**DEMOSTRACIÓN DE APLICACIÓN DE HARDENING A SQL SERVER 2019**

**Paso 1. Instalar la base de datos de SQL server 2019 en su versión 15.0.**

Descargamos el instalador de SQL Server 2019 desde la página oficial

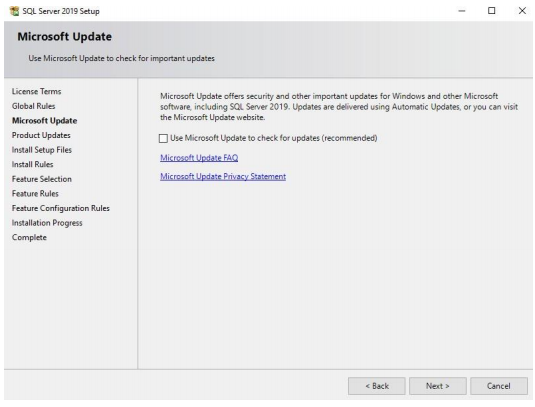
<https://www.microsoft.com/es-es/sql-server/sql-server-downloads>

Buscamos y seleccionamos la versión compatible con el sistema operativo deseado



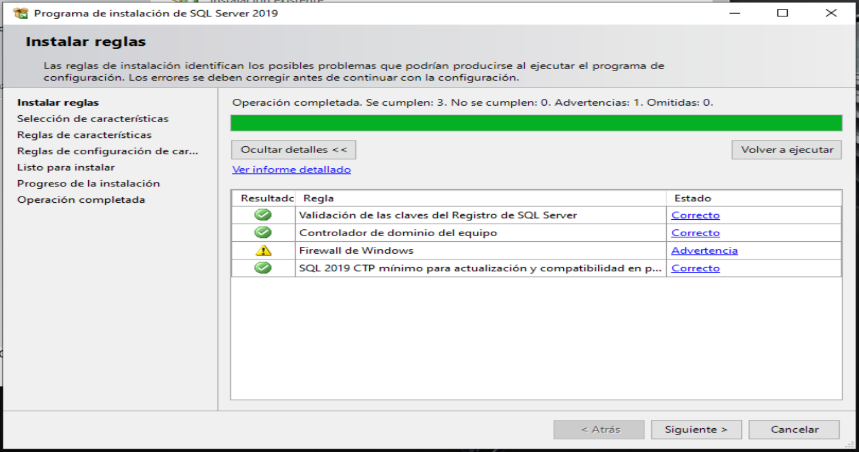
**Paso 2. Instalación de SQL Server 2019 y sus paquetes.**

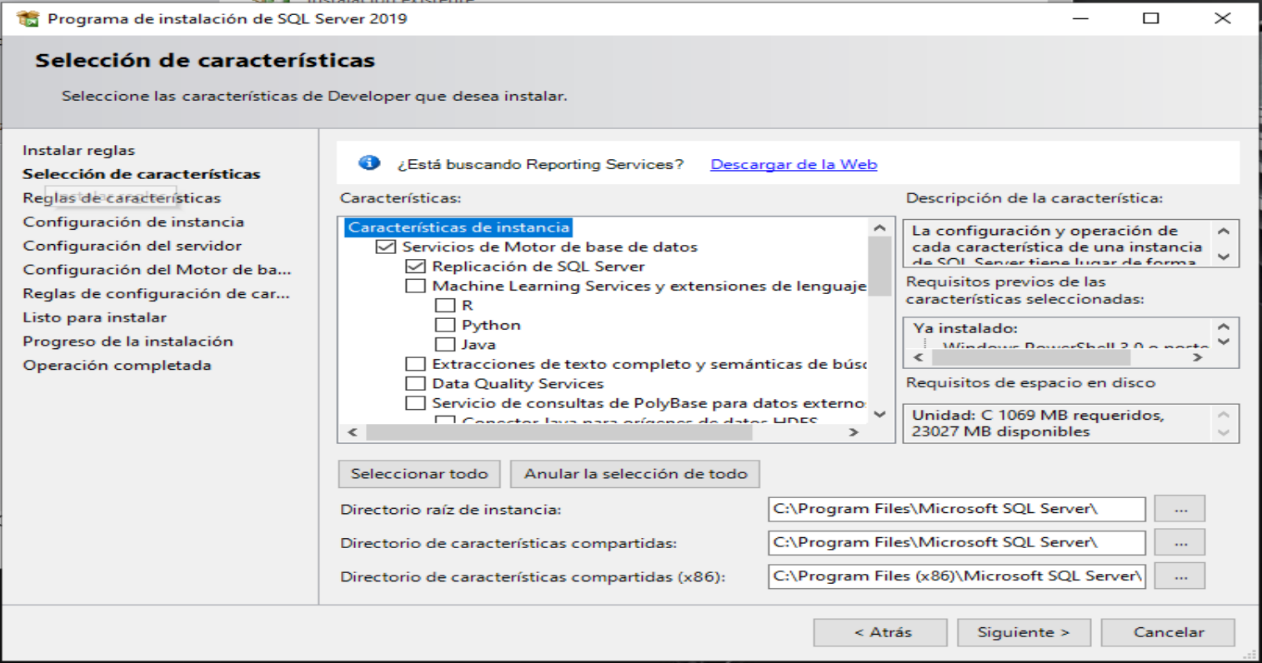
La instalación en Windows es bastante sencilla, ejecutamos el instalador SQL2019-SSEI-Dev.exe y automáticamente se hace la descompresión del archivo y se ejecuta el instalador.

**Paso 3.** El instalador nos permite, antes de instalar, hacer una revisión de las actualizaciones para tener el ultimo service pack o reléase (Los **Service Pack** mantienen actualizado un producto. Incluyen revisiones y correcciones para los problemas que se notifican a través de la Comunidad de Microsoft **SQL Server**), marcamos esta casilla (No obligatoria) para continuar con la instalación.

**Paso 4.** El instalador hace un análisis de requerimientos antes de continuar, en nuestro

caso tenemos un warning que nos menciona configurar el firewall de Windows por seguridad, esto lo corregiremos más adelante aplicando hardening. Continuamos con el proceso.

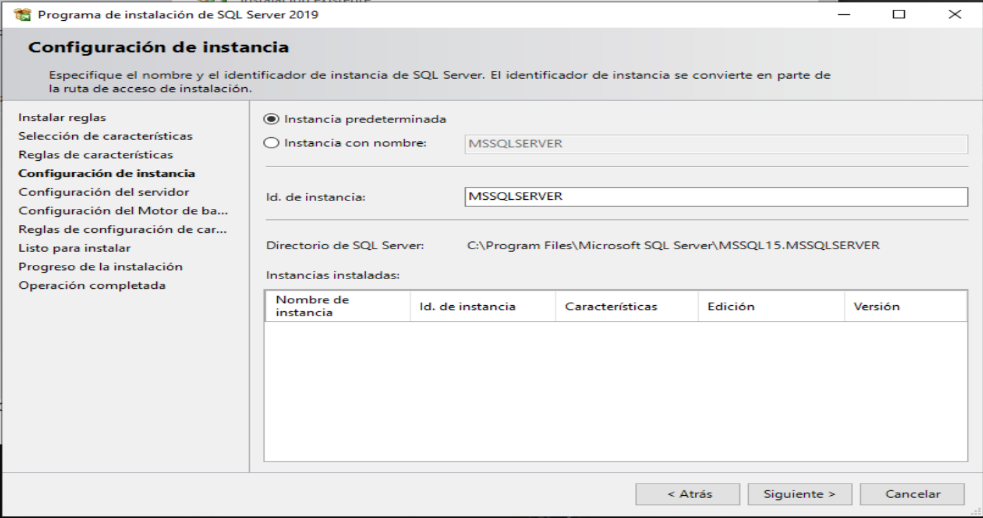


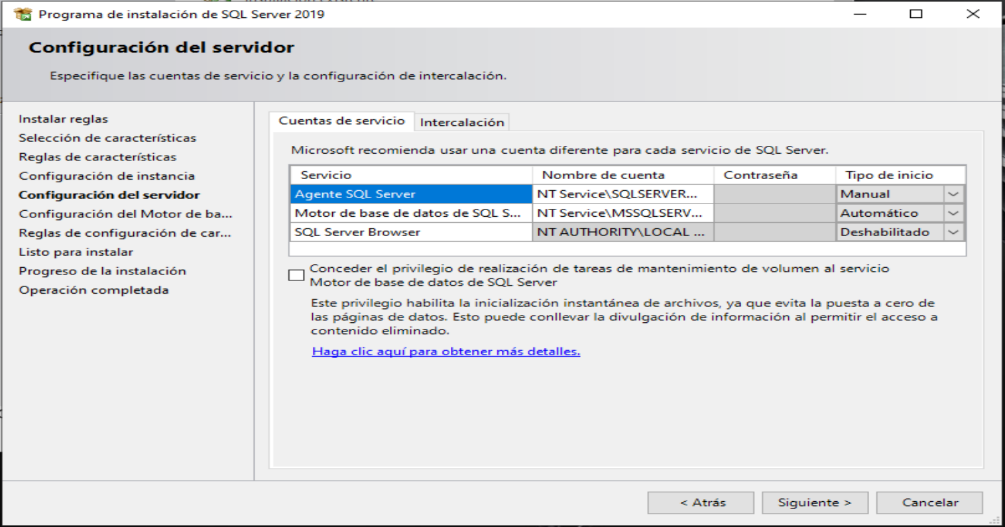
**Paso 5.** El asistente nos indica las rutas de instalación por defecto de la instalación de SQL Server

**Paso 6.** El asistente nos permite ingresar el nombre de la instancia de la base de datos.

Intencionalmente Dejamos el nombre por defecto de la instancia MSSQLSERVER para

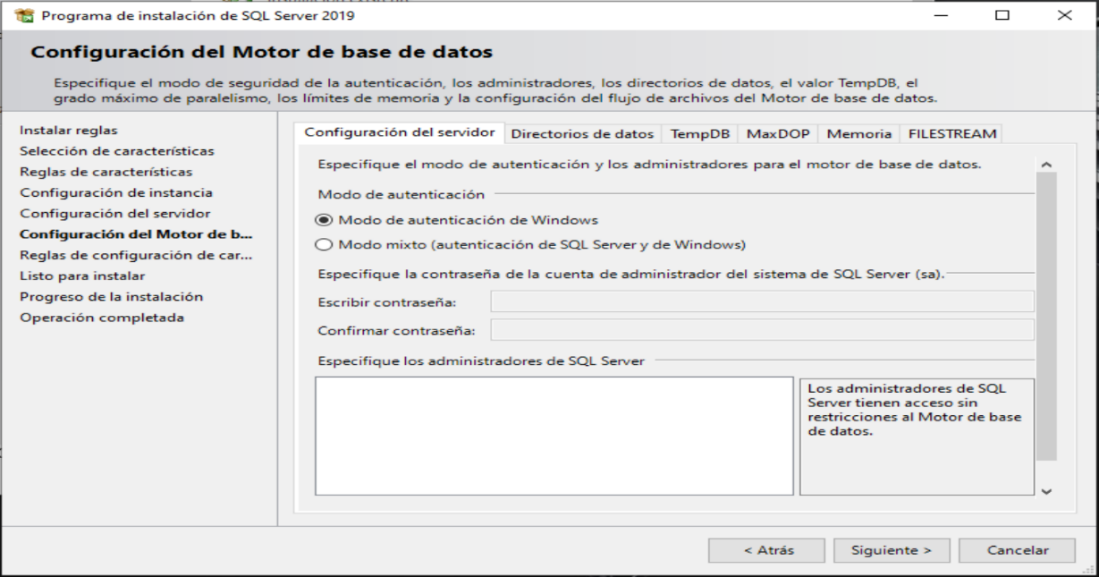
efectos prácticos mostraremos el cambio del nombre de la instancia al aplicar hardening post instalación.



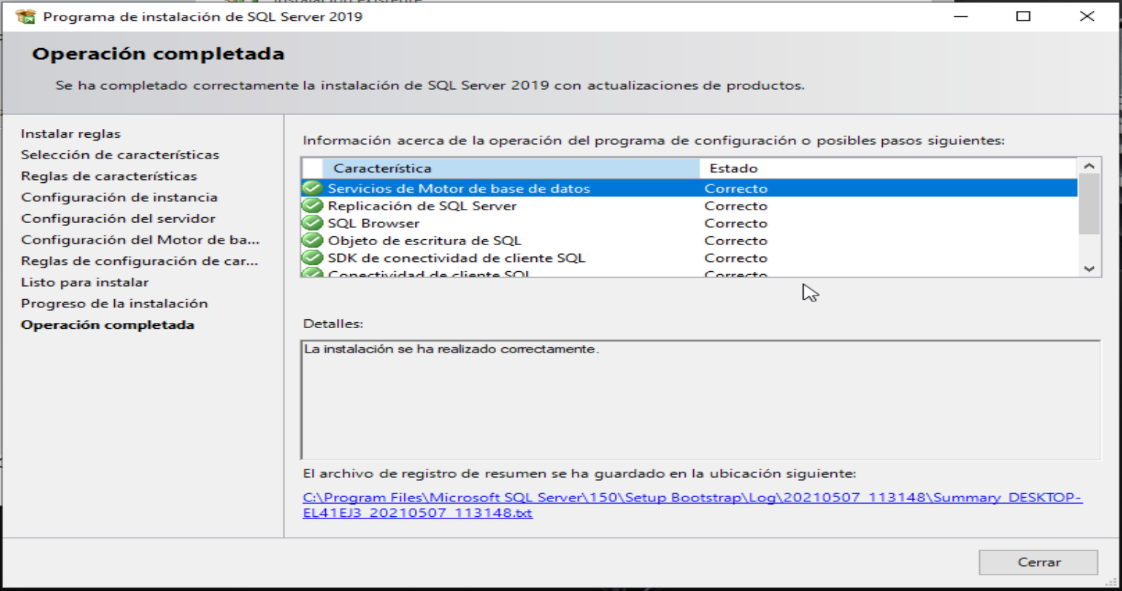
**Paso 7.** El asistente de SQL Server configura un servicio de Windows para controlar el motor de la base de datos, por defecto con una cuenta de servicio sin contraseña. Igualmente aplicaremos más adelante hardening para cambiar este usuario y aplicarle una contraseña.

**Paso 8.** El asistente ahora nos solicita configurar el modo de autenticación. Por defecto se encuentra la autenticación Windows que toma las credenciales del usuario logueado y se la pasa como parámetro al login de la base para evitar pedir un usuario y contraseña.

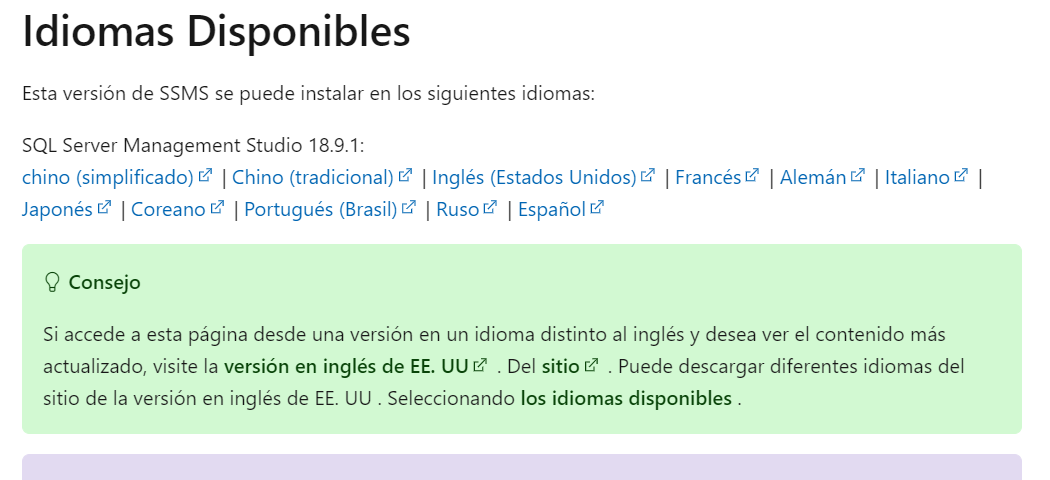
Aplicaremos hardening para corregir esto más adelante.



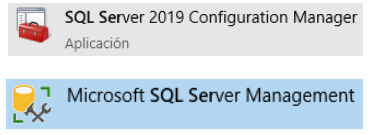
**Paso 9.** Finalmente hemos terminado la instalación de SQL Server 2019 es importante reiniciar el equipo para aplicar y configurar los cambios en la base de datos.



Cave mencionar que luego de terminar la instalación procederemos a descargar el instalador de SQL Server Management (es la herramienta de **SQL Server** que permite definir y gestionar todas las bases de datos almacenadas en el servidor **SQL Server** ) desde la pagina oficial descargamos el instalador.



Selecciona el idioma que se desea descargar y al dar clic se descargara el instalador luego solo se ejecuta como administrador luego seguir los pasos ya que en Windows es fácil su instalación.

Una vez instalado nos aparecerán estas opciones donde se puede realizar las configuraciones y también gestionar las bases de datos.

**Hardening de base de datos SQL Server 2019**

1. Instalar actualizaciones y parches de seguridad

**Descripción:**

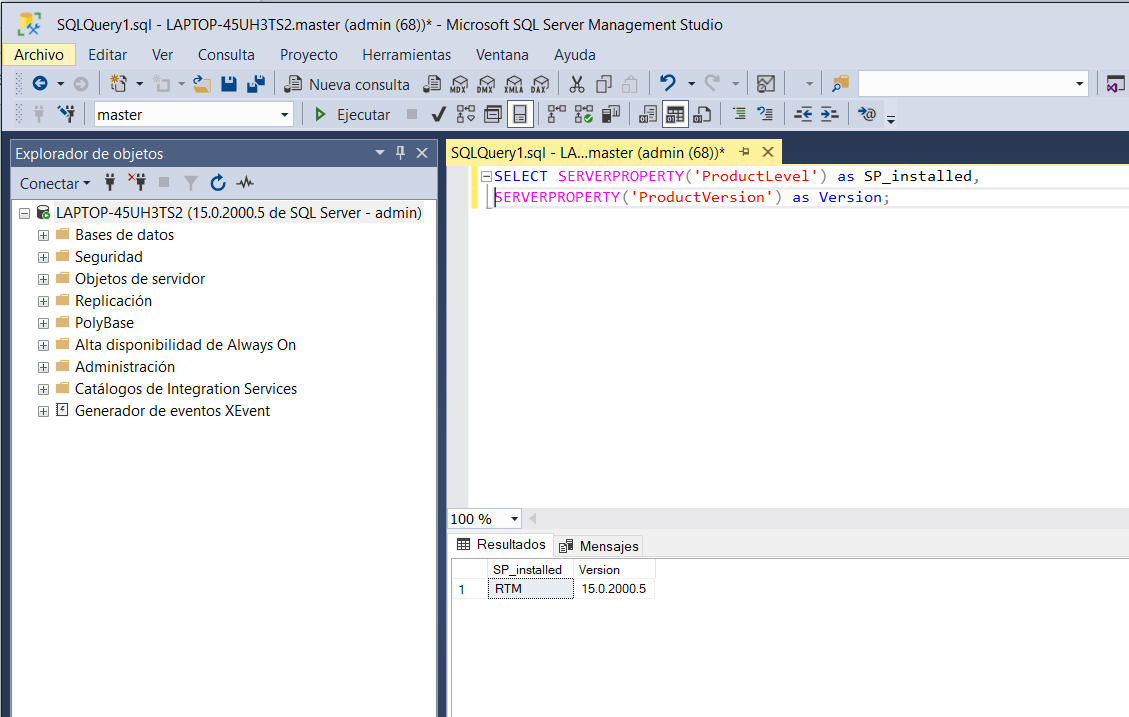
Los parches de SQL Server contienen actualizaciones del programa que corrigen la seguridad y la funcionalidad del producto y problemas encontrados en el software. Estos parches se pueden instalar con una actualización de seguridad, que es un solo parche, o una actualización acumulativa que es un grupo de parches. La versión de SQL Server y los niveles de parche deben ser los más recientes.

**Hallazgo:**

Para determinar su nivel de parche de SQL Server, ejecute el siguiente fragmento de código.

SELECT SERVERPROPERTY('ProductLevel') as SP\_installed,

SERVERPROPERTY('ProductVersion') as Version;



La primera columna devuelve el nivel de Service Pack instalado, la segunda es el número de compilación exacto.

Los parches más recientes de SQL Server se pueden encontrar aquí en la ruta url:

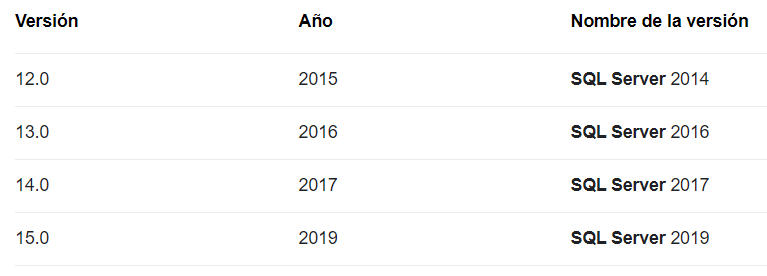
<https://docs.microsoft.com/en-us/sql/database-engine/install-windows/latest-updates-for-microsoft-sql-server?view=sql-server-ver15>

Revisiones y actualizaciones acumulativas de SQL Server 2019:

<https://support.microsoft.com/es-es/topic/kb4527376-actualizaci%C3%B3n-acumulativa-1-para-sql-server-2019-a8dae09e-96b5-9f13-9092-977341fafe17>

Riesgo hallado: Ninguno, la versión instalada es la última versión del producto disponible

en el mercado a la fecha debido a ello la seguridad es más eficiente.



1. Deshabilitar Ad Hoc Distributed Queries.

Descripción:

Habilitar consultas distribuidas ad hoc permite a los usuarios consultar datos y ejecutar declaraciones en fuentes de datos externas. Esta funcionalidad debe estar desactivada.

Lo que quiere decir más específicamente es que al habilitar su uso significa que cualquier inicio de sesión autenticado en SQL Server puede acceder al proveedor. Esta funcionalidad debe estar deshabilitada.

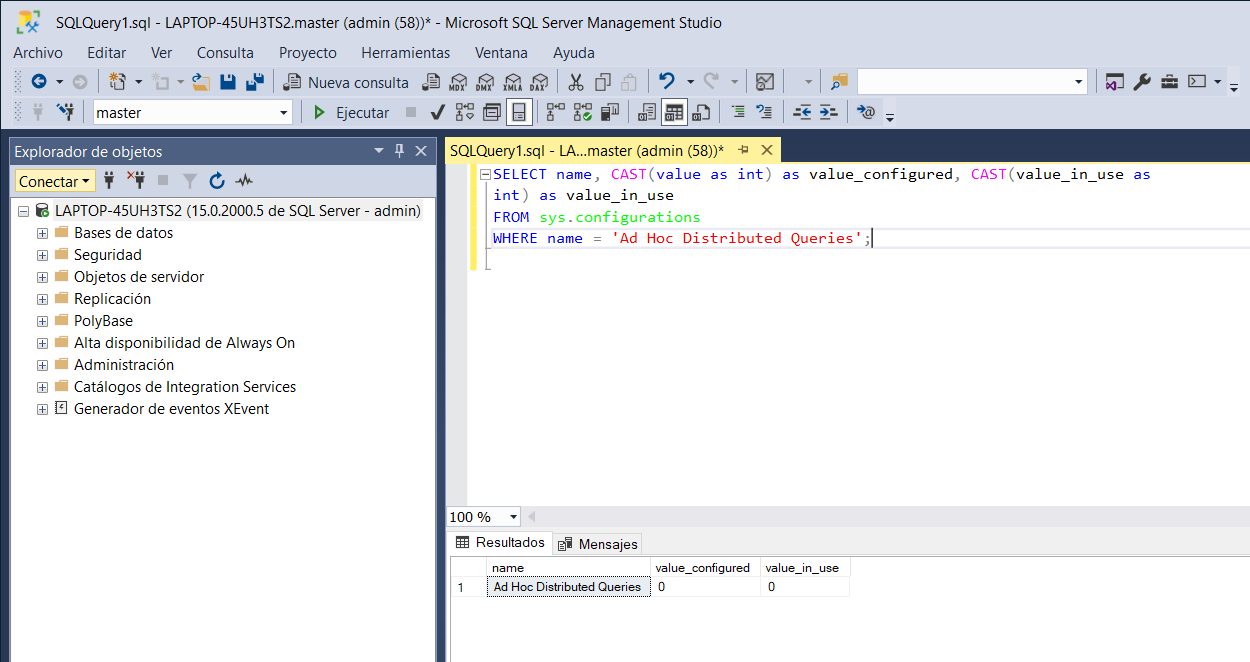
Hallazgo:

Al ejecutar el comando SQL

SELECT name, CAST(value as int) as value\_configured,

CAST(value\_in\_use as int) as value\_in\_use FROM sys.configurations WHERE name = 'Ad Hoc Distributed Queries';

Ad Hoc Distributed Queries al ejecutar el comando sea podido verificar que se encuentra deshabilitado.



Solución:

En dado caso se encuentre habilitado Ad Hoc puede ejecutar el siguiente comando SQL para deshabilitarlo

EXECUTE sp\_configure 'show advanced options', 1;

RECONFIGURE;

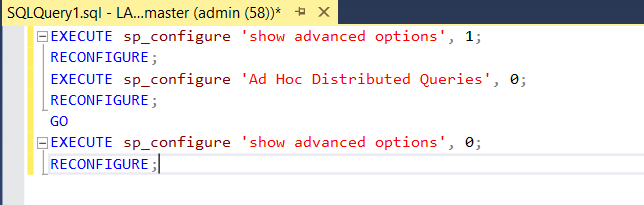
EXECUTE sp\_configure 'Ad Hoc Distributed Queries', 0;

RECONFIGURE;

GO

EXECUTE sp\_configure 'show advanced options', 0;

RECONFIGURE;



De esta manera podemos desactivar la opción ad hoc distribute queries que evitará que remotamente se acceda al proveedor de datos desde fuentes externas e inseguras.

Referencia:

<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/ad-hoc-distributed-queries-server-configuration-option?view=sql-server-ver15>

1. Deshabilitar el uso de ensamblados CLR

Descripción:

Permitir el uso de ensamblados CLR amplía la superficie de ataque de SQL Server y lo

pone en riesgo de ensamblados maliciosos. Un ensamblado se empaqueta como un

archivo DLL o un ejecutable.

Hallazgo:

Con la ejecución del siguiente comando de SQL encontramos que por defecto la

ejecución de Ensamblados CLR viene desactivado

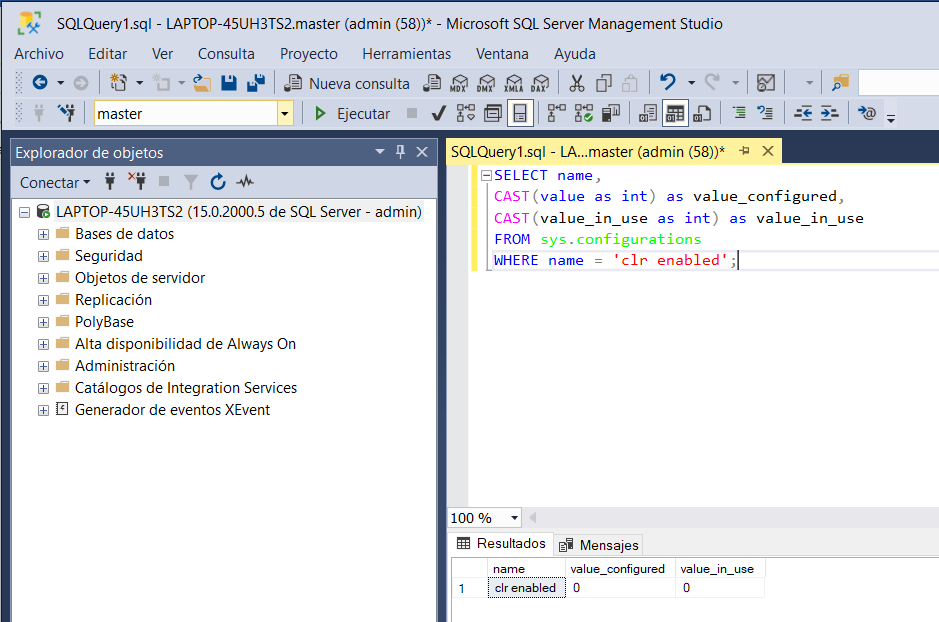
SELECT name,

CAST(value as int) as value\_configured,

CAST(value\_in\_use as int) as value\_in\_use

FROM sys.configurations

WHERE name = 'clr enabled';



Solución: Si la opción de ensamblado CLR se encontrara activada es necesario corregir esta configuración con el siguiente comando para desactivarlo:

EXECUTE sp\_configure 'clr enabled', 0;

RECONFIGURE;

Habilitar el uso de ensamblados CLR amplía la superficie de ataque de SQL Server y la pone en riesgo de ensamblajes tanto inadvertidos como maliciosos.

<https://docs.microsoft.com/en-us/sql/t-sql/statements/create-assembly-transact-sql?view=sql-server-ver15>

1. Asegúrarse de que la opción de configuración del servidor 'Cross DB Ownership Chaining' esté establecido en '0'

Descripción:Cuando está habilitada, esta opción permite que un miembro del rol db\_owner en una

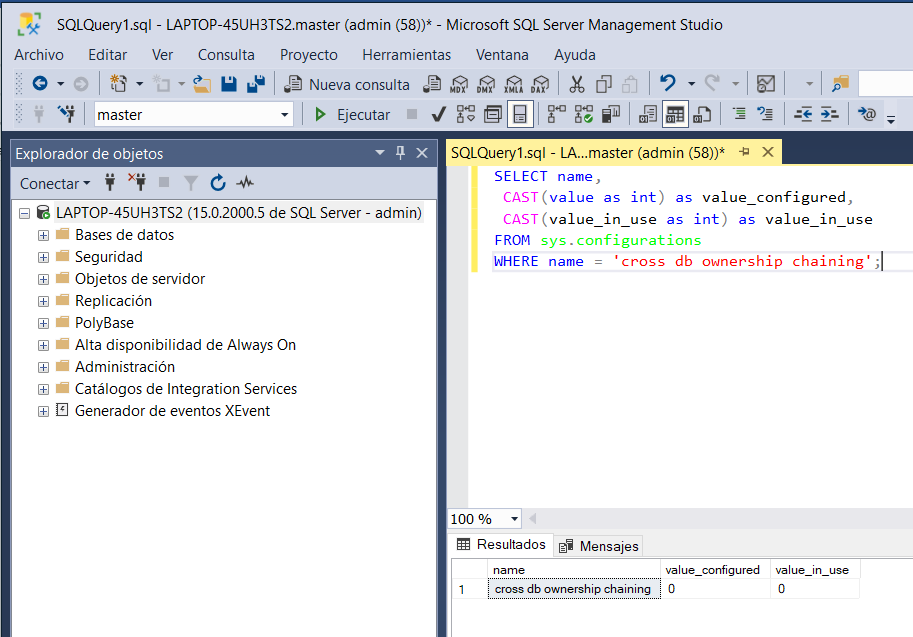
base de datos gane acceso a objetos que son propiedad de un inicio de sesión en cualquier otra base de datos, causando una innecesaria divulgación de información. Cuando sea necesario, el encadenamiento de propiedad entre bases de datos solo debe ser habilitado para las bases de datos específicas que lo requieren en lugar del nivel de instancia para todos las bases de datos, utilizando el comando ALTER DATABASE <database\_name>SET DB\_CHAINING ON se habilita para una base de datos en específico.

Hallazgo:

El rol de DB Owner para la base de datos está deshabilitado.

Con el comando SQL verificamos que se encuentre deshabilitado:

SELECT name, CAST(value as int) as value\_configured, CAST(value\_in\_use as int) as value\_in\_use FROM sys.configurations WHERE name = 'cross db ownership chaining';



En este caso se encuentra deshabilitado, pero en dado caso se encuentre habilitado se deberá deshabilitar con el comando:

EXECUTE sp\_configure 'cross db ownership chaining', 0;

RECONFIGURE;

GO

Referencia:

<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/cross-db-ownership-chaining-server-configuration-option?view=sql-server-ver15>

1. Asegúrese de que la opción de configuración del servidor 'Database Mail XPs' esté establecida en ‘0’

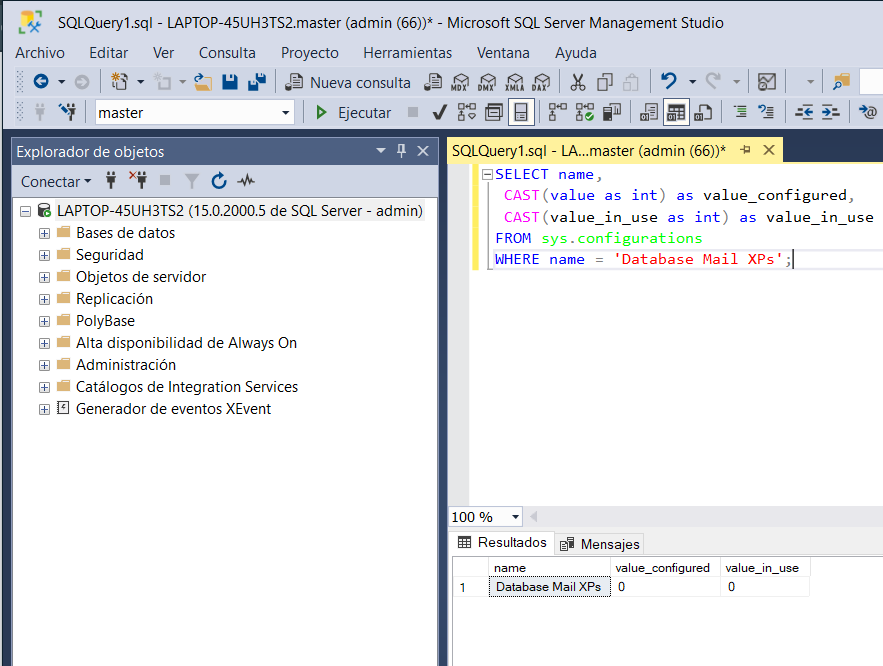
**Descripción:**

La opción Database Mail XPs controla la capacidad de generar y transmitir correo electrónico mensajes de SQL Server.

**Hallazgo:**

Deshabilitar la opción Database Mail XPs reduce la superficie de SQL Server, elimina un

DOS vectores de ataque y canal para filtrar datos del servidor de bases de datos a un host remoto.



Solución:

En nuestro caso la opción de Database Mail XPs se encontraba deshabilitada

por defecto, pero si es necesario remediar esta configuración se deberá ejecutar la siguiente sentencia de SQL.

EXECUTE sp\_configure 'show advanced options', 1;

RECONFIGURE; EXECUTE sp\_configure 'Database Mail XPs', 0;

RECONFIGURE;

GO EXECUTE sp\_configure 'show advanced options', 0;

RECONFIGURE;

Referencia:

<https://docs.microsoft.com/en-us/sql/relational-databases/database-mail/database-mail?view=sql-server-ver15>

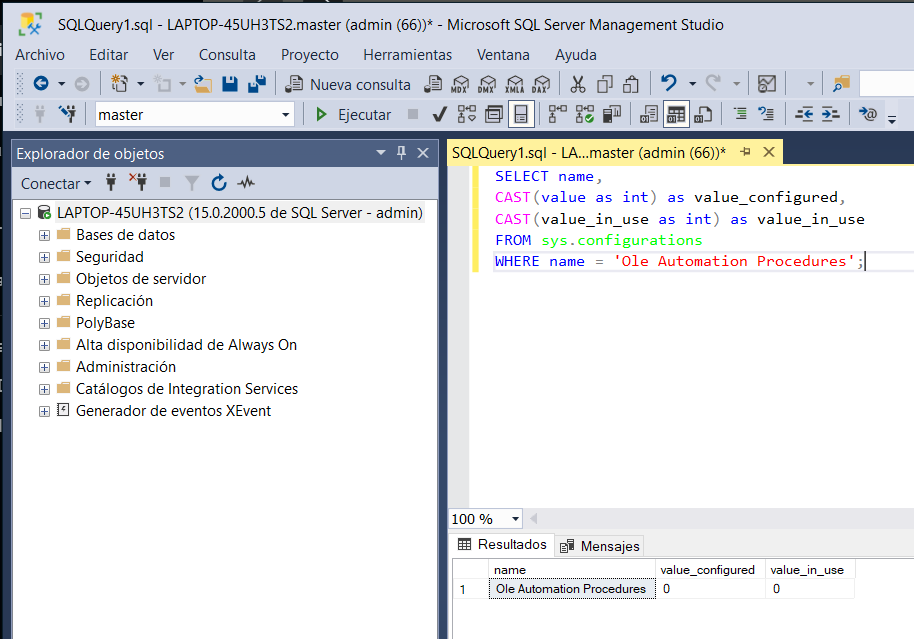
1. Asegúrese de que la opción de configuración del servidor 'Procedimientos de automatización de ole' esté establecido en '0'

**Descripción:**

La opción Procedimientos de automatización Ole controla si los objetos de automatización OLE pueden ser instanciado dentro de lotes de Transact-SQL. Estos son procedimientos almacenados extendidos que permiten Usuarios de SQL Server para ejecutar funciones externas a SQL Server.

Habilitar esta opción aumentará la superficie de ataque de SQL Server y permitirá a los

usuarios ejecutar funciones en el contexto de seguridad de SQL Server.



Solución:

De ser necesario activar o desactivar el procedimiento OLE Automation se debe ejecutar el siguiente comando SQL

EXECUTE sp\_configure 'show advanced options', 1;

RECONFIGURE;

EXECUTE sp\_configure 'Ole Automation Procedures', 0;

RECONFIGURE;

GO EXECUTE sp\_configure 'show advanced options', 0;

RECONFIGURE;

Referencia:

<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/ole-automation-procedures-server-configuration-option?view=sql-server-ver15>

1. Asegúrese de que la opción de configuración del servidor 'Acceso remoto' esté establecida en '0'.

**Descripción:**

La opción de acceso remoto controla la ejecución de procedimientos almacenados locales en remoto servidores o procedimientos almacenados remotos en el servidor local. Se puede abusar de la funcionalidad para lanzar un ataque de denegación de servicio (DoS) en servidores remotos descargando el procesamiento de consultas a un destino.

Hallazgos:

Con la ejecución del siguiente comando SQL encontramos que el acceso remoto está

habilitado.

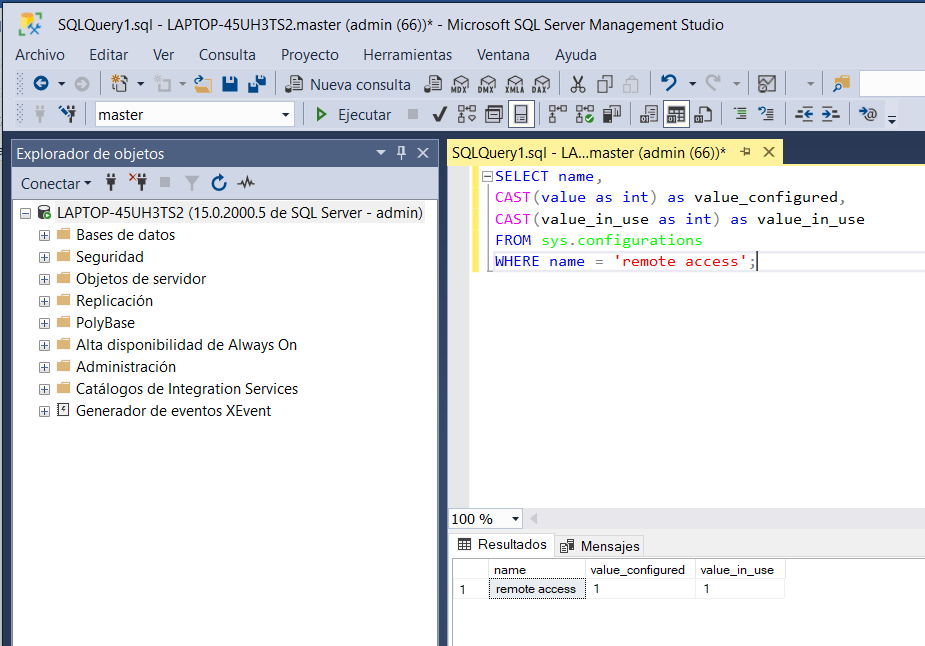
SELECT name,

CAST(value as int) as value\_configured,

CAST(value\_in\_use as int) as value\_in\_use

FROM sys.configurations

WHERE name = 'remote access';



Solución:

Para modificar la siguiente configuración es necesario ejecutar la siguiente línea de comandos SQL

EXECUTE sp\_configure 'show advanced options', 1;

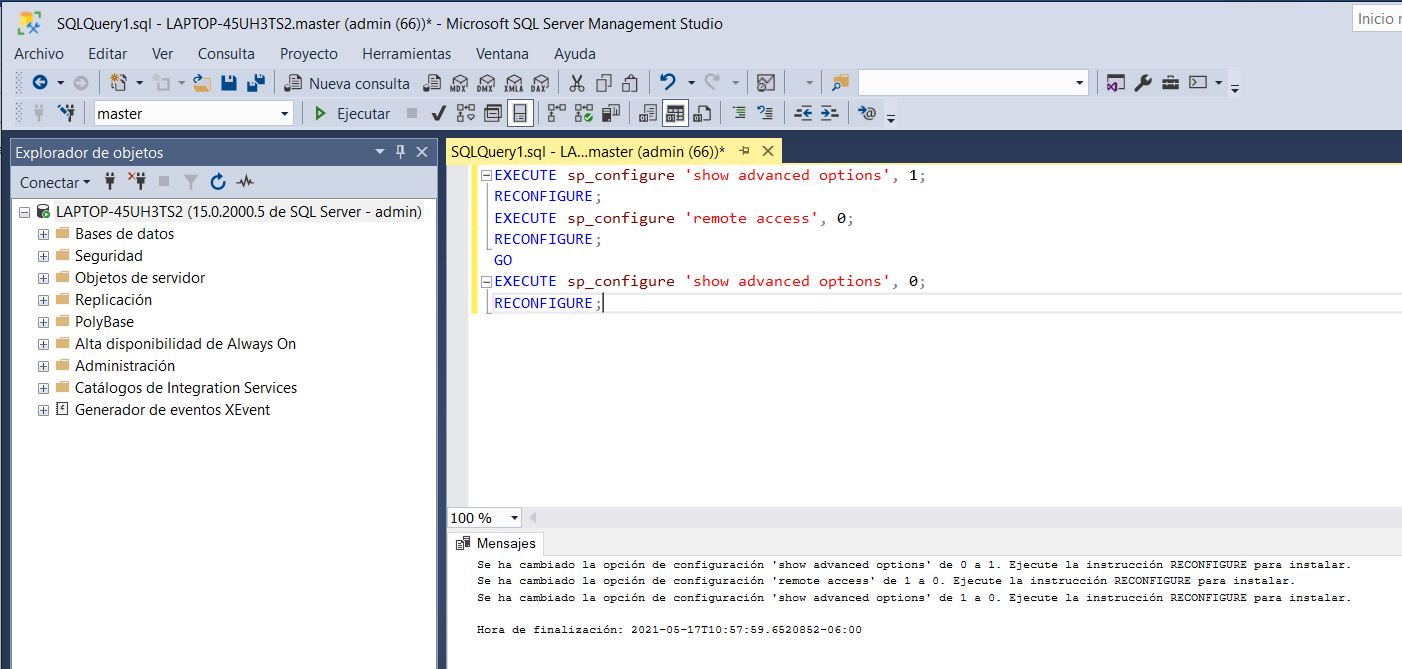
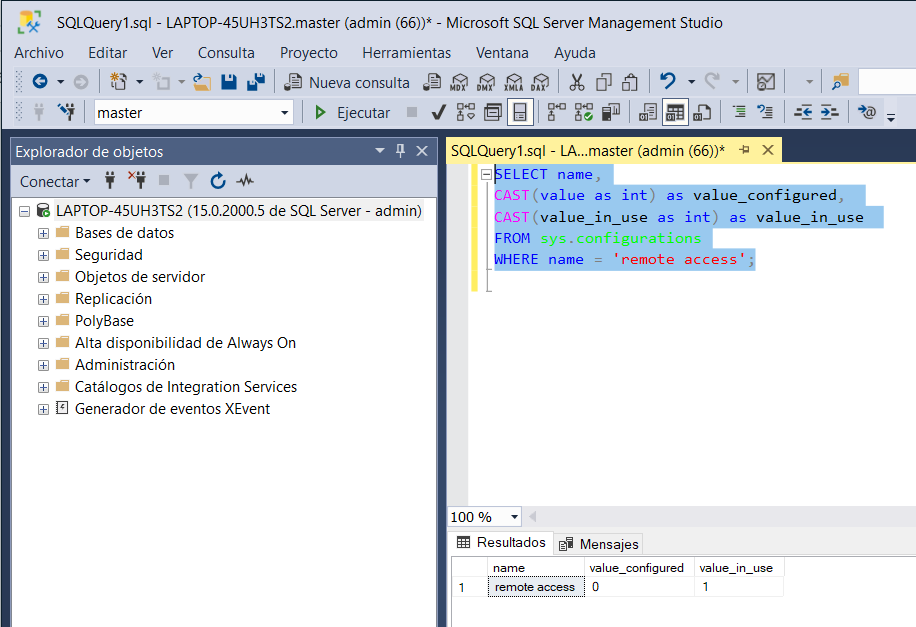
RECONFIGURE;

EXECUTE sp\_configure 'remote access', 0;

RECONFIGURE;

GO EXECUTE sp\_configure 'show advanced options', 0;

RECONFIGURE;



De esta manera deshabilitamos el acceso remoto.

La opción de acceso remoto controla la ejecución de procedimientos almacenados desde servidores locales o remotos en los que se ejecutan instancias de SQL Server.

Referencia:

<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-the-remote-access-server-configuration-option?view=sql-server-ver15>

1. Asegúrese de que la opción de configuración del servidor 'Conexiones de administración remota' esté establecido en '0'

La opción de conexiones de administrador remoto controla si una aplicación cliente en un remoto la computadora puede usar la Conexión de administrador dedicada (DAC). La conexión de administrador dedicada (DAC) permite a un administrador acceder a un servidor para ejecutar funciones de diagnóstico o declaraciones Transact-SQL, o para solucionar problemas, problemas en el servidor, incluso cuando el servidor está bloqueado o funcionando en un estado anormal y no responde a una conexión de motor de base de datos de SQL Server. En un escenario de clúster, Es posible que el administrador no haya iniciado sesión en el mismo nodo que aloja actualmente el Instancia de SQL Server y, por lo tanto, se considera "remota". Por lo tanto, esta configuración debería estar habilitado (1) para clústeres de conmutación por error de SQL Server; de lo contrario, debería estar deshabilitado (0) que es el valor por defecto.

USE master;

GO

SELECT name,

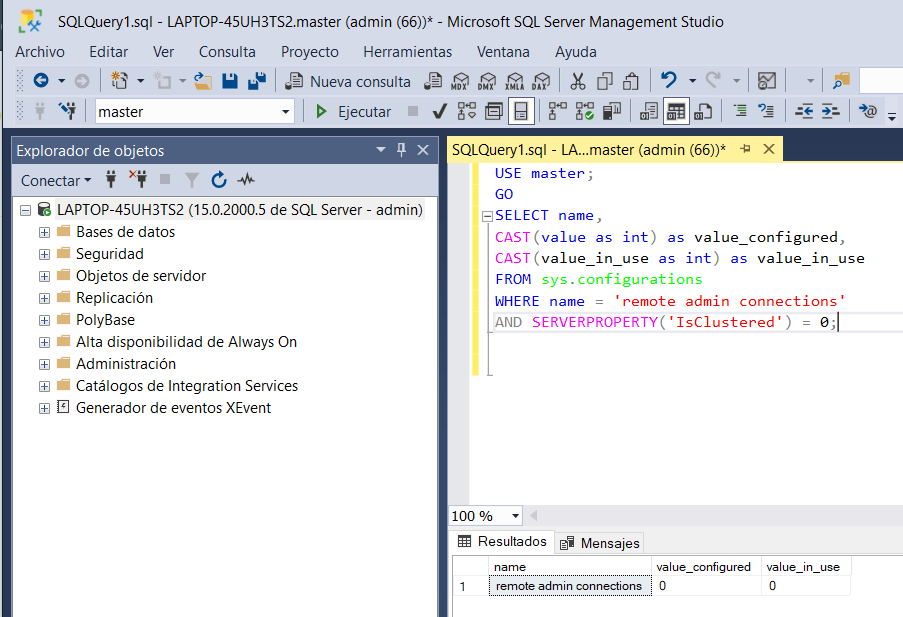
CAST(value as int) as value\_configured,

CAST(value\_in\_use as int) as value\_in\_use

FROM sys.configurations

WHERE name = 'remote admin connections'

AND SERVERPROPERTY('IsClustered') = 0;



**Hallazgo:**

En nuestro caso por defecto la conexión remota de administración se encuentra deshabilitada, si no fuera el caso es necesario ejecutar la siguiente consulta SQL para desactivar el acceso remoto

EXECUTE sp\_configure 'remote admin connections', 0;

RECONFIGURE;

GO

Información Adicional:

Si se trata de una instalación en clúster, esta opción debe estar habilitada ya que un SQL Server en clúster no puede enlazar a localhost y DAC no estará disponible de lo contrario. Habilítelo para agrupadas instalaciones. Deshabilítelo para instalaciones independientes donde no sea necesario.

Referencia:

<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/remote-admin-connections-server-configuration-option?view=sql-server-ver15>

1. Asegúrese de que la opción de configuración del servidor 'Buscar procesadores de inicio' esté configurada en '0'

Descripción:

La opción para buscar procesadores de inicio, si está habilitada, hace que SQL Server

busque y ejecute automáticamente todos los procedimientos almacenados que están

configurados para ejecutarse al iniciar el servicio.

Hacer cumplir este control reduce la amenaza de que una entidad aproveche estas

instalaciones para fines maliciososHallazgo:

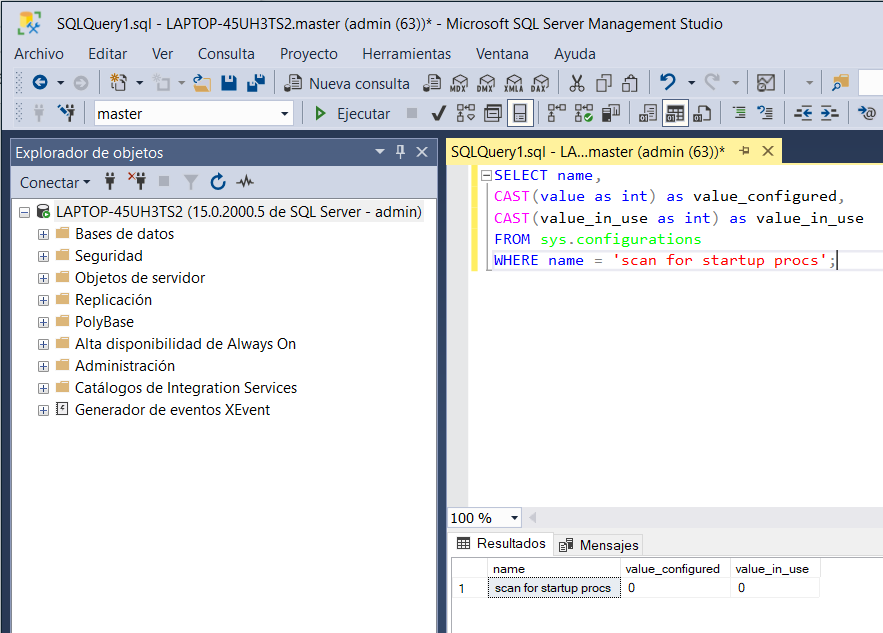
SELECT name,

CAST(value as int) as value\_configured,

CAST(value\_in\_use as int) as value\_in\_use

FROM sys.configurations

WHERE name = 'scan for startup procs';



Solución:

En nuestro caso los procesadores de inicio están configurados en '0', pero si no fuera el caso es necesario ejecutar el siguiente comando de SQL para remedar.

EXECUTE sp\_configure 'show advanced options', 1;

RECONFIGURE; EXECUTE sp\_configure 'scan for startup procs', 0;

RECONFIGURE; GO EXECUTE sp\_configure 'show advanced options', 0;

RECONFIGURE;

Referencia:

<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-the-scan-for-startup-procs-server-configuration-option?view=sql-server-ver15>

**HALLAZGOS, Y SOLUCIONES AL APLICAR HARDENING A LA BASE DE DATOS SQL SERVER**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | Aseguramiento (incluyendo sentencia) | Hallazgo (con evidencia) | Riesgo del hallazgo | Solución (con pasos de ejecución y evidencia) |
| 1. Instalar actualizaciones y parches de seguridad | Los parches de SQL Server contienen actualizaciones de programas que reparan la seguridad y la funcionalidad del producto. Estos parches se pueden instalar con una actualización que es un pequeño grupo de parches o un service pack. La versión de SQL Server y los niveles de parche deben de ser los más recientes.  Sentencia SQLserver para verificación de parches:  **SELECT SERVERPROPERTY('ProductLevel') as SP\_installed, SERVERPROPERTY('ProductVersion') as Version;** | La versión instalada es la última versión del producto disponible en el mercado a la fecha. | Ninguno. Tenemos instalada la última versión de SQL Server 2019 con sus service pack. | Es necesario buscar los parches más recientes de SQL Server y se pueden encontrar en el blog de Microsoft:   * Los parches más recientes de SQL Server:   <https://techcommunity.microsoft.com/t5/sql-server/bg-p/SQLServer/label-name/SQLReleases>   * Revisiones y actualizaciones acumulativas de SQL Server 2019:   <https://support.microsoft.com/es-es/topic/kb4527376-actualizaci%C3%B3n-acumulativa-1-para-sql-server-2019-a8dae09e-96b5-9f13-9092-977341fafe17> |
| 2. Deshabilitar Ad Hoc Distributed Queries | Las AD Hoc Distributed Queries permiten a los usuarios consultar datos y ejecutar declaraciones desde fuentes de datos externas. Habilitar su uso significa que cualquier inicio de sesión autenticado en SQL Server puede acceder al proveedor. Está funcionalidad debe estar deshabilitada.  **SELECT name, CAST(value as int) as value\_configured, CAST(value\_in\_use as int) as value\_in\_use FROM sys.configurations WHERE name = 'Ad Hoc Distributed Queries';** | Se encontró que las Distributed Queries se encontraban deshabilitadas. | El permitir accesos externos desde fuentes sospechosas implica un riesgo de seguridad mediante un ataque de inyección SQL. | En dado caso se encuentre habilitado la forma para solucionarlo es ejecutando el siguiente comando:  **EXECUTE sp\_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp\_configure 'Ad Hoc Distributed Queries', 0; RECONFIGURE; GO EXECUTE sp\_configure 'show advanced options', 0; RECONFIGURE;** |
| 3. Deshabilitar el uso de ensamblados CLR | Permitir el uso de ensamblados CLR amplía la superficie de ataque de SQL Server y lo pone en riesgo de ensamblados maliciosos.  Para verificar si está habilitado ejecutar el siguiente comando:  **SELECT name, CAST(value as int) as value\_configured, CAST(value\_in\_use as int) as value\_in\_use FROM sys.configurations WHERE name = 'clr enabled';** | Se encontró que los ensamblados CLR vienen desactivador por defecto. | Un ensamblado se empaqueta como un archivo DLL o un ejecutable, fácilmente podemos sufrir un ataque a nuestra base de datos, haciendouso de una librería infectada, un ejecutable descargado de internet, un virus o programa malicioso. Son muchos los vectores que se pueden aprovechar de esta vulnerabilidad. | En dado caso se encuentre habilitado el CLR para remediar esta configuración se ejecuta el siguiente comando  **EXECUTE sp\_configure 'clr enabled', 0; RECONFIGURE;** |
| 4. Deshabilitar el rol db\_owner | Cuando está habilitada, esta opción permite que un miembro del rol db\_owner en una base de datos gane acceso a objetos que son propiedad de un inicio de sesión en cualquier otra base de datos. | El rol de DB Owner para la base de datos está deshabilitado.  Para comprobar el estado se puede ejecutar el siguiente comando:  **Select name, CAST (value as int) as value\_configured,CAST(valu e\_in\_use as int) as value\_in\_use FROM sys.configurations WHERE name = ‘cross db ownership chaining’** | Un usuario con un rol de visita no propietario o administrador del equipo podría heredar accesos a otras bases de datos innecesariamente. Es mejor eliminar este usuario de las instancias. | En dado caso se encontrará habilitado para remediar esta configuración se ejecutando el siguiente comando para deshabilitarlo.  **EXECUTE sp\_configure ‘cross db ownership chaining’ , 0; RECONFIGURE; GO** |
| 5. Asegúrese de que la opción de configuración del servidor  'Database Mail XPs' esté configurada en '0' | La opción Database Mail XPs controla la capacidad de generar y transmitir mensajes de correo electrónico de SQL Server. | En nuestro caso la opción de Database Mail XPs se encontraba deshabilitada.  Para verificar si está o no activa con el comando siguiente se puede comprobar de la siguiente manera:  **SELECT name,CAST(value as int) as value\_configured,CAST(valu e\_in\_use as int) as value\_in\_use FROM sys.configurations WHERE name = ‘DATABASE MAIL XPs’** | Deshabilitar la opción Database Mail XPs reduce la posibilidad de sufrir un ataque DOS del servidor de bases de datos a un host remoto. | En algún caso se encuentre habilitada esta acción para remediar esta configuración se ejecutando el siguiente comando.  **EXECUTE sp\_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp\_configure 'Database Mail XPs', 0; RECONFIGURE; GO EXECUTE sp\_configure 'show advanced options', 0; RECONFIGURE;** |
| 6. Asegúrese de que la opción de configuración del servidor 'Procedimient os de automatización de Ole' sea establecido en '0' | La opción Procedimientos de automatización Ole controla si los objetos OLE pueden ser instanciado dentro de lotes de Transact-SQL. Estos son procedimientos almacenados extendidos que permiten Usuarios de SQL Server para ejecutar funciones externas a SQL Server.  Para evaluar esta recomendación, ejecute el siguiente comando:  **SELECT name, CAST(value as int) as value\_configured, CAST(value\_in\_use as int) as value\_in\_use FROM sys.configurations WHERE name = 'OleAutomation Procedures';** | Encontramos que por defecto en SQL Server 2019 esta opción se encuentra deshabilitada. | Si estos procesos OLE se encontraran activados en nuestra base de datos por defecto, se corre el riesgo que sea infectado uno de los procesos. Al ser procesos que se ejecutan automáticamente, algunos para mantenimiento y otros que activan funciones avanzadas para las consultas de base de datos, existe la posibilidad de una intrusión. | En algún caso se encuentre habilitada esta acción para remediar esta configuración se ejecutando el siguiente comando.  **EXECUTE sp\_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp\_configure 'Ole Automation Procedures', 0; RECONFIGURE; GO**  **EXECUTE sp\_configure 'show advanced options', 0; RECONFIGURE;** |
| 7. Asegúrese de que la opción de configuración del servidor 'Acceso remoto' esté configurada en '0' | La opción de acceso remoto controla la ejecución de procedimientos almacenados locales en remoto servidores o procedimientos almacenados remotos en el servidor local. | Esta configuración se encuentra activada por defecto en SQL Server 2019, es necesario remedar. | Se puede abusar de la funcionalidad para lanzar un ataque de denegación de servicio (DoS) en servidores remotos descargando el procesamiento de consultas. | Para corregir esta configuración se ejecutando el siguiente comando:  **EXECUTE sp\_configure 'show advanced options', 1; RECONFIGURE; EXECUTE sp\_configure 'remote access', 0; RECONFIGURE; GO EXECUTE sp\_configure 'show advanced options', 0; RECONFIGURE;** |
| 8. Asegúrese de que la opción de configuración del servidor 'Conexiones de administración remota' sea establecido en '0' | La opción de conexiones de administrador remoto controla si una aplicación cliente puede usar la Conexión de administrador dedicada (DAC). | La conexión de administrador dedicado (DAC) permite que un administrador acceda a un servidor para ejecutar funciones de diagnóstico o instrucciones Transact-SQL, o para solucionar problemas para ver el estado de esta configuración utilice la siguiente línea de comando:  **USE master; GO SELECT name, CAST(value as int) as value\_configured, CAST(value\_in\_use as int) as value\_in\_use FROM sys.configurations WHERE name = 'remote admin connections' AND SERVERPROPERTY('IsCluster ed') = 0;** | En nuestro caso por defecto la conexión remota de administración se encuentra deshabilitada, y esto nos garantiza que remotamente un administrador no podrá ejecutar un comando T-SQL. | En nuestro caso por defecto la conexión remota de administración se encuentra deshabilitada, si no fuera el caso es necesario ejecutar la siguiente consulta SQL para desactivar el acceso remoto  **EXECUTE sp\_configure 'remote admin connections', 0;**  **RECONFIGURE;**  **GO** |
| 9. Asegúrese de que la opción de configuración del servidor 'Buscar procesadores de inicio' esté configurada en '0' | La opción para buscar procesadores de inicio, si está habilitada, hace que SQL Server busque y ejecute automáticamente todos los procedimientos almacenados que están configurados para ejecutarse al iniciar el servidor.  **SELECT name, CAST(value as int) as value\_configured, CAST(value\_in\_use as int) as value\_in\_use FROM sys.configurations WHERE name = 'scan for startup procs';** | Se encontró que SQL Server 2019 trae deshabilitada esta opción. Lo que aumenta nuestra seguridad. | Un servidor SQL Server se podría ver comprometido con algún tipo de virus como una bomba de tiempo, o algún software malicioso que infecte algunos archivos de inicio. El virus puede estar residente en el equipo y tras un reinicio, una actualización o alguna acción que reinicio el servidor, se puede ejecutar un procedimiento de inicio infectado y dañar la base de datos. | En nuestro caso los procesadores de inicio están configurados en '0', pero si no fuera el caso es necesario ejecutar el siguiente comando de SQL para remedar.  **EXECUTE sp\_configure 'show advanced options', 1;**  **RECONFIGURE; EXECUTE sp\_configure 'scan for startup procs', 0;**  **RECONFIGURE; GO EXECUTE sp\_configure 'show advanced options', 0;**  **RECONFIGURE;** |
| 10. El uso de un puerto no predetermina do ayuda a proteger la base de datos de los ataques dirigidos al predetermina do | SQL MANAGEMENT CONSOLE es una interfaz gráfica que nos permite realizar ciertas configuraciones facilitándonos algunas tareas de personalización de la base de datos. El puerto por defecto de SQL Server es el 1433 | De manera predeterminada el puerto por el cual responde y corre el servicio de SQL Server es el 1433 | Es importante cambiar este puerto y asignar un puerto dedicado, el cual le causara complicaciones a un atacante.  **DECLARE @value nvarchar(256); EXECUTE master.dbo.xp\_instance\_regread N'HKEY\_LOCAL\_MACHINE', N'SOFTWARE\Microsoft\Microsoft SQL Server\MSSQLServer\SuperSocketNet Lib\Tcp\IPAll', N'TcpPort', @value OUTPUT, N'no\_output'; SELECT @value AS TCP\_Port WHERE @value = '1433';** | Remediar esta configuración ejecutando el siguiente comando 1. En el Administrador de configuración de SQL Server, en el panel de la consola, expanda SQL Server Configuración de red, expanda Protocolos para y luego haga doble clic el protocolo TCP /IP 2. En el cuadro de diálogoPropiedades de TCP / IP, en la pestaña Direcciones IP, varias direcciones IP aparecen en el formato IP1, IP2, hasta IPAll. Uno de estos es para la dirección IP del adaptador bucle invertido, 127.0.0.1. Aparecen direcciones IP adicionales para cada dirección IP en el ordenador. |
|  |  |  |  |  |

***use [master]***

***GO***

***ALTER LOGIN sa DISABLE;***

***ALTER LOGIN sa WITH NAME = [SQLsa]***

Si se quiere mantener el usuario 'sa' una buena práctica es cambiar el nombre y agregarle un password fuerte.

**Recomendaciones**

**Cambiar el nombre del usuario ‘sa’ y asegurarla con una contraseña fuerte o desactivar el usuario.**

**Usar grupos de usuarios y trabajar permisos por grupo y no por usuario.**

**Cambiar el puesto por defecto del gestor de bases de datos.**

**Deshabilitar el SQL Browser y cualquier otro servicio innecesario.**

**Habilitar el uso de ‘forzar cifrado’ lo cual habilita protocolos de SSL.**

**Encriptar los backups y aplicar certificados digitales al servidor de bases de datos.**

Se puede determinar que una instalación por defecto sin importar el tipo de producto o base de datos adquirido no tiene la suficiente seguridad. Una instalación por defecto está hecha para poner a trabajar un servidor casi de manera inmediata con una instalación simple, es posible que para iniciar un ambiente de pruebas podría ser esta una gran ventaja o para estudiantes que se inician en este mundo de las bases de datos; pero definitivamente son un riesgo para un ambiente de producción.

Por ello es importante aplicar medidas para una mejor seguridad, una de las mejores alternativas es aplicar hardening lo cual en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo. Su propósito, entorpecer la labor del atacante y ganar tiempo para poder minimizar las consecuencias de un inminente incidente de seguridad e incluso, en algunos casos, evitar que éste se concrete en su totalidad.

Como conclusión, el Hardening es una ayuda indispensable para ahorrarse bastantes dolores de cabeza por parte de los administradores de sistemas. Entre sus ventajas, se puede contar la disminución por incidentes de seguridad, mejoras en el rendimiento al disminuir niveles de carga inútil en el sistema, una administración más simple y mayor rapidez en la identificación de problemas, ya que muchas de las posibles causas de ellos quedarán descartadas en virtud de las medidas tomadas, y finalmente la posibilidad de poder hacer un seguimiento de los incidentes y en algunos casos identificar el origen de los mismos. Además, podemos concluir que sin importar el tipo de base de datos todas cuentan con una configuración adicional mediante una Terminal, Shell, una GUI, un script que nos ayudaran a aplicar los controles de hardening que nos permiten personalizar la instalación el cual es un trabajo que debe hacerse para minimizar los riesgos y mejorar la seguridad en los gestores de base de datos.