

TaurusDB

Preguntas frecuentes

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 Consultoría de productos.....	1
1.1 ¿A qué debo prestar atención al usar TaurusDB?.....	1
1.2 ¿Qué puedo hacer sobre la respuesta lenta de los sitios web cuando usan TaurusDB?.....	1
1.3 ¿TaurusDB admite la conmutación por error automática?.....	2
1.4 ¿TaurusDB admite el desacoplamiento de computación y almacenamiento?.....	2
1.5 Congelación, liberación, eliminación y cancelación de la suscripción de recursos.....	2
2 Conexión de base de datos.....	4
2.1 ¿Qué debo hacer si no puedo conectarme a mi instancia TaurusDB?.....	4
2.2 ¿Puede un servidor externo tener acceso a la base de datos de TaurusDB?.....	15
2.3 ¿Qué hago si el número de conexiones de base de datos de TaurusDB alcanza el límite superior?.....	16
2.4 ¿Cuál es el número máximo de conexiones a una instancia de TaurusDB?.....	16
2.5 ¿Qué debo hacer si un ECS no puede conectarse a una instancia de TaurusDB?.....	18
2.6 ¿Cómo puedo conectarme a una base de datos de MySQL a través de JDBC?.....	18
2.7 ¿Cómo puedo crear y conectarme a un ECS?.....	24
2.8 ¿Qué debo hacer si un cliente de una base de datos ocasiona una falla de conexión?.....	24
2.9 ¿Por qué no puedo hacer ping a mi EIP después de vincularlo a una instancia de base de datos?.....	25
2.10 ¿Qué puedo hacer si falla la prueba de conexión?.....	26
2.11 ¿Puedo acceder a una instancia de TaurusDB a través de una conexión de intranet en todas las regiones?.....	26
2.12 ¿Existen riesgos potenciales si hay demasiadas conexiones a una instancia de TaurusDB?.....	27
2.13 ¿Qué debo hacer si un ECS y una instancia de TaurusDB desplegados en diferentes VPC no pueden comunicarse entre sí?.....	27
2.14 ¿Cómo puedo ver todas las direcciones IP conectadas a una base de datos?.....	27
3 Instalación del cliente.....	28
3.1 ¿Cómo puedo instalar el cliente de MySQL?.....	28
4 Migración de base de datos.....	31
4.1 ¿Qué tipos de motores de base de datos admite TaurusDB para importar datos?.....	31
5 Permisos de base de datos.....	32
5.1 ¿Proporciona TaurusDB la cuenta raíz o súper permiso?.....	32
6 Rendimiento de bases de datos.....	33
6.1 ¿Qué debo hacer si el uso de la CPU de mi instancia es alto?.....	33
6.2 ¿Cómo manejo las sentencias SQL lentas causadas por configuraciones de índice compuesto inadecuadas?.....	33

6.3 ¿Cómo manejo un gran número de tablas temporales que se generan para transacciones largas y un alto uso de memoria?.....	36
6.4 ¿Qué debo hacer si los bloqueos en transacciones largas bloquean la ejecución de transacciones posteriores?.....	37
6.5 ¿Cómo puedo usar el disco temporal de TaurusDB?.....	38
7 Uso de base de datos.....	43
7.1 ¿Por qué los resultados son incoherentes después de que la sentencia MATCH AGAINST se ejecuta, respectivamente, en nodos primarios y réplicas de lectura?.....	43
7.2 ¿Cómo agrego columnas usando INSTANT?.....	43
7.3 ¿Cómo uso LOAD DATA para importar datos locales?.....	44
8 Copias de respaldo.....	47
8.1 ¿Durante cuánto tiempo almacena TaurusDB los datos de copia de respaldo?.....	47
8.2 ¿Cómo puedo borrar el espacio de copia de respaldo de TaurusDB?.....	47
8.3 ¿Cómo puedo hacer una copia de respaldo de una base de datos de TaurusDB en un ECS?.....	48
8.4 ¿Cómo puedo ver mi uso de almacenamiento de copia de respaldo?.....	48
8.5 ¿Por qué ha fallado mi copia de respaldo automatizada?.....	49
8.6 ¿Cómo se facturan los datos de copia de respaldo de TaurusDB?.....	49
9 Modificación de parámetros de base de datos.....	51
9.1 ¿Cómo puedo cambiar la zona horaria?.....	51
9.2 ¿Cómo configuro una política de caducidad de contraseñas para instancias de TaurusDB?.....	52
9.3 ¿Cómo me aseguro de que el conjunto de caracteres de la base de datos de una instancia de TaurusDB es correcto?.....	53
9.4 ¿Cómo uso el conjunto de caracteres de utf8mb4 para almacenar emojis en una instancia de TaurusDB?.....	55
9.5 ¿Cómo configuro la sensibilidad a mayúsculas y minúsculas para los nombres de tablas de TaurusDB?.....	56
9.6 ¿Puedo usar comandos SQL para modificar parámetros globales?.....	57
10 Seguridad de red.....	58
10.1 ¿Qué medidas de garantía de seguridad tiene TaurusDB?.....	58
10.2 ¿Cómo puedo evitar que las direcciones IP de origen no confiables accedan a TaurusDB?.....	58
10.3 ¿Cómo configuro un grupo de seguridad para habilitar el acceso a una instancia de TaurusDB?.....	59
10.4 ¿Cómo puedo importar el certificado raíz a un servidor Windows o Linux?.....	59
10.5 ¿Cómo puedo gestionar y garantizar la seguridad de TaurusDB?.....	60
11 Gestión de registros.....	61
11.1 ¿Cómo puedo ver todos los registros de SQL ejecutados por TaurusDB?.....	61
11.2 ¿Cómo puedo ver los registros de consultas lentas de TaurusDB?.....	62
11.3 ¿Cómo habilito y veo Binlog de mi instancia de TaurusDB?.....	62
11.4 ¿Cómo cambio el período de retención de Binlog?.....	63
11.5 ¿Cómo puedo ver los registros de interbloqueo de TaurusDB?.....	64
12 Actualización de versión.....	65
12.1 ¿Cómo puedo comprobar una versión de instancia de TaurusDB?.....	65
12.2 ¿Puedo actualizar versiones de instancias de TaurusDB?.....	66

1 Consultoría de productos

1.1 ¿A qué debo prestar atención al usar TaurusDB?

1. Los sistemas operativos (SO) de instancia son invisibles para usted. Sus aplicaciones solo pueden acceder a una base de datos a través de una dirección IP y un puerto.
2. Los archivos de copia de respaldo almacenados en los depósitos del servicio de almacenamiento de objetos (OBS) y los servidores de nube elásticos (ECS) utilizados por TaurusDB son invisibles para usted. Solo son visibles para el sistema de gestión de instancias.
3. Cuando vea la instancia en la lista de instancias, seleccione la región donde se encuentra la instancia.
4. Precauciones después de crear instancias de TaurusDB:
Una vez creada la instancia, no es necesario realizar operaciones básicas de O&M de la base de datos, como la aplicación de HA y parches de seguridad, pero debe prestar atención a:
 - a. vCPUs y memoria de su instancia. Si se vuelven insuficientes, debe cambiarlos de manera oportuna.
 - b. Espacio de almacenamiento de la instancia. Si el almacenamiento se ha agotado, se le facturará de forma de pago por uso cualquier almacenamiento adicional, pero si amplía el almacenamiento por adelantado, puede pagar el almacenamiento adicional a tarifas anuales/mensuales.
 - c. Rendimiento de su instancia. Es necesario comprobar si las sentencias SQL de consulta lenta, las sentencias SQL que se van a optimizar, o los índices redundantes o que faltan regularmente.

1.2 ¿Qué puedo hacer sobre la respuesta lenta de los sitios web cuando usan TaurusDB?

Para resolver este problema:

- Compruebe el rendimiento de las instancias de TaurusDB en la consola TaurusDB.
- Compare el estado de la conexión a la base de datos de las bases de datos locales y las instancias de TaurusDB. Este problema depende de las aplicaciones web.

1.3 ¿TaurusDB admite la conmutación por error automática?

Sí. Durante la creación de una instancia de TaurusDB, se crean un nodo principal y una réplica de lectura. Si el nodo primario falla, la réplica de lectura se promueve automáticamente al nodo primario para proporcionar servicios, y el nodo primario original se degrada para ser una réplica de lectura.

1.4 ¿TaurusDB admite el desacoplamiento de computación y almacenamiento?

TaurusDB es compatible con el desacoplamiento de cómputo y almacenamiento, mejorando la alta disponibilidad y la experiencia en copia de respaldo y restauración, actualización y ampliación de capacidad.

1.5 Congelación, liberación, eliminación y cancelación de la suscripción de recursos

¿Por qué se lanzan mis recursos?

Si sus suscripciones han caducado pero no han sido renovadas, o si está en mora debido a un saldo insuficiente, sus recursos ingresan un período de gracia. Si no renueva las suscripciones ni recarga su cuenta después de que expire el período de gracia, sus recursos entrarán en un período de retención. Durante el período de retención, los recursos no están disponibles. Si la renovación aún no se ha completado o el importe pendiente aún no se paga al finalizar el período de retención, los datos almacenados se eliminarán y se liberarán los recursos del servicio en la nube. Para obtener más información, consulte [Suspensión de servicio y versión de recursos](#).

¿Por qué mis recursos están congelados?

Sus recursos pueden ser congelados por una variedad de razones. La razón más común es que usted está en mora.

¿Puedo hacer copias de respaldo de los datos si mi instancia de base de datos está congelada?

No. Si su instancia está congelada debido a retrasos, primero debe descongelar la instancia.

¿Cómo puedo descongelar mis recursos?

Congelado debido a atrasos: Puede renovar sus recursos o recargar su cuenta. Las instancias congeladas debido a atrasos pueden renovarse, liberarse o eliminarse. Las instancias anuales/mensuales que han caducado no pueden darse de baja, mientras que las que no han caducado pueden darse de baja.

¿Qué sucede cuando mis recursos son congelados, descongelados o liberados?

- Después de congelar sus recursos:
 - No se puede acceder a ellos, lo que causa tiempo de inactividad. Por ejemplo, si la instancia está congelada, no se puede conectar.
 - Si son recursos anuales/mensuales, no se pueden hacer cambios en ellos.
 - Pueden darse de baja o eliminarse manualmente.
- Después de que sus recursos se descongelen, puede conectarse a ellos de nuevo.
- Si se liberan los recursos, se eliminará la instancia.

¿Cómo puedo renovar mis recursos?

Después de que caduque una instancia anual/mensual, puede renovarla en la página [Renewals](#). Para obtener más información, consulte [Gestión de renovación](#).

¿Se pueden recuperar mis recursos después de ser liberados? /¿Puedo recuperar una cancelación de suscripción incorrecta?

Puede restaurar la instancia eliminada desde una copia de respaldo manual o reconstruir la instancia en la papelera de reciclaje durante el período de retención. Para obtener más información, consulte Restauración de datos en una instancia de base de datos y Reconstrucción de una instancia eliminada de la papelera de reciclaje .

Antes de cancelar la suscripción a un recurso, confirme la información del recurso cuidadosamente. Si se ha dado de baja de una instancia por error, compre una nueva.

¿Cómo puedo eliminar mi instancia?

- Para las instancias de pago por uso, consulte Eliminación de una instancia de base de datos facturada en una base de pago por uso.
- Para instancias anuales/mensuales, consulte Cancelar suscripción a una instancia anual/mensual.

2 Conexión de base de datos

2.1 ¿Qué debo hacer si no puedo conectarme a mi instancia TaurusDB?

Causas posibles

Pruebe lo siguiente:

1. **Compruebe si la instancia de base de datos está disponible.**
por ejemplo, el estado de la instancia de base de datos es anormal.
2. **(Common) Compruebe si la conexión del cliente es correcta.**
 - Si se conecta a una instancia de base de datos a través de una red privada, asegúrese de que la instancia de base de datos y ECS están en la misma región y VPC.
 - Si se conecta a una instancia de base de datos a través de una red pública, enlaza un EIP a la instancia de base de datos y, a continuación, conéctese a la instancia de base de datos a través de la EIP.
3. **Compruebe que se utiliza la conexión SSL.**
Ejecute cualquiera de los siguientes comandos de ejemplo para habilitar o deshabilitar SSL:
 - SSL habilitado: `mysql -h 172.16.0.31 -P 3306 -u root -p --ssl-ca=/tmp/ca.pem`
 - SSL deshabilitado: `mysql -h 172.16.0.31 -P 3306 -u root -p`
4. **Compruebe si los parámetros del comando de conexión son correctos.**
Por ejemplo, compruebe si los siguientes parámetros están configurados correctamente: dirección de conexión, número de puerto, nombre de usuario, contraseña y método de conexión.
5. **(Common) Compruebe si la conexión de red es normal.**
 - Para una conexión de red privada:
 - i. Compruebe si el ECS y la instancia de base de datos están en la misma región y VPC.
 - ii. Compruebe las reglas del grupo de seguridad.

- iii. En el ECS, compruebe si se puede conectar el puerto de instancia de base de datos.
 - Para una conexión de red pública:
 - i. Compruebe las reglas del grupo de seguridad.
 - ii. Compruebe las reglas de ACL (lista de control de acceso) de la red.
 - iii. Haga ping a los ECS de la misma región a la instancia de base de datos.
6. **(Common) Compruebe si hay demasiadas conexiones a la instancia de base de datos.**

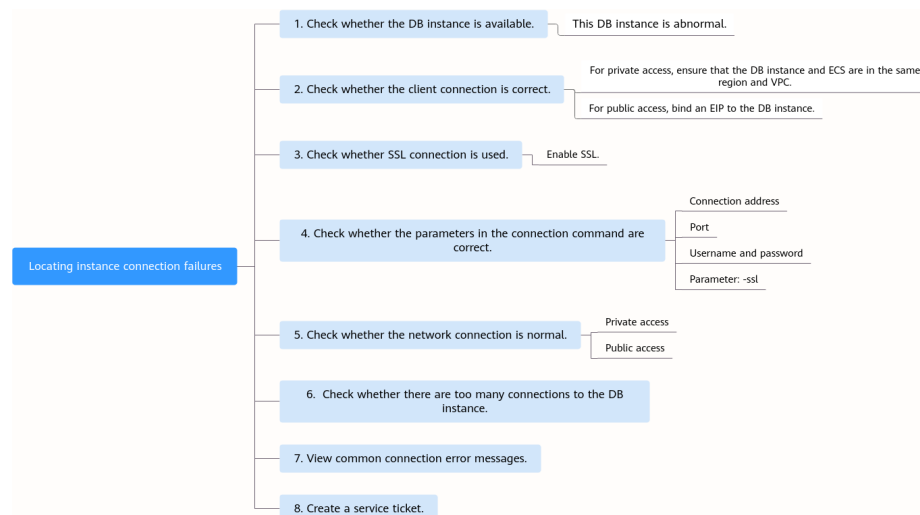
Si hay un número excesivo de conexiones de base de datos, es posible que las aplicaciones no puedan conectarse.

7. **Ver mensajes de error de conexión comunes.**

Encuentre las soluciones correspondientes basadas en mensajes de error de conexión.

Localización de fallas

Figura 2-1 ¿Qué puedo hacer si no puedo conectarme a mi instancia de base de datos?



1. **Compruebe si la instancia de base de datos está disponible.**

Compruebe si la instancia de base de datos está en el estado **Available**.

Posible causa: la instancia de base de datos es anormal.

Solución: Si la instancia de base de datos es anormal, reinicie la misma.

Figura 2-2 Comprobación del estado de la instancia de base de datos

NameID	Description	DB Instan...	DB Engine	Status	Billing Mode	Private IP Ad...	Enterprise Pr...	Created	Database Port	Storage Type	Operation
		PrimarySta...	GaussDB(for M...	Available	Pay-Per-Use	192.168.0.100	default	Aug 22, 2023 1...	3306	Shared	Log In View Metric More

2. **Compruebe si la conexión del cliente es correcta.**

Instale un **cliente de MySQL 8.0**.

Para obtener más información sobre cómo conectarse a una instancia de base de datos a través de una red privada o pública, consulte **¿Puede un servidor externo tener acceso a la base de datos de TaurusDB?**

Tabla 2-1 Modelo de conexión

Método de conexión	Escenario	Ejemplo
Red privada	De forma predeterminada, se proporciona una dirección IP privada. Si las aplicaciones se implementan en un ECS que se encuentra en la misma región y VPC que la instancia de base de datos, conéctese a la instancia de ECS y de base de datos a través de una dirección IP privada.	mysql -h <i>private IP address</i> -P 3306 -u root -p --ssl-ca=/tmp/ca.pem Vaya a la página Basic Information de la instancia y vea la dirección IP privada en el área Network Information .
Red pública	Si no puede acceder a la instancia de base de datos utilizando una dirección IP privada, enlaza un EIP a la instancia de base de datos y, a continuación, conéctese a la instancia de base de datos a través de la EIP. Para obtener información sobre los precios de EIP, consulte Detalles de facturación de EIP .	mysql -h <i>EIP</i> -P 3306 -u root -p --ssl-ca=/tmp/ca.pem Vaya a la página Basic Information de la instancia y vea la EIP en el área Network Information .

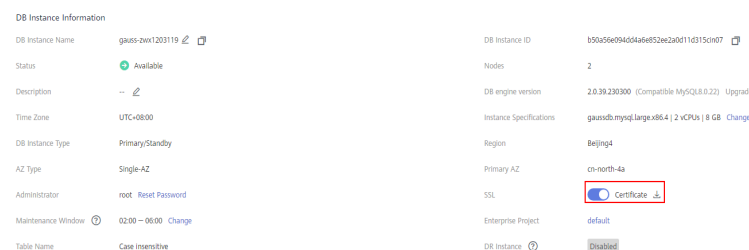
3. **Compruebe si la conexión SSL es usada.**

- (Recomendado) Habilite SSL en la página **Basic Information** de la instancia, descargue y descomprima el paquete y cargue el certificado raíz **ca.pem** en el directorio **/tmp** del ECS.

Ejemplo:

mysql -h 172.16.0.31 -P 3306 -u root -p --ssl-ca=/tmp/ca.pem

Figura 2-3 Habilitación de SSL



- Conexión común: Deshabilite SSL en la página **Basic Information**.

Ejemplo:

mysql -h 172.16.0.31 -P 3306 -u root -p

4. **Verifique los parámetros en el comando utilizado para conectarse.**

Asegúrese de que la dirección de conexión, el puerto, el nombre de usuario y la contraseña y el certificado SSL sean correctos e intente conectarse de nuevo a la instancia de base de datos.

- **Conexión a una instancia de base de datos a través de una red privada**

- **Connection command**
mysql -h connection address -P database port -u username -p --ssl-ca= SSL certificate name

Ejemplo:

mysql -h 192.168.0.153 -P 3306 -u root -p --ssl-ca=/tmp/ca.pem

- **Dirección de conexión**
Vaya a la página **Basic Information** de la instancia y vea la dirección IP privada en el área **Network Information**.

Figura 2-4 Dirección IP privada



- **puerto de base de datos**
Vaya a la página **Basic Information** de la instancia y vea el puerto de la base de datos en el área **Network Information**.
- **Nombre de usuario**
Ingrese **root** y su contraseña.
- **Nombre de certificado de SSL**
Nombre del archivo de certificado SSL. La ruta de acceso y el nombre del archivo deben ser los mismos que los del comando.

– **Conexión a una instancia de base de datos a través de una red pública**

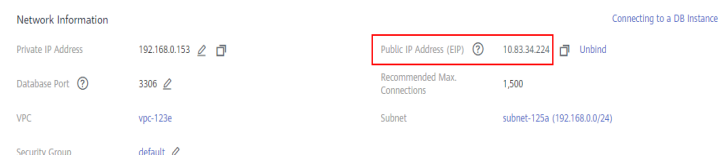
- **Comando de conexión**
mysql -h connection address -P database port -u username -p --ssl-ca= SSL certificate name

Ejemplo:

mysql -h 10.83.34.224 -P 3306 -u root -p --ssl-ca=/tmp/ca.pem

- **EIP**
Vaya a la página **Basic Information** de la instancia y vea la EIP en el área **Network Information**.

Figura 2-5 EIP



- **Puerto de base de datos**
Vaya a la página **Basic Information** de la instancia y vea el puerto de la base de datos en el área **Network Information**.

- Nombre de usuario y contraseña
Asegúrese de haber introducido correctamente la contraseña de root.
 - Certificado
Introduzca el nombre del archivo de certificado SSL. La ruta de acceso y el nombre del archivo deben ser los mismos que los del comando.
5. **Comprobar si la conexión de red es normal.**
- Conexión de red privada**
- a. Compruebe si el ECS y la instancia de base de datos están en la misma región y VPC.
 - Si la instancia ECS y DB están en diferentes regiones, no pueden comunicarse entre sí. Seleccione una región cercana a su área de servicio para reducir la latencia de la red y disfrutar de un acceso más rápido. Para conectarse a la instancia de base de datos en todas las regiones, utilice Cloud Connect (CC) o Virtual Private Network (VPN).
 - Si la instancia ECS y DB están en diferentes VPC de la misma región, no pueden comunicarse entre sí a través de una red privada. Después de crear una instancia de base de datos, no puede cambiar su VPC. En este caso, cree una conexión de interconexión de VPC. Para obtener más información, consulte [¿Qué debo hacer si un ECS y una instancia de TaurusDB desplegados en diferentes VPC no pueden comunicarse entre sí?](#)

Figura 2-6 Comprobación de la VPC de un ECS

ECS Information


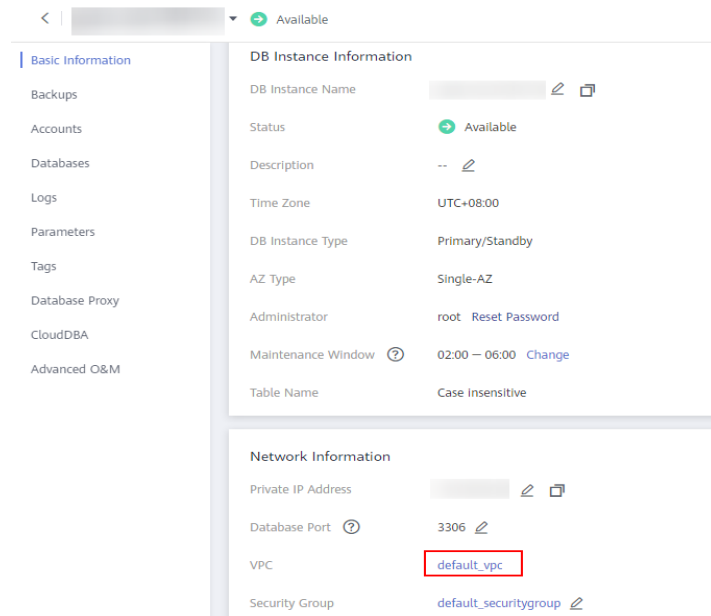
ID	37144dd6-2d7f-42c4-92bd-e6e1003361e8
Name	ecs-5948 
Description	-- 
Region	
AZ	AZ3
Specifications	General computing 1 vCPU 1 GiB sn3.small.1
Image	CentOS 8.2 64bit Public image
VPC	default_vpc

Figura 2-7 Comprobación de la VPC de una instancia de TaurusDB



- b. Compruebe las reglas del grupo de seguridad.
- Si **Destination** no es **0.0.0.0/0** y **Protocol & Port** no es **All** en la página **Outbound Rules** del ECS, agregue la dirección IP privada y el puerto de la instancia de base de datos a las reglas de salida.

Figura 2-8 Grupo de seguridad de ECS

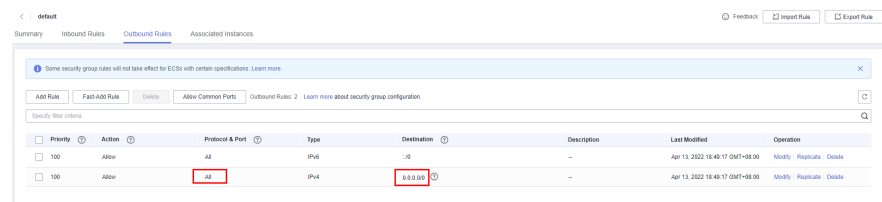


Figura 2-9 Adición rápida de una regla de salida (dirección IP privada de una instancia de base de datos)

Fast-Add Inbound Rule [Learn more about security group configuration.](#)

★ Protocols and Ports

Remote Login and Ping:

SSH (22) RDP (3389) FTP (20-21) Telnet (23) ICMP (All)

Web Service:

HTTP (80) HTTPS (443) HTTP_ALT (8080)

Database:

MySQL (3306) MS SQL (1433) PostgreSQL (5432) Oracle (1521) Redis (6379)

★ Type: IPv4

★ Source: IP address

Text input field for IP address

Action:

Figura 2-10 Adición de una regla de salida (dirección IP privada de una instancia de base de datos)

Add Inbound Rule [Learn more about security group configuration.](#)

Some security group rules will not take effect for ECSs with certain specifications. [Learn more](#)
If you select IP address for Source, you can enter multiple IP addresses in the same IP address box. Each IP address represents a different security group rule.

Security Group: default

You can import multiple rules in a batch.

Priority	Action	Type	Protocol & Port	Source	Description	Operation
1-100	Allow	IPv4	Protocols and Ports/... 3306	IP address		Replicate Delete

- Agregue la dirección IP privada y el puerto del ECS a las reglas entrantes.

Figura 2-11 Adición rápida de una regla de entrada (dirección IP privada de un ECS)

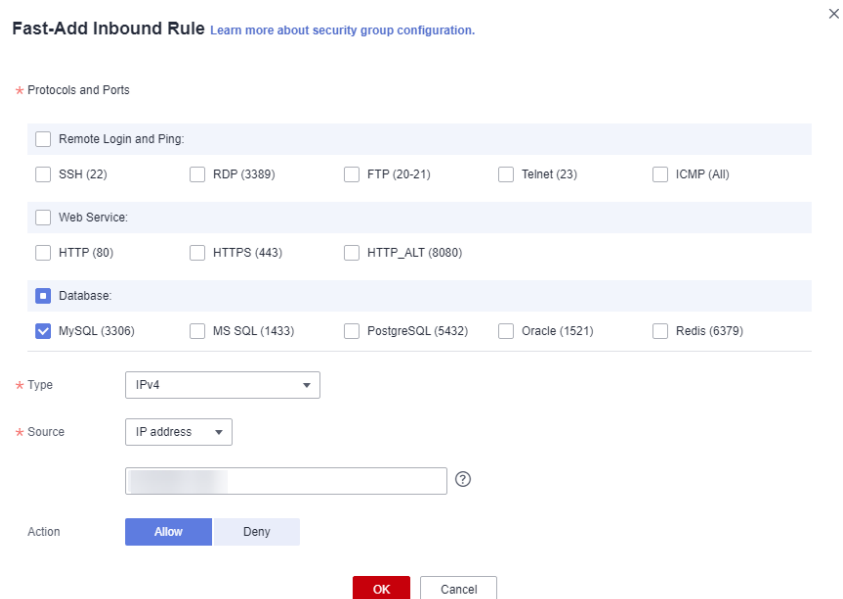
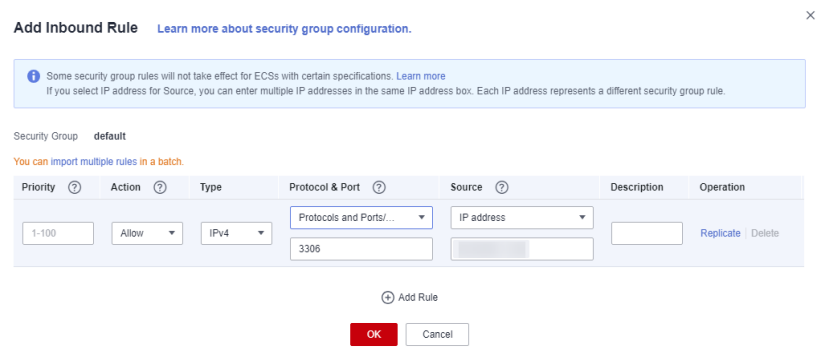


Figura 2-12 Adición de una regla de entrada (dirección IP privada de un ECS)



- c. En ECS, compruebe si se puede conectar la dirección IP privada de la instancia de base de datos.

telnet private IP address

Example:

telnet 192.168.0.153 3306

- Si la conexión es normal, la red es normal.
- Si la conexión falla, cree un ticket de servicio para ponerse en contacto con el servicio de atención al cliente para obtener ayuda.

Conexión de red pública

- a. Compruebe las reglas del grupo de seguridad.
- Si **Destination** no es **0.0.0/0** y **Protocol & Port** no es **All** en la página **Outbound Rules** del ECS, agregue la EIP y el puerto de la instancia de base de datos a las reglas salientes.

Figura 2-13 Grupo de seguridad de ECS

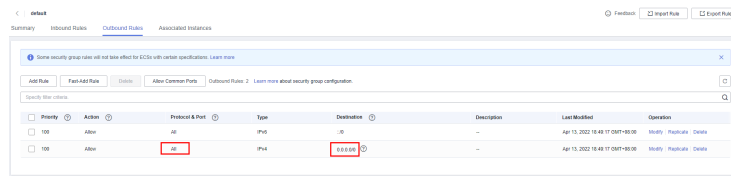


Figura 2-14 Adición rápida de una regla de salida (EIP de instancia de BD)

Fast-Add Inbound Rule [Learn more about security group configuration.](#)

* Protocols and Ports

Remote Login and Ping:
 SSH (22) RDP (3389) FTP (20-21) Telnet (23) ICMP (All)

Web Service:
 HTTP (80) HTTPS (443) HTTP_ALT (8080)

Database:
 MySQL (3306) MS SQL (1433) PostgreSQL (5432) Oracle (1521) Redis (6379)

* Type

* Source

Action

Figura 2-15 Adición de una regla de salida (EIP de instancia de BD)

Add Inbound Rule [Learn more about security group configuration.](#)

Some security group rules will not take effect for ECSs with certain specifications. [Learn more](#)
 If you select IP address for Source, you can enter multiple IP addresses in the same IP address box. Each IP address represents a different security group rule.

Security Group **default**

You can import multiple rules in a batch.

Priority	Action	Type	Protocol & Port	Source	Description	Operation
1-100	Allow	IPv4	Protocols and Ports/...	IP address		Replicate Delete
			3306			

- Agregue la EIP y el puerto del ECS a las reglas entrantes.

Figura 2-16 Adición de una regla de entrada (ECS EIP)

Fast-Add Inbound Rule [Learn more about security group configuration.](#)

* Protocols and Ports

Remote Login and Ping:

SSH (22) RDP (3389) FTP (20-21) Telnet (23) ICMP (All)

Web Service:

HTTP (80) HTTPS (443) HTTP_ALT (8080)

Database:

MySQL (3306) MS SQL (1433) PostgreSQL (5432) Oracle (1521) Redis (6379)

* Type: IPv4

* Source: IP address

Action:

Figura 2-17 Adición de una regla de entrada (ECS EIP)

Add Inbound Rule [Learn more about security group configuration.](#)

Security Group default

You can import multiple rules in a batch.

Priority	Action	Type	Protocol & Port	Source	Description	Operation
1-100	Allow	IPv4	Protocols and Ports/... 3306	IP address		Replicate Delete

- b. Compruebe las reglas de ACL (lista de control de acceso) de la red.
 - i. Vaya a la [ACL de la red](#).
 - ii. Compruebe si la NIC a la que el TaurusDB y la EIP enlazados pertenecen a la subred asociada a la ACL de la red.
 - iii. Compruebe si la ACL de red está habilitada.

En caso afirmativo, [agregue una regla ICMP para permitir el tráfico](#).



La regla ACL de red predeterminada deniega todos los paquetes entrantes y salientes. Esta regla predeterminada se sigue aplicando incluso si la ACL de red está deshabilitada.

- c. Hacer ping a la instancia de base de datos en un ECS en la misma región.

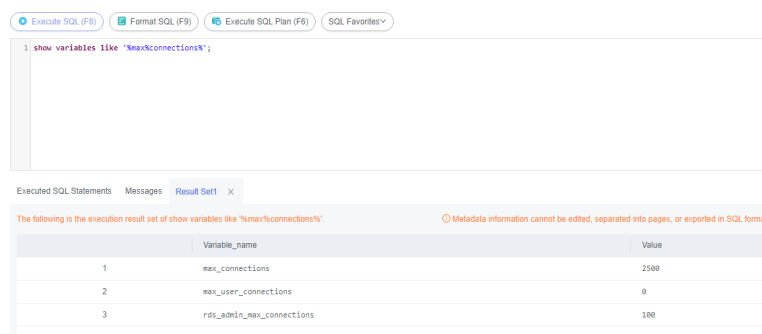
Si no puede hacer ping al EIP de la instancia de base de datos desde un ECS, intente hacer ping desde otro ECS en la misma región. Si la EIP se puede hacer ping, la red es normal. En este caso, cree un ticket de servicio para ponerse en contacto con el servicio de atención al cliente.

6. Compruebe si hay demasiadas conexiones a la instancia de base de datos.

Método de comprobación:

- a. [Log in to the management console.](#)
- b. Click  in the upper left corner and select a region and a project.
- c. Haga clic en  en la esquina superior izquierda de la página y elija **Databases > TaurusDB.**
- d. En la página **Instances**, busque la instancia de base de datos y haga clic en **Log In** en la columna **Operation.**
- e. Ingrese la contraseña y haga clic en **Test Connection.** Una vez que la conexión se haya realizado correctamente, haga clic en **Log In** para acceder a DAS.
- f. Elija **SQL Operations > SQL Query.**
- g. Ingrese el comando y haga clic en **Execute SQL** para comprobar el número de conexiones de instancia.

show variables like '%max%connections%';



- **max_connections:** el número máximo de clientes que se pueden conectar al mismo tiempo. Si este parámetro se establece en **default**, el número máximo de clientes depende de la cantidad de memoria configurada. Para obtener más información, consulte [¿Cuál es el número máximo de conexiones a una instancia de TaurusDB?](#)
 - **max_user_connections:** el número máximo de conexiones simultáneas permitidas para una cuenta específica de TaurusDB.
- h. Compruebe si el total de conexiones y las conexiones activas actuales han alcanzado los límites superiores consultando Consulta de métricas de monitoreo de instancia. Determine si desea liberar las conexiones.

Causa posible: si hay demasiadas conexiones de base de datos, es posible que las aplicaciones no puedan conectarse y que las copias de respaldo completas e incrementales fallen, lo que afecta a los servicios.

Solución:

- a. Compruebe si las aplicaciones están conectadas, optimice las conexiones y libere conexiones innecesarias.
- b. Si este parámetro se establece en **default**, puede escalar la instancia de base de datos para establecer **max_connections** en un valor mayor. Para obtener más información, consulte Cambio de las vCPU y memoria de una instancia de base de datos.
- c. Compruebe si las métricas son anormales y si se generan alarmas en la consola de Cloud Eye. Cloud Eye supervisa las métricas de la base de datos, como el uso de la

CPU, el uso de la memoria, el uso del espacio de almacenamiento y las conexiones a la base de datos, y le permite configurar políticas de alarmas para identificar los riesgos por adelantado si se generan alarmas. Para obtener más información sobre las métricas de monitorización compatibles, consulte Introducción a las métricas TaurusDB.

7. Ver mensajes de error de conexión comunes.

Cuando ejecuta comandos para conectarse a una instancia de base de datos, comprender los mensajes de error puede ayudar:

- ERROR 2013: Se perdió la conexión al servidor MySQL durante la consulta
Si los valores de **wait_timeout** y **interactive_timeout** son demasiado pequeños, el cliente de TaurusDB desconectará automáticamente la conexión vacía de tiempo de espera. Para obtener más información, consulte Cliente desconectado automáticamente de una instancia de base de datos.
- ERROR 1045 : Access denied for user 'root'@'192.168.0.30' (using password: YES)
Compruebe si la contraseña es correcta y si el ECS tiene el permiso para conectarse a la instancia de base de datos. Para obtener más información, consulte "Access denied" se muestra durante la conexión de base de datos.
- Error message "SSL routines: tls_early_post_process_client_hello:unsupported protocol"
Compruebe la versión TLS de TaurusDB, y actualice la versión TLS del cliente. Para obtener más información, consulte Error de conexión SSL debido a versiones TLS incoherentes.
- Error notificado cuando se utiliza JDBC para conectarse a la base de datos: "unable to find certification path to requested target"
El paquete JAR de MariaDB se utiliza para conectarse a la base de datos, que es ligeramente diferente del paquete de controladores oficial de MySQL. Para obtener más información, consulte Error al conectarse a una base de datos usando mariadb-connector en modo SSL.

8. Si el problema persiste, cree un ticket de servicio.

2.2 ¿Puede un servidor externo tener acceso a la base de datos de TaurusDB?

Una instancia enlazada con una EIP

Para un caso que ha sido vinculado con una EIP, puede acceder a él a través de la EIP.

Para más detalles, consulte:

Vinculación de una EIP

Una instancia no vinculada con una EIP

- Habilite una VPN en una VPC y use la VPN para conectarse a la instancia TaurusDB.
- Cree una instancia de TaurusDB y un TaurusDB en la misma VPC y acceda a TaurusDB a través del TaurusDB.

Para más detalles, consulte:

Conexión a una instancia de base de datos a través de una red privada

2.3 ¿Qué hago si el número de conexiones de base de datos de TaurusDB alcanza el límite superior?

El número de conexiones a la base de datos indica el número de aplicaciones que se pueden conectar simultáneamente a una base de datos y es irrelevante para el número máximo de usuarios permitidos por sus aplicaciones o sitios web.

Si hay un número excesivo de conexiones de base de datos, es posible que las aplicaciones no se conecten y que las copias de respaldo completas e incrementales fallen, lo que afecta a los servicios.

Localización de fallas

1. Compruebe si las aplicaciones están conectadas, optimice las conexiones y libere conexiones innecesarias.
2. Compruebe las especificaciones y escálelas si es necesario.
3. Compruebe si las métricas son anormales y si se generan alarmas en la consola de Cloud Eye. Cloud Eye supervisa las métricas de la base de datos, como el uso de la CPU, el uso de la memoria, el uso del espacio de almacenamiento y las conexiones a la base de datos, y le permite configurar políticas de alarmas para identificar los riesgos por adelantado si se generan alarmas. Para obtener más información, consulte el *Guía de usuario de Cloud Eye*.

Solución

1. Conéctese a una instancia a través de una red privada. El uso de una red privada evita la congestión causada por un ancho de banda insuficiente.
Para más detalles, consulte:
Conexión de una instancia de base de datos a través de una red privada
2. En la consola, establezca el parámetro **innodb_adaptive_hash_index** en **off** para reducir el tiempo de espera del bloqueo.
Para obtener más información, consulte *Modificación de una plantilla de parámetro*.
3. Optimice las consultas lentas.

2.4 ¿Cuál es el número máximo de conexiones a una instancia de TaurusDB?

TaurusDB no tiene restricciones sobre el número de conexiones. Este número está determinado por el valor predeterminado y el rango de valores del motor de base de datos. Por ejemplo, puede establecer **max_connections** y **max_user_connections** en una plantilla de parámetros para configurar el número máximo de conexiones para una instancia de TaurusDB.

Cambio del número máximo de conexiones

El número de conexiones se puede cambiar en línea. Para obtener más información, consulte *Modificación de una plantilla de parámetro*.

Puede ejecutar comandos para cambiar el número máximo de conexiones.

1. Compruebe el número máximo de conexiones:
show global variables like 'max_connections';
2. Cambie el valor de **max_connections** en **mysqld** en el archivo **my.cnf**.
[mysqld]
max_connections = 1000

Acerca de max_connections

max_connections indica el número máximo de clientes que se pueden conectar al mismo tiempo. Si este parámetro se establece en **default** está relacionado con la memoria de instancia (unidad: GB). La fórmula de cálculo es la siguiente:

Valor estimado de max_connections = Memoria disponible en el nodo/Memoria estimada ocupada por una única conexión.

- Memoria de nodo disponible = Memoria total – Memoria ocupada por el grupo de búferes – 1 GB (proceso mysqld, sistema operativo y programa de supervisión)
- Uso de memoria estimado de una sola conexión (single_thread_memory) = thread_stack (256 KB) + binlog_cache_size (32 KB) + join_buffer_size (256 KB) + sort_buffer_size (256 KB) + read_buffer_size (128 KB) + read_rnd_buffer_size (256 KB) ≈ 1 MB

En la siguiente tabla se enumeran los valores predeterminados de **max_connections** para diferentes especificaciones de memoria.

Tabla 2-2 Max_connections para diferentes especificaciones de memoria

Memoria (GB)	Conexiones
512	100,000
384	80,000
256	60,000
128	30,000
64	18,000
32	10,000
16	5,000
8	2,500
4	1,500
2	800

2.5 ¿Qué debo hacer si un ECS no puede conectarse a una instancia de TaurusDB?

Realice los siguientes pasos para identificar el problema:

Paso 1 Compruebe si la instancia ECS y TaurusDB están ubicadas en la misma VPC.

- Si están en la misma VPC, vaya a [Paso 2](#).
- Si se encuentran en VPC diferentes, cree un ECS en la VPC donde se encuentra la instancia.

Paso 2 Compruebe si se ha creado un grupo de seguridad para el ECS.

- Si se ha creado un grupo de seguridad, compruebe si sus reglas son apropiadas.
Para obtener más información, consulte la descripción del grupo de seguridad en "Creación de una instancia" en *Pasos iniciales de TaurusDB*. A continuación, vaya a [Paso 3](#).
- Si no se ha creado ningún grupo de seguridad, vaya a la consola de VPC desde la página de detalles de ECS y cree un grupo de seguridad.

Paso 3 Compruebe si el ECS puede conectarse a la instancia a través del puerto de la instancia.

El puerto predeterminado de una instancia primaria/en espera es **3306**.

```
telnet <IP address> {Port number}
```

- Si el ECS puede conectarse a la instancia, no se requiere ninguna acción adicional.
- Si el ECS aún no puede conectarse al puerto de instancia, póngase en contacto con el soporte técnico.

----Fin

2.6 ¿Cómo puedo conectarme a una base de datos de MySQL a través de JDBC?

Aunque el certificado SSL es opcional si elige conectarse a una base de datos a través de la conectividad de bases de datos Java (JDBC), se recomienda descargar el certificado SSL para cifrar las conexiones por motivos de seguridad. De forma predeterminada, la encriptación de datos SSL está habilitado para las instancias de TaurusDB recién creadas. Habilitar SSL aumentará el tiempo de respuesta de la conexión de red y el uso de la CPU. Antes de habilitar SSL, evalúe el impacto en el rendimiento del servicio. Para obtener más información sobre cómo habilitar o deshabilitar SSL, consulte Configuración de SSL.

Prerrequisitos

Familiarícese con:

- Conceptos básicos de la computadora
- Lenguaje de programación Java
- Conocimiento de JDBC

Conexión con el certificado SSL

El certificado SSL debe descargarse y verificarse para conectarse a bases de datos.


NOTA

Si el valor `ssl_type` de un usuario de base de datos es `x509`, este método no está disponible.

Para comprobar el valor `ssl_type` del usuario actual, ejecute el siguiente comando:

```
select ssl_type from mysql.user where user = 'xxx';
```

Paso 1 Descargue el certificado de CA o el paquete de certificados.

1. En la página **Instances**, haga clic en el nombre de la instancia para ir a la página **Basic Information**.
2. En el área **DB Instance Information**, haga clic en  junto a **SSL**.

Paso 2 Utilice la herramienta de claves para generar un archivo de almacén de confianza con el certificado de CA.

```
<keytool installation path> ./keytool.exe -importcert -alias <MySQLCACert> -file <ca.pem> -keystore <truststore_file> -storepass <password>
```

Tabla 2-3 Descripción de parámetros

Parámetro	Descripción
<keytool installation path>	Directorio bin en la ruta de instalación JDK o JRE, por ejemplo, C:\Program Files (x86)\Java\jdk11.0.7\bin .
<MySQLCACert>	Nombre del archivo de truststore. Establezca un nombre específico para el servicio para su identificación futura.
<ca.pem>	Nombre del certificado de CA descargado y descomprimido en Paso 1 , por ejemplo, ca.pem .
<truststore_file>	Ruta de acceso para almacenar el archivo truststore.
<password>	Contraseña del archivo truststore.

Ejemplo de código (uso de keytool en la ruta de instalación de JDK para generar el archivo truststore):

```
Owner: CN=MySQL_Server_8.0.22_Auto_Generated_CA_Certificate
Issuer: CN=MySQL_Server_8.0.22_Auto_Generated_CA_Certificate
Serial number: 1
Valid from: Thu Feb 16 11:42:43 EST 2017 until: Sun Feb 14 11:42:43 EST 2027
Certificate fingerprints:
    MD5: 18:87:97:37:EA:CB:0B:5A:24:AB:27:76:45:A4:78:C1
    SHA1: 2B:0D:D9:69:2C:99:BF:1E:2A:25:4E:8D:2D:38:B8:70:66:47:FA:ED
SHA256:C3:29:67:1B:E5:37:06:F7:A9:93:DF:C7:B3:27:5E:09:C7:FD:EE:2D:18:86:F4:9C:40:
D8:26:CB:DA:95: A0:24
    Signature algorithm name: SHA256withRSA Subject Public Key Algorithm: 2048-
bit RSA key
Version: 1
Trust this certificate? [no]: y
Certificate was added to keystore
```

Paso 3 Conéctese a la instancia TaurusDB a través de JDBC.

```
jdbc:mysql://<instance_ip>:<instance_port>/<database_name>?  
requireSSL=<value1>&useSSL=<value2>&verifyServerCertificate=<value3>&trustCertificateKeyStoreUrl=file:  
<truststore_file>&trustCertificateKeyStorePassword=<password>
```

Tabla 2-4 Descripción de parámetros

Parámetro	Descripción
<instance_ip>	Dirección IP de la instancia de base de datos. NOTA <ul style="list-style-type: none"> ● Si está accediendo a la instancia a través de ECS, <i>instance_ip</i> es la dirección IP privada de la instancia. Puede ver la dirección IP privada en el área Network Information del Basic Information. ● Si está accediendo a la instancia a través de una red pública, <i>instance_ip</i> indica la EIP que se ha enlazado a la instancia. Puede ver la dirección IP privada en el área Network Information del Basic Information.
<instance_port>	Puerto de base de datos de la instancia. El puerto predeterminado es 3306 . NOTA Puede ver la dirección IP privada en el área Network Information del Basic Information .
<database_name>	Nombre de la base de datos utilizada para conectarse a la instancia. El valor predeterminado es mysql .
<value1>	Valor de requireSSL que indica si el servidor admite SSL. Puede ser cualquiera de las siguientes: <ul style="list-style-type: none"> ● true: El servidor admite SSL. ● false: El servidor no admite SSL. NOTA Para obtener más información acerca de la relación entre requireSSL y sslmode consulte Tabla 2-5 .
<value2>	Valor de useSSL que indica si el cliente utiliza SSL para conectarse al servidor. Puede ser cualquiera de las siguientes: <ul style="list-style-type: none"> ● true: El cliente utiliza SSL para conectarse al servidor. ● false: El cliente no utiliza SSL para conectarse al servidor. NOTA Para obtener más información acerca de la relación entre useSSL y sslmode , consulte Tabla 2-5 .
<value3>	Valor de verifyServerCertificate que indica si el cliente verifica el certificado de servidor. Puede ser cualquiera de las siguientes: <ul style="list-style-type: none"> ● true: El cliente verifica el certificado del servidor. ● false: El cliente no comprueba el certificado del servidor. NOTA Para obtener más información acerca de la relación entre verifyServerCertificate y sslmode , consulte Tabla 2-5 .
<truststore_file>	Ruta de acceso para almacenar el archivo de almacén de confianza configurado en Paso 2 .

Parámetro	Descripción
<password>	Contraseña del archivo de almacén de confianza configurado en Paso 2 .

Tabla 2-5 Relación entre parámetros de conexión y sslmode

useSSL	requireSSL	verifyServerCertificate	sslMode
false	N/A	N/A	DISABLED
true	false	false	PREFERRED
true	true	false	REQUIRED
true	N/A	true	VERIFY_CA

Ejemplo de código (código Java para conectarse a una instancia de TaurusDB):

```
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.ResultSet;
import java.sql.Statement;
import java.sql.SQLException;
public class JDBCtest {
    static final String USER = "xxx";
    static final String PASS = "xxx";

    public static void main(String[] args) {
        Connection conn = null;
        Statement stmt = null;

        String url = "jdbc:mysql://<instance_ip>:<instance_port>/<database_name>?
requireSSL=true&useSSL=true&verifyServerCertificate=true&trustCertificateKeyStoreU
rl=file:
<truststore_file>&trustCertificateKeyStorePassword=<password>";
        try {
            Class.forName("com.mysql.cj.jdbc.Driver");
            conn = DriverManager.getConnection(url, USER, PASS);
            stmt = conn.createStatement();
            String sql = "show status like 'ssl%'";
            ResultSet rs = stmt.executeQuery(sql);

            int columns = rs.getMetaData().getColumnCount();
            for (int i = 1; i <= columns; i++) {
                System.out.print(rs.getMetaData().getColumnName(i));
                System.out.print("\t");
            }

            while (rs.next()) {
                System.out.println();
                for (int i = 1; i <= columns; i++) {
                    System.out.print(rs.getObject(i));
                    System.out.print("\t");
                }
            }
            rs.close();
            stmt.close();
            conn.close();
        } catch (SQLException se) {
```

```

        se.printStackTrace();
    } catch (Exception e) {
        e.printStackTrace();
    } finally {
        // release resource ....
    }
}
}
}

```

----Fin

Conexión sin el certificado SSL

NOTA

No es necesario descargar el certificado SSL porque no se requiere la verificación del certificado en el servidor.

Paso 1 Conéctese a su instancia TaurusDB a través de JDBC.

```
jdbc:mysql://<instance_ip>:<instance_port>/<database_name>?useSSL=false
```

Tabla 2-6 Descripción de parámetros

Parámetro	Descripción
<instance_ip>	Dirección IP de la instancia. NOTA <ul style="list-style-type: none"> ● Si está accediendo a la instancia a través de ECS, <i>instance_ip</i> es la dirección IP privada de la instancia. Puede ver la dirección IP privada en el área Network Information del Basic Information. ● Si está accediendo a la instancia a través de una red pública, <i>instance_ip</i> indica la EIP que se ha enlazado a la instancia. Puede ver la dirección IP privada en el área Network Information del Basic Information.
<instance_port>	Puerto de base de datos de la instancia. El puerto predeterminado es 3306 . NOTA Puede ver la dirección IP privada en el área Network Information del Basic Information .
<database_name>	Nombre de la base de datos utilizada para conectarse a la instancia. El valor predeterminado es mysql .

Ejemplo de código (código Java para conectarse a una instancia de TaurusDB):

```

import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.ResultSet;
import java.sql.Statement;

public class MyConnTest {
    final public static void main(String[] args) {
        Connection conn = null;
        // set sslmode here.
        // no ssl certificate, so do not specify path.
        String url = "jdbc:mysql://192.168.0.225:3306/my_db_test?useSSL=false";
        try {
            Class.forName("com.mysql.jdbc.Driver");
            conn = DriverManager.getConnection(url, "root", "password");
        }
    }
}

```

```
        System.out.println("Database connected");

        Statement stmt = conn.createStatement();
        ResultSet rs = stmt.executeQuery("SELECT * FROM mytable WHERE
columnfoo = 500");
        while (rs.next()) {
            System.out.println(rs.getString(1));
        }
        rs.close();
        stmt.close();
        conn.close();
    } catch (Exception e) {
        e.printStackTrace();
        System.out.println("Test failed");
    } finally {
        // release resource ....
    }
}
```

----Fin

Problemas relacionados

- Síntoma

Cuando utiliza JDK 8.0 o una versión posterior para conectarse a su instancia con un certificado SSL descargado, se notifica un error similar al siguiente:

```
javax.net.ssl.SSLHandshakeException: No appropriate protocol (protocol is
disabled or
cipher suites are inappropriate)
    at sun.security.ssl.HandshakeContext.<init>(HandshakeContext.java:171)
~[na:1.8.0_292]
    at
sun.security.ssl.ClientHandshakeContext.<init>(ClientHandshakeContext.java:98)
~
[na:1.8.0_292]
    at sun.security.ssl.TransportContext.kickstart(TransportContext.java:220)
~
[na:1.8.0_292]
    at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:428) ~
[na:1.8.0_292]
    at
com.mysql.cj.protocol.ExportControlled.performTlsHandshake(ExportControlled.ja
va:316) ~
[mysql-connector-java-8.0.17.jar:8.0.17]
    at
com.mysql.cj.protocol.StandardSocketFactory.performTlsHandshake(StandardSocket
Factory.java
:188) ~[mysql-connector-java8.0.17.jar:8.0.17]
    at
com.mysql.cj.protocol.a.NativeSocketConnection.performTlsHandshake(NativeSocke
tConnection.
java:99) ~[mysql-connector-java8.0.17.jar:8.0.17]
    at
com.mysql.cj.protocol.a.NativeProtocol.negotiateSSLConnection(NativeProtocol.j
ava:331) ~
[mysql-connector-java8.0.17.jar:8.0.17]
... 68 common frames omitted
```

- Solución

Especifique los valores de parámetro correspondientes en el enlace de código de [Paso 3](#) en función del paquete JAR utilizado por el cliente. Ejemplo:

– `mysql-connector-java-5.1.xx.jar`

```
jdbc:mysql://<instance_ip>:<instance_port>/<database_name>?
```

```
requireSSL=true&useSSL=true&verifyServerCertificate=true&trustCertificate
```

```
KeyStoreUrl=file:  
<truststore_file>&trustCertificateKeyStorePassword=<password>&  
enabledTLSProtocols=TLSv1.2
```

– mysql-connector-java-8.0.xx.jar

```
jdbc:mysql://<instance_ip>:<instance_port>/<database_name>?  
  
requireSSL=true&useSSL=true&verifyServerCertificate=true&trustCertificate  
KeyStoreUrl=file:  
<truststore_file>&trustCertificateKeyStorePassword=<password>&  
tlsVersions =TLSv1.2
```

2.7 ¿Cómo puedo crear y conectarme a un ECS?

1. Para obtener más información acerca de cómo crear un TaurusDB, consulte *Guía de usuario de Elastic Cloud Server*.
 - El TaurusDB a crear debe estar en la misma VPC con la instancia TaurusDB a la que se conecta.
 - Configure un grupo de seguridad para permitir que el TaurusDB acceda a la instancia a través de la dirección IP.
2. Para obtener más información sobre cómo conectarse a la TaurusDB, consulte la sección "Iniciar sesión en una TaurusDB" en la *Guía de usuario de Elastic Cloud Server*.

2.8 ¿Qué debo hacer si un cliente de una base de datos ocasiona una falla de conexión?

Compruebe los siguientes elementos para solucionar problemas de conexión a TaurusDB causados por un problema de cliente:

1. Política de seguridad de TaurusDB
En Windows, compruebe si el puerto de instancia TaurusDB está habilitado en la política de seguridad de Windows. En Linux, ejecute **iptables** para comprobar si el puerto de instancia TaurusDB está habilitado en la configuración del firewall.
2. Configuración de la aplicación
Compruebe si la dirección de conexión, la configuración del parámetro de puerto y la configuración del parámetro de conexión JDBC son correctas.
3. Nombre de usuario o contraseña
Compruebe si el nombre de usuario o la contraseña son correctos si se produce un error similar al siguiente durante la conexión a la base de datos:
 - [Warning] Access denied for user 'username'@'yourIp' (using password: NO)
 - [Warning] Access denied for user 'username'@'yourIp' (using password: YES)

NOTA

Si el problema persiste, póngase en contacto con el soporte técnico postventa.

2.9 ¿Por qué no puedo hacer ping a mi EIP después de vincularlo a una instancia de base de datos?

Localización de fallas

1. Compruebe las reglas del grupo de seguridad.
2. Compruebe las ACL de red.
3. Haga ping del ECS a la instancia en la misma región.

Solución

1. Compruebe las reglas del grupo de seguridad.
 - a. En la página **Instances**, haga clic en el nombre de la instancia para ir a la página **Basic Information**.
 - b. En el área **Network Information** de la página **Basic Information**, haga clic en el grupo de seguridad.
 - c. Compruebe si el grupo de seguridad NIC de ECS permite el tráfico ICMP entrante.

Tabla 2-7 Reglas de grupos de seguridad

Dirección	Tipo	Rango de protocolo/puerto	Dirección IP de origen
Inbound	IPv4	Any: Any	0.0.0.0/0 (todas las direcciones IP)
Inbound	IPv4	ICMP: Any	0.0.0.0/0 (todas las direcciones IP)

2. Compruebe las ACL de red.
 - a. Compruebe el estado de la ACL de la red.
 - b. Compruebe si la NIC a la que el EIP enlazado pertenece a la subred asociada a la ACL de la red.
 - c. Si la ACL de red está habilitada, agregue una regla ICMP para permitir el tráfico.

NOTA

La regla ACL de red predeterminada deniega todos los paquetes entrantes y salientes. Después de deshabilitar la ACL de red, la regla predeterminada todavía tiene efecto.

3. Haga ping a la EIP afectado de otro ECS en la misma región.
Si la EIP afectado se puede hacer ping desde otro ECS en la misma región, la red virtual es funcional. En tal caso, póngase en contacto con el servicio de atención al cliente para obtener soporte técnico.

2.10 ¿Qué puedo hacer si falla la prueba de conexión?

Localización de fallas

1. Compruebe las reglas del grupo de seguridad.
2. Compruebe las ACL de red.
3. Compruebe la información de la NIC de los ECS.
4. Compruebe los puertos desconectados.

Solución

Paso 1 En la página **Instances**, haga clic en el nombre de la instancia para ir a la página **Basic Information**. En el área **Network Information** de la página, vea la VPC donde se encuentra la instancia.

Paso 2 Compruebe si la instancia a la que se agregan las transacciones distribuidas está en la misma VPC que un ECS.

- Si están en la misma VPC, consulte [¿Por qué falla la comunicación entre dos ECS en la misma VPC u ocurre una pérdida de paquetes cuando se comunican?](#)
- Si están en diferentes VPC:
 - Acceso público: Enlazar una EIP a la instancia. Para más detalles, consulte [Vinculación de una EIP](#).
 - Acceso privado: Cree una interconexión de VPC. Para obtener más información, consulte [Descripción de interconexión de VPC](#).
 - Cambie la VPC que aloja el ECS a la misma que la que aloja el TaurusDB. Para obtener más información, consulte [Cambiar una VPC](#).

----Fin

2.11 ¿Puedo acceder a una instancia de TaurusDB a través de una conexión de intranet en todas las regiones?

De forma predeterminada, no se puede acceder a las instancias a través de una intranet en todas las regiones. Los servicios en la nube de diferentes regiones no pueden comunicarse entre sí a través de una intranet. Puede utilizar Cloud Connect (CC) o Virtual Private Network (VPN) para conectarse a instancias de distintas regiones.

- CC le permite conectar dos VPC de la misma cuenta o cuentas diferentes, incluso si se encuentran en regiones diferentes. Para obtener más información, consulte [Comunicación entre las VPC de la misma cuenta](#).
- VPN utiliza un túnel cifrado para conectar VPCs en diferentes regiones y envía tráfico a través de Internet. Es barato, fácil de configurar y fácil de usar. Sin embargo, la calidad de las conexiones de VPN depende de la calidad de las conexiones a Internet. Para obtener más información, consulte [Conectar un centro de datos local a una VPC a través de una VPN](#).

2.12 ¿Existen riesgos potenciales si hay demasiadas conexiones a una instancia de TaurusDB?

Si hay un número excesivo de conexiones de TaurusDB, es posible que las aplicaciones no se conecten y que las copias de respaldo completas e incrementales fallen, lo que afecta a los servicios.

Solución

1. Compruebe si las aplicaciones están conectadas, optimice las conexiones y libere conexiones innecesarias.
2. Cloud Eye supervisa las métricas de la base de datos, como el uso de la CPU, el uso de la memoria, el uso del espacio de almacenamiento y las conexiones a la base de datos, y le permite establecer políticas de alarmas para identificar riesgos potenciales si se generan alarmas.

2.13 ¿Qué debo hacer si un ECS y una instancia de TaurusDB desplegados en diferentes VPC no pueden comunicarse entre sí?

Cuando una instancia de TaurusDB y un ECS se despliegan en diferentes VPC de la misma región, no pueden comunicarse entre sí a través de una red privada. Después de crear una instancia de TaurusDB, no se puede cambiar su VPC.

Solución

1. Cree una interconexión de VPC. Para obtener más información, consulte [Descripción de interconexión de VPC](#).
2. Cambie la VPC que aloja el ECS a la misma que la que aloja el TaurusDB. Para obtener más información, consulte [Cambiar una VPC](#).

2.14 ¿Cómo puedo ver todas las direcciones IP conectadas a una base de datos?

Puede ejecutar la siguiente sentencia SQL en la base de datos para consultar el número de direcciones IP conectadas:

```
SELECT substring_index(host, ':',1) AS host_name,state,count(*) FROM  
information_schema.processlist GROUP BY state,host_name;
```

3 Instalación del cliente

3.1 ¿Cómo puedo instalar el cliente de MySQL?

MySQL proporciona paquetes de instalación de cliente para diferentes sistemas operativos en su sitio web oficial. Descargue el [paquete de instalación del cliente MySQL 8.0](#) o [paquetes de otras versiones](#). Lo siguiente usa Red Hat Linux como ejemplo para mostrar cómo obtener el paquete de instalación requerido e instalarlo.

Procedimiento

Paso 1 Obtenga el paquete de instalación.

Encuentre el [enlace](#) a la versión requerida en la página de descarga. El `mysql-community-client-8.0.21-1.el6.x86_64` se usa como ejemplo.

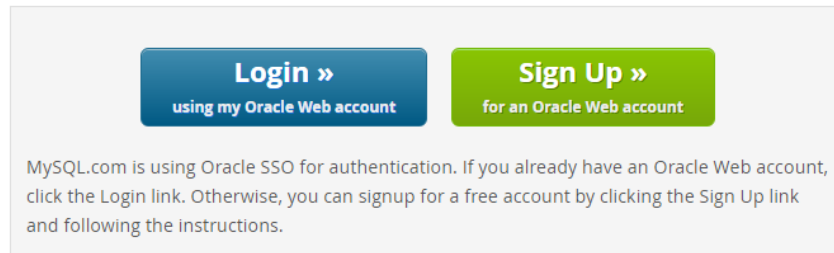
Figura 3-1 Descargar

MySQL Community Downloads

Login Now or Sign Up for a free account.

An Oracle Web Account provides you with the following advantages:

- Fast access to MySQL software downloads
- Download technical White Papers and Presentations
- Post messages in the MySQL Discussion Forums
- Report and track bugs in the MySQL bug system



No thanks, just start my download.

NOTA

Haga clic en **No thanks, just start my download.** para descargar el paquete de instalación.

Paso 2 Cargue el paquete de instalación a TaurusDB.

NOTA

Cuando cree una TaurusDB, seleccione un sistema operativo, como Red Hat 6.6, y enlace una EIP a él. A continuación, cargue el paquete de instalación en TaurusDB mediante una herramienta de conexión remota y use PuTTY para conectarse a TaurusDB.

Paso 3 Ejecute el siguiente comando para instalar el cliente de MySQL:

```
sudo rpm -ivh mysql-community-client-8.0.21-1.el6.x86_64.rpm
```

NOTA

- Si se producen conflictos durante la instalación, agregue el parámetro **replacefiles** al comando e intente instalar de nuevo el cliente. Ejemplo:

```
rpm -ivh --replacefiles mysql-community-client-8.0.21-1.el6.x86_64.rpm
```
- Si aparece un mensaje solicitando que instale un paquete de dependencias, puede agregar el parámetro **nodeps** al comando e instalar de nuevo el cliente. Ejemplo:

```
rpm -ivh --nodeps mysql-community-client-8.0.21-1.el6.x86_64.rpm
```

Paso 4 Utilice el cliente MySQL para conectarse a la base de datos y comprobar si el cliente puede ejecutarse correctamente.

```
mysql -h <hostIP> -P <port> -u <userName> -p --ssl-ca=<cafile>
```

Tabla 3-1 Descripción de parámetro

Parámetro	Descripción
<hostIP>	Dirección IP privada. Para obtener este parámetro, vaya a la página Basic Information de la instancia y vea la dirección IP privada en el área Network Information .
<port>	Puerto de base de datos. De forma predeterminada, el valor es 3306 . Para obtener este parámetro, vaya a la página Basic Information de la instancia y vea el puerto de la base de datos en el área Network Information .
<userName>	Nombre de usuario de la cuenta de administrador de base de datos de TaurusDB. El nombre de usuario predeterminado es root .
<cafile>	Archivo de certificado SSL, que debe almacenarse en el mismo directorio donde se ejecuta el comando.

Ejemplo:

Para conectarse a una instancia de base de datos a través de una conexión SSL como usuario **root**, ejecute el siguiente comando:

```
mysql -h 172.xx.xx.xx -P 3306 -u root -p --ssl-ca=ca.pem
```

Introduzca la contraseña de la cuenta de la base de datos como se le solicite.

Enter password:

NOTA

Si se muestra la información de error similar a "mysql: error while loading shared libraries: libxxx: cannot open shared object file: No such file or directory", realice los siguientes pasos:

Por ejemplo, si se muestra el error "mysql: error while loading shared libraries: libtinfo.so.5: cannot open shared object file: No such file or directory",

1. Consulte el archivo de versión actual de la biblioteca dinámica que informa del error en el host local.

```
find / -name libtinfo.so*
```

Supongamos que el resultado de la consulta es el siguiente:

```
/usr/lib64/libtinfo.so.6.2
```

```
/usr/lib64/libtinfo.so.6
```

2. Configure el enlace suave de la versión requerida.

```
ln -s /usr/lib64/libtinfo.so.6 /usr/lib64/libtinfo.so.5
```

3. Conéctese a la base de datos de nuevo.

```
mysql -h <hostIP> -P <port> -u <userName> -p --ssl-ca=<cafile>
```

----Fin

4 Migración de base de datos

4.1 ¿Qué tipos de motores de base de datos admite TaurusDB para importar datos?

- La exportación o importación de datos entre motores de base de datos del mismo tipo se denomina exportación o importación de bases de datos homogéneas.
- La exportación o importación de datos entre motores de base de datos de diferentes tipos se denomina exportación o importación de bases de datos heterogéneas. Por ejemplo, importe datos de Oracle a los motores de base de datos compatibles con TaurusDB.

Generalmente, los datos no se pueden exportar o importar entre bases de datos heterogéneas debido a los diferentes formatos de datos involucrados. Sin embargo, si los formatos de datos son compatibles, los datos de tabla pueden, en teoría, migrarse entre ellos.

Generalmente se requiere software de terceros para la replicación de datos para exportar e importar entre bases de datos heterogéneas. Por ejemplo, puede utilizar una herramienta de terceros para exportar registros de tabla desde el formato Oracle in.txt. A continuación, puede usar las sentencias Load para importar los registros de tabla exportados a los motores de base de datos soportados por TaurusDB.

5 Permisos de base de datos

5.1 ¿Proporciona TaurusDB la cuenta raíz o súper permiso?

TaurusDB proporciona al usuario administrador **root** que tiene los permisos excepto super, file, shutdown, y create tablespace.

La mayoría de las plataformas de servicios de base de datos en la nube no proporcionan el super permiso para el usuario **root**. Los super permisos permiten a los usuarios ejecutar muchos comandos de gestión, como reset master, set global, kill, y reset slave. Estas operaciones pueden causar excepciones y fallas impredecibles para TaurusDB. Esta es una diferencia importante entre las bases de datos en la nube y las bases de datos MySQL locales. Para garantizar un funcionamiento estable de las instancias, TaurusDB no proporciona el permiso super para el usuario **root**.

Si necesita realizar acciones que normalmente requieren super permisos, TaurusDB proporciona métodos alternativos.

Por ejemplo:

Puede modificar los valores de parámetros solo en la consola TaurusDB. No puede ejecutar el siguiente comando en una base de datos para modificar los valores de los parámetros.

set global parameter name=*Parameter value*;

Si el script contiene el comando **set global**, elimine el comando **set global** y modifique los valores de los parámetros de la consola.

Se informa de un error después de ejecutar el siguiente comando porque el usuario **root** no tiene super permisos. Puede eliminar **definer='root'** desde el comando.

create definer='root'@'%' trigger(procedure)...

Puede importar y exportar datos usando mysqldump. Para obtener más información, consulte Migración de datos a TaurusDB usando mysqldump.

6 Rendimiento de bases de datos

6.1 ¿Qué debo hacer si el uso de la CPU de mi instancia es alto?

Si el uso de CPU es alto o cercano al 100% cuando se utiliza TaurusDB, el procesamiento de lectura/escritura de datos se ralentiza, no se pueden establecer conexiones y se informan errores, interrumpiendo los servicios.

Solución

1. Compruebe los registros SQL lentos en busca de consultas lentas y examine sus características de rendimiento (si las hay) para localizar la causa.
Para obtener más información sobre cómo ver los registros de MySQL, consulte Consulta de registros de consultas lentas.
2. Vea el uso de la CPU de su instancia TaurusDB para facilitar la localización de problemas.
Para obtener más información, consulte Configuración de métricas mostradas.
3. Cree réplicas de lectura para descargar la presión de lectura del nodo principal.
4. Agregue índices para campos asociados en consultas de asociación de varias tablas.
5. No utilice la sentencia SELECT para analizar todas las tablas. Puede especificar campos o agregar la condición WHERE.

6.2 ¿Cómo manejo las sentencias SQL lentas causadas por configuraciones de índice compuesto inadecuadas?

Escenario

En su instancia, una consulta SQL que se ejecutaba a las 11:00 y se esperaba que durara 8 segundos tomó más de 30 segundos.

Causas posibles

1. Compruebe el uso de la CPU. En este ejemplo, durante ese período de tiempo, el uso de la CPU de la instancia no aumentó bruscamente y se mantuvo bajo, por lo que sabemos que la consulta lenta no fue causada por un uso alto de la CPU.

Figura 6-1 Uso de CPU



2. Analizar los registros de consultas lentas generados durante ese período. En este ejemplo, que se muestra a continuación, había varias sentencias SQL que involucraban millones de filas que se analizaban. Estas fueron las sentencias lentas. Pero no se insertó una gran cantidad de datos en la tabla durante ese tiempo, por lo que sabemos que la ejecución lenta fue causada por la falta de configuración de índice o incorrecta. Al ejecutar **EXPLAIN**, se puede encontrar que el plan de ejecución de la sentencia SQL era un análisis de tabla completo.

Figura 6-2 Registros de consultas lentas

select query_date, sum(queue) queue, sum(server_user_num) serverUserNum, su...	SELECT	1	6.027128 s	0.000105	125	2119000
select query_date, sum(queue) queue, sum(server_user_num) serverUserNum, su...	SELECT	1	5.479857 s	0.000104	123	2085096
select query_date, sum(queue) queue, sum(server_user_num) serverUserNum, su...	SELECT	1	5.288656 s	0.000106	123	2085096
select query_date, sum(queue) queue, sum(server_user_num) serverUserNum, su...	SELECT	1	33.601792 s	0.000064	140	16961077
select query_date, sum(queue) queue, sum(server_user_num) serverUserNum, su...	SELECT	1	34.342761 s	0.000171	140	16961077
select query_date, sum(queue) queue, sum(server_user_num) serverUserNum, su...	SELECT	1	44.536072 s	0.000167	140	16961077
select query_date, sum(queue) queue, sum(server_user_num) serverUserNum, su...	SELECT	1	46.501796 s	0.000095	140	16961077
select query_date, sum(queue) queue, sum(server_user_num) serverUserNum, su...	SELECT	1	33.050387 s	0.000099	139	16944097
select query_date, sum(queue) queue, sum(server_user_num) serverUserNum, su...	SELECT	1	38.523306 s	0.000101	139	16944097
select query_date, sum(queue) queue, sum(server_user_num) serverUserNum, su...	SELECT	1	40.108127 s	0.000090	139	16944097

3. Realice **SHOW INDEX FROM** en la tabla de la instancia para comprobar la cardinalidad de las tres columnas.

Figura 6-3 Cardinalidad del índice

```
***** 3. row *****
Table: [redacted]
Non_unique: 1
Key_name: idx_query_date_channel_group_id
Seq_in_index: 1
Column_name: query_date
Collation: A
Cardinality: 133994
Sub_part: NULL
Packed: NULL
Null: YES
Index_type: BTREE
Comment:
Index_comment:
***** 4. row *****
Table: [redacted]
Non_unique: 1
Key_name: idx_query_date_channel_group_id
Seq_in_index: 2
Column_name: channel
Collation: A
Cardinality: 405333
Sub_part: NULL
Packed: NULL
Null: YES
Index_type: BTREE
Comment:
Index_comment:
***** 5. row *****
Table: [redacted]
Non_unique: 1
Key_name: idx_query_date_channel_group_id
Seq_in_index: 3
Column_name: group_id
Collation: A
Cardinality: 16213328
Sub_part: NULL
Packed: NULL
Null: YES
Index_type: BTREE
```

El campo **query_date** con menor cardinalidad estaba en el primer lugar del índice compuesto, y el campo **group_id** con mayor cardinalidad estaba en el último lugar del índice compuesto. Además, la sentencia SQL contenía la consulta de rango del campo **query_date**. Como resultado, solo se indexó el campo **query_date**.

La sentencia SQL solo puede utilizar el índice de la columna **query_date**.

Adicionalmente, el optimizador puede haber seleccionado la exploración de tabla completa durante la estimación de costes debido a que la cardinalidad era demasiado pequeña.

Se creó un nuevo índice compuesto con el campo **group_id** en primer lugar y el campo **query_date** en último lugar. El tiempo de consulta cumplió con las expectativas.

Solución

1. Compruebe si la consulta lenta fue causada por recursos de CPU insuficientes.
2. Compruebe si la estructura de la tabla está diseñada correctamente y si la configuración del índice es correcta.
3. Ejecute la sentencia **ANALYZE TABLE** periódicamente para evitar planes de ejecución incorrectos, ya que realizar un gran número de operaciones **INSERT** o **DELETE** para los datos de la tabla puede resultar en estadísticas desactualizadas.

2. Optimice las sentencias SQL lentas según sea necesario.

6.4 ¿Qué debo hacer si los bloqueos en transacciones largas bloquean la ejecución de transacciones posteriores?

Escenario

Se informó del código de error 1205:

"MySQL error code MY-001205 (ER_LOCK_WAIT_TIMEOUT): **Lock wait timeout exceeded**; try restarting transaction"

Causas posibles

1. Compruebe el valor del **Row Lock Time** de la métrica de monitorización. En este ejemplo, el valor de esta métrica era alto, por lo que sabemos que hubo conflictos de bloqueo en el sistema.

Para obtener más información sobre las métricas de monitoreo, consulte Consulta de métricas de monitoreo de instancias.



2. Inicie sesión en la instancia de base de datos y ejecute la siguiente sentencia SQL para comprobar las transacciones largas en el sistema y los bloqueos de fila que mantienen las transacciones:

```
select trx_mysql_thread_id, trx_id, trx_state, trx_started,
trx_tables_locked, trx_rows_locked, trx_isolation_level, trx_query,
trx_operation_state from information_schema.innodb_trx order by trx_started;
```

```
mysql> select trx_mysql_thread_id, trx_id, trx_state, trx_started, trx_tables_locked, trx_rows_locked, trx_isolation_level, trx_query, trx_operation_state from information_schema.innodb_trx order by trx_started;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| trx_mysql_thread_id | trx_id | trx_state | trx_started | trx_tables_locked | trx_rows_locked | trx_isolation_level | trx_query | trx_operation_state |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 416 | 51965 | RUNNING | 2022-07-28 19:27:55 | 1 | 1 | READ COMMITTED | NULL | NULL |
| 415 | 51967 | LOCK WAIT | 2022-07-29 00:11:03 | 1 | 2 | READ COMMITTED | [REDACTED] | fetching rows |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

- **information_schema.innodb_trx**: información sobre las transacciones que se están ejecutando en InnoDB.
- **trx_started**: hora de inicio de una transacción, que se utiliza para determinar si la transacción actual es una transacción larga. El tiempo de ejecución de una transacción es el tiempo actual menos el tiempo de inicio.
- **trx_state**: Estado de la transacción actual. Los valores son los siguientes:
 - **RUNNING**

- **LOCK WAIT**

- 📖 **NOTA**

- Si el estado de una transacción es de **LOCK WAIT**, la transacción mantiene un bloqueo de fila.

- **ROLLING BACK**
- **COMMITTING**

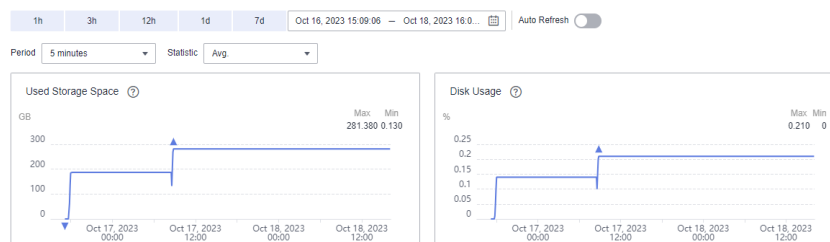
Solución

Elimine las transacciones largas.

6.5 ¿Cómo puedo usar el disco temporal de TaurusDB?

Los discos temporales de instancias de TaurusDB se utilizan para almacenar temporalmente tablas temporales, archivos temporales y cachés binlog generados durante el funcionamiento de la base de datos. En la consola de gestión, puede supervisar el espacio en disco temporal usado y el uso de disco temporal de la instancia en diferentes períodos de tiempo y granularidades en tiempo real, como se muestra en la siguiente figura.

Figura 6-6 Uso temporal del disco



Con la fluctuación de los servicios, puede encontrar que el uso de discos temporales aumenta repentinamente o continuamente. Para mejorar la disponibilidad y estabilidad de la base de datos, TaurusDB proporciona hasta 500 GB de espacio temporal en disco para una instancia de base de datos. El espacio temporal en disco es gratuito.

Para evitar que el uso temporal del disco aumente continuamente y alcance el límite superior, se recomienda comprobar los servicios lo antes posible en función del uso del disco consultado. En esta sección se describen los riesgos, los escenarios y la solución de problemas cuando los discos temporales están llenos.

Riesgos

- Las sentencias SQL no se pueden ejecutar y no se devuelven resultados.
- Las sentencias SQL ocupan recursos de bloqueo durante mucho tiempo y bloquean otras sentencias SQL. Como resultado, el número de conexiones aumenta o incluso alcanza el límite superior, afectando a otros servicios.
- El número de archivos temporales en la caché de binlog alcanza el límite superior. La base de datos se descompone y tarda mucho tiempo en restaurarse, por lo que los servicios se interrumpen durante mucho tiempo.

Escenarios y solución de problemas

1. Creación explícita de tablas de disco temporales

– Escenario

Ejecute la sentencia **create temporary table** para crear explícitamente tablas de disco temporales. Las tablas temporales cuyo motor de almacenamiento es InnoDB se almacenan en caché en el grupo de búferes y se vacían en los discos por subprocesos sucios.

En TaurusDB, los datos de las tablas temporales de disco se almacenan en el espacio temporal de sesión (la ruta se especifica mediante el parámetro **innodb_temp_tablespaces_dir**), y los registros de deshacer se almacenan en el espacio temporal global (la ruta se especifica mediante el parámetro **innodb_temp_data_file_path**).

Para evitar que las tablas de disco temporales ocupen demasiado espacio en disco, se recomienda eliminar las tablas de disco temporales innecesarias o desconectar las conexiones de base de datos innecesarias.

AVISO

- Espacio de tabla temporal de sesión: Se recupera cuando se libera la conexión de base de datos actual.
- Espacio de tabla temporal global: solo se recupera después de reiniciar la base de datos.

– Resolución de problemas

i. Vea información sobre las tablas temporales que creó en InnoDB.

```
mysql> select * from information_schema.innodb_temp_table_info;
+-----+-----+-----+-----+
| TABLE_ID          | NAME                | N_COLS | SPACE          |
+-----+-----+-----+-----+
| 18446744069414584311 | #sql055_24_0       | 5      | 4294502266    |
+-----+-----+-----+-----+
```

ii. Compruebe el uso de los archivos de tablas temporales de InnoDB.

En una tabla, la columna **ID** indica el ID de la sesión que está utilizando el archivo de tabla temporal. Si el valor es **0**, no se utiliza el archivo ibt. La columna **SIZE** indica el tamaño del archivo ibt, que aumenta automáticamente en función del uso y se recupera cuando finaliza la sesión. Si el valor de la columna **PURPOSE** es **INTRINSIC**, la tabla es una tabla temporal implícita. Si el valor de la columna **PURPOSE** es **USER**, la tabla es una tabla temporal explícita.

```
mysql> select * from
information_schema.innodb_session_temp_tablespaces;
+----+-----+-----+-----+-----+
| ID | SPACE          | PATH                                | SIZE | STATE |
PURPOSE |
+----+-----+-----+-----+-----+
| 31 | 4294502265    | ./#innodb_temp/temp_9.ibt         | 81920 | ACTIVE |
INTRINSIC |
| 36 | 4294502266    | ./#innodb_temp/temp_10.ibt        | 98304 | ACTIVE |
USER |
| 34 | 4294502264    | ./#innodb_temp/temp_8.ibt         | 81920 | ACTIVE |
INTRINSIC |
```

```

| 0 | 4294502257 | ./#innodb_temp/temp_1.ibt | 81920 | INACTIVE |
NONE |
| 0 | 4294502258 | ./#innodb_temp/temp_2.ibt | 81920 | INACTIVE |
NONE |
| 0 | 4294502259 | ./#innodb_temp/temp_3.ibt | 81920 | INACTIVE |
NONE |
| 0 | 4294502260 | ./#innodb_temp/temp_4.ibt | 81920 | INACTIVE |
NONE |
| 0 | 4294502261 | ./#innodb_temp/temp_5.ibt | 81920 | INACTIVE |
NONE |
| 0 | 4294502262 | ./#innodb_temp/temp_6.ibt | 81920 | INACTIVE |
NONE |
| 0 | 4294502263 | ./#innodb_temp/temp_7.ibt | 81920 | INACTIVE |
NONE |
+-----+-----+-----+-----+-----+
+-----+

```

2. Consulta de tablas temporales de disco o archivos temporales creados implícitamente

– Escenario

Cuando se selecciona un plan de ejecución para una consulta, el optimizador de consultas puede usar tablas temporales. Se usan preferentemente tablas de memoria temporal. Cuando el tamaño de las tablas de memoria temporal excede el umbral (dependiendo del valor menor entre **tmp_table_size** y **max_heap_table_size**), se utilizan tablas de disco temporales.

Las tablas temporales de disco son creadas implícitamente por consultas. Los datos entre las tablas que se crean implícita y explícitamente son los mismos y se almacenan en el espacio temporal de sesión. Si hay consultas complejas, incluidas, entre otras, palabras clave como UNION, GROUP BY y ORDER BY, en tablas más grandes, se pueden generar tablas de disco temporales. Además, cuando las consultas implican operaciones de ordenación, si el búfer de ordenación no puede almacenar todos los datos (el tamaño del búfer es especificado por **sort_buffer_size**), se pueden utilizar archivos de disco temporales para la ordenación auxiliar. En la mayoría de los escenarios, las tablas de disco temporales creadas implícitamente son la causa principal del espacio total en disco. Puede localizar consultas complejas o transacciones largas, optimizar sentencia de consulta, agregar índices adecuados y dividir transacciones largas para resolver estos problemas.

– Resolución de problemas

- i. Compruebe si hay sentencias SQL que utilizan tablas temporales o clasificación de archivos.

Si se muestra **Using temporary** en la columna **Extra**, se utilizan tablas temporales. Si se muestra **Using filesort**, se utiliza la clasificación de archivos.

```

mysql> explain {SQL};
+-----+-----+-----+-----+-----+-----+
| id | select_type | table | type | possible_keys | ... | Extra |
+-----+-----+-----+-----+-----+-----+
| 1 | SIMPLE | p | index | PRIMARY,org_contact_fk | ... | Using index; Using temporary; Using filesort |
| 1 | SIMPLE | c1 | eq_ref | PRIMARY | ... | |
| 1 | SIMPLE | t2p | ref | idx_publisher_id | ... | Using where |
| 1 | SIMPLE | t | eq_ref | PRIMARY,active_index | ... | Using where |
| ..... |
+-----+-----+-----+-----+-----+-----+

```

- ii. Consultar el uso de tablas temporales implícitas. El método es el mismo que las tablas temporales explícitas del disco.

3. Consulta de registros binarios generados para transacciones largas

– Escenario

Binlog es un archivo binario que registra los cambios en la base de datos, como DDL, DCL y DML (excluido SELECT). InnoDB almacena en caché los binlogs en

la memoria antes de que se realice una transacción y escribe binlogs en los discos solo después de que se realice la transacción. El tamaño del archivo binlog para cada conexión en la memoria se especifica mediante el parámetro **binlog_cache_size**. Cuando el tamaño del archivo binlog registrado por una transacción excede el valor de este parámetro, el archivo binlog se escribe en un archivo de disco temporal. Las transacciones largas pueden causar grandes binlogs. Como resultado, el tamaño de los binlogs temporales en el disco es grande y el disco puede estar lleno. Se recomienda controlar el tamaño de la transacción, separar transacciones largas o cambiar correctamente el valor de **binlog_cache_size**.

– Resolución de problemas

i. Compruebe si binlog está habilitado.

```
mysql> show variables like 'log_bin';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| log_bin       | ON    |
+-----+-----+
```

ii. Vea el uso de la caché de binlog.

Binlog_cache_disk_use indica el número de veces que los archivos temporales de disco se utilizan para almacenar en caché binlogs debido a la falta de memoria (especificada por **binlog_cache_size**). Si el valor de **binlog_cache_size** es grande, se invocan los archivos de disco temporales para almacenar en caché binlogs varias veces.

```
mysql> show global status like '%binlog_cache%';
+-----+-----+
| Variable_name          | Value      |
+-----+-----+
| Binlog_cache_disk_use | 1335006    |
| Binlog_cache_use      | 264240359 |
+-----+-----+
```

4. Comprobación de archivos temporales generados por DDL

– Escenario

Durante las operaciones DDL en tablas, los archivos de disco temporales se generan en algunas fases.

- A veces, es necesario volver a crear el espacio de tablas de la tabla original, lo que implica la recreación del índice de árbol B+ en la tabla. Si una tabla contiene una gran cantidad de datos, el búfer de ordenación no puede almacenar todos los datos. Es necesario crear un archivo temporal para ayudar a ordenar.
- Aunque algunas sentencias DDL en línea admiten operaciones DML en la tabla original, la tabla original no se puede modificar directamente. La modificación debe registrarse en registros en línea y aplicarse a la nueva tabla una vez completadas las operaciones de DDL. Los registros en línea se almacenan preferentemente en la memoria. El tamaño de los registros en línea se especifica mediante el parámetro **innodb_sort_buffer_size**. Si el tamaño de los registros en línea excede el valor del parámetro, los registros en línea se almacenan temporalmente en un archivo temporal.
- Cuando la sentencia **OPTIMIZE TABLE** se ejecuta en una tabla, los datos almacenados en el índice agrupado necesitan ser reorganizados, lo que puede generar archivos temporales.

– Resolución de problemas

- Ejecute el comando **SHOW PROCESSLIST** para comprobar si hay sentencias DDL que se han ejecutado durante mucho tiempo.
- Asegúrese de que hay suficiente espacio antes de realizar DDL para tablas grandes.

7

Uso de base de datos

7.1 ¿Por qué los resultados son incoherentes después de que la sentencia MATCH AGAINST se ejecuta, respectivamente, en nodos primarios y réplicas de lectura?

MATCH AGAINST se utiliza para buscar índices de texto completo de MySQL. Para las filas de la tabla, MATCH devuelve valores de relevancia, es decir, una medida de similitud entre la cadena de búsqueda (dada como argumento a la función AGAINST()) y el texto de esa fila en las columnas nombradas en la lista MATCH(). Esta sentencia utiliza el valor `stat_n_rows` para calcular el valor de relevancia. Los nodos primarios y las réplicas de lectura utilizan diferentes métodos para obtener el valor `stat_n_rows`. Los nodos primarios usan el método persistente y las réplicas de lectura usan el método transitorio. Por lo tanto, los valores obtenidos son ligeramente diferentes entre sí. El resultado de la ejecución de MATCH AGAINST en nodos primarios y réplicas de lectura es diferente.

7.2 ¿Cómo agrego columnas usando INSTANT?

TaurusDB es compatible con MySQL 8.0.22 de código abierto, por lo que puede usar `ALGORITHM=INSTANT` para agregar rápidamente columnas, evitando que el bloqueo de espera afecte los servicios o el tiempo de espera de ejecución de la sentencia SQL.

Restricciones

- Las columnas solo se pueden agregar en una sentencia. Si hay otras operaciones no instantáneas en la misma sentencia, las columnas no se pueden agregar inmediatamente.
- Las columnas solo se pueden agregar al final de las columnas existentes.
- No se admite el formato de fila COMPRESSED.
- Las tablas que ya tienen índices de texto completo no son compatibles.

NOTA


Si una tabla tiene un índice de texto completo, debe ejecutar la sentencia OPTIMIZE TABLE en la tabla después de eliminar el índice de texto completo.


- No se admiten tablas temporales.

- Un campo nuevo no puede tener un valor predeterminado.

Procedimiento

Paso 1 [Log in to the management console.](#)

Paso 2 Click  in the upper left corner and select a region and a project.

Paso 3 Haga clic en  en la esquina superior izquierda de la página y elija **Databases > TaurusDB**.

Paso 4 En la página **Instances**, busque la instancia y haga clic en **Log In** en la columna **Operation**.

Como alternativa, en la página **Instances**, haga clic en el nombre de la instancia para ir a la página **Basic Information**. Haga clic en **Log In** en la esquina superior derecha de la página.

Paso 5 En la página de inicio de sesión mostrada, ingrese el nombre de usuario y la contraseña correctos y haga clic en **Log In**.

Paso 6 En la barra de menú superior, elija **SQL Operations > SQL Query**.

Paso 7 Ejecute la siguiente sentencia SQL para agregar rápidamente una columna:

```
ALTER TABLE table_name ADD COLUMN column_name column_definition,  
ALGORITHM=INSTANT;
```

- *table_name*: nombre de tabla
- *column_name*: nombre de columna
- *column_definition*: comentarios de columna

----Fin

7.3 ¿Cómo uso LOAD DATA para importar datos locales?

Puede usar LOAD DATA para importar datos locales a TaurusDB.

Sintaxis

```
LOAD DATA LOCAL  
  INFILE 'file_name'  
  [REPLACE | IGNORE]  
  INTO TABLE tbl_name  
  [CHARACTER SET charset_name]  
  [{FIELDS | COLUMNS}  
   [TERMINATED BY 'string']  
   [[OPTIONALLY] ENCLOSED BY 'char']  
  ]  
  [LINES  
   [TERMINATED BY 'string']  
  ]  
  [IGNORE number {LINES | ROWS}]  
  [(col_name_or_user_var  
   [, col_name_or_user_var] ...)]
```

Parámetros

- **file_name**: ruta del archivo local que se va a importar.

- **REPLACE | IGNORE**: si se deben reemplazar o ignorar registros duplicados.
- **tbl_name**: nombre de la tabla que se va a importar.
- **CHARACTER SET charset_name**: formato de codificación de archivo. Se recomienda utilizar el formato de codificación de las instancias de TaurusDB para evitar caracteres confusos.
- **FIELDS TERMINATED BY 'string'**: separador entre columnas. El valor predeterminado es `\t`.
- **[OPTIONALLY] ENCLOSED BY 'char'**: se utiliza para omitir símbolos en campos de origen de datos.
- **LINES TERMINATED BY 'string'?**: carácter de nueva línea entre líneas. El valor predeterminado es `\n`.

NOTA

En algunos hosts que ejecutan Windows servers, los caracteres de nueva línea de los archivos de texto pueden ser `\r\n`, que es invisible.

- **IGNORE number LINES**: se utiliza para ignorar las líneas al inicio del archivo.
- **(column_name_or_user_var, ...)**: columnas que se van a importar. Si este parámetro no está configurado, los datos se importan según la secuencia de columnas de forma predeterminada.
- Para otros parámetros, consulte el [archivo de carga de datos](#) en el sitio web oficial de MySQL. La secuencia de otros parámetros debe ser correcta. Para obtener detalles de la secuencia, visite [el sitio web oficial de MySQL](#).

Ejemplo estándar

Prerrequisitos

- El parámetro **local_infile** debe estar habilitado en el servidor. Haga clic en el nombre de la instancia para ir a la página **Basic Information**. En la página **Parameters**, cambie el valor de este parámetro a **ON**.
- El parámetro **local-infile** debe estar habilitado en el cliente. Configure **local-infile** en el archivo **my.cnf** o utilice la opción **--local-infile=1** para conectarse a la base de datos.

```
[mysql]
local-infile
```

1. Importe los datos del archivo local **qq.txt** a la tabla **test**. El archivo **qq.txt** contiene cinco filas de datos. El separador de columna es de `,` y el separador de fila es de `\n`.

```
1,a
2,b
3,c
4,d
5,"e"
```

2. Cree la tabla **test**.

```
CREATE TABLE test (
  `id` int NOT NULL,
  `a` varchar(4) NOT NULL,
  PRIMARY KEY (`id`)
);
```

3. En el cliente, ejecute la sentencia **LOAD DATA** para importar datos del archivo **qq.txt** a la tabla **test** y establezca el conjunto de caracteres en **utf8** e ignore las comillas dobles del campo de origen de datos.

```
mysql> LOAD DATA LOCAL INFILE '/data/qq.txt' IGNORE INTO TABLE test CHARACTER
SET 'utf8' FIELDS TERMINATED BY ',' OPTIONALLY ENCLOSED BY '"' LINES
TERMINATED BY '\n';
```

```
Query OK, 5 rows affected, 1 warning (0.00 sec)
Records: 5 Deleted: 0 Skipped: 0 Warnings: 1

mysql> select * from test;
+----+----+
| id | a |
+----+----+
| 1 | a |
| 2 | b |
| 3 | c |
| 4 | d |
| 5 | e |
+----+----+
5 rows in set (0.00 sec)
```

AVISO

1. La importación de datos afecta al rendimiento de las instancias de TaurusDB. Importación de datos durante horas fuera de pico.
 2. No inicie varias solicitudes de LOAD DATA al mismo tiempo. Cuando se inician varias solicitudes de LOAD DATA, las transacciones SQL pueden expirar debido a operaciones de escritura de datos altamente simultáneas, bloqueo de tabla y ocupación de E/S del sistema, lo que resulta en una falla de todas las solicitudes de LOAD DATA.
-

8 Copias de respaldo

8.1 ¿Durante cuánto tiempo almacena TaurusDB los datos de copia de respaldo?

Los datos de copia de respaldo automatizados se guardan en función del período de retención de copia de respaldo especificado. Para obtener más información, consulte [Configuración de una política de copia de respaldo](#).

No hay límite para el período de retención de copias de respaldo manual. Para obtener más información, consulte [Eliminación de una copia de respaldo manual](#).

Los datos de copia de respaldo se almacenan en el TaurusDB y no ocupan el espacio de almacenamiento de la base de datos.

8.2 ¿Cómo puedo borrar el espacio de copia de respaldo de TaurusDB?

El espacio de copia de respaldo de TaurusDB almacena copias de respaldo automatizadas y copias de respaldo manuales.

- **Copias de respaldo completas e incrementales automatizadas**

Los archivos de copia de respaldo automatizados no se pueden eliminar manualmente. Es necesario cambiar el ciclo de copia de respaldo haciendo referencia a [Configuración de una política de copia de respaldo automatizada](#). Se eliminarán los archivos de copia de respaldo que hayan caducado.

- **Copias de respaldo completas manuales**

Puede eliminar manualmente las copias de respaldo manuales. Para obtener más información, consulte [Eliminación de una copia de respaldo manual](#).

8.3 ¿Cómo puedo hacer una copia de respaldo de una base de datos de TaurusDB en un ECS?

Puede realizar una copia de respaldo de los datos en un TaurusDB del mismo modo que exporta sentencias SQL. El servicio TaurusDB no tiene restricciones sobre los tipos de datos que se van a realizar copias de respaldo siempre y cuando los datos cumplan con las leyes y regulaciones locales. Puede almacenar los datos de copia de respaldo en un TaurusDB.


Sin embargo, se recomienda utilizar TaurusDB copias de respaldo automatizadas y copias de respaldo manuales para hacer copias de respaldo de datos a TaurusDB en busca de una mayor confiabilidad de los datos y garantía de servicio.


8.4 ¿Cómo puedo ver mi uso de almacenamiento de copia de respaldo?

En el área **Storage/Backup Space** de la página **Basic Information** de la consola, puede ver el uso del espacio de copia de respaldo.

Procedimiento

Paso 1 [Log in to the management console.](#)

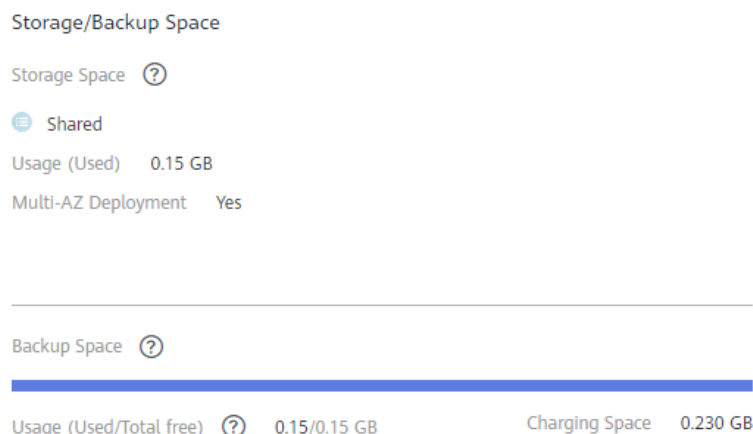
Paso 2 Click  in the upper left corner and select a region and a project.

Paso 3 Haga clic en  en la esquina superior izquierda de la página y elija **Databases > TaurusDB**.

Paso 4 En la página **Instances**, haga clic en el nombre de la instancia para ir a la página **Basic Information**.

Paso 5 En la página **Basic Information**, vea el uso del espacio de copia de respaldo en el área **Backup Space**.

Figura 8-1 Consulta del espacio de copia de respaldo



 **NOTA**

Hay copias de respaldo de datos y binlog de una instancia en el espacio de copia de respaldo.

Se proporciona un espacio de almacenamiento de copia de respaldo gratuito del mismo tamaño que el espacio de almacenamiento adquirido.

----Fin

8.5 ¿Por qué ha fallado mi copia de respaldo automatizada?

Las copias de respaldo automatizadas pueden fallar por las siguientes razones:

1. El entorno de red es inestable debido a problemas como el retraso o la interrupción de la red. TaurusDB detectará estos problemas y activará otra copia de respaldo automatizada media hora después. También puede realizar una copia de respaldo manual antes de eso.
2. Las ejecuciones multitareas son complicadas, lo que resulta en problemas como la espera de tareas o interrupciones. TaurusDB detectará estos problemas y activará otra copia de respaldo automatizada media hora después. También puede realizar una copia de respaldo manual.
3. Una instancia no está disponible, posiblemente porque la instancia está defectuosa o está siendo modificada. TaurusDB activará una copia de respaldo automatizada cuando el estado de la instancia esté disponible. También puede realizar una copia de respaldo manual antes de eso.
4. Un parámetro se cambia incorrectamente. Por ejemplo, una instancia puede llegar a ser defectuosa después de que se le haya aplicado una plantilla de parámetros que contenga parámetros incorrectos. Puede comprobar si los valores originales y actuales son correctos, comprobar si también es necesario cambiar algún parámetro relacionado, restablecer la plantilla de parámetro o reiniciar la instancia.
5. Se ha producido un error durante la importación de datos.
Si los registros del catálogo del sistema se pierden debido a la importación de datos incorrecta, puede importar datos de nuevo haciendo referencia a Migración de datos a TaurusDB mediante DRS.
6. Si el problema continúa, comuníquese con el servicio de asistencia técnica.

8.6 ¿Cómo se facturan los datos de copia de respaldo de TaurusDB?

Todas las copias de respaldo de TaurusDB se almacenan en OBS sin ocupar el almacenamiento de sus instancias de base de datos. TaurusDB proporciona espacio libre de copia de respaldo del mismo tamaño que el almacenamiento comprado.

El ciclo de vida de las copias de respaldo automatizadas es el mismo que el de la instancia de base de datos. Si elimina una instancia de base de datos, sus copias de seguridad automatizadas también se eliminan, pero las copias de seguridad manuales no se van a eliminar automáticamente. Para obtener más información, consulte Eliminación de una copia de respaldo manual.

Por ejemplo, si compra una instancia de base de datos con 200 GB de almacenamiento, puede obtener 200 GB adicionales de espacio de copia de seguridad y solo se le cobrará por copias

de seguridad de más de 200 GB. Los primeros 200 GB de datos de copia de seguridad son gratuitos. Cuando se agote el almacenamiento de 200 GB, las copias de respaldo se facturarán según el pago por uso. Para obtener más información sobre los precios, consulte [Detalles de precios del producto](#).

AVISO

Si su almacenamiento está congelado, ya no se cargará y el espacio de copia de seguridad gratuito tampoco estará disponible.

Si la instancia de base de datos está congelada, no hay espacio de copia de respaldo disponible. Como resultado, se cobrarán las copias de seguridad automatizadas originales de la instancia de base de datos.

- Si descongela la instancia de base de datos, se restaurará el espacio libre de la copia de respaldo.
 - Si elimina directamente la instancia de base de datos congelada, sus copias de seguridad automatizadas también se eliminarán y el espacio de copia de seguridad no se cobrará más.
-


9 Modificación de parámetros de base de datos


9.1 ¿Cómo puedo cambiar la zona horaria?

TaurusDB le permite seleccionar una zona horaria al crear una instancia y cambiar la zona horaria después de crear la instancia.

Procedimiento

Paso 1 [Log in to the management console.](#)

Paso 2 Click  in the upper left corner and select a region and a project.

Paso 3 Haga clic en  en la esquina superior izquierda de la página y elija **Databases > TaurusDB**.

Paso 4 En la página **Instances**, haga clic en el nombre de la instancia.

Paso 5 En el panel de navegación de la izquierda, elija **Parameters**.

Paso 6 Busque un parámetro de zona horaria en el cuadro de búsqueda, por ejemplo, **time_zone**.

Paso 7 Seleccione una zona horaria y haga clic en **Save**.

Paso 8 En el cuadro de diálogo que se muestra, haga clic en **OK**.

Por ejemplo, para cambiar la zona horaria a UTC+08:00, seleccione **Asia/Shanghai** en la lista desplegable.

----Fin

Parámetros de zona horaria

- **system_time_zone**: zona horaria del sistema operativo (OS). El cambio del valor de este parámetro no afecta a la zona horaria de la base de datos.
- **time_zone**: zona horaria de la base de datos. Puede modificar este parámetro para cambiar la zona horaria de la instancia.

9.2 ¿Cómo configuro una política de caducidad de contraseñas para instancias de TaurusDB?

En la versión 8.0 de TaurusDB, puede configurar la variable global **default_password_lifetime** para controlar el período de validez predeterminado de una contraseña de usuario.

El valor de **default_password_lifetime** indica cuántos días quedan hasta que caduque una contraseña. El valor predeterminado es **0**, que indica que la contraseña de usuario creada nunca caducará.

```
mysql> show variables like 'default_password_lifetime';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| default_password_lifetime | 0 |
+-----+-----+
1 row in set (0.00 sec)
```

Cambio de la política global de caducidad automática de contraseñas

- Cambie el valor del parámetro **default_password_lifetime** en la consola TaurusDB. Para obtener más información, consulte [Modificación de una plantilla de parámetro](#).
- Ejecute el siguiente comando para cambiar el valor de **default_password_lifetime**:
`mysql> set global default_password_lifetime=0;`

Comprobación de la fecha de caducidad de la contraseña de todos los usuarios

Ejecute el siguiente comando:

```
mysql> select user,host,password_expired,password_last_changed,password_lifetime
from user;
```

```
mysql> select user,host,password_expired,password_last_changed,password_lifetime from user;
+-----+-----+-----+-----+-----+
| user          | host      | password_expired | password_last_changed | password_lifetime |
+-----+-----+-----+-----+-----+
| mysql.session | localhost | N                | 2020-01-17 15:02:23   | NULL             |
| mysql.sys     | localhost | N                | 2020-01-17 15:02:23   | NULL             |
| rdsAdmin      | localhost | N                | 2020-01-17 15:02:30   | 0                |
| root          | %        | N                | 2020-03-05 14:23:54   | NULL             |
| rdsRepl       | 192.168.% | N                | 2020-01-17 15:02:45   | 0                |
| rdsMetric     | 192.168.% | N                | 2020-01-17 15:02:30   | 0                |
| rdsBackup     | localhost | N                | 2020-01-17 15:02:30   | 0                |
| u_test01      | %        | N                | 2020-03-05 14:28:10   | 30               |
| u_test02      | %        | N                | 2020-03-05 14:28:38   | NULL             |
| jeffrey       | localhost | N                | 2020-03-05 15:23:17   | NULL             |
+-----+-----+-----+-----+-----+
10 rows in set (0.00 sec)
```

Comprobación de la política de caducidad de contraseñas de un usuario especificado

Ejecute el siguiente comando:

```
mysql> show create user jeffrey@'localhost';
```



```
mysql> show create user 'jeffrey@localhost';
+-----+-----+
| CREATE USER for 'jeffrey@localhost' |
+-----+-----+
| CREATE USER 'jeffrey'@'localhost' IDENTIFIED WITH 'mysql_native_password' AS '*1369F151659FC90255853119A9CBB0554DB0D7F' REQUIRE NONE PASSWORD EXPIRE DEFAULT ACCOUNT UNLOCK |
+-----+-----+
1 row in set (0.00 sec)
```

EXPIRE DEFAULT indica que la contraseña sigue la política de caducidad global.

Configuración de la política de caducidad de contraseña para un usuario especificado

- Configuración de la política de caducidad de contraseña durante la creación del usuario
create user 'script'@'localhost' identified by '***' password expire interval 90 day;**
- Configuración de la política de caducidad de contraseña después de la creación del usuario
ALTER USER 'script'@'localhost' PASSWORD EXPIRE INTERVAL 90 DAY;
- Establecer la contraseña para que sea válida de forma permanente
mysql> CREATE USER 'mike'@'%' PASSWORD EXPIRE NEVER;
mysql> ALTER USER 'mike'@'%' PASSWORD EXPIRE NEVER;
- Establecer la contraseña para seguir la política de vencimiento global
mysql> CREATE USER 'mike'@'%' PASSWORD EXPIRE DEFAULT;
mysql> ALTER USER 'mike'@'%' PASSWORD EXPIRE DEFAULT;

9.3 ¿Cómo me aseguro de que el conjunto de caracteres de la base de datos de una instancia de TaurusDB es correcto?


UTF-8 soporta 4 caracteres de byte, pero TaurusDB utf8 soporta solo 3 caracteres de byte. Los emojis y los caracteres Unicode recién agregados no se pueden almacenar con el conjunto de caracteres MySQL utf8. MySQL lanzó el conjunto de caracteres utf8mb4 en 2010 y agregó el código utf8mb4 después de 5.5.3 para ser compatible con el unicode de 4 bytes. Solo necesita cambiar utf8 a utf8mb4. No se requiere ninguna otra conversión.

Data Admin Service (DAS) de Huawei Cloud es una herramienta profesional de gestión de bases de datos. Puede ver los conjuntos de caracteres del sistema y de la base de datos a través de la consola de DAS.

Procedimiento

Paso 1 [Log in to the management console.](#)

Paso 2 Click  in the upper left corner and select a region and a project.

Paso 3 Haga clic en  en la esquina superior izquierda de la página y elija **Databases > TaurusDB.**

Paso 4 En la página **Instances**, busque la instancia y haga clic en **Log In** en la columna **Operation.**

Como alternativa, en la página **Instances**, haga clic en el nombre de la instancia para ir a la página **Basic Information.** Haga clic en **Log In** en la esquina superior derecha de la página.

Paso 5 En la página de inicio de sesión mostrada, ingrese el nombre de usuario y la contraseña correctos y haga clic en **Log In**.

Paso 6 En la barra de menú superior, elija **SQL Operations > SQL Window**.

Paso 7 Ejecute la siguiente sentencia de SQL en la ventana de SQL para ver el conjunto de caracteres de la base de datos:

show variables like '%character%';

Figura 9-1 Resultado de ejecución SQL

The screenshot shows the execution result of the SQL query 'show variables like '%character%';'. The result is displayed in a table with two columns: 'Variable_name' and 'Value'. The table contains 8 rows of data. The interface also includes a toolbar with options like 'Copy Row', 'Copy Column', and 'Column Settings', and a status bar indicating 'Append Mode'.

Variable_name	Value
character_set_client	utf8mb4
character_set_connection	utf8mb4
character_set_database	utf8
character_set_filesystem	binary
character_set_results	
character_set_server	utf8
character_set_system	utf8
character_sets_dir	/usr/local/mysql-5.7.27...

Paso 8 Ejecute la siguiente sentencia SQL en la ventana de SQL para ver la codificación de la base de datos:

show variables like 'collation%';

Figura 9-2 Resultado de ejecución SQL

The screenshot shows the execution result of the SQL query 'show variables like 'collation%';'. The result is displayed in a table with two columns: 'Variable_name' and 'Value'. The table contains 3 rows of data. The interface also includes a toolbar with options like 'Copy Row', 'Copy Column', and 'Column Settings', and a status bar indicating 'Append Mode'.

Variable_name	Value
collation_connection	utf8mb4_general_ci
collation_database	utf8_general_ci
collation_server	utf8_general_ci

Paso 9 Cambie el conjunto de caracteres a utf8mb4.

1. Ejecute la siguiente sentencia SQL para cambiar los conjuntos de caracteres de la base de datos.

ALTER DATABASE *DATABASE_NAME* DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;

2. Ejecute la siguiente sentencia SQL para cambiar los conjuntos de caracteres de la tabla.

ALTER TABLE *TABLE_NAME* DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;

📖 NOTA

La sentencia SQL solo cambia los conjuntos de caracteres de las tablas. Los conjuntos de caracteres de los campos de las tablas no se modifican.

3. Ejecute la siguiente sentencia SQL para cambiar todos los conjuntos de caracteres de campo en las tablas:

ALTER TABLE *TABLE_NAME* CONVERT TO CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;

 **NOTA**

- **character_set_client**, **character_set_connection** y **character_set_results** son los ajustes del cliente.
- **character_set_system**, **character_set_server** y **character_set_database** son los ajustes del servidor.
- Las prioridades de los parámetros en el servidor son las siguientes: **character_set_database** > **character_set_server** > **character_set_system**.

----Fin

9.4 ¿Cómo uso el conjunto de caracteres de utf8mb4 para almacenar emojis en una instancia de TaurusDB?

Para almacenar emojis en una instancia de TaurusDB, asegúrese de que:

- El cliente genera el conjunto de caracteres utf8mb4.
- La conexión admite el conjunto de caracteres utf8mb4. Si desea utilizar una conexión JDBC, descargue MySQL Connector/J 5.1.13 o una versión posterior y deje **characterEncoding** sin definir para la cadena de conexión JDBC.
- Configure la instancia de la siguiente manera:
 - Configuración de **character_set_server** en **utf8mb4**

Parameter Name	Effective upon Reboot	Value	Allowed Values	Description
character_set_server	Yes	utf8mb4	utf8, latin1, gbk, utf8mb4	The server's default character set.



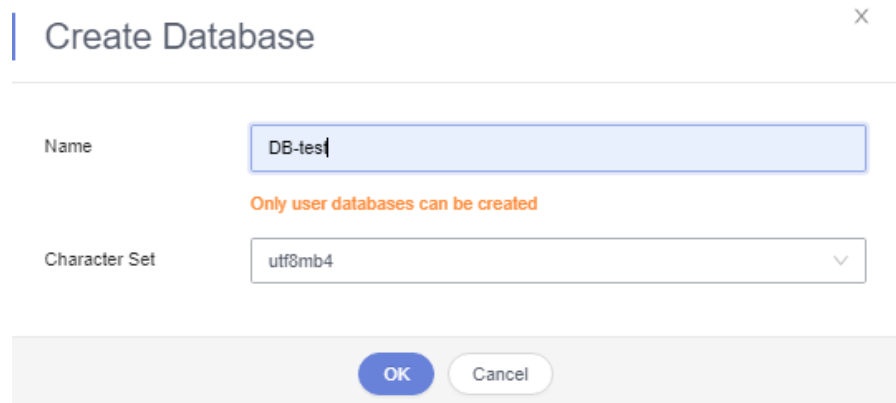
- Log in to the management console.**
 - Click  in the upper left corner and select a region and a project.
 - Haga clic en  en la esquina superior izquierda de la página y elija **Databases > TaurusDB**.
 - En la página **Instances**, haga clic en el nombre de la instancia.
 - En el panel de navegación de la izquierda, elija **Parameters**. En la página de pestaña **Parameters**, busque **character_set_server** y cambie su valor a **utf8mb4**.
 - Haga clic en **Save**. En el cuadro de diálogo que se muestra, haga clic en **Yes**.
- Selección de **utf8mb4** para el juego de caracteres de la base de datos
 - En la página **Instances**, busque la instancia y haga clic en **Log In** en la columna **Operation**.
Como alternativa, en la página **Instances**, haga clic en el nombre de la instancia para ir a la página **Basic Information**. Haga clic en **Log In** en la esquina superior derecha de la página.
 - En la página de inicio de sesión mostrada, ingrese el nombre de usuario y la contraseña correctos y haga clic en **Log In**.
 - En la página **Databases**, haga clic en **Create Database**. En el cuadro de diálogo que se muestra, escriba un nombre de base de datos, seleccione el juego de caracteres **utf8mb4** y autorice permisos de base de datos para los usuarios. A continuación, haga clic en **OK**.

Figura 9-3 Creación de una base de datos



- Establecer el juego de caracteres de la tabla en **utf8mb4**

```
([...]) [ ... ] > create table emoji_01 (id int auto_increment primary key, content varchar(255) default charset utf8mb4;
Query OK, 0 rows affected (0.01 sec)

([...]) [ ... ] > show create table emoji_01 \G
***** 1. row *****
Table: emoji_01
Create Table: CREATE TABLE 'emoji_01' (
  'id' int(11) NOT NULL AUTO_INCREMENT,
  'content' varchar(255) DEFAULT NULL,
  PRIMARY KEY ('id')
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4
1 row in set (0.00 sec)
```

Preguntas frecuentes

Si ha establecido **characterEncoding** en **utf8** para la cadena de conexión JDBC, o los datos de emoji no se pueden insertar correctamente después de haber realizado las operaciones anteriores, se recomienda establecer el conjunto de caracteres de conexión en **utf8mb4** de la siguiente manera:

```
String query = "set names utf8mb4";
stat.execute(query);
```

9.5 ¿Cómo configuro la sensibilidad a mayúsculas y minúsculas para los nombres de tablas de TaurusDB?

Puede especificar la distinción entre mayúsculas y minúsculas para los nombres de tablas al crear una instancia en la consola o usar API. No se puede cambiar después de crear la instancia.

- Establezca **Table Name Case Sensitivity** en la consola. Para obtener más información, consulte [Comprar una instancia de base de datos](#).

Figura 9-4 Configuración de la sensibilidad a mayúsculas y minúsculas para los nombres de tablas

The screenshot shows a configuration page for TaurusDB. At the top, there are fields for 'Administrator' (root) and 'Administrator Password' (with a note: 'Keep your password secure. The system cannot retrieve your password.'). Below that is a 'Confirm Password' field. A horizontal separator line follows. Then, there is a 'Parameter Template' dropdown menu set to 'Default-GaussDB-for-MySQL 8.0' with a 'View Parameter Template' link. Below that is the 'Table Name' section, which has two radio buttons: 'Case sensitive' (unselected) and 'Case Insensitive' (selected). A help icon and text next to it state: 'This option cannot be changed later.' At the bottom, there is an 'Enterprise Project' dropdown menu set to '--Select--' with a 'Create Enterprise Project' link.

- Establezca **lower_case_table_names** invocando una API. Para obtener más información, consulte Creación de una instancia de base de datos.

Rango de valores:


- **0**: Los nombres de las tablas distinguen entre mayúsculas y minúsculas.
- **1** (valor predeterminado): Los nombres de las tablas se almacenan en minúsculas y no distinguen entre mayúsculas y minúsculas.


9.6 ¿Puedo usar comandos SQL para modificar parámetros globales?

Lo sentimos, no puede utilizar comandos SQL para modificar parámetros globales, pero puede modificar parámetros específicos en la consola.

Procedimiento

Paso 1 [Log in to the management console.](#)

Paso 2 Click  in the upper left corner and select a region and a project.

Paso 3 Haga clic en  en la esquina superior izquierda de la página y elija **Databases > TaurusDB**.

Paso 4 En la página **Instances**, haga clic en la instancia de base de datos de destino.

Paso 5 En el panel de navegación de la izquierda, elija **Parameters**.

Paso 6 Cambie el valor del parámetro de destino y haga clic en **Save**.

Paso 7 En el cuadro de diálogo que se muestra, haga clic en **OK**.

----Fin

10 Seguridad de red

10.1 ¿Qué medidas de garantía de seguridad tiene TaurusDB?

Red

- TaurusDB le permite configurar sus instancias en una VPC, asegurando que las instancias estén aisladas de otros servicios.
- TaurusDB utiliza grupos de seguridad para garantizar que solo las fuentes de confianza puedan acceder a sus instancias.
- TaurusDB soporta conexiones SSL para cifrar datos durante la transmisión.

Gestión

Puede utilizar **Identity and Access Management (IAM)** para gestionar los permisos de TaurusDB.

10.2 ¿Cómo puedo evitar que las direcciones IP de origen no confiables accedan a TaurusDB?

- Si habilita la accesibilidad pública, su DNS EIP y el puerto de base de datos pueden ser vulnerables a la piratería. Para proteger información como su EIP, DNS, puerto de base de datos, cuenta de base de datos y contraseña, se recomienda especificar el rango de direcciones IP de origen en el grupo de seguridad de TaurusDB para garantizar que solo las direcciones IP de origen de confianza puedan tener acceso a sus instancias.
- Para evitar que se descifra la contraseña de la base de datos, especifique una contraseña segura y cámbiela periódicamente.

10.3 ¿Cómo configuro un grupo de seguridad para habilitar el acceso a una instancia de TaurusDB?

- Cuando intenta conectarse a una instancia de TaurusDB a través de una red privada, compruebe si la instancia ECS y TaurusDB están en el mismo grupo de seguridad.
 - Si la instancia de ECS y TaurusDB están en el mismo grupo de seguridad, pueden comunicarse entre sí de forma predeterminada. No es necesario configurar reglas de grupo de seguridad.
 - Si la instancia de ECS y TaurusDB están en diferentes grupos de seguridad, configure las reglas de grupo de seguridad para ECS y la instancia, respectivamente.
 - Instancia: Configure una **inbound rule** para el grupo de seguridad al que está asociada la instancia.
 - ECS: La regla de grupo de seguridad predeterminada permite todos los paquetes de datos salientes. En este caso, no es necesario configurar una regla de grupo de seguridad para el ECS. Si no se permite todo el tráfico saliente en el grupo de seguridad, es posible que deba configurar una regla saliente para que el ECS permita todos los paquetes salientes.
- Cuando intenta acceder a una instancia a través de una EIP, debe configurar un **inbound rule** para el grupo de seguridad asociado a la instancia.

10.4 ¿Cómo puedo importar el certificado raíz a un servidor Windows o Linux?

Importar el certificado raíz a un Windows Server

1. Haga clic en **Start** y seleccione **Run**. En el cuadro de diálogo **Run** que se muestra, escriba **MMC** y pulse **Enter**.
2. En la consola que se muestra, elija **File > Add/Remove Snap-in**.
3. En el panel **Available snap-ins** izquierdo del cuadro de diálogo que se muestra, seleccione **Certificates**. Haga clic en **Add** para agregar el certificado.
4. En el cuadro de diálogo **Certificates snap-in** que se muestra, seleccione **Computer account** y haga clic en **Next**.
5. En el cuadro de diálogo **Select Computer** que se muestra, haga clic en **Finish**.
6. En el cuadro de diálogo **Add or Remove Snap-ins**, haga clic en **OK**.
7. En la consola, haga doble clic en **Certificates**.
8. Haga clic con el botón derecho en **Trusted Root Certification Authorities** y elija **All Tasks > Import**.
9. Haga clic en **Next**.
10. Haga clic en **Browse** para cambiar el tipo de archivo a **All Files (*.*)**.
11. Localice el certificado raíz descargado (un archivo de **ca.pem**) y haga clic en **Open**. Luego, haga clic en **Next**.

AVISO

Debe cambiar el tipo de archivo a **All Files (*.*)** porque **.pem** no es un nombre de extensión de certificado estándar.

12. Haga clic en **Next**.
13. Haga clic en **Finish**.
14. Haga clic en **OK** para completar la importación del certificado raíz.

Importación del certificado raíz a un Linux Server

Puede utilizar una herramienta de conexión (como WinSCP o PuTTY) para cargar el certificado en cualquier directorio de un Linux Server.

10.5 ¿Cómo puedo gestionar y garantizar la seguridad de TaurusDB?

Por razones de seguridad, no utilice el nombre de usuario y la contraseña de su cuenta de Huawei Cloud. Le recomendamos que cree usuarios de IAM y otros usuarios (si es necesario) para los usuarios de la base de datos.

Puede producirse un error si no tiene suficientes permisos o si la configuración de su cuenta es incorrecta. Por ejemplo, no puede crear instancias si no tiene los permisos para hacerlo. Si es necesario, póngase en contacto con el administrador de IAM para asignar los permisos


11 Gestión de registros


11.1 ¿Cómo puedo ver todos los registros de SQL ejecutados por TaurusDB?

Puede utilizar el servicio de gestión de bases de datos visualizadas Data Admin Service (DAS) para buscar rápidamente registros de ejecución de SQL de destino.

Consulta de registros SQL a través de DAS

Paso 1 [Log in to the management console.](#)

Paso 2 Click  in the upper left corner and select a region and a project.

Paso 3 Haga clic en  en la esquina superior izquierda de la página y elija **Databases > TaurusDB**.

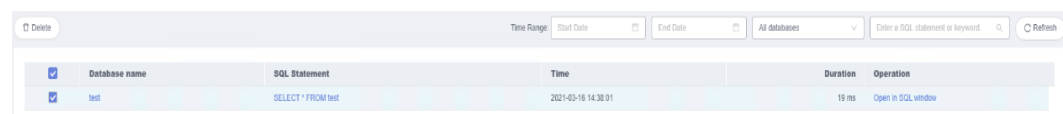
Paso 4 En la página **Instances**, busque la instancia que desea iniciar sesión y haga clic en **Log In** en la columna **Operation**.

Paso 5 En la página de inicio de sesión mostrada, ingrese el nombre de usuario y la contraseña correctos y haga clic en **Log In**.

Paso 6 En la barra de menú superior, elija **SQL Operations > SQL History**.

Paso 7 En la página mostrada, busque información de ejecución sobre la sentencia SQL de destino por intervalo de tiempo, nombre de base de datos o palabra clave.

Figura 11-1 Historial de SQL



<input checked="" type="checkbox"/>	Database name	SQL Statement	Time	Duration	Operation
<input checked="" type="checkbox"/>	test	SELECT * FROM test	2021-03-16 14:38:01	19 ms	Open in SQL window

- Para acceder a la página **Database Management**, haga clic en un nombre de base de datos.


- Para copiar y usar una sentencia SQL, haga clic en ella en la columna **SQL Statement**.
- Para ejecutar una sentencia SQL, busque la sentencia y haga clic en **Open in SQL Window** en la columna **Operation**.


----Fin

11.2 ¿Cómo puedo ver los registros de consultas lentas de TaurusDB?

Consulta de detalles de registro

Paso 1 [Log in to the management console](#).

Paso 2 Click  in the upper left corner and select a region and a project.

Paso 3 Haga clic en  en la esquina superior izquierda de la página y elija **Databases > TaurusDB**.

Paso 4 En la página **Instances**, haga clic en el nombre de la instancia para ir a la página **Basic Information**.

Paso 5 En el panel de navegación de la izquierda, elija **Logs**.

Paso 6 En la página **Slow Query Logs**, vea los detalles del registro de consultas lentas.

Puede ver los registros de registro de consultas lentas de un tipo de sentencia de ejecución especificado o un período de tiempo específico.


----Fin


11.3 ¿Cómo habilito y veo Binlog de mi instancia de TaurusDB?

Habilitación de Binlog

TaurusDB no admite la habilitación de binlog para réplicas de lectura. Para obtener más información acerca de cómo habilitar binlog para el nodo principal, realice los siguientes pasos:

Paso 1 [Log in to the management console](#).

Paso 2 Click  in the upper left corner and select a region and a project.

Paso 3 Haga clic en  en la esquina superior izquierda de la página y elija **Databases > TaurusDB**.

Paso 4 Haga clic en el nombre de la instancia para ir a la página **Basic Information**.

Paso 5 En el panel de navegación de la izquierda, elija **Parameters**.

Paso 6 Introduzca **log-bin** en el cuadro de búsqueda y haga clic en el botón de búsqueda. Busque el parámetro mostrado, seleccione **ON** en la lista desplegable **Value**. Haga clic en **Save** encima de la lista de parámetros.

Paso 7 Reinicie la instancia para que la modificación surta efecto.

----Fin

Consulta de archivos de Binlog

Paso 1 Conéctese a una instancia. Para obtener más información, consulte Conectar a una instancia de base de datos.

Paso 2 Ejecute el siguiente comando para ver los archivos binlog:

```
SHOW BINLOG EVENTS [IN 'log_name'] [FROM pos] [LIMIT [offset,] row_count];
```

NOTA

Si aparece un mensaje que indica que los permisos de la cuenta son insuficientes, utilice la cuenta **root**.

----Fin

Impacto de habilitación de Binlog en el rendimiento de TaurusDB

La habilitación de binlog no afecta a las operaciones SELECT, pero afecta a INSERT, UPDATE, DELETE y otras operaciones de escritura.

NOTA


No hay diferencias significativas entre el binlog de TaurusDB y el binlog de código abierto de MySQL. La sintaxis binlog de TaurusDB es totalmente compatible con la del código abierto de MySQL.


11.4 ¿Cómo cambio el período de retención de Binlog?

TaurusDB es compatible con el parámetro **binlog_expire_logs_seconds** de la comunidad versión 8.0. Puede cambiar el período de retención de binlog mediante este parámetro.

Procedimiento

Paso 1 [Log in to the management console.](#)

Paso 2 Click  in the upper left corner and select a region and a project.

Paso 3 Haga clic en  en la esquina superior izquierda de la página y elija **Databases > TaurusDB**.

Paso 4 En la página **Instances**, haga clic en el nombre de la instancia para ir a la página **Basic Information**.

Paso 5 En el panel de navegación de la izquierda, elija **Parameters**. En la pestaña **Parameters**, busque el parámetro **log-bin** y cambie su valor a **ON** (indicando que binlog está habilitado).

Paso 6 En la pestaña **Parameters**, configure **binlog_expire_logs_seconds**.

 **NOTA**

- Cuando se genera un nuevo archivo binlog, se eliminarán todos los archivos binlog existentes que hayan caducado.
- Si no se genera un nuevo archivo binlog, los archivos binlog históricos no se eliminarán aunque hayan caducado. Para eliminar archivos binlog manualmente, conéctese a la base de datos y ejecute **flush logs**; para generar a la fuerza un nuevo archivo binlog.


----Fin


11.5 ¿Cómo puedo ver los registros de interbloqueo de TaurusDB?

Los registros de interbloqueo de la base de datos no se registran en los registros de errores. Para ver los registros de interbloqueo, utilice Data Admin Service (DAS), una herramienta de gestión de bases de datos visualizada y profesional, para ejecutar rápidamente sentencias SQL.

Procedimiento

Paso 1 [Log in to the management console.](#)

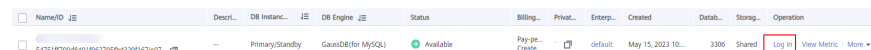
Paso 2 Click  in the upper left corner and select a region and a project.

Paso 3 Haga clic en  en la esquina superior izquierda de la página y elija **Databases > TaurusDB**.

Paso 4 En la página **Instances**, busque la instancia que desea iniciar sesión y haga clic en **Log In** en la columna **Operation**.

Paso 5 En la página de inicio de sesión mostrada, ingrese el nombre de usuario y la contraseña correctos y haga clic en **Log In**.

Figura 11-2 Inicio de sesión en una instancia



Name/ID	Descr...	DB Instanc...	DB Engine	Status	Billing...	Privet...	Enterp...	Created	Datab...	Storag...	Operation
s4751f77098491f962705fb32016767		Primary/Standby	GaussDB(for MySQL)	Available	Pay-As-You-Go	default	May 15, 2023 10...	3306	Shared		Log In View Metric More

Paso 6 Seleccione la base de datos de destino y haga clic en **SQL Operations > SQL Window**.

Paso 7 En la ventana SQL mostrada, ejecute **show engine innodb status** para ver los últimos registros de interbloqueo de la base de datos seleccionada. Utilice la palabra clave **LATEST DETECTED DEADLOCK** para localizar los últimos registros de interbloqueo. Los últimos registros de interbloqueo sobrescribirán los registros históricos de interbloqueo.

----Fin

12 Actualización de versión

12.1 ¿Cómo puedo comprobar una versión de instancia de TaurusDB?

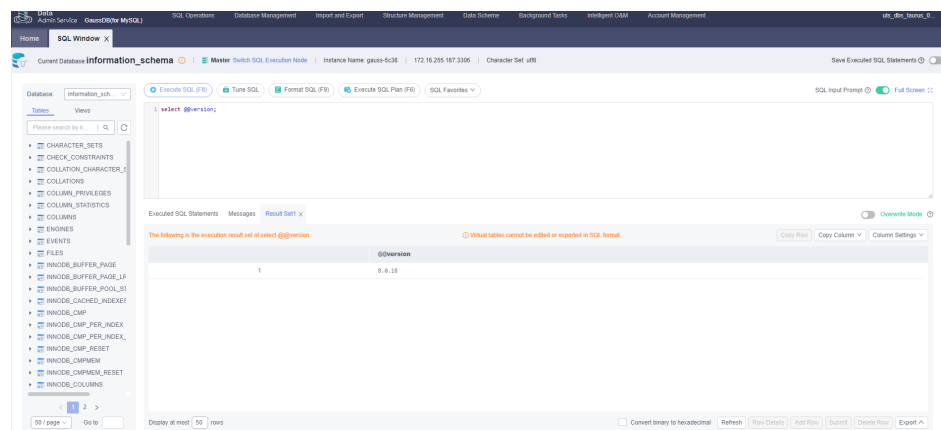
- En la página **Basic Information** de la instancia de destino, vea la versión de la instancia.

Figura 12-1 Consulta de información básica de instancia

DB Instance Information			
DB Instance Name	gauss	DB Instance ID	bf10ede6894043d9a029136cc3db31e4in07
Status	Available	Nodes	2
DB Engine Version	MySQL 8.0 Upgrade	Time Zone	UTC+08:00
Instance Class	gaussdb.mysql.2xlarge.x86_4 8 vCPUs 32 GB	Region	Beijing4
AZ Type	Single-AZ	Primary AZ	cn-north-4b
Administrator	root Reset Password	SSL	Certificate
Maintenance Window	02:00 – 06:00	Enterprise Project	default

- En la consola DAS, realice los siguientes pasos para ver la versión de la instancia de destino:
 - a. Inicie sesión en la instancia de destino.
 - b. En la barra de menú superior, elija **SQL Operations > SQL Query**.
 - c. Ejecute **select @@version;** para ver la versión de la instancia.

Figura 12-2 Consulta de la versión de instancia



12.2 ¿Puedo actualizar versiones de instancias de TaurusDB?

Puede actualizar manualmente las versiones menores de sus instancias para mejorar el rendimiento, agregar nuevas funciones y corregir errores.

Las réplicas de lectura se actualizan antes que el nodo principal.

Para obtener más información sobre las operaciones de actualización, consulte Actualización de versión secundaria.