Habilitación de la autenticación de bases de datos SQL

Dos componentes de cada base de datos segura son la autenticación y la autorización.

Por **autenticación** se entiende el proceso según el cual se demuestra que el usuario es quien dice ser. Un usuario se conecta a una base de datos a través de una cuenta de usuario. Cuando un usuario intenta conectarse a una base de datos, proporciona una cuenta de usuario y la información de autenticación. El usuario se autentica con uno de los dos métodos de autenticación siguientes:

- **Autenticación de SQL**: con este método de autenticación, el usuario envía un nombre de cuenta de usuario y una contraseña asociada para establecer una conexión. Esta contraseña se almacena en la base de datos maestra de cuentas de usuario vinculadas a un inicio de sesión, o bien en la base de datos que contiene las cuentas de usuario no vinculadas a un inicio de sesión.
- **Autenticación de Azure Active Directory**: con este método de autenticación, el usuario envía un nombre de cuenta de usuario y solicita que el servicio use la información de credenciales almacenada en Azure Active Directory.

Puede crear cuentas de usuario en la base de datos maestra y conceder permisos en todas las bases de datos del servidor, o bien puede crearlas en la propia base de datos (denominadas "usuarios de base de datos independiente"). Mediante el uso de bases de datos independientes, se obtiene una mejor portabilidad y escalabilidad.

Inicios de sesión y usuarios: En Azure SQL, una cuenta de usuario en una base de datos puede estar asociada a un inicio de sesión que está almacenado en la base de datos maestra, o bien puede ser un nombre de usuario que está almacenado en una base de datos individual.

- Un **inicio de sesión** es una cuenta individual en la base de datos maestra que se puede vincular a una cuenta de usuario en una o más bases de datos. Con un inicio de sesión, la información de credenciales de la cuenta de usuario se almacena en el propio inicio de sesión.
- Una **cuenta de usuario** es una cuenta individual en una base de datos que puede estar vinculada a un inicio de sesión, si bien esto no es obligatorio. En el caso de una cuenta de usuario que no está vinculada a un inicio de sesión, la información de las credenciales se almacena con la cuenta de usuario.

La **autorización** para acceder a los datos y realizar diversas acciones se administran con roles de base de datos y permisos explícitos. El término autorización hace referencia a los permisos asignados a un usuario, y determina qué puede hacer ese usuario. La autorización se controla por medio de las pertenencias a roles y los permisos de nivel de objeto de la base de datos de la cuenta de usuario. Como procedimiento recomendado, debe conceder a los usuarios los privilegios mínimos necesarios. Como procedimiento recomendado, su aplicación debe usar una cuenta dedicada para autenticarse. De esta manera, puede limitar los permisos concedidos a la

aplicación y reducir los riesgos de actividad malintencionada en caso de que el código de aplicación sea vulnerable a ataques de inyección SQL. Se recomienda crear un usuario de base de datos independiente, ya que esto permitirá que la aplicación se autentique directamente en la base de datos.

importante

Use la autenticación de Azure Active Directory para administrar identidades de usuarios de base de datos de forma centralizada y como alternativa a la autenticación de SQL Server.

Configuración de firewalls de base de datos SQL

Inicie el proceso de seguridad de la base de datos mediante la configuración de base de datos SQL.

Azure SQL Database y Azure Synapse Analytics, anteriormente SQL Data Warehouse (ambos denominados "SQL Database" en esta lección) proporcionan un servicio de base de datos relacional para Azure y otras aplicaciones basadas en Internet. Para ayudar a proteger los datos, los firewalls impiden todo acceso al servidor de bases de datos, excepto a aquellos equipos a los que haya concedido permiso. Asimismo, otorgan acceso a las bases de datos según la dirección IP de origen de cada solicitud.

Además de las reglas de IP, el firewall también administra reglas de red virtual. Las reglas de red virtual se basan en los puntos de conexión de servicio de red virtual. Es posible que las reglas de red virtual sean preferibles a las reglas de IP en algunos casos.

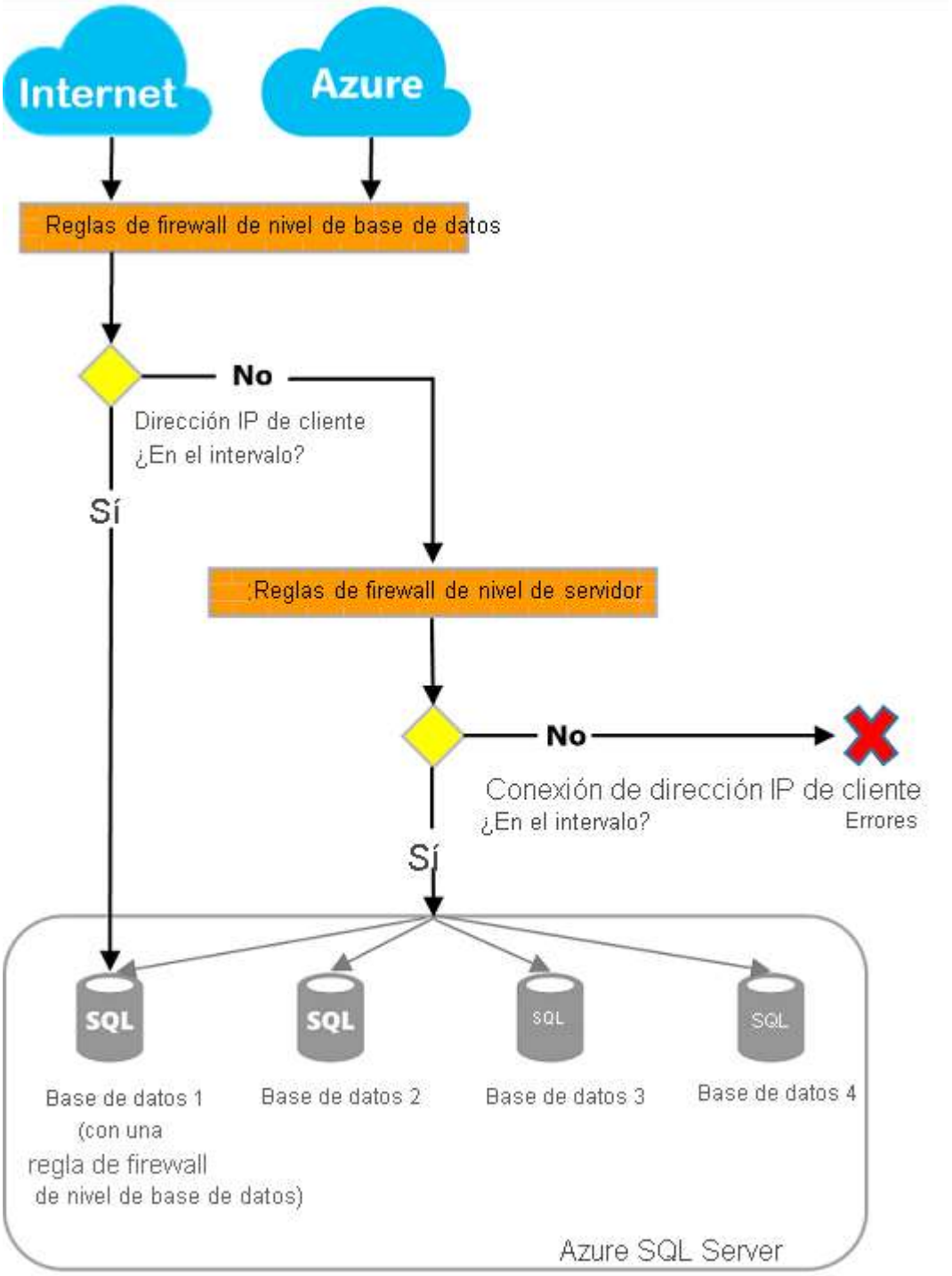
Información general

Inicialmente, todo el acceso público a su instancia de Azure SQL Database está bloqueado por el firewall de SQL Database. Para acceder a un servidor de bases de datos, debe especificar una o varias reglas de firewall de IP de nivel de servidor que permitan acceder a Azure SQL Database. Use las reglas de firewall de IP para especificar qué intervalos de direcciones IP de Internet se permiten y si las aplicaciones de Azure pueden tratar de conectarse a Azure SQL Database.

Para conceder acceso de forma selectiva a solo una de las bases de datos de su Azure SQL Database, debe crear una regla de nivel de base de datos para la base de datos necesaria. Especifique un intervalo de direcciones IP para la regla de firewall de IP de base de datos que quede fuera del intervalo de direcciones IP especificado en la regla de firewall de IP de nivel de servidor. Además, asegúrese de que la dirección IP del cliente se encuentre en el intervalo especificado en la regla de nivel de base de datos.

Nota

Azure Synapse Analytics solo es compatible con las reglas de firewall de IP de nivel del servidor y no lo es con las de nivel de base de datos.


Internet
Azure
Reglas de firewall de nivel de base de datos
No
Dirección IP de cliente
¿En el intervalo?
Sí
Reglas de firewall de nivel de servidor
No
Conexión de dirección IP de cliente
¿En el intervalo?
Errores
Sí
SQL
SQL
SQL
SQL
Base de datos 1
(con una
regla de firewall
de nivel de base de datos)
Base de datos 2
Base de datos 3
Base de datos 4
Azure SQL Server

Conexión desde Internet

Cuando un equipo intenta conectarse al servidor de bases de datos desde Internet, el firewall comprueba primero la dirección IP de origen de la solicitud con las reglas de firewall de IP de nivel de base de datos para la base de datos que solicita la conexión:

- Si la dirección IP de la solicitud se encuentra dentro de uno de los intervalos especificados en las reglas de firewall de IP de nivel de base de datos, la conexión se concede a la base de datos SQL que contiene la regla.
- Si la dirección IP de la solicitud no está dentro de uno de los intervalos especificados en las reglas de firewall de IP de nivel de base de datos, el firewall comprueba las reglas de firewall de IP de nivel de servidor. Si la dirección IP de la solicitud está comprendida en uno de los intervalos especificados en las reglas de firewall de IP de nivel de servidor, la conexión se concede. Las reglas de firewall de IP de nivel de servidor se aplican a todas las bases de datos SQL de Azure SQL Database.
- Si la dirección IP de la solicitud no se encuentra dentro de los intervalos especificados en cualquiera de las reglas de firewall de IP de nivel de base de datos o de servidor, la solicitud de conexión genera un error.

Conexión desde Azure

Para permitir que las aplicaciones de Azure se conecten a Azure SQL Database, las conexiones de Azure deben estar habilitadas. Cuando una aplicación desde Azure intenta conectarse a su servidor de s de datos, el firewall comprueba que se permiten las conexiones de Azure. Una configuración del firewall con una dirección inicial y final igual a 0.0.0.0 indica que se permiten las conexiones de Azure. Si no se permite el intento de conexión, la solicitud no alcanza el servidor de Azure SQL Database.

Esta opción configura el firewall para permitir todas las conexiones de Azure, incluidas las de las suscripciones de otros clientes. Al seleccionar esta opción, asegúrese de que los permisos de usuario y el inicio de sesión limiten el acceso solamente a los usuarios autorizados.

Reglas de firewall de IP en el nivel de servidor

Las reglas de firewall de IP de nivel de servidor permiten a los clientes acceder a toda la Azure SQL Database, es decir, todas las bases de datos dentro del mismo servidor de base de datos SQL. Estas reglas se almacenan en la base de datos maestra.

Puede configurar reglas de firewall de IP de nivel de servidor mediante Azure Portal, PowerShell o mediante instrucciones Transact-SQL. Para poder crear reglas de firewall de IP de nivel de servidor mediante Azure Portal o PowerShell, debe ser el propietario o un colaborador de la suscripción. Para crear una regla de firewall de IP de nivel de servidor mediante Transact-SQL, debe conectarse a la instancia de SQL Database como inicio de sesión de entidad de seguridad de nivel de servidor o administrador de Azure Active Directory (Azure AD), lo que significa que un usuario debe haber creado primero una regla de firewall de IP de nivel de servidor con permisos de nivel de Azure.

Reglas de firewall de IP en el nivel de base de datos

Las reglas de firewall de IP de nivel de base de datos permiten a los clientes acceder a determinadas bases de datos seguras dentro del mismo servidor de base de datos SQL. Puede crear estas reglas para cada base de datos (incluida la base de datos maestra) y se almacenan en las bases de datos individuales. Solo puede crear y administrar reglas de firewall de IP de nivel de base de datos para bases de datos maestras y bases de datos de usuario mediante instrucciones Transact-SQL y solo después de haber configurado el primer firewall de nivel de servidor. Si especifica un intervalo de direcciones IP en la regla de firewall de IP de nivel de base de datos que se encuentra fuera del intervalo especificado en la regla de firewall de IP de nivel de servidor, solo los clientes que tengan direcciones IP en el intervalo de nivel de base de datos pueden tener acceso a la base de datos. Puede tener un máximo de 128 reglas de firewall de IP de nivel de base de datos para una base de datos.

Importante

Como procedimiento recomendado, use reglas de firewall de IP de nivel de base de datos siempre que sea posible con el fin de mejorar la seguridad y aumentar la portabilidad de la base de datos. Use reglas de firewall de IP de nivel de servidor para administradores y cuando tenga varias bases de datos con los mismos requisitos de acceso y no quiera dedicar tiempo a configurar individualmente cada una de ellas.

Habilitación y supervisión de la auditoría de bases de datos

La auditoría para Azure SQL Database y Azure Synapse Analytics realiza el seguimiento de eventos de base de datos y los escribe en un registro de auditoría en la cuenta de Azure Storage, el área de trabajo de Log Analytics o Event Hubs.

La auditoría también puede hacer lo siguiente:

- Ayudar a mantener el cumplimiento de normativas, comprender la actividad de las bases de datos y conocer las discrepancias y anomalías que pueden indicar problemas en el negocio o infracciones de seguridad sospechosas.
- Posibilita y facilita la observancia de estándares reguladores **aunque no garantiza el cumplimiento**.

Información general

Puede usar la auditoría de base de datos SQL para:

- **Conservar** una traza de auditoría de eventos seleccionados. Puede definir categorías de acciones de base de datos para auditar.
- **Informar** sobre la actividad de la base de datos. Puede usar informes preconfigurados y un panel para dar los primeros pasos más rápido con el informe de actividades y eventos.

- **Analizar** informes. Puede buscar eventos sospechosos, actividades inusuales y tendencias.

Definir la directiva de auditoría de nivel de servidor frente la de nivel de base de datos

Puede definirse una directiva de auditoría para una base de datos específica o como directiva de servidor predeterminada:

- Una directiva de servidor se aplica a todas las bases de datos recién creadas en el servidor.
- Si la auditoría de servidor está habilitada, se aplica siempre a la base de datos. La base de datos se auditará, independientemente de la configuración de auditoría de la base de datos.
- Habilitar la auditoría en la base de datos o el almacenamiento de datos, además de en el servidor, no invalida ni cambia ninguno de los valores de configuración de la auditoría de servidor. Ambas auditorías existirán en paralelo. En otras palabras, la base de datos se auditará dos veces en paralelo; una vez por la directiva de servidor y otra vez por la directiva de base de datos.

  A continuación se muestra la configuración de la auditoría mediante Azure Portal.

Resumen de la auditoría de base de datos

- Conservación de una pista de auditoría de eventos seleccionados
- Informe sobre la actividad de la base de datos y análisis de resultados
- Configuración de directivas para el nivel de servidor o base de datos
- Configuración del destino del registro de auditoría
- Una nueva directiva de servidor se aplica a todas las bases de datos existentes y recién creadas

---

Implementación de la detección y clasificación de datos

Detección y clasificación de datos se integra en Azure SQL Database. Ofrece funcionalidades avanzadas para detectar, clasificar, etiquetar e informar de los datos confidenciales de las bases de datos.

Los datos más confidenciales pueden incluir información empresarial, financiera, sanitaria o personal. La detección y clasificación de estos datos puede representar un rol fundamental en el enfoque de la protección de la información de la organización. Puede servir como infraestructura para lo siguiente:

- Ayudar a satisfacer los estándares de privacidad de datos y los requisitos de cumplimiento normativo.
- Varios escenarios de seguridad, como la supervisión (auditoría) y las alertas relacionadas con accesos anómalos a información confidencial.
- Controlar el acceso y mejorar la seguridad de las bases de datos que contienen información altamente confidencial.

La clasificación y detección de datos forma parte de la oferta de Advanced Data Security. Dicha oferta es un paquete unificado de funcionalidades avanzadas de seguridad de SQL. Puede acceder y administrar la detección y clasificación de datos desde la sección central **Advanced Data Security de SQL** de Azure Portal.

Clasificar los datos e identificar cuáles son sus necesidades de protección de datos ayuda a seleccionar la solución en la nube adecuada en su organización. La clasificación de datos permite a las organizaciones encontrar optimizaciones de almacenamiento que podrían no ser posibles cuando todos los datos tienen asignado el mismo valor. La clasificación (o categorización) de los datos almacenados por confidencialidad e impacto de negocio permite a las organizaciones determinar los riesgos inherentes a los datos. Una vez clasificados los datos, las organizaciones pueden administrarlos de manera que reflejen su valor interno, en lugar de tratarlos todos de la misma forma.

La clasificación de datos puede ofrecer ventajas como la eficiencia del cumplimiento, mejores formas de administrar los recursos de la organización y una migración a la nube más sencilla. Algunas soluciones de protección de datos, como el cifrado, Rights Management y la prevención de pérdida de datos, se han trasladado a la nube y contribuyen a mitigar los riesgos en la nube. Con todo, cuando decidan pasar a la nube, las organizaciones deben procurar contemplar las reglas de clasificación de datos relativas a la retención de datos.

Los datos se encuentran en uno de estos tres estados: en **reposo**, en **proceso** y en **tránsito**. Los tres estados requieren soluciones técnicas únicas de clasificación de datos, pero los principios aplicados deben ser los mismos en todos ellos. Los datos clasificados como confidenciales deben mantenerse confidenciales cuando están en reposo, en proceso o en tránsito.

Los datos pueden ser además **estructurados** o **no estructurados**. Los procesos típicos de clasificación de los datos estructurados que se encuentran en bases de datos y hojas de cálculo son de menor complejidad, y se dedica menos tiempo a administrarlos en comparación con los datos no estructurados, como documentos, código fuente y correos electrónicos. Por lo general, las organizaciones tendrán más datos no estructurados que estructurados.

Independientemente de si los datos están estructurados o no estructurados, es importante que las organizaciones administren la confidencialidad de los datos. Cuando se implementa correctamente, la clasificación de datos ayuda a garantizar que los datos

confidenciales o sensibles se administran con mayor supervisión que los recursos de datos considerados como de distribución pública.

Protección de los datos en reposo

El cifrado de datos en reposo es un paso obligatorio en lo que respecta a la privacidad de los datos, el cumplimiento y la soberanía de los datos.

Procedimiento recomendado	Solución
Cifrar los discos para ayudar a proteger los datos	Use Microsoft Azure Disk Encryption, que permite a los administradores de TI cifrar discos de infraestructura como servicio (IaaS) de Windows y discos de máquina virtual IaaS de Linux. Disk Encryption combina la característica BitLocker estándar del sector y la característica DM-Crypt de Linux para facilitar el cifrado de volumen en el sistema operativo y los discos de datos. Azure Storage y Azure SQL Database cifran los datos en reposo de forma predeterminada, y muchos servicios ofrecen el cifrado como opción. Puede usar Azure Key Vault para mantener el control de las claves que se usan para acceder a los datos y cifrarlos.

Las organizaciones que no aplican el cifrado de datos se arriesgan a estar más expuestas a problemas de integridad de los datos. Por ejemplo, un usuario no autorizado o un hacker malintencionado pueden robar datos de las cuentas en peligro u obtener acceso no autorizado a los datos codificados en ClearFormat. Para cumplir las normativas del sector, las empresas también tienen que demostrar que son diligentes y que usan los controles adecuados para mejorar la seguridad de los datos.

Protección de los datos en tránsito

La protección de los datos en tránsito debe ser una parte esencial de su estrategia de protección de datos. Puesto que los datos se desplazan entre muchas ubicaciones, la recomendación general es utilizar siempre los protocolos SSL/TLS para intercambiar datos entre diferentes ubicaciones. En algunas circunstancias, es posible que desee aislar el canal de comunicación completo entre infraestructura local y en la nube mediante una VPN.

En relación con los datos que se desplazan entre la infraestructura local y Azure, plantee usar medidas de seguridad apropiadas, como HTTPS o VPN. Al enviar tráfico cifrado entre una instancia de Azure Virtual Network y una ubicación local a través de Internet público, use Azure VPN Gateway.

En la siguiente tabla figuran los procedimientos recomendados específicos para usar Azure VPN Gateway, SSL/TLS y HTTPS.

Procedimiento recomendado	Solución
Proteger el acceso a una red virtual de Azure desde varias estaciones de trabajo situadas en el entorno local	Use VPN de sitio a sitio.
Proteger el acceso a una red virtual de Azure desde una estación de trabajo situada en el entorno local	Use VPN de punto a sitio.
Mover los conjuntos de datos grandes a través de un vínculo de red de área extensa (WAN) de alta velocidad dedicado	Use Azure ExpressRoute. Si decide usar ExpressRoute, también puede cifrar los datos en el nivel de aplicación mediante SSL/TLS u otros protocolos para lograr una mayor protección.
Interactuar con Azure Storage a través de Azure Portal	Todas las transacciones se realizan a través de HTTPS. También se puede usar la API REST de almacenamiento a través de HTTPS para interactuar con Azure Storage y Azure SQL Database.

Las organizaciones que no protegen los datos en tránsito son más susceptibles a los ataques de tipo "Man in the middle", a la interceptación y al secuestro de sesión. Estos ataques pueden ser el primer paso para obtener acceso a datos confidenciales.

Ahora que hemos cubierto los aspectos físicos de la clasificación de datos, echemos un vistazo a la clasificación basada en la detección y clasificación.

Detección de datos

La clasificación y detección de datos facilitan funcionalidades avanzadas integradas en Azure SQL Database para detectar, clasificar, etiquetar y proteger la información confidencial (como los datos personales o la información de carácter empresarial o financiero) contenida en las bases de datos. La búsqueda y clasificación de estos datos puede desempeñar un papel fundamental en la talla de la protección de la información de la organización. Puede servir como infraestructura para lo siguiente:

- Ayudar a cumplir los requisitos de cumplimiento de normas y los estándares relacionados con la privacidad de datos
- Abordar diversos escenarios de seguridad, como la supervisión (auditoría) y las alertas relacionadas con accesos anómalos a información confidencial
- Controlar el acceso y mejorar la seguridad de las bases de datos que contienen información altamente confidencial

La clasificación y detección de datos forma parte de la oferta de Advanced Data Security. Dicha oferta es un paquete unificado de funcionalidades avanzadas de seguridad de Microsoft SQL Server. El acceso y la administración de la detección y la clasificación de datos se realizan a través del portal central de Advanced Data Security de SQL.

La clasificación y detección de datos incluye un conjunto de servicios avanzados y funcionalidades de SQL que forman un paradigma de SQL Information Protection destinado a proteger los datos, no solo la base de datos:

- **Detección y recomendaciones**: el motor de clasificación examina la base de datos e identifica las columnas que contienen datos potencialmente confidenciales. Tras ello, proporciona una forma sencilla de revisar y aplicar las recomendaciones de clasificación adecuadas a través de Azure Portal.
- **Etiquetado**: las etiquetas de clasificación de la confidencialidad se pueden etiquetar de forma persistente en columnas con nuevos atributos de metadatos de clasificación incluidos en el motor de SQL Server. Estos metadatos se pueden utilizar luego en escenarios avanzados de auditoría y protección basados en la confidencialidad.
- **Confidencialidad del conjunto de resultados de consulta**: la confidencialidad del conjunto de resultados de consulta se calcula en tiempo real con fines de auditoría.
- **Visibilidad**: el estado de clasificación de la base de datos se puede ver en un panel detallado en Azure Portal. También se puede descargar un informe (en formato de Microsoft Excel) que se puede usar con fines de auditoría y cumplimiento, además de para cubrir otras necesidades.

Pasos de detección, clasificación y etiquetado

La clasificación tiene dos atributos de metadatos:

- **Etiquetas**: son los atributos de clasificación principales, que se usan para definir el nivel de confidencialidad de los datos almacenados en la columna.
- **Tipos de información**: aportan una granularidad extra en el tipo de datos almacenados en la columna.

La detección y clasificación de datos de SQL incluye un conjunto integrado de etiquetas de confidencialidad y un conjunto integrado de tipos de información y lógica de detección. Ahora, puede personalizar esta taxonomía y definir un conjunto y la categoría de construcciones de clasificación específicamente para su entorno.

La definición y personalización de la taxonomía de clasificación se realiza en una ubicación central para todo el inquilino de Azure. Esa ubicación se encuentra en Microsoft Defender for Cloud, como parte de la directiva de seguridad. Solo un usuario con derechos administrativos en el grupo de administración raíz del inquilino puede realizar esta tarea.

Como parte de la administración de directivas de Azure Information Protection, puede definir etiquetas personalizadas, clasificarlas y asociarlas con un conjunto selecto de tipos de información. También puede agregar sus propios tipos de información personalizados y configurarlos con

patrones de cadena, que se agregan a la lógica de detección para identificar este tipo de datos en las bases de datos. Obtenga más información sobre cómo personalizar y administrar la directiva en la guía de procedimientos de directivas de Information Protection.

Una vez definida la directiva de todos los inquilinos, puede continuar con la clasificación de bases de datos individuales mediante la directiva personalizada.

Exploración de la evaluación de vulnerabilidad

La evaluación de vulnerabilidades de SQL es un servicio fácil de configurar que puede detectar, realizar un seguimiento y corregir posibles puntos vulnerables en la base de datos. Úsela para mejorar la seguridad de la base de datos de manera proactiva.

La evaluación de vulnerabilidades forma parte de la oferta de **Advanced Data Security**, que es un paquete unificado de funcionalidades avanzadas de seguridad de SQL. Puede acceder a la evaluación de vulnerabilidades y administrarla a través del portal central de Advanced Data Security de SQL.

Evaluación de vulnerabilidad

La evaluación de vulnerabilidades de SQL es un servicio que proporciona visibilidad del estado de seguridad. La evaluación de vulnerabilidades incluye pasos procesables para resolver problemas de seguridad y mejorar la seguridad de la base de datos. En este sentido, le puede ayudar a:

- Satisfacer los requisitos de cumplimiento que requieren los informes de examen de base de datos
- Cumplir los estándares de privacidad de los datos
- Supervisar un entorno de base de datos dinámico donde resulta difícil realizar un seguimiento de los cambios

Evaluación de vulnerabilidades es un **servicio de análisis integrado en Azure SQL Database**. Este servicio emplea una base de conocimiento de reglas que marcan las vulnerabilidades de seguridad. Se resaltan las desviaciones de los procedimientos recomendados, como configuraciones inadecuadas, permisos excesivos y datos confidenciales desprotegidos.

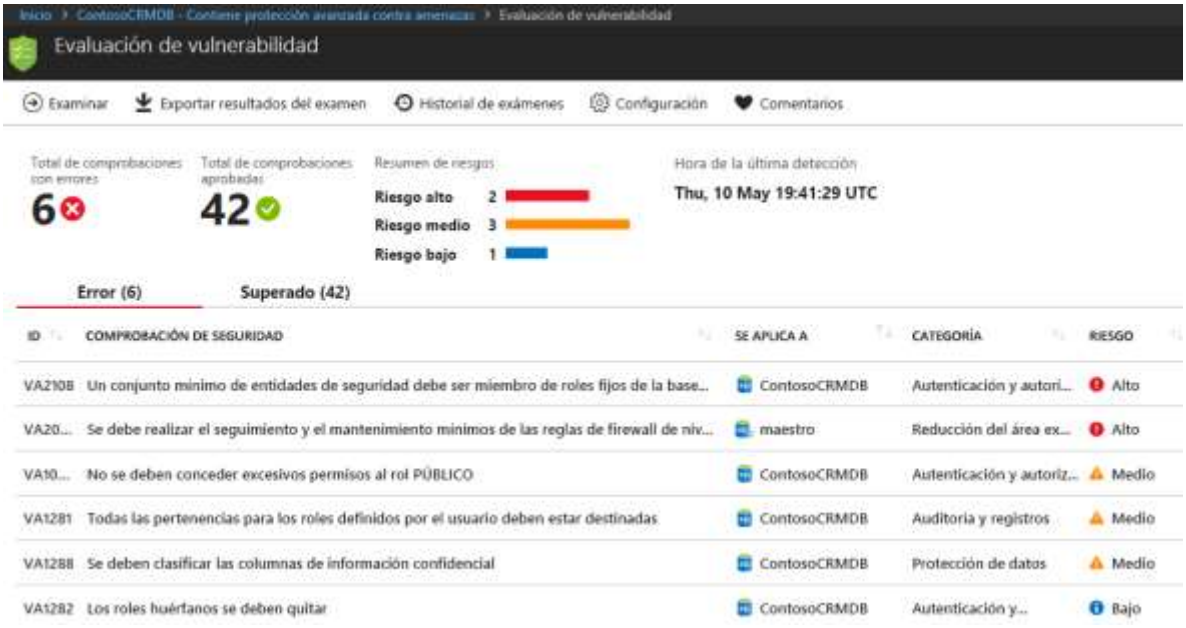
Las reglas se basan en los procedimientos recomendados de Microsoft y se centran en los problemas de seguridad que presentan mayores riesgos para la base de datos y sus valiosos datos. Tratan los problemas de nivel de base de datos y los problemas de seguridad de nivel de servidor, como la configuración del firewall de servidor y los permisos de nivel de servidor. Estas reglas también representan muchos de los requisitos que deben cumplir diversos organismos reguladores para satisfacer los estándares de cumplimiento.

Los resultados del examen incluyen pasos que requieren acción para corregir cada uno de los problemas y proporcionan scripts de solución personalizados donde sea aplicable. Para personalizar un informe de evaluación de su entorno, debe establecer una línea de base aceptable de lo siguiente:

- Configuraciones de permisos
- Configuraciones de características
- Configuración de base de datos

Visualización del informe

Una vez completado el examen, el informe del examen se muestra automáticamente en Azure Portal. El informe presenta una visión general del estado de seguridad. En él se muestra el número de problemas encontrados y sus respectivos niveles de gravedad. Los resultados incluyen advertencias sobre las desviaciones con respecto a los procedimientos recomendados, así como una instantánea de la configuración relacionada con la seguridad, como las entidades de seguridad y los roles de base de datos y sus permisos asociados. El informe de examen también proporciona un mapa de los datos confidenciales detectados en la base de datos, e incluye recomendaciones para clasificar los datos por medio de la detección y clasificación de datos. Los resultados del examen se muestran a continuación:



Establecimiento de la línea base

Cuando revise los resultados de la evaluación, puede marcar los resultados específicos como una línea de base aceptable en su entorno. La línea de base es fundamentalmente una personalización de cómo se notifican los resultados. Los resultados que coinciden con la línea de base se consideran como correctos en análisis posteriores. Una vez establecido el estado de seguridad de línea de base, la evaluación de vulnerabilidades solo informa de las desviaciones con respecto a esa línea de base. De esta manera, podrá centrar su atención en los problemas relevantes.

Habilitación de Defender para SQL (Advanced Threat Protection)

Microsoft Defender for Cloud para SQL (anteriormente conocido como Advanced Threat Protection [ATP]) para bases de datos únicas y agrupadas detecta actividades anómalas que indican intentos inusuales y potencialmente peligrosos de acceder a las bases de datos o de aprovecharse de ellas. Advanced Threat Protection puede identificar lo siguiente: **posible inyección SQL**, **acceso desde un centro de datos o una ubicación inusuales, acceso desde una aplicación potencialmente peligrosa o entidad de seguridad desconocida** y **credenciales SQL por fuerza bruta**.

Microsoft Defender for Cloud para SQL forma parte de la oferta de Advanced Data Security (ADS), que es un paquete unificado para funcionalidades avanzadas de seguridad de SQL. Puede acceder a Advanced Threat Protection y administrarlo a través del portal central de ADS en SQL. ATP proporciona una nueva capa de seguridad, que permite a los clientes detectar y responder a posibles amenazas a medida que se producen proporcionando alertas de seguridad sobre actividades anómalas.

Alertas de Microsoft Defender for Cloud para SQL

Advanced Threat Protection para Azure SQL Database detecta actividades anómalas que indican intentos inusuales y potencialmente peligrosos de acceder a bases de datos, o de vulnerar su seguridad, y puede desencadenar las siguientes alertas:

- **Vulnerabilidad a la inyección SQL**: esta alerta se desencadena cuando una aplicación genera una instrucción SQL en la base de datos. Esta alerta puede indicar una posible vulnerabilidad a los ataques de inyección de código SQL. Hay dos posibles razones para la generación de una instrucción errónea:
    - Existe un defecto en el código de la aplicación que crea la instrucción SQL errónea
    - El código de la aplicación o los procedimientos almacenados no corrigen los datos que proporciona el usuario al construir la instrucción SQL errónea, lo que se puede aprovechar para ataques por inyección de código SQL
- **Potencial inyección de código SQL**: esta alerta se desencadena cuando se produce una vulnerabilidad de seguridad activa contra una vulnerabilidad de la aplicación identificada ante inyección de código SQL. Esto significa que el atacante intentan inyectar instrucciones SQL malintencionadas mediante el código de la aplicación vulnerable o procedimientos almacenados.
- **Acceso desde una ubicación inusual**: esta alerta se desencadena cuando se produce un cambio en el patrón de acceso a SQL Server, donde alguien ha iniciado sesión en el servidor SQL Server desde una ubicación geográfica inusual. En algunos casos, la alerta detecta una acción legítima (una nueva aplicación o el mantenimiento de un desarrollador). En otros casos, la alerta detecta una acción malintencionada (por ejemplo, un antiguo empleado o un atacante externo).

- **Acceso desde un centro de datos de Azure inusual**: esta alerta se desencadena cuando se produce un cambio en el patrón de acceso a SQL Server, donde alguien ha iniciado sesión en el servidor SQL Server desde un centro de datos de Azure inusual que se vio en el servidor recientemente. En algunos casos, la alerta detecta una acción legítima (una aplicación nueva en Azure, Power BI o Azure SQL Query Editor). En otros casos, la alerta detecta una acción malintencionada procedente de un recurso o servicio de Azure (por ejemplo, un antiguo empleado o un atacante externo).
- **Acceso desde una entidad de seguridad desconocida**: esta alerta se desencadena cuando se produce un cambio en el patrón de acceso a SQL Server, donde alguien ha iniciado sesión en el servidor SQL Server mediante una entidad de seguridad inusual (usuario de SQL). En algunos casos, la alerta detecta una acción legítima (una nueva aplicación o el mantenimiento de un desarrollador). En otros casos, la alerta detecta una acción malintencionada (por ejemplo, un antiguo empleado o un atacante externo).
- **Acceso desde una aplicación potencialmente dañina**: esta alerta se desencadena cuando una aplicación potencialmente dañina se utiliza para tener acceso a la base de datos. En algunos casos, la alerta detecta la realización de pruebas de seguridad. En otros casos, la alerta detecta un ataque que se realiza con herramientas de ataque comunes.
- **Credenciales de SQL por fuerza bruta**: esta alerta se desencadena cuando hay un número anormalmente elevado de inicios de sesión infructuosos con distintas credenciales. En algunos casos, la alerta detecta la realización de pruebas de seguridad. En otros casos, la alerta detecta ataques por fuerza bruta.

ATP se integra con Microsoft Defender for Cloud para detectar amenazas potenciales y responder a ellas a medida que se producen.

Configuración del enmascaramiento de datos dinámicos

El enmascaramiento dinámico de datos de SQL Database limita la exposición de información confidencial ocultándolos a los usuarios sin privilegios.

El enmascaramiento de datos dinámicos ayuda a impedir el acceso no autorizado a datos confidenciales permitiendo a los usuarios designar la cantidad de los datos confidenciales que se revelarán con un impacto mínimo en el nivel 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.

Por ejemplo, un representante de servicio de un centro de llamadas podría identificar a los autores de las llamadas a partir de varios dígitos del número de su tarjeta de crédito, pero esa es una información que no debería exponerse por completo al representante del servicio. Se puede definir una regla de enmascaramiento que enmascare todo excepto los cuatro últimos dígitos de

un número de tarjeta de crédito en el conjunto de resultados de cualquier consulta. Otro ejemplo, una máscara de datos apropiada se puede definir para proteger los datos personales, para que un desarrollador pueda consultar los entornos de producción para solucionar problemas sin infringir las reglamentaciones de cumplimiento.

Aspectos básicos del enmascaramiento dinámico de datos

Para configurar una directiva de enmascaramiento dinámico de datos en Azure Portal, se selecciona la operación de enmascaramiento dinámico de datos en la hoja de configuración de SQL Database. Esta característica no se puede establecer mediante el portal para Azure Synapse

Directiva de enmascaramiento de datos dinámicos

- **Usuarios de SQL excluidos del enmascaramiento**: conjunto de usuarios de SQL o identidades de AAD que obtendrán datos sin máscara en los resultados de consulta SQL. Los usuarios con privilegios de administrador se excluirán siempre del enmascaramiento y verán los datos originales sin ninguna máscara.
- **Reglas de enmascaramiento**: un conjunto de reglas que definen los campos designados para el enmascaramiento y la función de enmascaramiento que se va a usar. Los campos designados se pueden definir mediante un nombre de esquema de base de datos, un nombre de tabla y un nombre de columna.
- **Funciones de enmascaramiento** : un conjunto de métodos que controlan la exposición de datos para diferentes escenarios.

Campos recomendados para enmascarar

El motor de recomendaciones de DDM marca determinados campos de la base de datos como campos potencialmente confidenciales, que pueden ser buenos candidatos para el enmascaramiento. En la hoja Enmascaramiento de datos dinámicos del portal, puede revisar las columnas recomendadas para la base de datos. Todo lo que debe hacer es hacer clic en **Agregar máscara** para una o más columnas y, después, en **Guardar** a fin de aplicar una máscara para estos campos.

Implementar cifrado de datos transparente

El cifrado de datos transparente (TDE) ayuda a proteger Azure SQL Database, Instancia administrada de Azure SQL y SQL de Synapse en Azure Synapse Analytics frente a la amenaza de actividades malintencionadas sin conexión, ya que cifra los datos en reposo. También realiza cifrado y descifrado de la base de datos en tiempo real, copias de seguridad asociadas y archivos de registro de transacciones en reposo sin necesidad de efectuar cambios en la aplicación. **De forma predeterminada, TDE está habilitado para todas las bases de datos SQL de Azure recién implementadas** y debe habilitarse manualmente para las bases de datos anteriores de Azure SQL Database, Azure SQL Managed Instance o Azure Synapse.

El TDE efectúa el cifrado y descifrado de E/S en tiempo real de los datos en el nivel de página. Todas las páginas se descifran cuando se leen en la memoria y, a continuación, se cifran antes de escribirse en el disco. El TDE cifra el almacenamiento de una base de datos completa mediante una clave simétrica denominada clave de cifrado de base de datos (DEK). Al iniciarse la base de datos, la DEK cifrada se descifra y luego se usa para descifrar y volver a cifrar los archivos de base de datos en el proceso del Motor de base de datos de SQL Server. A la clave de cifrado se le aplica el protector de TDE. El protector de TDE es un certificado administrado por el servicio (cifrado de datos transparentes administrado por el servicio) o una clave asimétrica almacenada en Azure Key Vault (cifrado de datos transparentes administrado por el cliente).

En el caso de Azure SQL Database y Azure Synapse, el protector de TDE se establece en el nivel de servidor con SQL Server lógico y lo heredan todas las bases de datos asociadas a dicho servidor. En el caso de Instancia administrada de Azure SQL Database (la característica BYOK está en versión preliminar), el protector de TDE se establece en el nivel de instancia y lo heredan todas las bases de datos cifradas que se encuentran en dicha instancia. El término servidor hace referencia tanto a servidor como a instancia a lo largo de este documento, a menos que se indique lo contrario.

Cifrado de datos transparente administrado por el servicio

En Azure, la configuración predeterminada de TDE es que la clave de cifrado está protegida mediante un certificado de servidor integrado. El certificado de servidor integrado es único para cada servidor y el algoritmo de cifrado que se usa es AES 256. Si una base de datos está en una relación de replicación geográfica, tanto la base de datos principal como la secundaria con replicación geográfica están protegidas por la clave de servidor principal de la base de datos principal. Si hay dos bases de datos conectadas al mismo servidor, también comparten el mismo certificado integrado. Microsoft rota automáticamente estos certificados en cumplimiento de la directiva de seguridad interna y se protege la clave raíz mediante un almacén secreto interno de Microsoft. Los clientes pueden verificar el cumplimiento de SQL Database con las directivas de seguridad internas en los informes de auditoría de terceros independientes disponibles en el Centro de confianza de Microsoft.

Microsoft también mueve y administra con total fluidez las claves según sea necesario para la replicación geográfica y las restauraciones.

Cifrado de datos transparente administrado por el cliente (Bring Your Own Key)

La TDE administrada por el cliente también se conoce como compatibilidad de Bring Your Own Key (BYOK) con TDE. En este escenario, el protector de TDE que cifra la clave de cifrado es una clave asimétrica administrada por el cliente, que se almacena en una instancia de Azure Key Vault que es propiedad del cliente y que este administra (un sistema de administración de claves externas basado en la nube de Azure), y que nunca sale del almacén de claves. El protector de TDE lo puede generar el almacén de claves, o bien se puede transferir a él desde un dispositivo del módulo de seguridad de hardware (HSM) local. Para cifrar y descifrar la clave de cifrado es preciso que SQL Database tenga los permisos necesarios en el almacén de claves que posee el cliente. Si se revocan los permisos del servidor con SQL Server lógico en el almacén de claves, no se podrá acceder a las bases de datos y se cifrarán todos los datos

Gracias al cifrado de datos transparente con integración de Azure Key Vault, los usuarios pueden controlar las tareas de administración de claves, entre las que se incluyen las rotaciones de claves, los permisos del almacén de claves y la copia de seguridad de claves, así como la opción de llevar a cabo auditorías o crear informes sobre todos los protectores de TDE mediante la funcionalidad de Azure Key Vault. Key Vault ofrece una administración centralizada de claves, aprovecha los módulos de seguridad de hardware, a los que se les supervisa intensamente, y permite la separación de obligaciones entre la administración de las claves y de los datos, lo que ayudar a cumplir las directivas de seguridad.

Administración de TDE en Azure Portal

Para configurar el TDE desde Azure Portal, es preciso estar conectado como propietario de Azure, colaborador o administrador de seguridad de SQL.

Active y desactive TDE en el nivel de base de datos. Para habilitar TDE en una base de datos, vaya a Azure Portal e inicie sesión con una cuenta de administrador o colaborador de Azure. Busque la configuración del TDE en la base de datos de usuario. De forma predeterminada, se usa el cifrado de datos transparente administrado por el servicio. Se genera automáticamente un certificado de cifrado de datos transparente para el servidor que contiene la base de datos. En el caso de Instancia administrada de Azure SQL Database, use T-SQL para activar y desactivar el cifrado de datos transparente en las bases de datos.

Implementar características de Always Encrypted

SQL Database Always Encrypted

Always Encrypted es una característica creada para proteger la información confidencial, como números de tarjetas de crédito o números de identificación nacionales (por ejemplo, números de la seguridad social de EE. UU.), almacenados en bases de datos de Azure SQL Database o SQL Server. Always Encrypted permite a los clientes cifrar información confidencial dentro de aplicaciones cliente y no revelar las claves de cifrado al motor de base de datos (SQL Database o SQL Server). De este modo, Always Encrypted ofrece una separación entre los usuarios que poseen los datos (y pueden verlos) y los que administran los datos (pero no deben tener acceso a ellos). **Asegurando que los administradores de las bases de datos locales, los operadores de las bases de datos en la nube u otros usuarios con altos privilegios, pero no autorizados, no puedan acceder a los datos cifrados**. Always Encrypted permite a los clientes almacenar datos confidenciales con confianza fuera de su control directo. Por lo tanto, Always Encrypted permite a las organizaciones cifrar datos en reposo y en uso para el almacenamiento en Azure, habilitar la delegación de la administración local de bases de datos a terceros o reducir los requisitos de autorización de seguridad para su propio personal de DBA.

Always Encrypted realiza cifrado transparente en las aplicaciones. Un controlador habilitado para Always Encrypted instalado en el equipo cliente consigue esto al cifrar y descifrar automáticamente la información confidencial en la aplicación cliente. El controlador cifra los datos en columnas confidenciales antes de pasar los datos a Motor de base de datosy vuelve a escribir las consultas automáticamente para que se conserve la semántica de la aplicación. De forma similar, el controlador descifra los datos de forma transparente, almacenados en columnas de bases de datos cifradas, incluidas en los resultados de la consulta.

Escenarios de uso de ejemplo

Cliente local con datos en Azure

Un cliente tiene una aplicación cliente local en su ubicación de la empresa. La aplicación trabaja sobre la información confidencial almacenada en una base de datos hospedada en Azure (SQL Database o SQL Server que se ejecutan en una máquina virtual en Microsoft Azure). El cliente usa Always Encrypted y almacena claves de Always Encrypted en un almacén de claves de confianza hospedado localmente, para asegurarse de que los administradores de la nube de Microsoft no tienen acceso a datos confidenciales.

Cliente y datos en Azure

Un cliente tiene una aplicación cliente hospedada en Microsoft Azure (por ejemplo, en un rol de trabajo o un rol web) que trabaja sobre la información confidencial almacenada en una base de datos hospedada en Azure (SQL Database o SQL Server se ejecutan en una máquina virtual en Microsoft Azure). Aunque Always Encrypted no proporciona un aislamiento completo de los datos

ante los administradores de la nube, dado que tanto los datos como las claves están expuestos a los administradores de la nube de la plataforma que hospeda el nivel de cliente, el cliente se sigue beneficiando de la reducción del área expuesta de ataque de seguridad (los datos siempre se cifran en la base de datos).

Características de Always Encrypted

El motor de base de datos nunca funciona en los datos de texto no cifrado almacenados en columnas cifradas, pero sigue admitiendo algunas consultas en datos cifrados, según el tipo de cifrado de la columna. Always Encrypted admite dos tipos de cifrado: **cifrado aleatorio y cifrado determinista**.

- El **cifrado determinista** usa un método que genera siempre el mismo valor cifrado para cualquier valor de texto no cifrado concreto. El empleo del cifrado determinista permite búsquedas de puntos, combinaciones de igualdad, agrupaciones e indexación en columnas cifradas. Pero también puede permitir que usuarios no autorizados adivinen información sobre los valores cifrados al examinar los patrones de la columna cifrada, especialmente si hay un pequeño conjunto de posibles valores cifrados, como verdadero/falso la región norte/sur/este/oeste. El cifrado determinista debe usar una intercalación de columna con un criterio de ordenación binario 2 para columnas de caracteres.
- El**cifrado aleatorio** utiliza un método que cifra los datos de una manera menos predecible. El cifrado aleatorio es más seguro, pero evita las búsquedas, la agrupación, la indexación y la combinación en columnas cifradas.

Utilice el cifrado determinista para las columnas que se usarán como parámetros de búsqueda o agrupación, por ejemplo un número de identificación de gobierno. Utilice el cifrado aleatorio para aquellos datos como comentarios de investigación confidenciales que no están agrupados con otros registros y no se utilizan para combinar tablas.

Implementación de Always Encrypted

Configuración de Always Encrypted

La configuración inicial de Always Encrypted en una base de datos implica la generación de claves de Always Encrypted, la creación de metadatos de clave, la configuración de propiedades de cifrado de columnas seleccionadas de la base de datos o el cifrado de los datos que puedan existir en las columnas que deban cifrarse. Recuerde que algunas de estas tareas no se admiten en Transact-SQL y requieren el uso de herramientas del lado cliente. Dado que las claves de Always Encrypted y la información confidencial protegida nunca se revelan en texto no cifrado al servidor, el motor de base de datos no puede estar implicado en el aprovisionamiento de claves ni realizar

operaciones de cifrado o descifrado de datos. Puede usar SQL Server Management Studio (SSMS) o PowerShell para realizar dichas tareas.

Task	SSMS	PowerShell	SQL
Aprovisionamiento de claves maestras de columna, claves de cifrado de columnas y claves de cifrado de columnas cifradas con sus claves maestras de columna correspondientes	Sí	Sí	No
Creación de metadatos clave en la base de datos	Sí	Sí	Sí
Creación de nuevas tablas con columnas cifradas	Sí	Sí	Sí
Cifrado de los datos existentes en las columnas seleccionadas de la base de datos	Sí	Sí	No

Al configurar el cifrado de una columna, especifique la información sobre el algoritmo de cifrado y las claves criptográficas usados para proteger los datos de la columna. Always Encrypted usa claves de dos tipos: claves maestras de columna y claves de cifrado de columna. Una clave de cifrado de columna se usa para cifrar los datos de una columna cifrada. Una clave maestra de columna es una clave de protección de claves que cifra una o varias claves de cifrado de columna.

El motor de base de datos almacena la configuración de cifrado de cada columna en los metadatos de la base de datos. Pero tenga en cuenta que el motor de base de datos nunca almacena ni usa las claves de cualquier tipo de texto no cifrado. Solo almacena valores cifrados de claves de cifrado de columna y la información sobre la ubicación de claves maestras de columna, que se almacenan en almacenes de claves de confianza externos, como el almacén de claves de Azure, el almacén de certificados de Windows en un equipo cliente o un módulo de seguridad de hardware.

Para acceder a los datos almacenados en una columna cifrada en texto no cifrado, una aplicación debe usar un controlador de cliente habilitado para Always Encrypted. Cuando una aplicación emite una consulta con parámetros, el controlador colabora de forma transparente con el motor de base de datos para determinar qué parámetros se dirigen a columnas cifradas y, por lo tanto, se deben cifrar. De cada parámetro que se tiene que cifrar, el controlador obtiene la información sobre el algoritmo de cifrado y el valor cifrado de la clave de cifrado de columna de la columna, los destinos del parámetro y la ubicación de su clave maestra de columna correspondiente.

Después, el controlador se pone en contacto con el almacén de claves, que contiene la clave maestra de columna, para descifrar el valor de clave de cifrado de columna cifrado y, luego, usa la clave de cifrado de columna de texto no cifrado para cifrar el parámetro. La clave de cifrado de columna de texto no cifrado resultante se almacena en la memoria caché para reducir el número de viajes de ida y vuelta al almacén de claves en usos posteriores de la misma clave de cifrado de columna. El controlador sustituye los valores de texto no cifrado de los parámetros que se dirigen a columnas cifradas por sus valores cifrados y envía la consulta al servidor para su procesamiento.

El servidor calcula el conjunto de resultados y, para cualquier columna cifrada incluida en el conjunto de resultados, el controlador adjunta los metadatos de cifrado de la columna, incluida la información sobre el algoritmo de cifrado y las claves correspondientes. El controlador primero intenta buscar la clave de cifrado de columna de texto no cifrado en la memoria caché local y, si no la encuentra, solo realiza una ronda en la clave maestra de columna. Luego, el controlador descifra los resultados y devuelve valores de texto no cifrado a la aplicación.

Un controlador cliente interactúa con un almacén de claves, que contiene una clave maestra de columna, mediante un proveedor de almacén de claves maestras de columna, que es un componente de software de cliente que encapsula un almacén de claves que contiene la clave maestra de columna. Los proveedores de los tipos comunes de almacenes de claves están disponibles en bibliotecas de controladores de cliente de Microsoft o como descargas independientes. También puede implementar su propio proveedor. Las funciones de Always Encrypted, incluidos los proveedores integrados de almacenes de claves maestras de columna, varían según la biblioteca de controladores y su versión.