

TaurusDB

Perguntas frequentes

Edição 01
Data 2025-02-07



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. Todos os direitos reservados.

Nenhuma parte deste documento pode ser reproduzida ou transmitida em qualquer forma ou por qualquer meio sem consentimento prévio por escrito da Huawei Cloud Computing Technologies Co., Ltd.

Marcas registadas e permissões



HUAWEI e outras marcas registadas da Huawei são marcas registadas da Huawei Technologies Co., Ltd. Todas as outras marcas registadas e os nomes registados mencionados neste documento são propriedade dos seus respectivos detentores.

Aviso

Os produtos, os serviços e as funcionalidades adquiridos são estipulados pelo contrato estabelecido entre a Huawei Cloud e o cliente. Os produtos, os serviços e as funcionalidades descritos neste documento, no todo ou em parte, podem não estar dentro do âmbito de aquisição ou do âmbito de uso. Salvo especificação em contrário no contrato, todas as declarações, informações e recomendações neste documento são fornecidas "TAL COMO ESTÃO" sem garantias ou representações de qualquer tipo, sejam expressas ou implícitas.

As informações contidas neste documento estão sujeitas a alterações sem aviso prévio. Foram feitos todos os esforços na preparação deste documento para assegurar a exatidão do conteúdo, mas todas as declarações, informações e recomendações contidas neste documento não constituem uma garantia de qualquer tipo, expressa ou implícita.

Huawei Cloud Computing Technologies Co., Ltd.

Endereço: Huawei Cloud Data Center, Rua Jiaoxinggong
Avenida Qianzhong
Novo Distrito de Gui'an
Guizhou 550029
República Popular da China

Site: <https://www.huaweicloud.com/intl/pt-br/>

Índice

1 Consultoria de produto.....	1
1.1 Em que devo prestar atenção ao usar o TaurusDB?.....	1
1.2 O que posso fazer sobre a resposta lenta dos sites quando eles usam TaurusDB?.....	1
1.3 O TaurusDB oferece suporte a failover automático?.....	2
1.4 O TaurusDB suporta o desacoplamento de computação e armazenamento?.....	2
1.5 Congelamento, liberação, exclusão e cancelamento de assinatura de recursos.....	2
2 Conexões de banco de dados.....	4
2.1 O que devo fazer se não conseguir me conectar à minha instância do TaurusDB?.....	4
2.2 Um servidor externo pode acessar o banco de dados do TaurusDB?.....	15
2.3 O que devo fazer se o número de conexões de banco de dados do TaurusDB atingir o limite superior?.....	16
2.4 Qual é o número máximo de conexões em uma instância do TaurusDB?.....	16
2.5 O que devo fazer se um ECS não puder se conectar a uma instância do TaurusDB?.....	17
2.6 Como me conectar a um banco de dados MySQL por meio de JDBC?.....	18
2.7 Como criar e me conectar a um ECS?.....	24
2.8 O que devo fazer se um problema no cliente de banco de dados causar uma falha de conexão?.....	24
2.9 Por que não é possível executar o ping do meu EIP depois que ele está vinculado a uma instância de BD?.....	25
2.10 O que posso fazer se o teste de conexão falhou?.....	26
2.11 Posso acessar uma instância do TaurusDB por meio de uma conexão de intranet entre regiões?.....	26
2.12 Existem riscos potenciais se houver muitas conexões com uma instância do TaurusDB?.....	27
2.13 O que devo fazer se uma instância do ECS e do TaurusDB implementada em VPCs diferentes não puder se comunicar entre si?.....	27
2.14 Como visualizar todos os endereços IP conectados a um banco de dados?.....	27
3 Instalação do cliente.....	28
3.1 Como instalar o cliente de MySQL?.....	28
4 Migração de banco de dados.....	31
4.1 Que tipos de mecanismos de banco de dados o TaurusDB suporta para importar dados?.....	31
5 Permissões do banco de dados.....	32
5.1 O TaurusDB fornece a conta raiz ou a superpermissão?.....	32
6 Desempenho do banco de dados.....	33
6.1 O que devo fazer se o uso da CPU da minha instância for alto?.....	33
6.2 Como lidar com instruções SQL lentas causadas por configurações de índice composto inapropriadas?.....	33

6.3 Como lidar com um grande número de tabelas temporárias sendo geradas para transações longas e alto uso de memória?.....	36
6.4 O que devo fazer se os bloqueios em transações longas bloquearem a execução de transações subsequentes?.....	37
6.5 Como usar o disco temporário do TaurusDB?.....	38
7 Uso do banco de dados.....	43
7.1 Por que os resultados são inconsistentes depois que a instrução MATCH AGAINST é executada, respectivamente, em nós primários e réplicas de leitura?.....	43
7.2 Como adicionar colunas usando INSTANT?.....	43
7.3 Como usar LOAD DATA para importar dados locais?.....	44
8 Backups.....	47
8.1 Por quanto tempo o TaurusDB armazena dados de backup?.....	47
8.2 Como limpar o espaço de backup do TaurusDB?.....	47
8.3 Como fazer backup de um banco de dados do TaurusDB em um ECS?.....	47
8.4 Como ver o uso do armazenamento do meu backup?.....	48
8.5 Por que meu backup automatizado falhou?.....	48
8.6 Como os dados de backup do TaurusDB são cobrados?.....	49
9 Modificação de parâmetro do banco de dados.....	50
9.1 Como alterar o fuso horário?.....	50
9.2 Como configurar uma política de expiração de senha para instâncias do TaurusDB?.....	51
9.3 Como garantir que o conjunto de caracteres do banco de dados de uma instância do TaurusDB esteja correto?.....	52
9.4 Como usar o conjunto de caracteres utf8mb4 para armazenar emojis em uma instância do TaurusDB?.....	54
9.5 Como definir a sensibilidade de maiúsculas e minúsculas para nomes de tabela do TaurusDB?.....	55
9.6 Posso usar comandos SQL para modificar parâmetros globais?.....	56
10 Segurança de rede.....	57
10.1 Quais são as medidas de garantia de segurança do TaurusDB?.....	57
10.2 Como impedir que endereços IP de origem não confiáveis acessem o TaurusDB?.....	57
10.3 Como configurar um grupo de segurança para permitir o acesso a uma instância do TaurusDB?.....	58
10.4 Como importar o certificado raiz para um servidor Windows ou Linux?.....	58
10.5 Como gerenciar e garantir a segurança do TaurusDB?.....	59
11 Gerenciamento de logs.....	60
11.1 Posso habilitar general_log para TaurusDB?.....	60
11.2 Como visualizar todos os logs SQL executados pelo TaurusDB?.....	60
11.3 Como visualizar logs de consulta lenta do TaurusDB?.....	61
11.4 Como ativar e visualizar o binlog da minha instância do TaurusDB?.....	61
11.5 Como alterar o período de retenção do binlog?.....	63
11.6 Como visualizar os logs de deadlock do TaurusDB?.....	64
12 Atualização de versão.....	65
12.1 Como verificar uma versão de instância do TaurusDB?.....	65
12.2 Posso atualizar as versões de instâncias do TaurusDB?.....	66

1 Consultoria de produto

1.1 Em que devo prestar atenção ao usar o TaurusDB?

1. Sistemas operacionais (SOs) de instância são invisíveis para você. Suas aplicações podem acessar um banco de dados somente por meio de um endereço IP e uma porta.
2. Os arquivos de backup armazenados nos buckets do Object Storage Service (OBS) e nos Elastic Cloud Servers (ECSs) usados pelo TaurusDB são invisíveis para você. Eles são visíveis apenas para o sistema de gerenciamento de instâncias.
3. Quando você visualizar sua instância na lista de instâncias, selecione a região onde ela está localizada.
4. Precauções após a criação de instâncias do TaurusDB:
Depois que sua instância é criada, você não precisa executar operações básicas de O&M do banco de dados, como aplicar patches de segurança e alta disponibilidade, mas deve prestar atenção a:
 - a. vCPUs e memória da sua instância. Se elas se tornarem insuficientes, você precisa mudá-las em tempo hábil.
 - b. Espaço de armazenamento da sua instância. Se o armazenamento for usado, você será cobrado em uma base de pagamento por uso por qualquer armazenamento adicional, mas se você expandir o armazenamento com antecedência, poderá pagar pelo armazenamento adicional com taxas anuais/mensais.
 - c. Desempenho da sua instância. Você precisa verificar regularmente se há instruções SQL de consulta lenta, instruções SQL a serem otimizadas ou índices redundantes ou ausentes.

1.2 O que posso fazer sobre a resposta lenta dos sites quando eles usam TaurusDB?

Para resolver este problema:

- Verifique o desempenho das instâncias do TaurusDB no console do TaurusDB.
- Compare o status da conexão do banco de dados dos bancos de dados locais e das instâncias do TaurusDB. Esse problema depende das aplicações Web.

1.3 O TaurusDB oferece suporte a failover automático?

Sim. Durante a criação de uma instância do TaurusDB, um nó primário e uma réplica de leitura são criados. Se o nó primário falhar, a réplica de leitura é automaticamente promovida para o nó primário para fornecer serviços e o nó primário original é rebaixado para ser uma réplica de leitura.

1.4 O TaurusDB suporta o desacoplamento de computação e armazenamento?

TaurusDB suporta o desacoplamento de computação e armazenamento, melhorando a alta disponibilidade e a experiência em backup e restauração, upgrade e expansão de capacidade.

1.5 Congelamento, liberação, exclusão e cancelamento de assinatura de recursos

Por que meus recursos são liberados?

Se suas assinaturas expiraram, mas não foram renovadas, ou você está em atraso devido a saldo insuficiente, seus recursos entram em um período de carência. Se você não renovar as assinaturas ou recarregar sua conta após o período de carência expirar, seus recursos entrarão em um período de retenção. Durante o período de retenção, os recursos não estão disponíveis. Se a renovação ainda não for concluída ou o valor pendente ainda não for pago quando o período de retenção terminar, os dados armazenados serão excluídos e os recursos do serviço de nuvem serão liberados. Para obter detalhes, consulte [Suspensão de serviço e liberação de recurso](#).

Por que meus recursos estão congelados?

Seus recursos podem ser congelados por vários motivos. A razão mais comum é que você está em atraso.

Ainda posso fazer backup de dados se minha instância de BD estiver congelada?

Não. Se sua instância estiver congelada devido a atrasos, você precisará descongelá-la primeiro.

Como descongelar meus recursos?

Congelados devido a atrasos: você pode renovar seus recursos ou recarregar sua conta. Instâncias congeladas devido a atrasos podem ser renovadas, liberadas ou excluídas. As instâncias anuais/mensais que expiraram não podem ser canceladas, enquanto as que não expiraram podem ser canceladas.

O que acontece quando meus recursos são congelados, descongelados ou liberados?

- Depois que seus recursos forem congelados:
 - Eles não podem ser acessados, causando tempo de inatividade. Por exemplo, se sua instância estiver congelada, ela não poderá ser conectada.
 - Se forem recursos anuais/mensais, nenhuma alteração poderá ser feita a eles.
 - Eles podem ser cancelados ou excluídos manualmente.
- Depois que seus recursos forem descongelados, você poderá se conectar a eles novamente.
- Se seus recursos forem liberados, sua instância será excluída.

Como renovar meus recursos?

Depois que uma instância anual/mensal expirar, você poderá renová-la na página [Renewals](#). Para obter detalhes, consulte [Gerenciamento de renovação](#).

Meus recursos podem ser recuperados após serem liberados? /Posso recuperar um cancelamento de assinatura incorreto?

Você pode restaurar sua instância excluída de um backup manual ou reconstruir sua instância na lixeira durante o período de retenção. Para obter detalhes, consulte [Restauração de dados em uma instância de BD](#) e [Reconstrução de uma instância excluída da lixeira](#).

Antes de cancelar a assinatura de um recurso, confirme as informações do recurso cuidadosamente. Se você cancelou a assinatura de uma instância por engano, compre uma nova.

Como excluir minha instância?

- Para instâncias de pagamento por uso, consulte [Exclusão de uma instância de BD cobrada com base no pagamento por uso](#).
- Para instâncias anuais/mensais, consulte [Cancelamento de assinatura de uma instância anual/mensal](#).

2 Conexões de banco de dados

2.1 O que devo fazer se não conseguir me conectar à minha instância do TaurusDB?

Possíveis causas

Tente o seguinte:

1. **Verifique se a instância de BD está disponível.**

Por exemplo, o status da instância de banco de dados é anormal.

2. **(Comum) Verifique se a conexão do cliente está correta.**

- Se você se conectar a uma instância de BD em uma rede privada, verifique se a instância de BD e o ECS estão na mesma região e VPC.
- Se você se conectar a uma instância de BD em uma rede pública, vincule um EIP à instância de BD e, em seguida, conecte-se à instância de BD por meio do EIP.

3. **Verifique se a conexão SSL está sendo usada.**

Execute um dos seguintes comandos de exemplo para ativar ou desativar o SSL:

- SSL ativado: `mysql -h 172.16.0.31 -P 3306 -u root -p --ssl-ca=/tmp/ca.pem`
- SSL desativado: `mysql -h 172.16.0.31 -P 3306 -u root -p`

4. **Verifique se os parâmetros do comando de conexão estão corretos.**

Por exemplo, verifique se os seguintes parâmetros estão configurados corretamente: connection address, port number, username, password e connection method.

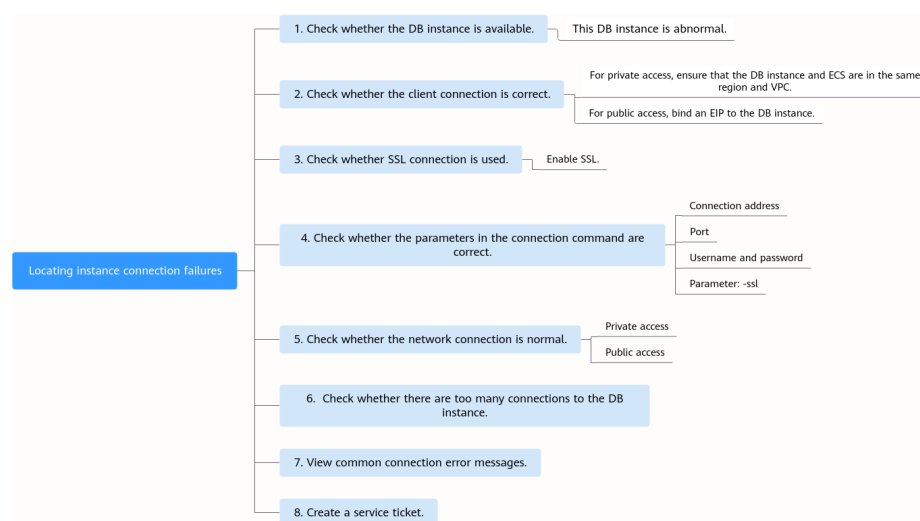
5. **(Comum) Verifique se a conexão de rede está normal.**

- Para uma conexão de rede privada:
 - i. Verifique se o ECS e a instância do BD estão na mesma região e VPC.
 - ii. Verifique as regras do grupo de segurança.
 - iii. No ECS, verifique se a porta da instância de BD pode ser conectada.
- Para uma conexão de rede pública:
 - i. Verifique as regras do grupo de segurança.

- ii. Verifique as regras de ACL de rede.
 - iii. Faça o ping dos ECSs na mesma região para a instância de BD.
6. **(Comum) Verifique se há muitas conexões com a instância de banco de dados.**
Se houver um número excessivo de conexões de banco de dados, as aplicações podem não ser conectadas.
7. **Exiba mensagens de erro de conexão comuns.**
Encontre soluções correspondentes com base em mensagens de erro de conexão.

Localização de falhas

Figura 2-1 O que posso fazer se não conseguir me conectar à minha instância de banco de dados?



1. **Verifique se a instância de BD está disponível.**
Verifique se a instância de BD está no estado **Available**.
Possível causa: a instância do BD está anormal.
Solução: se a instância de BD for anormal, reinicialize-a.

Figura 2-2 Verificar o status da instância de BD

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

2. **Verifique se a conexão do cliente está correta.**
Instale um **cliente de MySQL 8.0**.
Para obter detalhes sobre como se conectar a uma instância de BD em uma rede privada ou pública, consulte **Um servidor externo pode acessar o banco de dados do TaurusDB?**

Tabela 2-1 Modelo de conexão

Método de conexão	Cenário	Exemplo
Rede privada	Um endereço IP privado é fornecido por padrão. Se suas aplicações forem implementadas em um ECS que esteja na mesma região e VPC que a instância de BD, conecte-se ao ECS e à instância de BD por meio de um endereço IP privado.	mysql -h <i>private IP address</i> -P 3306 -u root -p --ssl-ca=/tmp/ca.pem Vá para a página Basic Information da instância e visualize o endereço IP privado na área Network Information .
Rede pública	Se não for possível acessar a instância de BD por meio de um endereço IP privado, vincule um EIP à instância de BD e, em seguida, conecte-se à instância de BD por meio do EIP. Para obter detalhes de preços do EIP, consulte Detalhes de cobrança do EIP .	mysql -h <i>EIP</i> -P 3306 -u root -p --ssl-ca=/tmp/ca.pem Vá para a página Basic Information da instância e visualize o EIP na área Network Information .

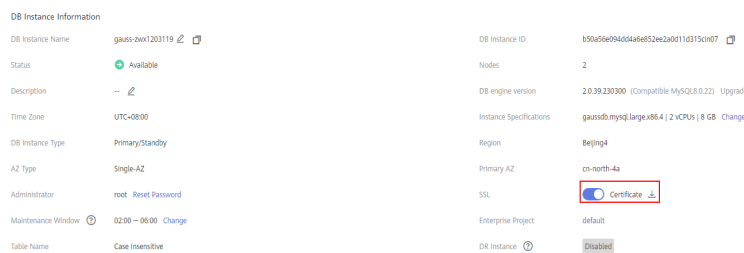
3. **Verifique se a conexão SSL é usada.**

- (Recomendado) Ative o SSL na página **Basic Information** da instância, faça download e descompacte o pacote e carregue o certificado raiz **ca.pem** no diretório **/tmp** do ECS.

Exemplo:

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

Figura 2-3 Ativação de SSL



- Conexão comum: desative o SSL na página **Basic Information**.

Exemplo:

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

4. **Verifique os parâmetros no comando usado para conectar.**

Certifique-se de que o endereço de conexão, a porta, o nome de usuário e a senha e o certificado SSL estejam corretos e tente se conectar à instância de banco de dados novamente.

- **Conexão a uma instância de BD por meio de uma rede privada**
 - Comando de conexão

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

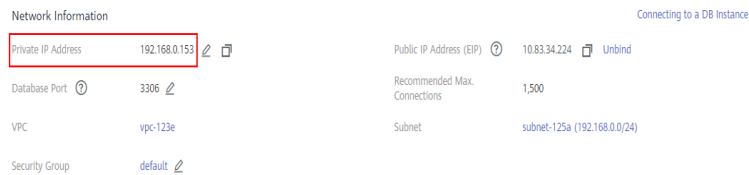
Exemplo:

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

- *connection address*

Vá para a página **Basic Information** da instância e visualize o endereço IP privado na área **Network Information**.

Figura 2-4 Endereço IP privado



- *database port*

Vá para a página **Basic Information** da instância e visualize a porta do banco de dados na área **Network Information**.

- *Username*

Digite **root** e sua senha.

- *SSL certificate name*

Nome do arquivo de certificado SSL. O caminho e o nome do arquivo devem ser os mesmos do comando.

- **Conexão a uma instância de BD em uma rede pública**

- *Comando de conexão*

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

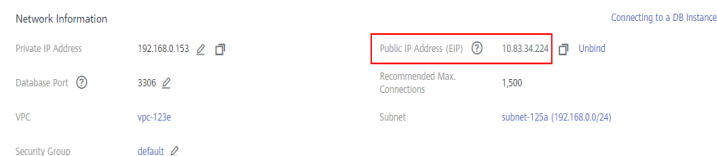
Exemplo:

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

- *EIP*

Vá para a página **Basic Information** da instância e visualize o EIP na área **Network Information**.

Figura 2-5 EIP



- *Porta do banco de dados*

Vá para a página **Basic Information** da instância e visualize a porta do banco de dados na área **Network Information**.

- *Nome do usuário e senha*

Certifique-se de ter inserido a senha de raiz corretamente.

- Certificado

Digite o nome do arquivo de certificado SSL. O caminho e o nome do arquivo devem ser os mesmos do comando.

5. **Verifique se a conexão de rede está normal.**

Conexão de rede privada

a. Verifique se o ECS e a instância do BD estão na mesma região e VPC.

- Se o ECS e a instância de BD estiverem em regiões diferentes, eles não poderão se comunicar entre si. Selecione uma região próxima à sua área de serviço para reduzir a latência da rede e obter acesso mais rápido. Para se conectar à instância de banco de dados entre regiões, use o Cloud Connect (CC) ou a Virtual Private Network (VPN).
- Se o ECS e a instância de banco de dados estiverem em VPCs diferentes da mesma região, eles não poderão se comunicar por meio de uma rede privada. Depois que uma instância de banco de dados é criada, você não pode alterar sua VPC. Nesse caso, crie uma conexão de emparelhamento de VPC. Para mais detalhes, consulte [O que devo fazer se uma instância do ECS e do TaurusDB implementada em VPCs diferentes não puder se comunicar entre si?](#).

Figura 2-6 Verificar a VPC de um ECS

ECS Information




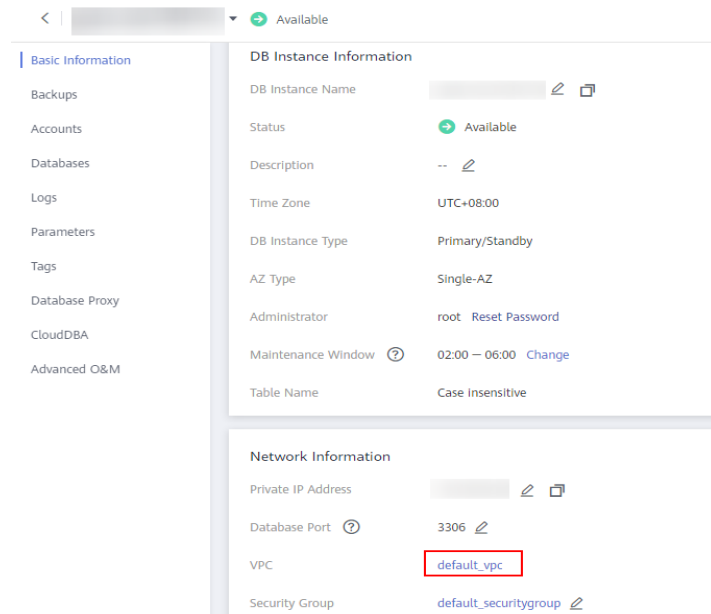
ID	37144dd6-2d7f-42c4-92bd-e6e1003361e8
Name	ecs-5948 
Description	-- 
Region	
AZ	AZ3
Specifications	General computing 1 vCPU 1 GiB sn3.small.1
Image	CentOS 8.2 64bit Public image
VPC	default_vpc

Figura 2-7 Verificar a VPC de uma instância de TaurusDB



- b. Verifique as regras do grupo de segurança.
- Se **Destination** não for **0.0.0.0/0** e **Protocol & Port** não for **All** na página **Outbound Rules** do ECS, adicione o endereço IP privado e a porta da instância de banco de dados às regras de saída.

Figura 2-8 Grupo de segurança do ECS

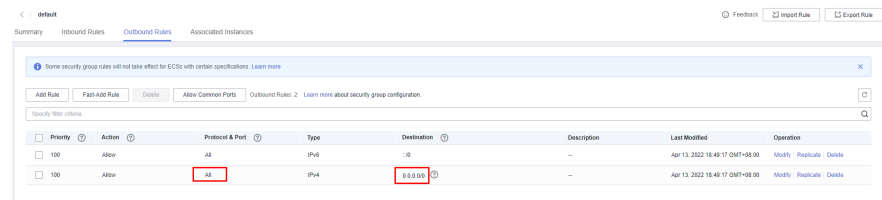


Figura 2-9 Adição rápida de uma regra de saída (endereço IP privado de uma instância de BD)

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: IPv4

* Source: IP address

Action:

Figura 2-10 Adição de uma regra de saída (endereço IP privado de uma instância 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	3306	IP address		Replicate Delete

- Adicione o endereço IP privado e a porta do ECS às **regras de entrada**.

Figura 2-11 Adição rápida de uma regra de entrada (endereço IP privado de um ECS)

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: **Allow** Deny

OK Cancel

Figura 2-12 Adição de uma regra de entrada (endereço IP privado de um ECS)

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

i 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

+ Add Rule

OK Cancel

- c. No ECS, verifique se o endereço IP privado da instância de banco de dados pode ser conectado.

telnet private IP address

Exemplo:

telnet 192.168.0.153 3306

- Se a conexão for normal, a rede é normal.
- Se a conexão falhar, **crie um tíquete de serviço** para entrar em contato com o atendimento ao cliente para obter assistência.

Conexão de rede pública

- a. Verifique as regras do grupo de segurança.
- Se **Destination** não for **0.0.0.0/0** e **Protocol & Port** não for **All** na página **Outbound Rules** do ECS, adicione o EIP e a porta da instância de banco de dados às regras de saída.

Figura 2-13 Grupo de segurança do ECS

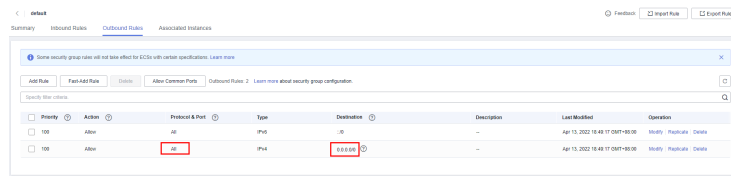


Figura 2-14 Adição rápida de uma regra de saída (instância de BD do EIP)

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:

* Source:

Action:

Figura 2-15 Adição de uma regra de saída (instância de BD do EIP)

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	3306	IP address		Replicate Delete

- Adicione o EIP e a porta do ECS às **regras de entrada**.

Figura 2-16 Adição de uma regra de entrada (EIP do ECS)

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 Adição de uma regra de entrada (EIP do ECS)

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

- b. Verifique as regras de ACL de rede.
 - i. Vá para **Network ACLs**.
 - ii. Verifique se a NIC à qual o TaurusDB e EIP vinculado pertence à sub-rede vinculada à ACL de rede.
 - iii. Verifique se a ACL de rede está ativada.

Se sim, **adicione uma regra ICMP para permitir o tráfego**.



A regra de ACL de rede padrão nega todos os pacotes de entrada e de saída. Essa regra padrão ainda é aplicada mesmo se a ACL da rede estiver desativada.

- c. Faça o ping da instância de banco de dados de um ECS na mesma região que a instância de banco de dados.

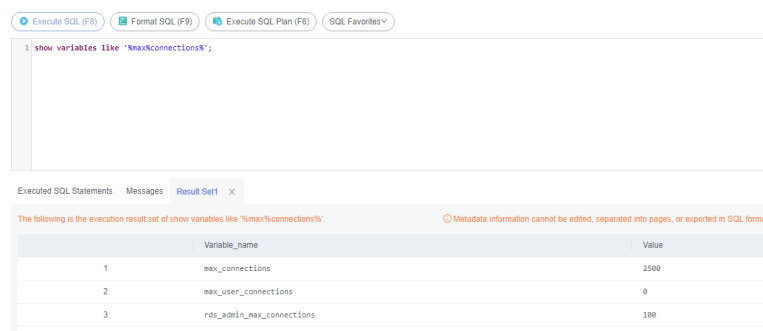
Se você não conseguir executar o ping do EIP da instância de banco de dados a partir de um ECS, tente fazer o ping a partir de outro ECS na mesma região. Se o EIP pode ser pingado, a rede é normal. Nesse caso, **crie um tíquete de serviço** para entrar em contato com o atendimento ao cliente.

6. Verifique se há muitas conexões com a instância de BD.

Método de verificação:

- a. **Faça login no console de gerenciamento.**
- b. Clique em  no canto superior esquerdo e selecione uma região e um projeto.
- c. Clique em  no canto superior esquerdo da página, escolha **Databases > TaurusDB**.
- d. Na página **Instances**, localize a instância de BD e clique em **Log In** na coluna **Operation**.
- e. Digite a senha e clique em **Test Connection**. Depois que a conexão for bem-sucedida, clique em **Log In** para acessar o DAS.
- f. Escolha **SQL Operations > SQL Query**.
- g. Digite o comando e clique em **Execute SQL** para verificar o número de conexões de instância.

show variables like '%max%connections%';



- **max_connections**: o número máximo de clientes que podem ser conectados ao mesmo tempo. Se este parâmetro for definido como **default**, o número máximo de clientes dependerá da quantidade de memória configurada. Para mais detalhes, consulte [Qual é o número máximo de conexões em uma instância do TaurusDB?](#)
 - **max_user_connections**: o número máximo de conexões simultâneas permitidas para uma conta específica do TaurusDB.
- h. Verifique se o total de conexões e as conexões ativas atuais atingiram os limites superiores, consultando [Visualização de métricas de monitoramento de instâncias](#). Determine se as conexões devem ser liberadas.

Possível causa: se houver muitas conexões de banco de dados, as aplicações podem não conseguir se conectar e os backups completos e incrementais podem falhar, afetando os serviços.

Solução:

- a. Verifique se as aplicações estão conectadas, otimize as conexões e libere conexões desnecessárias.
- b. Se esse parâmetro for definido como **default**, você poderá ampliar a instância de BD para definir **max_connections** como um valor maior. Para obter detalhes, consulte [Alteração de vCPUs e memória de uma instância de BD](#).
- c. Verifique se alguma métrica é anormal e se algum alarme é gerado no console do Cloud Eye. O Cloud Eye monitora as métricas do banco de dados, como o uso da CPU, o uso da memória, o uso do espaço de armazenamento e as conexões do

banco de dados, e permite que você configure políticas de alarme para identificar riscos antecipadamente se algum alarme for gerado. Para obter detalhes sobre as métricas de monitoramento suportadas, consulte [Introdução a métricas do TaurusDB](#).

7. Exiba mensagens de erro de conexão comuns.

Quando você executa comandos para se conectar a uma instância de BD, a compreensão das mensagens de erro pode ajudar:

- ERROR 2013: perda de conexão com o servidor MySQL durante a consulta

Se os valores de **wait_timeout** e **interactive_timeout** forem muito pequenos, o cliente de TaurusDB desconectará automaticamente a conexão vazia de tempo limite. Para obter detalhes, consulte [Cliente desconectado automaticamente de uma instância de banco de dados](#).

- ERROR 1045 : acesso negado para o usuário 'root'@'192.168.0.30' (usando a senha: YES)

Verifique se a senha está correta e se o ECS tem permissão para se conectar à instância de banco de dados. Para obter detalhes, consulte ["Access denied" exibido durante a conexão com o banco de dados](#).

- Mensagem de erro "SSL routines: tls_early_post_process_client_hello:unsupported protocol"

Verifique a versão de TLS do TaurusDB e atualize a versão de TLS do cliente. Para obter detalhes, consulte [Falha na conexão SSL devido a versões inconsistentes de TLS](#).

- Erro relatado quando o JDBC é usado para conectar-se ao banco de dados: "unable to find certification path to requested target"

O pacote JAR de MariaDB é usado para se conectar ao banco de dados, que é um pouco diferente do pacote de driver oficial do MySQL. Para obter detalhes, consulte [Falha ao conectar-se a um banco de dados usando mariadb-connector no modo de SSL](#).

- 8. Se o problema persistir, [crie um tíquete de serviço](#).

2.2 Um servidor externo pode acessar o banco de dados do TaurusDB?

Uma instância vinculada a um EIP

Para uma instância que tenha sido vinculada a um EIP, você pode acessá-la por meio do EIP.

Para obter detalhes, consulte:

[Vinculação de um EIP](#)

Uma instância não vinculada a um EIP

- Habilite uma VPN em uma VPC e use a VPN para se conectar à instância do TaurusDB.
- Crie uma instância do TaurusDB e um TaurusDB na mesma VPC e acesse o TaurusDB por meio do TaurusDB.

Para obter detalhes, consulte:

[Conexão a uma instância de BD por meio de uma rede privada](#)

2.3 O que devo fazer se o número de conexões de banco de dados do TaurusDB atingir o limite superior?

O número de conexões de banco de dados indica o número de aplicações que podem ser conectadas simultaneamente a um banco de dados e é irrelevante para o número máximo de usuários permitidos por suas aplicações ou sites.

Se houver um número excessivo de conexões de banco de dados, as aplicações poderão falhar ao serem conectadas e os backups completos e incrementais poderão falhar, afetando os serviços.

Localização de falhas

1. Verifique se as aplicações estão conectadas, otimize as conexões e libere conexões desnecessárias.
2. Verifique as especificações e amplie-as, se necessário.
3. Verifique se alguma métrica é anormal e se algum alarme é gerado no console do Cloud Eye. O Cloud Eye monitora as métricas do banco de dados, como o uso da CPU, o uso da memória, o uso do espaço de armazenamento e as conexões do banco de dados, e permite configurar políticas de alarme para identificar riscos antecipadamente se algum alarme for gerado. Para obter detalhes, consulte o *Guia de usuário do Cloud Eye*.

Solução

1. Conecte-se a uma instância por meio de uma rede privada. Usar uma rede privada evita o congestionamento causado por largura de banda insuficiente.
Para obter detalhes, consulte:
[Conexão de uma instância de BD em uma rede privada](#)
2. No console, defina o parâmetro `innodb_adaptive_hash_index` como `off` para reduzir o tempo de espera do bloqueio.
Para obter detalhes, consulte [Modificação de um modelo de parâmetro](#).
3. Otimize consultas lentas.

2.4 Qual é o número máximo de conexões em uma instância do TaurusDB?

TaurusDB não tem restrições sobre o número de conexões. Esse número é determinado pelo valor padrão e pelo intervalo de valores do mecanismo de banco de dados. Por exemplo, você pode definir `max_connections` e `max_user_connections` em um modelo de parâmetro para configurar o número máximo de conexões para uma instância do TaurusDB.

Alteração do número máximo de conexões

O número de conexões pode ser alterado on-line. Para obter detalhes, consulte [Modificação de um modelo de parâmetro](#).

Você pode executar comandos para alterar o número máximo de conexões.

1. Verifique o número máximo de conexões:
show global variables like 'max_connections';
2. Altere o valor de **max_connections** em **mysqld** no arquivo **my.cnf**.
[mysqld]
max_connections = 1000

Sobre max_connections

max_connections indica o número máximo de clientes que podem ser conectados ao mesmo tempo. Se este parâmetro for definido como **default**, ele está relacionado à memória da instância (unidade: GB). A fórmula de cálculo é a seguinte:

Valor estimado de max_connections = Memória disponível do nó/Memória estimada ocupada por uma única conexão

- Memória de nó disponível = Memória total – Memória ocupada pelo pool de buffers – 1 GB (processo mysqld, sistema operacional e programa de monitoramento)
- Uso estimado de memória de uma única conexão (**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

A tabela a seguir lista os valores padrão de **max_connections** para diferentes especificações de memória.

Tabela 2-2 Max_connections para diferentes especificações de memória

Memória (GB)	Conexões
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 O que devo fazer se um ECS não puder se conectar a uma instância do TaurusDB?

Execute as seguintes etapas para identificar o problema:

- Passo 1** Verifique se o ECS e a instância do TaurusDB estão localizados na mesma VPC.
- Se eles estiverem na mesma VPC, vá para [Passo 2](#).
 - Se eles estiverem em VPCs diferentes, crie um ECS na VPC onde a instância está localizada.
- Passo 2** Verifique se um grupo de segurança foi criado para o ECS.
- Se um grupo de segurança foi criado, verifique se suas regras são apropriadas. Para obter detalhes, consulte a descrição do grupo de segurança em "Criação de uma instância" em *Primeiros passos do TaurusDB*. Então, vá para [Passo 3](#).
 - Se nenhum grupo de segurança tiver sido criado, acesse o console da VPC na página de detalhes do ECS e crie um grupo de segurança.
- Passo 3** Verifique se o ECS pode se conectar à instância pela porta da instância.

A porta padrão de uma instância primária/em espera é **3306**.

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

- Se o ECS puder se conectar à instância, nenhuma ação adicional será necessária.
- Se o ECS ainda não puder se conectar à porta da instância, entre em contato com o suporte técnico.

----Fim

2.6 Como me conectar a um banco de dados MySQL por meio de JDBC?

Embora o certificado SSL seja opcional se você optar por se conectar a um banco de dados por meio de conectividade de banco de dados Java (JDBC), é aconselhável fazer o download do certificado SSL para criptografar as conexões para fins de segurança. Por padrão, a criptografia de dados SSL é ativada para instâncias de TaurusDB recém-criadas. A ativação do SSL aumentará o tempo de resposta da conexão de rede e o uso da CPU. Antes de ativar o SSL, avalie o impacto no desempenho do serviço. Para obter detalhes sobre como ativar ou desativar o SSL, consulte [Configuração de SSL](#).

Pré-requisitos

Familiarize-se com:

- Noções básicas de computação
- Linguagem de programação Java
- Conhecimento de JDBC

Conexão com o certificado SSL

O certificado SSL precisa ser baixado e verificado para conexão com bancos de dados.


NOTA

Se o valor `ssl_type` de um usuário de banco de dados for `x509`, esse método não estará disponível.

Para verificar o valor `ssl_type` do usuário atual, execute o seguinte comando:

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

Passo 1 Baixe o certificado de AC ou o pacote de certificados.

1. Na página **Instances**, clique no nome da instância para acessar a página **Basic Information**.
2. Na área **DB Instance Information**, clique em  ao lado de **SSL**.

Passo 2 Use keytool para gerar um arquivo truststore usando o certificado de AC.

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

Tabela 2-3 Descrição do parâmetro

Parâmetro	Descrição
<keytool installation path>	Diretório de bin no caminho de instalação JDK ou JRE, por exemplo, C:\Program Files (x86)\Java\jdk11.0.7\bin.
<MySQLCACert>	Nome do arquivo truststore. Defina-o com um nome específico para o serviço para identificação futura.
<ca.pem>	Nome do certificado de AC baixado e descompactado em Passo 1 , por exemplo, ca.pem .
<truststore_file>	Caminho para armazenar o arquivo truststore.
<password>	Senha do arquivo truststore.

Exemplo de código (usando keytool no caminho de instalação do JDK para gerar o arquivo 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
```

Passo 3 Conecte-se à instância do TaurusDB por meio de JDBC.

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

Tabela 2-4 Descrição do parâmetro

Parâmetro	Descrição
<instance_ip>	Endereço IP da instância de BD. NOTA <ul style="list-style-type: none"> ● Se você estiver acessando a instância por meio do ECS, <i>instance_ip</i> será o endereço IP privado da instância. Você pode visualizar o endereço IP privado na área Network Information em Basic Information. ● Se você estiver acessando a instância por meio de uma rede pública, <i>instance_ip</i> indicará o EIP vinculado à instância. Você pode visualizar o endereço IP privado na área Network Information em Basic Information.
<instance_port>	Porta do banco de dados da instância. A porta padrão é 3306 . NOTA Você pode visualizar o endereço IP privado na área Network Information em Basic Information .
<database_name>	Nome do banco de dados usado para conectar-se à instância. O valor padrão é mysql .
<value1>	Valor de requireSSL , indicando se o servidor suporta SSL. Pode ser uma das seguintes opções: <ul style="list-style-type: none"> ● true: o servidor suporta SSL. ● false: o servidor não suporta SSL. NOTA Para obter detalhes sobre a relação entre requireSSL e sslmode , consulte Tabela 2-5 .
<value2>	Valor de useSSL , indicando se o cliente usa SSL para se conectar ao servidor. Pode ser uma das seguintes opções: <ul style="list-style-type: none"> ● true: o cliente usa SSL para se conectar ao servidor. ● false: o cliente não usa SSL para se conectar ao servidor. NOTA Para obter detalhes sobre a relação entre useSSL e sslmode , consulte Tabela 2-5 .
<value3>	Valor de verifyServerCertificate , indicando se o cliente verifica o certificado do servidor. Pode ser uma das seguintes opções: <ul style="list-style-type: none"> ● true: o cliente verifica o certificado do servidor. ● false: o cliente não verifica o certificado do servidor. NOTA Para obter detalhes sobre a relação entre verifyServerCertificate e sslmode , consulte Tabela 2-5 .
<truststore_file>	Caminho para armazenar o arquivo truststore configurado em Passo 2 .
<password>	Senha do arquivo truststore configurado em Passo 2 .

Tabela 2-5 Relação entre parâmetros de conexão e 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

Exemplo de código (código Java para conexão com uma instância do TaurusDB):

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

public class JDBCtest {
    //There will be security risks if the username and password used for
    authentication are directly written into code. Store the username and password in
    ciphertext in the configuration file or environment variables.
    //In this example, the username and password are stored in the environment
    variables. Before running the code, set environment variables
    EXAMPLE_USERNAME_ENV and EXAMPLE_PASSWORD_ENV as needed.
    static final String USER = System.getenv("EXAMPLE_USERNAME_ENV");
    static final String PASS = System.getenv("EXAMPLE_PASSWORD_ENV");

    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 ....
    }
}
}
}

```

----Fim

Conexão sem o certificado SSL

NOTA

Você não precisa baixar o certificado SSL porque a verificação do certificado no servidor não é necessária.

Passo 1 Conecte-se à sua instância do TaurusDB por meio de JDBC.

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

Tabela 2-6 Descrição do parâmetro

Parâmetro	Descrição
<instance_ip>	Endereço IP da instância. NOTA <ul style="list-style-type: none"> Se você estiver acessando a instância por meio do ECS, <i>instance_ip</i> será o endereço IP privado da instância. Você pode visualizar o endereço IP privado na área Network Information em Basic Information. Se você estiver acessando a instância por meio de uma rede pública, <i>instance_ip</i> indicará o EIP vinculado à instância. Você pode visualizar o endereço IP privado na área Network Information em Basic Information.
<instance_port>	Porta do banco de dados da instância. A porta padrão é 3306 . NOTA Você pode visualizar o endereço IP privado na área Network Information em Basic Information .
<database_name>	Nome do banco de dados usado para conectar-se à instância. O valor padrão é mysql .

Exemplo de código (código Java para conexão com uma instância do 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");

```

```
//There will be security risks if the username and
password used for authentication are directly written into code. Store the
username and password in ciphertext in the configuration file or environment
variables.

//In this example, the username and password are stored
in the environment variables. Before running the code, set environment variables
EXAMPLE_USERNAME_ENV and EXAMPLE_PASSWORD_ENV as needed.
conn = DriverManager.getConnection(url,
System.getenv("EXAMPLE_USERNAME_ENV"), System.getenv("EXAMPLE_PASSWORD_ENV"));
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 ....
}
}
```

----Fim

Problemas relacionados

- Sintoma

Quando você usa o JDK 8.0 ou uma versão posterior para se conectar à sua instância com um certificado SSL baixado, um erro semelhante ao seguinte é relatado:

```
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
```

- Solução

Especifique os valores de parâmetro correspondentes no link de código de **Passo 3** com base no pacote JAR usado pelo cliente. Exemplo:

- 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 Como criar e me conectar a um ECS?

1. Para obter detalhes sobre como criar um TaurusDB, consulte *Guia de usuário do Elastic Cloud Server*.
 - O TaurusDB a ser criado deve estar na mesma VPC com a instância do TaurusDB à qual ele se conecta.
 - Configure um grupo de segurança para permitir que o TaurusDB acesse a instância por meio do endereço IP.
2. Para obter detalhes sobre como se conectar ao TaurusDB, consulte a seção "Fazer login em um TaurusDB" no *Guia de usuário do Elastic Cloud Server*.

2.8 O que devo fazer se um problema no cliente de banco de dados causar uma falha de conexão?

Verifique os itens a seguir para solucionar falhas de conexão do TaurusDB causadas por um problema do cliente:

1. Política de segurança do TaurusDB

No Windows, verifique se a porta da instância do TaurusDB está ativada na política de segurança do Windows. No Linux, execute **iptables** para verificar se a porta da instância do TaurusDB está ativada nas configurações de firewall.

2. Configuração da aplicação

Verifique se o endereço de conexão, a configuração do parâmetro de porta e a configuração do parâmetro de conexão JDBC estão corretos.

3. Nome do usuário ou senha

Verifique se o nome de usuário ou senha está correto se ocorrer um erro semelhante ao seguinte durante a conexão de banco de dados:

- [Warning] Access denied for user 'username'@'yourIp' (using password: NO)
- [Warning] Access denied for user 'username'@'yourIp' (using password: YES)

NOTA

Se o problema persistir, entre em contato com o suporte técnico pós-venda.

2.9 Por que não é possível executar o ping do meu EIP depois que ele está vinculado a uma instância de BD?

Localização de falhas

1. Verifique as regras do grupo de segurança.
2. Verifique as ACLs de rede.
3. Faça o ping do ECS na instância na mesma região.

Solução

1. Verifique as regras do grupo de segurança.
 - a. Na página **Instances**, clique no nome da instância para acessar a página **Basic Information**.
 - b. Na área **Network Information** da página **Basic Information**, clique no grupo de segurança.
 - c. Verifique se o grupo de segurança da NIC do ECS permite o tráfego ICMP de entrada.

Tabela 2-7 Regras de grupos de segurança

Direção	Tipo	Intervalo de protocolo/porta	Endereço IP de origem
Entrada	IPv4	Any: Any	0.0.0.0/0 (todos os endereços IP)
Entrada	IPv4	ICMP: Any	0.0.0.0/0 (todos os endereços IP)

2. Verifique as ACLs de rede.
 - a. Verifique o status da ACL da rede.
 - b. Verifique se a NIC à qual o EIP vinculado pertence à sub-rede vinculada à ACL de rede.
 - c. Se a ACL de rede estiver ativada, adicione uma regra ICMP para permitir o tráfego.

NOTA

A regra de ACL de rede padrão nega todos os pacotes de entrada e saída. Depois que a ACL da rede é desativada, a regra padrão ainda entra em vigor.

3. Faça o ping do EIP afetado de outro ECS na mesma região.

Se o EIP afetado puder ser pingado de outro ECS na mesma região, a rede virtual estará funcional. Nesse caso, entre em contato com o atendimento ao cliente para obter suporte técnico.

2.10 O que posso fazer se o teste de conexão falhou?

Localização de falhas

1. Verifique as regras do grupo de segurança.
2. Verifique as ACLs de rede.
3. Verifique as informações de NIC dos ECSs.
4. Verifique as portas desconectadas.

Solução

Passo 1 Na página **Instances**, clique no nome da instância para acessar a página **Basic Information**. Na área **Network Information** da página, visualize a VPC onde a instância está localizada.

Passo 2 Verifique se a instância à qual as transações distribuídas são adicionadas está na mesma VPC que um ECS.

- Se eles estiverem na mesma VPC, consulte [Por que há falha na comunicação entre dois ECSs na mesma VPC ou ocorre perda de pacotes quando eles se comunicam?](#)
- Se eles estiverem em VPCs diferentes:
 - Acesso público: vincule um EIP à instância. Para obter detalhes, consulte [Vinculação de um EIP](#).
 - Acesso privado: crie uma conexão de emparelhamento de VPC. Para obter detalhes, consulte [Visão geral da conexão de emparelhamento de VPC](#).
 - Altere a VPC que hospeda o ECS para a mesma que hospeda o TaurusDB. Para obter detalhes, consulte [Alteração de uma VPC](#).

----Fim

2.11 Posso acessar uma instância do TaurusDB por meio de uma conexão de intranet entre regiões?

Por padrão, as instâncias não podem ser acessadas por uma intranet entre regiões. Os serviços de nuvem em diferentes regiões não podem se comunicar entre si por meio de uma intranet. Você pode usar o Cloud Connect (CC) ou a Virtual Private Network (VPN) para se conectar a instâncias entre regiões.

- O CC permite que você conecte duas VPCs da mesma conta ou contas diferentes, mesmo que estejam em regiões diferentes. Para obter detalhes, consulte [Comunicação entre VPCs da mesma conta](#).
- A VPN usa um túnel criptografado para conectar VPCs em diferentes regiões e envia tráfego pela Internet. É barata, fácil de configurar e fácil de usar. No entanto, a qualidade das conexões de VPN depende da qualidade das conexões de Internet. Para obter detalhes, consulte [Conexão de um data center local a uma VPC por meio de uma VPN](#).

2.12 Existem riscos potenciais se houver muitas conexões com uma instância do TaurusDB?

Se houver um número excessivo de conexões do TaurusDB, as aplicações podem falhar ao serem conectadas e os backups completos e incrementais podem falhar, afetando os serviços.

Solução

1. Verifique se as aplicações estão conectadas, otimize as conexões e libere conexões desnecessárias.
2. O Cloud Eye monitora métricas do banco de dados, como o uso da CPU, o uso da memória, o uso do espaço de armazenamento e as conexões do banco de dados, e permite definir políticas de alarme para identificar riscos potenciais se algum alarme for gerado.

2.13 O que devo fazer se uma instância do ECS e do TaurusDB implementada em VPCs diferentes não puder se comunicar entre si?

Quando uma instância do TaurusDB e um ECS são implementados em diferentes VPCs da mesma região, eles não podem se comunicar uns com os outros por meio de uma rede privada. Depois que uma instância do TaurusDB é criada, você não pode alterar sua VPC.

Solução

1. Crie uma conexão de emparelhamento de VPC. Para obter detalhes, consulte [Visão geral da conexão de emparelhamento de VPC](#).
2. Altere a VPC que hospeda o ECS para a mesma que hospeda o TaurusDB. Para obter detalhes, consulte [Alteração de uma VPC](#).

2.14 Como visualizar todos os endereços IP conectados a um banco de dados?

Você pode executar a seguinte instrução SQL no banco de dados para consultar o número de endereços IP conectados:

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

3 Instalação do cliente

3.1 Como instalar o cliente de MySQL?

MySQL fornece pacotes de instalação de clientes para diferentes sistemas operacionais em seu site oficial. Baixe o [pacote de instalação do cliente de MySQL 8.0](#) ou [pacotes de outras versões](#). O seguinte usa o Red Hat Linux como um exemplo para mostrar como obter o pacote de instalação necessário e instalá-lo.

Procedimento

Passo 1 Obtenha o pacote de instalação.

Encontre o [link](#) para a versão necessária na página de download. O `mysql-community-client-8.0.21-1.el6.x86_64` é usado como um exemplo.

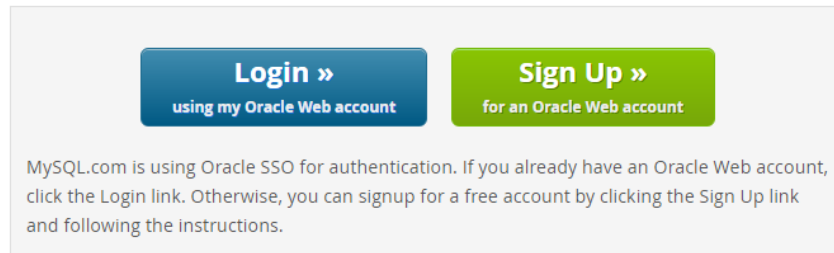
Figura 3-1 Download

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

Clique em **No thanks, just start my download.** para baixar o pacote de instalação.

Passo 2 Carregue o pacote de instalação para o TaurusDB.

NOTA

Ao criar um TaurusDB, selecione um sistema operacional, como o Red Hat 6.6, e vincule um EIP a ele. Em seguida, carregue o pacote de instalação para o TaurusDB usando uma ferramenta de conexão remota e use o PuTTY para se conectar ao TaurusDB.

Passo 3 Execute o seguinte comando para instalar o cliente de MySQL:

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

NOTA

- Se ocorrerem conflitos durante a instalação, adicione o parâmetro **replacefiles** ao comando e tente instalar o cliente novamente. Exemplo:

```
rpm -ivh --replacefiles mysql-community-client-8.0.21-1.el6.x86_64.rpm
```
- Se uma mensagem for exibida solicitando que você instale um pacote de dependência, você poderá adicionar o parâmetro **nodeps** ao comando e instalar o cliente novamente. Exemplo:

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

Passo 4 Use o cliente de MySQL para se conectar ao banco de dados e verificar se o cliente pode ser executado corretamente.

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

Tabela 3-1 Descrição do parâmetro

Parâmetro	Descrição
<hostIP>	Endereço IP privado. Para obter esse parâmetro, acesse a página Basic Information da instância e visualize o endereço IP privado na área Network Information .
<port>	Porta do banco de dados. Por padrão, o valor é 3306 . Para obter esse parâmetro, vá para a página Basic Information da instância e visualize a porta do banco de dados na área Network Information .
<userName>	Nome de usuário da conta de administrador do banco de dados do TaurusDB. O nome do usuário padrão é root .
<cafile>	Arquivo de certificado SSL, que deve ser armazenado no mesmo diretório onde o comando é executado.

Exemplo:

Para se conectar a uma instância de banco de dados por meio de uma conexão SSL como usuário **root**, execute o seguinte comando:

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

Digite a senha da conta do banco de dados conforme solicitado.

```
Enter password:
```

NOTA

Se informações de erro semelhantes a "mysql: error while loading shared libraries: libxxxx: cannot open shared object file: No such file or directory" forem exibidas, execute as seguintes etapas:

Por exemplo, se o erro "mysql: error while loading shared libraries: libtinfo.so.5: cannot open shared object file: No such file or directory" for exibido,

1. Consulte o arquivo de versão atual da biblioteca dinâmica que relata o erro no host local.

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

Suponha que o resultado da consulta seja o seguinte:

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

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

2. Configure o link simbólico da versão necessária.

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

3. Conecte-se ao banco de dados novamente.

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

----Fim

4 Migração de banco de dados

4.1 Que tipos de mecanismos de banco de dados o TaurusDB suporta para importar dados?

- A exportação ou importação de dados entre mecanismos de BD do mesmo tipo é chamada de exportação ou importação de banco de dados homogêneo.
- A exportação ou importação de dados entre mecanismos de banco de dados de diferentes tipos é chamada de exportação ou importação de banco de dados heterogêneo. Por exemplo, importe dados do Oracle para os mecanismos de banco de dados suportados pelo TaurusDB.

Geralmente, os dados não podem ser exportados ou importados entre bancos de dados heterogêneos devido aos diferentes formatos de dados envolvidos. No entanto, se os formatos de dados forem compatíveis, os dados da tabela podem, em teoria, ser migrados entre eles.

Software de terceiros é geralmente necessário para replicação de dados para exportação e importação entre bancos de dados heterogêneos. Por exemplo, você pode usar uma ferramenta de terceiros para exportar registros de tabela do Oracle no formato .txt. Em seguida, você pode usar as instruções Load para importar os registros da tabela exportada para os mecanismos de banco de dados suportados pelo TaurusDB.

5 Permissões do banco de dados

5.1 O TaurusDB fornece a conta raiz ou a superpermissão?

TaurusDB fornece ao usuário administrador **root** que tem permissões exceto super, arquivo, desligamento e criação de espaço de tabela.

A maioria das plataformas de serviços de banco de dados em nuvem não fornece a superpermissão para o usuário **root**. As superpermissões permitem que os usuários executem muitos comandos de gerenciamento, como reset master, set global, kill e reset slave. Essas operações podem causar exceções e falhas imprevisíveis para TaurusDB. Esta é uma grande diferença entre bancos de dados em nuvem e bancos de dados MySQL locais. Para garantir a execução estável de instâncias, o TaurusDB não fornece a superpermissão para o usuário **root**.

Se você precisa executar ações que normalmente exigem superpermissões, o TaurusDB fornece métodos alternativos.

Por exemplo:

Você pode modificar valores de parâmetros somente no console do TaurusDB. Você não pode executar o seguinte comando em um banco de dados para modificar valores de parâmetro.

```
set global parameter name=Parameter value;
```

Se o script contiver o comando **set global**, exclua o comando **set global** e modifique os valores dos parâmetros no console.

Um erro é relatado depois de executar o seguinte comando porque o usuário **root** não tem superpermissões. Você pode excluir **definer='root'** do comando.

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

Você pode importar e exportar dados usando mysqldump. Para obter detalhes, consulte [Migração de dados para o TaurusDB usando o mysqldump](#).

6 Desempenho do banco de dados

6.1 O que devo fazer se o uso da CPU da minha instância for alto?

Se o uso da CPU for alto ou próximo a 100% quando você usar TaurusDB, o processamento de leitura/gravação de dados ficará mais lento, as conexões não poderão ser estabelecidas e erros serão relatados, interrompendo os serviços.

Solução

1. Verifique logs SQL lentos para consultas lentas e examine suas características de desempenho (se houver) para localizar a causa.
Para obter detalhes sobre como exibir logs do MySQL, consulte [Visualização de logs de consultas lentas](#).
2. Visualize o uso da CPU da sua instância do TaurusDB para facilitar a localização de problemas.
Para obter detalhes, consulte [Configuração de métricas exibidas](#).
3. Crie réplicas de leitura para descarregar a pressão de leitura do nó primário.
4. Adicione índices para campos associados em consultas de associação de várias tabelas.
5. Não use a instrução SELECT para fazer a varredura de todas as tabelas. Você pode especificar campos ou adicionar a condição WHERE.

6.2 Como lidar com instruções SQL lentas causadas por configurações de índice composto inapropriadas?

Cenário

Em sua instância, uma consulta SQL executada às 11:00 e que deveria levar 8 segundos levou mais de 30 segundos.

Possíveis causas

1. Verifique o uso da CPU. Neste exemplo, durante esse período, o uso da CPU da instância não aumentou acentuadamente e permaneceu baixo, portanto, sabemos que a consulta lenta não foi causada pelo alto uso da CPU.

Figura 6-1 Uso da CPU



2. Analise logs de consulta lentos gerados durante esse período. Neste exemplo, mostrado abaixo, havia várias instruções SQL que envolviam milhões de linhas sendo verificadas. Essas foram as instruções lentas. Mas nenhuma grande quantidade de dados foi inserida na tabela durante esse tempo, então sabemos que a execução lenta foi causada por configurações de índice ausentes ou incorretas. Ao executar **EXPLAIN**, você pode descobrir que o plano de execução da instrução SQL era a verificação completa da tabela.

Figura 6-2 Logs de consulta lenta

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	33.601752 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. Execute **SHOW INDEX FROM** na tabela da instância para verificar a cardinalidade das três colunas.

Figura 6-3 Cardinalidade do índice

```
***** 3. row *****
Table: ██████████
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: ██████████
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: ██████████
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
```

O campo **query_date** com a menor cardinalidade estava no primeiro lugar do índice composto, e o campo **group_id** com a maior cardinalidade estava no último lugar do índice composto. Além disso, a instrução SQL continha a consulta de intervalo do campo **query_date**. Como resultado, apenas o campo **query_date** foi indexado.

A instrução SQL só podia usar o índice da coluna **query_date**. Além disso, o otimizador pode ter selecionado a varredura de tabela completa durante a estimativa de custo porque a cardinalidade era muito pequena.

Um novo índice composto foi criado com o campo **group_id** no primeiro lugar e o campo **query_date** no último lugar. O tempo de consulta atendeu à expectativa.

Solução

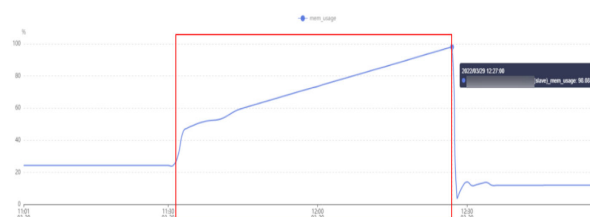
1. Verifique se a consulta lenta foi causada por recursos insuficientes da CPU.
2. Verifique se a estrutura da tabela foi projetada corretamente e se as configurações de índice estão corretas.
3. Execute a instrução **ANALYZE TABLE** periodicamente para evitar planos de execução incorretos, pois a execução de um grande número de operações **INSERT** ou **DELETE** para dados de tabela pode resultar em estatísticas desatualizadas.

6.3 Como lidar com um grande número de tabelas temporárias sendo geradas para transações longas e alto uso de memória?

Cenário

O uso de memória de uma instância do TaurusDB continuou aumentando das 11:30 às 12:27 e atingiu o limite de memória.

Figura 6-4 Uso da memória



Possíveis causas

1. Verifique o arquivo **processlist.log**. Neste exemplo, mostrado abaixo, havia duas instruções SQL lentas nesse período.

Figura 6-5 Instruções SQL lentas

```

2022-03-29 12:27:45 | @taurusdb | Query | 3811 | executing | select app_ver,pro_name,login_status,sum(case login_status when 'true' then 1 else 0 end)as success,sum(case login_status when 'false' then 1 else 0 end)as failed ,count(login_status),sum(case login_status when 'true' then 1 else 0 end) / count(login_status) from ( where login_status is not null and (date_format(pt_s, '%Y-%m-%d') BETWEEN '2022-03-11' AND '2022-03-28') group by app_ver
2022-03-29 12:27:45 | @taurusdb | Query | 3879 | executing | select app_ver,pro_name,login_status,sum(case login_status when 'true' then 1 else 0 end)as success,sum(case login_status when 'false' then 1 else 0 end)as failed ,count(login_status),sum(case login_status when 'true' then 1 else 0 end) / count(login_status) from ( where login_status is not null and (date_format(pt_s, '%Y-%m-%d') BETWEEN '2022-03-11' AND '2022-03-28') group by app_ver
  
```

2. Analise logs de consulta lentos gerados nesse período de tempo. Havia cerca de 90 GB de dados e cerca de 1 bilhão de linhas de dados nos logs, e havia duas instruções SQL que levavam de 40 a 50 minutos para serem executadas. O tempo de execução basicamente se sobrepôs quando o uso de memória subiu nos resultados de monitoramento, então sabemos que o alto uso de memória foi causado por tabelas temporárias.

```

mysql> explain select country, sum(.....)
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id | .. | .. | .. | .. | .. | .. | .. | .. | .. |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | .. | .. | .. | .. | .. | .. | .. | .. | .. |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Type | Index | .. | .. | .. | .. | .. | .. | .. | .. |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| S | .. | .. | .. | .. | .. | .. | .. | .. | .. |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Mem. | .. | .. | .. | .. | .. | .. | .. | .. | .. |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Mem. | .. | .. | .. | .. | .. | .. | .. | .. | .. |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Extra | .. | .. | .. | .. | .. | .. | .. | .. | .. |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 row in set (0.09 sec)

mysql> select table_name, table_size, data_length, index_length, free_innodb_buffers, where data_size.....
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| table_name | table_size | index_length | free_innodb_buffers | where data_size | .. | .. | .. | .. | .. |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| .. | .. | .. | .. | .. | .. | .. | .. | .. | .. |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| .. | .. | .. | .. | .. | .. | .. | .. | .. | .. |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
  
```

Solução

1. Atualize as especificações da instância para manter o uso da memória dentro de um intervalo adequado, evitando que um aumento repentino no tráfego cause uma falha em OOM. Para obter detalhes, consulte [Alteração de vCPUs e memória de uma instância de BD.](#)

2. Otimize instruções SQL lentas conforme necessário.

6.4 O que devo fazer se os bloqueios em transações longas bloquearem a execução de transações subsequentes?

Cenário

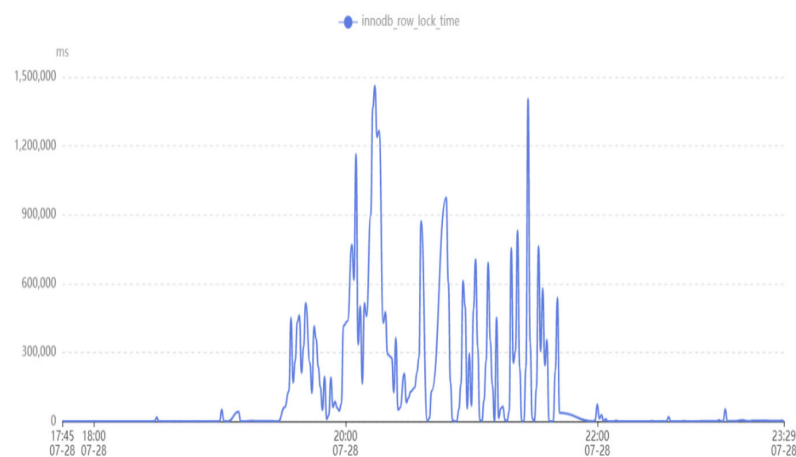
Foi relatado o código de erro 1205:

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

Possíveis causas

1. Verifique o valor da métrica de monitoramento **Row Lock Time**. Neste exemplo, o valor dessa métrica era alto, portanto sabemos que havia conflitos de bloqueio no sistema.

Para obter detalhes sobre métricas de monitoramento, consulte [Visualização de métricas de monitoramento de instâncias](#).



2. Faça login na instância de banco de dados e execute a seguinte instrução SQL para verificar as transações longas no sistema e os bloqueios de linha mantidos pelas transações:

```
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**: informações sobre transações que estão sendo executadas no InnoDB.
- **trx_started**: hora de início de uma transação, que é usada para determinar se a transação atual é uma transação longa. O tempo de execução de uma transação é a hora atual menos a hora de início.
- **trx_state**: status da transação atual. Os valores são os seguintes:
 - **RUNNING**
 - **LOCK WAIT**

📖 NOTA

Se o status de uma transação for **LOCK WAIT**, a transação manterá um bloqueio de linha.

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

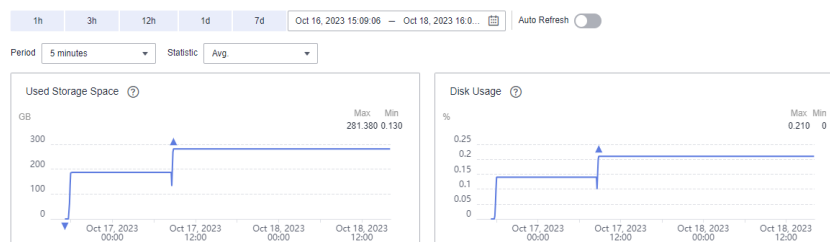
Solução

Elimine as transações longas.

6.5 Como usar o disco temporário do TaurusDB?

Discos temporários de instâncias do TaurusDB são usados para armazenar temporariamente tabelas temporárias, arquivos temporários e caches binlog gerados durante a operação do banco de dados. No console de gerenciamento, você pode monitorar o espaço em disco temporário usado e o uso temporário de disco da sua instância em diferentes períodos de tempo e granularidades em tempo real, conforme mostrado na figura a seguir.

Figura 6-6 Uso temporário do disco



À medida que os serviços flutuam, você pode descobrir que o uso de discos temporários aumenta repentinamente ou continuamente. Para melhorar a disponibilidade e estabilidade do banco de dados, o TaurusDB fornece até 500 GB de espaço em disco temporário para uma instância de banco de dados gratuitamente.

Para evitar que o uso temporário do disco aumente continuamente e, finalmente, fique cheio, é aconselhável verificar os serviços o mais rápido possível com base no uso do disco consultado. Esta seção descreve os riscos, cenários e solução de problemas que você pode executar quando os discos temporários estão cheios.

Riscos

- As instruções SQL falham ao serem executadas e nenhum resultado é retornado.
- Instruções SQL ocupam recursos de bloqueio por um longo tempo e bloqueiam outras instruções SQL. Como resultado, o número de conexões aumenta ou até atinge o limite superior, afetando outros serviços.
- Há muitos arquivos temporários no cache binlog, o que pode causar a quebra do banco de dados. Isso leva muito tempo para restaurar, então os serviços são interrompidos por um longo tempo.

Cenários e solução de problemas

1. Criação explícita de tabelas de disco temporárias

– Cenário

Você pode executar a instrução **create temporary table** para criar explicitamente tabelas de disco temporárias. As tabelas temporárias cujo mecanismo de armazenamento é o InnoDB são armazenadas em cache no pool de buffer e liberadas para os discos por threads sujas.

No TaurusDB, os dados em tabelas temporárias de disco são armazenados no espaço de tabela temporário de sessão (o caminho é especificado pelo parâmetro **innodb_temp_tablespaces_dir**), e os logs de desfazer são armazenados no espaço de tabela temporário global (o caminho é especificado pelo parâmetro **innodb_temp_data_file_path**).

Para evitar que tabelas de disco temporárias ocupem muito espaço em disco, é aconselhável excluir tabelas de disco temporárias desnecessárias ou desconectar conexões de banco de dados desnecessárias.

AVISO

- Espaço de tabela temporário da sessão: ele é recuperado quando a conexão de banco de dados atual é liberada.
- Espaço de tabela temporário global: ele é recuperado somente depois que o banco de dados é reiniciado.

– Solução de problemas

i. Visualize informações sobre as tabelas temporárias que você criou no InnoDB.

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

ii. Verifique o uso de arquivos de tabela temporários do InnoDB.

Em uma tabela, a coluna **ID** indica o ID da sessão que está usando o arquivo de tabela temporária. Se o valor for **0**, o arquivo ibt não será usado. A coluna **SIZE** indica o tamanho do arquivo ibt, que aumenta automaticamente com base no uso e é recuperado quando a sessão termina. Se o valor da coluna **PURPOSE** for **INTRINSIC**, a tabela é uma tabela temporária implícita. Se o valor da coluna **PURPOSE** for **USER**, a tabela é uma tabela temporária 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 tabelas temporárias de disco ou arquivos temporários criados implicitamente

– Cenário

Ao selecionar um plano de execução para uma consulta, o otimizador de consulta pode usar tabelas temporárias. Tabelas de memória temporárias são usadas preferencialmente. Quando o tamanho das tabelas de memória temporária excede um determinado limite (**tmp_table_size** ou **max_heap_table_size**, o que for menor), as tabelas de disco temporário são usadas.

Tabelas temporárias de disco são criadas implicitamente por consultas. Os dados entre tabelas que são criadas implícita e explicitamente são os mesmos e armazenados no espaço de tabela temporário de sessão. Se houver consultas complexas, incluindo, mas não limitadas a palavras-chave como UNION, GROUP BY e ORDER BY, em tabelas maiores, tabelas de disco temporárias podem ser geradas. Além disso, quando as consultas envolvem operações de classificação, se o buffer de classificação não puder armazenar todos os dados (o tamanho do buffer é especificado por **sort_buffer_size**), os arquivos de disco temporários podem ser usados para classificação auxiliar. Na maioria dos cenários, tabelas de disco temporárias implicitamente criadas são a principal razão pela qual os discos ficam cheios. Se o disco estiver ficando cheio, você poderá localizar consultas complexas ou transações longas, otimizar as instruções de consulta, adicionar índices adequados e dividir transações longas para resolver o problema.

– Solução de problemas

- i. Verifique se há instruções SQL usando tabelas temporárias ou classificação de arquivos.

Se **Using temporary** for exibido na coluna **Extra**, tabelas temporárias serão usadas. Se **Using filesort** for exibido, a classificação de arquivos será usada.

```

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. Consulte o uso de tabelas temporárias implícitas. O método é o mesmo das tabelas temporárias de disco explícito.

3. Consulta de binlogs gerados para transações longas

– Cenário

Um binlog é um binário que registra alterações no banco de dados, como DDL, DCL e DML (excluindo SELECT). O InnoDB armazena binlogs na memória antes

que as transações sejam confirmadas e grava binlogs em discos somente depois que as transações são confirmadas. O tamanho do arquivo binlog para cada conexão na memória é especificado pelo parâmetro **binlog_cache_size**. Quando o tamanho do arquivo binlog gravado por uma transação excede o valor desse parâmetro, o arquivo binlog é gravado em um arquivo de disco temporário. Transações longas podem causar grandes binlogs. Como resultado, o tamanho dos binlogs temporários no disco é grande e o disco pode estar cheio. É aconselhável controlar o tamanho da transação, dividir transações longas ou alterar **binlog_cache_size** para um valor mais apropriado.

– Solução de problemas

i. Verifique se o binlog está ativado.

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

ii. Veja o uso do cache do binlog.

Binlog_cache_disk_use indica o número de vezes que os arquivos de disco temporários são usados para armazenar em cache de binlogs devido à memória insuficiente (especificado por **binlog_cache_size**). Se o valor de **binlog_cache_size** for grande, os arquivos temporários de disco serão chamados para armazenar binlogs em cache várias vezes.

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

4. Verificação de arquivos temporários gerados por DDLs

– Cenário

Durante as operações DDL em tabelas, arquivos temporários de disco são gerados em algumas fases.

- Às vezes, você precisa recriar o espaço de tabela da tabela original, o que envolve a recriação do índice de árvore B+ na tabela. Se uma tabela contiver uma grande quantidade de dados, o buffer de classificação não poderá armazenar todos os dados. Você precisa criar um arquivo temporário para ajudar com a classificação.
- Embora algumas instruções DDL on-line suportem operações DML na tabela original, a tabela original não pode ser modificada diretamente. A modificação deve ser registrada em logs on-line e aplicada à nova tabela após a conclusão das operações DDL. Os logs on-line são preferencialmente armazenados na memória. O tamanho dos logs on-line é especificado pelo parâmetro **innodb_sort_buffer_size**. Se o tamanho dos logs on-line exceder o valor do parâmetro, os logs on-line serão armazenados temporariamente em um arquivo temporário.
- Quando a instrução **OPTIMIZE TABLE** é executada em uma tabela, os dados armazenados no índice clusterizado precisam ser reorganizados, o que pode gerar arquivos temporários.

– Solução de problemas

- Execute o comando **SHOW PROCESSLIST** para verificar se há instruções DDL que estão demorando muito para serem executadas.

- Certifique-se de que há espaço suficiente antes de executar DDLs para tabelas grandes.

7

Uso do banco de dados

7.1 Por que os resultados são inconsistentes depois que a instrução MATCH AGAINST é executada, respectivamente, em nós primários e réplicas de leitura?

MATCH AGAINST é usado para pesquisar índices de texto completo do MySQL. Para linhas na tabela, MATCH retorna valores de relevância, ou seja, uma medida de similaridade entre a cadeia de pesquisa (dada como o argumento da função AGAINST()) e o texto nessa linha nas colunas nomeadas na lista MATCH(). Esta instrução usa o valor `stat_n_rows` para calcular o valor de relevância. Os nós primários e as réplicas de leitura usam métodos diferentes para obter o valor de `stat_n_rows`. Os nós primários usam o método persistente e as réplicas de leitura usam o método transitório. Portanto, os valores obtidos são ligeiramente diferentes uns dos outros. O resultado da execução de MATCH AGAINST em nós primários e réplicas de leitura são diferentes.

7.2 Como adicionar colunas usando INSTANT?

TaurusDB é compatível com o MySQL 8.0.22 de código aberto, então você pode usar `ALGORITHM=INSTANT` para adicionar colunas rapidamente, evitando que o bloqueio de espera afete serviços ou o tempo limite de execução da instrução SQL.

Restrições

- As colunas só podem ser adicionadas em uma instrução. Se houver outras operações não-INSTANT na mesma instrução, as colunas não poderão ser adicionadas imediatamente.
- As colunas podem ser adicionadas somente no final das colunas existentes.
- O formato de linha COMPRESSED não é suportado.
- Tabelas que já têm índices de texto completo não são suportadas.

NOTA


Se uma tabela tiver um índice de texto completo, você deve executar a instrução `OPTIMIZE TABLE` na tabela depois de excluir o índice de texto completo.


- Tabelas temporárias não são suportadas.

- Um novo campo não pode ter um valor padrão.

Procedimento

Passo 1 [Faça logon no console de gerenciamento.](#)

Passo 2 Clique em  no canto superior esquerdo e selecione uma região e um projeto.

Passo 3 Clique em  no canto superior esquerdo da página, escolha **Databases** > **TaurusDB**.

Passo 4 Na página **Instances**, localize a instância e clique em **Log In** na coluna **Operation**.

Como alternativa, na página **Instances**, clique no nome da instância para acessar a página **Basic Information**. Clique em **Log In** no canto superior direito da página.

Passo 5 Na janela de logon exibida, insira o nome de usuário e a senha corretos e clique em **Log In**.

Passo 6 Na barra de menu superior, escolha **SQL Operations** > **SQL Query**.

Passo 7 Execute a seguinte instrução SQL para adicionar rapidamente uma coluna:

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

- *table_name*: nome da tabela
- *column_name*: nome da coluna
- *column_definition*: observações da coluna

----Fim

7.3 Como usar LOAD DATA para importar dados locais?

Você pode usar LOAD DATA para importar dados locais para o TaurusDB.

Sintaxe

```
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] ...)]
```

Parâmetros

- **file_name**: caminho do arquivo local a ser importado.
- **REPLACE | IGNORE**: se deve substituir ou ignorar registros duplicados.

- **tbl_name**: nome da tabela a ser importada.
- **CHARACTER SET charset_name**: formato de codificação do arquivo. É aconselhável usar o formato de codificação das instâncias do TaurusDB para evitar caracteres ilegíveis.
- **FIELDS TERMINATED BY 'string'**: separador entre colunas. O valor padrão é \t.
- **[OPTIONALLY] ENCLOSED BY 'char'**: usado para ignorar símbolos em campos de origem de dados.
- **LINES TERMINATED BY 'string'?**: caractere de nova linha entre linhas. O valor padrão é \n.

NOTA

Em alguns hosts que executam os servidores Windows, os caracteres de nova linha dos arquivos de texto podem ser \r\n, que é invisível.

- **IGNORE number LINES**: usado para ignorar linhas no início do arquivo.
- **(column_name_or_user_var, ...)**: colunas a serem importadas. Se esse parâmetro não estiver configurado, os dados serão importados com base na sequência de colunas por padrão.
- Para obter outros parâmetros, consulte o [arquivo de dados de carregamento](#) no site oficial do MySQL. A sequência de outros parâmetros deve estar correta. Para detalhes da sequência, visite [o site oficial do MySQL](#).

Exemplo padrão

Pré-requisitos

- O parâmetro **local_infile** deve ser ativado no servidor. Clique no nome da instância para acessar a página **Basic Information**. Na página **Parameters**, altere o valor deste parâmetro para **ON**.
- O parâmetro **local-infile** deve ser ativado no cliente. Configure **local-infile** no arquivo **my.cnf** ou use a opção **--local-infile=1** para se conectar ao banco de dados.

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

1. Importe os dados no arquivo local **qq.txt** para a tabela **test**. O arquivo **qq.txt** contém cinco linhas de dados. O separador de coluna é ',' e o separador de linha é '\n'.

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

2. Crie a tabela **test**.

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

3. No cliente, execute a instrução **LOAD DATA** para importar dados no arquivo **qq.txt** para a tabela **test**, defina o conjunto de caracteres como **utf8** e ignore as aspas duplas no campo de fonte de dados.

```
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. A importação de dados afeta o desempenho das instâncias do TaurusDB. Importe dados fora do horário de pico.
 2. Não inicie várias solicitações LOAD DATA ao mesmo tempo. Quando várias solicitações de LOAD DATA são iniciadas, as transações SQL podem ter um tempo limite devido a operações de gravação de dados altamente simultâneas, bloqueio de tabela e ocupação de I/O do sistema, resultando na falha de todas as solicitações de LOAD DATA.
-

8 Backups

8.1 Por quanto tempo o TaurusDB armazena dados de backup?

Os dados de backup automatizado são mantidos com base no período de retenção de backup especificado. Para obter detalhes, consulte a seção "Configuring an Automated Backup Policy" in *TaurusDB User Guide*.

Não há limite para o período de retenção de backup manual. For details, see section "Deleting a Manual Backup" in *TaurusDB User Guide*.

Os dados de backup são armazenados no TaurusDB e não ocupam o espaço de armazenamento do banco de dados.

8.2 Como limpar o espaço de backup do TaurusDB?

O espaço de backup do TaurusDB armazena backups automatizados e backups manuais.

- **Backups automatizados completos e incrementais**

Backups automatizados não podem ser excluídos manualmente. Para excluí-los, você pode ajustar o período de retenção especificado na política de backup. Os backups retidos serão excluídos automaticamente no final do período de retenção.

- **Backups completos manuais**

Você pode excluir manualmente os backups manuais. Para obter detalhes, consulte a seção "Exclusão de um backup manual" no *Guia de usuário do TaurusDB*.

8.3 Como fazer backup de um banco de dados do TaurusDB em um ECS?

Você pode fazer backup dos dados em um TaurusDB da mesma forma que exporta instruções SQL. O serviço TaurusDB não tem restrições sobre os tipos de dados a serem armazenados em backup, desde que os dados estejam em conformidade com as leis e regulamentos locais. Você pode armazenar dados de backup em um TaurusDB.


You are advised to store the data to TaurusDB for higher data reliability and service assurance.


8.4 Como ver o uso do armazenamento do meu backup?

Na área **Storage/Backup Space** da página **Basic Information** no console, você pode exibir o uso do espaço de backup.

Procedimento

Passo 1 **Faça login no console de gerenciamento.**

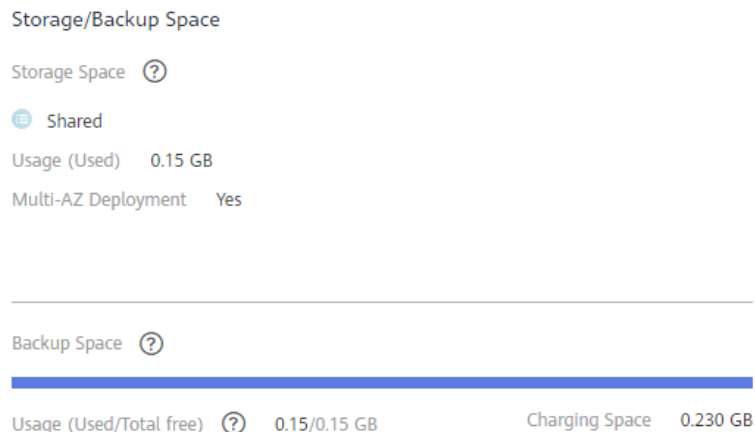
Passo 2 Clique em  no canto superior esquerdo e selecione uma região e um projeto.

Passo 3 Clique em  no canto superior esquerdo da página, escolha **Databases > TaurusDB**.

Passo 4 Na página **Instances**, clique no nome da instância para acessar a página **Basic Information**.

Passo 5 Na página **Basic Information**, exiba o uso do espaço de backup na área **Backup Space**.

Figura 8-1 Visualização do espaço de backup



NOTA

Há backups de dados e binlog de uma instância no espaço de backup.

Espaço de armazenamento de backup gratuito do mesmo tamanho que o espaço de armazenamento comprado é fornecido.

---Fim

8.5 Por que meu backup automatizado falhou?

Os backups automatizados podem falhar pelos seguintes motivos:

1. O ambiente de rede é instável devido a problemas como atraso ou interrupção da rede. TaurusDB irá detectar esses problemas e acionar outro backup automatizado meia hora depois. Você também pode executar um backup manual antes disso.
2. As execuções de várias tarefas são complicadas, resultando em problemas como espera de tarefas ou interrupções. TaurusDB irá detectar esses problemas e acionar outro backup automatizado meia hora depois. Você também pode realizar um backup manual.
3. Uma instância não está disponível, possivelmente porque a instância está com defeito ou sendo modificada. O TaurusDB acionará um backup automatizado quando o status da instância estiver disponível. Você também pode executar um backup manual antes disso.
4. Um parâmetro é alterado incorretamente. Por exemplo, uma instância pode se tornar defeituosa depois que um modelo de parâmetro contendo parâmetros incorretos foi aplicado a ela. Você pode verificar se os valores originais e atuais estão corretos, verificar se os parâmetros relacionados também precisam ser alterados, redefinir o modelo de parâmetro ou reinicializar a instância.
5. Ocorreu um erro durante a importação de dados.
Se os registros do catálogo do sistema forem perdidos devido à importação incorreta de dados, você poderá usar o DRS para importar os dados novamente.
6. Se o problema persistir, entre em contato com o suporte técnico.

8.6 Como os dados de backup do TaurusDB são cobrados?

Todos os backups do TaurusDB são armazenados no OBS sem ocupar o armazenamento de suas instâncias de banco de dados. TaurusDB fornece espaço livre de backup do mesmo tamanho que o armazenamento adquirido.

O ciclo de vida dos backups automatizados é o mesmo da instância de BD. Se você excluir uma instância de banco de dados, seus backups automatizados também serão excluídos, mas os backups manuais não serão excluídos automaticamente.

Por exemplo, se você comprar uma instância de banco de dados com 200 GB de armazenamento, poderá obter 200 GB adicionais de espaço de backup e só será cobrado pelos backups que excederem 200 GB. Os primeiros 200 GB de dados de backup são gratuitos. Quando o armazenamento de 200 GB for esgotado, os backups serão cobrados em uma base de pagamento por uso.

AVISO

Se o armazenamento estiver congelado, ele não será mais cobrado e o espaço livre de backup também estará indisponível.

Se sua instância de BD estiver congelada, nenhum espaço de backup livre estará disponível. Como resultado, os backups automatizados originais da instância de banco de dados serão cobrados.

- Se você descongelar a instância de BD, o espaço livre de backup será restaurado.
 - Se você excluir diretamente a instância de banco de dados congelada, seus backups automatizados também serão excluídos e o espaço de backup não será mais cobrado.
-


9 Modificação de parâmetro do banco de dados


9.1 Como alterar o fuso horário?

O TaurusDB permite que você selecione um fuso horário ao criar uma instância e altere o fuso horário após a criação da instância.

Procedimento

Passo 1 [Faça logon no console de gerenciamento.](#)

Passo 2 Clique em  no canto superior esquerdo e selecione uma região e um projeto.

Passo 3 Clique em  no canto superior esquerdo da página, escolha **Databases** > **TaurusDB**.

Passo 4 Na página **Instances**, clique no nome da instância.

Passo 5 No painel de navegação à esquerda, escolha **Parameters**.

Passo 6 Procure um parâmetro de fuso horário na caixa de pesquisa, por exemplo, **time_zone**.

Passo 7 Selecione um fuso horário e clique em **Save**.

Passo 8 Na caixa de diálogo exibida, clique em **OK**.

Por exemplo, para alterar o fuso horário para UTC+08:00, selecione **Asia/Shanghai** na lista suspensa.

----Fim

Parâmetros de fuso horário

- **system_time_zone**: fuso horário do sistema operacional (SO). A alteração do valor desse parâmetro não afeta o fuso horário do banco de dados.
- **time_zone**: fuso horário do banco de dados. Você pode modificar esse parâmetro para alterar o fuso horário da instância.

9.2 Como configurar uma política de expiração de senha para instâncias do TaurusDB?

No TaurusDB 8.0, você pode configurar a variável global **default_password_lifetime** para controlar o período de validade padrão de uma senha de usuário.

O valor de **default_password_lifetime** indica quantos dias até que uma senha expire. O valor padrão é **0**, indicando que a senha de usuário criada nunca expirará.

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

Alteração da política global de expiração automática de senha

- Altere o valor do parâmetro **default_password_lifetime** no console do TaurusDB. Para obter detalhes, consulte [Modificação de um modelo de parâmetro](#).
- Execute o seguinte comando para alterar o valor de **default_password_lifetime**:
`mysql> set global default_password_lifetime=0;`

Verificação da data de expiração da senha de todos os usuários

Execute o seguinte 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)
```

Verificação da política de expiração de senha de um usuário especificado

Execute o seguinte 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 ''1369F151659FC90255853119A9CBB0554DB007F' REQUIRE NONE PASSWORD EXPIRE DEFAULT ACCOUNT UNLOCK |
+-----+-----+
1 row in set (0.00 sec)
```

EXPIRE DEFAULT indica que a senha segue a política de expiração global.

Configuração da política de expiração de senha para um usuário específico

- Configurar a política de expiração de senha durante a criação do usuário
create user 'script'@'localhost' identified by '***' password expire interval 90 day;**
- Configurar a política de expiração de senha após a criação do usuário
ALTER USER 'script'@'localhost' PASSWORD EXPIRE INTERVAL 90 DAY;
- Configurar a senha para ser permanentemente válida
mysql> CREATE USER 'mike'@'%' PASSWORD EXPIRE NEVER;
mysql> ALTER USER 'mike'@'%' PASSWORD EXPIRE NEVER;
- Configurar a senha para seguir a política de expiração global
mysql> CREATE USER 'mike'@'%' PASSWORD EXPIRE DEFAULT;
mysql> ALTER USER 'mike'@'%' PASSWORD EXPIRE DEFAULT;


9.3 Como garantir que o conjunto de caracteres do banco de dados de uma instância do TaurusDB esteja correto?


UTF-8 suporta caracteres de 4 bytes, mas TaurusDB utf8 suporta apenas caracteres de 3 bytes. Emojis e caracteres Unicode recém-adicionados não podem ser armazenados usando o conjunto de caracteres MySQL utf8. O MySQL lançou o conjunto de caracteres utf8mb4 em 2010 e adicionou o código utf8mb4 após o 5.5.3 para ser compatível com o unicode de 4 bytes. Você só precisa mudar utf8 para utf8mb4. Nenhuma outra conversão é necessária.

O Data Admin Service (DAS) da Huawei Cloud é uma ferramenta profissional de gerenciamento de banco de dados. Você pode exibir os conjuntos de caracteres do banco de dados e do sistema por meio do console do DAS.

Procedimento

Passo 1 [Faça logon no console de gerenciamento.](#)

Passo 2 Clique em  no canto superior esquerdo e selecione uma região e um projeto.

Passo 3 Clique em  no canto superior esquerdo da página, escolha **Databases > TaurusDB**.

Passo 4 Na página **Instances**, localize a instância e clique em **Log In** na coluna **Operation**.

Como alternativa, na página **Instances**, clique no nome da instância para acessar a página **Basic Information**. Clique em **Log In** no canto superior direito da página.

Passo 5 Na janela de logon exibida, insira o nome de usuário e a senha corretos e clique em **Log In**.

Passo 6 Na barra de menu superior, escolha **SQL Operations > SQL Window**.

Passo 7 Execute a seguinte instrução SQL na janela de SQL para exibir o conjunto de caracteres do banco de dados:

```
show variables like '%character%';
```


Figura 9-1 Resultado da execução de SQL

The screenshot shows a SQL execution result window with the following table:

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...

Passo 8 Execute a seguinte instrução SQL na janela SQL para exibir a codificação do banco de dados:

show variables like 'collation%';

Figura 9-2 Resultado da execução de SQL

The screenshot shows a SQL execution result window with the following table:

Variable_name	Value
collation_connection	utf8mb4_general_ci
collation_database	utf8_general_ci
collation_server	utf8_general_ci

Passo 9 Altere o conjunto de caracteres para utf8mb4.

1. Execute a seguinte instrução SQL para alterar os conjuntos de caracteres do banco de dados.

ALTER DATABASE DATABASE_NAME DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;

2. Execute a seguinte instrução SQL para alterar os conjuntos de caracteres da tabela.

ALTER TABLE TABLE_NAME DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;

NOTA

A instrução SQL apenas altera os conjuntos de caracteres das tabelas. Os conjuntos de caracteres de campos nas tabelas não são alterados.

3. Execute a seguinte instrução SQL para alterar todos os conjuntos de caracteres de campo em tabelas:

ALTER TABLE TABLE_NAME CONVERT TO CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;

NOTA

- **character_set_client**, **character_set_connection** e **character_set_results** são as configurações do cliente.
- **character_set_system**, **character_set_server** e **character_set_database** são as configurações do servidor.
- As prioridades dos parâmetros no servidor são as seguintes: **character_set_database** > **character_set_server** > **character_set_system**.

----Fim

9.4 Como usar o conjunto de caracteres utf8mb4 para armazenar emojis em uma instância do TaurusDB?

Para armazenar emojis em uma instância do TaurusDB, certifique-se de que:

- O cliente gera o conjunto de caracteres utf8mb4.
- A conexão suporta o conjunto de caracteres utf8mb4. Se você deseja usar uma conexão JDBC, baixe o MySQL Connector/J 5.1.13 ou uma versão posterior e deixe **characterEncoding** indefinido para a cadeia de conexão JDBC.

- Configure a instância da seguinte forma:

- Definir **character_set_server** como **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.



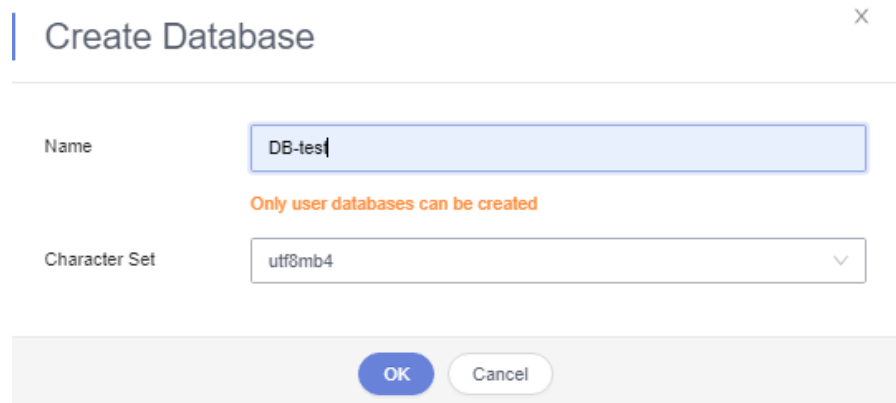
- Faça logon no console de gerenciamento.**
 - Clique em  no canto superior esquerdo e selecione uma região e um projeto.
 - Clique em  no canto superior esquerdo da página, escolha **Databases > TaurusDB**.
 - Na página **Instances**, clique no nome da instância.
 - No painel de navegação à esquerda, escolha **Parameters**. Na página de guia **Parameters**, localize **character_set_server** e altere seu valor para **utf8mb4**.
 - Clique em **Save**. Na caixa de diálogo exibida, clique em **Yes**.
- Selecionar **utf8mb4** para o conjunto de caracteres do banco de dados
 - Na página **Instances**, localize a instância e clique em **Log In** na coluna **Operation**.
Como alternativa, na página **Instances**, clique no nome da instância para acessar a página **Basic Information**. Clique em **Log In** no canto superior direito da página.
 - Na janela de logon exibida, insira o nome de usuário e a senha corretos e clique em **Log In**.
 - Na página **Databases**, clique em **Create Database**. Na caixa de diálogo exibida, insira um nome de banco de dados, selecione o conjunto de caracteres **utf8mb4** e autorize as permissões de banco de dados para os usuários. Em seguida, clique em **OK**.

Figura 9-3 Criação de um banco de dados



- Configurar o conjunto de caracteres da tabela para **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)
```

Perguntas frequentes

Se você tiver definido **characterEncoding** como **utf8** para a cadeia de conexão JDBC, ou os dados do emoji não puderem ser inseridos corretamente depois de executar as operações acima, é aconselhável definir o conjunto de caracteres de conexão como **utf8mb4** da seguinte maneira:

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

9.5 Como definir a sensibilidade de maiúsculas e minúsculas para nomes de tabela do TaurusDB?

Você pode especificar a sensibilidade de maiúsculas e minúsculas para nomes de tabela ao criar uma instância no console ou usar APIs. Isso não pode ser alterada depois que a instância é criada.

- Defina **Table Name Case Sensitivity** no console. Para obter detalhes, consulte [Compra de uma instância de BD](#).

Figura 9-4 Configuração de sensibilidade de maiúsculas e minúsculas para nomes de tabelas

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. Underneath, there is a 'Parameter Template' dropdown menu set to 'Default-GaussDB-for-MySQL 8.0' with a 'View Parameter Template' link. The 'Table Name' section has two radio buttons: 'Case sensitive' (unselected) and 'Case Insensitive' (selected), with a note: '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.

- Defina `lower_case_table_names` invocando uma API. Para obter detalhes, consulte [Criação de uma instância de BD](#).

Intervalo de valores:


- **0**: os nomes das tabelas diferenciam maiúsculas de minúsculas.
- **1** (valor padrão): os nomes das tabelas são armazenados em minúsculas e não diferenciam maiúsculas de minúsculas.


9.6 Posso usar comandos SQL para modificar parâmetros globais?

Desculpe, você não pode usar comandos SQL para modificar parâmetros globais, mas pode modificar parâmetros específicos no console.

Procedimento

Passo 1 [Faça logon no console de gerenciamento](#).

Passo 2 Clique em  no canto superior esquerdo e selecione uma região e um projeto.

Passo 3 Clique em  no canto superior esquerdo da página, escolha **Databases** > **TaurusDB**.

Passo 4 Na página **Instances**, clique na instância de BD de destino.

Passo 5 No painel de navegação à esquerda, escolha **Parameters**.

Passo 6 Altere o valor do parâmetro de destino e clique em **Save**.

Passo 7 Na caixa de diálogo exibida, clique em **OK**.

----Fim

10 Segurança de rede

10.1 Quais são as medidas de garantia de segurança do TaurusDB?

Rede

- TaurusDB permite configurar instâncias em uma VPC, garantindo que as instâncias sejam isoladas de outros serviços.
- O TaurusDB usa grupos de segurança para garantir que apenas fontes confiáveis possam acessar suas instâncias.
- TaurusDB suporta conexões SSL para criptografar dados durante a transmissão.

Gerenciamento

Você pode usar o [Identity and Access Management \(IAM\)](#) para gerenciar permissões do TaurusDB.

10.2 Como impedir que endereços IP de origem não confiáveis acessem o TaurusDB?

- Se você ativar a acessibilidade pública, seu DNS do EIP e a porta do banco de dados poderão estar vulneráveis a hackers. Para proteger informações como EIP, DNS, porta de banco de dados, conta de banco de dados e senha, é recomendável especificar o intervalo de endereços IP de origem no grupo de segurança do TaurusDB para garantir que apenas endereços IP de origem confiáveis possam acessar suas instâncias.
- Para evitar que a senha do seu banco de dados seja quebrada, especifique uma senha forte e altere-a periodicamente.

10.3 Como configurar um grupo de segurança para permitir o acesso a uma instância do TaurusDB?

- Ao tentar se conectar a uma instância do TaurusDB por meio de uma rede privada, verifique se o ECS e a instância do TaurusDB estão no mesmo grupo de segurança.
 - Se o ECS e a instância do TaurusDB estiverem no mesmo grupo de segurança, eles poderão se comunicar por padrão. Nenhuma regra de grupo de segurança precisa ser configurada.
 - Se o ECS e a instância do TaurusDB estiverem em grupos de segurança diferentes, configure as regras de grupo de segurança para o ECS e a instância, respectivamente.
 - Instância: configure uma **inbound rule** para o grupo de segurança ao qual a instância está vinculada.
 - ECS: a regra do grupo de segurança padrão permite todos os pacotes de dados de saída. Nesse caso, não é necessário configurar uma regra de grupo de segurança para o ECS. Se nem todo o tráfego de saída for permitido no grupo de segurança, talvez seja necessário configurar uma regra de saída para que o ECS permita todos os pacotes de saída.
- Quando você tenta acessar uma instância por meio de um EIP, precisa configurar uma **inbound rule** para o grupo de segurança vinculado à instância.

10.4 Como importar o certificado raiz para um servidor Windows ou Linux?

Importação do certificado raiz para um servidor Windows

1. Clique em **Start** e escolha **Run**. Na caixa de diálogo **Run** exibida, insira **MMC** e pressione **Enter**.
2. No console exibido, escolha **File > Add/Remove Snap-in**.
3. No painel esquerdo de **Available snap-ins** da caixa de diálogo exibida, selecione **Certificates**. Clique em **Add** para adicionar o certificado.
4. Na caixa de diálogo **Certificates snap-in** exibida, selecione **Computer account** e clique em **Next**.
5. Na caixa de diálogo **Select Computer** exibida, clique em **Finish**.
6. Na caixa de diálogo **Add or Remove Snap-ins**, clique em **OK**.
7. No console, clique duas vezes em **Certificates**.
8. Clique com o botão direito do mouse em **Trusted Root Certification Authorities** e escolha **All Tasks > Import**.
9. Clique em **Next**.
10. Clique em **Browse** para alterar o tipo de arquivo para **All Files (*.*)**.
11. Localize o certificado raiz baixado (um arquivo **ca.pem**) e clique em **Open**. Em seguida, clique em **Next**.

AVISO

Você deve alterar o tipo de arquivo para **All Files (*.*)** porque **.pem** não é um nome de extensão de certificado padrão.

12. Clique em **Next**.
13. Clique em **Finish**.
14. Clique em **OK** para concluir a importação do certificado raiz.

Importação do certificado raiz para um servidor Linux

Você pode usar uma ferramenta de conexão (como WinSCP ou PuTTY) para fazer upload do certificado para qualquer diretório em um servidor Linux.

10.5 Como gerenciar e garantir a segurança do TaurusDB?

Por motivos de segurança, não use o nome de usuário e a senha da sua conta da Huawei Cloud. Recomendamos que você crie usuários do IAM e outros usuários (se necessário) para os usuários do seu banco de dados.

Pode ocorrer um erro se você não tiver permissões suficientes ou se a configuração da sua conta estiver incorreta. Por exemplo, você não consegue criar instâncias se não tiver as permissões para isso. Se necessário, entre em contato com o administrador do IAM para atribuir as permissões

11 Gerenciamento de logs

11.1 Posso habilitar general_log para TaurusDB?

Não.


Se você precisar habilitar general_log para auditoria SQL completa e solução de problemas, você pode usar [SQL TOP](#) e [Insights SQL](#).


11.2 Como visualizar todos os logs SQL executados pelo TaurusDB?

Você pode usar o serviço de gerenciamento de banco de dados visualizado Data Admin Service (DAS) para pesquisar rapidamente os registros de execução SQL de destino.

Consulta de logs de SQL por meio do DAS

Passo 1 [Faça logon no console de gerenciamento.](#)

Passo 2 Clique em  no canto superior esquerdo e selecione uma região e um projeto.

Passo 3 Clique em  no canto superior esquerdo da página, escolha **Databases** > **TaurusDB**.

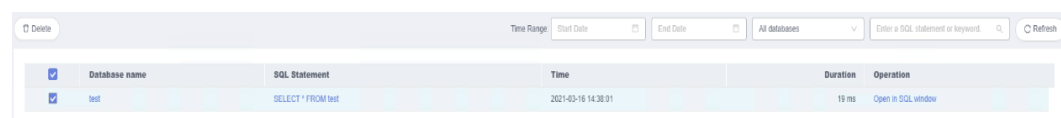
Passo 4 Na página **Instances**, localize a instância que deseja efetuar logon e clique em **Log In** na coluna **Operation**.

Passo 5 Na página de logon exibida, digite o nome de usuário e a senha corretos e clique em **Log In**.

Passo 6 Na barra de menu superior, escolha **SQL Operations** > **SQL History**.

Passo 7 Na página exibida, pesquise informações de execução sobre a instrução SQL de destino por intervalo de tempo, nome do banco de dados ou palavra-chave.

Figura 11-1 Histórico de SQL



Database name	SQL Statement	Time	Duration	Operation
test	SELECT * FROM test	2021-03-16 14:38:01	18 ms	Open in SQL window


- Para acessar a página **Database Management**, clique em um nome de banco de dados.
- Para copiar e usar uma instrução SQL, clique nela na coluna **SQL Statement**.
- Para executar uma instrução SQL, localize a instrução e clique em **Open in SQL Window** na coluna **Operation**.


----Fim

11.3 Como visualizar logs de consulta lenta do TaurusDB?

Visualização de detalhes do log

Passo 1 [Faça logon no console de gerenciamento.](#)

Passo 2 Clique em  no canto superior esquerdo e selecione uma região e um projeto.

Passo 3 Clique em  no canto superior esquerdo da página, escolha **Databases > TaurusDB**.

Passo 4 Na página **Instances**, clique no nome da instância para acessar a página **Basic Information**.

Passo 5 No painel de navegação à esquerda, escolha **Logs**.

Passo 6 Na página **Slow Query Logs**, exiba os detalhes do log de consulta lenta.

Você pode visualizar os registros de log de consultas lentas de um tipo de instrução de execução especificado ou de um período de tempo específico.


----Fim


11.4 Como ativar e visualizar o binlog da minha instância do TaurusDB?

Ativação do binlog

TaurusDB não suporta ativar binlog para réplicas de leitura. Para obter detalhes sobre como ativar o binlog para o nó primário, execute as seguintes etapas:

Passo 1 [Faça logon no console de gerenciamento.](#)

Passo 2 Clique em  no canto superior esquerdo e selecione uma região e um projeto.

Passo 3 Clique em  no canto superior esquerdo da página, escolha **Databases > TaurusDB**.

Passo 4 Clique no nome da instância para acessar a página **Basic Information**.

Passo 5 No painel de navegação à esquerda, escolha **Parameters**.

Passo 6 Configure os parâmetros da seguinte forma:

- Se a versão do kernel for anterior a 2.0.45.230900, procure o parâmetro **log-bin**, selecione **ON** na caixa de listagem suspensa na coluna **Value** e clique em **Save**. O valor do parâmetro modificado é aplicado somente após a reinicialização da instância de banco de dados.

NOTA

Para exibir a versão do kernel, clique no nome da instância para acessar a página **Basic Information**. Na área **DB Instance Information**, exiba o campo **DB Engine Version**.

Figura 11-2 Visualização da versão do kernel



- Se a versão do kernel for 2.0.45.230900 ou posterior, pesquise o parâmetro **rds_global_sql_log_bin**, selecione **ON** na caixa de listagem suspensa na coluna **Value** e clique em **Save**. O valor do parâmetro modificado é aplicado imediatamente. Você não precisa reinicializar a instância de BD.

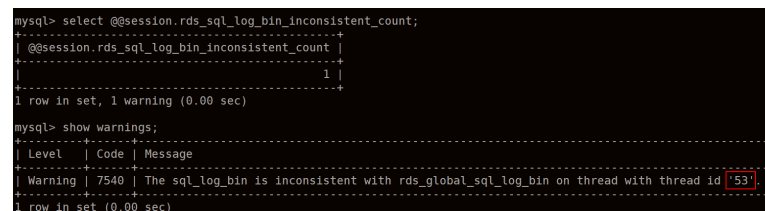
Depois que esse parâmetro for alterado, conecte-se ao banco de dados e execute o seguinte comando para verificar se o binlog está ativado para todos os threads:

select @@session.rds_sql_log_bin_inconsistent_count;

- Se a saída do comando for 0, o binlog está ativado com sucesso para todos os threads e todas as instruções podem ser registradas no binlog.
- Se o comando de saída não for 0, execute o seguinte comando para verificar os IDs dos threads para os quais o binlog não está ativado:

show warnings;

Figura 11-3 Consulta dos IDs dos threads para os quais o binlog não está ativado



As instruções executadas nos IDs de thread consultados não podem ser registradas no binlog temporariamente.

Verifique seus serviços com base nos IDs de thread obtidos (por exemplo, **53** em **Figura 11-3**), envie ou reverta transações e execute novas transações (por exemplo, **SELECT 1;**) em tempo hábil com base nos requisitos de serviço ou desconecte conexões ociosas e reconecte-as.

----Fim

Visualização de arquivos de binlog

Passo 1 Conecte-se a uma instância. Para obter detalhes, consulte [Conectar-se a uma instância de banco de dados](#).

Passo 2 Execute o seguinte comando para exibir arquivos de binlog:

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

 **NOTA**

Se uma mensagem indicando que as permissões da conta são insuficientes, use a conta **root**.

----**Fim**

Impacto da ativação do binlog no desempenho do TaurusDB

A ativação do binlog não afeta as operações SELECT, mas afeta INSERT, UPDATE, DELETE e outras operações de gravação.

 **NOTA**


Não há diferenças significativas entre o binlog do TaurusDB e o binlog do MySQL de código aberto. A sintaxe de binlog do TaurusDB é totalmente compatível com a do MySQL de código aberto.


11.5 Como alterar o período de retenção do binlog?

TaurusDB é compatível com o parâmetro **binlog_expire_logs_seconds** da versão 8.0 da comunidade. Você pode alterar o período de retenção do binlog usando esse parâmetro.

Procedimento

Passo 1 [Faça login no console de gerenciamento.](#)

Passo 2 Clique em  no canto superior esquerdo e selecione uma região e um projeto.

Passo 3 Clique em  no canto superior esquerdo da página, escolha **Databases** > **TaurusDB**.

Passo 4 Na página **Instances**, clique no nome da instância para acessar a página **Basic Information**.

Passo 5 No painel de navegação, escolha **Parameters**. Na guia **Parameters**, exiba os seguintes parâmetros.

- Se a versão do kernel for anterior a 2.0.45.230900, procure o parâmetro **log-bin**. Se o valor do parâmetro for **ON**, o binlog será ativado.
- Se a versão do kernel for 2.0.45.230900 ou posterior, procure o parâmetro **rds_global_sql_log_bin**. Se o valor do parâmetro for **ON**, o binlog será ativado.

 **NOTA**

Para exibir a versão do kernel, clique no nome da instância para acessar a página **Basic Information**. Na área **DB Instance Information**, exiba o campo **DB Engine Version**.

Figura 11-4 Visualização da versão do kernel



Passo 6 Na guia **Parameters**, configure **binlog_expire_logs_seconds**.

 **NOTA**

- Quando um novo arquivo binlog é gerado, todos os arquivos binlog existentes que expiraram serão excluídos.
- Se nenhum novo arquivo binlog for gerado, os arquivos binlog históricos não serão excluídos mesmo que tenham expirado. Para excluir arquivos binlog manualmente, conecte-se ao banco de dados e execute **flush logs**; para forçosamente gerar um novo arquivo binlog.


----Fim


11.6 Como visualizar os logs de deadlock do TaurusDB?

Os logs de deadlock do banco de dados não são registrados nos logs de erro. Para exibir logs de deadlock, use o Data Admin Service (DAS), uma ferramenta de gerenciamento de banco de dados visualizada e profissional, para executar rapidamente instruções SQL.

Procedimento

Passo 1 **Faça logon no console de gerenciamento.**

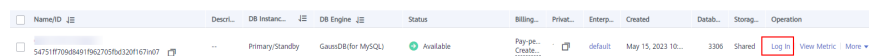
Passo 2 Clique em  no canto superior esquerdo e selecione uma região e um projeto.

Passo 3 Clique em  no canto superior esquerdo da página, escolha **Databases > TaurusDB**.

Passo 4 Na página **Instances**, localize a instância que deseja efetuar logon e clique em **Log In** na coluna **Operation**.

Passo 5 Na janela de logon exibida, insira o nome de usuário e a senha corretos e clique em **Log In**.

Figura 11-5 Efetuar logon em uma instância



Name	Descr...	DB Instanc...	DB Engine	Status	Billing...	Privat...	Enterp...	Created	Datab...	Storag...	Operation
54751f70968491f962795fb320f167607		Primary/Standby	GaussDB(for MySQL)	Available	Pay as-Create...		default	May 15, 2023 10...	3306	Shared	Log In View Metric More

Passo 6 Selecione o banco de dados de destino e clique em **SQL Operations > SQL Window**.

Passo 7 Na janela SQL exibida, execute **show engine innodb status** para exibir os logs de deadlock mais recentes do banco de dados selecionado. Use a palavra-chave **LATEST DETECTED DEADLOCK** para localizar os logs de deadlock mais recentes. Os últimos logs de deadlock substituirão os históricos.

----Fim

12 Atualização de versão

12.1 Como verificar uma versão de instância do TaurusDB?

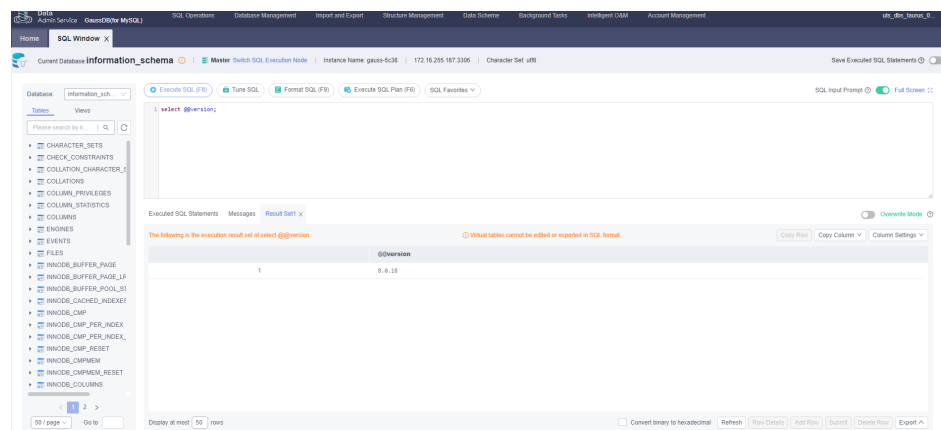
- Na página **Basic Information** da instância de destino, exiba a versão da instância.

Figura 12-1 Visualização das informações básicas da instância

DB Instance Information			
DB Instance Name	gauss	DB Instance ID	bfi0ede6894043d9a029136cc3db31e4in07
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 Change	Region	Beijing4
AZ Type	Single-AZ	Primary AZ	cn-north-4b
Administrator	root Reset Password	SSL	Certificate ↓
Maintenance Window	02:00 – 06:00 Change	Enterprise Project	default

- No console do DAS, execute as seguintes etapas para exibir a versão da instância de destino:
 - a. Efetue logon na instância de destino.
 - b. Na barra de menu superior, escolha **SQL Operations > SQL Query**.
 - c. Execute **select @@version;** para ver a versão da instância.

Figura 12-2 Visualização da versão da instância



12.2 Posso atualizar as versões de instâncias do TaurusDB?

Você pode atualizar manualmente versões secundárias de suas instâncias para melhorar o desempenho, adicionar novas funções e corrigir bugs.

As réplicas de leitura são atualizadas antes do nó primário.

Para obter mais informações sobre as operações de atualização, consulte [Atualização de uma versão secundária](#).