

TaurusDB

Descripción general del servicio

Edición 01
Fecha 2025-02-10



Copyright © Huawei Technologies Co., Ltd. 2025. Todos los derechos reservados.

Quedan terminantemente prohibidas la reproducción y la divulgación del presente documento en todo o en parte, de cualquier forma y por cualquier medio, sin la autorización previa de Huawei Technologies Co., Ltd. otorgada por escrito.

Marcas y permisos



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

Las funciones, los productos y los servicios adquiridos están estipulados en el contrato celebrado entre Huawei y el cliente. Es posible que la totalidad o parte de los productos, las funciones y los servicios descritos en el presente documento no se encuentren dentro del alcance de compra o de uso. A menos que el contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en este documento constituye garantía alguna, ni expresa ni implícita.

La información contenida en este documento se encuentra sujeta a cambios sin previo aviso. En la preparación de este documento se realizaron todos los esfuerzos para garantizar la precisión de sus contenidos. Sin embargo, ninguna declaración, información ni recomendación contenida en el presente constituye garantía alguna, ni expresa ni implícita.

Huawei Technologies Co., Ltd.

Dirección: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Sitio web: <https://www.huawei.com>

Email: support@huawei.com

Índice

1 ¿Qué es TaurusDB?	1
2 Arquitectura del producto	3
3 Conceptos básicos	5
4 Beneficios del producto	6
5 Descripción de la instancia	8
5.1 Especificaciones de instancias.....	8
5.2 Estado de instancia.....	10
5.3 Motores y versiones de DB.....	11
5.4 Descripción de la versión de kernel de base de datos.....	12
6 Seguridad	15
6.1 Responsabilidades compartidas.....	15
6.2 Autenticación de identidad y control de acceso.....	16
6.3 Protección de datos.....	17
6.4 Auditoría y registros.....	17
6.5 Monitoreo de riesgos.....	18
6.6 Rectificación de falla.....	19
6.7 Certificados.....	19
7 Gestión de permisos	21
8 Restricciones	27
9 Facturación	29
10 Servicios relacionados	31
11 Diferencias entre TaurusDB y RDS for MySQL	32

1 ¿Qué es TaurusDB?

TaurusDB es un servicio de base de datos distribuida de nivel empresarial compatible con MySQL. La virtualización de funciones de datos (DFV) se utiliza para desacoplar el almacenamiento de la computación y puede escalar automáticamente hasta 128 TB por instancia. Una conmutación por error se puede realizar en cuestión de segundos. Proporciona el rendimiento superior de una base de datos comercial al precio de una base de datos de código abierto.

TaurusDB actualmente soporta los motores de base de datos y las versiones listados en [Motores y versiones de DB](#).

Uso de TaurusDB

Puede crear y gestionar instancias de TaurusDB en la [consola de gestión](#) basada en web.

Para ayudarle a sacar el máximo provecho de TaurusDB, consulte [Beneficios del producto](#).

Ventajas

- Rendimiento
 - Al desacoplar la computación y el almacenamiento y usar una arquitectura de "log as database", TaurusDB ofrece siete veces el rendimiento de las bases de datos de código abierto.
 - El protocolo RDMA se utiliza para la transmisión de la base de datos para romper el cuello de botella de rendimiento de E/S.
 - TaurusDB soporta características 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 una instancia para satisfacer solicitudes de alta concurrente.
 - Escalado vertical: puede escalar hacia arriba o hacia abajo las vCPU y la memoria de una instancia según sea necesario.
- Confiabilidad
 - Puede desplegar una instancia en zonas de disponibilidad o regiones para mejorar las capacidades de recuperación ante desastres.

- Tres copias de la capa de almacenamiento garantizan la seguridad de los datos.
- TaurusDB utiliza almacenamiento distribuido compartido. Si el nodo primario está defectuoso, una réplica de lectura se promociona automáticamente para que sea primaria con un RPO cero.
- Seguridad
 - Con el almacenamiento distribuido compartido, TaurusDB puede lograr la recuperación del servicio en cuestión de segundos y la pérdida de datos casi cero.
 - 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 pasado más de 15 certificaciones de seguridad, incluyendo 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 reconstruir las aplicaciones existentes.
- Copia de respaldo
 - Las instantáneas se crean en segundos y se pueden utilizar para restaurar datos rápidamente.
 - Basado en la función de punto múltiple del sistema de almacenamiento subyacente, los datos se pueden restaurar a cualquier punto en el tiempo sin reproducir registros incrementales.
- Almacenamiento
 - Con el almacenamiento distribuido DFV, una instancia puede alcanzar hasta 128 TB de almacenamiento sin fragmentos.
 - TaurusDB aumenta automáticamente el almacenamiento según sea necesario.
- Pushdown del operador

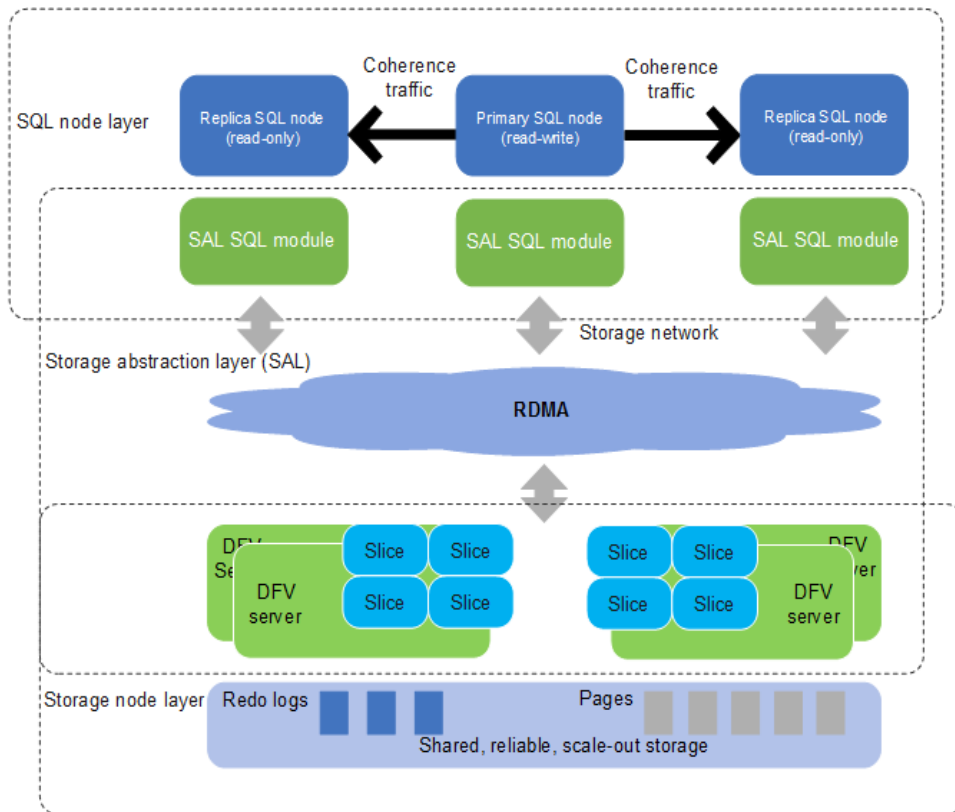
Las operaciones tales como la proyección de columnas, el filtrado de condiciones y el cálculo de agregación se envían a múltiples nodos en una capa de almacenamiento distribuida para su ejecución en paralelo. Esto mejora las capacidades de procesamiento de consultas y reduce la presión de tráfico de red en los nodos informáticos. 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 nodo de almacenamiento. El almacenamiento de virtualización de funciones de datos (DFV) proporciona almacenamiento distribuido, de gran consistencia y de alto rendimiento, con una alta confiabilidad de datos y una excelente escalabilidad horizontal. La confiabilidad de los datos no es inferior al 99.999999999% (11 nueves). DFV es una solución para una arquitectura de servicio de pila completa centrada en datos con almacenamiento y cómputo desacoplados.
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 SQL: 100% compatible con MySQL 8.0 de código abierto. Puede utilizar la sintaxis y las herramientas nativas de MySQL para migrar sus cargas de trabajo de MySQL a TaurusDB, ahorrando tiempo y esfuerzos. Además de la compatibilidad total con MySQL, TaurusDB viene con un núcleo optimizado y un sistema reforzado. Es parte de un ecosistema abierto y proporciona capacidades comerciales de MySQL nativo.

Figura 2-1 Arquitectura del producto



3 Conceptos básicos

Antes de usar TaurusDB, debería estar familiarizado con los siguientes conceptos.

- **Instancias principales/en espera:** TaurusDB tiene una arquitectura con almacenamiento y procesamiento desacoplados que escala automáticamente hasta 128 TB por instancia. Una instancia primaria/en espera puede contener un nodo primario y hasta 15 réplicas de lectura que se pueden crear en minutos.
- **Las regiones se definen mediante una combinación de 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) y Image Management Service (IMS), se comparten dentro de la misma región. 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. Generalmente, las instancias de TaurusDB y los ECS deben estar ubicados en la misma región para un alto rendimiento de acceso.
- **Zona de disponibilidad (AZ):** Una zona de disponibilidad contiene uno o varios centros de datos físicos. Cada AZ cuenta con refrigeración independiente, sistemas de extinción de incendios, protección contra la humedad e instalaciones eléctricas. Dentro de una zona de disponibilidad, la informática, la red, el almacenamiento y otros recursos se dividen lógicamente en instancias. Una zona de disponibilidad es una ubicación geográfica con fuente de alimentación independiente y instalaciones de red en una región.

Las zonas de disponibilidad están físicamente aisladas pero interconectadas a través de una intranet. Cada zona de disponibilidad proporciona conexiones de red rentables y de baja latencia que no se ven afectadas por fallos en otras zonas de disponibilidad. Como resultado, el aprovisionamiento de instancias de TaurusDB en zonas de disponibilidad separadas protege sus aplicaciones contra fallos locales que se producen en una sola ubicación. Las zonas de disponibilidad dentro de la misma región no tienen diferencias funcionales.

- **Especificaciones de instancia:** Cada instancia está configurada con recursos informáticos y de memoria, por ejemplo, 16 vCPUs y 64 GB.
- **Compatibilidad entre TaurusDB y navegadores:** consulte *¿Qué navegadores son compatibles?*

4 Beneficios del producto

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 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 cambiar las vCPU y la memoria de las instancias para procesar un 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.

Confiabilidad

TaurusDB soporta la recuperación ante desastres remota y cross-AZ para una confiabilidad de nivel financiero.

Hay tres copias de datos para garantizar la seguridad de los datos.

Compatibilidad

TaurusDB es totalmente compatible con MySQL, por lo que no hay necesidad de reconstruir 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 Especificaciones de instancias

Actualmente, se soportan especificaciones de propósito general y dedicadas.

- **Dedicated Edition** indica que una instancia contiene un nodo primario y hasta 15 réplicas de lectura. Sus 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. Es adecuado para escenarios que requieren estabilidad de alto rendimiento.
- **General-purpose Edition** indica que una instancia contiene un nodo primario y hasta 15 réplicas de lectura. Los recursos de CPU y memoria se comparten con otras instancias de base de datos de propósito general en la misma máquina física. El uso de la CPU se maximiza a través del exceso de compromiso de recursos. Es rentable y adecuado para escenarios en los que la estabilidad del rendimiento no es crítica.

Las especificaciones de instancia de TaurusDB se enumeran en la siguiente tabla.

 NOTA

Tabla 5-1 Especificaciones de instancia de x86

Especificaciones de instancia	Código de especificación	vCPUs	Memoria (GB)
Dedicated Edition	gaussdb.mysql.xlarge.x86.4	4	16
	gaussdb.mysql.xlarge.x86.8	4	32
	gaussdb.mysql.2xlarge.x86.4	8	32
	gaussdb.mysql.2xlarge.x86.8	8	64

Especificaciones de instancia	Código de especificación	vCPUs	Memoria (GB)
	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
General-purpose Edition NOTA Para utilizar las especificaciones de propósito general, póngase en contacto con el servicio de atención al cliente para solicitar los permisos necesarios.	gaussdb.mysql.large.x86.normal.2	2	4
	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

Tabla 5-2 Especificaciones de instancia de Kunpeng

Especificaciones de instancia	Código de especificación	vCPUs	Memoria (GB)
Dedicated Edition	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

Las especificaciones de instancia de base de datos varían según los requisitos del sitio.

 **NOTA**

Puede usar **max_connections** para configurar el número máximo de conexiones para una instancia. Para obtener más información, consulte Modificación de una plantilla de parámetro.

5.2 Estado de instancia

Estado de instancia

El estado de una instancia refleja el estado de la instancia. Puede ver el estado de la instancia en la consola.

Tabla 5-3 Estado de instancia

Estado	Descripción
Available	La instancia está disponible.
Abnormal	La instancia es anormal.
Creating	Se está creando la instancia.
Creation failed	No se pudo crear la instancia.
Rebooting	La instancia se está reiniciando.
Changing a DB instance name	Se está cambiando el nombre de la instancia.
Changing port	Se está cambiando el puerto de instancia.
Changing instance specifications	Se están cambiando las especificaciones de CPU y memoria de la instancia.
Adding read replicas	Se están agregando réplicas de lectura a la instancia.
Deleting a read replica	La réplica de lectura se está eliminando de la instancia de base de datos.
Promoting to primary	Se está promoviendo una réplica de lectura a primaria.
Isolating	La réplica de lectura está siendo aislada.
Isolated	Se aisló la réplica leída.
Creating	Se está creando la copia de respaldo.
Scaling up	Se está escalando el espacio de almacenamiento de la instancia.
Frozen	La instancia de base de datos se congela cuando el saldo de la cuenta es menor o igual a \$0 USD. Las instancias congeladas se descongelan solo después de que su cuenta se haya recargado y se hayan liquidado los pagos atrasados.
Changing certificate settings	Se está cambiando la configuración del certificado de la instancia.
Upgrading minor version	Se está actualizando la versión del núcleo de la instancia.
Deleted	La instancia se ha eliminado y no se mostrará en la lista de instancias.

5.3 Motores y versiones de DB

Tabla 5-4 enumera los motores de base de datos y las versiones compatibles con TaurusDB.

Tabla 5-4 Motores y versiones de DB

Motor DB	Versión	Minor Kernel Version
TaurusDB	MySQL 8.0	<ul style="list-style-type: none"> ● 2.0.28.12 ● 2.0.28.10 ● 2.0.28.9 ● 2.0.28.7 ● 2.0.28.4 ● 2.0.28.1

5.4 Descripción de la versión de kernel de base de datos

Esta sección describe las actualizaciones de la versión de kernel de TaurusDB.

2.0.28.12

Tabla 5-5 Versión 2.0.28.12

Fecha	Descripción
2022-12-07	Los errores de análisis activados por Skip Scans no se muestran cuando se actualiza una tabla con columnas virtuales.

2.0.28.10

Tabla 5-6 Versión 2.0.28.10

Fecha	Descripción
2022-11-16	Durante una conmutación primaria/en espera, la base de datos no se descompone debido al tiempo de espera de la conexión.

2.0.28.9

Tabla 5-7 Versión 2.0.28.9

Fecha	Descripción
2022-09-23	<ul style="list-style-type: none"> ● Se modifica la sentencia If (...) en Condition_pushdown::replace_columns_in_cond. ● La base de datos no se desglosa cuando: <ul style="list-style-type: none"> – Las funciones de almacenamiento se invocan recursivamente. – Se eliminan varias tablas o se realiza una búsqueda de texto completo. – Se ejecutan sentencias de consulta SQL de múltiples funciones de ventana. ● Los usuarios con permiso global pueden ejecutar SHOW CREATE DATABASE correctamente.

2.0.28.7

Tabla 5-8 Versión 2.0.28.7

Fecha	Descripción
2022-08-29	Se resuelve el problema de bloqueo de ptrc en el procedimiento almacenado.

2.0.28.4

Tabla 5-9 Versión 2.0.28.4

Fecha	Descripción
2022-07-22	<ul style="list-style-type: none"> ● La base de datos no se descompone debido a los usuarios vacíos. ● Cuando se actualiza la tabla temporal utilizada para la agregación, BLOB apunta a los datos más recientes.

2.0.28.1

Tabla 5-10 Versión 2.0.28.1

Fecha	Descripción
2022-05-19	<ul style="list-style-type: none">● Puede activar o desactivar orphaned definer check control.● TaurusDB admite la transmisión transparente de direcciones IP proxy.● Puede establecer el nivel de coherencia de las instancias de proxy en coherencia de sesión.

6 Seguridad

6.1 Responsabilidades compartidas

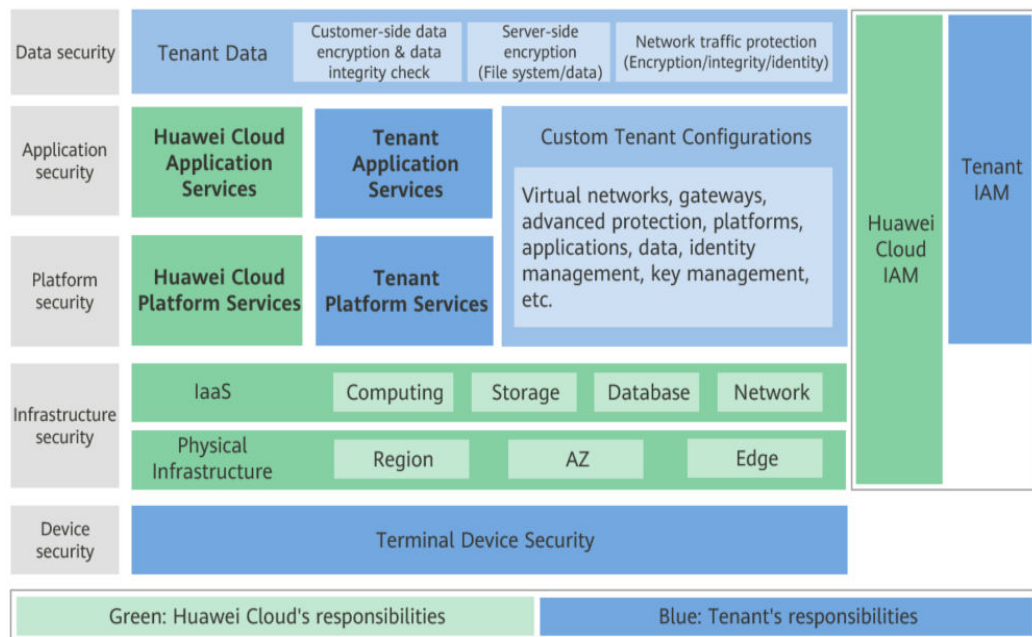
Huawei garantiza que su compromiso con la seguridad cibernética nunca se verá compensado por la consideración de intereses comerciales. Para hacer frente a los desafíos emergentes de seguridad en la nube y a las amenazas y ataques generalizados de seguridad en la nube, Huawei Cloud crea un sistema integral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

Figura 6-1 ilustra las responsabilidades compartidas por Huawei Cloud y los usuarios.

- **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 IaaS, PaaS y SaaS, así como los entornos físicos de los centros de datos de Huawei Cloud donde nuestros IaaS, PaaS, y los servicios 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 la nube y, en el sentido más amplio, del cumplimiento de seguridad de nuestra infraestructura y servicios.
- **Tenant:** Utilizar la nube de forma segura. Los inquilinos 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, el sistema operativo 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 inquilino, cuentas de identidad, y gestión de claves.

Libro blanco de seguridad de Huawei Cloud elabora las ideas y medidas para construir la seguridad en Huawei Cloud, 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, el servicio y la seguridad del inquilino, la seguridad de ingeniería, seguridad de O&M 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 identidad

Cuando accede a TaurusDB, el sistema autentica su identidad mediante contraseña y autenticación de IAM.

- **Verificación de contraseña**

Para gestionar su instancia, debe usar Data Admin Service (DAS) para iniciar sesión en su instancia. El inicio de sesión es exitoso solo después de que su cuenta y contraseña son verificados.

- **Verificación de IAM**

Puede usar **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, consulte [Paso 2: Crear usuarios de IAM e iniciar 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 obtener más información, consulte [Gestión de 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 para mayor seguridad.

Para obtener más información, consulte [Creación de un VPC](#).

- **Grupo de seguridad**

Un grupo de seguridad es un grupo lógico que proporciona políticas de control de acceso para las instancias de ECS y TaurusDB que tienen los mismos requisitos de protección 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 las instancias de acceso a direcciones IP y puertos específicos.

Para obtener más información, consulte Configuración de reglas de grupo de seguridad.

6.3 Protección de datos

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

Tabla 6-1 Métodos para la seguridad de los datos

Método	Descripción
Cifrado de transmisión (HTTPS)	HTTP y HTTPS son compatibles, pero HTTPS se recomienda para mejorar la seguridad.
Copia de 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 del usuario cuando realiza cualquier operación arriesgada, como eliminar un bucket. 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) registra las operaciones en los recursos de la nube de su cuenta. Puede utilizar los registros generados por CTS para realizar análisis de seguridad, realizar un seguimiento de los cambios de 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 grabar operaciones asociadas con TaurusDB para realizar consultas, auditorías y operaciones posteriores. Para obtener más información, consulte Operaciones clave admitidas por CTS.

Registros

TaurusDB ofrece una variedad de tipos de registros y funciones para el análisis o 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 los **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.
- SQL Explorer
Habilitar SQL Explorer permitirá a TaurusDB almacenar todos los registros de sentencias SQL para su análisis.
SQL Explorer de SQL está deshabilitado de forma predeterminada. Para habilitarlo, consulte [Habilitación y deshabilitación de SQL Explorer](#).
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. Para obtener más información, consulte [SQL Explorer](#).

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 de monitoreo

Puede supervisar recursos y operaciones, como el uso de la CPU y el rendimiento de la red con Cloud Eye. Para obtener más información sobre las métricas de monitorización compatibles y cómo crear reglas de alarma, consulte [Introducción de métricas de TaurusDB](#).

El intervalo de monitorización puede ser de 1 minuto, 1 segundo, o 5 segundos. El intervalo de supervisión 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 para usted. Para obtener más información sobre los eventos admitidos y cómo crear reglas de alarma, consulte [Introducción de monitoreo de evento](#).

6.6 Rectificación de falla

Las copias de respaldo automatizadas se crean durante la ventana de copia de respaldo de las instancias de base de datos. TaurusDB guarda copias de respaldo automatizadas basadas en el período de retención (1 a 732 días) especificado. Para obtener más información, consulte Configuración de una política de copia de respaldo automatizada.

En función de sus requisitos de servicio, puede:

- Restaurar datos en la instancia original, una nueva instancia o una instancia existente
- Restaurar datos de instancia en un punto específico en el tiempo
- Restaurar los datos de la tabla en un punto específico en el tiempo

Copias de respaldo entre regiones

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

Después de habilitar la copia de respaldo entre regiones, los archivos de copia de respaldo se almacenan automáticamente en la región especificada.

Despliegue de múltiples AZ

Una zona de disponibilidad 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 admite el despliegue de múltiples AZ para DR entre regiones.

Migración por falla

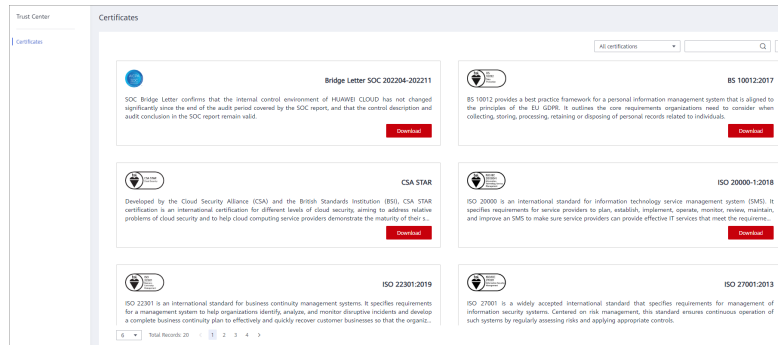
Una instancia de TaurusDB contiene un nodo principal y varias réplicas de lectura. Si un nodo primario no está disponible, TaurusDB falla automáticamente a una réplica de lectura.

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). Puedes [descargarlos](#).

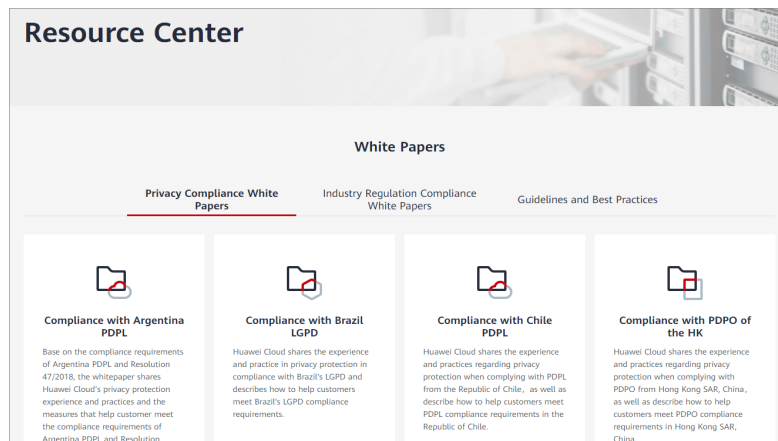
Figura 6-2 Descarga de certificados de cumplimiento



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 recurso](#).

Figura 6-3 Centro de recursos



7 Gestión de permisos

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

Si necesita asignar diferentes permisos a los empleados de su empresa para acceder a sus recursos de TaurusDB, **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.

Con IAM, puede usar su cuenta para crear usuarios de IAM para sus empleados y asignar permisos específicos a diferentes usuarios para controlar su acceso a tipos de recursos específicos. Por ejemplo, puede conceder a los desarrolladores de software de su empresa permisos para usar recursos de TaurusDB pero no permisos necesarios para eliminarlos o realizar operaciones de alto riesgo.

IAM se puede utilizar de forma gratuita. Solo paga por los recursos de su cuenta. Para obtener más información acerca de IAM, consulte [Descripción general del servicio IAM](#).

Permisos de TaurusDB

De forma predeterminada, los nuevos usuarios de IAM no tienen permisos asignados. Debe agregar un usuario a uno o más grupos y adjuntar políticas o roles de permisos a estos grupos. Los usuarios heredan permisos de los grupos a los que se agregan y pueden realizar operaciones específicas a servicios en la nube según los permisos.

TaurusDB es un servicio a nivel de proyecto implementado en regiones físicas específicas. Para asignar permisos de TaurusDB a un grupo de usuarios, especifique el ámbito como proyectos específicos de la región y seleccione proyectos para que los permisos surtan efecto. Si se selecciona **All projects**, los permisos se otorgarán al grupo de usuarios en todos los proyectos específicos de la región. Al acceder a TaurusDB, los usuarios deben cambiar a una región en la que se les haya autorizado a utilizar este servicio.

- **Políticas:** Un sistema más detallado. Las políticas le permiten definir los permisos necesarios para realizar operaciones en recursos específicos de la nube bajo ciertas condiciones. Permiten una gestión de permisos más flexible y cumplen con los requisitos de control de acceso seguro. Por ejemplo, puede conceder a los usuarios de TaurusDB solo los permisos necesarios para gestionar un determinado tipo de recursos de base de datos.

Tabla 7-1 enumera todas las funciones y políticas definidas por el sistema que TaurusDB admite.

Tabla 7-1 Funciones y políticas definidas por el sistema compatibles con TaurusDB

Política	Descripción	Tipo
GaussDB FullAccess	Permisos completos para TaurusDB	System-defined policy
GaussDB ReadOnlyAccess	Permisos de sólo lectura para TaurusDB	System-defined policy

Tabla 7-2 enumera las operaciones comunes soportadas por cada política o rol definido por el sistema de TaurusDB. Elija las directivas de sistema adecuadas basadas en esta tabla.

Tabla 7-2 Operaciones comunes respaldadas por cada política o función definida por el sistema de TaurusDB

Operación	GaussDB FullAccess	GaussDB ReadOnlyAccess
Creación de una instancia	Soportado	No soportado
Eliminación de una instancia	Soportado	No soportado
Consulta de una lista de instancias	Soportado	Soportado

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 base de datos	gaussdb:instance:create	<p>Para seleccionar una VPC, una subred y un grupo de seguridad, configure las siguientes acciones:</p> <p>vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get</p> <p>Para crear una instancia cifrada, configure el permiso de administrador de KMS para el proyecto.</p> <p>Para crear instancias anuales/mensuales, configure los permisos CBC: bss:renewal:view bss:renewal:update bss:balance:view bss:order:view</p>
Creación de una copia de respaldo manual	gaussdb:backup:create	-
Consulta de copias de respaldo	gaussdb:backup:list	-
Consulta de registros 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 parámetro	gaussdb:param:delete	-
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	-

Operación	Acción	Descripción
Eliminación de una copia de respaldo manual	gaussdb:backup:delete	-
Consulta de etiquetas de proyecto	gaussdb:tag:list	-
Aplicación de plantilla de parámetros	gaussdb:param:apply	-
Agregar o eliminar etiquetas de proyecto en 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 un 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	To select an IP address, configure the action: vpc:vpcs:listvpc: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	-
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 un EIP a una instancia de base de datos	gaussdb:instance:bindPublicIp	To display EIPs on the console, configure: vpc:publicIps:getvpc:publicIps:list

Operación	Acción	Descripción
Desvinculación de un 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	-
Asilamiento de nodos	gaussdb:instance:isolateNodes	-
Habilitación o deshabilitación del Explorador de SQL	gaussdb:instance:modifyTraceSQLPolicy	-
Creación de una instancia proxy de base de datos	gaussdb:proxy:create	-
Cambio de la dirección de división de lectura/escritura	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	-
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 proxy de base de datos	gaussdb:proxy:addNodes	-
Eliminación de nodos proxy de base de datos	gaussdb:proxy:deleteNodes	-

Operación	Acción	Descripción
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	-
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	-
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	-

8 Restricciones

Para garantizar la estabilidad y seguridad de TaurusDB, se establecen ciertas restricciones para el control de acceso o permisos. [Tabla 8-1](#) describe tales restricciones.

Tabla 8-1 Restricciones de función

Función	Restricciones
Acceso a TaurusDB	<ul style="list-style-type: none">● Si las instancias de TaurusDB no tienen EIP enlazadas, las instancias deben estar en la misma subred de VPC que los ECS asociados a 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 entrante al grupo de seguridad 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 base de datos predeterminado de TaurusDB: Para las instancias primarias/en espera, el puerto predeterminado es 3306. Puede cambiarlo si desea acceder a TaurusDB a través de otro puerto a través de una red privada o pública. Para obtener más información, consulte Cambiar un puerto de base de datos.
Permisos de raíz de base de datos	Sólo los permisos root para las instancias primarias y en espera están disponibles en la página de creación de instancias.
Modificación de parámetros de bases de datos	La mayoría de los parámetros se pueden modificar en la consola de TaurusDB.
Migración de datos	DRS o mysqldump se pueden utilizar para migrar datos a TaurusDB.
Motor de almacenamiento de MySQL	Solo se admite el motor de almacenamiento de InnoDB.

Función	Restricciones
Reinicio de instancia de TaurusDB	Las instancias de TaurusDB solo se pueden reiniciar en la consola de TaurusDB.
Archivos de copia de respaldo de TaurusDB	Los archivos de copia de respaldo de TaurusDB se almacenan en depósitos OBS y no son visibles para usted.
Binlog	No se puede habilitar Binlog para réplicas de lectura.
Tablas particionadas	TaurusDB es compatible con MySQL Community Server 8.0.22. Para una tabla con particiones de lista, hay hasta 256 valores en una partición, o se informa de un error. (Solución: Redistribuya el contenido de una partición de tabla en varias particiones.)

9 Facturación

Solo paga por lo que usa. No hay ningún cargo mínimo.

Concepto de facturación

Tabla 1 muestra los elementos de facturación de TaurusDB.

Tabla 9-1 Conceptos de facturación:

Concepto	Método de facturación
Instancia de base de datos	Anual/mensual o de pago por uso
Espacio de almacenamiento	Anual/mensual o de pago por uso <ul style="list-style-type: none"> ● Cuando compra una instancia anual/mensual, debe especificar su almacenamiento. Sin embargo, si el uso real excede el almacenamiento adquirido, se le facturará el almacenamiento adicional en una base de pago por uso. ● Cuando compra una instancia de pago por uso, no necesita especificar su almacenamiento, que se escalará dinámicamente en función de la cantidad de datos que se deben almacenar, y se factura cada hora en función de pago por uso.
Almacenamiento de copias de respaldo	TaurusDB proporciona espacio de almacenamiento para realizar copias de seguridad de todo el almacenamiento de su base de datos aprovisionada sin cargo adicional. Si el uso del almacenamiento de backup supera el 100% del almacenamiento de su base de datos aprovisionada, la parte adicional se facturará según el precio del almacenamiento de copia de respaldo.
Tráfico de red pública	Las instancias de TaurusDB son accesibles desde redes privadas y públicas, pero solo se factura el tráfico de redes públicas.
Monitoreo por segundos	Los precios se enumeran por hora, pero las facturas se calculan en función de la duración real del uso. TaurusDB proporciona monitorización cada 60 segundos de forma gratuita. Para obtener más información, consulte Configuración de monitoreo por segundos.

Para obtener más información, consulte [Detalles de precios del producto](#). Puede utilizar la calculadora de precios para calcular el costo de su uso de TaurusDB.

Modos de facturación

TaurusDB ofrece los dos modos de facturación siguientes:

- **Anual/Mensual:** Ofrece un descuento mayor que la facturación de pago por uso y se recomienda para uso a largo plazo. Si el espacio de almacenamiento de una instancia anual/mensual está lleno, el espacio adicional se facturará sobre una base de pago por uso.
- **Pago por uso (por hora):** le permite pagar solo por los recursos que realmente utiliza. Los precios se enumeran por hora, pero las facturas se calculan hasta la segunda.

Para cambiar el modo de facturación de tu instancia, consulte [Cambiar el modo de facturación de Pago por uso a anual/mensual](#) y [Cambiar el modo de facturación de anual/mensual a pago por uso](#).

Cambios de configuración

- **Modificación de las especificaciones de las instancias:** Puede cambiar las vCPU y la memoria de las instancias en función de los requisitos del servicio. Después de la modificación, se le facturará según las nuevas especificaciones.
- **Cambio de almacenamiento:** solo puede cambiar el almacenamiento de sus instancias anuales/mensuales en función de la cantidad de datos que deben almacenarse. Después del cambio, se le facturará en función del nuevo espacio de almacenamiento. El almacenamiento se puede escalar hacia arriba o hacia abajo solo en un múltiplo de 10 GB.

10 Servicios relacionados

La siguiente figura muestra la relación entre TaurusDB y otros servicios.

Tabla 10-1 Servicios relacionados

Servicio	Descripción
Elastic Cloud Service (ECS)	Le permite acceder a TaurusDB a través de 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 seguridad 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)	Se conecta a múltiples instancias de TaurusDB y le permite acceder a bases de datos distribuidas.

11 Diferencias entre TaurusDB y RDS for MySQL

TaurusDB tiene un buen rendimiento, escalabilidad y usabilidad. Para obtener más información, consulte [Tabla 11-1](#).

Tabla 11-1 Diferencias entre TaurusDB y RDS for MySQL

Concepto	RDS for MySQL	TaurusDB
Arquitectura	Arquitectura tradicional primaria/en espera. Los datos se sincronizan entre los nodos primario y en espera mediante binlog.	Arquitectura de computación y almacenamiento desacoplado. Los nodos de cómputo comparten los mismos datos y los datos no necesitan ser sincronizados mediante binlog.
Rendimiento	Cientos de miles de QPS, entregando tres veces el rendimiento del MySQL de código abierto en alta simultaneidad.	Millones de QPS, entregando siete veces el rendimiento del MySQL de código abierto. 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	<ul style="list-style-type: none"> ● Se pueden agregar hasta cinco réplicas de lectura para una instancia. El tiempo necesario para agregar réplicas de lectura depende del volumen de datos. La adición de réplicas de lectura requiere almacenamiento adicional. ● El almacenamiento puede crecer según sea necesario, con hasta 4 TB para una instancia. 	<ul style="list-style-type: none"> ● Se pueden agregar hasta 15 réplicas de lectura para una instancia. Gracias al almacenamiento compartido, el tiempo necesario para agregar réplicas de lectura no se ve afectado por el volumen de datos. Además, no se necesita almacenamiento adicional para la creación de réplicas de lectura. ● El almacenamiento crece según sea necesario con hasta 128 TB para una instancia.
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 una latencia más baja porque no se requiere sincronización de datos entre el nodo primario y las réplicas de lectura que usan binlog.
Restauración de copias de respaldo	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 utilizando copias de respaldo completas (instantáneas) y reproducción de rehacer. Su velocidad de restauración es más rápida.
Versión del motor de DB	MySQL 5.6, 5.7 y 8.0.	MySQL 8.0