**Introducción**

Este módulo está diseñado para capacitar a los administradores con los conocimientos y aptitudes necesarios para planear e implementar medidas de seguridad sólidas para Azure SQL Database y Azure SQL Managed Instance, lo que garantiza la protección de datos y el cumplimiento normativo.

**Escenario**

Imagine que es un administrador de bases de datos responsable de administrar Azure SQL Database y Azure SQL Managed Instance en su organización. Las bases de datos almacenan información confidencial y debe asegurarse de que los datos están protegidos contra el acceso no autorizado, las vulneraciones de datos y el incumplimiento normativo.

**Objetivos de aprendizaje**

Al final de este módulo, los participantes pueden:

* Planear e implementar medidas de seguridad para Azure SQL Database y Azure SQL Managed Instance para proteger los datos confidenciales.
* Habilitar la autenticación de base de datos mediante Microsoft Entra ID para el control de acceso seguro.
* Implementar la auditoría de bases de datos para realizar un seguimiento y supervisar las actividades de base de datos para el cumplimiento y la seguridad.
* Identificar los casos de uso del portal de gobernanza de Microsoft Purview y aprovechar sus funcionalidades para la gobernanza de datos.
* Implementar la clasificación de datos de información confidencial mediante el portal de gobernanza de Microsoft Purview para garantizar la protección de los datos y el cumplimiento normativo.
* Planear e implementar el enmascaramiento dinámico para controlar la exposición de datos confidenciales en los resultados de la consulta.
* Implementar cifrado de base de datos transparente (TDE) para cifrar los datos en reposo para mejorar la seguridad.
* Proporcionar recomendaciones sobre cuándo usar Always Encrypted de Azure SQL Database para el cifrado de datos del lado cliente.

**Objetivos**

El módulo tiene como objetivo proporcionar a los participantes los conocimientos y habilidades necesarios para diseñar, implementar y administrar medidas de seguridad avanzadas para Azure SQL Database y Azure SQL Managed Instance. Los participantes pueden proteger los datos, controlar el acceso, supervisar las actividades de la base de datos y cumplir con los requisitos de gobernanza de datos, y, en última instancia, proteger la información confidencial frente a posibles amenazas de seguridad y problemas normativos.

**Habilitación de la autenticación de base de datos mediante Microsoft Entra ID**

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 Microsoft Entra**: 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 Microsoft Entra ID.

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.

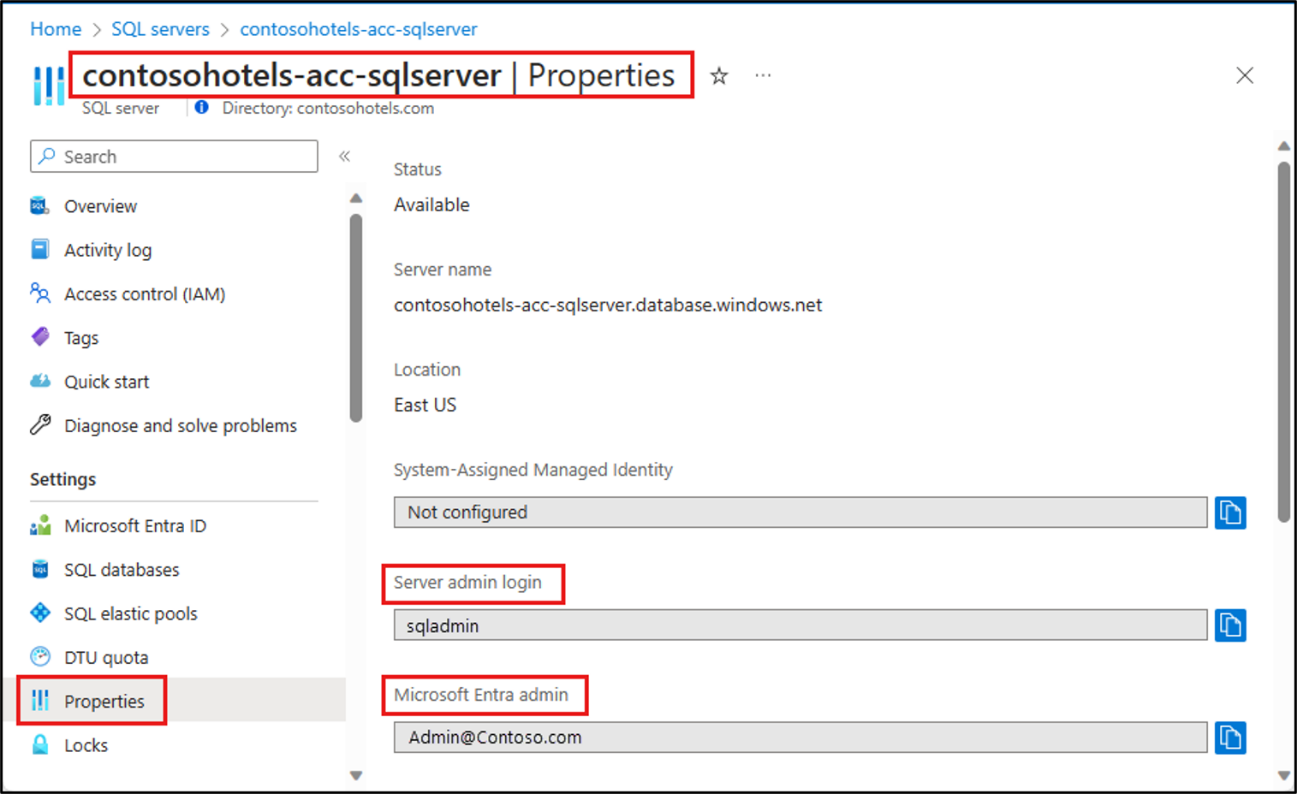
La **autorización** para acceder a los datos y realizar diversas acciones se administran con roles de base de datos y permisos explícitos. El término autorización hace referencia a los permisos asignados a un usuario, y determina qué puede hacer ese usuario. La autorización se controla por medio de las pertenencias a roles y los permisos de nivel de objeto de la base de datos de cada 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.

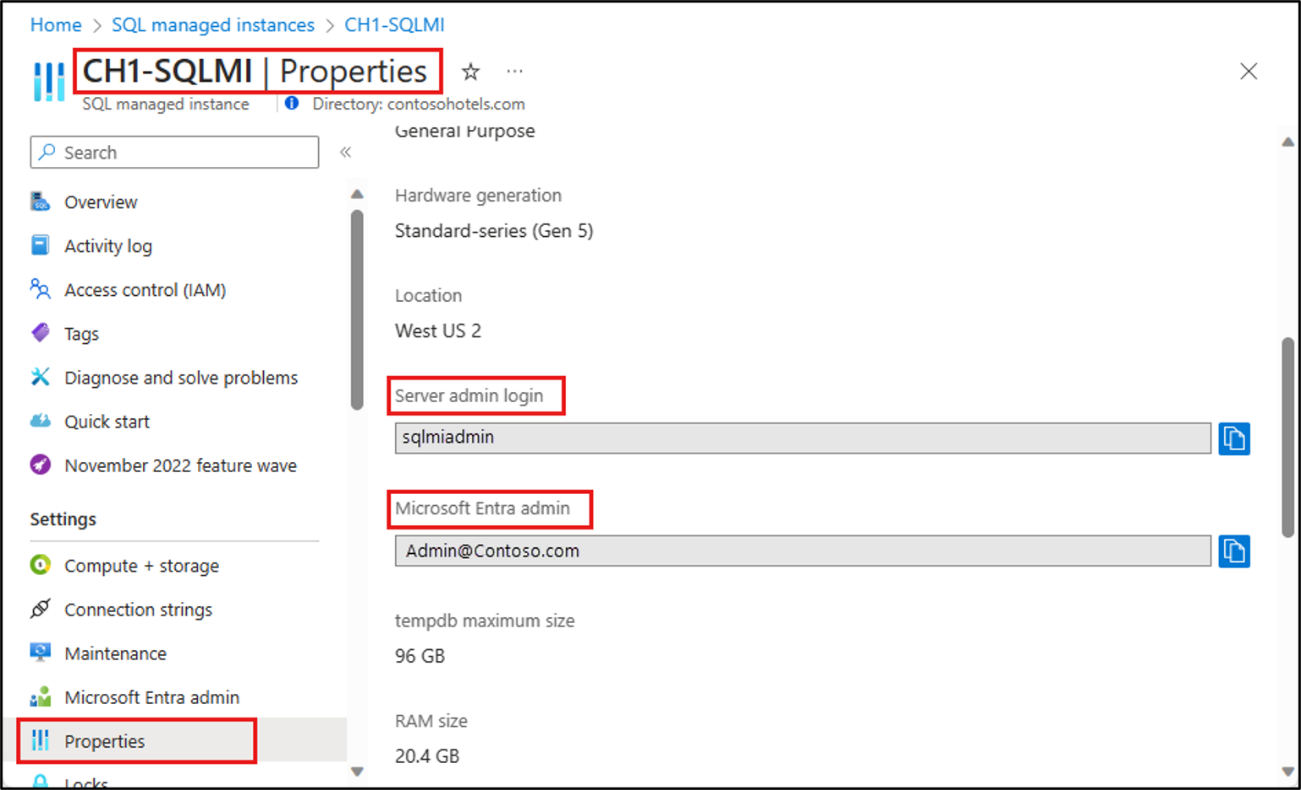
**Inicios de sesión y cuentas de usuario existentes después de crear una base de datos**

Al implementar por primera vez Azure SQL, puede especificar un nombre de inicio de sesión y una contraseña para un tipo especial de inicio de sesión administrativo, el **administrador del servidor**. La siguiente configuración de inicios de sesión y usuarios en las bases de datos maestras y de usuario se produce durante la implementación:

* Se crea un inicio de sesión de SQL con privilegios administrativos usando el nombre de inicio de sesión especificado. Un **inicio de sesión** es una cuenta individual para iniciar sesión en SQL Database, SQL Managed Instance y Azure Synapse.
* A este inicio de sesión se le conceden permisos administrativos completos en todas las bases de datos, como una **entidad de seguridad de nivel de servidor**. El inicio de sesión tiene todos los permisos disponibles y no puede ser limitado. En una instancia administrada de SQL, este inicio de sesión se agrega al **rol fijo de servidor sysadmin** (este rol no existe en Azure SQL Database).
* Cuando esta cuenta inicia sesión en una base de datos, se compara con la cuenta de usuario especial dbo (**cuenta de usuario**), que existe en cada base de datos de usuario. El usuario **dbo** posee todos los permisos de base de datos en la base de datos y es miembro del rol fijo de base de datos db\_owner.

Para identificar la cuenta de **administrador del servidor** de un servidor lógico, abra Azure Portal y navegue hasta la pestaña **Propiedades** de su servidor o instancia administrada.





El nombre de la cuenta de **administrador del servidor** no se puede cambiar después de crearla. Para restablecer la contraseña del administrador del servidor, vaya a Azure Portal, haga clic en **Servidores SQL Server**, seleccione el servidor en la lista y luego haga clic en **Restablecer contraseña**. Para restablecer la contraseña de la instancia administrada de SQL, vaya a **Azure Portal**, haga clic en la instancia y, después, en **Restablecer contraseña**. También puede usar PowerShell o la CLI de Azure.

**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:

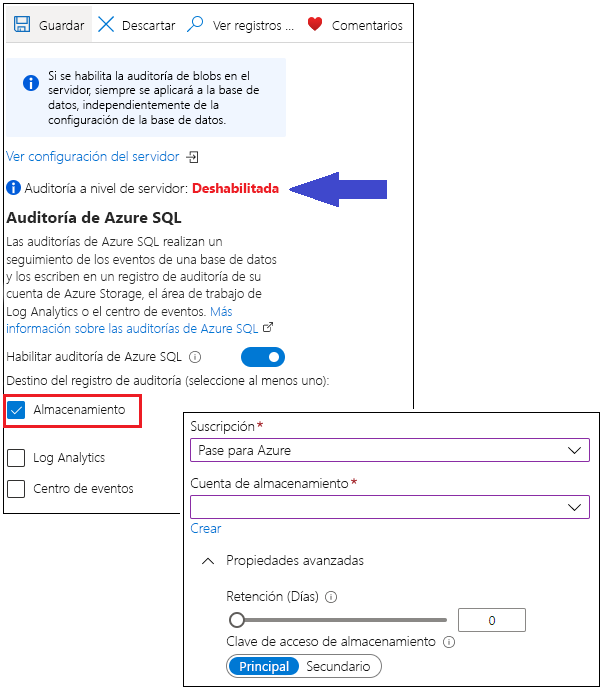
* **Conservar** una traza de auditoría de eventos seleccionados. Puede definir categorías de acciones de base de datos para auditar.
* **Informar** sobre la actividad de la base de datos. Puede usar informes preconfigurados y un panel para dar los primeros pasos más rápido con el informe de actividades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

* Conservar una traza de auditoría de eventos seleccionados.
* Informe sobre la actividad de la base de datos y análisis de resultados.
* Configure directivas para el nivel de servidor o base de datos.
* Configure el destino del registro de auditoría.
* Una nueva directiva de servidor se aplica a todas las bases de datos existentes y recién creadas.

**Identificar casos de uso del Portal de gobernanza de Microsoft Purview**

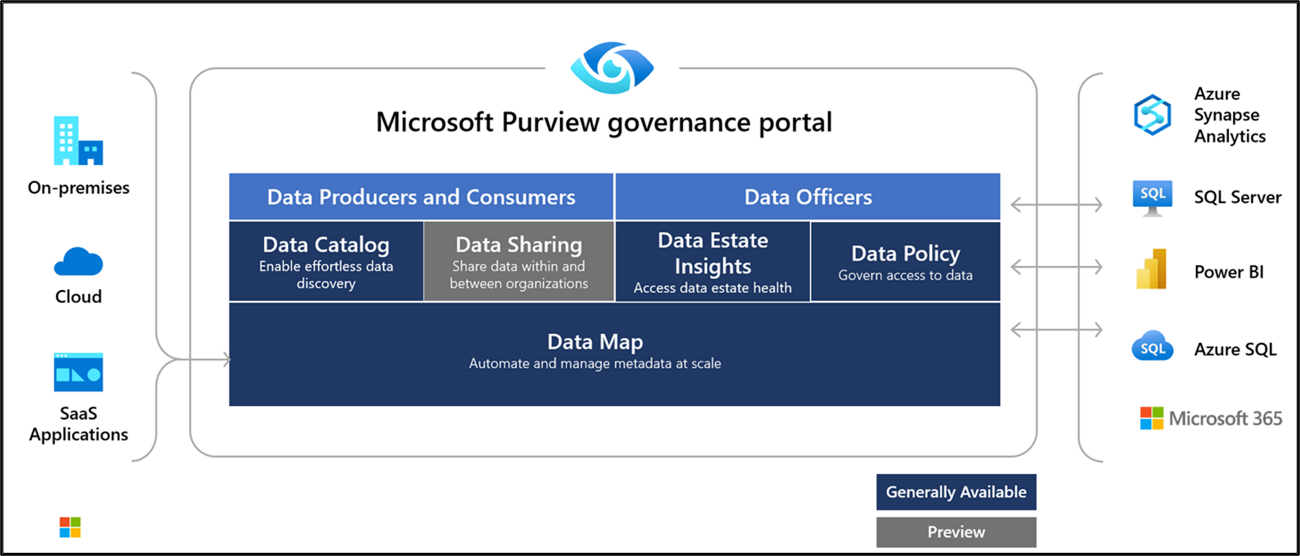
**Portal de gobernanza de Microsoft Purview**

Las soluciones del portal de gobernanza de Microsoft Purview constituyen un servicio de gobernanza de datos unificado que ayuda a administrar y controlar los datos ubicados en entornos locales y varias nubes, así como aquellos procedentes de los procesos de software como servicio (SaaS). El portal de gobernanza de Microsoft Purview le permite realizar las siguientes acciones:

* Cree un mapa holístico actualizado del panorama de sus datos con detección automatizada de datos, clasificación de datos confidenciales y linaje de datos de principio a fin.
* Habilite los conservadores de datos y los administradores de seguridad para administrar el patrimonio de datos seguro.
* Permita a los consumidores de datos encontrar datos valiosos y confiables.

**Requisitos previos**

* Ya se ha creado una cuenta de Microsoft Purview activa en Azure Portal.
* El usuario tiene permisos para acceder al **portal de gobernanza de Microsoft Purview**.



Las soluciones del portal de gobernanza de Microsoft Purview constituyen un servicio de gobernanza de datos unificado que ayuda a administrar y controlar los datos ubicados en entornos locales y varias nubes, así como aquellos procedentes de los procesos de software como servicio (SaaS).

**Mapa de datos**

Microsoft Purview automatiza la detección de datos al proporcionar examen y clasificación de datos para los recursos de su patrimonio de datos. Los metadatos y descripciones de los recursos de datos detectados se integran en un mapa holístico del patrimonio de datos. El Mapa de datos de Microsoft Purview proporciona la base para la detección de datos y la gobernanza de estos. Mapa de datos de Microsoft Purview es un servicio PaaS nativo de la nube que captura metadatos acerca de los datos empresariales presentes en los sistemas de operaciones y análisis locales y en la nube. Mapa de datos de Microsoft Purview se mantiene actualizado de forma automática con un sistema de examen y clasificación automatizados integrado. Los usuarios empresariales pueden configurar y usar el mapa de datos mediante una interfaz de usuario intuitiva, mientras que los desarrolladores pueden interactuar mediante programación con el mapa de datos gracias a las API de Apache Atlas 2.2 de código abierto. El Mapa de datos de Microsoft Purview alimenta el Catálogo de datos de Microsoft Purview, las Conclusiones de datos de infraestructura de Microsoft Purview y la Directiva de datos de Microsoft Purview como experiencias unificadas en el Portal de gobernanza de Microsoft Purview.

**Aplicación Data Catalog**

Con Microsoft Purview Data Catalog, los usuarios técnicos y empresariales pueden encontrar rápida y fácilmente datos pertinentes mediante una experiencia de búsqueda con filtros basados en lentes, como términos del glosario, clasificaciones, etiquetas de confidencialidad, etc. En el caso de los expertos en la materia, administradores de datos y personal responsable, Microsoft Purview Data Catalog proporciona características de protección de datos como la administración de un glosario empresarial y la capacidad de automatizar el etiquetado de los recursos de datos con los términos del glosario. Los consumidores y productores de datos también pueden realizar un seguimiento visual del linaje de los recursos de datos: por ejemplo, a partir de sistemas operativos locales, a través del movimiento, la transformación y el enriquecimiento con varios sistemas de procesamiento y almacenamiento de datos en la nube, para su consumo en un sistema de análisis como Power BI.

**Aplicación Conclusiones de datos de infraestructura**

Con la información de patrimonio de datos de Microsoft Purview, los directores de datos y otras partes interesadas de gobernanza pueden obtener una visión general de su patrimonio de datos y obtener información accionable sobre las brechas de gobernanza que se pueden resolver a partir de la propia experiencia.

**Aplicación de uso compartido de datos**

Uso compartido de datos de Microsoft Purview permite a las organizaciones compartir datos de forma segura tanto dentro de su organización como entre organizaciones con socios comerciales y clientes. Puede compartir o recibir datos con solo unos pocos clics. Los proveedores de datos pueden administrar y supervisar de forma centralizada las relaciones de uso compartido de datos y revocar el uso compartido en cualquier momento. Los consumidores de datos pueden acceder a los datos recibidos con sus propias herramientas de análisis y convertir los datos en conclusiones.

**Aplicación de directiva de datos**

La directiva de datos de Microsoft Purview es un conjunto de experiencias centrales basadas en la nube que le ayudan a administrar el acceso a orígenes de datos y conjuntos de datos de forma segura y a escala.

* Administra el acceso a los orígenes de datos desde una experiencia basada en la nube de un solo panel.
* Habilita el aprovisionamiento de acceso a escala.
* Presenta un nuevo modelo de permisos de plano de datos externo a los orígenes de datos.
* Está perfectamente integrado con el Mapa de datos de Microsoft Purview y con el catálogo:
  + Busque recursos de datos y conceda acceso solo a lo necesario con directivas específicas.
  + Ruta de acceso para admitir orígenes de datos SaaS, locales y multinube.
  + Ruta de acceso para crear directivas que aprovechen los metadatos asociados a los objetos de datos.
* Basado en definiciones de roles que son simples y abstractas (por ejemplo: **Leer**, **Modificar**).

**Implementar la clasificación de datos de información confidencial con el Portal de gobernanza de Microsoft Purview**

**Administración de orígenes de datos en Microsoft Purview**

1. Registro
2. Examen e ingesta
3. Clasificar
4. Etiqueta

**Nota**

El etiquetado en el Mapa de datos de Microsoft Purview está actualmente en **VERSIÓN PRELIMINAR**.

**Términos de uso complementarios para versiones preliminares de Microsoft Azure**

Es posible que Azure incluya versiones preliminares, betas u otras características de versiones preliminares, servicios, software o regiones ofrecidas por Microsoft para evaluación opcional ("Versiones preliminares"). Las versiones preliminares tienen licencia para usted como parte del contrato que rige el uso de Azure y están sujetas a los términos aplicables a "**Versiones preliminares**".

Ciertas Versiones preliminares nombradas están sujetas a condiciones adicionales según se establece a continuación, si procede. Estas Versiones preliminares se ponen a su disposición de acuerdo con los términos adicionales, que complementan el contrato que regula el uso de Azure. Los términos en mayúscula no definidos en este documento tendrán el significado establecido en el acuerdo. Si no acepta estos términos, no use las versiones preliminares.

**Registro de un dispositivo nuevo**

**Nota**

Deberá ser un Administrador de origen de datos y tener uno de los otros roles de Purview (por ejemplo, Lector de datos o Colaborador de recurso compartido de datos) para registrar un origen y administrarlo en el portal de gobernanza de Microsoft Purview.

En Microsoft Purview, después de registrar el origen de datos, puede examinar el origen para capturar metadatos técnicos, extraer un esquema y aplicar clasificaciones a los datos.

**Requisitos previos**

Aquí hay una lista de todos los orígenes disponibles actualmente para registro y examen en Microsoft Purview.

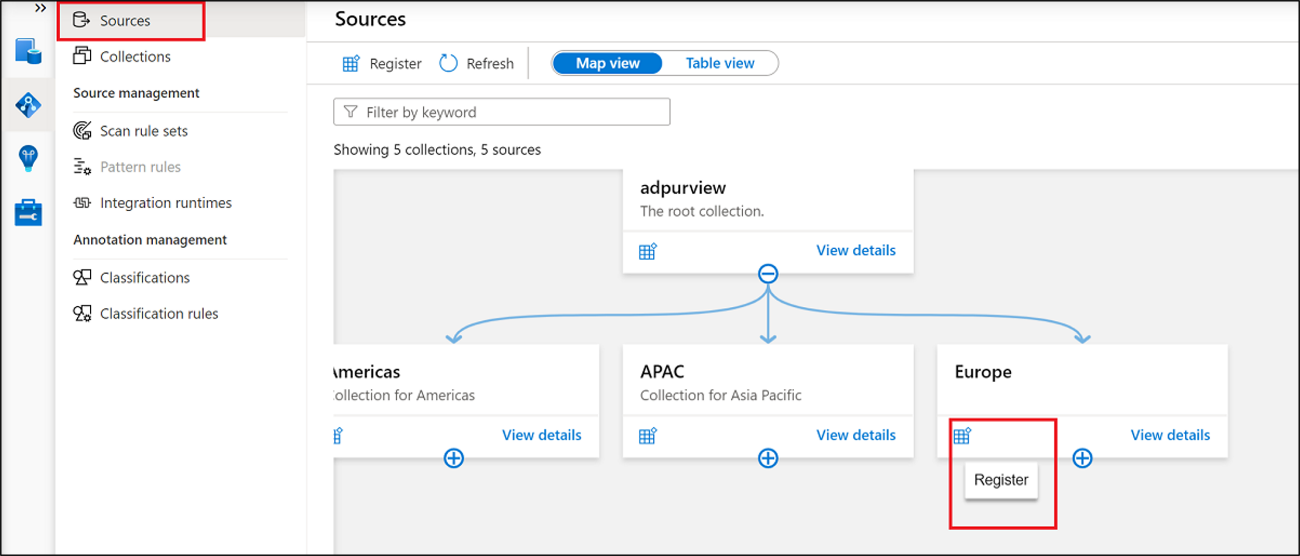
Para examinar el origen de datos, es necesario realizar estos pasos:

1. Registrar el origen de datos: básicamente proporciona a Microsoft Purview la dirección del origen de datos y la asigna a una colección en el Mapa de datos de Microsoft Purview.
2. Tenga en cuenta la red y elija la configuración del entorno de ejecución de integración que sea adecuada para su escenario.
3. Tenga en cuenta las credenciales que vaya a usar para conectarse al origen. Todas las páginas de origen tendrán una sección Examen que incluirá detalles sobre qué tipos de autenticación están disponibles.

**Exámenes e ingesta en Microsoft Purview**

Las características de exploración e ingesta de Microsoft Purview conectan su cuenta de Microsoft Purview a los orígenes para rellenar el mapa de datos y el catálogo de datos para que pueda empezar a explorar y administrar los datos a través de Microsoft Purview.

* El **examen** captura metadatos de orígenes de datos y los lleva a Microsoft Purview.
* La **ingesta** procesa los metadatos y los almacena en el catálogo de datos de ambos:
  + Análisis de orígenes de datos: los metadatos escaneados se agregan al Mapa de datos de Microsoft Purview.
  + Conexiones de linaje: los recursos de transformación agregan metadatos sobre sus orígenes, salidas y actividades al Mapa de datos de Microsoft Purview.



**Examen**

Una vez registrados los orígenes de datos en la cuenta de Microsoft Purview, el siguiente paso es proceder a su examen. El proceso de examen establece una conexión con el origen de datos y captura metadatos técnicos, como nombres, tamaño de archivo, columnas, etc. También extrae el esquema de los orígenes de datos estructurados, aplica clasificaciones en esquemas y aplica etiquetas de confidencialidad si la cuenta del mapa de datos de Microsoft Purview está conectada a un portal de cumplimiento de Microsoft Purview. El proceso de examen se puede desencadenar para ejecutarse inmediatamente o se puede programar a fin de ejecutarse periódicamente para mantener actualizada la cuenta de Microsoft Purview.

Para cada examen, hay personalizaciones que puede aplicar para que solo examine la información que necesita, en lugar de todo el origen.

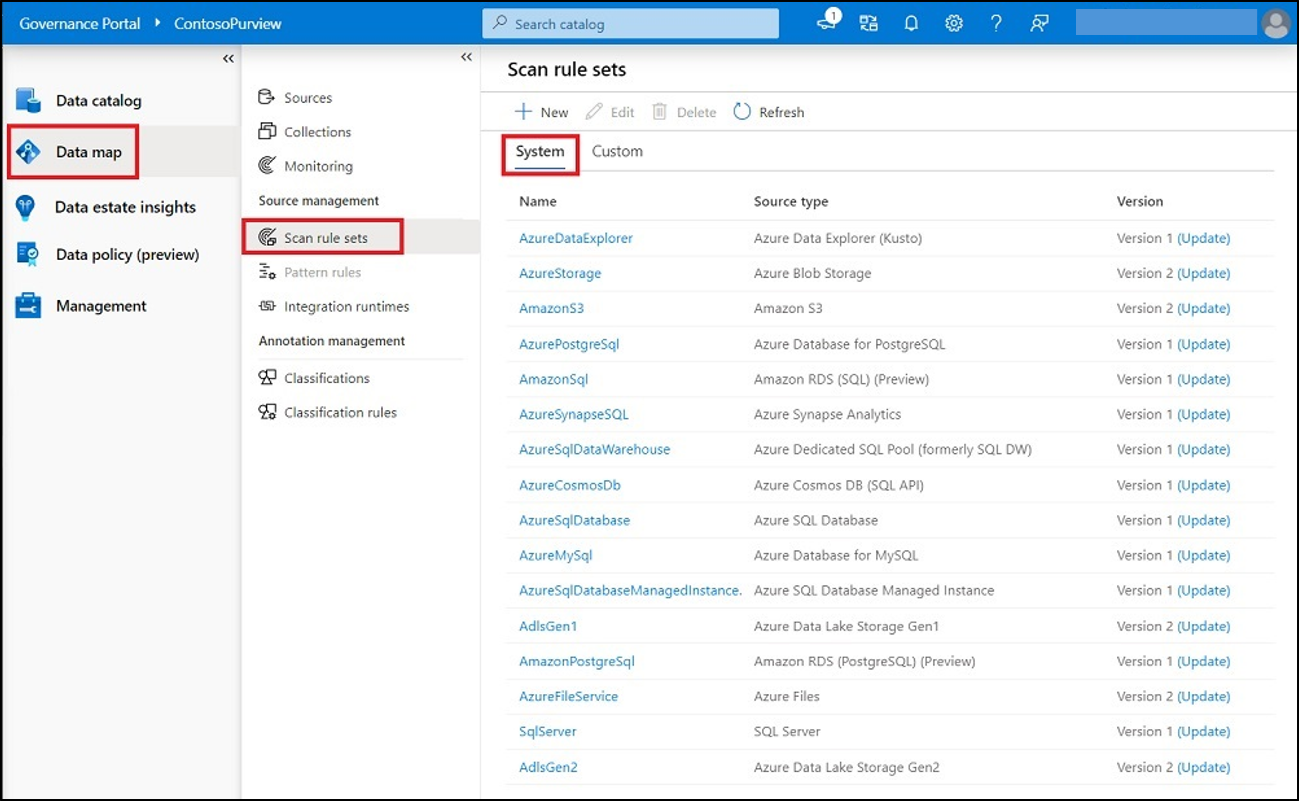
**Creación de un conjunto de reglas de examen**

En un catálogo de Microsoft Purview, puede crear conjuntos de reglas de examen para que pueda examinar rápidamente los orígenes de datos de su organización.

Un conjunto de reglas de examen es un contenedor para agrupar un conjunto de reglas de examen y que así pueda asociarlas fácilmente a un examen. Por ejemplo, puede crear un conjunto de reglas de examen predeterminado para cada uno de los tipos de orígenes de datos y, a continuación, usar estos conjuntos de reglas de examen de forma predeterminada en todos los exámenes de la empresa. También puede proporcionar a los usuarios los permisos adecuados para crear otros conjuntos de reglas de examen con diferentes configuraciones en función de las necesidades de la empresa.

**Conjuntos de reglas de examen del sistema**

Microsoft se encarga de definir los conjuntos de reglas de examen del sistema y se crean automáticamente para cada catálogo de Microsoft Purview. Cada conjunto de reglas de examen del sistema está asociado a un tipo de origen de datos específico. Al crear un examen, puede asociarlo a un conjunto de reglas de examen del sistema. Cada vez que Microsoft realiza una actualización en estos conjuntos de reglas del sistema, puede actualizarlos en el catálogo y aplicar la actualización en todos los exámenes asociados al conjunto.



**Clasificación: clasificación de datos en el Portal de gobernanza de Microsoft Purview**

La clasificación de datos, en el contexto del portal de gobernanza de Microsoft Purview, es una manera de categorizar los recursos de datos mediante la asignación de clases o etiquetas lógicas únicas a los recursos de datos. La clasificación se basa en el contexto empresarial de los datos. Por ejemplo, podría clasificar los recursos por *Número de pasaporte*, *Número de carné de conducir*, *Número de tarjeta de crédito*, *Código SWIFT*, *Nombre del usuario* y así sucesivamente.

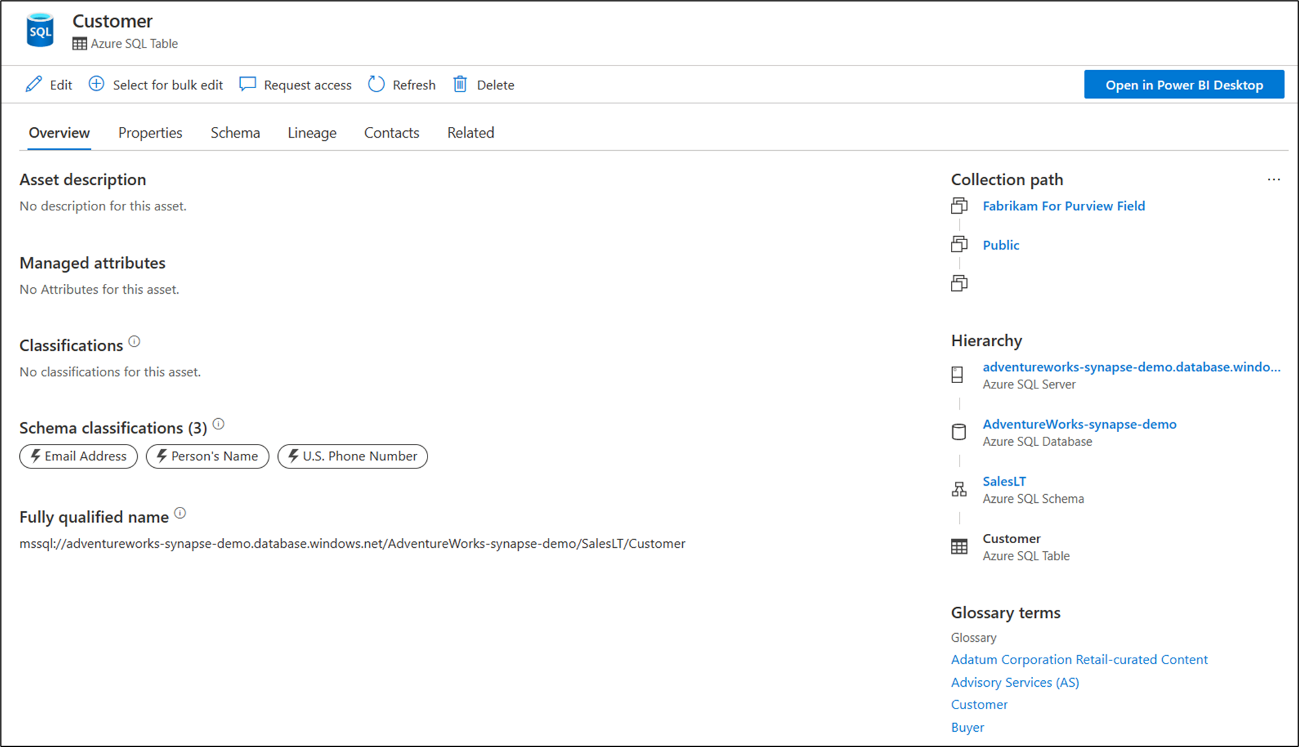
Al clasificar los recursos de datos, son más fáciles de entender, buscar y gobernar. La clasificación de recursos de datos también le ayuda a comprender los riesgos asociados a ellos. Esto, a su vez, puede ayudarle a implementar medidas para proteger los datos confidenciales o importantes frente a la proliferación no autorizada y el acceso no autorizado en todo el patrimonio de datos.

El mapa de datos de Microsoft Purview proporciona una capacidad de clasificación automatizada mientras se analizan los orígenes de datos. Se obtienen más de 200 clasificaciones del sistema integradas y la capacidad de crear clasificaciones personalizadas para los datos. Puede clasificar los recursos automáticamente cuando se ingieren como parte de un examen configurado, o bien puede editarlos manualmente en el Portal de gobernanza de Microsoft Purview después de examinarlos e ingerirlos.

**Usos de la clasificación**

La clasificación es el proceso de organizar los datos en *categorías lógicas* que hacen que los datos se recuperen, ordenen e identifiquen fácilmente para su uso futuro. Esto puede ser importante para la gobernanza de datos. Entre otras razones, la clasificación de recursos de datos es importante porque le ayuda a:

* Limitar la búsqueda de recursos de datos que le interesan.
* Organizar y comprender la variedad de clases de datos que son importantes en la organización y dónde se almacenan.
* Comprender los riesgos asociados a los recursos de datos más importantes y, después, tomar las medidas adecuadas para mitigarlos.



**Tipos de clasificación**

El portal de gobernanza de Microsoft Purview admite clasificaciones tanto del sistema como personalizadas.

* **Clasificaciones del sistema**: se admiten más de 200 clasificaciones del sistema, las que están listas para usar.

En el ejemplo de la imagen anterior, Nombre del usuario es una clasificación del sistema. La clasificación del sistema tiene el icono de rayo junto con el nombre de la clasificación. Mantener el puntero sobre la propia clasificación proporciona más detalles sobre el tipo de clasificación y más detalles sobre cómo se aplicó.

* **Clasificaciones personalizadas**: puede crear clasificaciones personalizadas cuando quiera clasificar recursos en función de un patrón o un nombre de columna específico que no esté disponible como clasificación del sistema. Las reglas de clasificación personalizada se pueden basar en un patrón de expresión regular o en un diccionario.

Imagine que la columna Employee ID sigue el patrón EMPLOYEE{GUID} (por ejemplo, EMPLOYEE9c55c474-9996-420c-a285-0d0fc23f1f55). Es posible la creación de su propia clasificación personalizada mediante una expresión regular, como \^Employee\[A-Za-z0-9\]{8}-\[A-Za-z0-9\]{4}-\[A-Za-z0-9\]{4}-\[A-Za-z0-9\]{4}-\[A-Za-z0-9\]{12}\$.

**Nota**

Las etiquetas de confidencialidad son diferentes de las clasificaciones. Las etiquetas de confidencialidad clasifican los recursos en el contexto de la seguridad y la privacidad de los datos, como *Extremadamente confidencial*, *Restringido*, *Público* y así sucesivamente. Para usar etiquetas de confidencialidad en el Mapa de datos de Microsoft Purview, necesitará al menos una licencia o cuenta de Microsoft 365 dentro del mismo inquilino de Microsoft Entra que el Mapa de datos de Microsoft Purview.

**Etiquetado en el mapa de datos de Microsoft Purview**

**Importante**

El etiquetado en el mapa de datos de Microsoft Purview se encuentra actualmente en versión preliminar. Los Términos de uso complementarios para las versiones preliminares de Microsoft Azure incluyen términos legales adicionales que se aplican a las características de Azure que se encuentran en la versión beta, en versión preliminar o que todavía no se han publicado con disponibilidad general.

Para trabajar, las personas de la organización colaboran con otras dentro y fuera de la organización. Los datos no siempre permanecen en la nube y, a menudo, se mueven por todas partes, en dispositivos, aplicaciones y servicios. Cuando los datos usen un perfil itinerante, deseará que estén protegidos de forma que se satisfagan las directivas empresariales y de cumplimiento de la organización.

La aplicación de etiquetas de confidencialidad al contenido le permite proteger los datos de su organización indicando la sensibilidad de algunos de ellos. También se sintetizan los propios datos, por lo que puede usar etiquetas para realizar un seguimiento del tipo de datos, sin exponer datos confidenciales en otra plataforma.

Por ejemplo, la aplicación de una etiqueta de confidencialidad "extremadamente confidencial" a un documento que contiene números de tarjeta de crédito y el número del seguro social ayuda a identificar la confidencialidad del documento sin conocer los datos reales del mismo.

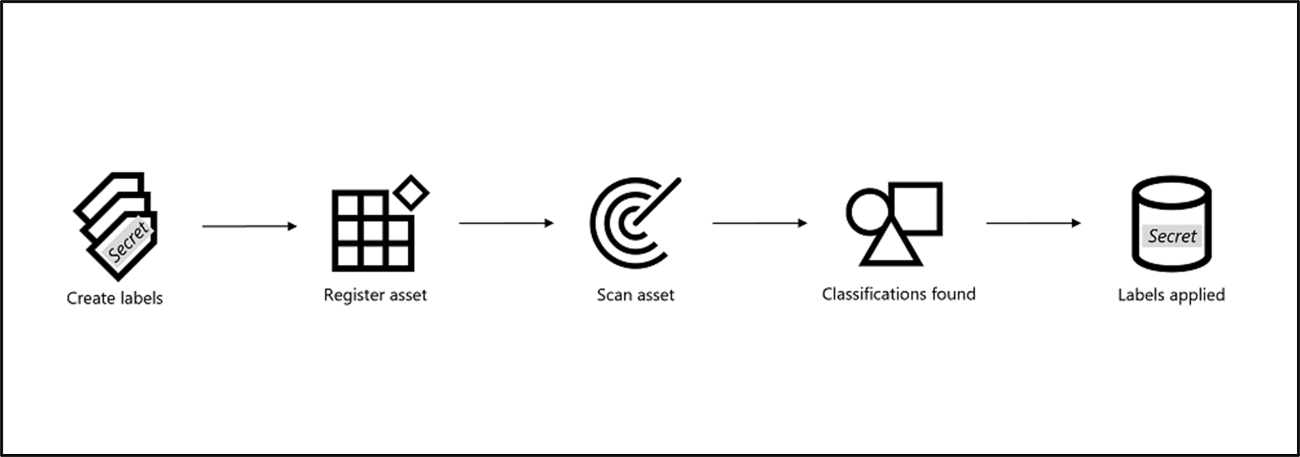
**Ventajas del etiquetado en Microsoft Purview**

Microsoft Purview permite aplicar etiquetas de confidencialidad a los recursos, de modo que puede clasificar y proteger los datos.

* **La etiqueta acompaña a los datos**: las etiquetas de confidencialidad creadas en Microsoft Purview Information Protection también se pueden ampliar al mapa de datos de Microsoft Purview, SharePoint, Teams, Power BI y SQL. Al aplicar una etiqueta a un documento de Office y, a continuación, examinarla en el mapa de datos de Microsoft Purview, la etiqueta se aplicará en el recurso de datos. Aunque la etiqueta se aplica al archivo real en Microsoft Purview Information Protection, solo se agrega como metadatos en el mapa de Microsoft Purview. Aunque hay diferencias en la forma de aplicar una etiqueta a un recurso en varios servicios o aplicaciones, las etiquetas viajan con los datos y todos los servicios a los que se extienden los reconocen.
* **Información general sobre el patrimonio de datos**: Microsoft Purview proporciona información sobre los datos mediante informes predefinidos. Al examinar datos en el mapa de datos de Microsoft Purview, los informes se hidratan con información sobre los recursos que tiene, el historial de análisis, las clasificaciones encontradas en los datos, las etiquetas aplicadas, los términos del glosario, etc.
* **Etiquetado automático:** las etiquetas se pueden aplicar automáticamente en función de la confidencialidad de los datos. Cuando se examina un recurso en busca de datos confidenciales, se usan reglas de etiquetado automático para decidir qué etiqueta de confidencialidad se va a aplicar. A fin de crear reglas de etiquetado automático para cada etiqueta de confidencialidad, defina qué tipo de clasificación o información confidencial constituye una etiqueta.
* **Aplicar etiquetas a archivos y columnas de base de datos**: Se pueden aplicar etiquetas a archivos en almacenamiento, como Azure Data Lake o Azure Files, así como a datos esquematizados, como columnas de Azure SQL Database.

**Etiquetas de confidencialidad** son etiquetas que es posible aplicar en los recursos para clasificar y proteger los datos.

**Procedimientos para aplicar etiquetas a recursos en el mapa de datos de Microsoft Purview**



Para poder aplicar etiquetas al recurso en el mapa de datos, es necesario realizar los pasos siguientes:

1. Crear etiquetas de confidencialidad nuevas o aplicar las existentes en el portal de cumplimiento de Microsoft Purview. La creación de etiquetas de confidencialidad incluye reglas de etiquetado automático que indican qué etiqueta se debe aplicar en función de las clasificaciones encontradas en los datos.
2. Registre y examine el recurso en el mapa de datos de Microsoft Purview.
3. Microsoft Purview aplica **clasificaciones**: al programar un examen en un recurso, Microsoft Purview examina el tipo de datos del recurso y le aplica clasificaciones en el mapa de datos. Microsoft Purview realiza automáticamente la aplicación de clasificaciones; no se tiene que realizar ninguna acción.
4. Microsoft Purview aplica **etiquetas**: una vez que se encuentran las clasificaciones en un recurso, Microsoft Purview le aplicará etiquetas en función de las reglas de etiquetado automático. Microsoft Purview realiza automáticamente la aplicación de etiquetas; no se tiene que realizar ninguna acción, siempre que se hayan creado etiquetas con reglas de etiquetado automático en el paso 1.

**Nota**

Las **reglas de etiquetado automático** son condiciones que se pueden especificar e indican cuándo se debería aplicar una etiqueta determinada. Cuando se cumplan estas condiciones, la etiqueta se asigna automáticamente a los datos. Al crear las etiquetas, asegúrese de definir reglas de etiquetado automático para los archivos y las columnas de bases de datos para aplicar las etiquetas automáticamente con cada examen de datos.

**Etiquetado de bases de datos SQL**

Además del etiquetado de Mapa de datos de Microsoft Purview para recursos de datos esquematizados, Microsoft también admite el etiquetado para columnas de base de datos SQL mediante la clasificación de datos SQL en SQL Server Management Studio (SSMS). Aunque Microsoft Purview usa las etiquetas de confidencialidad globales, SSMS solo usa etiquetas definidas localmente.

El etiquetado en Microsoft Purview y el etiquetado en SSMS son procesos independientes que actualmente no interactúan entre sí. Por lo tanto, **las etiquetas que se aplican en SSMS no se muestran en Microsoft Purview, y viceversa**. Se recomienda Microsoft Purview para etiquetar las bases de datos SQL, porque las etiquetas se pueden aplicar globalmente en varias plataformas.

**Planeamiento e implementación de enmascaramiento dinámico**

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 Microsoft Entra ID que obtendrán datos sin máscara en los resultados de la 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**

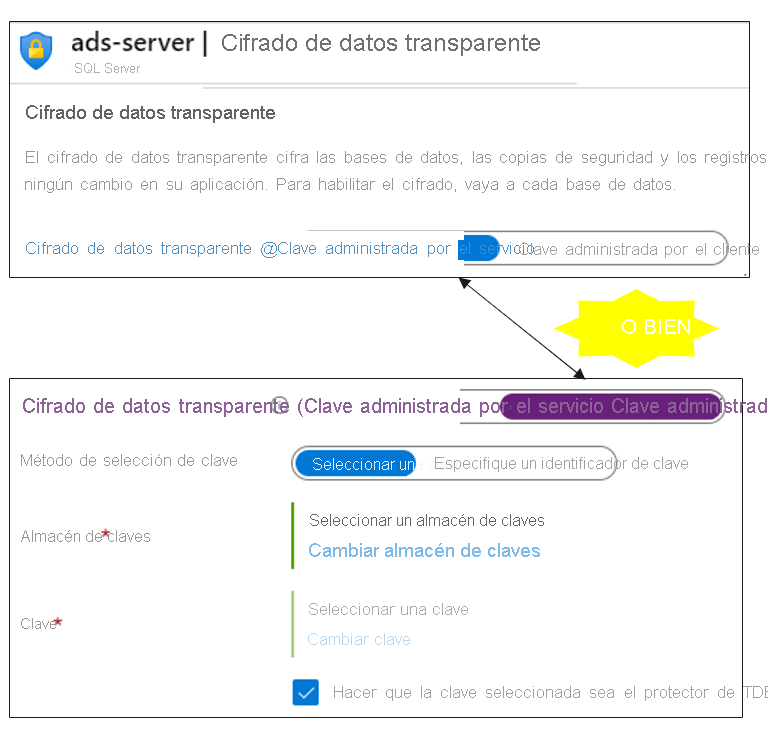
En Azure, la configuración predeterminada de TDE es que la clave de cifrado está protegida mediante un certificado de servidor integrado. El certificado de servidor integrado es único para cada servidor y el algoritmo de cifrado que se usa es AES 256. Si una base de datos está en una relación de replicación 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.

**Recomendar cuándo usar Always Encrypted de Azure SQL Database**

Asegúrese de que la base de datos siempre está cifrada.

**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.

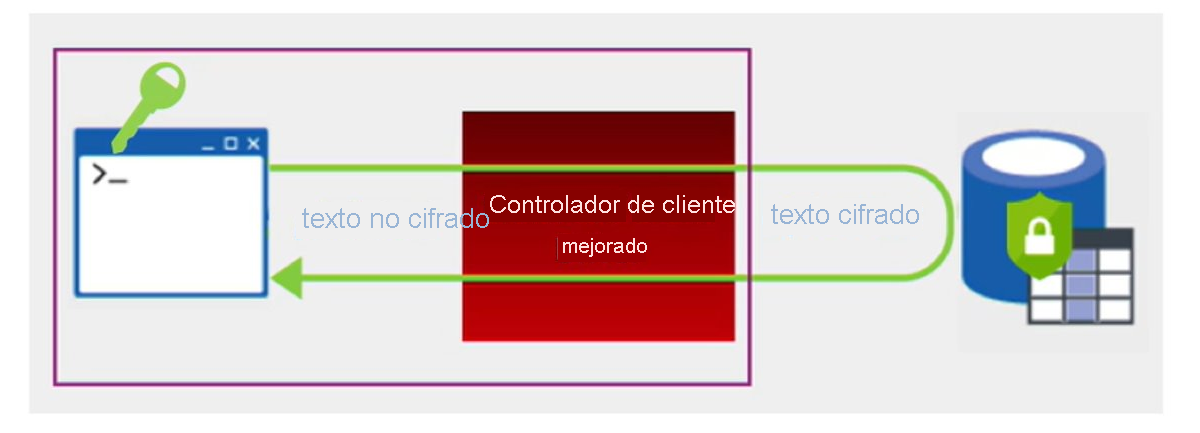
**Escenarios de uso de ejemplo**

**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.

**Prueba de conocimientos**

Elija la mejor respuesta para cada una de las preguntas. Después, seleccione **Comprobar las respuestas**.

**Comprobación de conocimientos**

Principio del formulario

**1. ¿Cuál es el propósito de examinar un origen de datos en Microsoft Purview?**

1. Para modificar el origen de datos en el portal de gobernanza de Microsoft Purview
2. Para eliminar el origen de datos del mapa de datos de Microsoft Purview
3. Para capturar metadatos técnicos, extraiga el esquema y aplique clasificaciones a los datos

**2. ¿Cuál es el propósito de la automatización y validación del entorno?**

1. Habilita la creación y desmontaje manual de entornos
2. Habilita la creación de plataformas de hospedaje de aplicaciones inestables
3. Permite la automatización y la validación de la creación y el desmontaje de entornos para contribuir a ofrecer plataformas de hospedaje de aplicaciones seguras y estables

**3. ¿Cuál es el propósito de la autenticación en una base de datos segura?**

1. Para limitar los permisos concedidos a la aplicación
2. Para determinar qué acciones puede realizar un usuario
3. Para demostrar que el usuario es quien dice ser

**4. Una aplicación web de App Service usa una base de datos SQL. Los usuarios deben autenticarse en la base de datos con sus credenciales de Azure AD. ¿Cuál de las siguientes tareas de configuración habilitaría esto?**

1. Creación de un administrador de SQL Database
2. Creación de un administrador de base de datos de Azure AD
3. Creación de usuarios en cada base de datos

**5. ¿Cuál es el propósito del cifrado determinista?**

1. Para evitar la búsqueda, agrupación, indexación y combinación en columnas cifradas
2. Para cifrar los datos de una manera menos predecible
3. Habilitar la automatización y validación de la creación y el desmontaje de entornos para contribuir a ofrecer plataformas de hospedaje de aplicaciones seguras y estables
4. C
5. C
6. C
7. C
8. C

Final del formulario

**Resumen**

En este módulo, ha aprendido a planear e implementar medidas de seguridad sólidas para Azure SQL Database y Azure SQL Managed Instance, incluida la habilitación de la autenticación segura de bases de datos con Microsoft Enterprise Identity, auditoría de bases de datos, uso del portal de gobernanza de Microsoft Purview para la clasificación de datos, la implementación de enmascaramiento dinámico para información confidencial, cifrado de base de datos transparente (TDE) y la toma de decisiones fundamentadas sobre cuándo usar Azure SQL Database Always Encrypted para cifrado de datos del lado cliente.