SeServiceLogonRight) Reemplazar un token de nivel de proceso (SeAssignPrimaryTokenPrivilege) Omitir comprobación de recorrido (SeChangeNotifyPrivilege) Ajustar las cuotas de la memoria para un proceso (SeIncreaseQuotaPrivilege)

Servicio	Grupo de usuarios	Permisos concedidos
Motor de PolyBase y DMS		Iniciar sesión como servicio (SeServiceLogonRight)
R Services: SQLRUser Group		Permitir el inicio de sesión local

Nota: La tabla mostrada anteriormente puede variar en función de las características de SQL Server 2016 instaladas en el servidor.

Las cuentas de servicio de SQL Server deben tener acceso a los recursos. Las listas de control de acceso se establecen para el SID por servicio o el grupo local de Windows, dependiendo del tipo de instalación y el servicio.

A continuación, se muestran las entradas de listas de control de acceso (ACL´s) establecidas durante el proceso de instalación.

Servicio	Recurso	Acceso
MSSQLServer	Instid\MSSQL\backup	Control total
	Instid\MSSQL\binn	Lectura, Ejecución
	Instid\MSSQL\data	Control total
	Instid\MSSQL\FTData	Control total
	Instid\MSSQL\Install	Lectura, Ejecución
	Instid\MSSQL\Log	Control total
	Instid\MSSQL\Repldata	Control total
	130\shared	Lectura, Ejecución
	Instid\MSSQL\Template Data (solo SQL Server Express)	Lectura
SQLServerAgent	Instid\MSSQL\binn	Control total
	Instid\MSSQL\binn	Control total
	Instid\MSSQL\Log	Lectura, Escritura, Eliminación, Ejecución
	130\com	Lectura, Ejecución
	130\shared	Lectura, Ejecución
	130\shared\Errordumps	Lectura, Escritura
	ServerName\EventLog	Control total
FTS	Instid\MSSQL\FTData	Control total
	Instid\MSSQL\FTRef	Lectura, Ejecución
	120\shared	Lectura, Ejecución
	120\shared\Errordumps	Lectura, Escritura
	Instid\MSSQL\Install	Lectura, Ejecución
	Instid\MSSQL\jobs	Lectura, Escritura
MSSQLServer OLAPservice	130\shared\ASConfig	Control total
	Instid\OLAP	Lectura, Ejecución
	Instid\Olap\Data	Control total
	Instid\Olap\Log	Lectura, Escritura
	Instid\OLAP\Backup	Lectura, Escritura
	Instid\OLAP\Temp	Lectura, Escritura
	130\shared\Errordumps	Lectura, Escritura

Servicio	Recurso	Acceso
SQLServerReportServerUser	Instid\Reporting Services\Log Files	Lectura, Escritura, Eliminación
	Instid\Reporting Services\ReportServer	Lectura, Ejecución
	Instid\Reportingservices\Reportserver\global.asax	Control total
	Instid\Reportingservices\Reportserver\Reportserver. config	Lectura
	Instid\Reporting Services\reportManager	Lectura, Ejecución
	Instid\Reporting Services\RSTempfiles	Lectura, Escritura, Ejecución, Eliminación
	130\shared	Lectura, Ejecución
	130\shared\Errordumps	Lectura, Escritura
MSDTSServer100	130\dts\binn\MsDtsSrvr.ini.xml	Lectura
	130\dts\binn	Lectura, Ejecución
	130\shared	Lectura, Ejecución
	130\shared\Errordumps	Lectura, Escritura
SQL Server Browser	130\shared\ASConfig	Lectura
	130\shared	Lectura, Ejecución
	130\shared\Errordumps	Lectura, Escritura
SQLWriter	N/D (Se ejecuta como sistema local)	N/A
Usuario	Instid\MSSQL\binn	Lectura, Ejecución
	Instid\Reporting Services\ReportServer	Lectura, Ejecución, Mostrar el contenido de la carpeta
	Instid\Reportingservices\Reportserver\global.asax	Lectura
	Instid\Reporting Services\ReportManager	Lectura, Ejecución
	Instid\Reporting Services\ReportManager\pages	Lectura
	Instid\Reporting Services\ReportManager\Styles	Lectura
	130\dts	Lectura, Ejecución
	130\tools	Lectura, Ejecución
	100\tools	Lectura, Ejecución
	90\tools	Lectura, Ejecución
	80\tools	Lectura, Ejecución
	130\sdk	Lectura
	Microsoft SQL Server\130\Setup Bootstrap	Lectura, Ejecución
SQL Server Distributed Replay Controller	<ToolsDir>\DReplayController\Log\ (directorio vacío)	Lectura, Ejecución, Mostrar el contenido de la carpeta
	<ToolsDir>\DReplayController\ DReplayController.exe	Lectura, Ejecución, Mostrar el contenido de la carpeta
	<ToolsDir>\DReplayController\resources\	Lectura, Ejecución, Mostrar el contenido de la carpeta
	<ToolsDir>\DReplayController\{Todas las DLL}	Lectura, Ejecución, Mostrar el contenido de la carpeta
	<ToolsDir>\DReplayController\ DReplayController.config	Lectura, Ejecución, Mostrar el contenido de la carpeta
	<ToolsDir>\DReplayController\ IRTemplate.tdf	Lectura, Ejecución, Mostrar el contenido de la carpeta
	<ToolsDir>\DReplayController\ IRDefinition.xml	Lectura, Ejecución, Mostrar el contenido de la carpeta

Servicio	Recurso	Acceso
SQL Server Distributed Replay Client	<ToolsDir>\DReplayClient\Log\	Lectura, Ejecución, Mostrar el contenido de la carpeta
	<ToolsDir>\DReplayClient\ DReplayClient.exe	Lectura, Ejecución, Mostrar el contenido de la carpeta
	<ToolsDir>\DReplayClient\resources\	Lectura, Ejecución, Mostrar el contenido de la carpeta
	<ToolsDir>\DReplayClient\ (Todas las DLL)	Lectura, Ejecución, Mostrar el contenido de la carpeta
	<ToolsDir>\DReplayClient\ DReplayClient.config	Lectura, Ejecución, Mostrar el contenido de la carpeta
	<ToolsDir>\DReplayClient\IRTemplate.tdf	Lectura, Ejecución, Mostrar el contenido de la carpeta
	<ToolsDir>\DReplayClient\IRDefinition.xml	Lectura, Ejecución, Mostrar el contenido de la carpeta

Nota: La tabla mostrada anteriormente puede variar en función de las características de SQL Server 2016 instaladas en el servidor.

Además, durante el proceso de instalación se conceden algunos permisos de control de acceso a cuentas integradas o a otras cuentas del servicio de SQL Server. En la siguiente tabla se muestra esta información.

Cuenta	Recurso	Permisos concedidos
MSSQLServer	Usuarios del registro de rendimiento	Instid\MSSQL\binn
	Usuarios del monitor de sistema	Instid\MSSQL\binn
	Usuarios del registro de rendimiento, Usuarios del monitor de rendimiento	\WINNT\system32\sqlctr130.dll
	Solo el administrador	\\.\root\Microsoft\SqlServer\ServerEvents\<nombre_instancia_sql>1
	Administradores, sistema	\tools\binn\schemas\sqlserver\2004\07\showplan
	Usuarios	\tools\binn\schemas\sqlserver\2004\07\showplan
Reporting Services	<Cuenta de servicio web del servidor de informes>	<*install*>\Reporting Services\LogFiles
	Identidad del grupo de aplicaciones del Administrador de informes, cuenta ASP.NET, Todos	<*install*>\Reporting Services\ReportManager, <*install*>\Reporting Services\ReportManager\Pages*.*, <*install*>\Reporting Services\ReportManager\Styles*.*, <*install*>\Reporting Services\ReportManager\webctrl_client\1_0*.*
	Identidad del grupo de aplicaciones del Administrador de informes	<*install*>\Reporting Services\ReportManager\Pages*.*
	<Cuenta de servicio web del servidor de informes>	<*install*>\Reporting Services\ReportServer
	<Cuenta de servicio web del servidor de informes>	<*install*>\Reporting Services\ ReportServer\global.asax

Cuenta	Recurso	Permisos concedidos
Reporting Services	Todos	<*install*>\Reporting Services\ ReportServer\global.asax
	Servicio de red	<*install*>\Reporting Services\ ReportServer\ReportService.asmx
	Todos	<*install*>\Reporting Services\ReportServer\ ReportService.asmx
	Cuenta de servicios de Windows ReportServer	<*install*>\Reporting Services\ReportServer\ RSReportServer.config
	Todos	Claves del Servidor de informes (subárbol Instid)
	Usuario de Terminal Services	Claves del Servidor de informes (subárbol Instid)
	Usuarios avanzados	Claves del Servidor de informes (subárbol Instid)

Cuando se instala una unidad local que no es la predeterminada, el SID por servicio debe tener acceso a la ubicación del archivo. SQL Server proporcionará el acceso necesario.

Por último, para que los servicios de SQL Server puedan proporcionar algunas funcionalidades adicionales, es necesario tener permisos adicionales. A continuación, se muestra una tabla con estos permisos.

Servicio/Aplicación	Funcionalidad	Permisos necesarios
SQL Server	Escribir en un buzón de correo mediante xp_sendmail.	Permisos de escritura de la red.
SQL Server	Ejecutar xp_cmdshell para un usuario que no sea administrador de SQL Server.	Actuar como parte del sistema operativo y reemplazar un token de nivel de proceso.
Agente SQL Server	Usar la característica de reinicio automático.	Miembro del grupo local administradores.
Asistente para la optimización de Motor de base de datos	Optimiza las bases de datos para un rendimiento óptimo de las consultas.	Al utilizarla por primera vez, un usuario que tenga credenciales administrativas debe inicializar la aplicación. Después de la inicialización, los usuarios de dbo pueden usar el Asistente para la optimización del Motor de base de datos para optimizar solo aquellas tablas de las que son propietarios.

Para configurar adecuadamente todas las instancias de SQL Server disponibles en una organización, SQL Server 2016 cuenta con una tecnología de gestión basada en políticas.

Gracias a la gestión basada en políticas, es posible configurar toda una serie de aspectos de seguridad y propiedades del servicio según los criterios y necesidades de cada organización. Se puede definir una política de seguridad para controlar el estado de uno o varios servidores SQL Server 2016.

Es posible utilizar Windows Update para aplicar automáticamente los parches y reducir las amenazas causadas por vulnerabilidades conocidas, siendo muy recomendable, mantener actualizados los servidores de la organización.

En SQL Server 2016 se mejora la separación de roles, no se aprovisionan automáticamente el grupo "BUILTIN\administrators" ni el sistema local (NT AUTHORITY\SYSTEM) en el rol fijo de servidor "sysadmin", aunque los administradores locales todavía pueden tener acceso al motor de base de datos en modo de usuario único.

Con SQL Server 2016 es posible definir un esquema predeterminado para un grupo de Windows. Cuando un usuario de Windows crea un objeto y no se ha especificado un esquema predeterminado, SQL Server ya no crea automáticamente un esquema.

8.2 PROTECCIÓN DE ARCHIVOS

Una instancia de SQL Server, ya sea predeterminada o con nombre, tiene su propio conjunto de archivos de programa y datos, así como un conjunto de archivos comunes compartidos entre todas las instancias de SQL Server. Los archivos comunes que usan todas las instancias se instalan en la carpeta "<unidad>:\Archivos de programa\Microsoft SQL Server\130". Siendo la ruta de instalación de SQL Server configurable durante el propio proceso de instalación.

Para aislar las ubicaciones de instalación de cada componente, se generan identificadores de instancia únicos. En el caso del componente de motor de base de datos se genera el identificador con el formato MSSQL, seguido del número de versión principal y un punto, y a continuación el nombre de instancia. Así, por ejemplo, para la instancia predeterminada de SQL Server 2016 se generaría el identificador MSSQL13.MSSQLSERVER.

Durante el proceso de instalación de la característica de motor de base de datos se define la ruta de instalación (generada por defecto a partir de los identificadores de instancia), la cual se utilizará como directorio raíz de todas las carpetas específicas de la instancia de dicha instalación. De este modo los directorios de datos de una instancia SQL Server serían los siguientes:

Directorio	Directorio predeterminado
Raíz de datos	C:\Archivos de programa\Microsoft SQL Server\
Base de datos de usuario	C:\Archivos de programa\Microsoft SQL Server\ MSSQL13<Instancia>\Data
Registro de base de datos de usuario	C:\Archivos de programa\Microsoft SQL Server\ MSSQL13<Instancia>\Data
Base de datos temporales	C:\Archivos de programa\Microsoft SQL Server\ MSSQL13<Instancia>\Data
Registro de base de datos temporales	C:\Archivos de programa\Microsoft SQL Server\ MSSQL13<Instancia>\Data
Copia de seguridad	C:\Archivos de programa\Microsoft SQL Server\ MSSQL13<Instancia>\Backup

Durante el proceso de instalación de una instancia de motor de base de datos de SQL Server 2016 se configuran las ACL´s para todos los directorios, anulándose la herencia como parte de la configuración.

Es necesario asegurarse que los directorios implicados tengan el espacio suficiente, y establecer los permisos apropiados en el directorio de copia de seguridad para evitar la pérdida de datos.

8.3 CONFIGURACIÓN DE RED

SQL Server 2016 permite el acceso a los datos a través de los "endpoints" o extremos. Un endpoint consiste en un servicio que permanece a la escucha con el objetivo de atender las peticiones de los clientes o aplicaciones.

Se pueden otorgar, revocar y denegar permisos para endpoints de Transact-SQL. De manera predeterminada, todos los usuarios tienen permisos para obtener acceso a un endpoint, a menos que los permisos sean denegados o revocados por un miembro del grupo sysadmin o por el propietario del endpoint.

Los tipos de endpoints vienen determinados por el tipo de peticiones que van a recibir, los tipos disponibles en SQL Server 2016 son:

a) Database mirroring

b) SOAP.

c) Service Broker.

d) Transact-SQL.

Los endpoints de SQL Server 2016 admiten los siguientes protocolos:

a) HTTP.

b) TCP/IP.

c) Canalizaciones con nombre (NAMED_PIPES).

d) Memoria compartida (SHARED_MEMORY).

e) Adaptador de interfaz virtual (VIA).

A continuación, se muestra una tabla que relaciona los tipos de endpoints con los protocolos soportados:

Tipo de endpoint	HTTP	TCP	NAMED PIPES	SHARED MEMORY	VIA
Database mirroring		X			
SOAP	X				
Service Broker		X			
TDS/TSQL		X	X	X	X

Nota: Database mirroring se encuentra descontinuada en SQL Server 2016.

El extremo TDS o TSQL es el objeto que representa el punto de comunicación entre SQL Server y un cliente. Esta comunicación se puede realizar a través de los protocolos TCP/IP, canalizaciones con nombre, memoria compartida y adaptador de interfaz virtual.

Es importante señalar que en una instalación de clúster de conmutación por error solo se admiten los protocolos TCP/IP y canalizaciones con nombre. En una instalación por defecto de SQL Server 2016 Enterprise únicamente se encuentran activos los protocolos TCP/IP y memoria compartida, siendo el protocolo TCP/IP el utilizado habitualmente para la comunicación a través de la red.

A continuación, se indica el posible uso de los otros tres protocolos:

a) Memoria compartida. Este protocolo solo se puede utilizar en una conexión local, donde el servidor y el cliente residen en la misma máquina.

b) Canalizaciones con nombre. Similar al protocolo TCP/IP pero donde se soporta la comunicación entre los servidores de una red de área local (LAN). Este protocolo debe utilizarse solo en aplicaciones específicas que impliquen implementaciones en red en un único dominio de seguridad donde no se encuentren expuestos a tráfico externo.

c) Adaptador de interfaz virtual. Protocolo que depende de la implementación de los fabricantes y que se suele utilizar para conexiones de alto rendimiento entre dos servidores.

Por defecto, la instancia predeterminada del motor de base de datos SQL Server 2016 escucha en el puerto TCP 1433 cuando se utilizan los protocolos de conexión TCP/IP o VIA.

Las instancias con nombre utilizan puertos dinámicos, siendo el servicio explorador de SQL Server quien ayuda a los clientes a identificar el puerto cuando se conectan a la instancia con nombre.

Si se utiliza el protocolo de canalizaciones con nombre, la instancia predeterminada del motor de base de datos SQL Server escucha en la canalización con nombre \\.\pipe\sql\query, mientras que las instancias con nombre escuchan en \\.\pipe\MSSQL$<nombreDeInstancia>\sql\query. Nuevamente, será el servicio explorador de SQL Server quien ayude a los clientes a identificar la canalización cuando se conecten.

Cuando se utiliza el protocolo TCP/IP es necesario configurar el firewall para permitir el acceso al puerto TCP donde escucha la instancia SQL Server (1433 en una configuración por defecto), ya que SQL Server no lo hace durante el proceso de instalación.

Esta guía contempla la utilización del puerto TCP 1433 como puerto de comunicaciones de la instancia predeterminada de SQL Server, por lo que no tiene que realizar ninguna acción adicional para habilitar este puerto.

Si se utilizan instancias con nombre y puertos dinámicos, será necesario tener en ejecución el servicio de explorador de SQL Server y abierto el puerto UDP 1434.

Nota: Para lograr un entorno más seguro se recomienda detener el explorador de SQL Server, configurar las instancias con nombre en un puerto TCP fijo, y habilitar el firewall para el acceso a ese puerto. Los clientes deberán especificar en su conexión el puerto TCP utilizado.

Sin embargo, desactivar el explorador de SQL Server también puede tener consecuencias no deseadas, ya que esto implica actualizar y mantener el código de las aplicaciones clientes para asegurarse de que se conectan al puerto apropiado.

Además, es posible que otro servicio o aplicación del servidor llegue a utilizar el puerto elegido para cada instancia, haciendo que la instancia de SQL Server no esté disponible.

Si es necesario mantener el explorador de SQL Server en ejecución, es posible ocultar instancias que no se quieran mostrar en la red. Utilizando la bandera "HideInstance" es posible indicar al explorador de SQL Server que no debe responder con información acerca de determinadas instancias, manteniendo éstas ocultas a su descubrimiento por parte de aplicaciones clientes.

Cuando SQL Server 2016 se configura para escuchar peticiones a través del protocolo de canalizaciones con nombre, SQL Server utiliza el puerto TCP 445 para las comunicaciones. Por ello se debe configurar el firewall para mantener abierto dicho puerto.

SQL Server 2016 también admite el cifrado de las comunicaciones a través de SSL (Capa de sockets seguros) y es compatible con IPSec (Protocolo de seguridad de Internet). El cifrado se realiza en la capa del protocolo y permite el cifrado de los datos transmitidos a través de una red entre una instancia SQL Server y una aplicación.

Para habilitar el cifrado es necesario que la instancia utilice un certificado asignado al equipo servidor y que el cliente confíe en la entidad emisora del mismo. Se recomienda que el nivel de cifrado SSL sea de 128 bits.

Al habilitar el cifrado SSL se aumenta la seguridad de los datos que se transmiten a través de redes entre instancias de SQL Server y aplicaciones. Cuando se cifra mediante SSL todo el tráfico entre SQL Server y una aplicación cliente es necesario realizar el siguiente proceso adicional:

a) Se requiere un ciclo adicional de ida y vuelta de red en el momento de la conexión.

b) La biblioteca de red del cliente es la encargada de cifrar los paquetes enviados desde la aplicación a la instancia de SQL Server y la biblioteca de red del servidor se encargará posteriormente de descifrarlos.

c) La biblioteca de red del servidor es la encargada de cifrar los paquetes enviados desde la instancia de SQL Server a la aplicación; la biblioteca de red del cliente se encargará posteriormente de descifrarlos.

Cuando se hace uso del cifrado de las sesiones en el servidor, se requiere que la API de cliente también soporte el mismo nivel de cifrado. Las implementaciones de Microsoft de OLE DB, ODBC, JDBC 1.2 y ADO.NET soportan sesiones cifradas.

Como ya es sabido, el protocolo SSL 3.0 y TLS 1.0, así como sus versiones anteriores han sido declarados inseguros debido a las vulnerabilidades encontradas. Es por ello que se recomienda habilitar el cifrado de las comunicaciones en SQL Server haciendo uso de TLS 1.2.

Todas las versiones de SQL Server 2016 son compatibles para el uso del protocolo TLS 1.2.

Nota: Se dispone de información más detallada sobre las versiones y las descargas de actualizaciones necesarias para dar soporte a TLS 1.2 en la siguiente página Web de Microsoft TechNet: https://support.microsoft.com/es-es/kb/3135244

8.4 AUTENTICACIÓN

Como en ediciones anteriores, SQL Server 2016 admite dos modos de autenticación de usuarios sobre el motor de base de datos: modo de autenticación de Windows y modo mixto. El modo de autenticación de Windows habilita la autenticación a través de una cuenta de usuario de Windows y deshabilita la autenticación de SQL Server. El modo mixto habilita tanto la autenticación de Windows como la de SQL Server. El modo de autenticación de Windows no se puede deshabilitar.

SQL Server 2016 incluye mejoras sobre los inicios de sesión SQL Server (basados en usuario y contraseña), donde, de forma automática y predeterminada, se admite el cifrado de las comunicaciones a través de la utilización de certificados generados por SQL Server. De este modo, aun cuando los administradores no hayan desplegado certificados de confianza, las comunicaciones se realizan de forma cifrada.

Además de esto, SQL Server 2016 mejora los procesos de autenticación en un segundo aspecto, ya que, por defecto, el motor utiliza las directivas de grupo de Windows para la complejidad de contraseñas, caducidad de contraseña y bloqueos de cuentas sobre los inicios de sesión SQL.

De este modo, la aplicación de políticas de contraseñas está integrada en el servidor, validándose éstas durante la autenticación, establecimiento y reseteo de contraseñas. Las directivas de complejidad de contraseñas son las siguientes:

a) La contraseña no debe contener parte o todo el nombre de la cuenta del usuario.

b) La contraseña debe tener una longitud de ocho caracteres como mínimo.

c) La contraseña debe contener caracteres de tres de las siguientes categorías:

   i. Letras en mayúsculas del alfabeto latín (de la "A" a la "Z").

   ii. Letras en minúsculas del alfabeto latín (de la "a" a la "z").

   iii. Dígitos en base 10 (del 0 al 9).

   iv. Caracteres no alfanuméricos, como el signo de admiración (¡), de moneda ($), almohadilla (#) o porcentaje (%).

La complejidad de contraseñas se aplica no solo a la autenticación de usuarios SQL Server, sino a todas las contraseñas, incluyendo el inicio de sesión del usuario SA, los roles de aplicación, las claves maestras de cifrado y las claves de cifrado simétrico.

8.4.1 SOPORTE DE PROTECCIÓN AMPLIADA

SQL Server 2016 admite la protección ampliada para la autenticación de conexiones de clientes. Esta es una característica de los componentes de red que implementan los sistemas operativos desde Windows 7 y Windows Server 2008 R2, y que se extiende a los sistemas operativos anteriores a través de los correspondientes Service Pack.

Para poder usar la protección ampliada, tanto el servidor como el cliente deben tener un sistema operativo en el que se admita y se encuentre habilitada la protección ampliada.

La protección ampliada para la autenticación tiene como objetivo el de proteger la retransmisión de credenciales de autenticación entre diferentes sistemas y servicios, evitando, por ejemplo, que un atacante pueda reutilizar las credenciales de un cliente que ha realizado una autenticación NTLM sobre el explorador de Windows o el Outlook para conectarse a la instancia del servicio de motor de base de datos.

La protección ampliada usa el enlace de servicio y el enlace de canal para ayudar a evitar un ataque de retransmisión de autenticación. En un ataque de retransmisión de autenticación, un cliente que puede realizar la autenticación NTLM se conecta a un atacante. Posteriormente, el atacante utiliza las credenciales del cliente para hacerse pasar por éste y autenticarse en un servicio diferente, como una instancia de motor de base de datos.

Existen fundamentalmente dos variaciones de este ataque:

a) En un ataque por señuelo, el cliente es atraído para conectarse voluntariamente con el atacante.

b) En un ataque de suplantación, el cliente pretende conectarse a un servicio válido, pero no es consciente de que el registro DNS o el enrutamiento IP, o ambos, se han alterado para redirigir la conexión al atacante en su lugar.

En este sentido, SQL Server admite el enlace de servicio y el enlace de canal para ayudar a reducir estos ataques en sesiones de SQL Server:

a) Enlace de servicio. El enlace de servicio soluciona los ataques por señuelo exigiendo que un cliente envíe un nombre principal de servicio (SPN) firmado del servicio de SQL Server al que el cliente pretende conectarse. Como parte de la respuesta de la autenticación, el servicio valida que el SPN recibido en el paquete coincida con su propio SPN. Si un cliente es atraído para conectarse a un atacante, el cliente incluirá el SPN firmado del atacante. El atacante no puede retransmitir el paquete para autenticar al servicio de SQL Server real como el cliente, porque incluiría el SPN del atacante. El enlace de servicio incurre en un costo insignificante una sola vez, pero no soluciona los ataques de suplantación. El enlace de servicio se produce cuando una aplicación cliente no usa el cifrado para conectarse a SQL Server.

b) Enlace de canal. El enlace de canal establece un canal seguro (Schannel) entre un cliente y una instancia del servicio SQL Server. El servicio comprueba la autenticidad del cliente comparando el token de enlace de canal (CBT) del cliente específico de ese canal, con su propio CBT. El enlace de canal trata tanto los ataques de suplantación como los de atracción. Sin embargo, incurre en un costo de tiempo de ejecución mayor, porque requiere cifrado de seguridad de la capa de transporte (TLS) de todo el tráfico de la sesión. El enlace de canal se produce cuando una aplicación cliente usa el cifrado para conectarse a SQL Server, independientemente de si el cifrado lo fuerza el cliente o el servidor.

Nota: SQL Server y Microsoft de SQL Server soporta TLS 1.0 y SSL 3.0. Si se fuerza un protocolo diferente (por ejemplo, TLS 1.1 o TLS 1.2) realizando cambios en la capa Schannel del sistema operativo, las conexiones a SQL Server podrían no funcionar adecuadamente. Se recomienda probar este tipo de modificaciones en un entorno de preproducción o laboratorio antes de pasarlos a producción.

Hay tres opciones de configuración de la conexión de SQL Server que afectan al enlace de servicio y al enlace de canal. Dichas opciones se pueden configurar utilizando el administrador de configuración de SQL Server o WMI, y se pueden visualizar mediante la opción de configuración del protocolo del servidor de la administración basada en directivas.

a) Forzar el cifrado. Los valores posibles son "Activado" y "Desactivado". Para usar el enlace de canal, forzar cifrado debe estar establecido en "Activado" y todos los clientes se verán obligados a realizar el cifrado. Si está desactivado, solo se puede garantizar el enlace de servicio.

b) Protección ampliada. Los valores posibles son "Desactivado", "Permitido" y "Requerido".

   i. Cuando se establece en "Desactivado", la protección ampliada se deshabilita y la instancia de SQL Server aceptará todas las conexiones de cualquier cliente independientemente de que esté o no protegido. Esta configuración es compatible con los sistemas operativos sin revisiones y anteriores, pero es menos segura. Se pude utilizar este valor cuando se sepa con certeza que los sistemas operativos clientes no admiten la protección ampliada.

   ii. Cuando se establece en "Permitido", la protección ampliada se requiere para las conexiones de los sistemas operativos que admiten la protección ampliada. Por el contrario, se omite para las conexiones de los sistemas operativos que no admiten la protección ampliada. Se rechazan las conexiones de las aplicaciones cliente no protegidas que se estén ejecutando en sistemas operativos clientes protegidos. Esta configuración es más segura que "Desactivado", pero no es la más segura. Se puede utilizar esta configuración en entornos mixtos, donde no todos los sistemas operativos admitan protección ampliada.

   iii. Cuando se establece en "Requerido", solo se aceptan las conexiones de las aplicaciones protegidas en sistemas operativos protegidos. Esta configuración es la más segura y restrictiva, pero los sistemas operativos o las aplicaciones que no admitan la protección ampliada no podrán conectarse a SQL Server.

c) Se aceptan SPN NTLM. Cuando un servidor se conoce por más de un SPN, se necesita la variable "Se aceptan SPN NTLM". De esta forma, cuando un cliente intenta conectarse al servidor utilizando un SPN válido que el servidor no conoce, el enlace de servicio dará un error. Para evitar este problema, los usuarios pueden especificar varios SPN que representan al servidor utilizando "Se aceptan SPN NTLM". Estos son una serie de SPN separados por punto y coma.

Nota: Debido a que la protección extendida puede ser incompatible con clientes que no hayan sido debidamente actualizados o aplicaciones de terceros que no soporte esta funcionalidad, en esta guía no se habilita de forma predeterminada. Sin embargo, se recomienda analizar en su infraestructura si las aplicaciones cliente o los sistemas operativos cliente pueden hacer uso de esta característica de seguridad y habilitarla en dicho caso. Se puede obtener más información en los siguientes enlaces de TechNet: https://docs.microsoft.com/es-es/sql/database-engine/configure-windows/connect-to-the-database-engine-using-extended-protection?view=sql-server-2017&viewFallbackFrom=sql-server-2016%20y%20https%3A%2F%2Fsupport.microsoft.com%2Fes-es%2Fhelp%2F968389

8.5 AUTORIZACIÓN Y PROTECCIÓN DE DATOS

Con Microsoft SQL Server 2016 es posible administrar roles de servidor definidos por el usuario.

Uno de los grandes beneficios de SQL Server, es la posibilidad de aplicar permisos de una forma granular sin necesidad de asignar un usuario a un rol de servidor que posiblemente le otorgue más permisos de los que realmente necesita.

Por motivos de compatibilidad con versiones anteriores y por comodidad, se siguen manteniendo los roles a nivel de servidor, los cuales agrupan a otras entidades de seguridad.

Se recomienda, sin embargo, asignar permisos más concretos siempre que sea posible. Los roles a nivel de servidor y sus capacidades son los siguientes:

Rol a nivel de servidor	Descripción
SYSADMIN	Los miembros del rol sysadmin pueden realizar cualquier actividad en el servidor.
SERVERADMIN	Los miembros de este rol pueden cambiar las opciones de configuración en el servidor y cerrar el servidor.
SECURITYADMIN	Los miembros de este rol administran los inicios de sesión y sus propiedades, pueden restablecer las contraseñas de los inicios de sesión de SQL Server y administran los permisos GRANT, DENY y REVOKE del servidor y base de datos.
PROCESSADMIN	Los miembros de este rol pueden finalizar los procesos que se ejecutan en una instancia.
SETUPADMIN	Los miembros de este rol pueden agregar y quitar los servidores vinculados.
BULKADMIN	Los miembros de este rol pueden ejecutar instrucciones BULK INSERT.
DISKADMIN	Permite a los miembros de este grupo administrar los archivos de disco.
DBCREATOR	Los miembros de este grupo pueden crear, modificar, quitar y restaurar cualquier base de datos en el servidor.
PUBLIC	Todos los inicios de sesión pertenecen al rol public. Cuando a un elemento de servidor no se le ha concedido ni denegado ningún permiso específico para el inicio se sesión, éste hereda los permisos concedidos al rol public sobre ese objeto.

SQL Server 2016 también cuenta con roles a nivel de base de datos, los cuales permiten administrar con mayor facilidad los permisos en una base de datos.

A diferencia de los roles a nivel de servidor, donde no se pueden crear nuevos roles, a nivel de base de datos es posible crear nuevos roles, los denominados roles flexibles de base de datos.

Los roles y capacidades a nivel de base de datos predefinidos en SQL Server 2016 son los siguientes:

Rol a nivel de servidor	Descripción
DB_OWNER	Los miembros de este rol pueden realizar todas las actividades de configuración y mantenimiento en la base de datos, incluyendo quitar la base de datos.
DB_SECURITYADMIN	Los miembros de este rol pueden modificar la pertenencia a roles y administrar permisos.
DB_ACCESSADMIN	Los miembros de este rol pueden agregar o quitar el acceso a la base de datos para los inicios de sesión.
DB_BACKUPOPERATOR	Los miembros de este rol pueden crear copias de seguridad de la base de datos.
DB_DDLADMIN	Los miembros de este rol pueden ejecutar cualquier comando del lenguaje de definición de datos (DDL) en la base de datos.
DB_DATAWRITER	Los miembros de este rol pueden agregar, eliminar o cambiar datos en todas las tablas de usuario.
DB_DATAREADER	Los miembros de este rol pueden leer todos los datos de las tablas de usuario.
DB_DENYDATAWRITER	Los miembros de este rol no pueden agregar, modificar, ni eliminar datos de tablas de usuario de la base de datos.
DB_DENYDATAREADER	Los miembros de este rol no pueden leer datos de las tablas de usuario de una base de datos.
PUBLIC	Todos los usuarios de la base de datos pertenecen al rol public. Cuando a un usuario no se le ha concedido ni denegado permisos específicos para un objeto, el usuario hereda los permisos concedidos al rol public para ese objeto.

Por último, además de los roles a nivel de servidor y base de datos, SQL Server 2016 soporta los roles a nivel de aplicación, que permiten que una aplicación en concreto se ejecute con sus propios permisos de usuario.

No existen roles de aplicación predefinidos y están inactivos de forma predeterminada. Cuando una aplicación se conecta a SQL Server lo hace con un usuario. Una vez conectado y haciendo uso del procedimiento almacenado sp_setapprole, se habilita la función de aplicación de modo que a partir de ese momento la conexión pierde los permisos de usuario y asume los permisos del rol de aplicación.

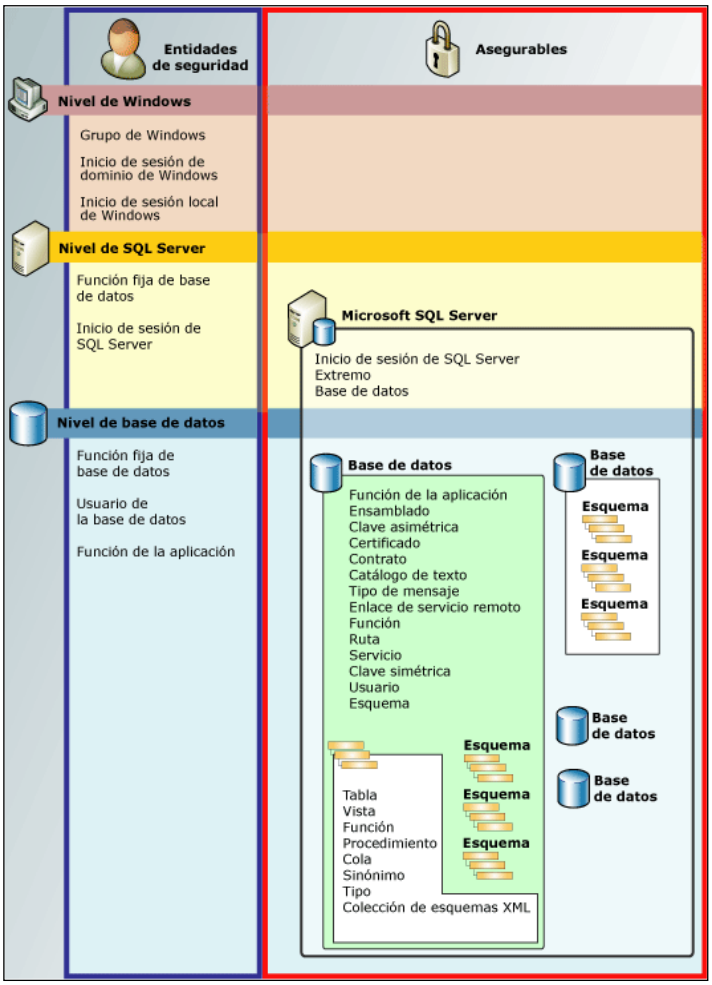
Los roles de aplicación no pueden tener acceso a los metadatos de nivel de servidor porque no están asociadas a una entidad de seguridad a nivel de servidor.

En SQL Server 2016, un "principal" o entidad de seguridad es cualquier individuo, grupo o proceso que puede solicitar acceso a un recurso protegido y se le pueden conceder permisos para acceder al mismo.

Para lograr el principio de menor privilegio, se utiliza el rol "public", al que pertenecen todos los principales de SQL Server y del que heredan todos los permisos sobre un objeto, si no se han concedido o denegado permisos específicos. A partir de aquí, si un principal necesita realizar más tareas se pueden ir asignando los permisos necesarios.

La otra parte de la autorización lo componen los "securables" o elementos protegibles, que son los objetos que se pueden proteger a través de la concesión o denegación de permisos, incluyéndose aquí prácticamente todos los objetos que se pueden crear, incluyendo los creados dentro de un esquema.

Los objetos "principal" de SQL Server 2016 se definen en tres niveles diferentes: a nivel de Windows, a nivel SQL Server y a nivel de base de datos, mientras que los objetos "securables" se definen a nivel de servidor, de base de datos y de esquema, tal y como se muestra en la siguiente imagen sobre jerarquía de permisos.



Nota: Esta imagen de jerarquía de permisos está disponible en Microsoft Docs. Sin embargo, para obtener un mayor nivel de detalle, se recomienda descargar el gráfico completo con todos los permisos del motor de base de datos en formato PDF desde la siguiente URL: https://aka.ms/sql-permissions-poster

Existen una gran cantidad de permisos que pueden ser asignados o denegados a un "securable" para un "principal". Estos permisos son asignados mediante los comandos GRANT, DENY o REVOKE, teniendo en cuenta las nuevas opciones de permiso, como el ámbito de aplicación o si el principal puede conceder el permiso a otros principales.

Los tipos de permisos disponibles en SQL Server son:

Tipo de permiso	Descripción
CONTROL	Concede al *principal* todos los permisos definidos en el *securable*, incluyendo todos los *securables* que abarca dicho ámbito. Se incluyen permisos para conceder estos permisos a otros *principales*. De este modo, por ejemplo, CONTROL SERVER sería equivalente a pertenecer al rol de servidor sysadmin.
ALTER	Confiere los permisos necesarios para cambiar las propiedades de un *securable* y todos los del ámbito, salvo la propiedad de los mismos. Así, por ejemplo, el permiso ALTER sobre una base de datos incluye los permisos necesarios para crear, modificar y eliminar objetos del esquema.
ALTER ANY <securable>	Concede permisos para cambiar cualquier *securable* del tipo especificado. Por ejemplo, ALTER ANY LOGIN permite al *principal* modificar cualquier login del servidor.
TAKE OWNERSHIP	Permite al receptor del permiso tomar propiedad del elemento protegible para el que se concede este permiso.
IMPERSONATE <User>	Permite al principal receptor del permiso suplantar al usuario.
CREATE <securable>	Concede el permiso para crear el *securable*. Dependiendo de si el *securable* es a nivel de servidor, base de datos o esquema, será necesario contar con el permiso ALTER necesario.
VIEW DEFINITION	Concede el permiso para acceder a los metadatos.
REFERENCES	Concede permisos para crear un FOREIGN KEY en una tabla especificada, y la posibilidad de crear funciones y vistas con la cláusula WITH SCHEMABINDING que hace referencia a ese *securable*.

No todos los permisos pueden asignarse a todas las entidades protegibles. La siguiente tabla muestra una relación de los permisos y los objetos a los que se puede aplicar.

Permiso	Securables a los que aplica
SELECT	Sinónimos, Tablas y columnas, Funciones con valores de tabla, Transact-SQL y Common Language Runtime (CLR), Vistas y columnas
VIEW CHANGE TRACKING	Tablas, Esquemas
UPDATE	Sinónimos, Tablas y columnas, Vistas y columnas, Objetos de secuencia
REFERENCES	Funciones escalares y de agregado (Transact-SQL y CLR), Colas de Service Broker, Tablas y columnas, Funciones con valores de tabla (Transact-SQL y CLR), y columnas, Tipos, Vistas y columnas, Objetos de secuencia
INSERT	Sinónimos, Tablas y columnas, Vistas y columnas
DELETE	Sinónimos, Tablas y columnas, Vistas y columnas
EXECUTE	Procedimientos (Transact-SQL y CLR), Funciones escalares y de agregado (Transact-SQL y CLR), Sinónimos, Tipos CLR
RECEIVE	Colas de Service Broker
VIEW DEFINITION	Grupos de disponibilidad, Procedimientos (Transact-SQL y CLR), Colas de Service Broker, Funciones escalares y de agregado (Transact-SQL y CLR), Sinónimos, Inicios de sesión, usuarios y roles, Sinónimos, Tablas, Funciones con valores de tabla (Transact-SQL y CLR), Vistas, Objetos de secuencia
ALTER	Procedimientos (Transact-SQL y CLR), Funciones escalares y de agregado (Transact-SQL y CLR), Colas de Service Broker, Tablas, Funciones con valores de tabla (Transact-SQL y CLR), Vistas

Permiso	Securables a los que aplica
TAKE OWNERSHIP	Grupos de disponibilidad, Roles, Procedimientos (Transact-SQL y CLR), Funciones escalares y de agregado (Transact-SQL y CLR), Roles del servidor, Sinónimos, Tablas, Funciones con valores de tabla (Transact-SQL y CLR), Vistas, Objetos de secuencia
CONTROL	Grupos de disponibilidad, Procedimientos (Transact-SQL y CLR), Funciones escalares y de agregado (Transact-SQL y CLR), Inicios de sesión, usuarios y toles, Colas de Service Broker, Sinónimos, Tablas, Funciones con valores de tabla (Transact-SQL y CLR), Vistas, Objetos de secuencia
IMPERSONATE	Inicios de sesión y usuarios

Nota: Los permisos predeterminados que se conceden a objetos del sistema en el momento de la instalación se evalúan detenidamente frente a posibles amenazas y no necesitan modificarse como parte de la protección de la instalación de SQL Server. Los cambios a los permisos de los objetos del sistema podrían limitar o interrumpir la funcionalidad y dejar potencialmente la instalación de SQL Server en un estado no admitido.

La siguiente tabla muestra una lista completa de los permisos de SQL Server a nivel de servidor, base de datos y esquema, entre otros. Los permisos de base de datos solo están disponibles para los elementos protegibles de base que se admiten. No se pueden conceder permisos de nivel de servidor en base de datos, sin embargo, en algunos casos los permisos de base de datos están disponibles en su lugar.

Elemento protegible base	Permisos granulares del elemento protegible base	Código del tipo de permiso	Elemento protegible que contiene un elemento protegible base	Permiso para el elemento protegible contenedor que implica permiso granular para el elemento protegible base
APPLICATION ROLE	ALTER	AL	DATABASE	ALTER ANY APPLICATION ROLE
	CONTROL	CL	DATABASE	CONTROL
	VIEW DEFINITION	VW	DATABASE	VIEW DEFINITION
ASSEMBLY	ALTER	AL	DATABASE	ALTER ANY ASSEMBLY
	CONTROL	CL	DATABASE	CONTROL
	REFERENCES	RF	DATABASE	REFERENCES
	TAKE OWNERSHIP	TO	DATABASE	CONTROL
	VIEW DEFINITION	VW	DATABASE	VIEW DEFINITION
ASYMMETRIC KEY	ALTER	AL	DATABASE	ALTER ANY ASYMMETRIC KEY
	CONTROL	CL	DATABASE	CONTROL
	REFERENCES	RF	DATABASE	REFERENCES
	TAKE OWNERSHIP	TO	DATABASE	CONTROL
	VIEW DEFINITION	VW	DATABASE	VIEW DEFINITION
AVAILABILITY GROUP	ALTER	AL	SERVER	ALTER ANY AVAILABILITY GROUP
	CONTROL	CL	SERVER	CONTROL SERVER
	TAKE OWNERSHIP	TO	SERVER	CONTROL SERVER
	VIEW DEFINITION	VW	SERVER	VIEW ANY DEFINITION

Elemento protegible base	Permisos granulares del elemento protegible base	Código del tipo de permiso	Elemento protegible que contiene un elemento protegible base	Permiso para el elemento protegible contenedor que implica permiso granular para el elemento protegible base
CERTIFICATE	ALTER	AL	DATABASE	ALTER ANY CERTIFICATE
	CONTROL	CL	DATABASE	CONTROL
	REFERENCES	RF	DATABASE	REFERENCES
	TAKE OWNERSHIP	TO	DATABASE	CONTROL
	VIEW DEFINITION	VW	DATABASE	VIEW DEFINITION
CONTRACT	ALTER	AL	DATABASE	ALTER ANY CONTRACT
	CONTROL	CL	DATABASE	CONTROL
	REFERENCES	RF	DATABASE	REFERENCES
	TAKE OWNERSHIP	TO	DATABASE	CONTROL
	VIEW DEFINITION	VW	DATABASE	VIEW DEFINITION
DATABASE	ALTER	AL	SERVER	ALTER ANY DATABASE
	ALTER ANY APPLICATION ROLE	ALAR	SERVER	CONTROL SERVER
	ALTER ANY ASSEMBLY	ALAS	SERVER	CONTROL SERVER
	ALTER ANY ASYMMETRIC KEY	ALAK	SERVER	CONTROL SERVER
	ALTER ANY CERTIFICATE	ALCF	SERVER	CONTROL SERVER
	ALTER ANY CONTRACT	ALSC	SERVER	CONTROL SERVER
	ALTER ANY DATABASE AUDIT	ALDA	SERVER	ALTER ANY SERVER AUDIT
	ALTER ANY DATABASE DDL TRIGGER	ALTG	SERVER	CONTROL SERVER
	ALTER ANY DATABASE EVENT NOTIFICATION	ALED	SERVER	ALTER ANY EVENT NOTIFICATION
	ALTER ANY DATABASE EVENT SESSION	AADS (solo se aplica a Base de datos SQL).	SERVER	ALTER ANY EVENT SESSION
	ALTER ANY DATASPACE	ALDS	SERVER	CONTROL SERVER
	ALTER ANY FULLTEXT CATALOG	ALFT	SERVER	CONTROL SERVER
	ALTER ANY MESSAGE TYPE	ALMT	SERVER	CONTROL SERVER
	ALTER ANY REMOTE SERVICE BINDING	ALSB	SERVER	CONTROL SERVER
	ALTER ANY ROLE	ALRL	SERVER	CONTROL SERVER
	ALTER ANY ROUTE	ALRT	SERVER	CONTROL SERVER

Elemento protegible base	Permisos granulares del elemento protegible base	Código del tipo de permiso	Elemento protegible que contiene un elemento protegible base	Permiso para el elemento protegible contenedor que implica permiso granular para el elemento protegible base
DATABASE	ALTER ANY SCHEMA	ALSM	SERVER	CONTROL SERVER
	ALTER ANY SECURITY POLICY	ALSP (solo se aplica a Base de datos SQL).	SERVER	CONTROL SERVER
	ALTER ANY SERVICE	ALSV	SERVER	CONTROL SERVER
	ALTER ANY SYMMETRIC KEY	ALSK	SERVER	CONTROL SERVER
	ALTER ANY USER	ALUS	SERVER	CONTROL SERVER
	AUTHENTICATE	AUTH	SERVER	AUTHENTICATE SERVER
	BACKUP DATABASE	BADB	SERVER	CONTROL SERVER
	BACKUP LOG	BALO	SERVER	CONTROL SERVER
	CHECKPOINT	CP	SERVER	CONTROL SERVER
	CONNECT	CO	SERVER	CONTROL SERVER
	CONNECT REPLICATION	CORP	SERVER	CONTROL SERVER
	CONTROL	CL	SERVER	CONTROL SERVER
	CREATE AGGREGATE	CRAG	SERVER	CONTROL SERVER
	CREATE ASSEMBLY	CRAS	SERVER	CONTROL SERVER
	CREATE ASYMMETRIC KEY	CRAK	SERVER	CONTROL SERVER
	CREATE CERTIFICATE	CRCF	SERVER	CONTROL SERVER
	CREATE CONTRACT	CRSC	SERVER	CONTROL SERVER
	CREATE DATABASE	CRDB	SERVER	CREATE ANY DATABASE
	CREATE DATABASE DDL EVENT NOTIFICATION	CRED	SERVER	CREATE DDL EVENT NOTIFICATION
	CREATE DEFAULT	CRDF	SERVER	CONTROL SERVER
	CREATE FULLTEXT CATALOG	CRFT	SERVER	CONTROL SERVER
	CREATE FUNCTION	CRFN	SERVER	CONTROL SERVER
	CREATE MESSAGE TYPE	CRMT	SERVER	CONTROL SERVER
	CREATE PROCEDURE	CRPR	SERVER	CONTROL SERVER
	CREATE QUEUE	CRQU	SERVER	CONTROL SERVER

Elemento protegible base	Permisos granulares del elemento protegible base	Código del tipo de permiso	Elemento protegible que contiene un elemento protegible base	Permiso para el elemento protegible contenedor que implica permiso granular para el elemento protegible base
DATABASE	CREATE REMOTE SERVICE BINDING	CRSB	SERVER	CONTROL SERVER
	CREATE ROLE	CRRL	SERVER	CONTROL SERVER
	CREATE ROUTE	CRRT	SERVER	CONTROL SERVER
	CREATE RULE	CRRU	SERVER	CONTROL SERVER
	CREATE SCHEMA	CRSM	SERVER	CONTROL SERVER
	CREATE SERVICE	CRSV	SERVER	CONTROL SERVER
	CREATE SYMMETRIC KEY	CRSK	SERVER	CONTROL SERVER
	CREATE SYNONYM	CRSN	SERVER	CONTROL SERVER
	CREATE TABLE	CRTB	SERVER	CONTROL SERVER
	CREATE TYPE	CRTY	SERVER	CONTROL SERVER
	CREATE VIEW	CRVW	SERVER	CONTROL SERVER
	CREATE XML SCHEMA COLLECTION	CRXS	SERVER	CONTROL SERVER
	DELETE	DL	SERVER	CONTROL SERVER
	EXECUTE	EX	SERVER	CONTROL SERVER
	INSERT	IN	SERVER	CONTROL SERVER
	KILL DATABASE CONNECTION	KIDC (solo se aplica a Base de datos SQL. Utilice ALTER ANY CONNECTION en SQL Server).	SERVER	ALTER ANY CONNECTION
	REFERENCES	RF	SERVER	CONTROL SERVER
	SELECT	SL	SERVER	CONTROL SERVER
	SHOWPLAN	SPLN	SERVER	ALTER TRACE
	SUBSCRIBE QUERY NOTIFICATIONS	SUQN	SERVER	CONTROL SERVER
	TAKE OWNERSHIP	TO	SERVER	CONTROL SERVER
	UPDATE	UP	SERVER	CONTROL SERVER
	VIEW DATABASE STATE	VWDS	SERVER	VIEW SERVER STATE
	VIEW DEFINITION	VW	SERVER	VIEW ANY DEFINITION
ENDPOINT	ALTER	AL	SERVER	ALTER ANY ENDPOINT
	CONNECT	CO	SERVER	CONTROL SERVER
	CONTROL	CL	SERVER	CONTROL SERVER
	TAKE OWNERSHIP	TO	SERVER	CONTROL SERVER
	VIEW DEFINITION	VW	SERVER	VIEW ANY DEFINITION

Elemento protegible base	Permisos granulares del elemento protegible base	Código del tipo de permiso	Elemento protegible que contiene un elemento protegible base	Permiso para el elemento protegible contenedor que implica permiso granular para el elemento protegible base
FULLTEXT CATALOG	ALTER	AL	DATABASE	ALTER ANY FULLTEXT CATALOG
	CONTROL	CL	DATABASE	CONTROL
	REFERENCES	RF	DATABASE	REFERENCES
	TAKE OWNERSHIP	TO	DATABASE	CONTROL
	VIEW DEFINITION	VW	DATABASE	VIEW DEFINITION
FULLTEXT STOPLIST	ALTER	AL	DATABASE	ALTER ANY FULLTEXT CATALOG
	CONTROL	CL	DATABASE	CONTROL
	REFERENCES	RF	DATABASE	REFERENCES
	TAKE OWNERSHIP	TO	DATABASE	CONTROL
	VIEW DEFINITION	VW	DATABASE	VIEW DEFINITION
LOGIN	ALTER	AL	SERVER	ALTER ANY LOGIN
	CONTROL	CL	SERVER	CONTROL SERVER
	IMPERSONATE	IM	SERVER	CONTROL SERVER
	VIEW DEFINITION	VW	SERVER	VIEW ANY DEFINITION
MESSAGE TYPE	ALTER	AL	DATABASE	ALTER ANY MESSAGE TYPE
	CONTROL	CL	DATABASE	CONTROL
	REFERENCES	RF	DATABASE	REFERENCES
	TAKE OWNERSHIP	TO	DATABASE	CONTROL
	VIEW DEFINITION	VW	DATABASE	VIEW DEFINITION
OBJECT	ALTER	AL	SCHEMA	ALTER
	CONTROL	CL	SCHEMA	CONTROL
	DELETE	DL	SCHEMA	DELETE
	EXECUTE	EX	SCHEMA	EXECUTE
	INSERT	IN	SCHEMA	INSERT
	RECEIVE	RC	SCHEMA	CONTROL
	REFERENCES	RF	SCHEMA	REFERENCES
	SELECT	SL	SCHEMA	SELECT
	TAKE OWNERSHIP	TO	SCHEMA	CONTROL
	UPDATE	UP	SCHEMA	UPDATE
	VIEW CHANGE TRACKING	VWCT	SCHEMA	VIEW CHANGE TRACKING
	VIEW DEFINITION	VW	SCHEMA	VIEW DEFINITION
REMOTE SERVICE BINDING	ALTER	AL	DATABASE	ALTER ANY REMOTE SERVICE BINDING
	CONTROL	CL	DATABASE	CONTROL
	TAKE OWNERSHIP	TO	DATABASE	CONTROL
	VIEW DEFINITION	VW	DATABASE	VIEW DEFINITION
ROLE	ALTER	AL	DATABASE	ALTER ANY ROLE
	CONTROL	CL	DATABASE	CONTROL
	TAKE OWNERSHIP	TO	DATABASE	CONTROL
	VIEW DEFINITION	VW	DATABASE	VIEW DEFINITION

Elemento protegible base	Permisos granulares del elemento protegible base	Código del tipo de permiso	Elemento protegible que contiene un elemento protegible base	Permiso para el elemento protegible contenedor que implica permiso granular para el elemento protegible base
ROUTE	ALTER	AL	DATABASE	ALTER ANY ROUTE
	CONTROL	CL	DATABASE	CONTROL
	TAKE OWNERSHIP	TO	DATABASE	CONTROL
	VIEW DEFINITION	VW	DATABASE	VIEW DEFINITION
SEARCH PROPERTY LIST	ALTER	AL	SERVER	ALTER ANY FULLTEXT CATALOG
	CONTROL	CL	SERVER	CONTROL
	REFERENCES	RF	SERVER	REFERENCES
	TAKE OWNERSHIP	TO	SERVER	CONTROL
	VIEW DEFINITION	VW	SERVER	VIEW DEFINITION
SCHEMA	ALTER	AL	DATABASE	ALTER ANY SCHEMA
	CONTROL	CL	DATABASE	CONTROL
	CREATE SEQUENCE	CRSO	DATABASE	CONTROL
	DELETE	DL	DATABASE	DELETE
	EXECUTE	EX	DATABASE	EXECUTE
	INSERT	IN	DATABASE	INSERT
	REFERENCES	RF	DATABASE	REFERENCES
	SELECT	SL	DATABASE	SELECT
	TAKE OWNERSHIP	TO	DATABASE	CONTROL
	UPDATE	UP	DATABASE	UPDATE
	VIEW CHANGE TRACKING	VWCT	DATABASE	VIEW CHANGE TRACKING
	VIEW DEFINITION	VW	DATABASE	VIEW DEFINITION
SERVER	ADMINISTER BULK OPERATIONS	ADBO	No aplicable	No aplicable
	ALTER ANY CONNECTION	ALCO	No aplicable	No aplicable
	ALTER ANY CREDENTIAL	ALCD	No aplicable	No aplicable
	ALTER ANY DATABASE	ALDB	No aplicable	No aplicable
	ALTER ANY ENDPOINT	ALHE	No aplicable	No aplicable
	ALTER ANY EVENT NOTIFICATION	ALES	No aplicable	No aplicable
	ALTER ANY EVENT SESSION	AAES	No aplicable	No aplicable
	ALTER ANY LINKED SERVER	ALLS	No aplicable	No aplicable
	ALTER ANY LOGIN	ALLG	No aplicable	No aplicable
	ALTER ANY SERVER AUDIT	ALAA	No aplicable	No aplicable
	ALTER ANY SERVER ROLE	ALSR	No aplicable	No aplicable

Elemento protegible base	Permisos granulares del elemento protegible base	Código del tipo de permiso	Elemento protegible que contiene un elemento protegible base	Permiso para el elemento protegible contenedor que implica permiso granular para el elemento protegible base
SERVER	ALTER AVAILABILITY GROUP	ALAG	No aplicable	No aplicable
	ALTER RESOURCES	ALRS	No aplicable	No aplicable
	ALTER SERVER STATE	ALSS	No aplicable	No aplicable
	ALTER SETTINGS	ALST	No aplicable	No aplicable
	ALTER TRACE	ALTR	No aplicable	No aplicable
	AUTHENTICATE SERVER	AUTH	No aplicable	No aplicable
	CONNECT ANY DATABASE	CADB	No aplicable	No aplicable
	CONNECT SQL	COSQ	No aplicable	No aplicable
	CONTROL SERVER	CL	No aplicable	No aplicable
	CREATE ANY DATABASE	CRDB	No aplicable	No aplicable
	CREATE AVAILABILTITY GROUP	CRAC	No aplicable	No aplicable
	CREATE DDL EVENT NOTIFICATION	CRDE	No aplicable	No aplicable
	CREATE ENDPOINT	CRHE	No aplicable	No aplicable
	CREATE SERVER ROLE	CRSR	No aplicable	No aplicable
	CREATE TRACE EVENT NOTIFICATION	CRTE	No aplicable	No aplicable
	EXTERNAL ACCESS ASSEMBLY	XA	No aplicable	No aplicable
	IMPERSONATE ANY LOGIN	IAL	No aplicable	No aplicable
	SELECT ALL USER SECURABLES	SUS	No aplicable	No aplicable
	SHUTDOWN	SHDN	No aplicable	No aplicable
	UNSAFE ASSEMBLY	XU	No aplicable	No aplicable
	VIEW ANY DATABASE	VWDB	No aplicable	No aplicable
	VIEW ANY DEFINITION	VWAD	No aplicable	No aplicable
	VIEW SERVER STATE	VWSS	No aplicable	No aplicable

Elemento protegible base	Permisos granulares del elemento protegible base	Código del tipo de permiso	Elemento protegible que contiene un elemento protegible base	Permiso para el elemento protegible contenedor que implica permiso granular para el elemento protegible base
SERVER ROLE	ALTER	AL	SERVER	ALTER ANY SERVER ROLE
	CONTROL	CL	SERVER	CONTROL SERVER
	TAKE OWNERSHIP	TO	SERVER	CONTROL SERVER
	VIEW DEFINITION	VW	SERVER	VIEW ANY DEFINITION
SERVICE	ALTER	AL	DATABASE	ALTER ANY SERVICE
	CONTROL	CL	DATABASE	CONTROL
	ENVIAR	SN	DATABASE	CONTROL
	TAKE OWNERSHIP	TO	DATABASE	CONTROL
	VIEW DEFINITION	VW	DATABASE	VIEW DEFINITION
SYMMETRIC KEY	ALTER	AL	DATABASE	ALTER ANY SYMMETRIC KEY
	CONTROL	CL	DATABASE	CONTROL
	REFERENCES	RF	DATABASE	REFERENCES
	TAKE OWNERSHIP	TO	DATABASE	CONTROL
	VIEW DEFINITION	VW	DATABASE	VIEW DEFINITION
TYPE	CONTROL	CL	SCHEMA	CONTROL
	EXECUTE	EX	SCHEMA	EXECUTE
	REFERENCES	RF	SCHEMA	REFERENCES
	TAKE OWNERSHIP	TO	SCHEMA	CONTROL
	VIEW DEFINITION	VW	SCHEMA	VIEW DEFINITION
USER	ALTER	AL	DATABASE	ALTER ANY USER
	CONTROL	CL	DATABASE	CONTROL
	IMPERSONATE	IM	DATABASE	CONTROL
	VIEW DEFINITION	VW	DATABASE	VIEW DEFINITION
XML SCHEMA COLLECTION	ALTER	AL	SCHEMA	ALTER
	CONTROL	CL	SCHEMA	CONTROL
	EXECUTE	EX	SCHEMA	EXECUTE
	REFERENCES	RF	SCHEMA	REFERENCES
	TAKE OWNERSHIP	TO	SCHEMA	CONTROL
	VIEW DEFINITION	VW	SCHEMA	VIEW DEFINITION

La comprobación de los permisos puede llegar a ser un proceso complejo. Es por ello que el algoritmo de comprobación de permisos incluye la superposición de la pertenencia a grupos y el encadenamiento de propiedad, tanto el permiso explícito como el implícito, y puede ser afectado por los permisos en las clases protegibles y que contienen la entidad protegible.

En términos generales, el algoritmo reúne todos los permisos pertinentes. Si no se encuentra ningún bloqueo DENY, el algoritmo busca un permiso GRANT que proporcione el acceso suficiente.

El algoritmo contiene tres elementos esenciales, el contexto de seguridad, el espacio de permisos y los permisos requeridos.

a) Contexto de seguridad. Es el grupo de entidades de seguridad que aportan los permisos para la comprobación de acceso. Son los permisos que están relacionados con el inicio de sesión actual o el usuario, a menos que el contexto de seguridad se cambiara a otro inicio de sesión o usuario utilizando la instrucción EXECUTE AS. El contexto de seguridad incluye las entidades de seguridad siguientes:

   i. El inicio de sesión.

   ii. El usuario.

   iii. Pertenecientes al rol.

   iv. Pertenecientes al grupo Windows.

   v. Si se utiliza la firma de módulo, cualquier cuenta de inicio de sesión o de usuario se percata del certificado utilizado para firmar el módulo que el usuario está ejecutando actualmente, así como de los pertenecientes al rol asociados de esa entidad de seguridad.

b) Espacio del permiso. Es la entidad protegible y todas las clases protegibles que contiene dicha entidad. Por ejemplo, una tabla (una entidad protegible) está contenida en la clase de esquema protegible y en la clase de base de datos protegible. El acceso puede verse afectado por permisos de nivel de tabla, esquema, base de datos y servidor.

c) Permiso necesario. Corresponde al tipo de permiso que se necesita. (INSERT, UPDATE, DELETE, SELECT, EXECUTE, ALTER, CONTROL, etc.).

   i. El acceso puede requerir varios permisos, por ejemplo, un procedimiento almacenado puede requerir el permiso EXECUTE sobre el procedimiento almacenado y el permiso INSERT sobre varias tablas a las que hace referencia el procedimiento almacenado.

   ii. Una vista de administración dinámica puede requerir los permisos VIEW SERVER STATE y SELECT sobre la vista.

Uno de los beneficios de contar con un sistema granular de permisos, es que SQL Server protege tanto los datos como los metadatos. SQL Server examina los permisos de un principal y solo muestra los objetos si es propietario o tiene algún permiso sobre ellos.

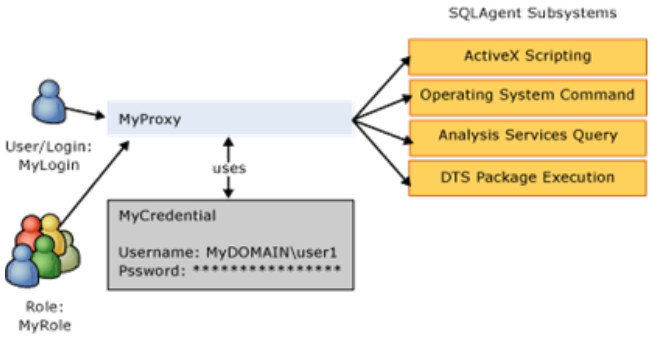
Con el permiso VIEW DEFINITION es posible conceder permisos para ver los metadatos de un objeto sin tener ningún permiso sobre él. Además, esta protección se extiende a los mensajes de error cuando un principal intenta acceder a objetos sin permisos, ya que no se distingue entre si el objeto existe o no se tiene permisos sobre él.

Otra característica importante, es el uso de credenciales. Una credencial es un registro que contiene la información de autenticación necesaria para conectarse a un recurso fuera de SQL Server.

Estas credenciales se pueden asignar a uno o varios inicios de sesión SQL, de forma que utilicen estas credenciales cuando necesiten acceder a recursos situados fuera de la instancia del servidor. Es posible asignar una única credencial a múltiples inicios de sesión SQL Server, pero un inicio de sesión solo puede tener asignada una credencial.

El uso de credenciales también permite al Agente SQL Server ejecutar cada paso en un contexto seguro, en el que, en cada paso, solo se cuenta con los permisos necesarios para el trabajo.

Esto se consigue gracias a la creación de servidores proxy del Agente SQL Server. Cada servidor proxy tiene asignado una credencial y éste se asocia a uno o varios pasos de un trabajo del Agente SQL Server, consiguiendo de esta forma un sistema robusto aplicando el principio de menor privilegio.



Como ya se ha indicado anteriormente, SQL Server determina el contexto de ejecución por el usuario o inicio de sesión conectado a la sesión que ejecuta un módulo (procedimiento almacenado, funciones, desencadenadores, etc.).

Este contexto establece la identidad con la que se comprueban los permisos para ejecutar las diferentes acciones. A partir de SQL Server 2005 es posible cambiar el contexto de ejecución haciendo uso de la instrucción EXECUTE AS, bien de forma explícita o de forma implícita en un módulo.

Cuando se realiza un cambio de contexto, SQL Server comprueba los permisos con el inicio de sesión de dicha cuenta, en vez de hacerlo con la identidad del usuario que llama al módulo.

El inicio de sesión se suplanta durante el resto de la sesión hasta que finaliza el modulo o hasta que el cambio de sesión se revierta específicamente.

En este sentido, SQL Server 2016 implementa los esquemas según la especificación ANSI SQL-92, entendiendo éstos como una colección de objetos de base de datos con un único principal como propietario, y que constituyen un espacio de nombres único.

Cada usuario tendrá asignado un esquema predeterminado de modo que SQL Server lo toma por defecto cuando se referencian objetos sin nombre de esquema. De este modo, se consigue un aislamiento total entre usuarios y esquemas, utilizando estos últimos para dotar de seguridad a la base de datos sin asignar permisos directamente a los objetos de la base de datos.

SQL Server incluye diez esquemas predefinidos que usan el mismo nombre que los usuarios y los roles de base de datos integrados. Estos esquemas se crean por compatibilidad con versiones anteriores. Los esquemas "dbo", "guest", "sys" e "information_schema" no pueden eliminarse.

Los esquemas "information_schema" y "sys" están reservados para los objetos del sistema, por lo que no es posible crear o eliminar objetos de ellos. El esquema "dbo" pertenece a la cuenta de usuario dbo y es el esquema predeterminado de los usuarios si no se les asigna ningún otro. El esquema "guest" pertenece al usuario guest, incluido de forma predeterminada en todas las bases de datos y cuyos permisos se aplican a todos los usuarios que no tienen una cuenta en la base de datos.

8.6 CIFRADO DE DATOS

Para lograr una defensa en profundidad y poder adecuarse a las leyes actuales, como el Reglamento General de Protección de Datos (RGPD), es necesario aplicar medidas de protección en diferentes capas.

La última de estas capas consiste en la protección de los datos almacenados en la base de datos. SQL Server 2016 cuenta con soporte para diferentes tipos de cifrados a través de claves simétricas, asimétricas y certificados digitales.

SQL Server 2016 admite varios algoritmos de cifrado de clave simétrica, incluidos DES, Triple DES, RC2, DESX, AES de 128 bits, AES de 192 bits y AES de 256 bits. Los algoritmos se implementan con la API Windows Crypto.

A la hora de seleccionar un algoritmo de cifrado, se pueden seguir las siguientes recomendaciones:

a) El cifrado más seguro generalmente consume más recursos de la CPU que un cifrado menos seguro.

b) Las claves largas suelen producir un cifrado más seguro que las claves cortas.

c) El cifrado asimétrico es menos seguro que el simétrico con la misma longitud de clave, pero es relativamente lento.

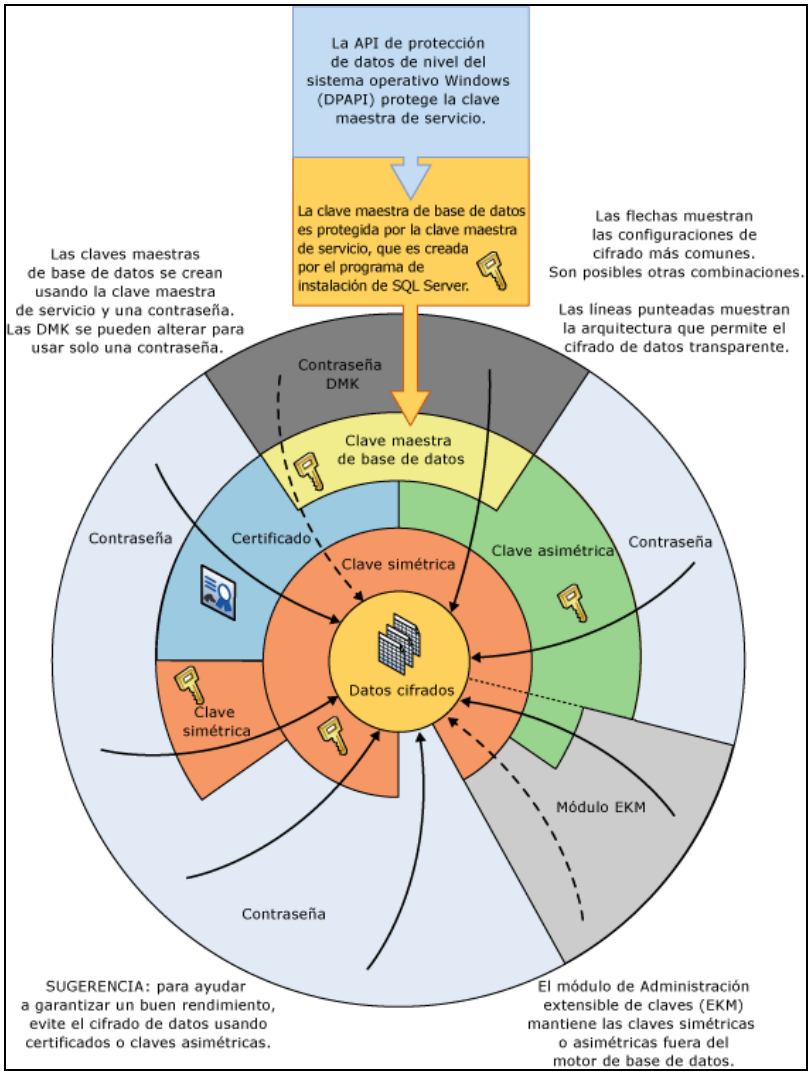
d) Los cifrados en bloque con claves largas son más seguros que los cifrados de flujo.

e) Las contraseñas largas y complejas son más seguras que las contraseñas cortas.

f) Si se tiene que cifrar una gran cantidad de datos, se recomienda cifrar los datos con una clave simétrica y cifrar la clave simétrica con una clave asimétrica.

g) Los datos cifrados no se pueden comprimir, pero los datos comprimidos se pueden cifrar. Si se va a hacer uso de compresión, se debe comprimir los datos antes de cifrarlos.

SQL Server 2016 cifra los datos con una infraestructura jerárquica, tanto para el cifrado como para la administración de las claves. Cada capa cifra la capa inferior utilizando combinaciones de certificados, claves simétricas y asimétricas. Las claves simétricas y asimétricas pueden residir fuera de SQL Server en un módulo de administración extensible de claves (EMK).



Tal y como se puede observar en la imagen del fabricante, la clave maestra de bases de datos (DMK) se protege mediante la clave maestra de servicio, que se crea durante la instalación de SQL Server y se cifra con la API de protección de datos de Windows (DPAPI).

Este proceso se repite con los siguientes niveles de la jerarquía donde cada nivel cifra el nivel que tiene por debajo.

A los mecanismos de cifrado disponibles en SQL Server 2005, que son el uso de certificados, claves asimétricas y claves simétricas, se añaden, a partir de SQL Server 2008, dos nuevos mecanismos: funciones de Transact-SQL y cifrado de datos transparente (TDE).

En SQL Server 2016 el material cifrado con RC4 o RC4_128 solo se puede descifrar en nivel de compatibilidad 90 o 100, los cuales no son recomendables por ser retirados en la próxima versión de SQL Server. En su lugar se recomienda aplicar algoritmos más recientes como puede ser AES.

Gracias al mecanismo de cifrado de funciones de Transact-SQL es posible cifrar los datos a medida que se insertan o actualizan los datos sobre la base de datos.

En Microsoft SQL Server 2016 la función HASHBYTES admite los algoritmos SHA2_256 y SHA2_512. 256 bits (32 bytes) para SHA2_256 y 512 bits (64 bytes). En el caso de SHA2_512 se aplica a partir de SQL Server 2012 en adelante.

El uso de certificados de clave pública permite liberar al servidor de la necesidad de establecer contraseñas para sujetos individuales, el certificado contiene una firma digital que enlaza el valor de la clave pública con la identidad de la persona, residiendo la responsabilidad de identificar al sujeto en la entidad emisora de los certificados.

Además, SQL Server 2016 soporta la generación de certificados autofirmados que cumplen con el standard X.509 y son compatibles con los campos de X.509 v1.

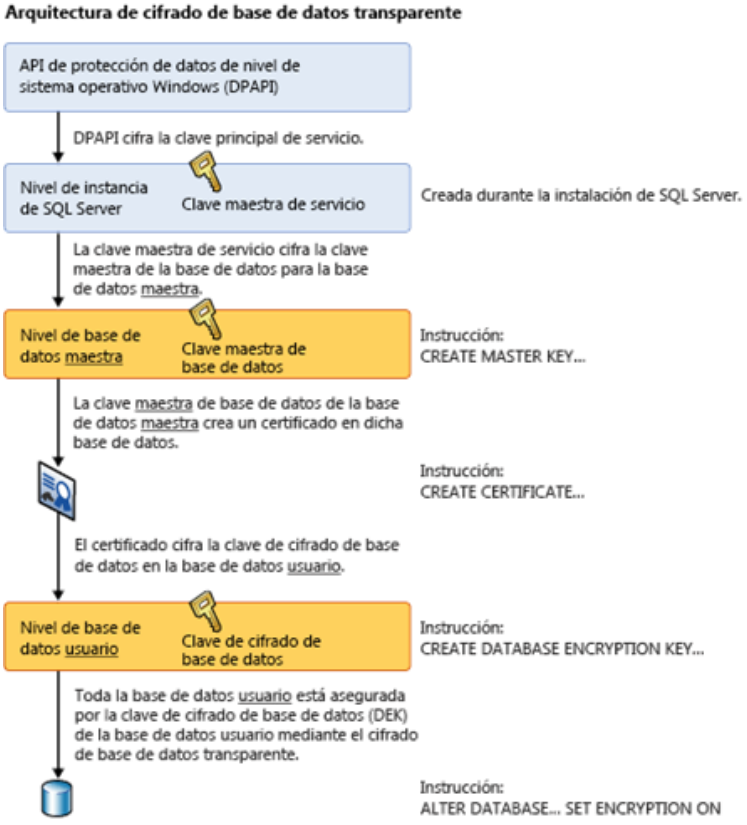
Las claves privadas generadas por SQL Server 2016 tienen una longitud predeterminada de 1024 bits. Las claves privadas importadas de un origen externo presentan una longitud mínima de 384 bits y una longitud máxima de 4.096 bits.

Una clave simétrica se compone de una clave privada y una clave pública. Cada clave puede descifrar los datos cifrados con la otra. El consumo de recursos en el cifrado asimétrico es superior al simétrico, sin embargo, asegura una mayor protección de los datos. Es posible utilizar una clave asimétrica para proteger una clave simétrica.

Las claves simétricas permiten el cifrado y descifrado de datos de forma rápida, constituyendo el mecanismo más adecuado para el cifrado habitual de datos confidenciales.

La funcionalidad de cifrado de datos transparente (TDE) utiliza una clave simétrica denominada clave de cifrado de base de datos y permite cifrar de forma trasparente a usuarios y aplicaciones toda la base de datos. La clave de cifrado de la base de datos se protege con la clave maestra de la base de datos o con una clave asimétrica almacenada en un módulo EKM.

TDE realiza el cifrado y descifrado de E/S en tiempo real de los datos y los archivos de registro. El cifrado utiliza una clave de cifrado de la base de datos (DEK), que está almacenada en el registro de arranque de la base de datos para que esté disponible durante la recuperación.



SQL Server permite exponer la funcionalidad de cifrado para su uso por terceros. De esta forma, si la organización cuenta con un mecanismo para el almacenamiento, generación y retirada de claves, se puede integrar con SQL Server 2016.

Además, también soporta el uso de HSM (Modulo de Seguridad hardware), que consiste en un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas, logrando así una completa separación entre datos y claves.

Gracias al soporte de cifrado, SQL Server 2016 proporciona la capacidad para firmar módulos de código (procedimientos almacenados, funciones, disparadores y notificaciones de eventos) con certificados.

El uso de módulos firmados brinda varios beneficios, entre los que se encuentra la posibilidad de afinar aún más los permisos de acceso a tablas y objetos, ya que ahora se podrá limitar al código firmado. Otro beneficio es la protección de los propios módulos, ya que al igual que sucede con la firma de un documento digital, si se modifica el código del módulo se invalida la firma.

SQL Server 2016 usa el algoritmo de cifrado AES para proteger la clave maestra de servicio (SMK) y la clave maestra de la base de datos (DMK).

AES es un algoritmo de cifrado más reciente que el algoritmo 3DES, el cual se empleaba en versiones anteriores. Es por ello que, después de actualizar una instancia de motor de base de datos a SQL Server 2016 se deben volver a generar las claves SMK y DMK para actualizarlas al algoritmo AES.

8.7 AUDITORÍA Y REGISTRO

SQL Server 2016 incluye una serie de características que permiten auditar las actividades y cambios en un servidor SQL Server. Estas características incluyen la auditoría de inicio de sesión, el modo de auditoría C2, la auditoría a través de SQL Server Profiler, el uso de desencadenadores DDL o la auditoría a través de SQL Server Audit, característica introducida a partir de SQL Server 2008.

A través de las propiedades del servidor es posible activar la auditoría de inicio de sesión, de modo que se puede indicar qué eventos se registran: ninguno, los inicios de sesión erróneos, los inicios de sesión correctos, o los inicios de sesión correctos y erróneos.

Todos estos registros de auditoría se almacenan en el registro de aplicación de Windows.

SQL Server permite la activación del modo de auditoría C2. En este modo, el servidor registra todos los intentos de acceso a instrucciones y objetos de SQL Server, tanto si son correctos como incorrectos. El registro se hace sobre un fichero en el directorio por defecto de la instancia. Cuando el fichero alcanza los 200 MB, se genera un nuevo fichero y se pasa a escribir en este.

A partir del Service Pack 2 de SQL Server 2008, el estándar de seguridad C2 se ha sustituido por Common Criteria Certification.

La activación de la compatibilidad con los estándares internacionales de seguridad habilita los siguientes elementos:

Criterio	Descripción
Protección de información residual (RIP)	RIP requiere que una asignación de memoria se sobrescriba con un patrón de bits conocido antes de que la memoria se reasigne a un nuevo recurso. Ajustarse al estándar RIP puede mejorar la seguridad, pero puede ralentizar el rendimiento.
La capacidad para ver estadísticas de inicio de sesión	Habilita la auditoría de inicio de sesión. Cada vez que un usuario inicia sesión correctamente en SQL Server, se muestra la información acerca del último inicio de sesión correcto, el último inicio de sesión incorrecto y el número de intentos realizados entre la hora del último inicio de sesión correcto y la hora actual.
La columna GRANT no debe invalidar la tabla DENY	La instrucción DENY de nivel de tabla tiene prioridad sobre una instrucción GRANT de nivel de columna. Cuando no está habilitada la opción, una instrucción GRANT de columna tiene prioridad sobre una instrucción DENY de tabla.

La opción common criteria compliance enabled es una opción avanzada. Solo se evalúan y certifican los criterios comunes para las ediciones Enterprise y Datacenter

Los estándares internacionales de seguridad permiten comparar los resultados entre evaluaciones de productos independientes. El proceso de evaluación establece un nivel de confianza en el grado en el que el producto TI satisface la funcionalidad de seguridad de estos productos y ha superado las medidas de evaluación aplicadas.

El uso del analizador de SQL Server (SQL Server Profiler) permite configurar un seguimiento del servidor añadiendo aquellos eventos que el auditor quiere registrar. Los eventos van desde la agregación o eliminación de un inicio de sesión en una base de datos, hasta la ejecución de una instrucción CREATE, ALTER o DROP sobre un objeto de una base de datos o la ejecución de una consulta SELECT. Los eventos de auditoría de seguridad son los siguientes:

Tipo evento	Descripción
Audit Add DB User	Indica que se ha agregado o quitado un inicio de sesión como usuario de base de datos en una base de datos.
Audit Add Login to Server Role	Indica que se ha agregado o quitado un inicio de sesión de una función fija de servidor.
Audit Add Member to DB Role	Indica que se ha agregado o quitado un inicio de sesión de una función.
Audit Add Role	Indica que se ha agregado o quitado una función de base de datos de una base de datos.
Audit Addlogin	Indica que se ha agregado o quitado un inicio de sesión.
Audit App Role Change Password	Indica que se ha cambiado una contraseña para una función de aplicación.
Audit Backup/Restore	Indica que se ha enviado una instrucción de copia de seguridad o restauración.
Audit Broker Conversation	Informa de los mensajes de auditoría relacionados con la seguridad de diálogo de Service Broker.
Clase de eventos Audit Broker Login	Informa de los mensajes de auditoría relacionados con la seguridad de transporte de Service Broker.
Audit Change Audit	Indica que se ha realizado una modificación de traza de auditoría.
Audit Change Database Owner	Indica que se han comprobado los permisos para cambiar el propietario de una base de datos.

Tipo evento	Descripción
Audit Database Management	Indica que se ha creado, modificado o quitado una base de datos.
Audit Database Mirroring Login	Informa de los mensajes de auditoría relacionados con la seguridad en el transporte para la creación del reflejo de una base de datos.
Audit Database Object Access	Indica que se ha obtenido acceso a un objeto de base de datos, como un esquema.
Audit Database Object GDR	Indica que se ha producido un evento GDR para un objeto de base de datos.
Audit Database Object Management	Indica que se ha ejecutado una instrucción CREATE, ALTER o DROP en un objeto de base de datos.
Audit Database Object Take Ownership	Indica que ha habido un cambio de propietario para objetos en el ámbito de una base de datos.
Audit Database Operation	Indica que se han realizado varias operaciones como la notificación de una consulta de punto de comprobación o suscripción.
Audit Database Principal Impersonation	Indica que se ha producido una suplantación en el ámbito de la base de datos.
Audit Database Principal Management	Indica que se han creado, modificado o quitado entidades de seguridad en una base de datos.
Audit Database Scope GDR	Indica que un usuario de Microsoft SQL Server ha emitido una instrucción GRANT, REVOKE o DENY para un permiso de instrucción.
Audit DBCC	Indica que se ha emitido un comando DBCC.
Clase de eventos Audit Fulltext	Indica que se ha producido un evento de texto completo.
Audit Login Change Password	Indica que un usuario ha cambiado su contraseña de inicio de sesión en SQL Server.
Audit Login Change Property	Indica que se ha usado sp_defaultdb, sp_defaultlanguage o ALTER LOGIN para modificar una propiedad de un inicio de sesión.
Audit Login	Indica que un usuario ha iniciado una sesión de SQL Server.
Audit Login Failed	Indica que un usuario intentó iniciar una sesión de SQL Server, pero no lo consiguió.
Audit Login GDR	Indica que se ha agregado o quitado un derecho de inicio de sesión de Microsoft Windows.
Audit Logout	Indica que un usuario ha finalizado una sesión de SQL Server.
Audit Object Derived Permission	Indica que se ha emitido una instrucción CREATE, ALTER o DROP para un objeto.
Audit Schema Object Access	Indica que se ha utilizado un permiso de objeto (como SELECT).
Audit Schema Object GDR	Indica que un usuario de SQL Server ha emitido una instrucción GRANT, REVOKE o DENY para un permiso de objeto de esquema.
Audit Schema Object Management	Indica que se ha creado, modificado o quitado un objeto de servidor.
Audit Schema Object Take Ownership	Indica que se han comprobado los permisos para cambiar el propietario de un objeto de esquema.
Audit Server Alter Trace	Indica que se ha comprobado el permiso ALTER TRACE.
Audit Server Object GDR	Indica que se ha producido un evento GDR para un objeto de esquema.

Tipo evento	Descripción
Audit Server Object Management	Indica que se ha producido un evento CREATE, ALTER o DROP para un objeto de servidor.
Audit Server Object Take Ownership	Indica que ha cambiado el propietario de un objeto de servidor.
Audit Server Operation	Indica que se han realizado operaciones de auditoría en el servidor.
Audit Server Principal Impersonation	Indica que se ha producido una suplantación en el ámbito del servidor.
Audit Server Principal Management	Indica que se ha emitido una instrucción CREATE, ALTER o DROP para una entidad se seguridad de servidor.
Audit Server Scope GDR	Indica que se ha producido un evento GDR para permisos de servidor.
Audit Server Starts and Stops	Indica que se ha modificado el estado de servicio de SQL Server.
Audit Statement Permission	Indica que se ha utilizado un permiso de instrucción.

Nota: SQL Server Profiler es una interfaz para crear y administrar seguimientos, así como analizar y reproducir resultados de seguimiento. Microsoft anunció que el uso de SQL Profiler para la captura y la reproducción de seguimiento de motor de base de datos han quedado obsoleto. Esta herramienta aún está disponible en SQL Server 2016, pero es posible que se elimine de versiones posteriores.

En la siguiente tabla se muestran las características que se recomienda utilizar en SQL Server 2016 para capturar y reproducir los datos de seguimiento:

Característica \ Carga de trabajo de destino	Motor relacional	Analysis Services
Captura de seguimiento	Interfaz gráfica de usuario de eventos extendidos en SQL Server Management Studio	SQL Server Profiler
Reproducción de seguimiento	Distributed Replay	SQL Server Profiler

La característica Distributed Replay ayuda a evaluar el impacto de las actualizaciones de SQL Server en un entorno aislado. También se puede utilizar para analizar el rendimiento y optimizar las consultas a las bases de datos. Además, proporciona una solución más escalable que SQL Server Profiler.

Con Distributed Replay, se puede reproducir una carga de trabajo de varios equipos y simular mejor una carga de trabajo esencial. A diferencia de SQL Server Profiler, Distributed Replay no se limita a volver a consultar la carga de trabajo de un único equipo.

La utilización de Distributed Replay es recomendable si se desea evaluar la compatibilidad de las aplicaciones. Por ejemplo, en el caso de probar escenarios de actualización de sistemas operativos y SQL Server, actualizaciones de hardware o la optimización de los índices.

También es recomendable su uso debido a que la simultaneidad en el seguimiento capturado es tan alta que un solo cliente de reproducción no basta para simularla.

Los siguientes componentes conforman el entorno de Distributed Replay:

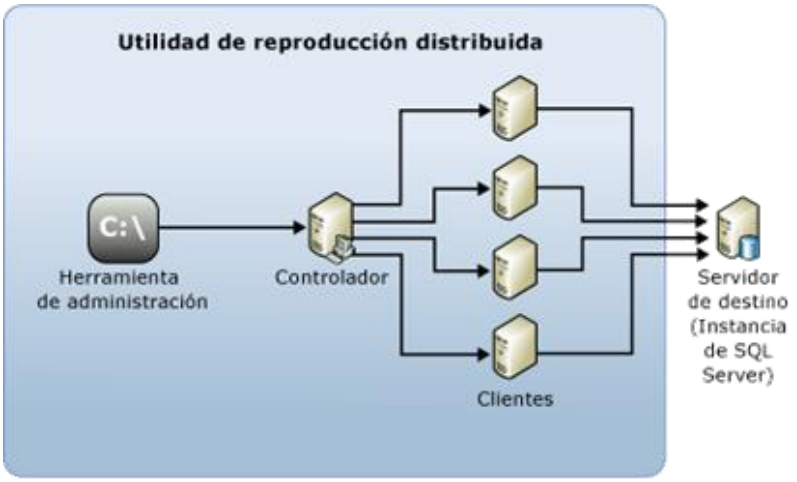
a) Herramienta de administración de Distributed Replay. Se usa para comunicarse con Distributed Replay Controller.

b) Distributed Replay Controller. Orquestra las acciones de los clientes de reproducción distribuida. Solo puede haber una instancia de controlador en cada entorno de Distributed Replay.

c) Distributed Replay Clients. Colaboran para simular cargas de trabajo en una instancia de SQL Server. Puede haber uno o varios clientes en cada entorno de Distributed Replay.

d) Servidor de destino: Es una instancia de SQL Server que Distributed Replay Clients pueden emplear para reproducir datos de seguimiento. Es recomendable que el servidor de destino se encuentre en un entorno de prueba.

La siguiente imagen muestra la arquitectura física de Distributed Replay de SQL Server.



A partir de SQL Server 2005 se incluyó la posibilidad de crear los desencadenadores DDL, un tipo especial de desencadenadores que se activan en respuesta a las instrucciones del lenguaje de definición de datos (DDL). Estos desencadenadores se pueden utilizar para auditar las operaciones que se realizan sobre el servidor.

Es posible emplear desencadenadores DLL cuando desee hacer lo siguiente:

a) Impedir determinados cambios en el esquema de la base de datos.

b) Que ocurra algo en la base de datos como respuesta a un cambio realizado en el esquema de la base de datos.

c) Registrar cambios o eventos en el esquema de la base de datos.

A partir de SQL Server 2008 es posible configurar una auditoría automática a través de SQL Server Audit. Las ventajas de utilizar SQL Server Audit frente a otras soluciones de auditoría son las siguientes:

a) Una auditoría recopila un conjunto de acciones y grupos de acciones a nivel de servidor y/o a nivel de base de datos en una sola instancia.

b) Es posible tener configuradas y funcionando varias auditorías para una instancia de SQL Server.

c) La auditoría permite especificar el destino para los resultados generados. El destino puede ser un archivo, el registro de eventos de seguridad de Windows o el registro de eventos de aplicación de Windows.

d) Es posible aplicar dos configuraciones en caso de que la auditoría de un evento falle: cerrar y continuar. En la primera configuración, si se produce un error al registrar un evento el servidor se cerrará, en el segundo caso, si no es posible registrar el evento el servidor continuará funcionando normalmente.

e) El impacto sobre el servidor del uso de SQL Server Audit es notablemente inferior al uso del analizador de SQL Server.

SQL Server Audit es más resistente a errores de escritura en el registro de auditoria, en caso de interrumpirse el servicio de red, una vez restablecido el servicio.

El objeto SQL Server Audit recopila una única instancia de acciones y grupos de acciones de nivel de servidor o de base de datos para su supervisión.

La auditoría a través de SQL Server Audit consta de cero o más elementos de acción de auditoría, los cuales pueden ser grupos de acciones o acciones individuales. Las auditorías pueden tener las siguientes categorías de acciones: nivel de servidor, nivel de base de datos y nivel de auditoría.

a) Nivel de servidor. Estas acciones incluyen las operaciones del servidor, como cambios de administración y operaciones de inicio y cierre de sesión.

b) Nivel de base de datos. Estas acciones comprenden operaciones de lenguaje de manipulación de datos (DML) y de lenguaje de definición de datos (DDL).

c) Nivel de auditoría. Son las acciones relacionadas con el proceso de auditoría.

Las acciones a nivel de servidor incluyen las operaciones de servidor, como cambios en la administración y operaciones de inicio y cierre de sesión. Los grupos de acciones de auditoría a nivel de servidor y sus eventos equivalentes son los siguientes:

Grupo de acciones de auditoria a nivel de servidor	Eventos equivalentes
APPLICATION_ROLE_CHANGE_PASSWORD_GROUP	Audit App Role Change Password
AUDIT_CHANGE_GROUP	Audit Change Audit
BACKUP_RESTORE_GROUP	Audit Backup/Restore
BROKER_LOGIN_GROUP	Audit Broker Login
DATABASE_CHANGE_GROUP	Audit Database Management
DATABASE_LOGOUT_GROUP	Auditoría de cierre de sesión de base de datos
DATABASE_MIRRORING_LOGIN_GROUP	Audit Database Mirroring Login
DATABASE_OBJECT_ACCESS_GROUP	Audit Database Object Access
DATABASE_OBJECT_CHANGE_GROUP	Audit Database Object Management

Grupo de acciones de auditoria a nivel de servidor	Eventos equivalentes
DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP	Audit Database Object Take Ownership
DATABASE_OBJECT_PERMISSION_CHANGE_GROUP	Audit Database Object GDR
DATABASE_OPERATION_GROUP	Audit Database Operation
DATABASE_OWNERSHIP_CHANGE_GROUP	Audit Change Database Owner
DATABASE_PERMISSION_CHANGE_GROUP	Audit Database Scope GDR
DATABASE_PRINCIPAL_CHANGE_GROUP	Audit Database Principal Management
DATABASE_PRINCIPAL_IMPERSONATION_GROUP	Audit Database Principal Impersonation
DATABASE_ROLE_MEMBER_CHANGE_GROUP	Audit Add Member to DB Role
DBCC_GROUP	Audit DBCC
FAILED_DATABASE_AUTHENTICATION_GROUP	Audit Login Failed
FAILED_LOGIN_GROUP	Audit Login Failed
FULLTEXT_GROUP	Audit Fulltext.
LOGIN_CHANGE_PASSWORD_GROUP	Audit Login Change Password
LOGOUT_GROUP	Audit Logout
SCHEMA_OBJECT_ACCESS_GROUP	Audit Schema Object Access
SCHEMA_OBJECT_CHANGE_GROUP	Audit Schema Object Management
SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP	Audit Schema Object Take Ownership
SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP	Audit Schema Object GDR
SERVER_OBJECT_CHANGE_GROUP	Audit Server Object Management
SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP	Audit Server Object Take Ownership
SERVER_OBJECT_PERMISSION_CHANGE_GROUP	Audit Server Object GDR
SERVER_OPERATION_GROUP	Audit Server Operation
SERVER_PERMISSION_CHANGE_GROUP	Audit Server Scope GDR
SERVER_PRINCIPAL_CHANGE_GROUP	Audit Server Principal Management
SERVER_PRINCIPAL_IMPERSONATION_GROUP	Audit Server Principal Impersonation
SERVER_ROLE_MEMBER_CHANGE_GROUP	Audit Add Login to Server Role
SERVER_STATE_CHANGE_GROUP	Audit Server Starts and Stops
SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP	Auditoría correcta de autenticación de base de datos
SUCCESSFUL_LOGIN_GROUP	Audit Login
TRACE_CHANGE_GROUP	Audit Server Alter Trace
TRANSACTION_GROUP	Audit Action Group
USER_CHANGE_PASSWORD_GROUP	Audit Action Group
USER_DEFINED_AUDIT_GROUP	Audit Action Group

Las acciones a nivel de base de datos comprenden operaciones del lenguaje de manipulación de datos (DML) y del lenguaje de definición de datos. A este nivel se tienen tanto grupos de acciones como acciones individuales. Las siguientes tablas muestran estas acciones.

Grupo de acciones de auditoria a nivel de base de datos	Eventos equivalentes
APPLICATION_ROLE_CHANGE_PASSWORD_GROUP	Audit App Role Change Password
AUDIT_CHANGE_GROUP	Audit Change Audit
BACKUP_RESTORE_GROUP	Audit Backup/Restore
DATABASE_CHANGE_GROUP	Audit Database Management
DATABASE_LOGOUT_GROUP	Auditoría de cierre de sesión de base de datos
DATABASE_OBJECT_ACCESS_GROUP	Audit Database Object Access
DATABASE_OBJECT_CHANGE_GROUP	Audit Database Object Management

Grupo de acciones de auditoria a nivel de base de datos	Eventos equivalentes
DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP	Audit Database Object Take Ownership
DATABASE_OBJECT_PERMISSION_CHANGE_GROUP	Audit Database Object GDR
DATABASE_OPERATION_GROUP	Audit Database Operation
DATABASE_OWNERSHIP_CHANGE_GROUP	Audit Change Database Owner
DATABASE_PERMISSION_CHANGE_GROUP	Audit Database Scope GDR
DATABASE_PRINCIPAL_CHANGE_GROUP	Audit Database Principal Management
DATABASE_PRINCIPAL_IMPERSONATION_GROUP	Audit Database Principal Impersonation
DATABASE_ROLE_MEMBER_CHANGE_GROUP	Audit Add Member to DB Role
DBCC_GROUP	Audit DBCC
FAILED_DATABASE_AUTHENTICATION_GROUP	Audit Action Group
SCHEMA_OBJECT_ACCESS_GROUP	Audit Schema Object Access
SCHEMA_OBJECT_CHANGE_GROUP	Audit Schema Object Management
SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP	Audit Schema Object Take Ownership
SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP	Audit Schema Object GDR
SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP	Auditoría correcta de autenticación de base de datos
USER_CHANGE_PASSWORD_GROUP	Audit Action Group
USER_DEFINED_AUDIT_GROUP	Audit Action Group

Acciones	Descripción
SELECT	Se desencadena al emitir una instrucción SELECT.
UPDATE	Se desencadena al emitir una instrucción UPDATE.
INSERT	Se desencadena al emitir una instrucción INSERT.
DELETE	Se desencadena al emitir una instrucción DELETE.
EXECUTE	Se desencadena al emitir una instrucción EXECUTE.
RECEIVE	Se desencadena al emitir una instrucción RECEIVE.
REFERENCES	Se desencadena al comprobar un permiso REFERENCES.

Las acciones a nivel de auditoría se pueden realizar en el ámbito del servidor y en el ámbito de la base de datos. En el ámbito de la base de datos, solo se produce para las especificaciones de auditoría de base de datos. Los grupos de acciones disponibles a este nivel son los siguientes:

Grupo de acciones	Comandos que desencadena el evento
AUDIT_CHANGE_GROUP	CREATE SERVER AUDIT
	ALTER SERVER AUDIT
	DROP SERVER AUDIT
	CREATE SERVER AUDIT SPECIFICATION
	ALTER SERVER AUDIT SPECIFICATION
	DROP SERVER AUDIT SPECIFICATION
	CREATE DATABASE AUDIT SPECIFICATION
	ALTER DATABASE AUDIT SPECIFICATION
	DROP DATABASE AUDIT SPECIFICATION