TaurusDB

Descripción del servicio

Edición	01
Fecha	2025-08-06

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Marcas registradas y permisos

El logotipo HUAWEI y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd.
Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

Aviso

Es posible que la totalidad o parte de los productos, las funcionalidades y/o los servicios que figuran en el presente documento no se encuentren dentro del alcance de un contrato vigente entre Huawei Cloud y el cliente. Las funcionalidades, los productos y los servicios adquiridos se limitan a los estipulados en el respectivo contrato. A menos que un contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en el presente documento constituye garantía alguna, ni expresa ni implícita.

Huawei está permanentemente preocupada por la calidad de los contenidos de este documento; sin embargo, ninguna declaración, información ni recomendación aquí contenida constituye garantía alguna, ni expresa ni implícita. La información contenida en este documento se encuentra sujeta a cambios sin previo aviso.

Huawei Cloud Computing Technologies Co., Ltd.

Dirección: Huawei Cloud Data Center Jiaoxinggong Road
Avenida Qianzhong
Nuevo distrito de Gui'an
Gui Zhou, 550029
República Popular China

Sitio web: https://www.huaweicloud.com/intl/es-us/

Índice

1 Qué es TaurusDB

TaurusDB es una base de datos nativa de la nube de grado empresarial totalmente compatible con MySQL. Desacopla el cómputo del almacenamiento y utiliza la virtualización de funciones de datos (DFV) desarrollada por Huawei, que escala hasta 128 TB por instancia. Una conmutación por falla se puede completar en segundos. Proporciona el rendimiento superior y la alta disponibilidad de una base de datos comercial al precio de una base de datos de código abierto.

Para obtener detalles sobre los motores y las versiones de BD compatibles con TaurusDB, véase **Motores y versiones de BD**.

Aprendizaje progresivo

Puede ir a **Conocimiento progresivo** para aprender sobre los conceptos básicos y el uso de TaurusDB.

Cómo usar TaurusDB

Puede crear y gestionar instancias de TaurusDB en la **consola de gestión** basada en web.

Para ayudarle a sacar el máximo partido de TaurusDB, vea **Ventajas**.

Ventajas

- Rendimiento
  - Al desacoplar el cómputo del almacenamiento y usar una arquitectura de "registro como base de datos", TaurusDB ofrece siete veces el rendimiento de las bases de datos de código abierto.
  - Remote Direct Memory Access (RDMA) se utiliza para la transferencia de datos en sistemas de bases de datos para romper el cuello de botella de rendimiento de E/S.
  - TaurusDB admite funciones del núcleo, como caché de resultados de consultas, caché de planes de consultas y DDL en línea, para mejorar la experiencia del usuario.
- Escalabilidad
  - Escalado horizontal: además de un nodo principal, puede agregar hasta 15 réplicas de lectura para que una instancia maneje solicitudes de alta simultaneidad.
  - Escalado vertical: puede escalar hacia arriba o hacia abajo las especificaciones de instancia según sea necesario.

- Disponibilidad
  - Puede desplegar una instancia en zonas de disponibilidad o regiones para mejorar las capacidades de recuperación ante desastres.
  - Se almacenan tres copias de los datos para garantizar la confiabilidad.
  - TaurusDB utiliza almacenamiento distribuido compartido. Si el nodo primario falla, una de las réplicas de lectura se promueve a primaria con un RPO de cero.
  - La latencia entre el nodo primario y sus réplicas de lectura es de varios milisegundos, lo que garantiza una alta disponibilidad.
- Seguridad
  - Con el almacenamiento distribuido compartido, TaurusDB puede lograr la recuperación del servicio en segundos y casi cero pérdida de datos.
  - Las VPC, los grupos de seguridad, las conexiones SSL y la encriptación de datos se utilizan para controlar estrictamente la seguridad del acceso.
  - TaurusDB ha aprobado más de 15 certificaciones de seguridad, incluidas ISO 27001, CSA, Trusted Cloud y la certificación de nivel 3 de China para la protección de la seguridad de la información. Es el primero de China en obtener la más alta certificación NIST CSF.
- Compatibilidad

  TaurusDB es totalmente compatible con MySQL. Puede migrar fácilmente sus bases de datos MySQL a TaurusDB sin refactorizar las aplicaciones existentes.
- Copia de seguridad
  - Las instantáneas se crean en segundos y se pueden utilizar para restaurar datos rápidamente.
  - El sistema de almacenamiento permite restaurar los datos a cualquier punto en el tiempo sin reproducir logs incrementales.
- Almacenamiento
  - TaurusDB, basado en el almacenamiento distribuido DFV desarrollado por Huawei, soporta hasta 128 TB de almacenamiento.
  - TaurusDB aumenta automáticamente el almacenamiento según sea necesario.
- Pushdown del operador

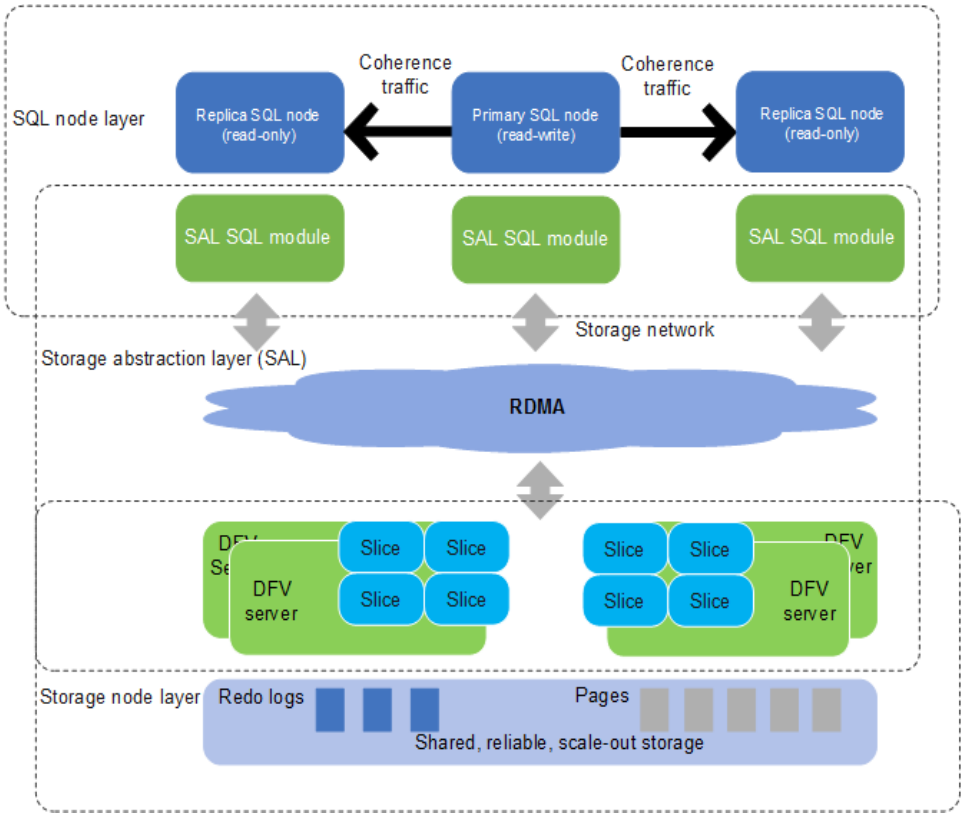
  La proyección de columnas, el filtrado de condiciones y el cálculo de agregación se envían a una capa de almacenamiento distribuido para el procesamiento en paralelo. Esto mejora el rendimiento de las consultas y reduce el tráfico de red y la carga en los nodos de cómputo. El pushdown del operador está integrado con la consulta paralela para ejecutar todo el proceso en paralelo.

2 Arquitectura del producto

La arquitectura de TaurusDB consta de tres capas. De abajo hacia arriba, son:

1. Capa de nodos de almacenamiento: esta capa se basa en el almacenamiento de Data Function Virtualization (DFV) de Huawei, que proporciona almacenamiento distribuido, de alta consistencia y alto rendimiento. Esta capa garantiza la confiabilidad de los datos y la escalabilidad horizontal, con una tasa de confiabilidad no inferior al 99.999999999 % (11 nueves). DFV es un sistema de almacenamiento distribuido de alto rendimiento y alta confiabilidad que se integra verticalmente con las bases de datos. Los clústeres de almacenamiento se despliegan en grupos para mejorar la utilización del almacenamiento y crear una arquitectura de servicio de datos full stack centrada en los datos.
2. Capa de abstracción de almacenamiento: esta capa es clave para garantizar el rendimiento de la base de datos. Se conecta al grupo de almacenamiento DFV debajo de él y proporciona semántica hacia arriba para garantizar una planificación eficiente del almacenamiento. Las operaciones de archivo de tabla se abstraen en almacenamiento distribuido.
3. Capa de análisis de SQL: Esta capa es totalmente compatible con MySQL 8.0 de código abierto, lo que le permite migrar fácilmente sus cargas de trabajo de MySQL a TaurusDB usando la sintaxis y herramientas nativas de MySQL. Esto le ahorra tiempo y esfuerzos. Además de la compatibilidad total con MySQL, TaurusDB viene con un núcleo optimizado y un sistema reforzado.

Figura 2-1 Arquitectura del producto



3 Conceptos básicos

Antes de utilizar TaurusDB debe estar familiarizado con los siguientes conceptos.

Instancia de clúster

TaurusDB utiliza una arquitectura de cómputo y almacenamiento desacoplada que amplia automáticamente hasta 128 TB por instancia de BD. Una instancia de BD de clúster contiene un nodo principal y hasta 15 réplicas de lectura que se pueden crear en minutos.

Instancias de nodo único

Una instancia de nodo único contiene solo un nodo principal y no hay réplicas de lectura. Las instancias de nodo único no implican la sincronización de datos entre nodos y pueden garantizar fácilmente la atómica, la consistencia, el aislamiento y la durabilidad de las transacciones. Las instancias de nodo único no pueden garantizar una alta disponibilidad. Si se produce una falla, los servicios no se pueden recuperar de manera oportuna.

Especificaciones de instancias

Cada instancia se configura con recursos de cómputo y memoria, por ejemplo, 16 vCPU y 64 GB.

Regiones y AZ

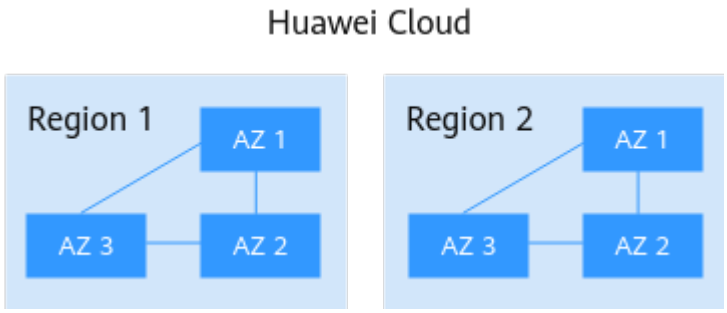
Una región y una zona de disponibilidad (AZ) identifican la ubicación de un centro de datos. Puede crear recursos en una región específica y AZ.

- Las regiones se definen por su ubicación geográfica y latencia de red. Los servicios públicos, como Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP) e Image Management Service (IMS), pueden compartirse en una región determinada. Las regiones pueden ser universales o dedicadas. Una región universal ofrece todo tipo de servicios en la nube para todos los usuarios. Una región dedicada solo proporciona servicios de un tipo determinado o solo para usuarios específicos.
- Una zona de disponibilidad contiene uno o varios centros de datos físicos. Cada zona de disponibilidad tiene sus propias instalaciones independientes de refrigeración, extinción de incendios, a prueba de humedad e instalaciones eléctricas. Dentro de una zona de disponibilidad, los recursos informáticos, la red, el almacenamiento y otros se dividen

lógicamente en múltiples clústeres. Las zonas de disponibilidad dentro de una región están interconectadas mediante fibras ópticas de alta velocidad para que pueda construir sistemas de alta disponibilidad cruzados.

La **Figura 3-1** muestra la relación entre las regiones y las AZ.

Figura 3-1 Regiones y AZ



Huawei Cloud ofrece servicios en muchas regiones de todo el mundo. Puede seleccionar una región y una AZ según sea necesario. Para obtener más información, consulte **Productos y servicios globales**.

Compatibilidad entre TaurusDB y navegadores

Para obtener más información, véase **¿Qué navegadores se admiten?**

4 Ventajas

TaurusDB es una base de datos en la nube de nivel empresarial con computación y almacenamiento desacoplados.

Rendimiento

TaurusDB puede ofrecer siete veces el rendimiento de MySQL de código abierto para ciertas cargas de trabajo y lograr millones de consultas por segundo (QPS).

Escalabilidad

- Escalamiento horizontal: puede agregar hasta 15 réplicas de lectura en cuestión de minutos según sea necesario.
- Escalamiento vertical: puede escalar hacia arriba o hacia abajo las especificaciones de instancia para manejar el crecimiento incierto de la carga de trabajo.
- Escalamiento de almacenamiento: el almacenamiento crece automáticamente a medida que aumenta la cantidad de datos en la base de datos. Una instancia admite hasta 128 TB de almacenamiento.

Disponibilidad

TaurusDB admite la recuperación ante desastres remota y entre AZ para lograr una confiabilidad de nivel financiero.

Hay tres copias de datos para garantizar la confiabilidad.

Compatibilidad

TaurusDB es totalmente compatible con MySQL, por lo que no hay necesidad de refactorizar las aplicaciones.

Costo

Solo el 10% de las bases de datos comerciales

Arquitectura sin middleware

Cuando el rendimiento del servicio es normal, no se requiere Distributed Database Middleware (DDM).

5 Descripción de la instancia

5.1 Motores y versiones de BD

Tabla 5-1 enumera los motores de base de datos y las versiones compatibles con TaurusDB.

Tabla 5-1 Motores y versiones de BD

Motor de base de datos	Version	Versión de kernel menor
TaurusDB	MySQL 8.0	• 2.0.57.240900 • 2.0.54.240600 • 2.0.51.240300 • 2.0.48.231200 • 2.0.45.230900 • 2.0.42.230600 • 2.0.39.230300 • 2.0.28.18 • 2.0.28.17 • 2.0.28.16 • 2.0.28.15 • 2.0.28.12 • 2.0.28.10 • 2.0.28.9 • 2.0.28.7 • 2.0.28.4 • 2.0.28.1

NOTA

Para obtener detalles sobre las actualizaciones en cada versión menor del kernel, véase **Historial de versiones del kernel TaurusDB**.

5.2 Especificaciones de instancias

La arquitectura de CPU de las instancias de TaurusDB puede ser x86 o Kunpeng.

- Las instancias x86 utilizan procesadores Intel® Xeon® Scalable y un rendimiento informático sólido y estable de característica. Cuando se trabaja en redes de alto rendimiento, las instancias proporcionan el rendimiento y la estabilidad adicionales que exigen las aplicaciones de clase empresarial.
- Las instancias de Kunpeng utilizan procesadores de Kunpeng 920 y NIC inteligentes de alta velocidad 25GE para redes informáticas potentes y de alto rendimiento, lo que las convierte en una excelente opción para empresas que necesitan servicios en la nube rentables, seguros y confiables.

Diferentes arquitecturas de CPU soportan diferentes especificaciones de instancia. Dichos cambios se detallan a continuación.

Especificaciones de instancia de x86

Las instancias x86 admiten especificaciones dedicadas y de uso general.

- **Dedicated**: su instancia obtiene vCPU y memoria dedicadas, por lo que el rendimiento es estable. No se ve afectada por otras instancias en la misma máquina física. Las instancias dedicadas son buenas para escenarios que requieren un rendimiento estable.

  Hay instancias dedicadas disponibles en las siguientes regiones: CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Guangzhou-InvitationOnly, CN Southwest-Guiyang1, CN North-Ulanqab1, AP-Singapore, AP-Jakarta, TR-Istanbul y LA-Sao Paulo1.
- **General-purpose**: las vCPU y la memoria se comparten con otras instancias de uso general en la misma máquina física. El uso de la vCPU se maximiza mediante el sobrecompromiso de recursos. Las instancias de propósito general son rentables y adecuadas para escenarios donde el rendimiento estable no es crítico.

  Las instancias de uso general están disponibles en las siguientes regiones: CN North-Beijing4, CN East-Shanghai1 y CN South-Guangzhou.

Tabla 5-2 Especificaciones de instancia de x86

Especificaciones	Código de especificación	vCPUs	Memoria (GB)
Dedicado	gaussdb.mysql.large.x86.4	2	8
	gaussdb.mysql.large.x86.8	2	16
	gaussdb.mysql.xlarge.x86.4	4	16
	gaussdb.mysql.xlarge.x86.8	4	32
	gaussdb.mysql.2xlarge.x86.4	8	32

Especificaciones	Código de especificación	vCPUs	Memoria (GB)
	gaussdb.mysql.2xlarge.x86.8	8	64
	gaussdb.mysql.4xlarge.x86.4	16	64
	gaussdb.mysql.4xlarge.x86.8	16	128
	gaussdb.mysql.8xlarge.x86.4	32	128
	gaussdb.mysql.8xlarge.x86.8	32	256
	gaussdb.mysql.16xlarge.x86.4	60	256
	gaussdb.mysql.16xlarge.x86.8	64	512
Uso general	gaussdb.mysql.large.x86.normal.4	2	8
	gaussdb.mysql.xlarge.x86.normal.2	4	8
	gaussdb.mysql.xlarge.x86.normal.4	4	16
	gaussdb.mysql.2xlarge.x86.normal.2	8	16
	gaussdb.mysql.2xlarge.x86.normal.4	8	32
	gaussdb.mysql.4xlarge.x86.normal.2	16	32
	gaussdb.mysql.4xlarge.x86.normal.4	16	64
	gaussdb.mysql.8xlarge.x86.normal.2	32	64
	gaussdb.mysql.8xlarge.x86.normal.4	32	128

AVISO

- Las especificaciones de instancia de base de datos varían según los requisitos del sitio.
- Para obtener información sobre Transactions Per Second (TPS) y Queries Per Second (QPS), véase **Nota técnica de rendimiento**.

Especificaciones de instancia de Kunpeng

Las instancias de Kunpeng solo admiten especificaciones dedicadas.

Dedicated: Los recursos de CPU y memoria están dedicados para su uso y el rendimiento es estable sin verse afectado por otras instancias en la misma máquina física. Las instancias dedicadas son buenas para escenarios que requieren un rendimiento estable.

Hay instancias dedicadas disponibles en las siguientes regiones: CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Guangzhou-InvitationOnly, CN Southwest-Guiyang1, CN North-Ulanqab1, AP-Singapore, AP-Jakarta, TR-Istanbul y LA-Sao Paulo1.

Tabla 5-3 Especificaciones de instancia de Kunpeng

Especificaciones	Código de especificación	vCPUs	Memory (GB)
Dedicado	gaussdb.mysql.xlarge.arm.4	4	16
	gaussdb.mysql.xlarge.arm.8	4	32
	gaussdb.mysql.2xlarge.arm.4	8	32
	gaussdb.mysql.2xlarge.arm.8	8	64
	gaussdb.mysql.4xlarge.arm.4	16	64
	gaussdb.mysql.4xlarge.arm.8	16	128
	gaussdb.mysql.8xlarge.arm.4	32	128
	gaussdb.mysql.8xlarge.arm.8	32	256
	gaussdb.mysql.12xlarge.arm.4	48	192
	gaussdb.mysql.12xlarge.arm.8	48	384
	gaussdb.mysql.15xlarge.arm.8	60	480

AVISO

- Las especificaciones de instancia de base de datos varían según los requisitos del sitio.
- Para obtener información sobre Transactions Per Second (TPS) y Queries Per Second (QPS), véase **Nota técnica de rendimiento**.

5.3 Tipos de almacenamiento

TaurusDB ofrece dos tipos de almacenamiento: Cloud Database Engine Level 6 (DL6) y Cloud Database Engine Level 5 (DL5).

Esta sección describe las diferencias entre los dos tipos de almacenamiento, ayudándole a elegir el que mejor se adapte a sus necesidades.

Descripción del tipo de almacenamiento

Tabla 5-4 Descripción del tipo de almacenamiento

Tipo de almacenamiento	Descripción	Escenario aplicable
DL6	El almacenamiento compartido es el tipo de almacenamiento predeterminado para las instancias de TaurusDB creadas antes de julio de 2024. Las instancias basadas en DL6 logran cero RPO con un despliegue de 3 AZ y ofrecen mejor rendimiento y mayor throughput máximos.	Sistemas de aplicaciones principales que son sensibles al rendimiento y tienen requerimientos exigentes de E/S de almacenamiento durante las horas pico, como los de finanzas, comercio electrónico, gobierno y juegos
DL5	El nuevo tipo de almacenamiento utiliza hardware y tecnologías de infraestructura de red de Huawei Cloud, lo que garantiza que las instancias basadas en DL5 mantengan la misma alta disponibilidad (cero RPO en el despliegue 3-AZ) que las instancias basadas en DL6. Aunque el rendimiento máximo puede disminuir, el costo por unidad de capacidad se reduce significativamente.	Módulos de aplicaciones o sistemas empresariales sub-core de uso intensivo de la CPU que se centran en costos mínimos

NOTA

Como los dos tipos de almacenamiento dependen de diferentes medios físicos, no puede cambiar el tipo de almacenamiento para una instancia existente. Para cambiar el tipo de almacenamiento, se recomienda comprar una nueva instancia de TaurusDB, seleccionar el tipo de almacenamiento deseado y migrar datos de la instancia original a la nueva instancia usando DRS.

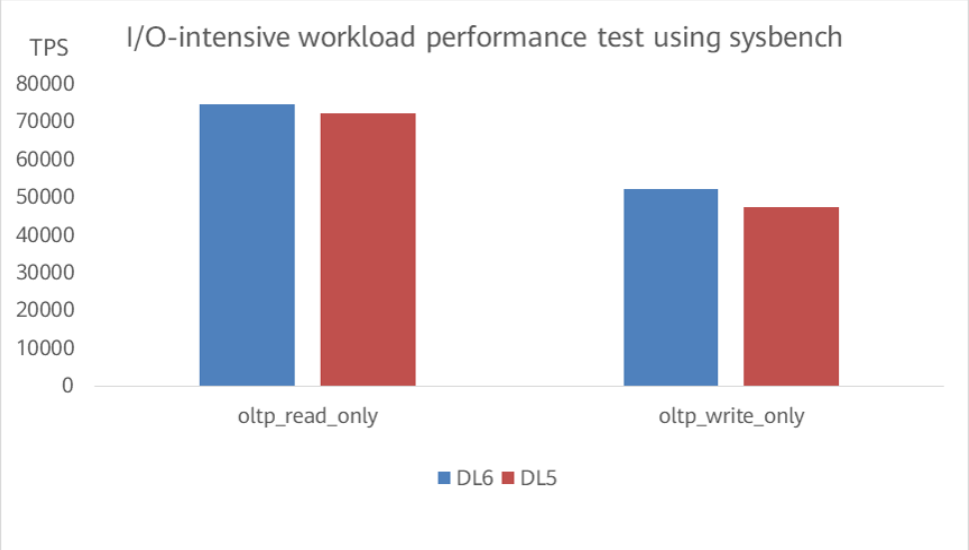
Facturación

Para obtener más información, véase **Calculadora de precios**.

Comparación de rendimiento

Cuando las instancias basadas en DL6 y DL5 con las mismas especificaciones de cómputo y cargas de trabajo intensivas de E/S se compararon con sysbench, solo había una diferencia de aproximadamente un 3 % en el rendimiento de lectura y menos del 10 % en el rendimiento de escritura.

Figura 5-1 Resultados de la comparación de rendimiento



5.4 Estados de instancia

El estado de una instancia de base de datos indica el estado de la instancia de base de datos. Puede ver el estado de una instancia de BD en la consola de gestión.

Tabla 5-5 Estado de instancia de base de datos

Estado	Descripción
Disponible	Una instancia de base de datos está disponible.
Anormal	Una instancia de base de datos es anormal.
Creando	Se está creando una instancia de base de datos.
Error al crear	Error al crear una instancia de BD.
Reiniciando	Se está reiniciando una instancia de base de datos.
Cambiando el nombre de una instancia de BD	Se está cambiando el nombre de una instancia de BD.

Estado	Descripción
Cambiando puerto	Se está cambiando el puerto de una instancia de BD.
Cambiando las especificaciones de instancia	Se está cambiando la CPU o la memoria de una instancia de base de datos.
Agregando réplicas de lectura	Se están agregando réplicas de lectura a una instancia de BD.
Eliminando una réplica de lectura	Se está eliminando una réplica de lectura de una instancia de BD.
Convirtiendo en principal	Se está promoviendo una réplica de lectura a primaria.
Aislando	Se está aislando una réplica de lectura.
Aislada	Se ha aislado una réplica de lectura.
Creando	Se está creando una copia de respaldo.
Ampliando verticalmente	Se está ampliando el espacio de almacenamiento de una instancia de BD.
Congelado	Una instancia de base de datos se congela cuando el saldo de su cuenta es menor o igual a $0 USD. Las instancias de base de datos congeladas retenidas se descongelan solo después de que se haya recargado su cuenta y se hayan liquidado los pagos atrasados.
Cambiando la configuración del certificado	Se está cambiando la configuración del certificado de una instancia de BD.
Cambio de recursos informáticos sin servidor	Se están cambiando los recursos informáticos de una instancia de BD sin servidor.
Actualizando la versión secundaria	Se está actualizando la versión del kernel de una instancia de BD.
Eliminado	Se ha eliminado una instancia de base de datos y no se mostrará en la lista de instancias.

6 Seguridad

6.1 Responsabilidades compartidas

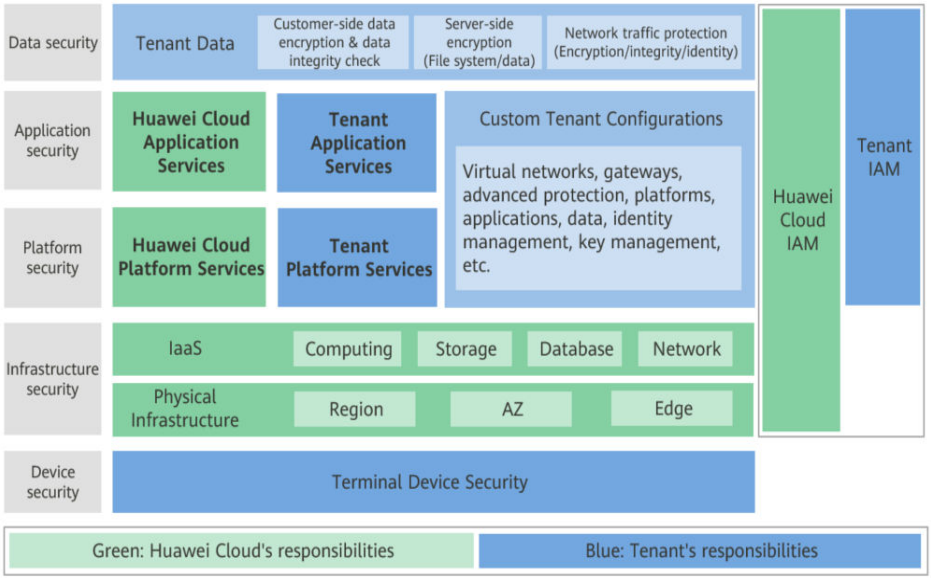
Huawei garantiza que su compromiso con la seguridad cibernética nunca se verá compensado por la consideración de intereses comerciales. Para hacer frente a los desafíos emergentes de seguridad en la nube y a las amenazas y ataques generalizados a la seguridad en la nube, Huawei Cloud construye un sistema integral de garantía de seguridad de servicios en la nube para diferentes regiones e industrias basado en las ventajas únicas de software y hardware de Huawei, las leyes, las regulaciones, los estándares de la industria y el ecosistema de seguridad.

El modelo de responsabilidad compartida para Huawei Cloud y los tenants que usan los servicios de Huawei Cloud se ilustra en **Figura 6-1**. Las responsabilidades son las siguientes:

- **Huawei Cloud**: Garantizar la seguridad de los servicios en la nube y proporcionar nubes seguras. Las responsabilidades de seguridad de Huawei Cloud incluyen garantizar la seguridad de nuestros servicios de IaaS, PaaS y SaaS, así como los entornos físicos de los centros de datos de Huawei Cloud, donde nuestros servicios de IaaS, PaaS, y SaaS operan. Huawei Cloud es responsable no solo de las funciones de seguridad y el rendimiento de nuestra infraestructura, servicios en la nube y tecnologías, sino también de la seguridad general de O&M en la nube y, en un sentido más amplio, de la seguridad y el cumplimiento de nuestra infraestructura y servicios.
- **Tenant**: utilice la nube de forma segura. Los tenants de Huawei Cloud son responsables de la gestión segura y efectiva de las configuraciones personalizadas por el inquilino de los servicios en la nube, incluidos IaaS, PaaS y SaaS. Esto incluye, entre otros, redes virtuales, los sistemas operativos de los hosts e invitados de máquinas virtuales, firewalls virtuales, API Gateway, servicios de seguridad avanzados, todo tipo de servicios en la nube, datos del tenant, cuentas de identidad, y gestión de claves.

Libro blanco de seguridad de Huawei Cloud explica las ideas y las medidas utilizadas para garantizar la seguridad en la nube de Huawei, incluidas las estrategias de seguridad en la nube, el modelo de responsabilidad compartida, el cumplimiento y la privacidad, las organizaciones y el personal de seguridad, la seguridad de la infraestructura, servicio y seguridad del tenant, seguridad de ingeniería, seguridad de operación y seguridad del ecosistema.

Figura 6-1 Modelo de responsabilidad de seguridad compartida de Huawei Cloud



6.2 Autenticación de identidad y control de acceso

Autenticación de identidades

Al acceder a TaurusDB, el sistema autentica su identidad mediante la contraseña o la autenticación de IAM.

- **Autenticación de contraseñas**

  Para gestionar su instancia, debe utilizar Data Admin Service (DAS) para iniciar sesión en su instancia. El inicio de sesión se realiza correctamente solo después de verificar la cuenta y la contraseña.

- **Autenticación de IAM**

  Puede utilizar **Identity and Access Management (IAM)** para proporcionar un control detallado de los permisos de TaurusDB. IAM proporciona autenticación de identidad, gestión de permisos y control de acceso, lo que le ayuda a proteger el acceso a sus recursos de Huawei Cloud. Los usuarios de IAM pueden usar recursos de TaurusDB solo después de verificar sus cuentas y contraseñas. Para obtener más información, véase **Creación de un usuario de IAM e inicio de sesión**.

Control de acceso

- **Control de permisos**

  Si necesita asignar diferentes permisos a diferentes empleados de su empresa para acceder a sus recursos de instancia, IAM es una buena opción. Para más detalles, véase **Permisos**.

- **VPC y subred**

  Una VPC es una red virtual lógicamente aislada, configurable y manejable. Ayuda a mejorar la seguridad de los recursos en la nube y simplifica el despliegue de la red. Puede definir grupos de seguridad, redes privadas virtuales (VPN), segmentos de direcciones IP y ancho de banda para una VPC. Esto facilita la configuración y gestión de la red interna y le permite cambiar su red de una manera segura y conveniente.

Una subred proporciona recursos de red dedicados que están lógicamente aislados de otras redes por motivos de seguridad.

Para obtener más información, véase **Creación de una VPC**.

- **Grupo de seguridad**

  Un grupo de seguridad es un grupo lógico que proporciona políticas de control de acceso para ECS e instancias de TaurusDB que tienen los mismos requisitos de seguridad y son de confianza mutua en una VPC. Para garantizar la seguridad y confiabilidad de la base de datos, debe configurar reglas de grupo de seguridad para permitir que solo determinadas direcciones IP y puertos accedan a instancias de TaurusDB.

6.3 Protección de datos

TaurusDB ofrece una serie de métodos y funciones para la seguridad y confiabilidad de los datos.

Tabla 6-1 Métodos para la seguridad de los datos

Método	Descripción
Encriptación de transmisión (HTTPS)	HTTP y HTTPS son compatibles, pero HTTPS se recomienda para mejorar la seguridad.
Respaldo de datos	Puede realizar copias de respaldo y restaurar bases de datos para garantizar la confiabilidad de los datos.
Protección de operaciones críticas	Con esta función habilitada, el sistema autentica la identidad de un usuario cuando realiza operaciones riesgosas como eliminar una instancia. Esto mejora la protección de sus datos y configuración.
SSL	Puede utilizar SSL para cifrar la conexión entre TaurusDB y el cliente. Proporciona privacidad, autenticación e integridad a las comunicaciones por Internet.

6.4 Auditoría y registros

Auditoría

- Cloud Trace Service (CTS)

  CTS registra operaciones en los recursos en la nube de su cuenta. Puede utilizar los registros generados por CTS para llevar a cabo análisis de seguridad, realizar un seguimiento de los cambios en los recursos, auditar el cumplimiento y localizar fallas.

  Para obtener más información acerca de cómo habilitar y configurar CTS, consulte **Habilitación de CTS**.

  Con CTS, puede registrar operaciones asociadas con TaurusDB para futuras consultas, auditorías y seguimientos.

- Database Security Service (DBSS)

  DBSS se basa en tecnologías de aprendizaje automático y análisis de big data. Proporciona funciones como auditoría de bases de datos, detección de ataques de

inyección SQL e identificación de operaciones riesgosas para garantizar la seguridad de las bases de datos en la nube.

Se recomienda utilizar DBSS para proporcionar capacidades de seguridad de datos ampliadas. Para obtener más información, vea **Servicio de seguridad de base de datos**.

Ventajas:

- DBSS puede ayudarle a cumplir con los requisitos de cumplimiento de seguridad.
  - DBSS puede ayudarle a cumplir con los estándares DJCP (protección gradual) para la auditoría de bases de datos.
  - DBSS puede ayudarle a cumplir con las leyes y regulaciones de seguridad y proporcionar informes de cumplimiento que cumplan con los estándares de seguridad de datos (como Sarbanes-Oxley).
- DBSS puede realizar copias de seguridad y restaurar registros de auditoría de bases de datos y cumplir con los requisitos de retención de datos de auditoría.
- DBSS puede monitorear riesgos, sesiones, distribución de sesiones y distribución SQL en tiempo real.
- DBSS puede reportar alarmas por comportamientos riesgosos y ataques y responder a ataques de bases de datos en tiempo real.
- DBSS puede localizar violaciones internas y operaciones incorrectas y mantener los activos de datos seguros.

Implementada en un patrón de derivación, la auditoría de base de datos puede realizar auditorías flexibles en la base de datos sin afectar a los servicios de usuario.

- La auditoría de la base de datos supervisa los inicios de sesión de la base de datos, los tipos de operación (definición de datos, operación y control) y los objetos de operación basados en operaciones de riesgo para auditar la base de datos de manera efectiva.
- La auditoría de la base de datos analiza los riesgos y las sesiones, y detecta los intentos de inyección de SQL para que pueda estar informado del estado de su base de datos.
- La auditoría de bases de datos proporciona una biblioteca de plantillas de informes para generar informes de auditoría diarios, semanales o mensuales según sus configuraciones. Envía notificaciones de alarma en tiempo real para ayudarle a obtener informes de auditoría de manera oportuna.

Registros

TaurusDB ofrece una variedad de tipos de registros y funciones para el análisis o la auditoría de bases de datos. Puede ver los registros en la consola de gestión.

- Registros de errores

  TaurusDB le permite ver los registros a nivel de base de datos, incluidos los registros de errores y los registros de consultas SQL lentas.
- Registros de consultas lentas

  Los registros de consultas lentas registran sentencias que superan **long_query_time** (de 10 segundos de forma predeterminada). Puede ver los detalles del registro y las estadísticas para identificar sentencias lentas, de modo que pueda optimizarlas.
- Explorador SQL

  La habilitación de SQL Explorer permitirá a TaurusDB almacenar todos los registros de sentencias SQL para su análisis.

SQL Explorer de SQL está deshabilitado de forma predeterminada.

Si SQL Explorer está habilitado, puede usar DAS para ver la duración promedio de la ejecución, la duración total de la ejecución, el tiempo promedio de espera de bloqueo, las filas promedio analizadas y similares.

6.5 Monitoreo de riesgos

Cloud Eye es una plataforma de monitoreo integral para recursos como bases de datos en la nube y servidores en la nube. Le permite supervisar recursos, configurar reglas de alarma, identificar excepciones de recursos y responder rápidamente a los cambios de recursos.

Métricas

Puede supervisar recursos y operaciones, como el uso de la CPU y el rendimiento de la red con Cloud Eye.

El intervalo de monitorización puede ser de 1 minuto, 1 segundo, o 5 segundos. El intervalo de monitoreo predeterminado es 1 minuto. Para mejorar la precisión de las métricas de monitoreo, puede habilitar Monitoreo por Segundos.

Monitoreo de evento

El monitoreo de eventos ofrece funciones de consulta y de alarmas relacionadas con datos de eventos. Puede crear reglas de alarma tanto para eventos del sistema como para eventos personalizados. Cuando ocurren eventos específicos, Cloud Eye genera alarmas.

6.6 Rectificación de fallas

Las copias de respaldo automatizadas se crean durante la ventana de copia de respaldo de las instancias de base de datos. TaurusDB guarda las copia de respaldo automatizadas según el período de retención (de 1 a 732 días) especificado.

Copias de respaldo entre regiones

TaurusDB puede almacenar copias de respaldo en una región diferente de la instancia de base de datos para la recuperación ante desastres. Si una instancia de BD en una región es defectuosa, puede utilizar las copias de respaldo en otra región para restaurar los datos en una nueva instancia de BD.

Después de habilitar la copia de respaldo entre regiones, las copias de respaldo se almacenan automáticamente en la región que especifique.

Despliegue de múltiples AZ

Una AZ es una región física donde los recursos tienen su propia fuente de alimentación y redes independientes. Las zonas de disponibilidad están físicamente aisladas pero interconectadas a través de una red interna. TaurusDB soporta despliegue de múltiples AZ para DR entre AZ.

Conmutación automática por fallas

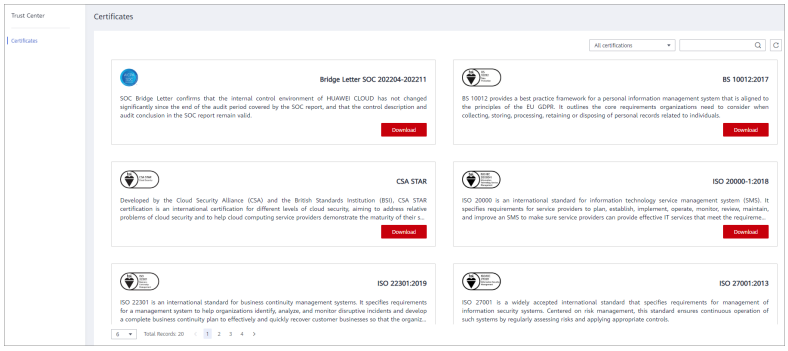
Una instancia de TaurusDB contiene un nodo principal y varias réplicas de lectura. Si el nodo primario deja de estar disponible, TaurusDB conmuta automáticamente por error a una réplica de lectura.

6.7 Certificados

Certificado de cumplimiento

Los servicios y plataformas de Huawei Cloud han obtenido diversas certificaciones de seguridad y cumplimiento de organizaciones autorizadas, como los estándares de cumplimiento de la Organización Internacional de Normalización (ISO), Controles de Sistemas y Organizaciones (SOC) y de la Industria de Tarjetas de Pago (PCI). Puede **descargarlos**.

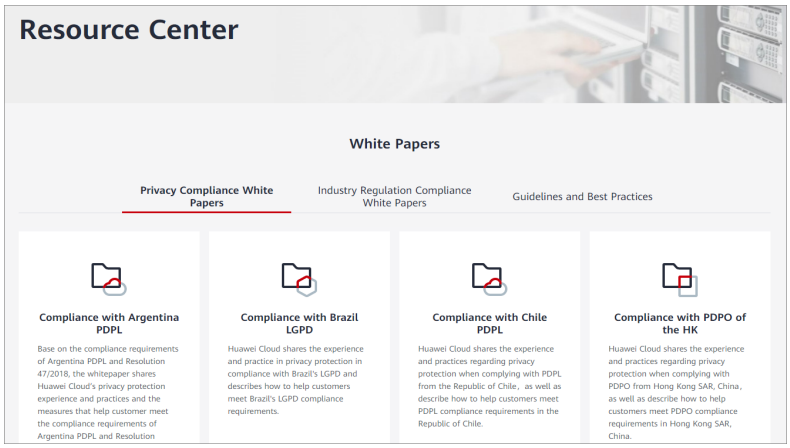
Figura 6-2 Descarga de certificados de cumplimiento



Centro de recursos

Huawei Cloud también proporciona los siguientes recursos para ayudar a los usuarios a cumplir con los requisitos de cumplimiento. Para obtener más información, consulte **Centro de recursos**.

Figura 6-3 Centro de recursos



7 Permisos

Si necesita asignar diferentes permisos al personal de su empresa para acceder a los recursos de TaurusDB, Identity and Access Management (IAM) es una buena opción para la gestión de permisos detallada. IAM proporciona autenticación de identidad, gestión de permisos y control de acceso, lo que le ayuda a proteger el acceso a sus recursos de Huawei Cloud.

Con IAM, puede crear usuarios de IAM y asignar permisos para controlar su acceso a recursos específicos. Por ejemplo, si desea que algunos desarrolladores de software de su empresa usen recursos de TaurusDB pero no desea que eliminen recursos de TaurusDB ni realicen ninguna otra operación de alto riesgo, puede crear usuarios de IAM para los desarrolladores de software y concederles solo los permisos necesarios para usar recursos de TaurusDB.

Si su cuenta de Huawei Cloud no requiere usuarios individuales de IAM para la gestión de permisos, puede omitir esta sección.

IAM es gratuito. Usted paga solo por los recursos de su cuenta. Para obtener más información acerca de IAM, consulte **Descripción del servicio IAM**.

Permisos de TaurusDB

Los nuevos usuarios de IAM no tienen ningún permiso asignado de forma predeterminada. Primero debe agregarlos a uno o más grupos y adjuntar políticas o roles a estos grupos. A continuación, los usuarios heredan los permisos de los grupos y pueden realizar operaciones específicas en servicios en la nube en función de los permisos que se les han asignado.

TaurusDB es un servicio a nivel de proyecto implementado en regiones físicas específicas. Si establece **Scope** en **Region-specific projects** y selecciona los proyectos especificados en las regiones especificadas, los usuarios solo tendrán permisos para instancias de TaurusDB en los proyectos seleccionados. Si establece **Scope** en **All projects**, los usuarios tendrán permisos para instancias de TaurusDB en todos los proyectos específicos de la región. Al acceder a instancias de TaurusDB, los usuarios deben cambiar a la región autorizada.

Puede conceder permisos mediante roles y políticas.

- Roles: Una estrategia de autorización de grano grueso proporcionada por IAM para asignar permisos en función de las responsabilidades del trabajo de los usuarios. Solo un número limitado de roles de nivel de servicio están disponibles para autorización. Los servicios en la nube dependen unos de otros. Cuando concede permisos mediante roles, también debe adjuntar las dependencias de roles existentes. Los roles no son ideales para una autorización detallada y un acceso mínimo de permisos.

- Políticas: Una estrategia de autorización detallada que define los permisos necesarios para realizar operaciones en recursos específicos en la nube bajo ciertas condiciones. Este tipo de autorización es más flexible y es ideal para el acceso con menos permisos. Por ejemplo, solo puede conceder a los usuarios permiso para gestionar recursos de base de datos de un tipo determinado. La mayoría de las políticas detalladas contienen permisos para API específicas, y los permisos se definen mediante acciones de API. Para ver las acciones de API admitidas por TaurusDB, consulte **Permisos y acciones admitidas**.

Tabla 7-1 enumera todos los permisos de TaurusDB definidos por el sistema.

Tabla 7-1 Permisos definidos por el sistema para TaurusDB

Nombre de rol/ política	Descripción	Tipo
GaussDB FullAccess	Permisos completos para TaurusDB	Política definida por el sistema
GaussDB ReadOnlyAccess	Permisos de solo lectura para TaurusDB	Política definida por el sistema

Tabla 7-2 enumera las operaciones comunes admitidas por cada permiso de TaurusDB definido por el sistema.

Tabla 7-2 Operaciones comunes admitidas por permisos definidos por el sistema

Operación	GaussDB FullAccess	GaussDB ReadOnlyAccess
Creación de una instancia de TaurusDB	Se admite	No se admite
Eliminación de una instancia de TaurusDB	Se admite	No se admite
Consulta de instancias de TaurusDB	Se admite	Se admite

Tabla 7-3 Operaciones comunes y acciones apoyadas

Operación	Acción	Descripción
Modificación de parámetros en una plantilla de parámetros	gaussdb:param:modify	-
Cambio de las especificaciones de instancia de base de datos	gaussdb:instance:modifySpec	-

Operación	Acción	Descripción
Creación de una instancia de BD	gaussdb:instance:create	Para seleccionar una VPC, una subred y un grupo de seguridad, configure las siguientes acciones: vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get Para crear una instancia cifrada, configure el permiso de administrador de KMS para el proyecto. Para crear instancias anuales/mensuales, configure las siguientes acciones de CBC: bss:renewal:view bss:renewal:update bss:balance:view bss:order:view bss:order:update bss:order:pay Para configurar TDE durante la creación de instancias, configure la siguiente acción: iam:agencies:createServiceLinkedAgencyV5
Creación de una copia de respaldo manual	gaussdb:backup:create	-
Consulta de copias de respaldo	gaussdb:backup:list	-
Consulta de logs de errores	gaussdb:log:list	-
Reinicio de una instancia de base de datos	gaussdb:instance:restart	-
Consulta de instancias de base de datos	gaussdb:instance:list	-
Creación de una plantilla de parámetros	gaussdb:param:create	-
Eliminación de una plantilla de parámetros	gaussdb:param:delete	-

Operación	Acción	Descripción
Modificación de una política de copia de respaldo	gaussdb:instance:modifyBackupPolicy	-
Consulta de plantillas de parámetros.	gaussdb:param:list	-
Eliminación de una instancia de base de datos	gaussdb:instance:delete	Para cancelar la suscripción de una instancia anual/mensual, configure la siguiente acción: bss:unsubscribe:update
Eliminación de una copia de respaldo manual	gaussdb:backup:delete	-
Consulta de etiquetas de proyecto	gaussdb:tag:list	-
Aplicación de una plantilla de parámetros	gaussdb:param:apply	-
Agregar o eliminar etiquetas de proyecto por lotes	gaussdb:instance:dealTag	-
Cambio de cuotas	gaussdb:quota:modify	-
Actualización de una versión de instancia de base de datos	gaussdb:instance:upgrade	-
Promoción de una réplica de lectura en el nodo principal	gaussdb:instance:switchover	-
Cambio de puerto de base de datos	gaussdb:instance:modifyPort	-
Cambio de un grupo de seguridad	gaussdb:instance:modifySecurityGroup	-
Cambio de la dirección IP privada	gaussdb:instance:modifyIp	Para seleccionar una dirección IP, configure las siguientes acciones: vpc:vpcs:list vpc:vpcs:get
Habilitación o deshabilitación de SSL	gaussdb:instance:modifySSL	-
Cambio del nombre de una instancia	gaussdb:instance:rename	-
Adición de réplicas de lectura	gaussdb:instance:addNodes	-

Operación	Acción	Descripción
Eliminación de réplicas de lectura	gaussdb:instance:deleteNodes	-
Escalamiento del espacio de almacenamiento	gaussdb:instance:modifyStorageSize	-
Cambio de la contraseña de una instancia de base de datos	gaussdb:instance:modifyPassword	-
Vinculación de una EIP a una instancia de base de datos	gaussdb:instance:bindPublicIp	Para mostrar las EIP en la consola, configure: vpc:publicIps:get vpc:publicIps:list
Desvinculación de una EIP de una instancia de base de datos	gaussdb:instance:unbindPublicIp	-
Modificación de una política de supervisión	gaussdb:instance:modifyMonitorPolicy	-
Cambio de una prioridad de conmutación por error	gaussdb:instance:modifySwitchoverPriority	-
Cambio de la ventana de mantenimiento	gaussdb:instance:modifyMaintenanceWindow	-
Aislamiento de nodos	gaussdb:instance:isolateNodes	-
Habilitación o deshabilitación del Explorador de SQL	gaussdb:instance:modifyTraceSQLPolicy	-
Consulta de instancias HTAP	gaussdb:htapInstance:list	-
Creación de una instancia HTAP	gaussdb:htapInstance:create	-
Modificación de una instancia HTAP de GaussDB.	gaussdb:htapInstance:modify	-
Eliminación de una instancia de HTAP	gaussdb:htapInstance:delete	-
Cambio de un nombre de instancia HTAP	gaussdb:htapInstance:rename	-
Reinicio de una instancia HTAP	gaussdb:htapInstance:restart	-

Operación	Acción	Descripción
Actualización de una versión de instancia HTAP	gaussdb:htapInstance:upgrade	-
Promoción de una réplica de lectura de una instancia HTAP a primaria	gaussdb:htapInstance:switchover	-
Cambio de las especificaciones de una instancia HTAP	gaussdb:htapInstance:modifySpec	-
Ampliación del almacenamiento de una instancia HTAP	gaussdb:htapInstance:modifyStorageSize	-
Vinculación de una EIP para una instancia de HTAP	gaussdb:htapInstance:bindPublicIp	-
Desvinculación de una EIP de una instancia de HTAP	gaussdb:htapInstance:unbindPublicIp	-
Cambio del puerto de una instancia de HTAP	gaussdb:htapInstance:modifyPort	-
Cambio de la contraseña de instancia de HTAP	gaussdb:htapInstance:modifyPassword	-
Creación de una Tarea de Sincronización de Datos HTAP	gaussdb:htapInstance:createDataSync	-
Modificación de una tarea de sincronización de datos de HTAP	gaussdb:htapInstance:modifyDataSync	-
Eliminación de una tarea de sincronización de datos HTAP	gaussdb:htapInstance:deleteDataSync	-
Creación de una instancia proxy de base de datos	gaussdb:proxy:create	-
Cambio de la dirección IP de una instancia de proxy	gaussdb:proxy:modifyIp	-
Modificación de los pesos de lectura de una instancia proxy	gaussdb:proxy:modifyWeight	-
Cambio del puerto proxy de la base de datos	gaussdb:proxy:modifyPort	-
Modificación del control de acceso de proxy de base de datos	gaussdb:proxy:modifyAccess	-

Operación	Acción	Descripción
Eliminación de una instancia de proxy	gaussdb:proxy:delete	-
Consulta de instancias de proxy	gaussdb:proxy:list	-
Actualización de una versión de instancia de proxy	gaussdb:proxy:upgrade	-
Cambio del nombre de una instancia de proxy	gaussdb:proxy:rename	-
Adición de nodos de proxy de base de datos	gaussdb:proxy:addNodes	-
Eliminación de nodos proxy de base de datos	gaussdb:proxy:deleteNodes	-
Cambio de las especificaciones de una instancia de proxy	gaussdb:proxy:modifySpec	-
Solicitud de un nombre de dominio privado para una instancia proxy de base de datos	gaussdb:proxy:createDns	-
Cambio del nombre de dominio de la instancia de proxy	gaussdb:proxy:modifyDns	-
Eliminar el nombre de dominio de una instancia de proxy	gaussdb:proxy:deleteDns	-
Cambio de la política de enrutamiento de una instancia de proxy	gaussdb:proxy:modifyRouteMode	-
Habilitación o deshabilitación de SSL para una instancia de proxy	gaussdb:proxy:modifySSL	-
Creación de usuarios de base de datos	gaussdb:user:create	-
Eliminación de usuarios de base de datos	gaussdb:user:delete	-
Cambio de la contraseña de un usuario de base de datos	gaussdb:user:modify	-
Consulta de usuarios de base de datos	gaussdb:user:list	-

Operación	Acción	Descripción
Autorización de permisos de base de datos a los usuarios	gaussdb:user:grantPrivilege	-
Revocación de los permisos de base de datos de los usuarios	gaussdb:user:revokePrivilege	-
Creación de bases de datos	gaussdb:database:create	-
Eliminación de bases de datos	gaussdb:database:delete	-
Consulta de bases de datos	gaussdb:database:list	-
Consulta de etiquetas predefinidas	-	Para consultar etiquetas predefinidas, configure la siguiente acción: tms:resourceTags:list
Consulta de grupos de logs configurados	-	Para consultar grupos de logs configurados, configure la siguiente acción: lts:groups:get
Consulta de flujos de log configurados	-	Para consultar los flujos de log configurados, configure la siguiente acción: lts:topics:get
Modificación de políticas de escalado automático	gaussdb:autoscaling:createPolicy	Para modificar las políticas de escalado automático, configure la siguiente acción: iam:agencies:listAgencies

8 Restricciones

Para mejorar la estabilidad y la seguridad de las instancias, TaurusDB tiene determinadas restricciones.

Especificaciones y rendimiento

Tabla 8-1 Limitaciones de especificación y de rendimiento

Tipo de recurso	Restricción	Notas
Espacio de almacenamiento	● Instancia de pago por uso: un máximo de 128,000 GB ● Instancia anual/mensual: de 40 GB a 128,000 GB ● Instancia sin servidor: un máximo de 128,000 GB ● Instancia HTAP estándar: 50 GB a 32,000 GB para nodos backend; 50 GB a 1,000 GB para nodos frontend	-
Temporary disk space	500 GB como máximo	Para obtener más información, consulte **¿Cómo puedo usar el disco temporal de TaurusDB?**
Conexiones	TaurusDB no tiene restricciones en el número de conexiones. Depende de los valores predeterminados y los rangos de valores de ciertos parámetros en su motor de BD.	Para obtener más información, consulte **¿Cuál es el número máximo de conexiones a una instancia de TaurusDB?**

Cuotas

Tabla 8-2 Restricciones de la cuota

Cuota	Restricción	Notas
Instancias de TaurusDB	50 instancias como máximo	Para obtener detalles sobre cómo aumentar la cuota, consulte **Aumento de cuotas**.
Réplicas de lectura	● Una sola instancia anual/mensual: de 0 a 15 réplicas de lectura ● Una sola instancia de pago por uso: de 0 a 15 réplicas de lectura ● Una sola instancia sin servidor: de 0 a 7 réplicas de lectura	Para obtener más información, consulte **Introducción a réplicas de lectura**.
Etiquetas	Un máximo de 20 etiquetas para cada instancia	Para obtener más información, véase **Gestión de etiquetas**.
Espacio gratuito para copias de respaldo	Alrededor del 100 % del espacio de almacenamiento comprado	Para obtener más información, véase **¿Cómo se facturan los datos de copia de respaldo de TaurusDB?**
Período de retención de copia de respaldo automatizado	● Copia de respaldo de la misma región: de 1 a 732 días (7 días por defecto). Puede ponerse en contacto con el servicio al cliente para ampliar el período de retención a 3,660 días. ● Copia de respaldo entre regiones: de 1 a 1,825 días	Para obtener más información, véase **Configuración de una política de copia de respaldo de la misma región** y **Configuración de una política de copia de respaldo entre regiones**.
Período de conservación de registro	● Registros de errores: 30 días ● Registros de consultas lentas: 30 días ● Registros de consultas lentas en texto sin formato: 30 días	Para obtener más información, véase **Gestión de registros**.

Denominación

Tabla 8-3 Restricciones de denominación

Concepto	Restricción	Notas
Nombre de la instancia	El nombre debe comenzar con una letra y debe contener entre 4 y 64 caracteres. Solo se admiten letras, dígitos, guiones (-) y guiones bajos (_).	Para obtener más información, consulte **Cambio de nombre de instancia de BD**.
Nombre de la base de datos	● El nombre de la base de datos debe contener entre 1 y 64 caracteres. Solo se admiten letras, dígitos, guiones (-) y guiones bajos (_). El número total de guiones (-) no puede exceder de 10. ● Para evitar errores, no se pueden usar palabras clave reservadas.	Para obtener más información, consulte **Creación de una base de datos**.
Nombre de usuario	● El nombre de usuario debe contener entre 1 y 32 caracteres. Solo se permiten letras, dígitos y guiones bajos (_). ● Para evitar errores, no se pueden usar palabras clave reservadas.	Para obtener más información, consulte **Creación de una cuenta**.
Nombre de plantilla de parámetro	El nombre de la plantilla debe constar de 1 a 64 caracteres. Solo se permiten letras (distinguiendo mayúsculas y minúsculas), dígitos, guiones (-), guiones bajos (_), y puntos (.).	Para obtener más información, véase **Creación de una plantilla de parámetros**.
Nombre de copia de respaldo	El nombre debe comenzar con una letra y debe contener entre 4 y 64 caracteres. Solo se admiten letras, dígitos, guiones (-) y guiones bajos (_).	Para obtener más información, consulte **Creación de una copia de respaldo manual**.
Nombre de tabla/ nombre de función/ nombre de procedimiento almacenado/nombre de vista	Para evitar errores, no se pueden usar palabras clave reservadas.	Para obtener más información, consulte **Uso de tabla de base de datos**.

Seguridad

Tabla 8-4 Restricciones de seguridad

Concepto	Restricción	Notas
Permisos de raíz de base de datos	Solo el usuario **root** está disponible en la página de creación de instancias.	-
Contraseña de la cuenta	● Debe contener entre 8 y 32 caracteres. ● Debe contener al menos tres tipos de los siguientes caracteres: letras mayúsculas, letras minúsculas, dígitos y caracteres especiales (~!@#$%^*-_=+?,()&|.). ● No puede ser el nombre de usuario ni el nombre de usuario en orden inverso. ● Debe cumplir con los valores de los parámetros de **validate_password**. Para verificar los valores de parámetros relacionados con contraseña, haga clic en un nombre de instancia, elija **Parameters** en el panel de navegación y busque **validate_password** en la esquina superior derecha de la página.	Para obtener más información, consulte **Restablecimiento de la contraseña de administrador**.
Puerto	● El valor predeterminado es 3306 y se puede cambiar manualmente. ● El puerto de la base de datos oscila entre 1025 y 65534, excepto 5342, 5343, 5344, 5345, 12017, 20000, 20201, 20202, 33060, 33062 y 33071, que están reservados para el uso del sistema.	Para obtener más información, consulte **Cambio de un puerto de base de datos**.
VPC	Después de crear una instancia de TaurusDB, la VPC no se puede cambiar.	-

Concepto	Restricción	Notas
Grupo de seguridad	● De forma predeterminada, puede crear un máximo de 100 grupos de seguridad en su cuenta en la nube. ● De forma predeterminada, puede agregar un máximo de 50 reglas a un grupo de seguridad. ● Una instancia de TaurusDB se puede vincular a varios grupos de seguridad y un grupo de seguridad se puede asociar a varias instancias de TaurusDB. ● Al crear una instancia, puede seleccionar varios grupos de seguridad. (Para un mejor rendimiento de la red, se recomienda seleccionar como máximo cinco grupos de seguridad)	-

Concepto	Restricción	Notas
Cuentas del sistema	Para proporcionar servicios de O&M, el sistema crea automáticamente cuentas del sistema cuando crea instancias de TaurusDB. Estas cuentas del sistema no están disponibles para usted. ● **rdsAdmin**: una cuenta de gestión con los permisos más altos, que se utiliza para consultar y modificar información de instancia, rectificar fallas, migrar datos y restaurar datos. ● **rdsRepl**: una cuenta de replicación, que se utiliza para sincronizar datos de nodos primarios con nodos de en espera o réplicas de lectura. ● **rdsBackup**: una cuenta de copia de respaldo, que se utiliza para hacer copias de respaldo de los datos en segundo plano. ● **rdsMetric**: una cuenta de monitoreo de métricas, que es utilizada por el organismo de control para recopilar datos de estado de la base de datos. ● **rdsProxy**: una cuenta de proxy de base de datos, que se utiliza para la autenticación cuando la base de datos está conectada con una dirección de proxy. Esta cuenta se crea automáticamente al crear una instancia de proxy.	-
Parámetros de instancia	La mayoría de los parámetros se pueden modificar con la consola o las API. Para garantizar la seguridad y estabilidad de las instancias, algunos parámetros no se pueden modificar.	Para obtener más información, consulte **Modificación de parámetros de una instancia de BD**.

Operaciones de instancias

Tabla 8-5 Restricciones de función

Concepto	Restricción	Notas
Motor de almacenamiento de MySQL	TaurusDB solo admite el motor de almacenamiento de InnoDB.	-
Acceso a TaurusDB	● Si las instancias de TaurusDB no tienen EIP vinculadas, las instancias deben estar en la misma VPC que los ECS asociados con estas instancias. ● Se deben agregar reglas de grupo de seguridad para permitir que los ECS accedan a las instancias de TaurusDB. De forma predeterminada, un ECS de un grupo de seguridad diferente no puede acceder a una instancia de TaurusDB. Para habilitar el acceso, debe agregar una regla de entrada al grupo de seguridad de una instancia de TaurusDB. Al agregar la regla, establezca el protocolo y el puerto, respectivamente, en TCP y en el puerto de base de datos predeterminado de la instancia. ● Puerto de una instancia de TaurusDB: El puerto predeterminado es **3306**. Puede cambiarlo si desea acceder a una instancia de TaurusDB con otro puerto en una red privada o pública. Para obtener más información, véase **Cambio de un puerto de base de datos**.	-
Migración de datos	DRS o mysqldump se pueden utilizar para migrar datos a TaurusDB.	Para obtener más información, véase **Migración de datos**.
Reinicio de instancia de TaurusDB	Las instancias solo se pueden reiniciar en la consola de TaurusDB.	Para obtener más información, consulte **Reinicio de una instancia de BD**.

Concepto	Restricción	Notas
Copia de respaldos de TaurusDB	Las copias de respaldo de TaurusDB se almacenan en buckets de OBS y no son visibles para usted.	-
Función de Binlog	Binlog no se puede habilitar para réplicas de lectura de TaurusDB.	Para obtener más información, véase **¿Cómo habilito y veo Binlog de mi instancia de TaurusDB?**
Tablas particionadas	TaurusDB es compatible con MySQL Community Server 8.0.22. Para una tabla particionada en listas, hay un máximo de 256 valores en una partición o se informa de un error. (Solución: Redistribuya el contenido de una partición de tabla en varias particiones.)	-
Instancias de pequeña escala	Para las instancias de TaurusDB con 2 vCPU y 8 GB de memoria, hay un máximo de tablas de 300,000 en una sola instancia y un máximo de tablas de 5,000 en una sola base de datos.	-

9 Servicios relacionados

La Tabla 9-1 muestra la relación entre TaurusDB y otros servicios.

Tabla 9-1 Servicios relacionados

Servicio	Descripción
Elastic Cloud Service (ECS)	Permite acceder a TaurusDB con una red interna. A continuación, puede acceder a las aplicaciones más rápido y no necesita pagar por el tráfico de red pública.
Virtual Private Cloud (VPC)	Aísla las redes y controla el acceso a las instancias de TaurusDB.
Object Storage Service (OBS)	Almacena copias de respaldo automatizadas y manuales de sus instancias de TaurusDB.
Cloud Eye	Supervisa los recursos de TaurusDB en tiempo real e informa las alarmas y advertencias con prontitud si las hay.
Cloud Trace Service (CTS)	Registra operaciones en recursos de servicios en la nube para consultas futuras, auditorías y de retroceso.
Data Replication Service (DRS)	Migra sin problemas las bases de datos a la nube.
Enterprise Project Management Service (EPS)	Le permite gestionar recursos en la nube y grupos de usuarios por proyecto empresarial.
Tag Management Service (TMS)	Facilita a los usuarios la implementación, gestión y mantenimiento de etiquetas en los recursos de la nube.
Distributed Database Middleware (DDM)	Conecta a varias instancias de TaurusDB y le permite acceder a bases de datos distribuidas.

10 Diferencias entre TaurusDB y RDS for MySQL

TaurusDB tiene buen rendimiento, escalabilidad y facilidad de uso. Para más detalles, véase **Tabla 10-1**.

Tabla 10-1 Diferencias entre TaurusDB y RDS for MySQL

Concepto	RDS for MySQL	TaurusDB
Arquitectura	Arquitectura tradicional primaria/en espera. Los datos se sincronizan entre las bases de datos primaria y en espera con binlogs.	Arquitectura de computación y almacenamiento desacoplado. Los nodos de cómputo comparten los mismos datos. No es necesario sincronizar los datos con binlogs.
Rendimiento	Cientos de miles de QPS, tres veces el rendimiento del MySQL de código abierto en alta concurrencia.	Millones de QPS, siete veces el rendimiento de MySQL de código abierto para ciertas cargas de trabajo. En consultas complejas, las operaciones, como la extracción de columnas, el filtrado condicional y el cálculo de agregación, pueden ser empujadas a la capa de almacenamiento, mejorando el rendimiento docenas de veces en comparación con las bases de datos tradicionales.

Concepto	RDS for MySQL	TaurusDB
Escalabilidad	● Se pueden agregar hasta cinco réplicas de lectura para cada instancia de BD. El tiempo necesario para agregar réplicas de lectura depende de la cantidad de datos que haya. La adición de réplicas de lectura requiere almacenamiento adicional. ● El almacenamiento crece según sea necesario, hasta 4 TB por instancia de BD.	● Se pueden agregar hasta 15 réplicas de lectura para cada instancia de BD. Gracias al almacenamiento compartido, el tiempo necesario para agregar réplicas de lectura no se ve afectado por la cantidad de datos que haya, y no se necesita almacenamiento adicional para la creación de réplicas de lectura. ● El almacenamiento crece según sea necesario, hasta 128 TB por instancia de BD.
Disponibilidad	Si la instancia principal falla, la instancia en espera se puede promover automáticamente a la principal, con un RTO de menos de 30 segundos.	Si el nodo primario es defectuoso, una réplica de lectura se puede promover automáticamente al primario, con un RTO de menos de 10 segundos. Tiene menos latencia porque no se requiere sincronización de datos con binlogs entre el nodo primario y las réplicas de lectura.
Copia de respaldo y restauración	Los datos se pueden restaurar a un punto específico en el tiempo mediante copias de respaldo completas y reproducción de binlog.	Los datos se pueden restaurar a un punto específico en el tiempo mediante copias de respaldo completas (instantáneas) y la reproducción logs de redo, lo que es más rápido.
Versión del motor de DB	MySQL 5.6, 5.7 y 8.0	MySQL 8.0

