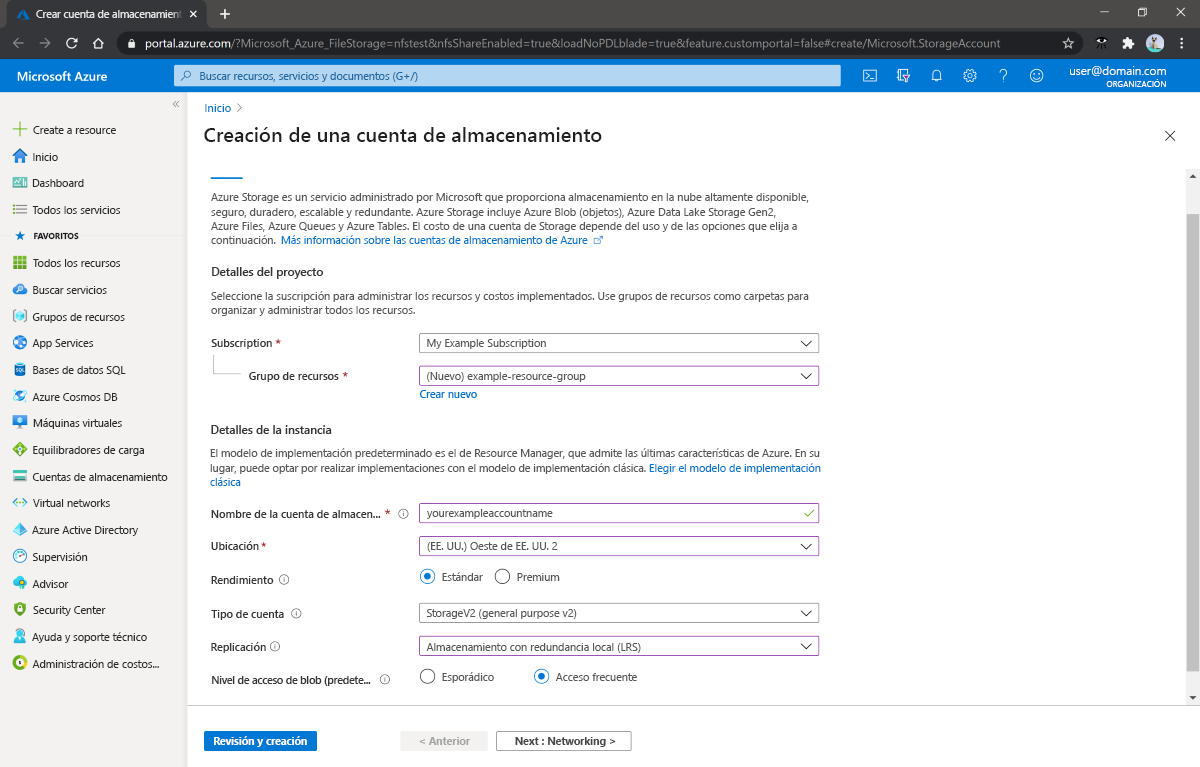
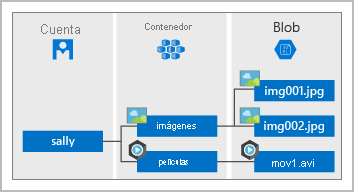
Para empezar a usar Azure Storage, cree primero una cuenta de Azure Storage para almacenar los objetos de datos. Puede crear una cuenta de Azure Storage mediante Azure Portal, PowerShell o la CLI de Azure.



La cuenta de almacenamiento contendrá todos los objetos de datos de Azure Storage, como blobs, archivos y discos.

**Nota**

Las VM de Azure usan Azure Disk Storage para almacenar discos virtuales. Sin embargo, no puede usar Azure Disk Storage para almacenar un disco fuera de una máquina virtual.



Una cuenta de almacenamiento proporciona un espacio de nombres único para los datos de Azure Storage, al que se puede acceder desde cualquier lugar del mundo a través de HTTP o HTTPS. Los datos de esta cuenta son seguros, de alta disponibilidad, duraderos y escalables de forma masiva.

Para obtener más información, consulte [Creación de una cuenta de almacenamiento](https://docs.microsoft.com/es-es/azure/storage/common/storage-account-create).

**Aspectos básicos de Disk Storage**

Completado100 XP

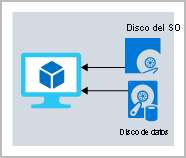
* 4 minutos

Disk Storage proporciona discos para Azure Virtual Machines. Las aplicaciones y otros servicios pueden acceder a estos discos y usarlos cuando sea necesario, igual que se haría en escenarios locales. Disk Storage permite que los datos se almacenen de forma persistente y que se acceda a ellos desde un disco duro virtual conectado.



Los discos tienen diferentes tamaños y niveles de rendimiento, desde unidades de estado sólido (SSD) a unidades de disco duro (HDD) giratorias tradicionales, con diferentes niveles de rendimiento. Puede usar discos SSD y HDD estándar para cargas de trabajo menos críticas, discos SSD Premium para aplicaciones de producción críticas y Ultra Disks para cargas de trabajo con un uso intensivo de datos como SAP HANA, bases de datos de nivel superior y cargas de trabajo con mucha actividad de transacciones. Azure han ofrecido durabilidad de nivel empresarial de forma coherente para los discos de infraestructura como servicio (IaaS), con una tasa de error anualizada del 0 % líder del sector.

En la siguiente ilustración se muestra una máquina virtual de Azure que usa discos independientes para almacenar datos diferentes.



**Aspectos básicos de Azure Blob Storage**

Completado100 XP

* 4 minutos

Azure Blob Storage es una solución de almacenamiento de objetos para la nube. Puede almacenar grandes cantidades de datos, como datos de texto o binarios. Azure Blob Storage es no estructurado, lo que significa que no hay ninguna restricción en cuanto a los tipos de datos que puede contener. Blob Storage puede administrar miles de cargas simultáneas, cantidades enormes de datos de vídeo, archivos de registro en constante crecimiento y es accesible desde cualquier lugar con conexión a Internet.



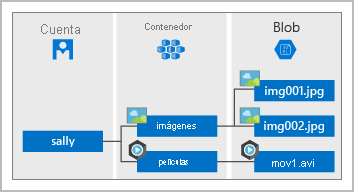
Los blobs no están limitados a formatos de archivo comunes. Un blob podría contener gigabytes de datos binarios transmitidos desde un instrumento científico, un mensaje cifrado para otra aplicación o datos en un formato personalizado para una aplicación que se está desarrollando. Una ventaja del almacenamiento en blobs con respecto al almacenamiento en disco es que no requiere que los desarrolladores piensen en discos o los administren; los datos se cargan como blobs y Azure se encarga de las necesidades de almacenamiento físico.

Blob Storage resulta ideal para lo siguiente:

* Visualización de imágenes o documentos directamente en un explorador.
* Almacenamiento de archivos para acceso distribuido.
* Streaming de audio y vídeo.
* Almacenamiento de datos para copia de seguridad y restauración, recuperación ante desastres y archivado.
* Almacenamiento de datos para el análisis en local o en un servicio hospedado de Azure.
* Almacenamiento de hasta 8 TB de datos para máquinas virtuales.

Los blobs se almacenan en contenedores, lo que ayuda a organizar los blobs en función de sus necesidades empresariales.

En el diagrama siguiente se muestra cómo puede usar las cuentas, los contenedores y los blobs de Azure.



**Aspectos básicos de Azure Files**

Completado100 XP

* 4 minutos

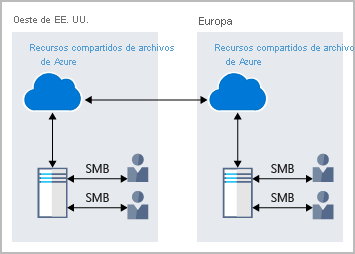
Azure Files ofrece recursos compartidos de archivos totalmente administrados en la nube a los que se puede acceder mediante los protocolos del Bloque de mensajes del servidor y Network File System (versión preliminar). Los recursos compartidos de Azure se pueden montar simultáneamente en implementaciones de Windows, Linux y macOS en la nube o locales. Las aplicaciones que se ejecutan en máquinas virtuales o servicios en la nube de Azure pueden montar un recurso compartido de almacenamiento de archivos para acceder a datos de archivos, del mismo modo que una aplicación de escritorio montaría un recurso compartido SMB normal. Cualquier número de roles o máquinas virtuales de Azure puede montar y acceder simultáneamente al recurso compartido de almacenamiento de archivos. Los escenarios de uso típicos serían el uso compartido de archivos en cualquier lugar del mundo, los datos de diagnóstico o el uso compartido de datos de aplicación.



Use Azure Files para las siguientes situaciones:

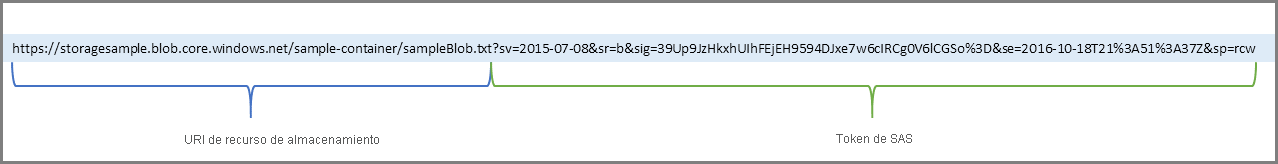
* Muchas aplicaciones locales usan recursos compartidos de archivos. Azure Files facilita la migración de esas aplicaciones que comparten datos a Azure. Si monta el recurso compartido de archivos en la misma letra de unidad que usa la aplicación local, la parte de la aplicación que accede al recurso compartido de archivos debe funcionar con cambios mínimos, si los hay.
* Almacene archivos de configuración en un recurso compartido de archivos y acceda a ellos desde varias máquinas virtuales. Las herramientas y utilidades que usen varios desarrolladores de un grupo pueden almacenarse en un recurso compartido de archivos, lo que garantiza que todos los usuarios puedan encontrarlas y que utilizan la misma versión.
* Escriba datos en un recurso compartido de archivos y procese o analice los datos más adelante. Por ejemplo, puede que desee hacerlo con registros de diagnóstico, métricas y volcados de memoria.

La siguiente ilustración muestra el uso de Azure Files para compartir datos entre dos ubicaciones geográficas. Azure Files garantiza que los datos se cifren en reposo, y el protocolo SMB garantiza que los datos se cifren en tránsito.



Una cosa que distingue Azure Files de los archivos ubicados en un recurso compartido de archivos corporativo es que puede tener acceso a los archivos desde cualquier lugar del mundo mediante una dirección URL que apunte al archivo. También puede usar tokens de Firma de acceso compartido (SAS) para permitir el acceso a un recurso privado durante un período de tiempo determinado.

Este es un ejemplo de un URI de SAS de servicio, que muestra el URI de recurso y el token de SAS:



**Descripción de los niveles de acceso de blobs**

Completado100 XP

* 4 minutos

Los datos almacenados en la nube pueden crecer a un ritmo exponencial. Para administrar los costos de las crecientes necesidades de almacenamiento, resulta útil organizar los datos en función de atributos como la frecuencia de acceso y el período de retención planeada. Los datos almacenados en la nube pueden ser diferentes según la forma en que se generan, se procesan y se accede a ellos a lo largo de su vigencia. A algunos datos se accede y se modifican activamente a lo largo de su duración. A algunos datos se accede con frecuencia al principio de su duración, mientras que el acceso cae drásticamente a medida que envejecen los datos. Algunos datos permanecen inactivos en la nube y, después de que se almacenan, no se accede a ellos prácticamente nunca. Para dar cabida a estas diferentes necesidades de acceso, Azure proporciona varios *niveles de acceso*, que puede usar para equilibrar los costos de almacenamiento con sus necesidades de acceso.



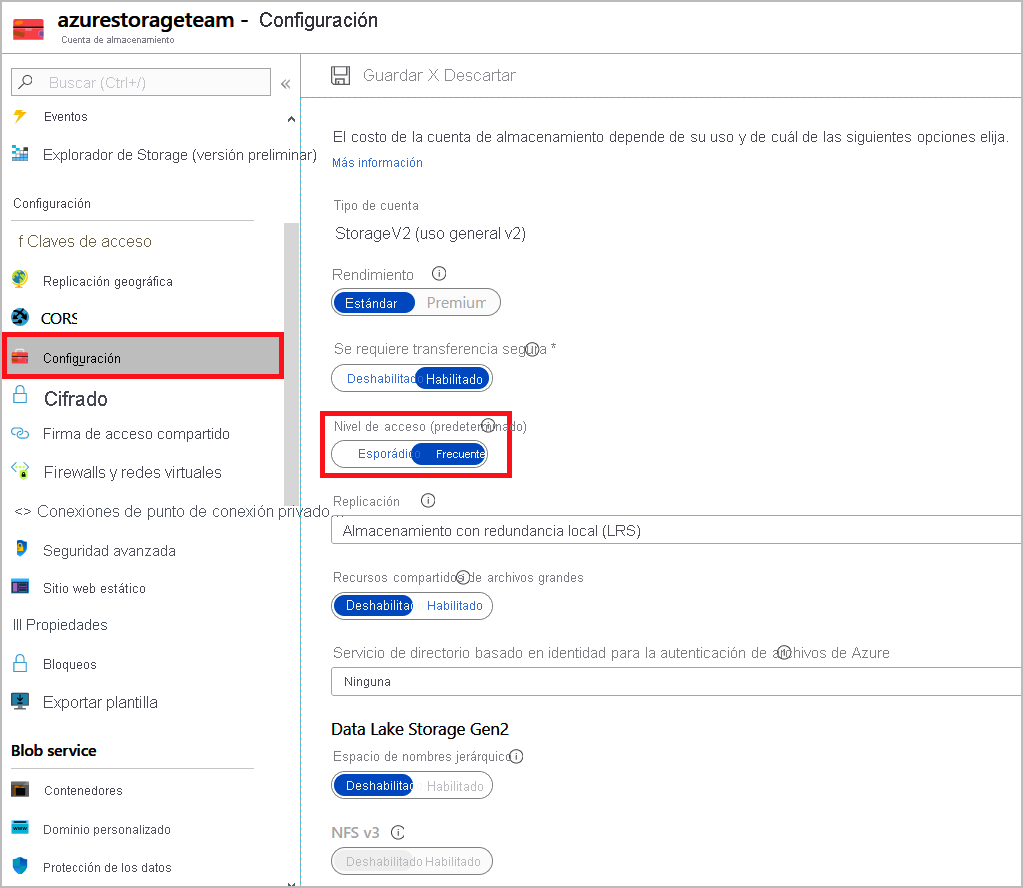
Azure Storage ofrece diferentes niveles de acceso para el almacenamiento de blobs, lo que le ayuda a almacenar datos de objetos de la manera más rentable. Entre los niveles de acceso disponibles se incluyen:

* **Nivel de acceso frecuente**: optimizado para almacenar datos a los que se accede con frecuencia (por ejemplo, imágenes para el sitio web).
* **Nivel de acceso esporádico**: optimizado para datos a los que se accede con poca frecuencia y que se almacenan al menos durante 30 días (por ejemplo, las facturas de los clientes).
* **Nivel de acceso de archivo**: conveniente para datos a los que raramente se accede y que se almacenan durante al menos 180 días con requisitos de latencia flexibles (por ejemplo, copias de seguridad a largo plazo).

Las siguientes consideraciones se aplican a los distintos niveles de acceso:

* Solo los niveles de acceso frecuente y esporádico se pueden establecer en el nivel de cuenta. El nivel de acceso de archivo no está disponible en el nivel de cuenta.
* Los niveles frecuente, esporádico y de archivo se pueden establecer en el nivel de blob durante la carga o después de esta.
* Los datos del nivel de acceso esporádico pueden tolerar una disponibilidad ligeramente inferior, pero aun así requieren una gran durabilidad, una latencia de recuperación y unas características de rendimiento similares a las de los datos de acceso frecuente. En el caso de los datos de acceso esporádico, un contrato de nivel de servicio (SLA) con una disponibilidad ligeramente inferior y unos costos de acceso mayores, en comparación con los datos de acceso frecuente, es aceptable a cambio de unos costos de almacenamiento menores.
* El almacenamiento de archivo almacena datos sin conexión y ofrece los menores costos de almacenamiento, pero los mayores costos de acceso y rehidratación de datos.

En la ilustración siguiente se muestra cómo elegir entre los niveles de acceso frecuente y esporádico en una cuenta de almacenamiento de uso general.



# Ejercicio: Creación de una base de datos SQL

Completado100 XP

* 12 minutos

Microsoft Learn necesita su permiso para crear recursos de Azure.

Para obtener más información, consulte la [**página de la guía de solución de problemas**](https://docs.microsoft.com/en-us/learn/support/troubleshooting).

[**Revisar permisos**](https://login.microsoftonline.com/redeem?rd=https%3a%2f%2finvitations.microsoft.com%2fredeem%2f%3ftenant%3d604c1504-c6a3-4080-81aa-b33091104187%26user%3d174a88e4-e24c-4183-b6be-6fe9086d2128%26ticket%3dohcEKJ7umXL9q2hLqFd4CZjvgy6M%25252bohRlx7HS5vVfBI%25253d%26ver%3d2.0)

Tailwind Traders ha elegido Azure SQL Database para parte de la migración. Se le ha encargado la creación de la base de datos.

En este ejercicio, creará una base de datos SQL en Azure y, después, consultará los datos de dicha base de datos.

## Tarea 1: Creación de la base de datos

En esta tarea, creará una base de datos SQL basada en la base de datos de ejemplo AdventureWorksLT.

1. Inicie sesión en [Azure Portal](https://portal.azure.com/learn.docs.microsoft.com).
2. Seleccione **Crear un recurso**>**Bases de datos**>**SQL Database**. Aparecerá el panel **Crear base de datos SQL**.
3. Escriba los valores siguientes para cada opción.

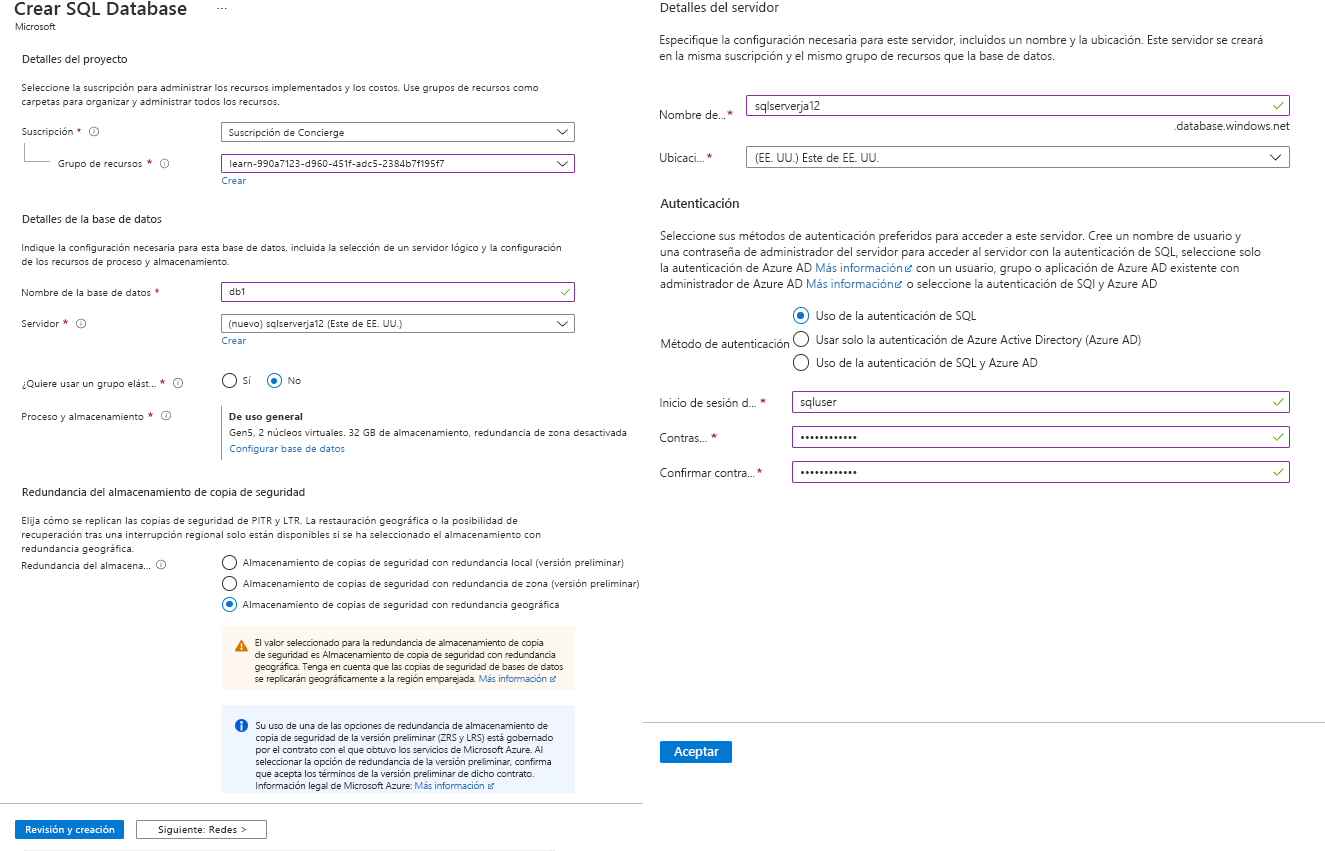
| **Configuración** | **Value** |
| --- | --- |
| **Detalles del proyecto** |  |
| Subscription | Suscripción de Concierge |
| Grupo de recursos | [Grupo de recursos del espacio aislado] |
| **Detalles de la base de datos** |  |
| Nombre de la base de datos | bd1 |
| Servidor | Seleccione **Crear nuevo**. |

1. Aparecerá el panel **Crear un servidor de SQL Database**.
2. Escriba los valores siguientes para cada opción.

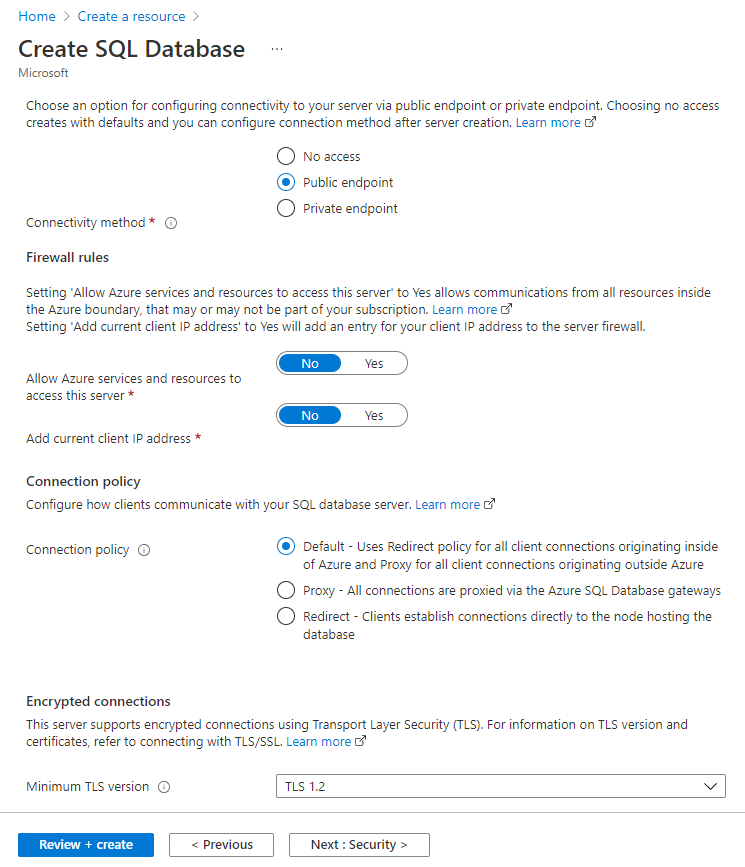
| **Configuración** | **Valor** |
| --- | --- |
| **Detalles del servidor** |  |
| Nombre de servidor | sqlservernnnn (reemplace **nnnn** por letras y dígitos para crear un nombre globalmente único) |
| Location | (EE. UU.) Este de EE. UU. |
| **Autenticación** |  |
| Método de autenticación | Uso de la autenticación de SQL |
| Inicio de sesión del administrador del servidor | sqluser |
| Contraseña | Pa$$w0rd1234 |

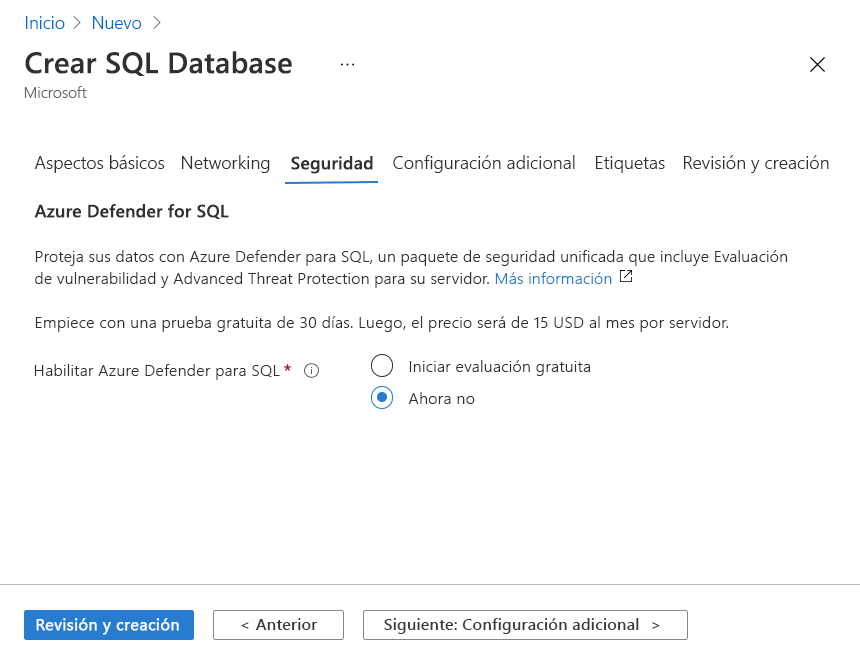
1. Seleccione **Aceptar**.
2. Complete los campos restantes de **Crear una base de datos SQL** con los valores siguientes.

| **Configuración** | **Valor** |
| --- | --- |
| ¿Quiere usar un grupo elástico de SQL? | No (valor predeterminado) |
| Proceso y almacenamiento | De uso general (valor predeterminado) |
| **Redundancia del almacenamiento de copia de seguridad** |  |
| Redundancia del almacenamiento de copia de seguridad | Almacenamiento de copias de seguridad con redundancia geográfica |

1. [](https://docs.microsoft.com/es-es/learn/azure-fundamentals/azure-database-fundamentals/media/server-pane-df80b536.png#lightbox)
2. Seleccione **Siguiente: Redes** y configure las siguientes opciones (acepte los valores predeterminados para los campos no especificados).

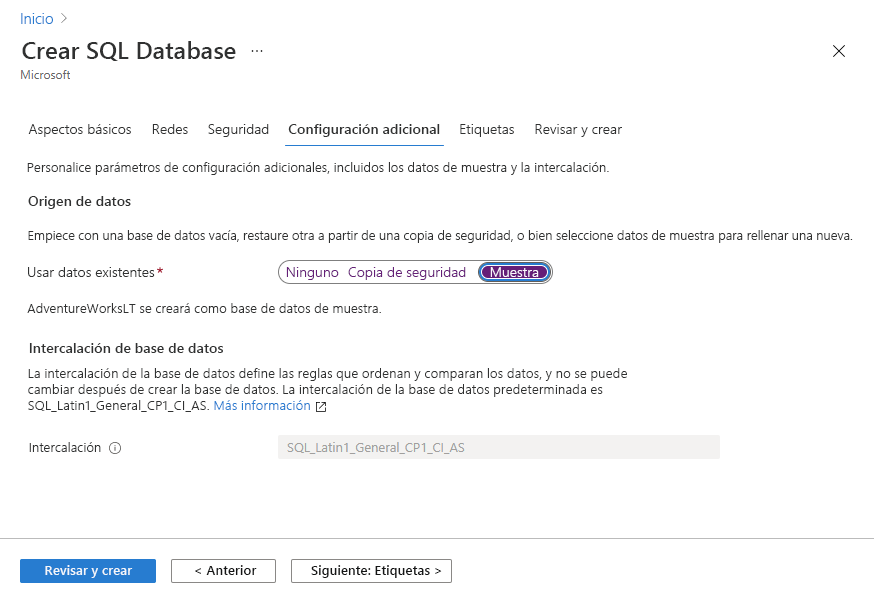
| **Configuración** | **Valor** |
| --- | --- |
| **Conectividad de red** |  |
| Método de conectividad | Punto de conexión público |

1. 
2. Seleccione **Siguiente: Seguridad** y, en **Habilitar Azure Defender para SQL**, elija **Ahora no**. Deje la configuración restante como predeterminada (no configurada).



1. Seleccione **Siguiente: Configuración adicional** y configure las siguientes opciones.

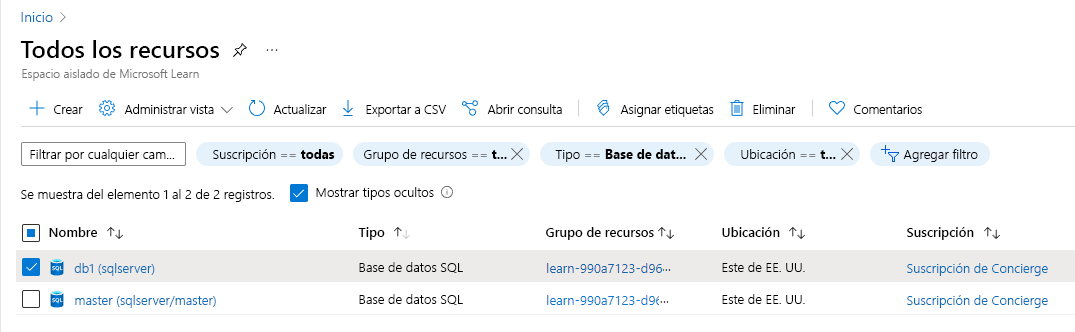
| **Configuración** | **Valor** |
| --- | --- |
| **Origen de datos** |  |
| Usar datos existentes | Muestra |
| **Intercalación de base de datos** |  |
| Intercalación | SQL\_Latin1\_General\_CP1\_CI\_AS (default) |

1. 
2. Seleccione **Revisar y crear** para validar las entradas de la configuración.
3. Seleccione **Crear** para implementar el servidor y la base de datos. La creación del servidor y la implementación de la base de datos de ejemplo pueden tardar aproximadamente entre dos y cinco minutos. El panel de implementación muestra el estado, con actualizaciones para cada recurso que se crea.
4. Una vez finalizada la implementación, seleccione **Ir al recurso**. El panel de información general de la base de datos SQL db1 muestra los aspectos básicos de la base de datos recién implementada.
5. En la barra de comandos, seleccione **Establecer el firewall del servidor**. Aparecerá la página **Configuración de firewall**.
6. Active la casilla junto a **Permitir que los servicios y recursos de Azure accedan a este servidor** en la parte inferior de la página, y deje las demás opciones de configuración en sus valores predeterminados.
7. Seleccione **Guardar** para actualizar la configuración del firewall y, a continuación, cierre el panel de configuración del firewall.

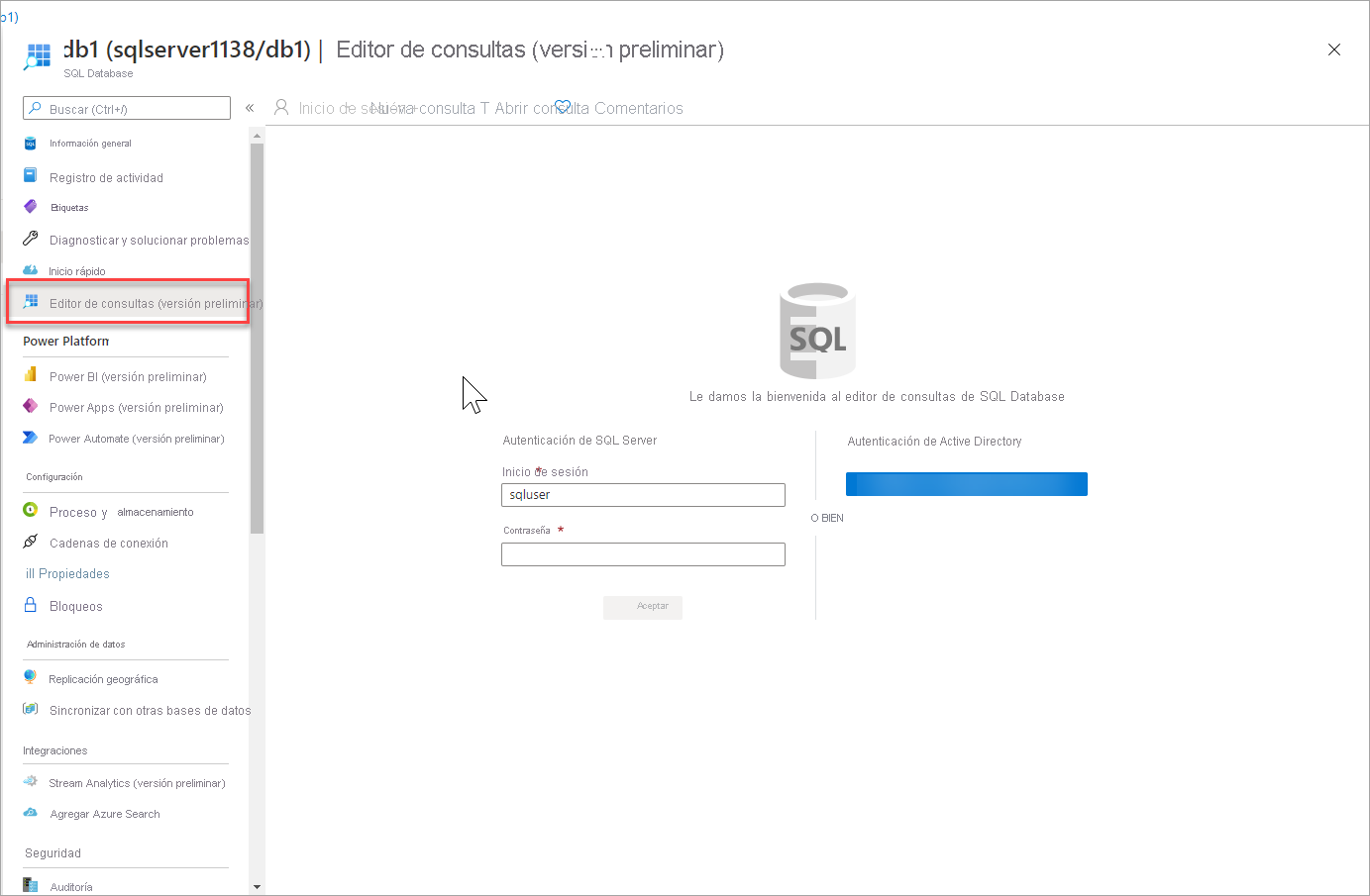
## Tarea 2: Probar la base de datos

En esta tarea, configurará el servidor y ejecutará una consulta SQL.

1. En el menú de recursos de Azure, seleccione **Todos los recursos**. En Tipo de recurso, busque y seleccione **Base de datos SQL** y asegúrese de que se ha creado la nueva base de datos. Es posible que tenga que actualizar la página.

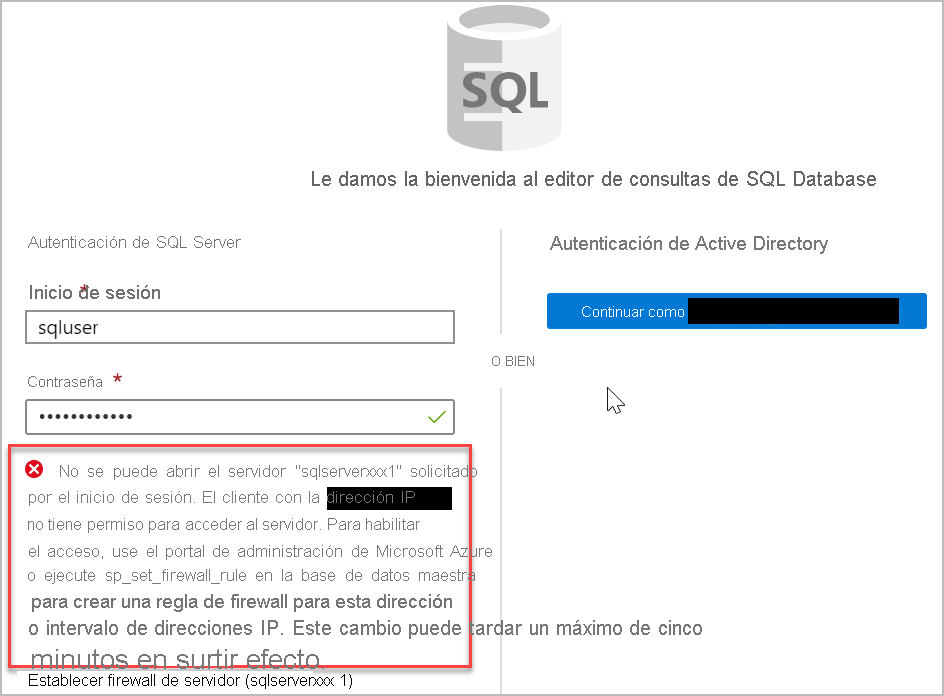


1. Seleccione **db1**, la base de datos SQL que ha creado.
2. En el menú de Base de datos SQL, seleccione **Editor de consultas (versión preliminar)** . Aparecerá el panel **Editor de consultas (versión preliminar)**.

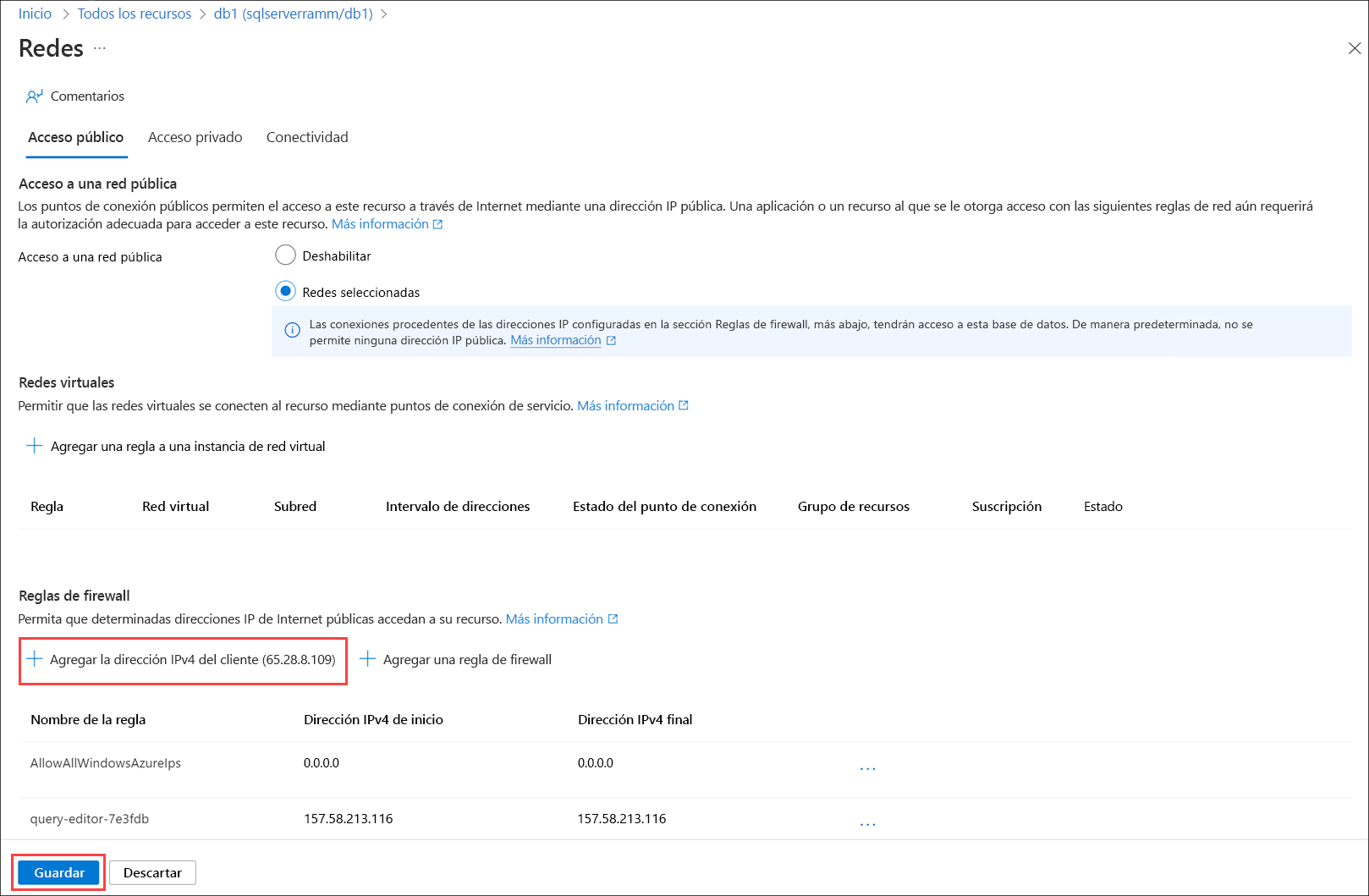


1. Inicie sesión como **sqluser** con la contraseña **Pa$$w0rd1234**.

No podrá iniciar sesión porque la dirección IP debe estar habilitada en una regla del firewall.



1. En el menú Editor de consultas, seleccione **Información general** (los cambios se perderán) y, en la barra de comandos, seleccione **Establecer el firewall del servidor**. Aparecerá la página **Configuración de firewall**.
2. En la sección **Dirección IP del cliente**, se mostrará la dirección IP; compruebe que se trata de la misma dirección IP del cliente del error que ha recibido en el paso anterior.
3. En la barra de comandos, seleccione **Agregar dirección IPv4 del cliente**. Se agregará un **Nombre de regla** que contiene la dirección IP en los campos **IP inicial** e **IP final**.
4. Seleccione **Guardar** para guardar esta regla de firewall.

[](https://docs.microsoft.com/es-es/learn/azure-fundamentals/azure-database-fundamentals/media/sql-server-firewall-settings-1b917b84.png#lightbox)

1. Seleccione la base de datos db1 en la ruta de navegación de la parte superior de la página para volver a la base de datos SQL y, a continuación, seleccione **Editor de consultas (versión preliminar)** en el menú.
2. Vuelva a iniciar sesión como **sqluser** con la contraseña **Pa$$w0rd1234**. Esta vez debería poder hacerlo. La nueva regla de firewall podría tardar un par de minutos en implementarse. Si sigue apareciendo un error, compruebe la dirección IP del cliente en el error y vuelva **Configuración del firewall** para agregar la dirección IP correcta del cliente.
3. Después de iniciar sesión correctamente, aparece el panel de consulta. Escriba la siguiente consulta SQL en el panel del editor.

SQLCopiar

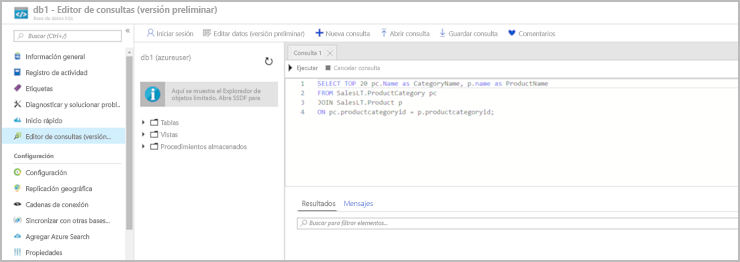
SELECT TOP 20 pc.Name as CategoryName, p.name as ProductName

FROM SalesLT.ProductCategory pc

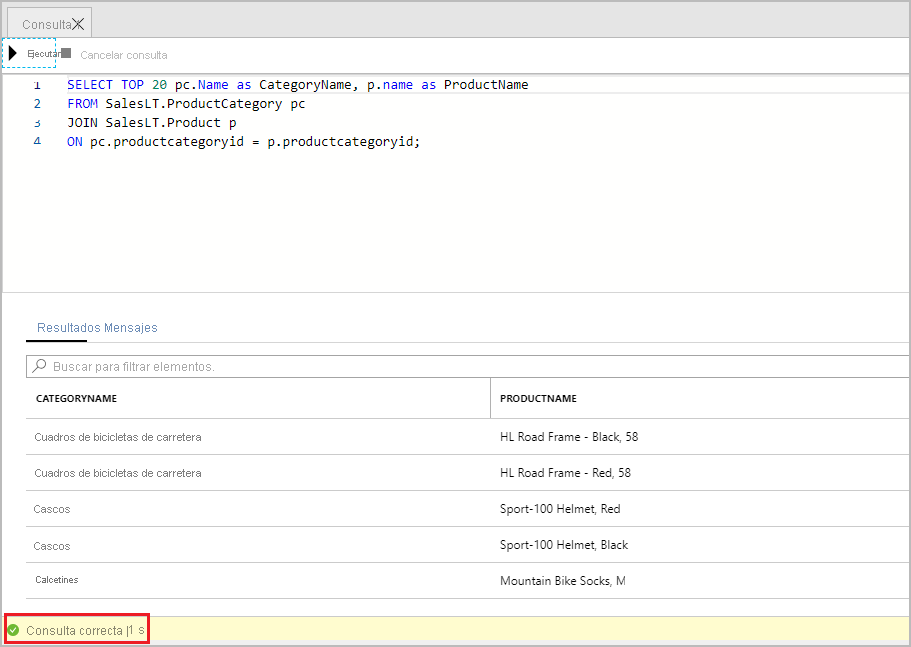
JOIN SalesLT.Product p

ON pc.productcategoryid = p.productcategoryid;

Explain



1. Seleccione **Ejecutar** y examine los resultados de la consulta en el panel **Resultados**. La consulta debería ejecutarse correctamente.



¡Enhorabuena! Ha creado una base de datos SQL en Azure y ha consultado correctamente los datos de dicha base de datos.