## Document Database Service

# Primeiros passos

**Edição** 01

**Data** 15-12-2022

**HUAWEI TECHNOLOGIES CO., LTD.**

## Marcas registadas e permissões


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

## Aviso

Os produtos, serviços e funcionalidades adquiridos são estipulados pelo contrato feito entre a Huawei e o cliente. Todos ou parte dos produtos, serviços e funcionalidades descritos neste documento pode 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 ESTÁ" sem garantias, ou representações de qualquer tipo, seja expressa ou implícita.

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.

# Índice



# 1 Visão geral

Você pode criar e se conectar a instâncias no console de gerenciamento.

## Processo

Para criar e usar uma instância, você precisa executar as operações descritas no fluxograma a seguir.

**Figura 1-1** Processo

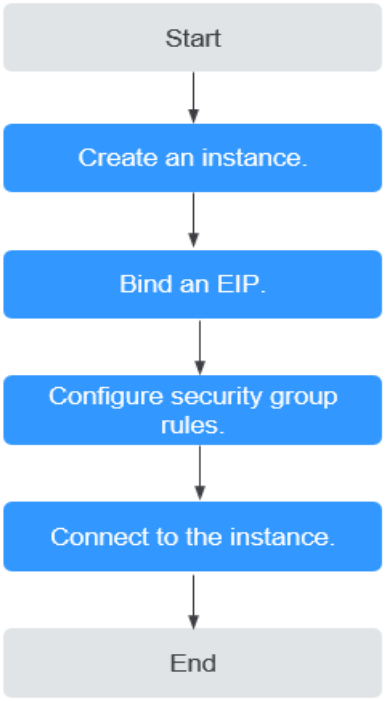


**Tabela 1-1** Processo de operação

| Procedimento | Descrição | Referência |
| --- | --- | --- |
| Criar uma instância | Você pode personalizar os recursos de computação e o armazenamento disponíveis para sua instância. | ● **Compra de uma instância de cluster**<br>● **Compra de uma instância de conjunto de réplicas**<br>● **Compra de uma instância de nó único** |
| Vincular um EIP | (Opcional)<br>Ao se conectar a uma instância da Internet, você precisa configurar um EIP. | **Vinculação ou desvinculação de um EIP** |
| Configurar regras de grupo de segurança | (Opcional)<br>Adicione os dispositivos que acessam a instância ao grupo de segurança associado à instância, para que você possa acessar a instância a partir dos dispositivos.<br>● Se você acessar a instância de um ECS que esteja em uma segurança diferente da instância em uma rede privada, será necessário configurar a regra do grupo de segurança.<br>● Se você se conectar a uma instância através de uma rede pública, será necessário configurar regras de grupo de segurança. | ● **Configuração de regras de grupo de Segurança (rede privada)**<br>● **Configuração de regras de grupo de segurança (rede pública)** |
| Conectar a uma instância | Você pode se conectar a instâncias por meio de DAS, uma rede privada, uma rede pública ou código de programa. | ● **Conexão a uma instância de cluster**<br>● **Conexão a uma instância de conjunto de réplicas**<br>● **Conexão a uma instância de nó único** |

# 2 Primeiros passos com clusters

## 2.1 Compra de uma instância de cluster

### 2.1.1 Configuração rápida

Esta seção descreve como comprar rapidamente uma instância de cluster no console de gerenciamento. O DDS ajuda você a configurar e criar rapidamente um cluster em poucos minutos.

#### Precauções

Cada conta pode criar até 10 instâncias de cluster.

#### Pré-requisitos

- Você registrou uma conta da Huawei Cloud.

#### Procedimento

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

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

Se você quiser recursos de computação e rede dedicados ao seu uso exclusivo, **ative uma DeC** e **solicite recursos do DCC**. Depois de ativar uma DeC, você pode selecionar a região da DeC e o projeto.

**Passo 3** Clique em no canto superior esquerdo da página e escolha **Databases** > **Document Database Service**.

**Passo 4** Na página **Instances**, clique em **Comprar instância de BD**. A página **Quick Config** é exibida por padrão.

**Passo 5** Selecione um modo de cobrança. Especifique os detalhes da instância e clique em **Próximo**.

**Figura 2-1** Configurações básicas

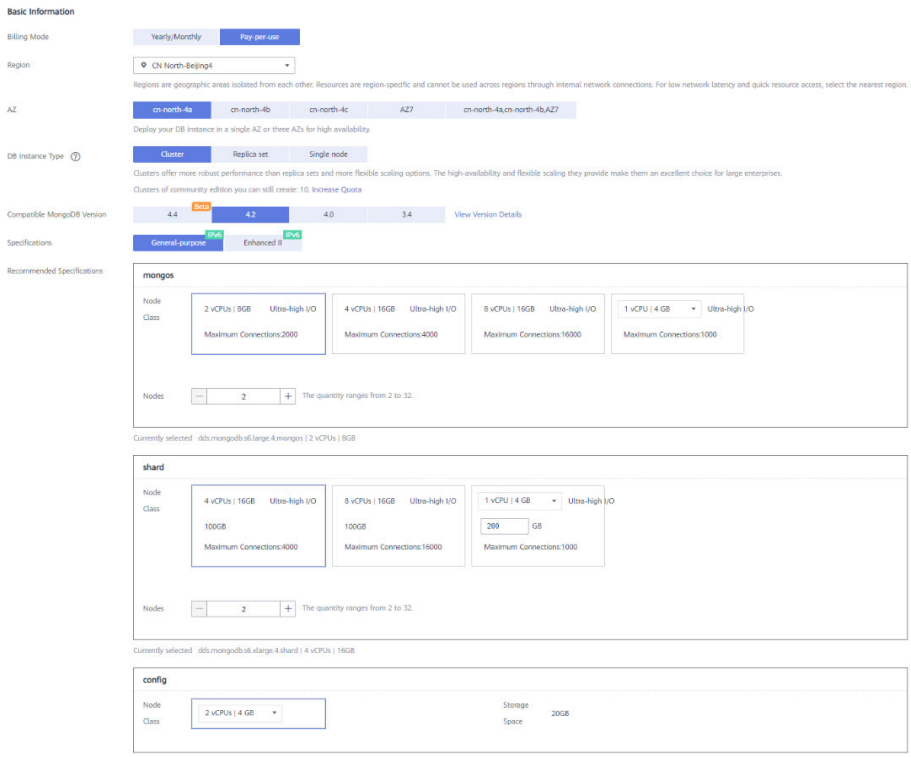



**Tabela 2-1** Configurações básicas

| Parâmetro | Descrição |
| --- | --- |
| Billing Mode | Selecione um modo de cobrança, **Yearly/Monthly** ou **Pay-per-use**.<br>● Para instâncias anuais/mensais<br>– Especifique a **Required Duration** e o sistema deduz as taxas incorridas da sua conta com base no preço do serviço.<br>– Se você não espera continuar usando a instância muito depois que ela expirar, altere o modo de cobrança de anual/mensal para pagamento por uso. Para obter detalhes, consulte **Alteração do modo de cobrança de anual/mensal para pagamento por uso**.<br>**NOTA**<br>As instâncias cobradas anualmente/mensalmente não podem ser excluídas. Elas só podem ser canceladas. Para obter detalhes, consulte **Cancelamento da assinatura de uma instância anual/mensal**.<br>● Para instâncias de pagamento por uso<br>– Você é cobrado pelo uso com base em quanto tempo o serviço está em uso.<br>– Se você espera usar o serviço extensivamente durante um longo período de tempo, você pode alterar seu modo de cobrança de pagamento por uso para anual/mensal para reduzir os custos. Para obter detalhes, consulte **Alteração do modo de cobrança de pagamento por uso para anual/mensal**.. |

| Parâmetro | Descrição |
| --- | --- |
| Region | A região onde o recurso está localizado.<br>**NOTA**<br>As instâncias implementadas em diferentes regiões não podem se comunicar entre si por meio de uma rede privada, e você não pode alterar a região de uma instância depois que ela for comprada. Tenha cuidado ao selecionar uma região. |
| AZ | Uma AZ é uma parte de uma região com sua própria fonte de alimentação e rede independentes. As AZs são fisicamente isoladas, mas podem se comunicar através de conexões de rede interna.<br>As instâncias podem ser implementadas em uma única AZ ou três AZs.<br>**NOTA**<br>A implantação de 3-AZ não está disponível em todas as regiões. Se a opção 3-AZ não for exibida na página para você comprar uma instância, tente uma região diferente.<br>● Se o serviço exigir baixa latência de rede entre instâncias, implante os componentes da instância na mesma AZ. Se você selecionar uma única AZ para implantar sua instância, a implementação de anti-afinidade será usada por padrão. Com uma implantação anti-afinidade, seus nós primários, secundários e ocultos são implementados em diferentes máquinas físicas para alta disponibilidade.<br>● Se você quiser implementar uma instância em AZs para recuperação de desastres, selecione três AZs. Nesse modo de implementação, os nós mongos, shard e config são distribuídos uniformemente pelas três AZs. |
| DB Instance Type | Selecione **Cluster**.<br>Uma instância de cluster inclui três tipos de nós: mongos, shard e config. Cada shard e config é um conjunto de réplicas de três nós para garantir alta disponibilidade. |
| Compatible MongoDB Version | ● 4.4<br>● 4.2<br>● 4.0<br>● 3.4 |

| Parâmetro | Descrição |
| --- | --- |
| CPU Type | O DDS suporta arquiteturas de CPU x86 e Kunpeng.<br>**NOTA**<br>Esse parâmetro está disponível apenas para o MongoDB 4.0 e 3.4. O valor padrão é **Kunpeng**.<br>● x86<br>As CPUs x86 usam o conjunto de instruções CISC (Complex Instruction Set Computing). Cada instrução pode ser usada para executar operações de hardware de baixo nível. As instruções CISC variam em comprimento e tendem a ser complicadas e lentas em comparação com RISC (Reductiond Instruction Set Computing).<br>● Kunpeng<br>A arquitetura de CPU Kunpeng usa RISC. O conjunto de instruções RISC é menor e mais rápido que CISC, graças à arquitetura simplificada. CPUs Kunpeng também oferecem um melhor equilíbrio entre energia e desempenho do que x86.<br>As CPUs Kunpeng oferecem uma opção de alta densidade e baixo consumo de energia que é mais econômica para cargas de trabalho pesadas. |
| Especificações | Com uma arquitetura x86, você tem as seguintes opções:<br>● Uso geral (s6): as instâncias S6 são adequadas para aplicações que exigem desempenho moderado em geral, mas explosões ocasionais de alto desempenho, como servidores Web de carga leve, ambientes corporativos de P&D e testes e bancos de dados de baixo e médio desempenho.<br>● Aprimorada II (c6): as instâncias C6 têm várias tecnologias otimizadas para fornecer desempenho computacional robusto e estável. NICs inteligentes de alta velocidade de 25 GE são usadas para fornecer largura de banda e taxa de transferência ultra-altas, o que as torna uma excelente opção para cenários de carga pesada. É adequada para sites, aplicações Web, bancos de dados gerais e servidores de cache que têm requisitos de desempenho mais altos para recursos de computação e rede; e aplicações corporativas de carga média e pesada.<br>Para obter detalhes sobre as especificações de instância suportadas, consulte **Especificações de instância de cluster**. |
| mongos Node Class | Para obter detalhes sobre CPU e memória mongos, consulte **Especificações da instância de cluster**. Você pode alterar a classe de uma instância depois que ela for criada. Para obter detalhes, consulte **Alteração da classe de instância**. |
| mongos Nodes | O valor varia de 2 a 16. Se necessário, você pode adicionar nós a uma instância depois que ela for criada. Para obter detalhes, consulte **Adição de nós de instância de cluster**. |

| Parâmetro | Descrição |
| --- | --- |
| shard Node Class | Para obter detalhes sobre CPU e memória de shard, consulte **Especificações da instância de cluster**. O nó shard armazena dados do usuário, mas não pode ser acessado diretamente. Você pode alterar a classe de uma instância depois que ela for criada. Para obter detalhes, consulte **Alteração da classe de instância**. |
| shard Storage Space | O valor varia de 10 GB a 2000 GB e deve ser um múltiplo de 10. Você pode expandir uma instância depois que ela é criada.Para obter detalhes, consulte **Expensão de uma instância de cluster**.<br>**NOTA**<br>● Se o espaço de armazenamento comprado exceder 600 GB e o espaço de armazenamento restante for 18 GB, a instância se tornará **Read-only**.<br>● Se o espaço de armazenamento comprado for inferior a 600 GB e o uso do espaço de armazenamento atingir 97%, a instância se tornará **Read-only**.<br>Nesses casos, exclua recursos desnecessários ou expanda a capacidade. |
| shard Nodes | O valor varia de 2 a 16. Se necessário, você pode adicionar nós a uma instância depois que ela for criada. Para obter detalhes, consulte **Adição de nós de instância de cluster**. |
| config Node Class | Para obter detalhes sobre a CPU e a memória do nó de configuração, consulte **Especificações da instância de cluster**. Você pode alterar a classe de uma instância depois que ela for criada. Para obter detalhes, consulte **Alteração da classe de instância**. |
| config Storage Space | Com base nas funções e nos requisitos mínimos do nó config, o espaço de armazenamento do nó config é definido como 20 GB por padrão. Não é possível expandir o armazenamento do nó depois que ele é criado. |

**Figura 2-2** Rede, duração necessária e quantidade

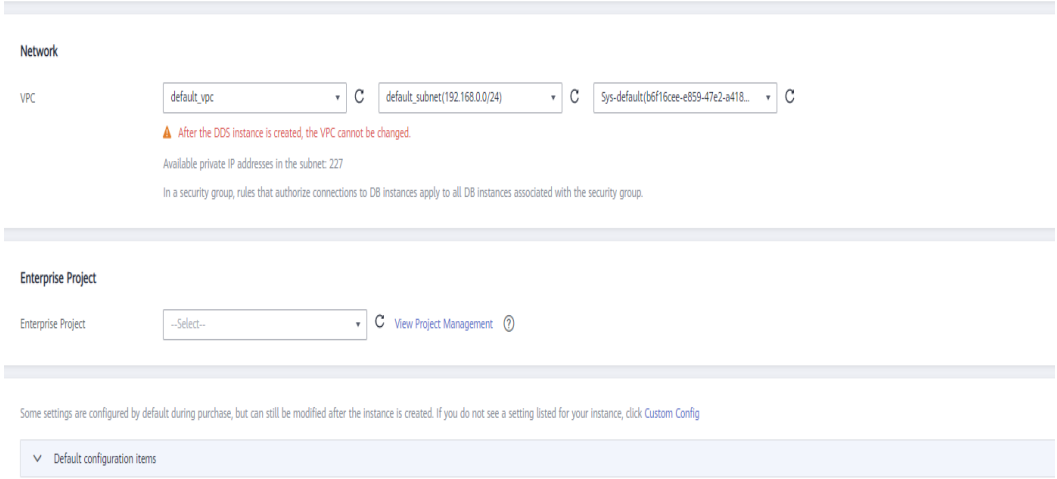


**Tabela 2-2** Configurações da rede

| Parâmetro | Descrição |
| --- | --- |
| VPC | A VPC onde suas instâncias de BD estão localizadas. Uma VPC isola redes para diferentes serviços. Ela permite que você gerencie e configure facilmente redes privadas e altere as configurações de rede. Você precisará criar ou selecionar a VPC necessária. Para obter detalhes, consulte **Criação de uma VPC** no *Guia de usuário da Virtual Private Cloud*. Para obter detalhes sobre as restrições sobre o uso de VPCs, consulte **Métodos de conexão**.<br>Se não houver VPCs disponíveis, o DDS criará uma para você por padrão.<br>**NOTA**<br>Após a criação da instância de DDS, a VPC não poderá ser alterada. |
| Enterprise Project | Somente usuários empresariais podem usar essa função. Para usar essa função, entre em contato com o atendimento ao cliente.<br>Um projeto empresarial é um modo de gerenciamento de recursos em nuvem, no qual os recursos e os membros da nuvem são gerenciados centralmente pelo projeto.<br>selecione um projeto da empresa na lista suspensa. O projeto padrão é **default**. Para obter mais informações sobre o projeto da empresa, consulte **Gerenciamento de projetos** no *Guia de usuário do Enterprise Management*.<br>Para personalizar um projeto empresarial, clique em **Enterprise** no canto superior direito do console. A página **Enterprise Management** é exibida. Para obter detalhes, consulte **Criação de um projeto empresarial** no *Guia de usuário do Enterprise Management*. |

**Tabela 2-3** Duração necessária e quantidade

| Parâmetro | Descrição |
| --- | --- |
| Required Duration | A duração da sua assinatura se você selecionar **Yearly/Monthly**. A duração da assinatura varia de um mês a três anos. |
| Auto-renew | ● Por padrão, essa opção não está selecionada.<br>● Se você selecionar essa opção, o ciclo de renovação automática será determinado pela duração da assinatura. |
| Quantity | A quantidade de compra depende da cota da instância do cluster. Se sua cota atual não permitir que você compre o número necessário de instâncias, você poderá solicitar uma cota aumentada. As instâncias anuais/mensais que foram compradas em lotes têm as mesmas especificações, exceto o nome e o ID da instância. |

**Tabela 2-4** Itens de configuração padrão

| Especificações | Valor | Editável após a criação da instância |
| --- | --- | --- |
| Nome da instância de BD | dds-6c01 | Sim |
| Tipo de CPU | x86 | Não |
| Mecanismo de armazenamento | WiredTiger | Não |
| Configurações de senha | Não configurado | Sim |
| SSL | Desabilitado | Sim |
| Porta do banco de dados | 8635 | Sim |
| Modelo de parâmetro do cluster | Default-DDS-4.0-Mongos<br>Default-DDS-4.0-Shard<br>Default-DDS-4.0-Config | Sim |
| Tags | Não configurado | Sim |
| Configurações avançadas | Não configurado | Sim |

NOTA

- Algumas configurações são configuradas por padrão durante a compra, mas ainda podem ser modificadas após a criação da instância. Se você não vir uma configuração listada para sua instância, clique em **Configuração personalizada**.
- O desempenho da instância depende das especificações selecionadas durante a criação. Os itens de configuração de hardware que podem ser selecionados incluem a classe de nó e o espaço de armazenamento.

**Passo 6** Na página exibida, confirme os detalhes da instância.

- Para instâncias anuais/mensais
  - Se você precisar modificar as especificações, clique em **Previous** para retornar à página anterior.
  - Se você não precisar modificar as especificações, leia e concorde com o contrato de serviço e clique em **Pay Now** para ir para a página de pagamento e concluir o pagamento.
- Para instâncias de pagamento por uso
  - Se você precisar modificar as especificações, clique em **Previous** para retornar à página anterior.
  - Se você não precisar modificar as especificações, leia e concorde com o contrato de serviço e clique em **Submit** para começar a criar a instância.

**Passo 7** Depois que uma instância do DDS for criada, você poderá exibi-la e gerenciá-la na página **Instances**.

- Quando uma instância está sendo criada, o status exibido na coluna **Status** é **Creating**. Este processo leva cerca de 15 minutos. Após a conclusão da criação, o status muda para **Available**.
- O DDS ativa a política de backup automatizado por padrão. Depois que uma instância é criada, você pode modificar ou desativar a política de backup automatizado. Um backup completo automatizado é acionado imediatamente após a criação de uma instância.
- As instâncias anuais/mensais que foram compradas em lotes têm as mesmas especificações, exceto o nome e o ID da instância.

**----Fim**

## 2.1.2 Configuração personalizada

Esta seção descreve como comprar uma instância de cluster no modo personalizado no console de gerenciamento. Você pode personalizar os recursos de computação e o espaço de armazenamento de uma instância de cluster com base em seus requisitos de serviço. Além disso, você pode definir configurações avançadas, como log de consultas lentas e backup automatizado.

### Precauções

Cada conta pode criar até 10 instâncias de cluster.

### Pré-requisitos

- Você registrou uma conta da Huawei Cloud.

### Procedimento

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

**Passo 2** Clique em ☰ no canto superior esquerdo da página e escolha **Databases** > **Document Database Service**.

**Passo 3** Na página **Instances**, clique em **Comprar instância de BD**.

**Passo 4** Clique na guia **Custom Config**.

**Passo 5** Selecione um modo de cobrança. Especifique os detalhes da instância e clique em **Próximo**.

**Figura 2-3** Configurações básicas

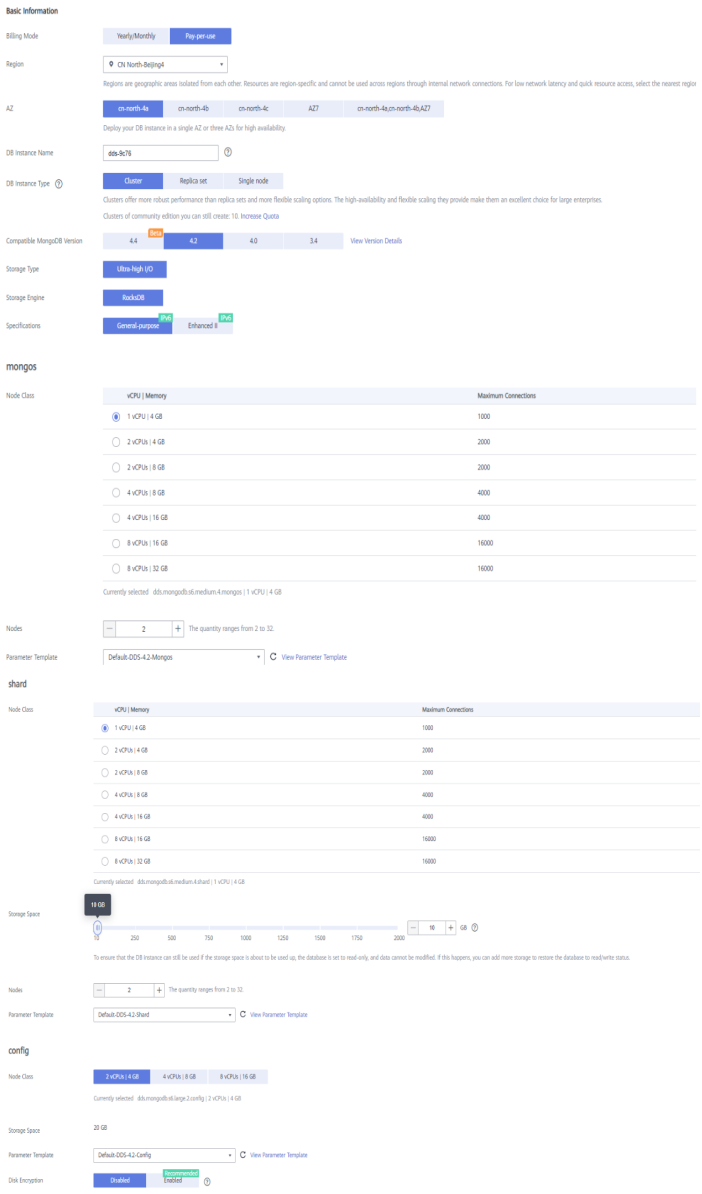


**Tabela 2-5** Configurações básicas

| Parâmetro | Descrição |
| --- | --- |
| Billing Mode | Selecione um modo de cobrança, **Yearly/Monthly** ou **Pay-per-use**.<br>● Para instâncias anuais/mensais<br>– Especifique a **Required Duration** e o sistema deduz as taxas incorridas da sua conta com base no preço do serviço.<br>– Se você não espera continuar usando a instância muito depois que ela expirar, altere o modo de cobrança de anual/mensal para pagamento por uso. Para obter detalhes, consulte **Alteração do modo de cobrança de anual/mensal para pagamento por uso**.<br>**NOTA**<br>As instâncias cobradas anualmente/mensalmente não podem ser excluídas. Elas só podem ser canceladas. Para obter detalhes, consulte **Cancelamento da assinatura de uma instancia anual/mensal**.<br>● Para instâncias de pagamento por uso<br>– Você é cobrado pelo uso com base em quanto tempo o serviço está em uso.<br>– Se você espera usar o serviço extensivamente durante um longo período de tempo, você pode alterar seu modo de cobrança de pagamento por uso para anual/mensal para reduzir os custos. Para obter detalhes, consulte **Alteração do modo de cobrança de pagamento por uso para anual/mensal**.. |
| Region | A região onde o recurso está localizado.<br>**NOTA**<br>As instâncias implementadas em diferentes regiões não podem se comunicar entre si por meio de uma rede privada, e você não pode alterar a região de uma instância depois que ela for comprada. Tenha cuidado ao selecionar uma região. |
| AZ | Uma AZ é uma parte de uma região com sua própria fonte de alimentação e rede independentes. As AZs são fisicamente isoladas, mas podem se comunicar através de conexões de rede internas.<br>As instâncias podem ser implementadas em uma única AZ ou três AZs.<br>● Se o serviço exigir baixa latência de rede entre instâncias, implemente os componentes da instância na mesma AZ. Se você selecionar uma única AZ para implementar sua instância, a implementação de anti-afinidade será usada por padrão. Com uma implementação anti-afinidade, seus nós primários, secundários e ocultos são implementados em diferentes máquinas físicas para alta disponibilidade.<br>● Se você quiser implementar uma instância em AZs para recuperação de desastres, selecione três AZs. Nesse modo de implementação, os nós mongos, shard e config são distribuídos uniformemente pelas três AZs.<br>**NOTA**<br>A implementação de 3-AZ não está disponível em todas as regiões. Se a opção 3-AZ não for exibida na página para você comprar uma instância, tente uma região diferente. |

| Parâmetro | Descrição |
| --- | --- |
| DB Instance Name | ● O nome da instância pode ser igual a um nome de instância existente.<br>● O nome da instância que você especificar após a compra. O nome da ocorrência deve conter de 4 a 64 caracteres e deve começar com uma letra. Ele diferencia maiúsculas de minúsculas e minúsculas e pode conter letras, dígitos, hifens (-) e sublinhados (_). Não pode conter outros caracteres especiais.<br>● Se você comprar um lote de instâncias de uma só vez, um sufixo numérico de 4 dígitos será adicionado aos nomes das instâncias, começando com **-0001**. Se mais tarde você fizer outra compra em lote, os novos nomes de instância serão numerados primeiro usando quaisquer sufixos ausentes da sequência de suas instâncias existentes e, em seguida, continuando a partir de onde sua última compra em lote parou. Por exemplo, um lote de 3 instâncias obtém os sufixos **-0001**, **-0002** e **-0003**. Se você excluir a instância **0002** e depois comprar mais 3 instâncias, as novas instâncias receberão os sufixos **-0002**, **-0004** e **-0005**.<br>● Depois que a instância de BD for criada, você poderá alterar seu nome. Para mais detalhes, consulte **Alteração de um nome de instância**. |
| DB Instance Type | Selecione **Cluster**.<br>Uma instância de cluster inclui três tipos de nós: mongos, shard e config. Cada shard e config é um conjunto de réplicas de três nós para garantir alta disponibilidade. |
| Compatible MongoDB Version | ● 4.4<br>● 4.2<br>● 4.0<br>● 3.4 |

| Parâmetro | Descrição |
| --- | --- |
| CPU Type | O DDS suporta arquiteturas de CPU x86 e Kunpeng.<br>**NOTA**<br>Esse parâmetro está disponível apenas para o MongoDB 4.0 e 3.4. O valor padrão é **Kunpeng**.<br>● x86<br>As CPUs x86 usam o conjunto de instruções CISC (Complex Instruction Set Computing). Cada instrução pode ser usada para executar operações de hardware de baixo nível. As instruções CISC variam em comprimento e tendem a ser complicadas e lentas em comparação com RISC (Reductiond Instruction Set Computing).<br>● Kunpeng<br>A arquitetura de CPU Kunpeng usa RISC. O conjunto de instruções RISC é menor e mais rápido que CISC, graças à arquitetura simplificada. CPUs Kunpeng também oferecem um melhor equilíbrio entre energia e desempenho do que x86.<br>As CPUs Kunpeng oferecem uma opção de alta densidade e baixo consumo de energia que é mais econômica para cargas de trabalho pesadas. |
| Storage Type | Se você não usar a DeC, o tipo de armazenamento é de I/O ultra-alta por padrão.<br>Para usuários da DeC, os tipos de armazenamento suportados dependem do tipo de recurso selecionado.<br>● Se você selecionar **EVS** para **Resource Type**, **Storage Type** será definido como **Ultra-high I/O**.<br>● Se você selecionar **DSS** para **Resource Type**, **Storage Type** pode ser definido como **Common I/O**, **High I/O** ou **Ultra-high I/O**. |
| Storage Engine | ● WiredTiger<br>O WiredTiger é o mecanismo de armazenamento padrão do DDS 3.4 e 4.0. O WiredTiger fornece controle de simultaneidade de granularidade diferente e mecanismo de compactação para gerenciamento de dados. Ele pode fornecer o melhor desempenho e eficiência de armazenamento para diferentes tipos de aplicações.<br>● RocksDB<br>O RocksDB é o mecanismo de armazenamento padrão do DDS 4.2 e 4.4. O RocksDB suporta pesquisa de pontos eficiente, varredura de alcance e gravação de alta velocidade. O RocksDB pode ser usado como o mecanismo de armazenamento de dados subjacente do MongoDB e é adequado para cenários com um grande número de operações de gravação. |

| Parâmetro | Descrição |
| --- | --- |
| Specifications | Com uma arquitetura x86, você tem as seguintes opções:<br>● Uso geral (s6): as instâncias S6 são adequadas para aplicações que exigem desempenho moderado em geral, mas explosões ocasionais de alto desempenho, como servidores da Web de carga leve, ambientes corporativos de P&D e testes e bancos de dados de baixo e médio desempenho.<br>● Aprimorada II (c6): as instâncias C6 têm várias tecnologias otimizadas para fornecer desempenho computacional robusto e estável. NICs inteligentes de alta velocidade de 25 GE são usadas para fornecer largura de banda e taxa de transferência ultra-altas, o que as torna uma excelente opção para cenários de carga pesada. É adequada para sites, aplicações Web, bancos de dados gerais e servidores de cache que têm requisitos de desempenho mais altos para recursos de computação e rede; e aplicações corporativos de carga média e pesada.<br>Para obter detalhes sobre as especificações de instância suportadas, consulte **Especificações de instância de cluster**. |
| mongos Node Class | Para obter detalhes sobre CPU e memória mongos, consulte **Especificações da instância de cluster**. Você pode alterar a classe de uma instância depois que ela for criada. Para mais detalhes, consulte **Alteração da classe de instância**. |
| mongos Nodes | O valor varia de 2 a 16. Você pode adicionar nós a uma instância depois que ela for criada, se necessário. Para obter detalhes, consulte **Adição de nós de instância de cluster**. |
| mongos Parameter Template | Os parâmetros que se aplicam aos nós mongos. Depois que uma instância é criada, você pode alterar o modelo de parâmetro de um nó para trazer o melhor desempenho.<br>Para obter detalhes, consulte **Editação de um modelo de parâmetro**. |
| shard Node Class | Para obter detalhes sobre CPU e memória de shard, consulte **Especificações da instância de cluster**. O nó shard armazena dados do usuário, mas não pode ser acessado diretamente. Você pode alterar a classe de uma instância depois que ela for criada. Para mais detalhes, consulte **Alteração da classe de instância**. |
| shard Storage Space | O valor varia de 10 GB a 2000 GB e deve ser um múltiplo de 10. Você pode expandir uma instância depois que ela é criada.Para obter detalhes, consulte **Expensão de uma instância de cluster**.<br>**NOTA**<br>● Se o espaço de armazenamento comprado exceder 600 GB e o espaço de armazenamento restante for 18 GB, a instância se tornará **Read-only**.<br>● Se o espaço de armazenamento comprado for inferior a 600 GB e o uso do espaço de armazenamento atingir 97%, a instância se tornará **Read-only**.<br>Nesses casos, exclua recursos desnecessários ou expanda a capacidade. |
| shard Nodes | O valor varia de 2 a 16. Se necessário, você pode adicionar nós a uma instância depois que ela for criada. Para obter detalhes, consulte **Adição de nós de instância de cluster**. |

| Parâmetro | Descrição |
| --- | --- |
| shard Parameter Template | Os parâmetros que se aplicam aos nós shard. Depois que uma instância é criada, você pode alterar o modelo de parâmetro de um nó para trazer o melhor desempenho.<br>Para obter detalhes, consulte **Editação de um modelo de parâmetro**. |
| config Node Class | Para obter detalhes sobre a CPU e a memória do nó de configuração, consulte **Especificações da instância de cluster**. Você pode alterar a classe de uma instância depois que ela for criada. Para obter detalhes, consulte **Alteração da classe de instância**. |
| config Storage Space | Com base nas funções e nos requisitos mínimos do nó config, o espaço de armazenamento do nó config é definido como 20 GB por padrão. Não é possível expandir o armazenamento do nó depois que ele é criado. |
| config Parameter Template | Os parâmetros que se aplicam aos nós de configuração. Depois que uma instância é criada, você pode alterar o modelo de parâmetro de um nó para trazer o melhor desempenho.<br>Para obter detalhes, consulte **Editação de um modelo de parâmetro**. |
| Disk Encryption | ● **Disabled**: desativar a criptografia.<br>● **Enabled**: ativar a criptografia. Esse recurso melhora a segurança dos dados, mas afeta um pouco o desempenho de leitura/gravação. **Key Name**: selecione ou crie uma chave privada, que é a chave do locatário.<br>**NOTA**<br>– Depois que uma instância é criada, o status de criptografia de disco e a chave não podem ser alterados. Os dados de backup armazenados no OBS não são criptografados.<br>– A chave não pode ser desativada, excluída ou congelada ao ser usada. Caso contrário, o banco de dados ficará indisponível.<br>– Para obter detalhes sobre como criar uma chave, consulte "**Criação de uma CMK**" no *Guia de usuário do Data Encryption Workshop*. |

**Figura 2-4** Configurações do administrador

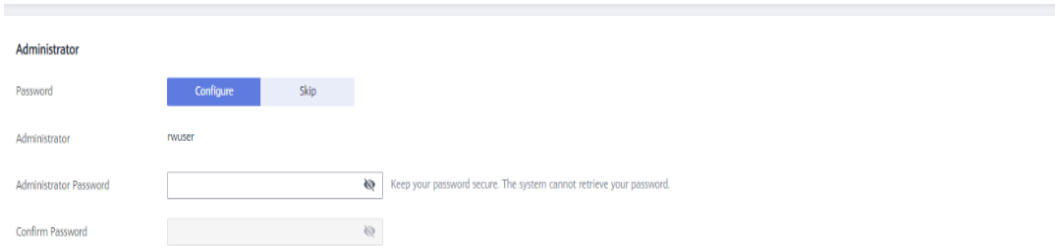


**Tabela 2-6** Configurações do administrador

| Parâmetro | Descrição |
| --- | --- |
| Password | ● Configure<br>Digite e confirme a nova senha de administrador. Depois que uma instância é criada, você pode se conectar à instância usando a senha.<br>● Skip<br>Para fazer logon, você terá que redefinir a senha mais tarde na página **Basic Information**. Se você precisar se conectar a uma instância depois que ela for criada, localize a instância e escolha **More** > **Reset Password** na coluna **Operation** para definir uma senha para a instância primeiro. |
| Administrator | A conta padrão é **rwuser**. |
| Administrator Password | Defina uma senha para o administrador. A senha deve ter de 8 a 32 caracteres e conter letras maiúsculas, minúsculas, dígitos e pelo menos um dos seguintes caracteres especiais: ~!@#%^*-_=+?<br>Mantenha esta senha segura. Se for perdida, o sistema não poderá recuperá-la para você. |
| Confirm Password | Digite a senha do administrador novamente. |

**Figura 2-5** Rede e duração necessária

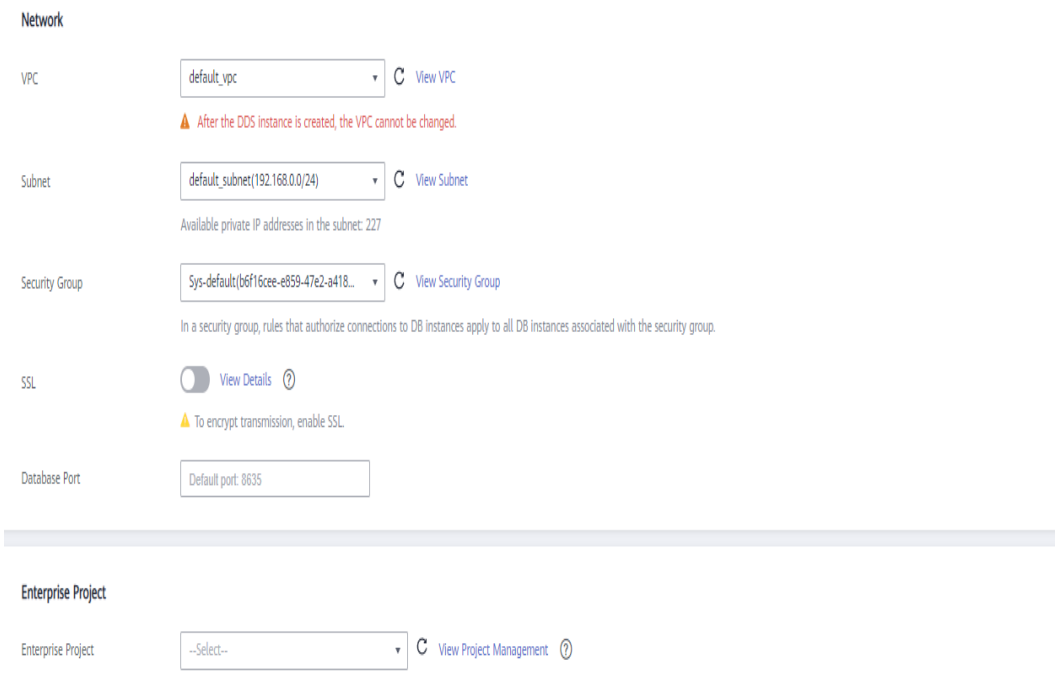


**Tabela 2-7** Configurações da rede

| Parâmetro | Descrição |
| --- | --- |
| VPC | A VPC onde suas instâncias de BD estão localizadas. Uma VPC isola redes para diferentes serviços. Ela permite que você gerencie e configure facilmente redes privadas e altere as configurações de rede. Você precisará criar ou selecionar a VPC necessária. Para obter detalhes sobre como criar uma VPC, consulte "Criação de uma VPC" no *Guia de usuário da Virtual Private Cloud*. Para obter detalhes sobre as restrições sobre o uso de VPCs, consulte **Métodos de conexão**.<br>Se não houver VPCs disponíveis, o DDS criará uma para você por padrão.<br>**NOTA**<br>Após a criação da instância de DDS, a VPC não poderá ser alterada. |
| Subnet | Uma sub-rede fornece recursos de rede dedicados que são logicamente isolados de outras redes por razões de segurança.<br>Depois que a instância é criada, você pode alterar o endereço IP privado atribuído pela sub-rede. Para obter detalhes, consulte **Alteração um endereço IP privado**.<br>**NOTA**<br>As sub-redes IPv6 não são suportadas. Recomendamos que você crie e selecione sub-redes IPv4. |
| Security Group | Um grupo de segurança controla o acesso entre o DDS e outros serviços.<br>Se não houver grupos de segurança disponíveis, o DDS criará um para você por padrão.<br>**NOTA**<br>Certifique-se de que haja uma regra de grupo de segurança configurada que permita que os clientes acessem instâncias. Por exemplo, selecione uma regra TCP de entrada com a porta padrão 8635 e insira um endereço IP de sub-rede ou selecione um grupo de segurança ao qual a instância pertence. |
| SSL | A Camada de soquete seguro (SSL) criptografa as conexões entre clientes e servidores, impedindo que os dados sejam adulterados ou roubados durante a transmissão.<br>Você pode ativar SSL para melhorar a segurança dos dados. Depois que uma instância é criada, você pode se conectar a ela usando SSL. |
| Database Port | A porta do DDS padrão é 8635, mas esta porta pode ser modificada se necessário. Se você alterar a porta, adicione uma regra de grupo de segurança correspondente para permitir o acesso à instância.<br>**NOTA**<br>● A porta do banco de dados é a porta do nó mongos. A porta padrão é 8635. Para alterar a porta, consulte **Alteração de uma porta do banco de dados**.<br>● A porta do nó shard é 8637 e a porta do nó config é 8636, que não pode ser alterada. Para obter detalhes sobre como se conectar aos nós shard e config, consulte **Habilitação de endereços IP de nós shard e config**. |

| Parâmetro | Descrição |
| --- | --- |
| Enterprise Project | Somente usuários empresariais podem usar essa função. Para usar essa função, entre em contato com o atendimento ao cliente.<br>Um projeto empresarial é um modo de gerenciamento de recursos em nuvem, no qual os recursos e os membros da nuvem são gerenciados centralmente pelo projeto.<br>selecione um projeto empresarial na lista suspensa. O projeto padrão é **default**. Para obter mais informações sobre projetos corporativos, consulte *Guia de usuário do Enterprise Management*. |

**Figura 2-6** Configurações avançadas

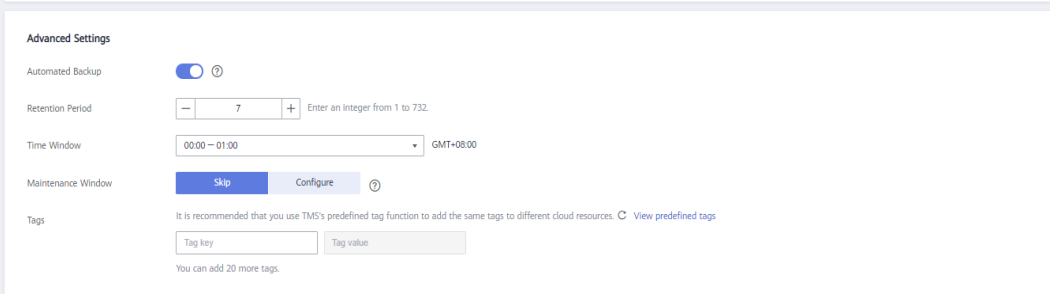



**Tabela 2-8** Configurações avançadas

| Parâmetro | Descrição |
| --- | --- |
| Automated Backup | O DDS ativa uma política de backup automatizado por padrão, mas você pode desativá-la após a criação de uma instância. Um backup completo automatizado é acionado imediatamente após a criação de uma instância.<br>Para obter detalhes, consulte **Configuração de uma política de backup automatizado**. |
| Retention Period (days) | **Retention Period** refere-se ao número de dias que os dados são mantidos. Você pode aumentar o período de retenção para melhorar a confiabilidade dos dados.<br>O período de retenção do backup é de 1 a 732 dias. |
| Time Window | Um período de uma hora, o backup será agendado dentro de 24 horas, como 01:00-02:00. O tempo de backup está no formato UTC. |

| Parâmetro | Descrição |
| --- | --- |
| Tags | (Opcional) Você pode adicionar tags a instâncias do DDS para que possa pesquisar rapidamente e filtrar instâncias especificadas por tag. Cada instância do DDS pode ter até 20 tags.<br>● Criar uma tag.<br>Você pode criar tags no console do DDS e configurar a **chave** e o **valor** da tag.<br>Key: este parâmetro é obrigatório.<br>– Cada chave de tag deve ser exclusiva para cada instância.<br>– Uma chave de tag consiste em até 36 caracteres.<br>– A chave deve consistir apenas em dígitos, letras, sublinhados (_) e hifens (-).<br>Value: este parâmetro é opcional.<br>– O valor consiste em até 43 caracteres.<br>– O valor deve consistir apenas em dígitos, letras, sublinhados (_), pontos (.) e hifens.<br>● Adicionar uma tag predefinida.<br>Tags predefinidas podem ser usadas para identificar vários recursos de nuvem.<br>Para marcar um recurso de nuvem, você pode selecionar uma tag predefinida criada na lista suspensa, sem inserir uma chave e um valor para a tag.<br>Por exemplo, se uma tag predefinida tiver sido criada, sua chave será Usage e o valor será Project1. Quando você configura a chave e o valor para um recurso de nuvem, a tag predefinida criada será exibida na página.<br>Depois que uma instância é criada, você pode clicar no nome da instância para exibir suas tags. Na página **Tags**, você também pode **modificar ou excluir as tags**. Além disso, você pode **pesquisar e filtrar rapidamente instâncias especificadas por tag**.<br>Você pode adicionar uma tag a uma instância depois que ela for criada. Para obter detalhes, consulte **Adição de uma tag**. |

Se você tiver alguma dúvida sobre o preço, clique em **Price Details**.

NOTA

O desempenho da instância depende das especificações selecionadas durante a criação. Os itens de configuração de hardware que podem ser selecionados incluem a classe de nó e o espaço de armazenamento.

**Passo 6** Na página exibida, confirme os detalhes da instância.

- Para instâncias anuais/mensais
  - Se você precisar modificar as especificações, clique em **Previous** para retornar à página anterior.

  - Se você não precisar modificar as especificações, leia e concorde com o contrato de serviço e clique em **Pay Now** para ir para a página de pagamento e concluir o pagamento.
- Para instâncias de pagamento por uso
  - Se você precisar modificar as especificações, clique em **Previous** para retornar à página anterior.
  - Se você não precisar modificar as especificações, leia e concorde com o contrato de serviço e clique em **Submit** para começar a criar a instância.

**Passo 7** Depois que uma instância do DDS for criada, você poderá exibi-la e gerenciá-la na página **Instances**.

- Quando uma instância está sendo criada, o status exibido na coluna **Status** é **Creating**. Este processo leva cerca de 15 minutos. Após a conclusão da criação, o status muda para **Available**.
- As instâncias anuais/mensais que foram compradas em lotes têm as mesmas especificações, exceto o nome e o ID da instância.

**----Fim**

# 2.2 Conexão a uma instância de cluster

## 2.2.1 Métodos de conexão

Você pode acessar o DDS em redes privadas ou públicas.

**Tabela 2-9** Métodos de conexão

| Método | Endereço IP | Cenário | Descrição |
| --- | --- | --- | --- |
| DAS | Não necessário | O DAS fornece uma GUI e permite que você execute operações visualizadas no console. Execução SQL, gerenciamento de banco de dados avançado e O&M inteligente estão todos disponíveis para tornar o gerenciamento de banco de dados simples, seguro e inteligente.<br>Por padrão, a permissão para se conectar ao DAS está habilitada. | • Fácil de usar, seguro, avançado e inteligente<br>• Recomendado |

| Método | Endereço IP | Cenário | Descrição |
| --- | --- | --- | --- |
| **Rede privada** | Endereço IP privado | O DDS fornece um endereço IP privado por padrão.<br>Se suas aplicações estiverem sendo executadas em um ECS na mesma região e VPC que sua instância do DDS, recomendamos que você use um endereço IP privado para conectar o ECS às instâncias do DDS. | ● Seguro e desempenho excelente<br>● Para uma transmissão mais rápida e segurança aprimorada, é recomendável migrar suas aplicações para um ECS que esteja na mesma sub-rede da instância do DDS e usar um endereço IP privado para acessar a instância. |
| **Rede pública** | EIP | ● Se suas aplicações estiverem sendo executadas em um ECS que esteja em uma região diferente daquela em que a instância do DDS está localizada, use um EIP para conectar o ECS às suas instâncias do DDS.<br>● Se você usar um dispositivo de terceiros ou seu dispositivo local para se conectar a uma instância do DDS, poderá usar um EIP para se conectar à instância de BD. | ● Baixa segurança |

# 2.2.2 (Recomendada) Conexão a instâncias de cluster por meio do DAS

## 2.2.2.1 Visão geral

O DAS fornece uma GUI e permite que você execute operações visualizadas no console. Execução SQL, gerenciamento de banco de dados avançado e O&M inteligente estão todos disponíveis para tornar o gerenciamento de banco de dados simples, seguro e inteligente. Recomendamos que você use o DAS para se conectar às instâncias.

Esta seção descreve como comprar uma instância de cluster no console de gerenciamento e como se conectar à instância do cluster por meio do DAS.

## Processo

Para comprar e se conectar a uma instância de cluster, execute as seguintes etapas:

1. **Compre uma instância de cluster.**
2. **Conecte-se à instância de cluster por meio do DAS.**

### 2.2.2.2 Conexão a uma instância de cluster por meio do DAS

Data Admin Service (DAS) permite que você gerencie instâncias de BD em um console baseado na Web, simplificando o gerenciamento de banco de dados e melhorando a eficiência do trabalho. Você pode se conectar e gerenciar instâncias por meio do DAS. Por padrão, você tem a permissão necessária para o logon remoto. Recomenda-se que você use o serviço DAS para se conectar a instâncias de BD. O DAS é seguro e conveniente.

## 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 e escolha **Databases** > **Document Database Service**.

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

Como alternativa, clique na instância de destino na página **Instances**. Na página **Basic Information** exibida, clique em **Log In** no canto superior direito da página.

**Passo 5** Na caixa de diálogo **Instance Login**, insira as informações corretas e clique em **Log In** para acessar e gerenciar seu banco de dados.

**Passo 6** Depois que o logon for bem-sucedido, você poderá executar operações como criar um banco de dados, gerenciar contas e gerenciar bancos de dados.

Para obter detalhes, consulte **Gerenciamento de dados**.

**----Fim**

# 2.2.3 Conexão a uma instância de cluster em uma rede privada

### 2.2.3.1 Configuração de regras de grupo de segurança

Um grupo de segurança é uma coleção de regras de controle de acesso para ECSs e instâncias do DDS que têm os mesmos requisitos de proteção de segurança e são mutuamente confiáveis em uma VPC.

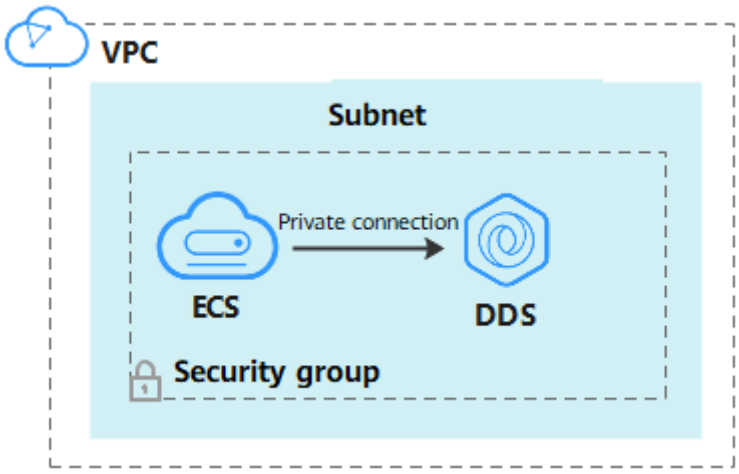
Para garantir a segurança e a confiabilidade do banco de dados, você precisa configurar regras de grupo de segurança para permitir que endereços IP e portas específicos acessem instâncias do DDS.

Você pode se conectar a uma instância configurando regras de grupo de segurança de duas maneiras:

- Se o ECS e a instância estiverem no mesmo grupo de segurança, eles poderão se comunicar entre si por padrão. Nenhuma regra de grupo de segurança precisa ser configurada. Vá para **Conexão a uma instância de cluster usando Mongo Shell (rede privada)**.

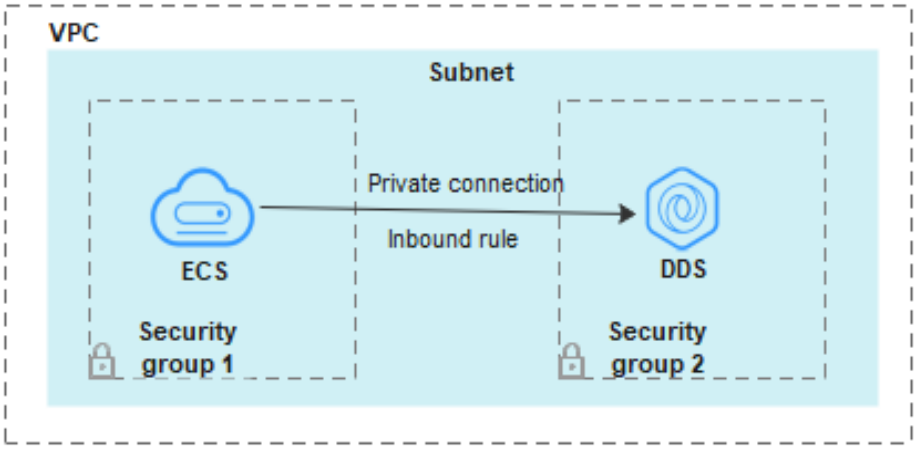
  

**Figura 2-7** Mesmo grupo de segurança




- Se o ECS e a instância estiverem em grupos de segurança diferentes, será necessário configurar as regras de grupo de segurança para eles separadamente.

**Figura 2-8** Diferentes grupos de segurança




  - Instância: configure uma **inbound rule** para o grupo de segurança associado à instância.
  - 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 puder chegar à instância, configure uma regra **de saída** para o ECS.

Esta seção descreve como configurar uma regra **de entrada** para uma instância.

## Precauções

- Por predefinição, uma conta pode criar até 500 regras de grupo de segurança.
- Muitas regras de grupo de segurança aumentarão a latência do primeiro pacote, portanto, recomenda-se um máximo de 50 regras para cada grupo de segurança.
- Uma instância do DDS só pode ser associada a um grupo de segurança.

## 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 e escolha **Databases** > **Document Database Service**.

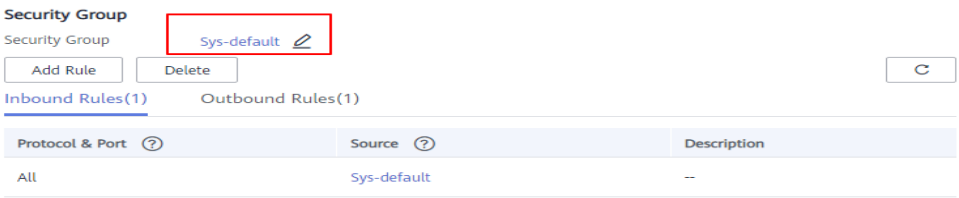
**Passo 4** Na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida.

**Passo 5** Na área **Network Information** da página **Basic Information**, clique no grupo de segurança.

**Figura 2-9** Grupo de segurança


Você também pode escolher **Connections** no painel de navegação à esquerda. Na guia **Private Connection**, na área **Security Group**, clique no nome do grupo de segurança.

**Figura 2-10** Grupo de segurança




**Passo 6** Na página **Security Group**, localize o grupo de segurança de destino e clique em **Manage Rule** na coluna **Operation**.

**Passo 7** Na guia **Inbound Rules**, clique em **Add Rule**. A caixa de diálogo **Add Inbound Rule** é exibida.

**Passo 8** Adicione uma regra de grupo de segurança conforme solicitado.

**Figura 2-11** Adicionar regra de entrada

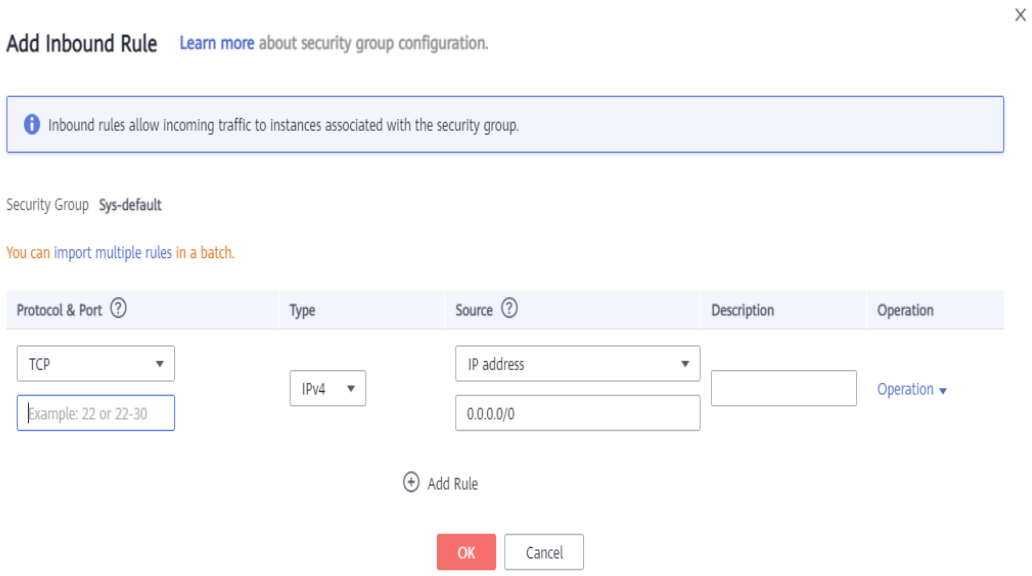



**Tabela 2-10** Configurações da regra de entrada

| Parâmetro | Descrição | Exemplo |
| --- | --- | --- |
| Priority | A prioridade da regra do grupo de segurança.<br>O valor de prioridade varia de 1 a 100. A prioridade padrão é 1 e tem a prioridade mais alta. A regra de grupo de segurança com um valor menor tem uma prioridade mais alta. | 1 |
| Action | As ações de regra do grupo de segurança.<br>Uma regra com uma ação de negação substitui outra com uma ação de permitir se as duas regras tiverem a mesma prioridade. | Allow |
| Protocol & Port | O protocolo de rede necessário para o acesso. Opções disponíveis: **TCP**, **UDP**, **ICMP** ou **GRE** | TCP |
| | Porta: a porta na qual você deseja permitir o acesso ao DDS. A porta padrão é 8635. A porta varia de 2100 a 9500 ou pode ser 27017, 27018 ou 27019. | 8635 |
| Type | Tipo do endereço IP. Apenas **IPv4** e I**IPv6** são suportados. | IPv4 |

| Parâmetro | Descrição | Exemplo |
| --- | --- | --- |
| Source | Especifica o endereço IP, o grupo de segurança e o grupo de endereços IP suportados, que permitem o acesso de endereços IP ou instâncias em outro grupo de segurança. Exemplo:<br>● Endereço IP único: 192.168.10.10/32<br>● Segmento do endereço IP: 192.168.1.0/24<br>● Todos os endereços IP: 0.0.0.0/0<br>● Grupo de segurança: sg-abc<br>● Grupo de endereço IP: ipGroup-test<br>Se você inserir um grupo de segurança, todos os ECSs associados ao grupo de segurança estarão em conformidade com a regra criada.<br>Para obter mais informações sobre grupos de endereços IP, consulte **Grupo de endereços IP**. | 0.0.0.0/0 |
| Description | (Opcional) Fornece informações complementares sobre a regra de grupo de segurança. Este parâmetro é opcional.<br>A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >). | - |

**Passo 9** Clique em **OK**.

**----Fim**

## 2.2.3.2 Conexão a uma instância de cluster usando Mongo Shell (rede privada)

O Mongo shell é o cliente padrão para o servidor de banco de dados MongoDB. Você pode usar o Mongo Shell para se conectar a instâncias de BD e consultar, atualizar e gerenciar dados em bancos de dados. Para usar o Mongo Shell, baixe e instale o cliente de MongoDB primeiro e, em seguida, use o Mongo shell para se conectar à instância de BD.

Por padrão, uma instância do DDS fornece um endereço IP privado. Se suas aplicações forem implementadas em um ECS e estiverem na mesma região e VPC que as instâncias do DDS, você poderá se conectar a instâncias do DDS usando um endereço IP privado para obter uma taxa de transmissão rápida e alta segurança.

Esta seção descreve como usar o Mongo Shell para se conectar a uma instância de cluster em uma rede privada.

Você pode se conectar a uma instância usando uma conexão SSL ou uma conexão não criptografada. A conexão SSL é criptografada e mais segura. Para melhorar a segurança da transmissão de dados, conecte-se a instâncias usando SSL.

## Pré-requisitos

1. Para obter detalhes sobre como criar e fazer logon em um ECS, consulte **Compra de um ECS** e **Logon em um ECS**.
2. Instale o cliente de MongoDB no ECS. Para garantir a autenticação bem-sucedida, instale o cliente de MongoDB da mesma versão da instância de destino.

   Para obter detalhes sobre como instalar um cliente de MongoDB, consulte **Como instalar um cliente de MongoDB?**
3. O ECS pode se comunicar com a instância do DDS. Para mais detalhes, consulte **Configuração de regras de grupo de segurança**.

## Conexão SSL

AVISO

Se você se conectar a uma instância por meio da conexão SSL, ative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como ativar SSL, consulte **Ativação e desativação de SSL**.

**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 e escolha **Databases** > **Document Database Service**.

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

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

**Passo 6** Na área **Basic Information**, clique em ao lado do campo **SSL**.

**Passo 7** Carregue o certificado raiz para o ECS a ser conectado à instância.

A seguir, descrevemos como fazer upload do certificado para um ECS do Linux e Window:

- No Linux, execute o seguinte comando:

  **scp** *<IDENTITY_FILE><REMOTE_USER>@<REMOTE_ADDRESS>*:*<REMOTE_DIR>*

  NOTA

  - **IDENTITY_FILE** é o diretório onde o certificado raiz reside. A permissão de acesso ao arquivo é 600.
  - **REMOTE_USER** é o usuário do sistema operacional ECS.
  - **REMOTE_ADDRESS** é o endereço do ECS.
  - **REMOTE_DIR** é o diretório do ECS no qual o certificado raiz é carregado.
- No Windows, carregue o certificado raiz usando uma ferramenta de conexão remota.

**Passo 8** Conecte-se à instância no diretório em que o cliente de MongoDB está localizado.

Método 1: endereço de conexão HA privada (recomendado)

O DDS fornece um endereço de conexão HA privada que consiste em endereços IP e portas de todos os nós do MongoDB em uma instância de cluster. Você pode usar esse endereço para se conectar à instância de cluster para melhorar a disponibilidade da instância de cluster.

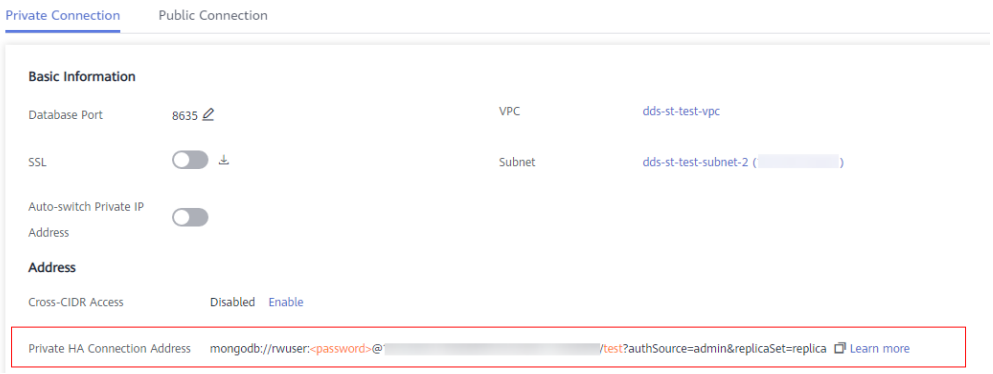
Exemplo de comando:

**./mongo** <*Private HA connection address*> **--ssl --sslCAFile** <*FILE_PATH*> **--sslAllowInvalidHostnames**

Descrição do parâmetro:

- **Private HA Connection Address**: na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida. Escolha **Connections**. Clique na guia **Private Connection** e obtenha o endereço de conexão da instância atual do campo **Private HA Connection Address**.

  **Figura 2-12** Obter o endereço de conexão HA privada

  O formato do endereço de conexão privada é o seguinte. O nome de usuário do banco de dados **rwuser** e o banco de dados de autenticação **admin** não podem ser alterados.

  **mongodb://rwuser:**<*password*>*@192.168.xx.xx:8635,192.168.xx.xx:8635*/**test?authSource=admin**

  Preste atenção aos seguintes parâmetros no endereço HA privado:

  **Tabela 2-11** Informações de parâmetro

| Parâmetro | Descrição |
| --- | --- |
| rwuser | Nome de usuário do banco de dados |
| <password> | Senha para o nome de usuário do banco de dados. Substitua-a pela senha atual.<br>Se a senha contiver sinais de arroba (@), pontos de exclamação (!) ou sinais de porcentagem (%), substitua-os por códigos de URL hexadecimais (ASCII) %40, %21 e %25, respectivamente.<br>Por exemplo, se a senha for ****@ %***!, o código de URL correspondente será **** %40%25*** %21. |
| 192.168.xx.xx:8635,192.168.xx.xx:8635 | Endereço IP e porta do nó mongos da instância de cluster a ser conectada |

| Parâmetro | Descrição |
| --- | --- |
| test | O nome do banco de dados de teste. Você pode definir esse parâmetro com base em seus requisitos de serviço. |
| authSource=admin | O banco de dados de autenticação do usuário **rwuser** deve ser **admin**. **authSource=admin** é corrigido no comando. |

- **FILE_PATH** é o caminho para armazenar o certificado raiz.
- **--sslAllowInvalidHostnames**: para garantir que a comunicação interna do cluster não ocupe recursos como o endereço IP do usuário e a largura de banda, o certificado do cluster é gerado usando o endereço IP de gerenciamento interno. **--sslAllowInvalidHostnames** é necessário para a conexão SSL por meio de uma rede privada.

Exemplo de comando:

**./mongo mongodb://rwuser:***<password>*@192.168.xx.xx:8635,192.168.xx.xx:8635/**test?authSource=admin --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames**

Método 2: conexão HA privada (banco de dados e conta definidos pelo usuário)

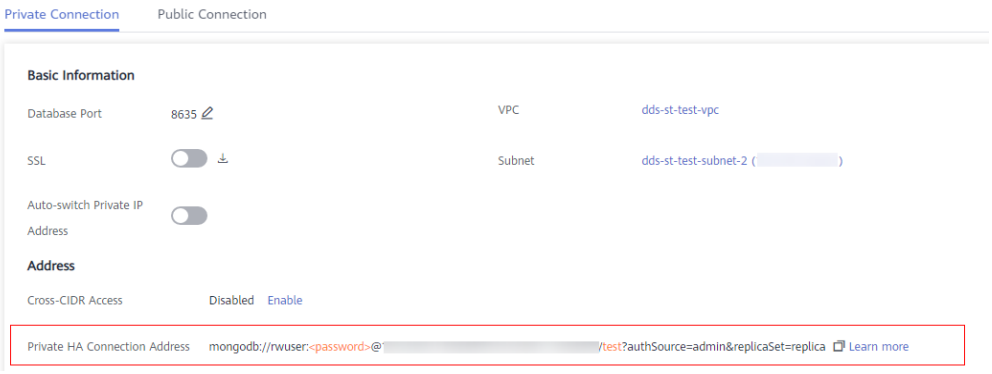
Exemplo de comando:

**./mongo "***<Private HA Connection Address>***"**

Descrição do parâmetro:

- **Private HA Connection Address**: na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida. Escolha **Connections**. Clique na guia **Private Connection** e obtenha o endereço de conexão da instância atual do campo **Private HA Connection Address**.

  **Figura 2-13** Obter o endereço de conexão HA privada




  O formato do endereço de conexão HA privada obtido é o seguinte:

  **mongodb://rwuser:***<password>*@192.168.xx.xx:8635,192.168.xx.xx:8635/**test?authSource=admin**

  A tabela a seguir lista os parâmetros necessários no endereço HA privado.

**Tabela 2-12** Informações de parâmetro

| Parâmetro | Descrição |
| --- | --- |
| rwuser | Nome de usuário do banco de dados. O valor padrão é **rwuser**. Você pode alterar o valor para o nome de usuário com base em seus requisitos de serviço. |
| <password> | Senha para o nome de usuário do banco de dados. Substitua-a pela senha atual.<br>Se a senha contiver sinais de arroba (@), pontos de exclamação (!) ou sinais de porcentagem (%), substitua-os por códigos de URL hexadecimais (ASCII) %40, %21 e %25, respectivamente.<br>Por exemplo, se a senha for ****@ %***!, o código de URL correspondente será **** %40%25*** %21. |
| 192.168.xx.xx:8635,192.168.xx.xx:8635 | Endereço IP e porta do nó mongos da instância de cluster a ser conectada |
| test | O nome do banco de dados de teste. Você pode definir esse parâmetro com base em seus requisitos de serviço. |
| authSource=admin | O banco de dados de autenticação do usuário **rwuser** é **admin**.<br>**NOTA**<br>Se você usar um banco de dados definido pelo usuário para autenticação, altere o banco de dados de autenticação no endereço de conexão de alta disponibilidade para o nome do banco de dados definido pelo usuário. Além disso, substitua **rwuser** pelo nome de usuário criado no banco de dados definido pelo usuário. |

- **FILE_PATH** é o caminho para armazenar o certificado raiz.
- **--sslAllowInvalidHostnames**: para garantir que a comunicação interna do cluster não ocupe recursos como o endereço IP do usuário e a largura de banda, o certificado do cluster é gerado usando o endereço IP de gerenciamento interno. **--sslAllowInvalidHostnames** é necessário para a conexão SSL por meio de uma rede privada.

Por exemplo, se você criar um banco de dados definido pelo usuário **Database** e um usuário **test1** no banco de dados, o comando de conexão será o seguinte:

**./mongo mongodb://test1:***<password>*@192.168.xx.xx:8635,192.168.xx.xx:8635/**Database? authSource=Database --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames**

Método 3: usar um endereço IP privado

Exemplo de comando:

**./mongo --host** <*DB_HOST*> **--port** <*DB_PORT*> **-u** <*DB_USER*> **-p --authenticationDatabase admin --ssl --sslCAFile** <*FILE_PATH*> **--sslAllowInvalidHostnames**

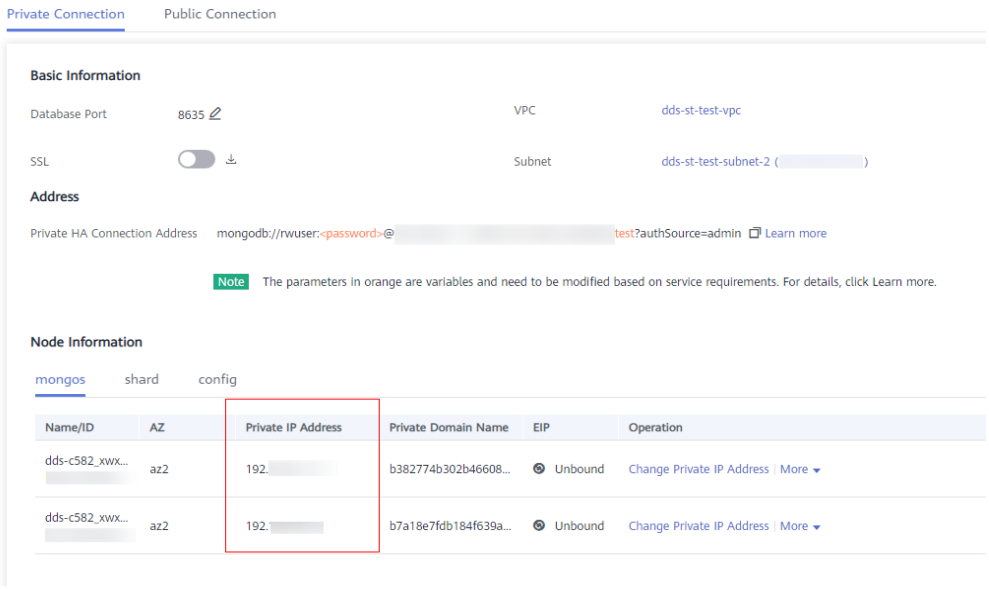
Descrição do parâmetro:

- **DB_HOST** é o endereço IP do nó mongos da instância de cluster a ser conectada.

  Clique no nome da instância. Na página **Basic Information**, escolha **Connections** > **Private Connection**, obtenha o endereço IP privado do nó mongos na guia **mongos** na área **Node Information**.

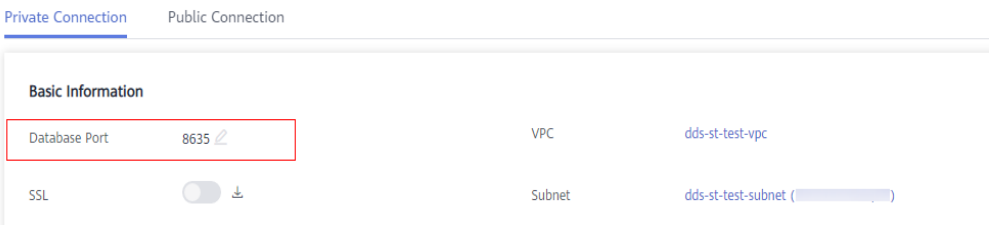
  **Figura 2-14** Obter o endereço IP privado

- **DB_PORT** é a porta da instância a ser conectada. A porta padrão é 8635.

  Clique no nome da instância. Na página **Basic Information**, escolha **Connections**. Na guia **Private Connection**, obtenha as informações da porta do banco de dados no campo **Database Port** da página **Basic Information**.

  **Figura 2-15** Obter a porta

- **DB_USER** é o usuário do banco de dados. O valor padrão é **rwuser**.
- **FILE_PATH** é o caminho para armazenar o certificado raiz.
- **--sslAllowInvalidHostnames**: para garantir que a comunicação interna do cluster não ocupe recursos como o endereço IP do usuário e a largura de banda, o certificado do cluster é gerado usando o endereço IP de gerenciamento interno. **--sslAllowInvalidHostnames** é necessário para a conexão SSL por meio de uma rede privada.

Digite a senha da conta do banco de dados quando solicitado:

```
Enter password:
```

Exemplo de comando:

**./mongo --host 192.168.1.6 --port 8635 -u rwuser -p --authenticationDatabase admin --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames**

**Passo 9** Verifique o resultado da conexão. Se as informações a seguir forem exibidas, a conexão será bem-sucedida.

```
mongos>
```

**----Fim**

## Conexão não criptografada

**AVISO**

Se você se conectar a uma instância por meio de uma conexão não criptografada, desative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como desabilitar SSL, consulte **Ativação e desativação de SSL**.

**Passo 1** Conecte-se ao ECS.

**Passo 2** Conecte-se à instância no diretório em que o cliente de MongoDB está localizado.

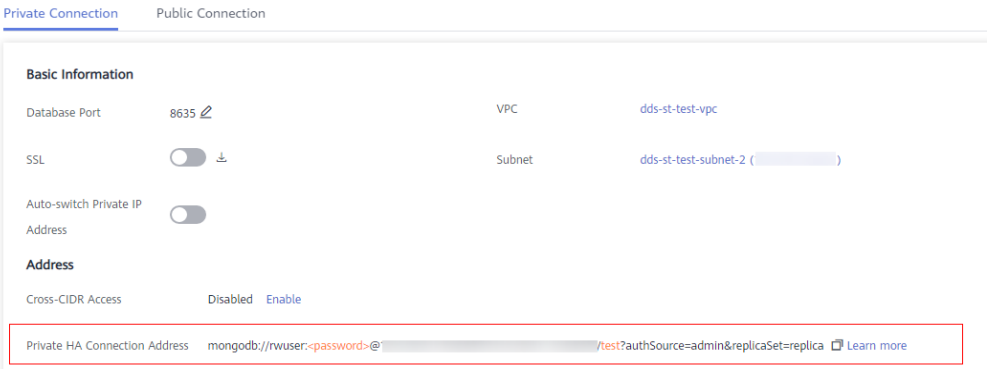
Método 1: endereço de conexão HA privada (recomendado)

Exemplo de comando:

**./mongo "***<Private HA Connection Address>***"**

**Private HA Connection Address**: na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida. Escolha **Connections**. Clique na guia **Private Connection** e obtenha o endereço de conexão da instância atual do campo **Private HA Connection Address**.

**Figura 2-16** Obter o endereço de conexão HA privada




O formato do endereço de conexão privada é o seguinte. O nome de usuário do banco de dados **rwuser** e o banco de dados de autenticação **admin** não podem ser alterados.

**mongodb://rwuser:***<password>@192.168.xx.xx:8635,192.168.xx.xx:8635***/test?authSource=admin**

A tabela a seguir lista os parâmetros necessários no endereço HA privado.

**Tabela 2-13** Informações de parâmetro

| Parâmetro | Descrição |
| --- | --- |
| rwuser | Nome de usuário do banco de dados |
| <password> | Senha para o nome de usuário do banco de dados. Substitua-a pela senha atual.<br>Se a senha contiver sinais de arroba (@), pontos de exclamação (!) ou sinais de porcentagem (%), substitua-os por códigos de URL hexadecimais (ASCII) %40, %21 e %25, respectivamente.<br>Por exemplo, se a senha for ****@ %***!, o código de URL correspondente será **** %40%25*** %21. |
| 192.168.xx.xx:8635,192.168.xx.xx:8635 | Endereço IP e porta do nó mongos da instância de cluster a ser conectada |
| test | O nome do banco de dados de teste. Você pode definir esse parâmetro com base em seus requisitos de serviço. |
| authSource=admin | O banco de dados de autenticação do usuário **rwuser** deve ser **admin**. **authSource=admin** é corrigido no comando. |

Exemplo de comando:

**./mongo mongodb://rwuser:***<password>*@*192.168.xx.xx:8635,192.168.xx.xx:8635*/**test?authSource=admin**

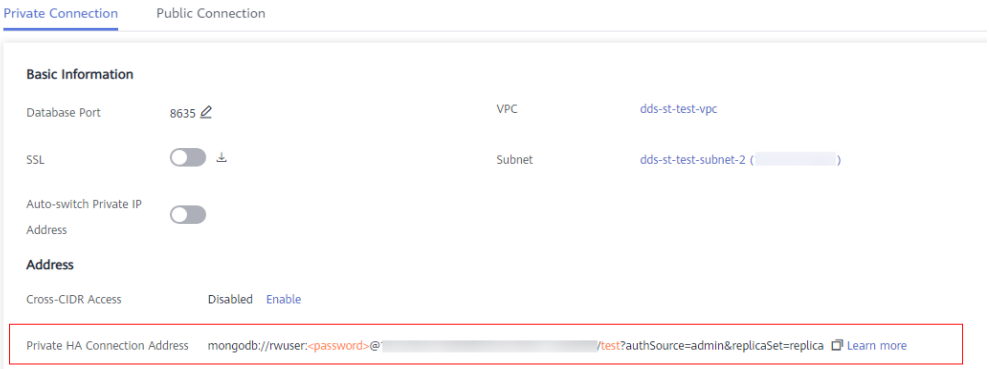
Método 2: conexão HA privada (banco de dados e conta definidos pelo usuário)

Exemplo de comando:

**./mongo "***<Private HA Connection Address>***"**

**Private HA Connection Address**: na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida. Escolha **Connections**. Clique na guia **Private Connection** e obtenha o endereço de conexão da instância atual do campo **Private HA Connection Address**.

**Figura 2-17** Obter o endereço de conexão HA privada



O formato do endereço de conexão HA privada obtido é o seguinte:

**mongodb://rwuser:**<*password*>*@192.168.xx.xx:8635,192.168.xx.xx:8635*/**test?authSource=admin**

A tabela a seguir lista os parâmetros necessários no endereço HA privado.

**Tabela 2-14** Informações de parâmetro

| Parâmetro | Descrição |
| --- | --- |
| rwuser | Nome de usuário do banco de dados. O valor padrão é **rwuser**. Você pode alterar o valor para o nome de usuário com base em seus requisitos de serviço. |
| <password> | Senha para o nome de usuário do banco de dados. Substitua-a pela senha atual.<br>Se a senha contiver sinais de arroba (@), pontos de exclamação (!) ou sinais de porcentagem (%), substitua-os por códigos de URL hexadecimais (ASCII) %40, %21 e %25, respectivamente.<br>Por exemplo, se a senha for ****@ %***!, o código de URL correspondente será **** %40%25*** %21. |
| 192.168.xx.xx:8635,192.168.xx.xx:8635 | Endereço IP e porta do nó mongos da instância de cluster a ser conectada |
| test | O nome do banco de dados de teste. Você pode definir esse parâmetro com base em seus requisitos de serviço. |
| authSource=admin | O banco de dados de autenticação do usuário **rwuser** é **admin**.<br>**NOTA**<br>Se você usar um banco de dados definido pelo usuário para autenticação, altere o banco de dados de autenticação no endereço de conexão de alta disponibilidade para o nome do banco de dados definido pelo usuário. Além disso, substitua **rwuser** pelo nome de usuário criado no banco de dados definido pelo usuário. |

Por exemplo, se você criar um banco de dados definido pelo usuário **Database** e um usuário **test1** no banco de dados, o comando de conexão será o seguinte:

**./mongo mongodb://test1:**<*password*>*@192.168.xx.xx:8635,192.168.xx.xx:8635*/**Database?authSource=Database**

Método 3: usar um endereço IP privado

Exemplo de comando:

**./mongo --host** <*DB_HOST*> **--port** <*DB_PORT*> **-u** <*DB_USER*> **-p --authenticationDatabase admin**

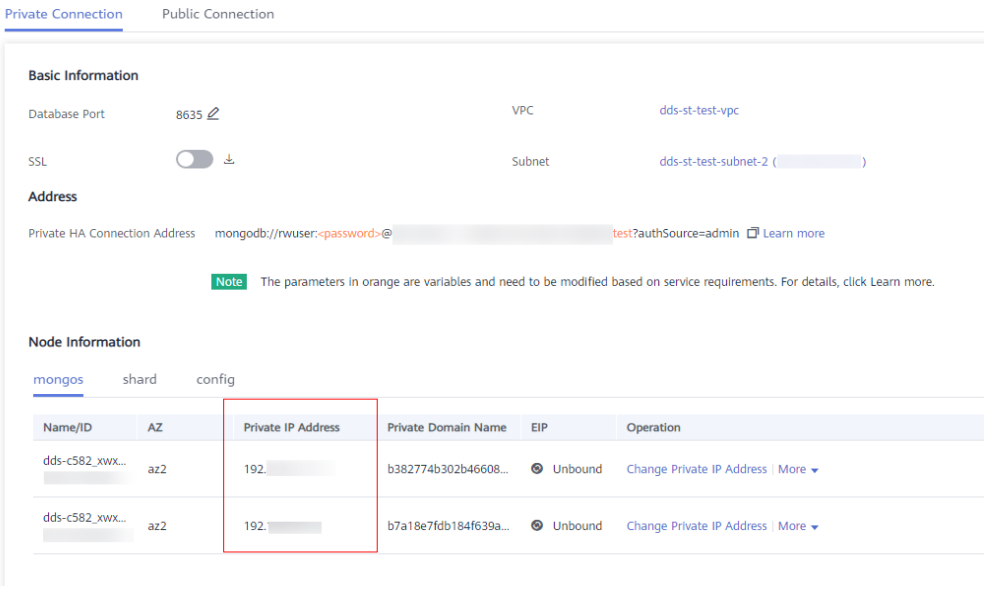
Descrição do parâmetro:

- **DB_HOST** é o endereço IP do nó mongos da instância de cluster a ser conectada.

Clique no nome da instância. Na página **Basic Information**, escolha **Connections** > **Private Connection**, obtenha o endereço IP privado do nó mongos na guia **mongos** na área **Node Information**.

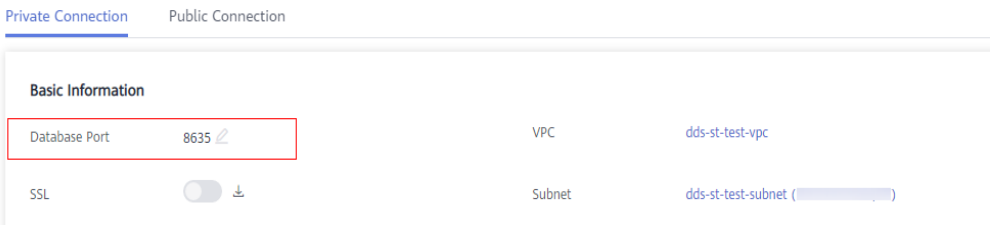
**Figura 2-18** Obter o endereço IP privado




- **DB_PORT** é a porta da instância a ser conectada. A porta padrão é 8635.

  Clique no nome da instância. Na página **Basic Information**, escolha **Connections**. Na guia **Private Connection**, obtenha as informações da porta do banco de dados no campo **Database Port** da página **Basic Information**.

  **Figura 2-19** Obter a porta

- **DB_USER** é o usuário do banco de dados. O valor padrão é **rwuser**.

Digite a senha do banco de dados quando solicitado:

```
Enter password:
```

Exemplo de comando:

**./mongo --host 192.168.1.6 --port 8635 -u rwuser -p --authenticationDatabase admin**

**Passo 3** Verifique o resultado da conexão. Se as informações a seguir forem exibidas, a conexão será bem-sucedida.

```
mongos>
```

**----Fim**

## 2.2.4 Conexão a uma instância de cluster em uma rede pública

## 2.2.4.1 Vinculação ou desvinculação de um EIP

Depois de criar uma instância de cluster, você pode vincular um EIP a ela para permitir acesso externo. Se mais tarde você quiser proibir o acesso externo, você também pode desvincular o EIP da instância.

## Precauções

- A exclusão de um EIP vinculado não significa que o EIP não esteja vinculado.
- Antes de acessar um banco de dados, solicite um EIP no console da VPC. Em seguida, adicione uma regra de entrada para permitir os endereços IP ou intervalos de endereços IP de ECSs. Para mais detalhes, consulte **Configuração de um grupo de segurança**.
- Na instância do cluster, somente os mongos podem ter um EIP vinculado. Para alterar o EIP que foi vinculado a um nó, você precisa desvinculá-lo do nó primeiro.

## Vincular um EIP

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

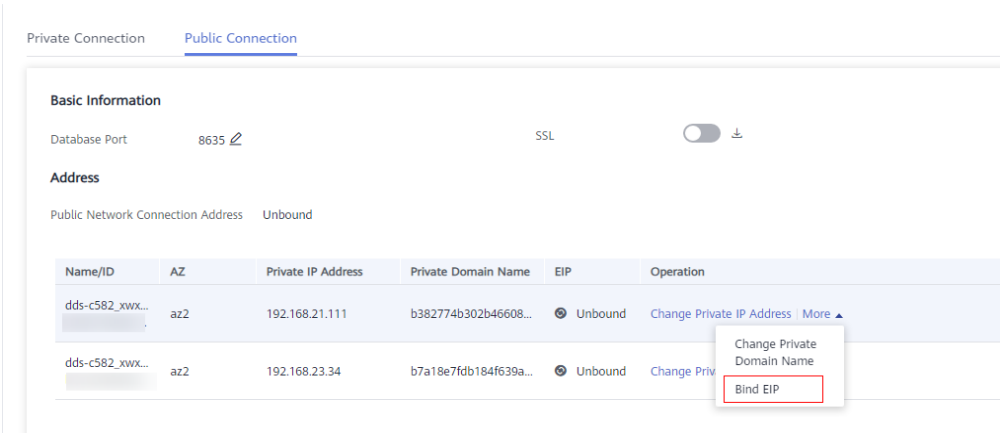
**Passo 2** Clique em no canto superior esquerdo e selecione uma região e um projeto.

**Passo 3** Clique em no canto superior esquerdo da página e escolha **Databases** > **Document Database Service**.

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

**Passo 5** No painel de navegação à esquerda, escolha **Connections**. Clique na guia **Public Connection**. Na área **Basic Information**, localize o nó e clique em **Bind EIP** na coluna **Operation**.

**Figura 2-20** Vincular um EIP



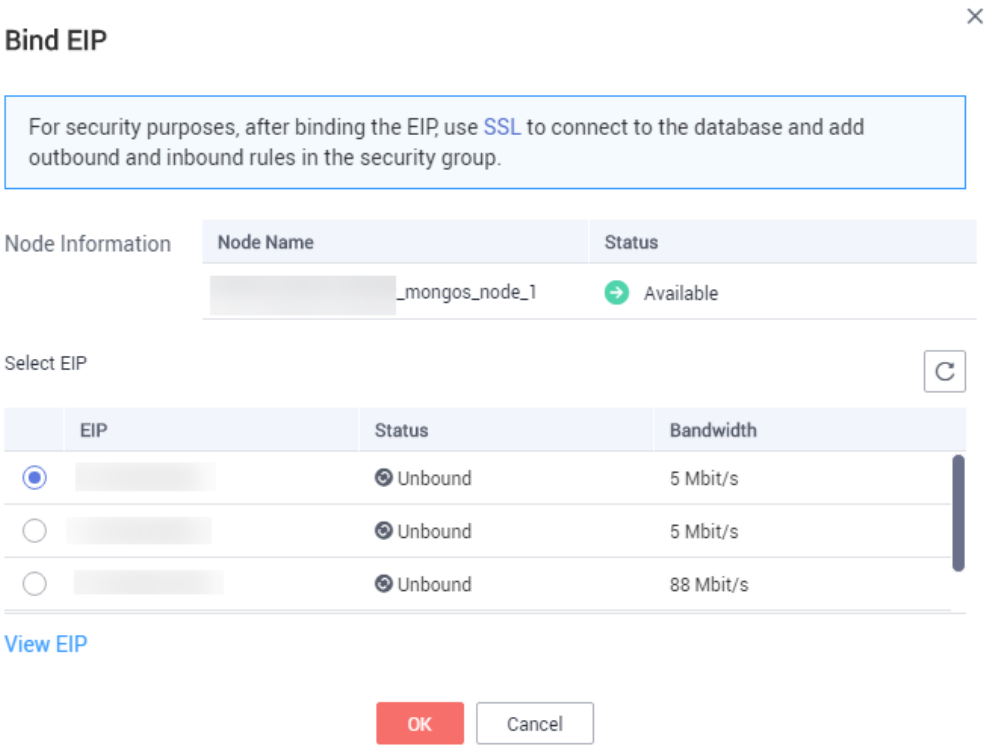

Alternativamente, na área **Node Information** na página **Basic Information**, localize o nó mongos e escolha **More** > **Bind EIP** na coluna **Operation**.

**Figura 2-21** Vincular um EIP


**Passo 6** Na caixa de diálogo exibida, todos os EIPs não vinculados e disponíveis são listados. Selecione o EIP necessário e clique em **OK**. Se nenhum EIP disponível for exibido, clique em **View EIP** e crie um EIP no console da VPC.

**Figura 2-22** Selecionar um EIP




**Passo 7** Na coluna **EIP** na guia **mongos**, você pode exibir o EIP que foi vinculado.

Para desvincular um EIP da instância, consulte **Desvinculação de um EIP**.

**----Fim**

## Desvinculação de um EIP

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

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

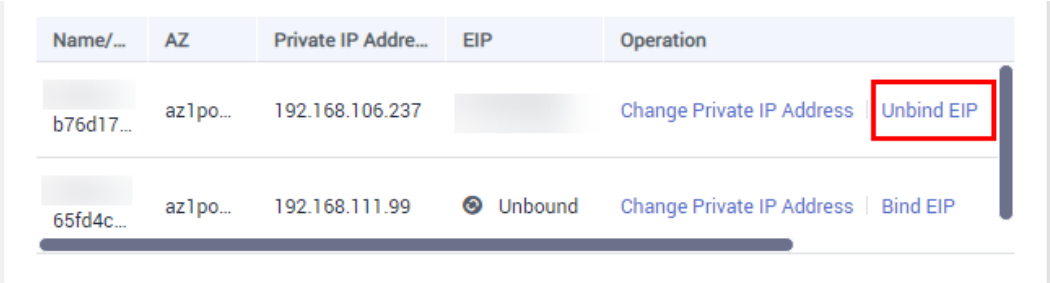
**Passo 3** Clique em no canto superior esquerdo da página e escolha **Databases** > **Document Database Service**.

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

**Passo 5** No painel de navegação à esquerda, escolha **Connections**. Clique na guia **Public Connection**. Na área **Basic Information**, localize o nó mongos e clique em **Unbind EIP** na coluna **Operation**.

**Figura 2-23** Desvinculação de um EIP




Alternativamente, na área **Node Information** da página **Basic Information**, localize o nó mongos e escolha **More** > **Unbind EIP** na coluna **Operation**.

**Passo 6** Na caixa de diálogo exibida, clique em **Yes**.

Para vincular um EIP à instância novamente, consulte **Vincular um EIP**.

**----Fim**

## 2.2.4.2 Configuração de um grupo de segurança

Um grupo de segurança é uma coleção de regras de controle de acesso para ECSs e instâncias do DDS que têm os mesmos requisitos de proteção de segurança e são mutuamente confiáveis em uma VPC.

Para garantir a segurança e a confiabilidade do banco de dados, é necessário configurar regras de grupo de segurança para permitir que endereços IP e portas específicos acessem instâncias do DDS.

Para acessar uma instância da Internet, adicione uma regra de entrada para o grupo de segurança associado à instância.

## Precauções

- Por predefinição, uma conta pode criar até 500 regras de grupo de segurança.
- Muitas regras de grupo de segurança aumentarão a latência do primeiro pacote, portanto, recomenda-se um máximo de 50 regras para cada grupo de segurança.
- Uma instância do DDS só pode ser associada a um grupo de segurança.

## 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 e escolha **Databases** > **Document Database Service**.

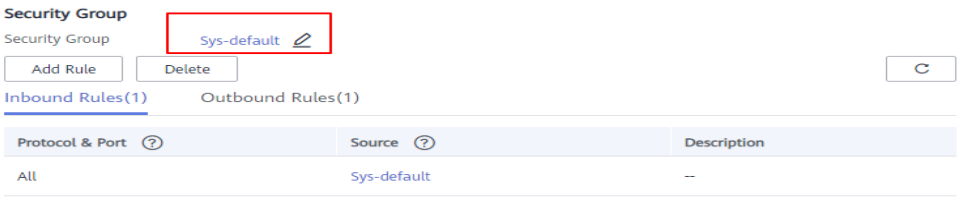
**Passo 4** Na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida.

**Passo 5** Na área **Network Information** da página **Basic Information**, clique no nome do grupo de segurança.

**Figura 2-24** Grupo de segurança


Você também pode escolher **Connections** no painel de navegação à esquerda. Na guia **Public Connection**, na área **Security Group**, clique no nome do grupo de segurança.

**Figura 2-25** Grupo de segurança




**Passo 6** Na página **Security Group**, localize o grupo de segurança de destino e clique em **Manage Rule** na coluna **Operation**.

**Passo 7** Na guia **Inbound Rules**, clique em **Add Rule**. A caixa de diálogo **Add Inbound Rule** é exibida.

**Passo 8** Adicione uma regra de grupo de segurança conforme solicitado.

**Figura 2-26** Adicionar regra de entrada

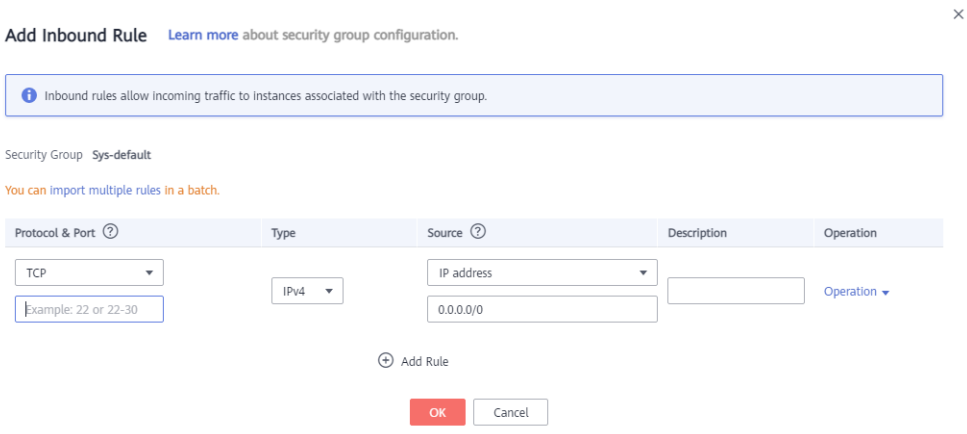


**Tabela 2-15** Configurações da regra de entrada

| Parâmetro | Descrição | Exemplo de valor |
| --- | --- | --- |
| Priority | A prioridade da regra do grupo de segurança.<br>O valor de prioridade varia de 1 a 100. A prioridade padrão é 1 e tem a prioridade mais alta. A regra de grupo de segurança com um valor menor tem uma prioridade mais alta. | 1 |
| Action | As ações de regra do grupo de segurança.<br>Uma regra com uma ação de negação substitui outra com uma ação de permitir se as duas regras tiverem a mesma prioridade. | Allow |
| Protocol & Port | O protocolo de rede necessário para o acesso. A opção pode ser **All**, **TCP**, **UDP**, **ICMP** ou **GRE**. | TCP |
| | Porta: a porta na qual você deseja permitir o acesso ao DDS. A porta padrão é 8635. A porta varia de 2100 a 9500 ou pode ser 27017, 27018 ou 27019. | 8635 |
| Type | Tipo do endereço IP. Apenas **IPv4** e **IPv6** são suportados. | IPv4 |
| Source | Especifica o endereço IP, o grupo de segurança e o grupo de endereços IP suportados, que permitem o acesso de endereços IP ou instâncias em outro grupo de segurança. Exemplo:<br>● Endereço IP único: 192.168.10.10/32<br>● Segmento do endereço IP: 192.168.1.0/24<br>● Todos os endereços IP: 0.0.0.0/0<br>● Grupo de segurança: sg-abc<br>● Grupo de endereço IP: ipGroup-test<br>Se você inserir um grupo de segurança, todos os ECSs associados ao grupo de segurança estarão em conformidade com a regra criada.<br>Para obter mais informações sobre grupos de endereços IP, consulte **Grupo de endereços IP**. | 0.0.0.0/0 |
| Description | (Opcional) Fornece informações complementares sobre a regra de grupo de segurança. Este parâmetro é opcional.<br>A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >). | - |

**Passo 9** Clique em **OK**.

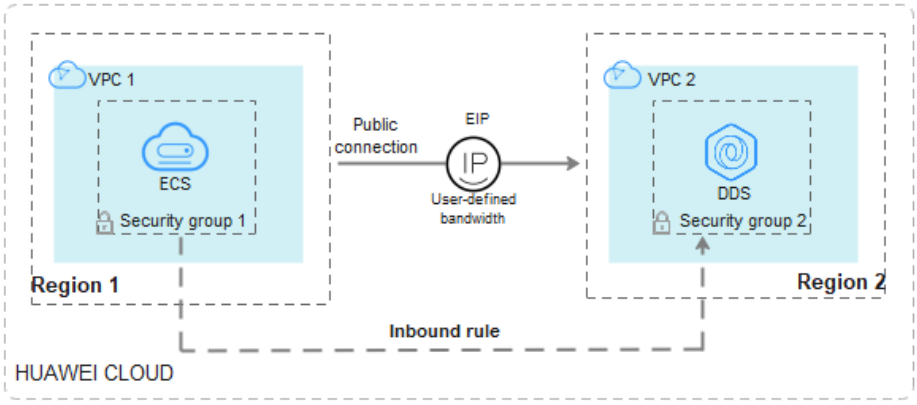
**----Fim**

## 2.2.4.3 Conexão a uma instância de cluster usando Mongo Shell (rede pública)

Nos cenários a seguir, você pode acessar uma instância do DDS da Internet vinculando um EIP à instância.

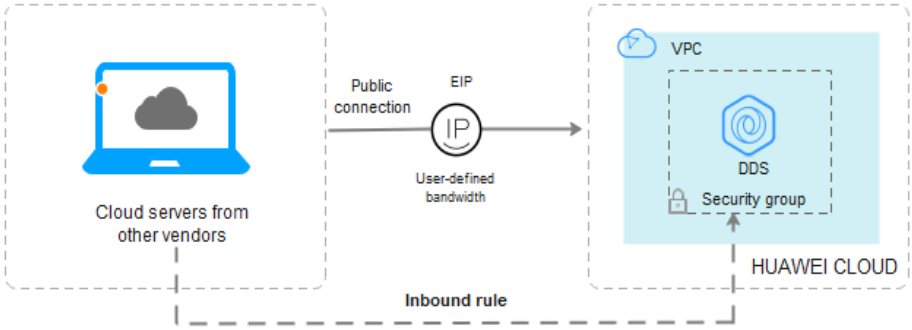
Cenário 1: suas aplicações são implementadas em um ECS e não estão na mesma região que a instância do DDS.

**Figura 2-27** Acessar o DDS a partir do ECS em todas as regiões




Cenário 2: suas aplicações são implementadas em um servidor de nuvem fornecido por outros fornecedores.

**Figura 2-28** Acessar o DDS de outros servidores em nuvem




Esta seção descreve como usar o Mongo Shell para se conectar a uma instância de cluster em uma rede pública.

Você pode se conectar a uma instância usando uma conexão SSL ou uma conexão não criptografada. A conexão SSL é criptografada e mais segura. Para melhorar a segurança da transmissão de dados, conecte-se a instâncias usando SSL.

## Pré-requisitos

1. Para obter detalhes sobre como criar e fazer logon em um ECS, consulte **Compra de um ECS** e **Logon em um ECS**.
2. **Vincular um EIP** à instância de cluster e **definir regras de grupo de segurança** para garantir que a instância possa ser acessada a partir do ECS.
3. Instale o cliente de MongoDB no ECS.

   Para obter detalhes sobre como instalar um cliente de MongoDB, consulte **Como instalar um cliente de MongoDB?**

## SSL

AVISO

Se você se conectar a uma instância por meio da conexão SSL, ative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como ativar SSL, consulte **Ativação e desativação de SSL**.

**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 e escolha **Databases** > **Document Database Service**.

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

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

**Passo 6** Na área **Basic Information**, clique em ao lado do campo **SSL**.

**Passo 7** Carregue o certificado raiz obtido na **Passo 6** no ECS.

A seguir, descrevemos como fazer upload do certificado para um ECS do Linux e Window:

- No Linux, execute o seguinte comando:

  **scp***<IDENTITY_FILE>**<REMOTE_USER>**@***<REMOTE_ADDRESS>***:***<REMOTE_DIR>*

  NOTA

  - **IDENTITY_FILE** é o diretório onde o certificado raiz reside. A permissão de acesso ao arquivo é 600.
  - **REMOTE_USER** é o usuário do sistema operacional ECS.
  - **REMOTE_ADDRESS** é o endereço do ECS.
  - **REMOTE_DIR** é o diretório do ECS no qual o certificado raiz é carregado.
- No Windows, carregue o certificado raiz usando uma ferramenta de conexão remota.

**Passo 8** Conecte-se à instância no diretório em que o cliente de MongoDB está localizado.

Método 1: utilizar um endereço de conexão de rede pública

Exemplo de comando:

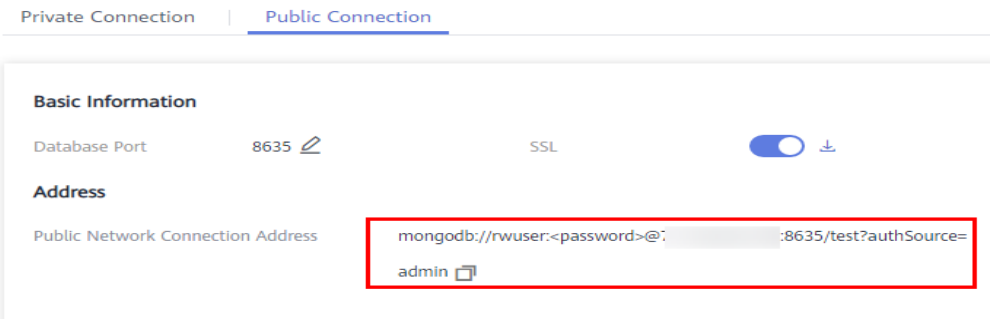
  

**./mongo** <*Public network connection address*> **--ssl --sslCAFile** <*FILE_PATH*> **--sslAllowInvalidHostnames**

Descrição do parâmetro:

- **Public Network Connection Address**: na página **Instances**, clique na instância para navegar até a página **Basic Information**. No painel de navegação à esquerda, escolha **Connections**. Na página exibida, clique na guia **Public Connection**. Na área **Address**, obtenha o endereço de conexão da instância no campo **Public Network Connection Address**.

  **Figura 2-29** Obter o endereço de conexão de rede pública

  O formato do endereço de conexão pública é o seguinte. O nome de usuário do banco de dados **rwuser** e o banco de dados de autenticação **admin** não podem ser alterados.

  **mongodb://rwuser:**<*password*>@192.168.*xx.xx*:8635**/test?authSource=admin**

  Preste atenção aos seguintes parâmetros no endereço de conexão pública:

  **Tabela 2-16** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| rwuser | Nome da conta, ou seja, o nome de usuário do banco de dados. |
| <*password*> | Senha da conta do banco de dados. Substitua-a pela senha atual.<br>Se a senha contiver sinais de arroba (@), pontos de exclamação (!), substitua-os por códigos de URL hexadecimais (ASCII) %40, %21 e %25, respectivamente.<br>Por exemplo, se a senha for ****@ %***!, o código de URL correspondente será **** %40%25*** %21. |
| 192.168.*xx.xx*:8635 | EIP e porta vinculados ao nó mongos da instância de cluster |
| test | O nome do banco de dados de teste. Você pode definir esse parâmetro com base em seus requisitos de serviço. |
| authSource=admin | O banco de dados de autenticação do usuário **rwuser** deve ser **admin**. **authSource=admin** é corrigido no comando. |

- **FILE_PATH** é o caminho para armazenar o certificado raiz.
- **--sslAllowInvalidHostnames**: para garantir que a comunicação interna do cluster não ocupe recursos como o endereço IP do usuário e a largura de banda, o certificado do

cluster é gerado usando o endereço IP de gerenciamento interno. **--sslAllowInvalidHostnames** é necessário para a conexão SSL por meio de uma rede pública.

Exemplo de comando:

**./mongo mongodb://rwuser:**<*password*>@192.168.*xx.xx*:8635**/test?authSource=admin --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames**

Método 2: conectar-se a uma instância usando um EIP.

Exemplo de comando:

**./mongo --host** <*DB_HOST*> **--port** <*DB_PORT*> **-u** <*DB_USER*> **-p --authenticationDatabase admin --ssl --sslCAFile** <*FILE_PATH*> **--sslAllowInvalidHostnames**

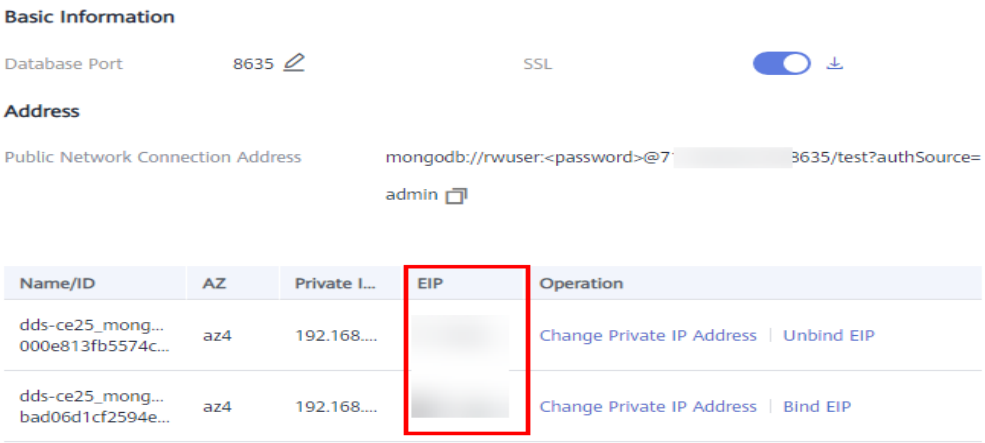
Descrição do parâmetro:

- **DB_HOST** é o EIP vinculado à instância a ser conectada.

  você pode clicar no nome da instância para ir para a página **Basic Information**. No painel de navegação à esquerda, escolha **Connections**. Na guia **Public Connection**, obtenha o EIP vinculado ao nó mongos na coluna **EIP**.

  Se houver vários nós do MongoDB, o EIP de qualquer nó pode ser usado para se conectar à instância.

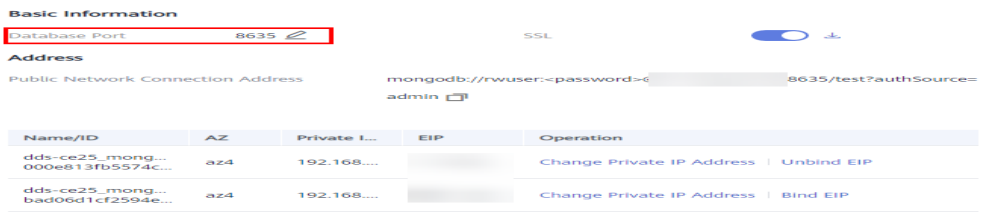
  **Figura 2-30** Obter um EIP

- **DB_PORT** é a porta da instância a ser conectada. O número de porta padrão é 8635.

  Você pode clicar na instância para ir para a página **Basic Information**. No painel de navegação à esquerda, escolha **Connections**. Na página exibida, clique na guia **Public Connection** e obtenha a porta no campo **Database Port** na área **Basic Information**.

  **Figura 2-31** Obter a porta

- **DB_USER** é o usuário do banco de dados. O valor padrão é **rwuser**.
- **FILE_PATH** é o caminho para armazenar o certificado raiz.
- **--sslAllowInvalidHostnames**: para garantir que a comunicação interna do cluster não ocupe recursos como o endereço IP do usuário e a largura de banda, o certificado do cluster é gerado usando o endereço IP de gerenciamento interno. **--sslAllowInvalidHostnames** é necessário para a conexão SSL por meio de uma rede pública.

Digite a senha da conta do banco de dados quando solicitado:

```
Enter password:
```

Exemplo de comando:

**./mongo --host** *192.168.xx.xx* **--port 8635 -u rwuser -p --authenticationDatabase admin --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames**

**Passo 9** Verifique o resultado da conexão. Se as informações a seguir forem exibidas, a conexão será bem-sucedida.

```
mongos>
```

**----Fim**

## Conexão não criptografada

**AVISO**

Se você se conectar a uma instância por meio de uma conexão não criptografada, desative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como desabilitar SSL, consulte **Ativação e desativação de SSL**.

**Passo 1** Efetue logon no ECS.

**Passo 2** Conecte-se à instância no diretório em que o cliente de MongoDB está localizado.

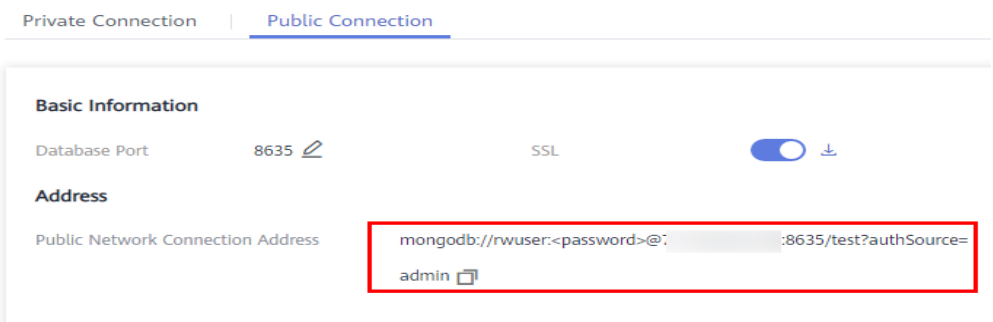
Método 1: utilizar um endereço de conexão de rede pública

Exemplo de comando:

**./mongo** <*Public network address*>

**Public Network Connection Address**: você pode clicar no nome da instância para ir para a página **Basic Information**. No painel de navegação à esquerda, escolha **Connections**. Na página exibida, clique na guia **Public Connection**. Na área **Address**, obtenha o endereço de conexão da instância no campo **Public Network Connection Address**.

**Figura 2-32** Obter o endereço de conexão de rede pública



O formato do endereço de conexão pública é o seguinte. O nome de usuário do banco de dados **rwuser** e o banco de dados de autenticação **admin** não podem ser alterados.

**mongodb://rwuser:**<*password*>@192.168.*xx.xx*:8635**/test?authSource=admin**

A tabela a seguir descreve os parâmetros necessários no endereço de conexão pública.

**Tabela 2-17** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| rwuser | Nome da conta, ou seja, o nome de usuário do banco de dados. |
| <*password*> | Senha da conta do banco de dados. Substitua-a pela senha atual.<br>Se a senha contiver sinais de arroba (@), pontos de exclamação (!), substitua-os por códigos de URL hexadecimais (ASCII) %40, %21 e %25, respectivamente.<br>Por exemplo, se a senha for ****@ %***!, o código de URL correspondente será **** %40%25*** %21. |
| 192.168.*xx.xx*:8635 | EIP e porta vinculados ao nó mongos da instância de cluster |
| test | O nome do banco de dados de teste. Você pode definir esse parâmetro com base em seus requisitos de serviço. |
| authSource=admin | O banco de dados de autenticação do usuário **rwuser** deve ser **admin**. **authSource=admin** é corrigido no comando. |

Exemplo de comando:

**./mongo mongodb://rwuser:**<*password*>@192.168.*xx.xx*:8635**/test?authSource=admin**

Método 2: usar um EIP

Exemplo de comando:

**./mongo --host** <*DB_HOST*> **--port** <*DB_PORT*> **-u** <*DB_USER*> **-p --authenticationDatabase admin**

Descrição do parâmetro:

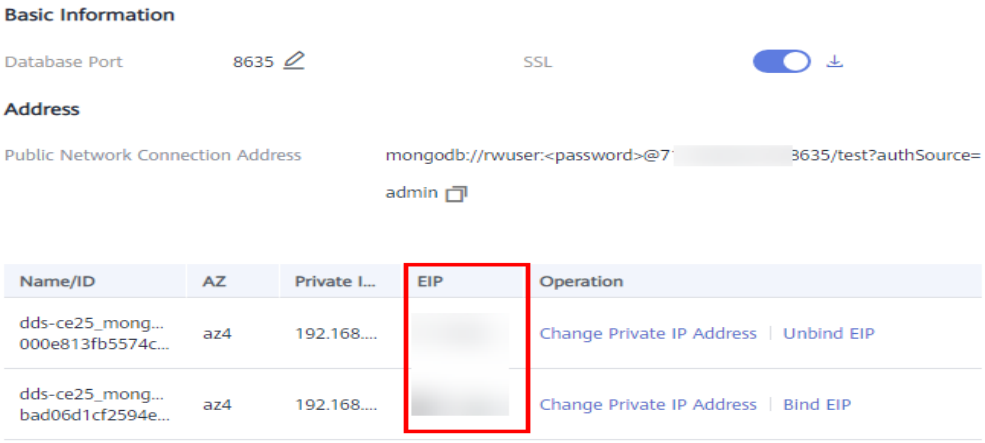
- **DB_HOST** é o EIP vinculado à instância a ser conectada.

  você pode clicar no nome da instância para ir para a página **Basic Information**. No painel de navegação à esquerda, escolha **Connections**. Na guia **Public Connection**, obtenha o EIP vinculado ao nó mongos na coluna **EIP**.

  Se houver vários nós do MongoDB, o EIP de qualquer nó pode ser usado para se conectar à instância.

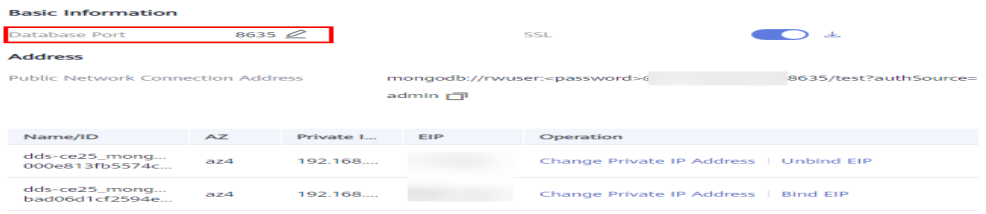
**Figura 2-33** Obter um EIP




- **DB_PORT** é a porta da instância a ser conectada. O número de porta padrão é 8635.

  Você pode clicar na instância para ir para a página **Basic Information**. No painel de navegação à esquerda, escolha **Connections**. Na página exibida, clique na guia **Public Connection** e obtenha a porta no campo **Database Port** na área **Basic Information**.

**Figura 2-34** Obter a porta




- **DB_USER** é o usuário do banco de dados. O valor padrão é **rwuser**.

Digite a senha da conta do banco de dados quando solicitado:

```
Enter password:
```

Exemplo de comando:

**./mongo --host** *192.168.xx.xx* **--port 8635 -u rwuser -p --authenticationDatabase admin**

**Passo 3** Verifique o resultado da conexão. Se as informações a seguir forem exibidas, a conexão será bem-sucedida.

```
mongos>
```

**----Fim**

## 2.2.4.4 Conexão a uma instância de cluster usando Robo 3T

Para se conectar a uma instância a partir de um dispositivo local, você pode usar o Robo 3T para acessar a instância a partir da Internet.

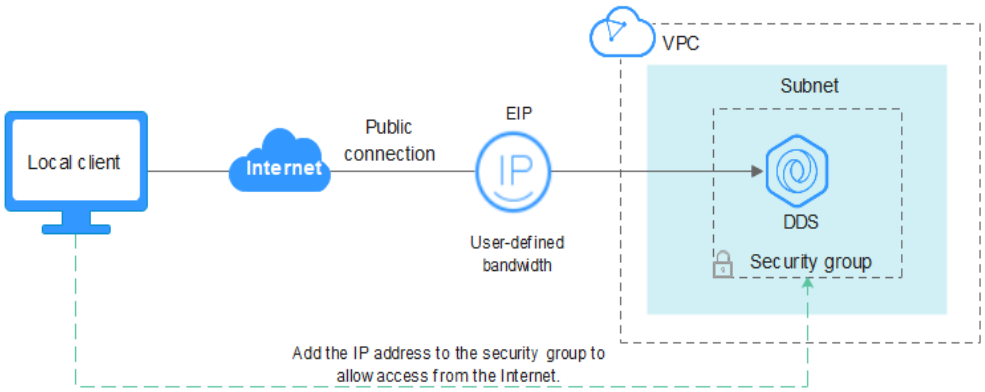
Esta seção descreve como usar o Robo 3T para se conectar a uma instância de cluster a partir de um dispositivo local. Nesta seção, o sistema operacional (SO) Windows usado pelo cliente é usado como um exemplo.

O Robo 3T pode se conectar a uma instância com uma conexão não criptografada ou uma conexão criptografada (SSL). Para melhorar a segurança da transmissão de dados, conecte-se a instâncias usando SSL.

## Diagrama de conexão

**Figura 2-35** Diagrama de conexão




## Pré-requisitos

1. **Vincule um EIP** à instância de cluster e **configure regras de grupo de segurança** para garantir que a instância possa ser acessada usando o Robo 3T
2. Instale Robo 3T.

   Para obter detalhes, consulte **Instalação do Robo 3T**.

## SSL

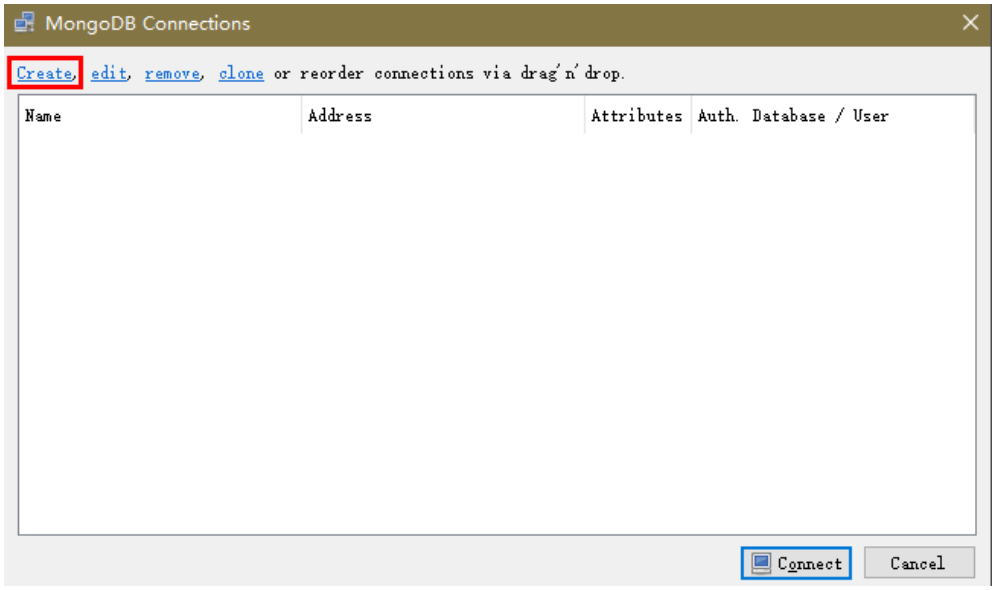
**AVISO**

Se você se conectar a uma instância por meio da conexão SSL, ative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como ativar SSL, consulte **Ativação e desativação de SSL**.

**Passo 1** Execute o Robo 3T instalado. Na caixa de diálogo exibida, clique em **Create**.

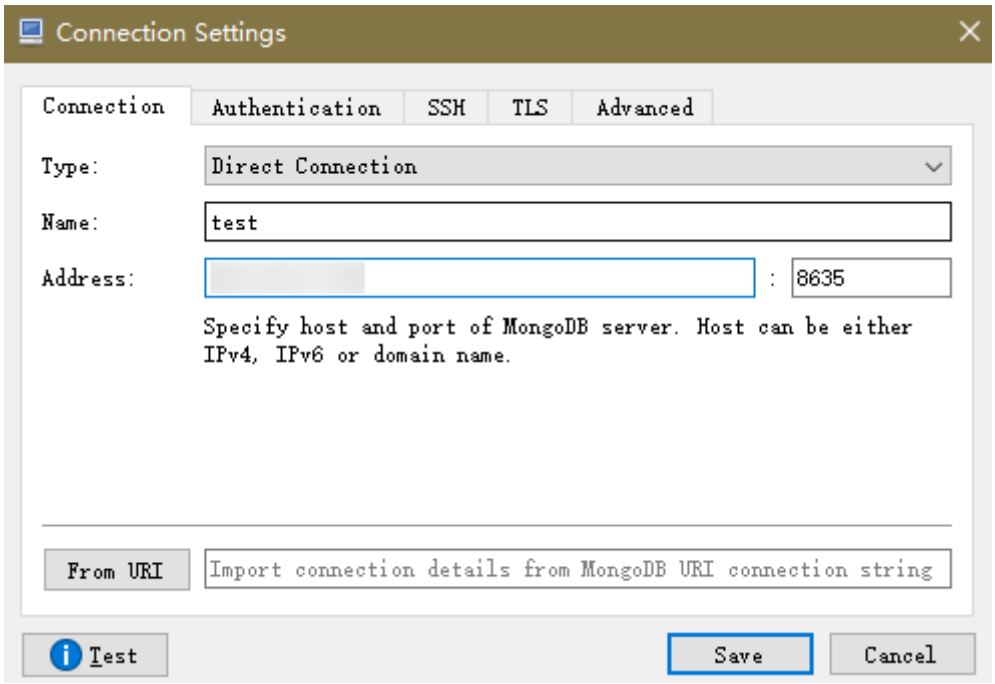
**Figura 2-36** Conexões




**Passo 2** Na caixa de diálogo **Connection Settings**, defina os parâmetros da nova conexão.

1. Na guia **Connection**, digite o nome da nova conexão na caixa de texto **Name** e insira o EIP e a porta do banco de dados vinculada à instância de BD do DDS na caixa de texto **Address**.

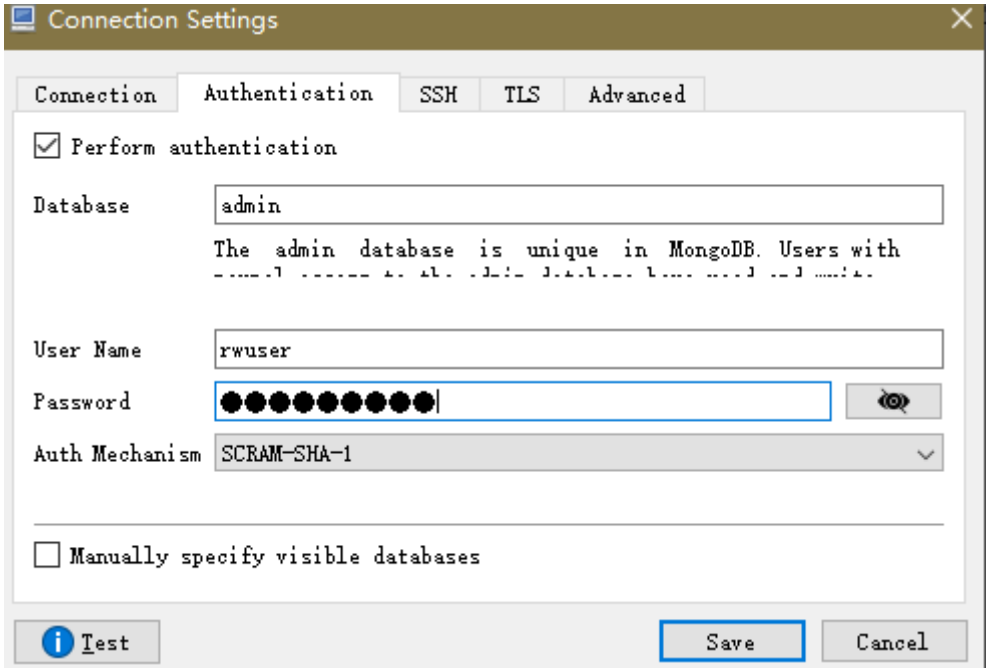
   **Figura 2-37** Conexão

2. Na guia **Authentication**, defina **Database** como **admin**, **User Name** como **rwuser** e **Password** como a senha de administrador definida durante a criação da instância de cluster.

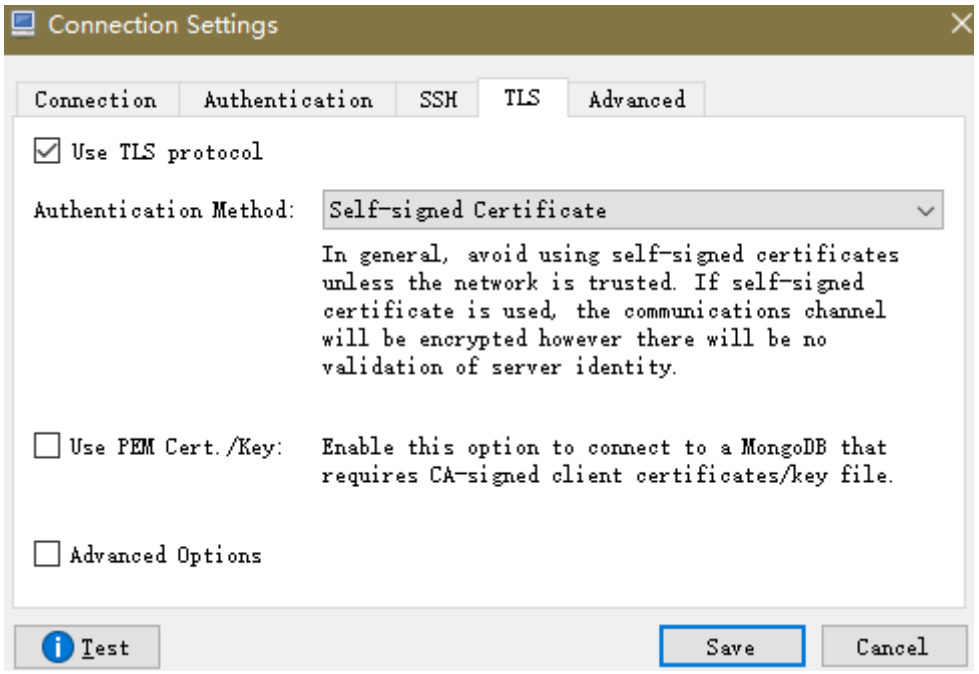
  

**Figura 2-38** Autenticação




3. Na guia **TLS**, selecione **Use TLS protocol** e selecione **Self-signed Certificate** para **Authentication Method**.

**Figura 2-39** SSL

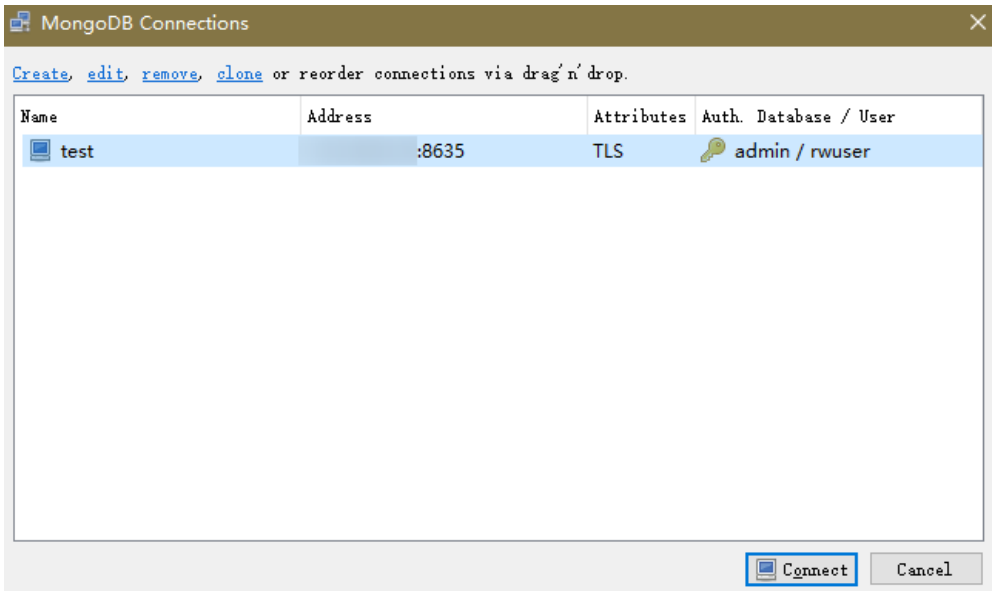



4. Clique em **Save**.

**Passo 3** Na página **MongoDB Connections**, clique em **Connect** para conectar-se à instância de cluster.

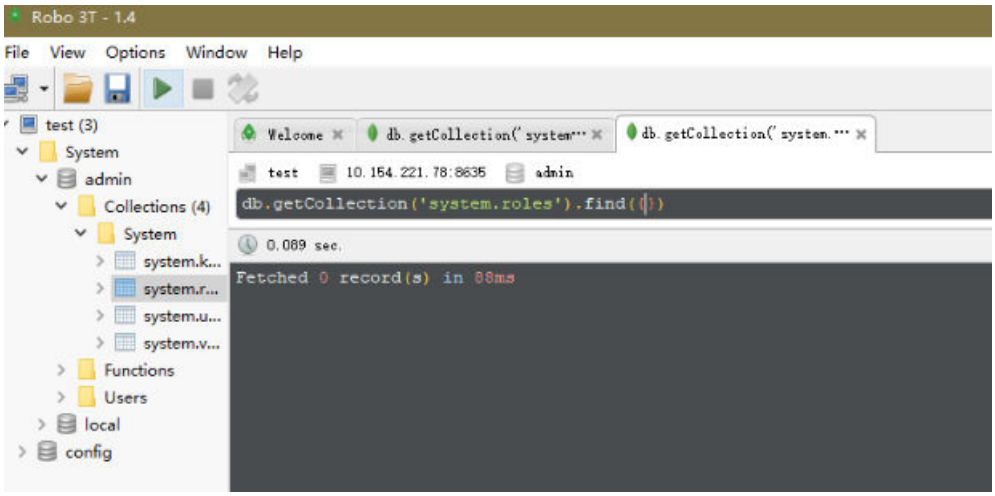
  

**Figura 2-40** Informações de conexão do cluster




**Passo 4** Se a instância de cluster for conectada com êxito, a página mostrada em **Figura 2-41** será exibida.

**Figura 2-41** Cluster conectado com sucesso.




**----Fim**

## Conexão não criptografada

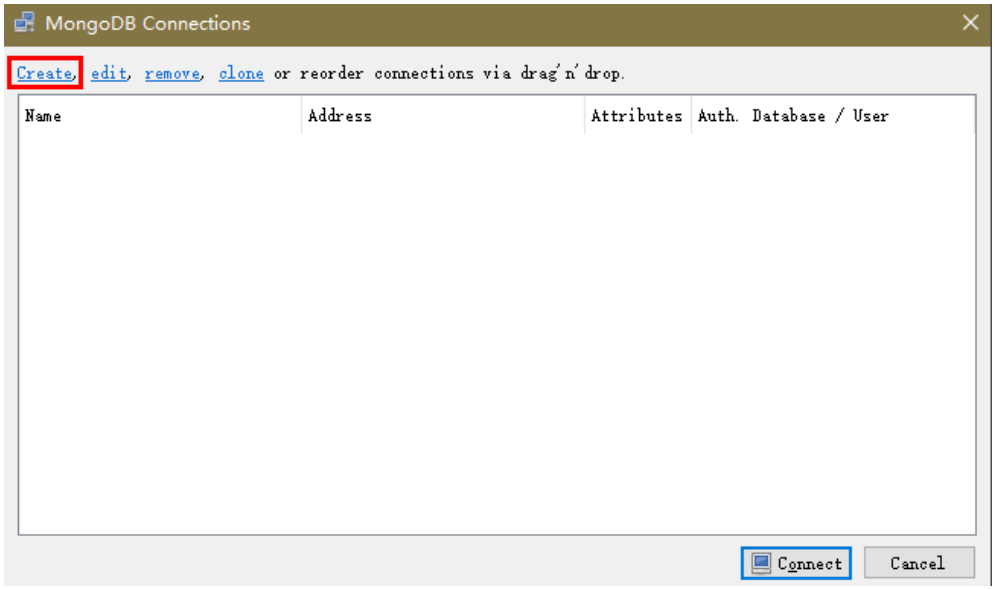
**AVISO**

Se você se conectar a uma instância por meio de uma conexão não criptografada, desative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes, consulte **Ativação e desativação de SSL**.

**Passo 1** Execute o Robo 3T instalado. Na caixa de diálogo exibida, clique em **Create**.

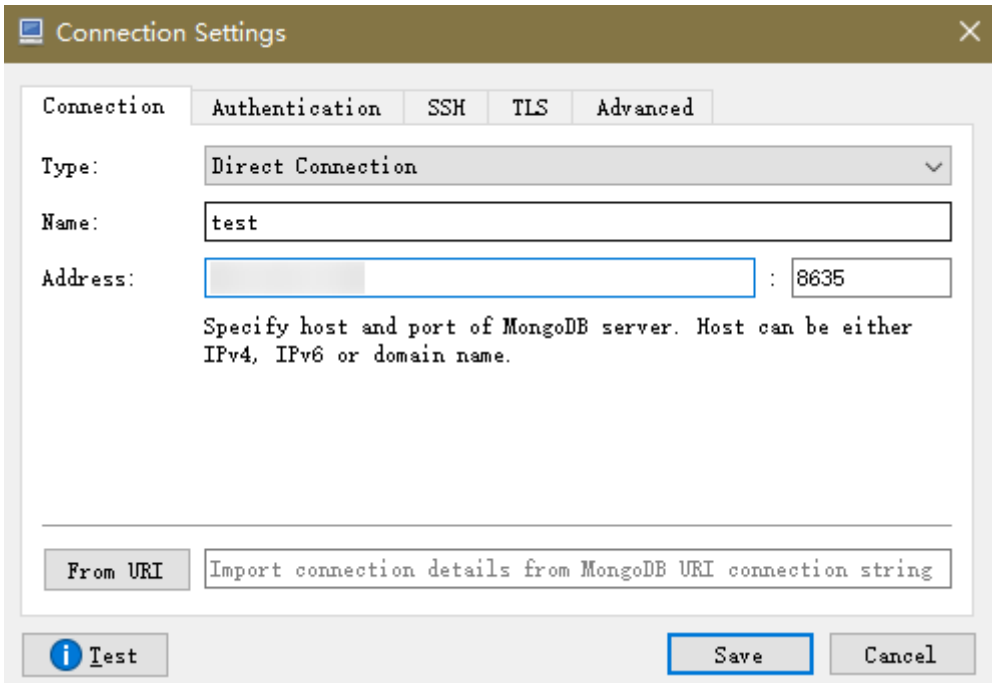
**Figura 2-42** Conexões




**Passo 2** Na caixa de diálogo **Connection Settings**, defina os parâmetros da nova conexão.

1. Na guia **Connection**, digite o nome da nova conexão na caixa de texto **Name** e insira o EIP e a porta do banco de dados vinculada à instância de BD do DDS na caixa de texto **Address**.

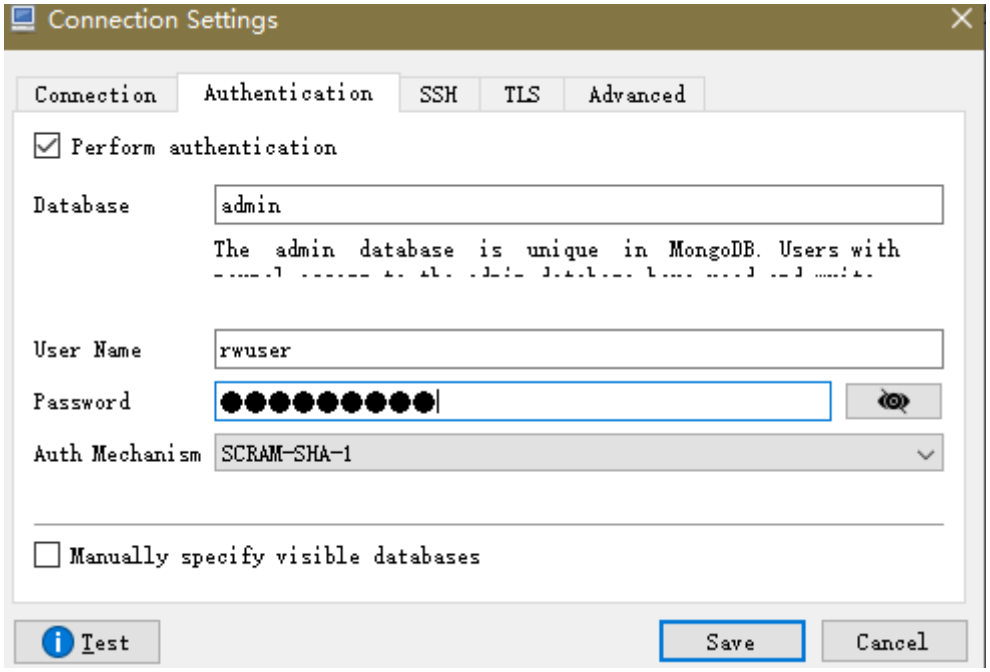
   **Figura 2-43** Conexão

2. Na guia **Authentication**, defina **Database** como **admin**, **User Name** como **rwuser** e **Password** como a senha de administrador definida durante a criação da instância de cluster.

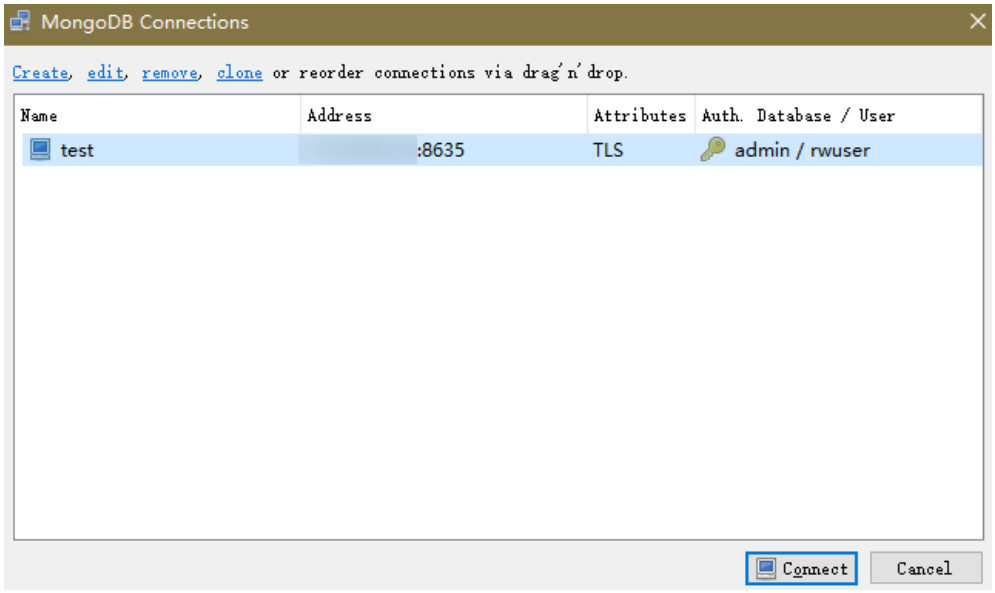
**Figura 2-44** Autenticação




3. Clique em **Save**.

**Passo 3** Na página **MongoDB Connections**, clique em **Connect** para conectar-se à instância de cluster.

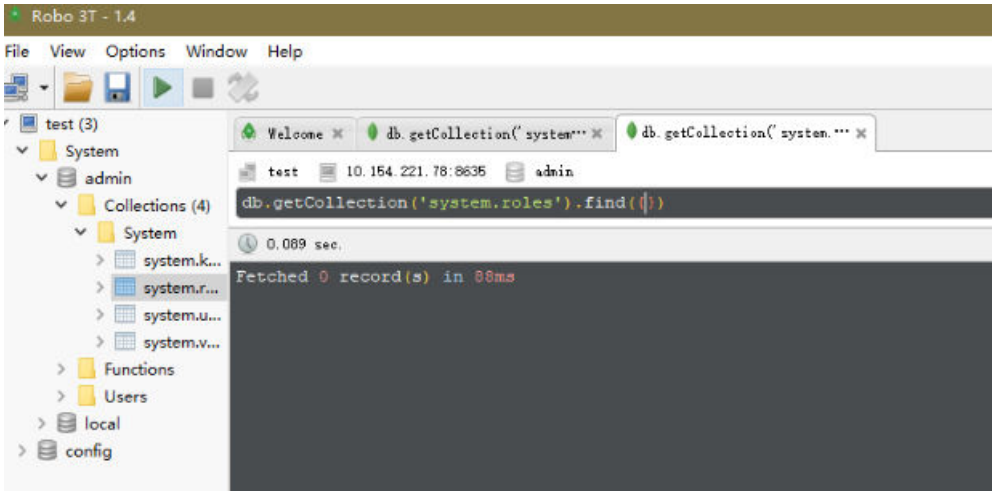
**Figura 2-45** Informações de conexão do cluster




**Passo 4** Se a instância de cluster for conectada com êxito, a página mostrada em **Figura 2-46** será exibida.

**Figura 2-46** Cluster conectado com sucesso




**----Fim**

# 2.2.5 Conexão a uma instância de cluster usando código do programa

## 2.2.5.1 Java

Se você estiver se conectando a uma instância usando Java, um certificado SSL é opcional, mas baixar um certificado SSL e criptografar a conexão melhorarão a segurança de sua instância. SSL é desativado por padrão para instâncias recém-criadas, mas você pode ativar SSL consultando **Ativação ou desativação de SSL**. SSL criptografa conexões com bancos de dados, mas aumenta o tempo de resposta da conexão e o uso da CPU. Por esse motivo, a ativação de SSL não é recomendada.

## Pré-requisitos

Familiarize-se com:

- Noções básicas de computador
- Código Java

## Obter e utilizar Java

- Baixe o driver do Jar em **https://repo1.maven.org/maven2/org/mongodb/mongo-java-driver/3.0.4/**
- Para ver o guia de uso, visite **https://mongodb.github.io/mongo-java-driver/4.2/driver/getting-started/installation/**.

## Usar um certificado SSL

NOTA

- Baixe o certificado SSL e verifique o certificado antes de se conectar aos bancos de dados.
- Na página **Instances**, clique no nome da instância de BD de destino. Na área **DB Information** da página **Basic Information**, clique em no campo **SSL** para baixar certificado raiz ou do pacote de certificados.
- Para obter detalhes sobre como configurar uma conexão SSL, consulte o documento oficial do driver Java do MongoDB em **https://www.mongodb.com/docs/drivers/java/sync/current/fundamentals/connection/tls/#std-label-tls-ssl**.

Se você se conectar a uma instância de cluster usando Java, o formato do código será o seguinte:

```
mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>?authSource=admin&ssl=true
```

**Tabela 2-18** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| <username> | Nome de usuário atual. |
| <password> | Senha para o nome de usuário atual |
| <instance_ip> | Se você tentar acessar a instância de um ECS, defina *instance_ip* como o endereço IP privado exibido na página **Basic Information** da instância à qual você pretende se conectar. |
| | Se você tentar acessar a instância por meio de um EIP, defina *instance_ip* como o EIP vinculado à instância. |
| | Se vários endereços de host forem necessários, liste os endereços no formato de <instance_ip1>:<instance_port1>,<instance_ip2>:<instance_port2>. ..... Exemplo: mongodb:// username:*****@127.***.***.1:8635,127.***.***.2:8635/?authSource=admin |
| <instance_port> | Porta do banco de dados exibida na página **Basic Information**. Valor padrão: **8635** |
| <database_name> | Nome do banco de dados a ser conectado. |
| authSource | Base de dados de utilizadores de autenticação. O valor é **admin**. |
| ssl | Modo de conexão. **true** indica que o modo de conexão SSL é usado. |

Use a keytool para configurar o certificado de AC. Para obter detalhes sobre os parâmetros, consulte **Tabela 2-19**.

```
keytool -importcert -trustcacerts -file <path to certificate authority file> -keystore <path to trust store> -storepass <password>
```

**Tabela 2-19** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| <path to certificate authority file> | Caminho para armazenar o certificado SSL. |
| <path to trust store> | Caminho para armazenar o repositório confiável. Defina este parâmetro conforme necessário, por exemplo, **./trust/certs.keystore**. |
| <password> | Senha personalizada. |

Defina as propriedades do sistema JVM no programa para apontar para o repositório confiável e repositório de chaves corretos:

- System.setProperty("javax.net.ssl.trustStore","<path to trust store>");
- System.setProperty("javax.net.ssl.trustStorePassword","<password>");

Para obter detalhes sobre o código Java, consulte o exemplo a seguir:

```
public class Connector { public static void main(String[] args) { try
{ System.setProperty("javax.net.ssl.trustStore", "./trust/
certs.keystore"); System.setProperty("javax.net.ssl.trustStorePassword",
"123456"); ConnectionString connString = new ConnectionString("mongodb://
<username>:<password>@<instance_ip>:<instance_port>/<database_name>?
authSource=admin&ssl=true"); MongoClientSettings settings =
MongoClientSettings.builder() .applyConnectionString(connString) .applyTo
SslSettings(builder ->
builder.enabled(true)) .applyToSslSettings(builder ->
builder.invalidHostNameAllowed(true)) .build(); MongoClient mongoClient
= MongoClients.create(settings); MongoDatabase database =
mongoClient.getDatabase("admin"); //Ping the database. Se a operação
falhar, ocorre uma exceção. BsonDocument command = new
BsonDocument("ping", new BsonInt64(1)); Document commandResult =
database.runCommand(command); System.out.println("Connect to database
successfully"); } catch (Exception e) { e.printStackTrace();
System.out.println("Test failed"); } } }
```

## Conexão sem o certificado SSL

**NOTA**

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

Se você se conectar a uma instância de cluster usando Java, o formato do código será o seguinte:

```
mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>?
authSource=admin
```

**Tabela 2-20** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| <username> | Nome de usuário atual. |
| <password> | Senha para o nome de usuário atual |

| Parâmetro | Descrição |
| --- | --- |
| <instance_ip> | Se você tentar acessar a instância de um ECS, defina *instance_ip* como o endereço IP privado exibido na página **Basic Information** da instância à qual você pretende se conectar. |
| | Se você tentar acessar a instância por meio de um EIP, defina *instance_ip* como o EIP vinculado à instância. |
| | Se vários endereços de host forem necessários, liste os endereços no formato de <instance_ip1>:<instance_port1>,<instance_ip2>:<instance_port2>. ..... Exemplo: mongodb:// username:*****@127.***.***.1:8635,127.***.***.2:8635/?authSource=admin |
| <instance_port> | Porta do banco de dados exibida na página **Basic Information**. Valor padrão: **8635** |
| <database_name> | Nome do banco de dados a ser conectado. |
| authSource | Base de dados de utilizadores de autenticação. O valor é **admin**. |

Para obter detalhes sobre o código Java, consulte o exemplo a seguir:

```
public class Connector { public static void main(String[] args) { try
{ ConnectionString connString = new ConnectionString("mongodb://
<username>:<password>@<instance_ip>:<instance_port>/<database_name>?
authSource=admin"); MongoClientSettings settings =
MongoClientSettings.builder() .applyConnectionString(connString) .retryWr
ites(true) .build(); MongoClient mongoClient =
MongoClients.create(settings); MongoDatabase database =
mongoClient.getDatabase("admin"); //Ping the database. Se a operação
falhar, ocorre uma exceção. BsonDocument command = new
BsonDocument("ping", new BsonInt64(1)); Document commandResult =
database.runCommand(command); System.out.println("Connect to database
successfully"); } catch (Exception e) { e.printStackTrace();
System.out.println("Test failed"); } } }
```

## 2.2.5.2 Python

Esta seção descreve como usar o cliente de MongoDB no Python para se conectar a uma instância de cluster.

## Pré-requisitos

1. Para conectar um ECS a uma instância, o ECS deve ser capaz de se comunicar com a instância do DDS. Você pode executar o seguinte comando para conectar-se ao endereço IP e à porta do servidor de instância para testar a conectividade de rede.

   **curl** *ip:port*

   Se a mensagem **It looks like you are trying to access MongoDB over HTTP on the native driver port** for exibida, a conectividade de rede é normal.

2. Instale Python e o pacote de instalação de terceiros **pymongo** no ECS. Pymongo 2.8 é recomendado.

3. Se SSL estiver ativado, você precisará baixar o certificado raiz e carregá-lo no ECS.

## Código de conexão

- Ativar SSL

```
import ssl
from pymongo import MongoClient
conn_urls="mongodb://rwuser:rwuserpassword@ip:port/{mydb}?
authSource=admin"
connection = MongoClient(conn_urls,connectTimeoutMS=5000,ssl=True,
ssl_cert_reqs=ssl.CERT_REQUIRED,ssl_match_hostname=False,ssl_ca_certs
=${path to certificate authority file})
dbs = connection.database_names()
print "connect database success! database names is %s" % dbs
```

- Desativar SSLi

```
import ssl
from pymongo import MongoClient
conn_urls="mongodb://rwuser:rwuserpassword@ip:port/{mydb}?
authSource=admin"
connection = MongoClient(conn_urls,connectTimeoutMS=5000)
dbs = connection.database_names()
print "connect database success! database names is %s" % dbs
```

NOTA

- O banco de dados de autenticação no URL deve ser **admin**. Isso significa definir **authSource** como **admin**.
- No modo SSL, você precisa gerar manualmente o arquivo trustStore.
- A base de dados de autenticação tem de ser **admin** e, em seguida, mudar para a base de dados de serviço.

# 3 Primeiros passos com conjuntos de réplicas

## 3.1 Compra de uma instância de conjunto de réplicas

### 3.1.1 Configuração rápida

Esta seção descreve como comprar rapidamente uma instância do conjunto de réplicas no console de gerenciamento. O DDS fornece várias configurações recomendadas para ajudá-lo a comprar uma instância do conjunto de réplicas em alguns minutos.

#### Pré-requisitos

- Você registrou uma conta da Huawei Cloud.

#### Procedimento

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

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

Se você quiser recursos de computação e rede dedicados ao seu uso exclusivo, **ative uma DeC** e **solicite recursos do DCC**. Depois de ativar uma DeC, você pode selecionar a região da DeC e o projeto.

**Passo 3** Clique em no canto superior esquerdo da página e escolha **Databases** > **Document Database Service**.

**Passo 4** Na página **Instances**, clique em **Comprar instância de BD**. A página **Quick Config** é exibida por padrão.

**Passo 5** Selecione um modo de cobrança. Especifique os detalhes da instância e clique em **Próximo**.

**Figura 3-1** Configurações básicas

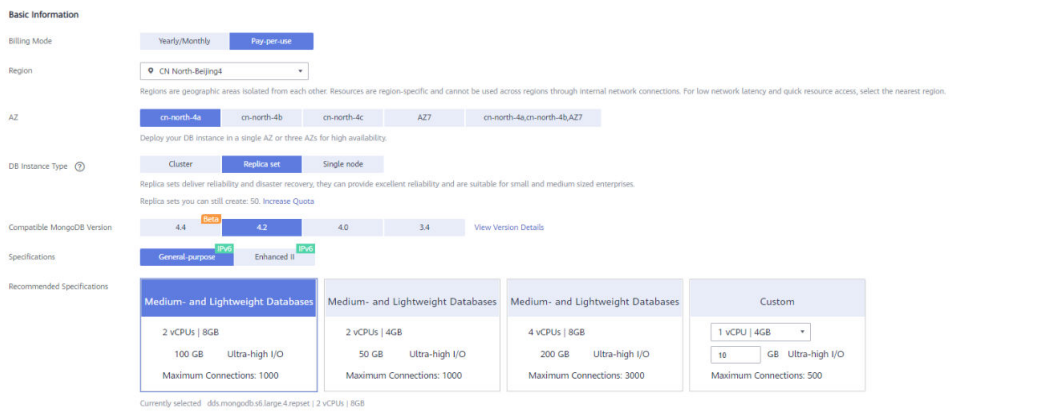



**Tabela 3-1** Configurações básicas

| Parâmetro | Descrição |
| --- | --- |
| Billing Mode | Selecione um modo de cobrança, **Yearly/Monthly** ou **Pay-per-use**.<br>● Para instâncias anuais/mensais<br>– Especifique a **Required Duration** e o sistema deduz as taxas incorridas da sua conta com base no preço do serviço.<br>– Se você não espera continuar usando a instância muito depois que ela expirar, altere o modo de cobrança de anual/mensal para pagamento por uso. Para obter detalhes, consulte **Alteração do modo de cobrança de anual/mensal para pagamento por uso**.<br>**NOTA**<br>As instâncias cobradas anualmente/mensalmente não podem ser excluídas. Elas só podem ser canceladas. Para obter detalhes, consulte **Cancelamento da assinatura de uma instancia anual/mensal**.<br>● Para instâncias de pagamento por uso<br>– Você é cobrado pelo uso com base em quanto tempo o serviço está em uso.<br>– Se você espera usar o serviço extensivamente durante um longo período de tempo, você pode alterar seu modo de cobrança de pagamento por uso para anual/mensal para reduzir os custos. Para obter detalhes, consulte **Alteração do modo de cobrança de pagamento por uso para anual/mensal**.. |
| Region | A região onde o recurso está localizado.<br>**NOTA**<br>As instâncias implementadas em diferentes regiões não podem se comunicar entre si por meio de uma rede privada, e você não pode alterar a região de uma instância depois que ela for comprada. Tenha cuidado ao selecionar uma região. |

| Parâmetro | Descrição |
| --- | --- |
| AZ | Uma AZ é uma parte de uma região com sua própria fonte de alimentação e rede independentes. As AZs são fisicamente isoladas, mas podem se comunicar através de conexões de rede internas.<br>As instâncias podem ser implementadas em uma única AZ ou três AZs.<br>● Se o serviço exigir baixa latência de rede entre instâncias, implemente os componentes da instância na mesma AZ. Se você selecionar uma única AZ para implementar sua instância, a implementação de anti-afinidade será usada por padrão. Com uma implementação anti-afinidade, seus nós primários, secundários e ocultos são implementados em diferentes máquinas físicas para alta disponibilidade.<br>● Se você quiser implementar uma instância em AZs para recuperação de desastres, selecione três AZs. Nesse modo de implementação, os nós primário, secundário e oculto são distribuídos uniformemente em três AZs.<br>**NOTA**<br>A implementação de 3-AZ não está disponível em todas as regiões. Se a opção 3-AZ não for exibida na página para você comprar uma instância, tente uma região diferente. |
| DB Instance Type | Selecione **Replica set**.<br>Um conjunto de réplicas consiste no nó primário, nó secundário e nó oculto. Se um nó primário cair ou se tornar defeituoso, um nó secundário será automaticamente atribuído à função principal e continuará a operação normal. Se um nó secundário não estiver disponível, um nó oculto assumirá o papel do secundário para garantir alta disponibilidade. |
| Compatible MongoDB Version | ● 4.2<br>● 4.0<br>● 3.4 |
| CPU Type | O DDS suporta arquiteturas de CPU x86 e Kunpeng.<br>● x86<br>As CPUs x86 usam o conjunto de instruções CISC (Complex Instruction Set Computing). Cada instrução pode ser usada para executar operações de hardware de baixo nível. As instruções CISC variam em comprimento e tendem a ser complicadas e lentas em comparação com RISC (Reductiond Instruction Set Computing).<br>● Kunpeng<br>A arquitetura de CPU Kunpeng usa RISC. O conjunto de instruções RISC é menor e mais rápido que CISC, graças à arquitetura simplificada. CPUs Kunpeng também oferecem um melhor equilíbrio entre energia e desempenho do que x86.<br>As CPUs Kunpeng oferecem uma opção de alta densidade e baixo consumo de energia que é mais econômica para cargas de trabalho pesadas. |

| Parâmetro | Descrição |
| --- | --- |
| Especificações | Com uma arquitetura x86, você tem as seguintes opções:<br>● Uso geral (s6): as instâncias S6 são adequadas para aplicações que exigem desempenho moderado em geral, mas explosões ocasionais de alto desempenho, como servidores Web de carga leve, ambientes corporativos de P&D e testes e bancos de dados de baixo e médio desempenho.<br>● Aprimorada II (c6): as instâncias C6 têm várias tecnologias otimizadas para fornecer desempenho computacional robusto e estável. NICs inteligentes de alta velocidade de 25 GE são usadas para fornecer largura de banda e taxa de transferência ultra-altas, o que as torna uma excelente opção para cenários de carga pesada. É adequada para sites, aplicações Web, bancos de dados gerais e servidores de cache que têm requisitos de desempenho mais altos para recursos de computação e rede; e aplicações corporativos de carga média e pesada. |
| Recommended Specifications | Atualmente, as especificações de banco de dados médio e leve e as especificações personalizadas são suportadas.<br>**NOTA**<br>Se uma instância tiver menos de 16 vCPUs, o espaço de armazenamento varia de 10 GB a 2000 GB.<br>Se uma instância tiver mais de 16 vCPUs, o espaço de armazenamento varia de 10 GB a 4000 GB. |

**Figura 3-2** Rede, duração necessária e quantidade

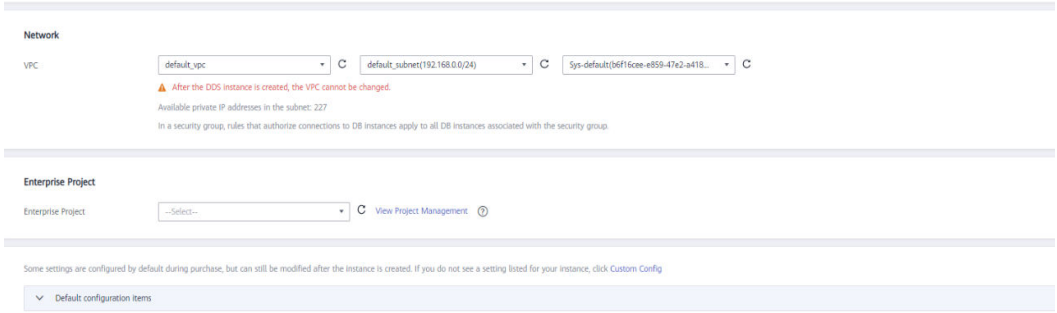



**Tabela 3-2** Configurações da rede

| Parâmetro | Descrição |
| --- | --- |
| VPC | A VPC onde suas instâncias de BD estão localizadas. Uma VPC isola redes para diferentes serviços. Ela permite que você gerencie e configure facilmente redes privadas e altere as configurações de rede.<br>Você precisar criar ou selecionar a VPC necessária. Para obter detalhes, consulte **Criação de uma VPC** no *Guia de usuário da Virtual Private Cloud*. Para obter detalhes sobre as restrições sobre o uso de VPCs, consulte **Métodos de conexão**.<br>Se não houver VPCs disponíveis, o DDS criará uma para você por padrão. |

| Parâmetro | Descrição |
| --- | --- |
| Enterprise Project | Somente usuários empresariais podem usar essa função. Para usar essa função, entre em contato com o atendimento ao cliente.<br>Um projeto empresarial é um modo de gerenciamento de recursos em nuvem, no qual os recursos e os membros da nuvem são gerenciados centralmente pelo projeto.<br>selecione um projeto da empresa na lista suspensa. O projeto padrão é **default**. Para obter mais informações sobre o projeto da empresa, consulte **Gerenciamento de projetos** no *Guia de usuário do Enterprise Management*.<br>Para personalizar um projeto empresarial, clique em **Enterprise** no canto superior direito do console. A página **Enterprise Management** é exibida. Para obter detalhes, consulte **Criação de um projeto empresarial** no *Guia de usuário do Enterprise Management*. |

**Tabela 3-3** Duração necessária e quantidade

| Parâmetro | Descrição |
| --- | --- |
| Duração necessária | O sistema calculará automaticamente a taxa com base no período de validade selecionado. |
| Auto-renew | ● Por padrão, essa opção não está selecionada.<br>● Se você selecionar essa opção, o ciclo de renovação automática será determinado pela duração da assinatura. |
| Quantity | A quantidade de compra depende da cota da instância do conjunto de réplicas. Se sua cota atual não permitir que você compre o número necessário de instâncias, você poderá solicitar o aumento da cota conforme solicitado. As instâncias anuais/mensais que foram compradas em lotes têm as mesmas especificações, exceto o nome e o ID da instância. |

**Tabela 3-4** Itens de configuração padrão

| Especificações | Valor | Editável após a criação da instância |
| --- | --- | --- |
| Nome da instância de BD | dds-c1c1 | Sim |
| Tipo de CPU | x86 | Não |
| Mecanismo de armazenamento | WiredTiger | Não |
| Configurações de senha | Não configurado | Sim |

| Especificações | Valor | Editável após a criação da instância |
| --- | --- | --- |
| SSL | Desabilitado | Sim |
| Porta do banco de dados | 8635 | Sim |
| Acesso entre CIDRs | Não configurado | Sim |
| Modelo de parâmetro de conjunto de réplicas | Default-DDS-4.0-Replica | Sim |
| Tags | Não configurado | Sim |
| Configurações avançadas | Não configurado | Sim |

NOTA

- Algumas configurações são configuradas por padrão durante a compra, mas ainda podem ser modificadas após a criação da instância. Se você não vir uma configuração listada para sua instância, clique em **Configuração personalizada**.
- O desempenho da instância depende das especificações selecionadas durante a criação. Os itens de configuração de hardware que podem ser selecionados incluem a classe de nó e o espaço de armazenamento.

**Passo 6** Na página exibida, confirme os detalhes da instância.

- Para instâncias anuais/mensais
  - Se você precisar modificar as especificações, clique em **Previous** para retornar à página anterior.
  - Se você não precisar modificar as especificações, leia e concorde com o contrato de serviço e clique em **Pay Now** para ir para a página de pagamento e concluir o pagamento.
- Para instâncias de pagamento por uso
  - Se você precisar modificar as especificações, clique em **Previous** para retornar à página anterior.
  - Se você não precisar modificar as especificações, leia e concorde com o contrato de serviço e clique em **Submit** para começar a criar a instância.

**Passo 7** Depois que uma instância do DDS for criada, você poderá exibi-la e gerenciá-la na página **Instances**.

- Quando uma instância está sendo criada, o status exibido na coluna **Status** é **Creating**. Este processo leva cerca de 15 minutos. Após a conclusão da criação, o status muda para **Available**.
- O DDS ativa a política de backup automatizado por padrão. Depois que uma instância é criada, você pode modificar ou desativar a política de backup automatizado. Um backup completo automatizado é acionado imediatamente após a criação de uma instância.

- As instâncias anuais/mensais que foram compradas em lotes têm as mesmas especificações, exceto o nome e o ID da instância.

**----Fim**

## 3.1.2 Configuração personalizada

Esta seção descreve como comprar uma instância de conjunto de réplicas no modo personalizado no console de gerenciamento. Você pode personalizar os recursos de computação e o espaço de armazenamento de uma instância de conjunto de réplicas com base nos seus requisitos de serviço. Além disso, você pode definir configurações avançadas, como log de consultas lentas e backup automatizado.

### Precauções

Cada conta pode criar até 50 instâncias de conjunto de réplicas.

### Pré-requisitos

- Você registrou uma conta da Huawei Cloud.
- Se você quiser recursos de computação e rede dedicados ao seu uso exclusivo, **ative uma DeC** e **solicite recursos do DCC**. Em seguida, você pode criar instâncias do DDS.

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

  NOTA

  Você será cobrado adicionalmente pelo uso da DeC.

  Somente instâncias de conjunto de réplicas com pagamento por uso podem ser compradas por meio da DeC.

### 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 e escolha **Databases** > **Document Database Service**.

**Passo 4** Na página **Instances**, clique em **Comprar instância de BD**.

**Passo 5** Clique na guia **Custom Config**.

**Passo 6** Selecione um modo de cobrança. Especifique os detalhes da instância e clique em **Próximo**.

**Figura 3-3** Configuração básica

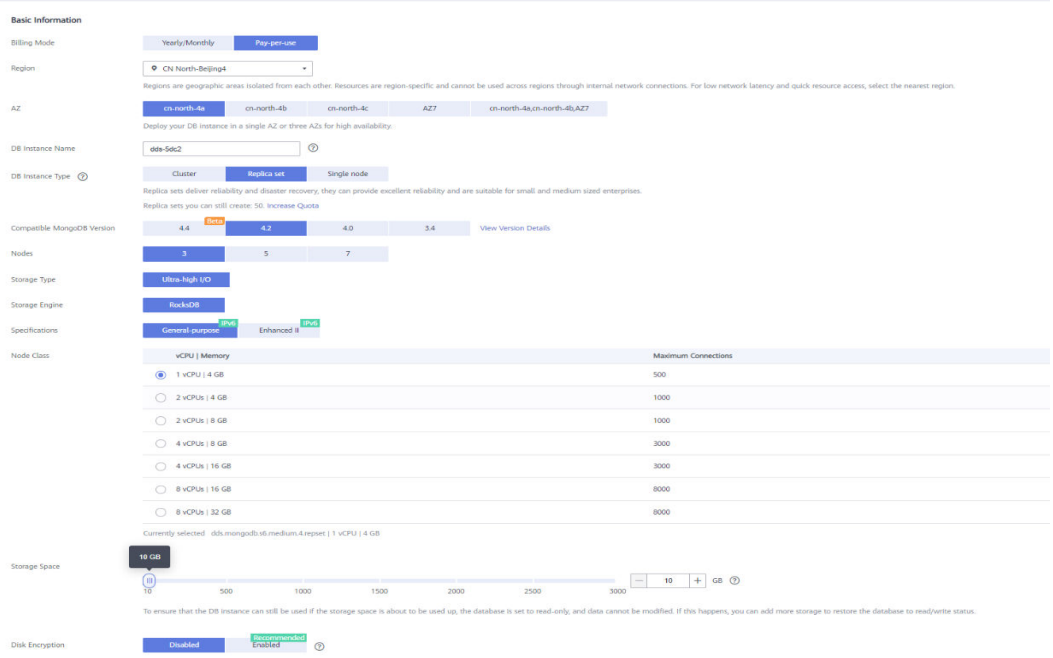



**Tabela 3-5** Modo de cobrança

| Parâmetro | Descrição |
| --- | --- |
| Billing Mode | Selecione um modo de cobrança, **Yearly/Monthly** ou **Pay-per-use**.<br>● Para instâncias anuais/mensais<br>– Especifique a **Required Duration** e o sistema deduz as taxas incorridas da sua conta com base no preço do serviço.<br>– Se você não espera continuar usando a instância muito depois que ela expirar, altere o modo de cobrança de anual/mensal para pagamento por uso. Para obter detalhes, consulte **Alteração do modo de cobrança de anual/mensal para pagamento por uso**.<br>**NOTA**<br>As instâncias cobradas anualmente/mensalmente não podem ser excluídas. Elas só podem ser canceladas. Para obter detalhes, consulte **Cancelamento da assinatura de uma instância anual/mensal**.<br>● Para instâncias de pagamento por uso<br>– Você é cobrado pelo uso com base em quanto tempo o serviço está em uso.<br>– Se você espera usar o serviço extensivamente durante um longo período de tempo, você pode alterar seu modo de cobrança de pagamento por uso para anual/mensal para reduzir os custos. Para obter detalhes, consulte **Alteração do modo de cobrança de pagamento por uso para anual/mensal**. |

| Parâmetro | Descrição |
| --- | --- |
| Region | A região onde o recurso está localizado.<br>**NOTA**<br>As instâncias implementadas em diferentes regiões não podem se comunicar entre si por meio de uma rede privada, e você não pode alterar a região de uma instância depois que ela for comprada. Tenha cuidado ao selecionar uma região. |
| AZ | Uma AZ é uma parte de uma região com sua própria fonte de alimentação e rede independentes. As AZs são fisicamente isoladas, mas podem se comunicar através de conexões de rede internas.<br>As instâncias podem ser implementadas em uma única AZ ou três AZs.<br>● Se o serviço exigir baixa latência de rede entre instâncias, implemente os componentes da instância na mesma AZ. Se você selecionar uma única AZ para implementar sua instância, a implementação de anti-afinidade será usada por padrão. Com uma implementação anti-afinidade, seus nós primários, secundários e ocultos são implementados em diferentes máquinas físicas para alta disponibilidade.<br>● Se você quiser implementar uma instância em AZs para recuperação de desastres, selecione três AZs. Nesse modo de implementação, os nós primário, secundário e oculto são distribuídos uniformemente em três AZs.<br>**NOTA**<br>A implantação de 3-AZ não está disponível em todas as regiões. Se a opção 3-AZ não for exibida na página para você comprar uma instância, tente uma região diferente. |
| DB Instance Name | ● O nome da instância pode ser igual a um nome de instância existente.<br>● O nome da instância que você especificar após a compra. O nome da ocorrência deve conter de 4 a 64 caracteres e deve começar com uma letra. Ele diferencia maiúsculas de minúsculas e minúsculas e pode conter letras, dígitos, hifens (-) e sublinhados (_). Não pode conter outros caracteres especiais.<br>● Se você comprar um lote de instâncias de uma só vez, um sufixo numérico de 4 dígitos será adicionado aos nomes das instâncias, começando com **-0001**. Se mais tarde você fizer outra compra em lote, os novos nomes de instância serão numerados primeiro usando quaisquer sufixos ausentes da sequência de suas instâncias existentes e, em seguida, continuando a partir de onde sua última compra em lote parou. Por exemplo, um lote de 3 instâncias obtém os sufixos **-0001**, **-0002** e **-0003**. Se você excluir a instância **0002** e depois comprar mais 3 instâncias, as novas instâncias receberão os sufixos **-0002**, **-0004** e **-0005**.<br>● Depois que a instância de BD for criada, você poderá alterar seu nome. Para mais detalhes, consulte **Alteração de um nome de instância**. |

| Parâmetro | Descrição |
| --- | --- |
| DB Instance Type | Selecione **Replica set**.<br>Um conjunto de réplicas consiste no nó primário, nó secundário e nó oculto. Se um nó primário cair ou se tornar defeituoso, um nó secundário será automaticamente atribuído à função principal e continuará a operação normal. Se um nó secundário não estiver disponível, um nó oculto assumirá o papel do secundário para garantir alta disponibilidade. |
| Compatible MongoDB Version | ● 4.2<br>● 4.0<br>● 3.4 |
| CPU Type | O DDS suporta arquiteturas de CPU x86 e Kunpeng.<br>● x86<br>As CPUs x86 usam o conjunto de instruções CISC (Complex Instruction Set Computing). Cada instrução pode ser usada para executar operações de hardware de baixo nível. As instruções CISC variam em comprimento e tendem a ser complicadas e lentas em comparação com RISC (Reductiond Instruction Set Computing).<br>● Kunpeng<br>A arquitetura de CPU Kunpeng usa RISC. O conjunto de instruções RISC é menor e mais rápido que CISC, graças à arquitetura simplificada. CPUs Kunpeng também oferecem um melhor equilíbrio entre energia e desempenho do que x86.<br>As CPUs Kunpeng oferecem uma opção de alta densidade e baixo consumo de energia que é mais econômica para cargas de trabalho pesadas. |
| Storage Type | Se você não usar a DeC, o tipo de armazenamento é de I/O ultra-alta por padrão.<br>Para usuários da DeC, os tipos de armazenamento suportados dependem do tipo de recurso selecionado.<br>● Se você selecionar **EVS** para **Resource Type**, **Storage Type** será definido como **Ultra-high I/O**.<br>● Se você selecionar **DSS** para **Resource Type**, **Storage Type** pode ser definido como **Common I/O**, **High I/O** ou **Ultra-high I/O**. |

| Parâmetro | Descrição |
| --- | --- |
| Storage Engine | ● WiredTiger<br>O WiredTiger é o mecanismo de armazenamento padrão do DDS 3.4 e 4.0. O WiredTiger fornece controle de simultaneidade de granularidade diferente e mecanismo de compactação para gerenciamento de dados. Ele pode fornecer o melhor desempenho e eficiência de armazenamento para diferentes tipos de aplicações.<br>● RocksDB<br>RocksDB é o mecanismo de armazenamento padrão do DDS 4.2. O RocksDB suporta pesquisa de pontos eficiente, varredura de alcance e gravação de alta velocidade. O RocksDB pode ser usado como o mecanismo de armazenamento de dados subjacente do MongoDB e é adequado para cenários com um grande número de operações de gravação. |
| Specifications | Com uma arquitetura x86, você tem as seguintes opções:<br>● Uso geral (s6): as instâncias S6 são adequadas para aplicações que exigem desempenho moderado em geral, mas explosões ocasionais de alto desempenho, como servidores Web de carga leve, ambientes corporativos de P&D e testes e bancos de dados de baixo e médio desempenho.<br>● Aprimorada II (c6): as instâncias C6 têm várias tecnologias otimizadas para fornecer desempenho computacional robusto e estável. NICs inteligentes de alta velocidade de 25 GE são usadas para fornecer largura de banda e taxa de transferência ultra-altas, o que as torna uma excelente opção para cenários de carga pesada. É adequada para sites, aplicações Web, bancos de dados gerais e servidores de cache que têm requisitos de desempenho mais altos para recursos de computação e rede; e aplicações corporativas de carga média e pesada. |
| Node Class | Para obter detalhes sobre as especificações da instância, consulte **Especificações da instância**.<br>Para obter detalhes sobre os dados de desempenho de instâncias de BD de especificações diferentes, consulte **Livro branco de desempenho**.<br>Se a CPU ou a memória de uma instância de BD criada não puder atender aos requisitos de serviço, você poderá alterá-la no console de gerenciamento. Para obter detalhes, consulte **Alteração de uma classe de instância de conjunto de réplicas**. |

| Parâmetro | Descrição |
| --- | --- |
| Storage Space | Se uma instância tiver menos de 16 vCPUs, o espaço de armazenamento varia de 10 GB a 2000 GB.<br>Se uma instância tiver mais de 16 vCPUs, o espaço de armazenamento varia de 10 GB a 4000 GB.<br>O valor varia de 10 GB a 2000 GB e deve ser um múltiplo de 10.<br>Você pode expandir uma instância depois que ela é criada.Para obter detalhes, consulte **Expensão de uma instância de conjunto de réplicas**.<br>**NOTA**<br>● Se o espaço de armazenamento comprado exceder 600 GB e o espaço de armazenamento restante for 18 GB, a instância se tornará **Read-only**.<br>● Se o espaço de armazenamento comprado for inferior a 600 GB e o uso do espaço de armazenamento atingir 97%, a instância se tornará **Read-only**.<br>Nesses casos, exclua recursos desnecessários ou expanda a capacidade. |
| Criptografia de disco | ● **Disabled**: desativar a criptografia.<br>● **Enabled**: ativar a criptografia. Esse recurso melhora a segurança dos dados, mas afeta um pouco o desempenho de leitura/gravação. **Key Name**: selecione ou crie uma chave privada, que é a chave do locatário.<br>**NOTA**<br>● Depois que uma instância é criada, o status de criptografia de disco e a chave não podem ser alterados. Os dados de backup armazenados no OBS não são criptografados.<br>● A chave não pode ser desativada, excluída ou congelada ao ser usada. Caso contrário, o banco de dados ficará indisponível.<br>● Para obter detalhes sobre como criar uma chave, consulte "Criação de uma CMK" no *Guia de usuário do Data Encryption Workshop*. |

**Figura 3-4** Configurações do administrador

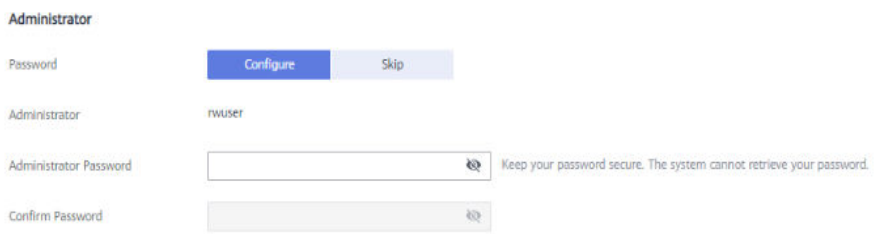


**Tabela 3-6** Configurações do administrador

| Parâmetro | Descrição |
| --- | --- |
| Password | ● Configure<br>Digite e confirme a nova senha de administrador. Depois que uma instância é criada, você pode se conectar à instância usando a senha.<br>● Skip<br>Para fazer logon, você terá que redefinir a senha mais tarde na página **Basic Information**. Se você precisar se conectar a uma instância depois que ela for criada, localize a instância e escolha **More** > **Reset Password** na coluna **Operation** para definir uma senha para a instância primeiro. |
| Administrator | A conta padrão é **rwuser**. |
| Administrator Password | Defina uma senha para o administrador. A senha deve ter de 8 a 32 caracteres e conter letras maiúsculas, minúsculas, dígitos e pelo menos um dos seguintes caracteres especiais: ~!@#%^*-_=+?<br>Mantenha esta senha segura. Se for perdida, o sistema não poderá recuperá-la para você. |
| Confirm Password | Digite a senha do administrador novamente. |

**Figura 3-5** Rede, duração necessária e quantidade

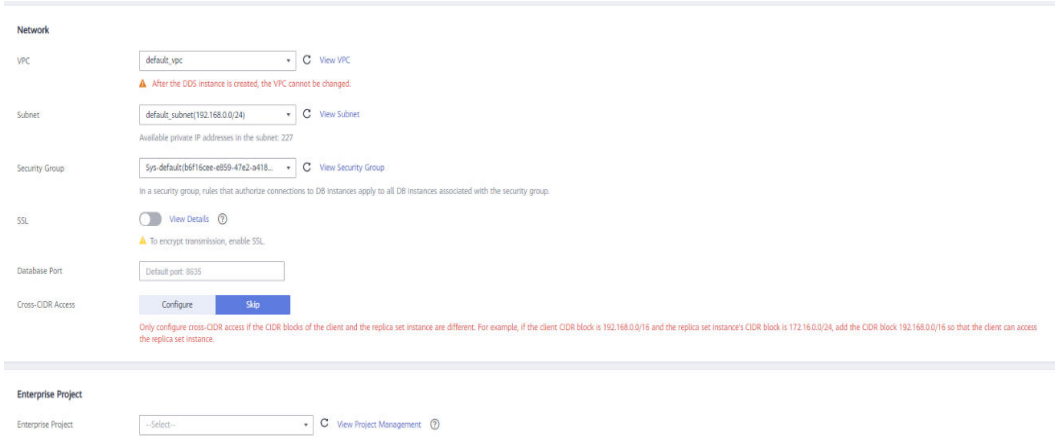


**Tabela 3-7** Rede

| Parâmetro | Descrição |
| --- | --- |
| VPC | A VPC onde suas instâncias de BD estão localizadas. Uma VPC isola redes para diferentes serviços. Ela permite que você gerencie e configure facilmente redes privadas e altere as configurações de rede.<br>Você precisará criar ou selecionar a VPC necessária. Para obter detalhes sobre como criar uma VPC, consulte "Criação de uma VPC" no *Guia de usuário da Virtual Private Cloud*. Para obter detalhes sobre as restrições sobre o uso de VPCs, consulte **Métodos de conexão**.<br>Se não houver VPCs disponíveis, o DDS criará uma para você por padrão. |
| Subnet | Uma sub-rede fornece recursos de rede dedicados que são logicamente isolados de outras redes por razões de segurança.<br>Depois que a instância é criada, você pode alterar o endereço IP privado atribuído pela sub-rede. Para obter detalhes, consulte **Alteração um endereço IP privado**.<br>**NOTA**<br>As sub-redes IPv6 não são suportadas. Recomendamos que você crie e selecione sub-redes IPv4. |
| Security Group | Um grupo de segurança controla o acesso entre o DDS e outros serviços.<br>Se não houver grupos de segurança disponíveis, o DDS criará um para você por padrão.<br>**NOTA**<br>Certifique-se de que haja uma regra de grupo de segurança configurada que permita que os clientes acessem instâncias. Por exemplo, selecione uma regra TCP de entrada com a porta padrão 8635 e insira um endereço IP de sub-rede ou selecione um grupo de segurança ao qual a instância pertence. |
| SSL | A Camada de soquete seguro (SSL) criptografa as conexões entre clientes e servidores, impedindo que os dados sejam adulterados ou roubados durante a transmissão.<br>Você pode ativar SSL para melhorar a segurança dos dados. Depois que uma instância é criada, você pode se conectar a ela usando SSL. |
| Porta do banco de dados | A porta do DDS padrão é 8635, mas esta porta pode ser modificada se necessário. Se você alterar a porta, adicione uma regra de grupo de segurança correspondente para permitir o acesso à instância. |

| Parâmetro | Descrição |
| --- | --- |
| Cross-CIDR Access | ● Configure<br>Se um cliente e uma instância de conjunto de réplicas forem implementados em blocos CIDR diferentes e o cliente não estiver em 192.168.0.0/16, 172.16.0.0/24 ou 10.0.0.0/8, configure o Acesso entre CIDRs para que a instância se comunique com o cliente.<br>**NOTA**<br>– Para garantir que o ECS e a instância de BD possam se comunicar entre si, configure a conexão consultando **Visão geral da conexão de emparelhamento de VPC**.<br>– Até 30 blocos CIDR podem ser configurados, e cada um deles pode se sobrepor, mas eles não podem ser os mesmos. Ou seja, os blocos CIDR de origem podem se sobrepor, mas não pode ser o mesmo. Os blocos CIDR não podem começar com 127. A máscara de IP permitida varia de 8 a 32.<br>● Skip<br>Configurar o bloco CIDR do cliente mais tarde. Depois que uma instância de banco de dados é criada, você pode configurar o acesso entre CIDRs consultando **Configuração do acesso entre CIDRs**. |
| Enterprise Project | Somente usuários empresariais podem usar essa função. Para usar essa função, entre em contato com o atendimento ao cliente.<br>Um projeto empresarial é um modo de gerenciamento de recursos em nuvem, no qual os recursos e os membros da nuvem são gerenciados centralmente pelo projeto.<br>selecione um projeto da empresa na lista suspensa. O projeto padrão é **default**. |

**Figura 3-6** Configurações avançadas

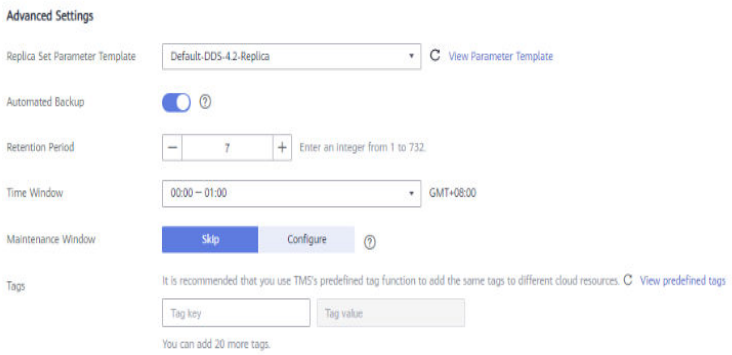


**Tabela 3-8** Configurações avançadas

| Parâmetro | Descrição |
| --- | --- |
| Replica Set Parameter Template | Os parâmetros que se aplicam às instâncias de conjunto de réplicas. Depois que uma instância é criada, você pode alterar o modelo de parâmetro configurado para a instância para obter o melhor desempenho.<br>Para obter detalhes, consulte **Editação de um modelo de parâmetro**. |
| Automated Backup | O DDS ativa uma política de backup automatizado por padrão, mas você pode desativá-la após a criação de uma instância. Um backup completo automatizado é acionado imediatamente após a criação de uma instância.<br>Para obter detalhes, consulte **Configuração de uma política de backup automatizado**. |
| Retention Period (days) | **Retention Period** refere-se ao número de dias que os dados são mantidos. Você pode aumentar o período de retenção para melhorar a confiabilidade dos dados.<br>O período de retenção do backup é de 1 a 732 dias. |
| Time Window | O intervalo de backup é de 1 hora. |

| Parâmetro | Descrição |
| --- | --- |
| Tags | (Opcional) Você pode adicionar tags a instâncias do DDS para que possa pesquisar rapidamente e filtrar instâncias especificadas por tag. Cada instância do DDS pode ter até 20 tags.<br>● Criar uma tag.<br>Você pode criar tags no console do DDS e configurar a **chave** e o **valor** da tag.<br>Key: este parâmetro é obrigatório.<br>– Cada chave de tag deve ser exclusiva para cada instância.<br>– Uma chave de tag consiste em até 36 caracteres.<br>– A chave deve consistir apenas em dígitos, letras, sublinhados (_) e hifens (-).<br>Value: este parâmetro é opcional.<br>– O valor consiste em até 43 caracteres.<br>– O valor deve consistir apenas em dígitos, letras, sublinhados (_), pontos (.) e hifens.<br>● Adicionar uma tag predefinida.<br>Tags predefinidas podem ser usadas para identificar vários recursos de nuvem.<br>Para marcar um recurso de nuvem, você pode selecionar uma tag predefinida criada na lista suspensa, sem inserir uma chave e um valor para a tag.<br>Por exemplo, se uma tag predefinida tiver sido criada, sua chave será Usage e o valor será Project1. Quando você configura a chave e o valor para um recurso de nuvem, a tag predefinida criada será exibida na página.<br>Depois que uma instância é criada, você pode clicar no nome da instância para exibir suas tags. Na página **Tags**, você também pode **modificar ou excluir as tags**. Além disso, você pode **pesquisar e filtrar rapidamente instâncias especificadas por tag**.<br>Você pode adicionar uma tag a uma instância depois que ela for criada. Para obter detalhes, consulte **Adição de uma tag**. |

Se você tiver alguma dúvida sobre o preço, clique em **Price Details**.

NOTA

O desempenho da instância depende das especificações selecionadas durante a criação. Os itens de configuração de hardware que podem ser selecionados incluem a classe de instância e o espaço de armazenamento.

**Passo 7** Na página exibida, confirme os detalhes da instância.

- Para instâncias anuais/mensais
  - Se você precisar modificar as especificações, clique em **Previous** para retornar à página anterior.

  - Se você não precisar modificar as especificações, leia e concorde com o contrato de serviço e clique em **Pay Now** para ir para a página de pagamento e concluir o pagamento.
- Para instâncias de pagamento por uso
  - Se você precisar modificar as especificações, clique em **Previous** para retornar à página anterior.
  - Se você não precisar modificar as especificações, leia e concorde com o contrato de serviço e clique em **Submit** para começar a criar a instância.

**Passo 8** Depois que uma instância do DDS for criada, você poderá exibi-la e gerenciá-la na página **Instances**.

- Quando uma instância está sendo criada, o status exibido na coluna **Status** é **Creating**. Este processo leva cerca de 15 minutos. Após a conclusão da criação, o status muda para **Available**.
- As instâncias anuais/mensais que foram compradas em lotes têm as mesmas especificações, exceto o nome e o ID da instância.

**----Fim**

# 3.2 Conexão a uma instância do conjunto de réplicas

## 3.2.1 Métodos de conexão

Você pode acessar o DDS em redes privadas ou públicas.

**Tabela 3-9** Métodos de conexão

| Método | Endereço IP | Cenário | Descrição |
| --- | --- | --- | --- |
| **DAS** | Não necessário | O DAS fornece uma GUI e permite que você execute operações visualizadas no console. Execução SQL, gerenciamento avançado de banco de dados e O&M inteligente estão disponíveis para tornar o gerenciamento de banco de dados simples, seguro e inteligente. | ● Fácil de usar, seguro, avançado e inteligente<br>● Recomendado |
| **Rede privada** | Endereço IP privado | O DDS fornece um endereço IP privado por padrão.<br>Se suas aplicações estiverem sendo executadas em um ECS na mesma região, AZ e sub-rede da VPC que sua instância do DDS, recomendamos que você use um endereço IP privado para conectar o ECS às instâncias do DDS. | Seguro e desempenho excelente |

| Método | Endereço IP | Cenário | Descrição |
| --- | --- | --- | --- |
| **Rede pública** | EIP | ● Se suas aplicações estiverem sendo executadas em um ECS que esteja em uma região diferente daquela em que a instância de BD está localizada, use um EIP para conectar o ECS às instâncias de BD do DDS.<br>● Se suas aplicações forem implementadas em outra plataforma de nuvem, o EIP é recomendado. | ● Baixa segurança<br>● Para uma transmissão mais rápida e segurança aprimorada, é recomendável migrar suas aplicações para um ECS que esteja na mesma sub-rede da instância do DDS e usar um endereço IP privado para acessar a instância. |

# 3.2.2 (Recomendada) Conexão a instâncias de conjunto de réplicas por meio do DAS

## 3.2.2.1 Visão geral

O DAS fornece uma GUI e permite que você execute operações visualizadas no console. Execução SQL, gerenciamento avançado de banco de dados e O&M inteligente estão disponíveis para tornar o gerenciamento de banco de dados simples, seguro e inteligente. Recomendamos que você use o DAS para se conectar a instâncias de BD.

Esta seção descreve como comprar uma instância do conjunto de réplicas no console de gerenciamento e como se conectar à instância do conjunto de réplicas por meio do DAS.

## Processo

Para comprar e se conectar a uma instância do conjunto de réplicas, execute as seguintes etapas:

1. **Compre uma instância do conjunto de réplicas.**
2. **Conecte-se à instância do conjunto de réplicas por meio do DAS.**

## 3.2.2.2 Conexão a uma instância de conjunto de réplicas por meio do DAS

Data Admin Service (DAS) permite que você gerencie instâncias de BD em um console baseado na Web, simplificando o gerenciamento de banco de dados e melhorando a eficiência do trabalho. Você pode se conectar e gerenciar instâncias por meio do DAS. Por padrão, você tem a permissão necessária para o logon remoto. Recomenda-se que você use o serviço DAS para se conectar a instâncias. O DAS é seguro e conveniente.

## Procedimento

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

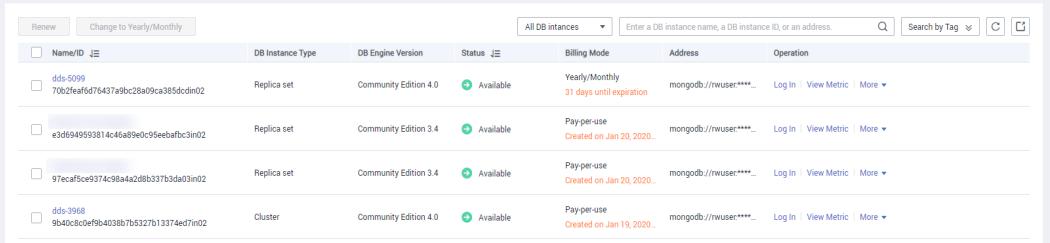
**Passo 2** Clique em no canto superior esquerdo e selecione uma região e um projeto.

**Passo 3** Clique em no canto superior esquerdo da página e escolha **Databases** > **Document Database Service**.

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

Como alternativa, clique na instância de BD de destino na página **Instances**. Na página **Basic Information** exibida, clique em **Log In** no canto superior direito da página.

**Figura 3-7** Gerenciamento de instâncias




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

Para obter detalhes sobre como gerenciar bancos de dados por meio do DAS, consulte **Gerenciamento de instância do DDS**.

**----Fim**

# 3.2.3 Conexão a uma instância do conjunto de réplicas em uma rede privada

## 3.2.3.1 Configuração de regras de grupo de segurança

Um grupo de segurança é uma coleção de regras de controle de acesso para ECSs e instâncias do DDS que têm os mesmos requisitos de proteção de segurança e são mutuamente confiáveis em uma VPC.

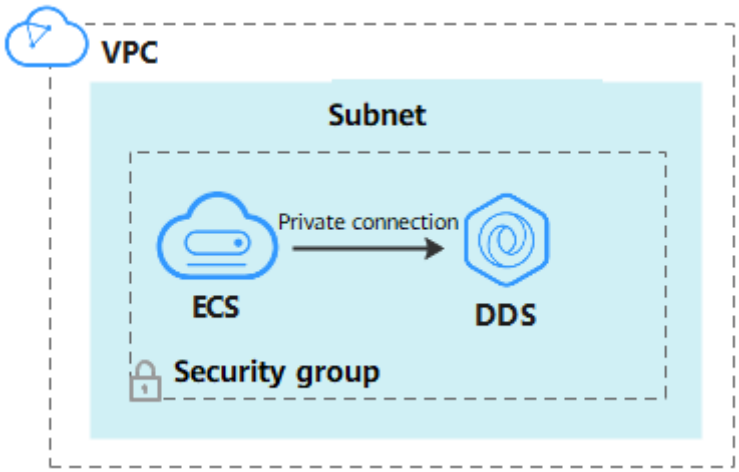
Para garantir a segurança e a confiabilidade do banco de dados, é necessário configurar regras de grupo de segurança para permitir que endereços IP e portas específicos acessem instâncias do DDS.

Você pode se conectar a uma instância configurando regras de grupo de segurança de duas maneiras:

- Se o ECS e a instância estiverem no mesmo grupo de segurança, eles poderão se comunicar entre si por padrão. Nenhuma regra de grupo de segurança precisa ser configurada. Vá para **Conexão a uma instância de conjunto de réplicas usando Mongo Shell (rede privada)**.

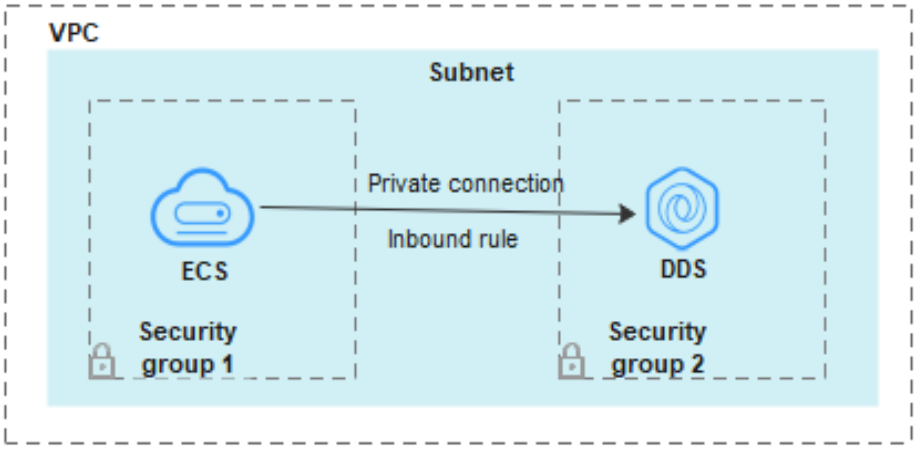
  

**Figura 3-8** Mesmo grupo de segurança




- Se o ECS e a instância estiverem em grupos de segurança diferentes, será necessário configurar as regras de grupo de segurança para eles separadamente.

**Figura 3-9** Diferentes grupos de segurança




  - Instância: configure uma **inbound rule** para o grupo de segurança associado à instância.
  - 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 puder chegar à instância, configure uma regra **de saída** para o ECS.

Esta seção descreve como configurar uma regra de entrada para uma instância.

## Precauções

- Por predefinição, uma conta pode criar até 500 regras de grupo de segurança.
- Muitas regras de grupo de segurança aumentarão a latência do primeiro pacote, portanto, recomenda-se um máximo de 50 regras para cada grupo de segurança.
- Uma instância do DDS só pode ser associada a um grupo de segurança.

## 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 e escolha **Databases** > **Document Database Service**.

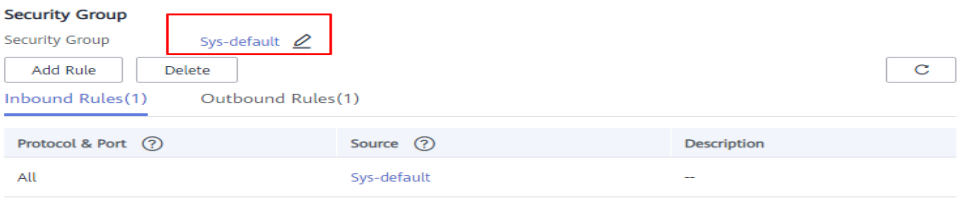
**Passo 4** Na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida.

**Passo 5** Na área **Network Information** da página **Basic Information**, clique no grupo de segurança.

**Figura 3-10** Grupo de segurança


Você também pode escolher **Connections** no painel de navegação à esquerda. Na guia **Private Connection**, na área **Security Group**, clique no nome do grupo de segurança.

**Figura 3-11** Grupo de segurança




**Passo 6** Na página **Security Group**, localize o grupo de segurança de destino e clique em **Manage Rule** na coluna **Operation**.

**Passo 7** Na guia **Inbound Rules**, clique em **Add Rule**. A caixa de diálogo **Add Inbound Rule** é exibida.

**Passo 8** Adicione uma regra de grupo de segurança conforme solicitado.

**Figura 3-12** Adicionar regra de entrada

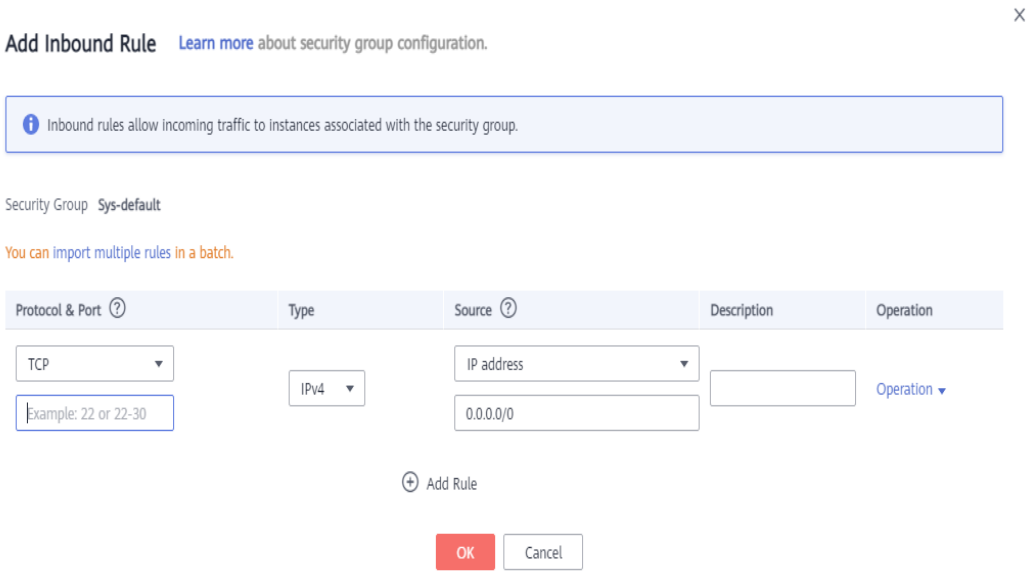



**Tabela 3-10** Configurações da regra de entrada

| Parâmetro | Descrição | Exemplo |
| --- | --- | --- |
| Priority | A prioridade da regra do grupo de segurança.<br>O valor de prioridade varia de 1 a 100. A prioridade padrão é 1 e tem a prioridade mais alta. A regra de grupo de segurança com um valor menor tem uma prioridade mais alta. | 1 |
| Action | As ações de regra do grupo de segurança.<br>Uma regra com uma ação de negação substitui outra com uma ação de permitir se as duas regras tiverem a mesma prioridade. | Allow |
| Protocol & Port | O protocolo de rede necessário para o acesso. Opções disponíveis: **TCP**, **UDP**, **ICMP** ou **GRE** | TCP |
| | Porta: a porta na qual você deseja permitir o acesso ao DDS. A porta padrão é 8635. A porta varia de 2100 a 9500 ou pode ser 27017, 27018 ou 27019. | 8635 |
| Type | Tipo do endereço IP. Apenas **IPv4** e I**IPv6** são suportados. | IPv4 |

| Parâmetro | Descrição | Exemplo |
| --- | --- | --- |
| Source | Especifica o endereço IP, o grupo de segurança e o grupo de endereços IP suportados, que permitem o acesso de endereços IP ou instâncias em outro grupo de segurança. Exemplo:<br>● Endereço IP único: 192.168.10.10/32<br>● Segmento do endereço IP: 192.168.1.0/24<br>● Todos os endereços IP: 0.0.0.0/0<br>● Grupo de segurança: sg-abc<br>● Grupo de endereço IP: ipGroup-test<br>Se você inserir um grupo de segurança, todos os ECSs associados ao grupo de segurança estarão em conformidade com a regra criada.<br>Para obter mais informações sobre grupos de endereços IP, consulte **Grupo de endereços IP**. | 0.0.0.0/0 |
| Description | (Opcional) Fornece informações complementares sobre a regra de grupo de segurança. Este parâmetro é opcional.<br>A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >). | - |

**Passo 9** Clique em **OK**.

**----Fim**

## 3.2.3.2 Conexão a uma instância de conjunto de réplicas usando Mongo Shell (rede privada)

O Mongo shell é o cliente padrão para o servidor de banco de dados MongoDB. Você pode usar o Mongo Shell para se conectar a instâncias de BD e consultar, atualizar e gerenciar dados em bancos de dados. Para usar o Mongo Shell, baixe e instale o cliente de MongoDB primeiro e, em seguida, use o Mongo shell para se conectar à instância de BD.

Por padrão, uma instância do DDS fornece um endereço IP privado. Se suas aplicações forem implementadas em um ECS e estiverem na mesma região e VPC que as instâncias do DDS, você poderá se conectar a instâncias do DDS usando um endereço IP privado para obter uma taxa de transmissão rápida e alta segurança.

Esta seção descreve como usar o Mongo Shell para se conectar a uma instância de conjunto de réplicas em uma rede privada.

O cliente de MongoDB pode se conectar a uma instância com uma conexão não criptografada ou uma conexão criptografada (SSL). Para melhorar a segurança da transmissão de dados, conecte-se a instâncias usando SSL.

## Pré-requisitos

1. Para obter detalhes sobre como criar e fazer logon em um ECS, consulte **Compra de um ECS** e **Logon em um ECS**.
2. Instale o cliente de MongoDB no ECS. Para garantir a autenticação bem-sucedida, instale o cliente de MongoDB da mesma versão da instância de destino.

   Para obter detalhes sobre como instalar um cliente de MongoDB, consulte **Como instalar um cliente de MongoDB?**
3. O ECS pode se comunicar com a instância do DDS. Para mais detalhes, consulte **Configuração de regras de grupo de segurança**.

## Conexão SSL

AVISO

Se você se conectar a uma instância por meio da conexão SSL, ative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como ativar SSL, consulte **Ativação e desativação de SSL**.

**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 e escolha **Databases** > **Document Database Service**.

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

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

**Passo 6** Na área **Basic Information**, clique em ao lado do campo **SSL**.

**Passo 7** Faça upload do certificado raiz para o ECS a ser conectado à instância.

A seguir, descrevemos como fazer upload do certificado para um ECS do Linux e Window:

- No Linux, execute o seguinte comando:

  **scp***<IDENTITY_FILE>**<REMOTE_USER>**@***<REMOTE_ADDRESS>***:***<REMOTE_DIR>*

  NOTA

  - **IDENTITY_FILE** é o diretório onde o certificado raiz reside. A permissão de acesso ao arquivo é 600.
  - **REMOTE_USER** é o usuário do sistema operacional ECS.
  - **REMOTE_ADDRESS** é o endereço do ECS.
  - **REMOTE_DIR** é o diretório do ECS no qual o certificado raiz é carregado.
- No Windows, carregue o certificado raiz usando uma ferramenta de conexão remota.

**Passo 8** Conecte-se a uma instância do DDS.

Método 1: conexão de alta disponibilidade (recomendada)

O DDS fornece o endereço de conexão HA. Usar esse endereço para se conectar a uma instância do conjunto de réplicas melhora o desempenho de leitura/gravação de dados e evita erros relatados quando os dados são gravados do cliente após uma alternância primária/em espera.

Exemplo de comando:

**./mongo "***<Private HA connection address>***" --ssl --sslCAFile***<FILE_PATH>* **--sslAllowInvalidHostnames**

Descrição do parâmetro:

- **Private HA Connection Address**: na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida. Escolha **Connections**. Clique na guia **Private Connection** e obtenha o endereço de conexão da instância atual do campo **Private HA Connection Address**.

  **Figura 3-13** Obter o endereço de conexão HA privada

  O formato do endereço de conexão privada é o seguinte. O nome de usuário do banco de dados **rwuser** e o banco de dados de autenticação **admin** não podem ser alterados.

  **mongodb://rwuser:***<password>@192.168.xx.xx:8635,192.168.xx.xx:8635***/test?authSource=admin&replicaSet=replica**

  Preste atenção aos seguintes parâmetros no endereço HA privado:

  **Tabela 3-11** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| rwuser | Nome da conta, ou seja, o nome de usuário do banco de dados. |
| *<password>* | Senha da conta do banco de dados. Substitua-a pela senha atual.<br>Se a senha contiver sinais de arroba (@), pontos de exclamação (!) ou sinais de porcentagem (%), substitua-os por códigos de URL hexadecimais (ASCII) %40, %21 e %25, respectivamente.<br>Por exemplo, se a senha for ****@ %***!, o código de URL correspondente será **** %40%25*** %21. |

| Parâmetro | Descrição |
| --- | --- |
| *192.168.xx.xx:8635,192.168.xx.xx:8635* | Endereço IP e porta do nó da instância do conjunto de réplicas |
| test | O nome do banco de dados de teste. Você pode definir esse parâmetro com base em seus requisitos de serviço. |
| authSource=admin&replicaSet=replica | – O banco de dados de autenticação do usuário **rwuser** deve ser **admin**. **authSource=admin** é corrigido no comando.<br>– **replica** em **replicaSet=replica** é o nome de um conjunto de réplicas. O conjunto de réplicas padrão do DDS da Huawei Cloud é **replica**. |

- **FILE_PATH** é o caminho para armazenar o certificado raiz.
- --sslAllowInvalidHostnames: o certificado do conjunto de réplicas é gerado usando o endereço IP de gerenciamento interno para garantir que a comunicação interna não ocupe recursos como o endereço IP do usuário e a largura de banda. **--sslAllowInvalidHostnames** é necessário para a conexão SSL por meio de uma rede privada.

Exemplo de comando:

**./mongo "mongodb://rwuser:**<*password*>**@192.168.xx.xx:8635,192.168.xx.xx:8635/test?authSource=admin&replicaSet=replica" --ssl --sslCAFile/tmp/ca.crt --sslAllowInvalidHostnames**

NOTA

- Se você se conectar a uma instância por meio de um endereço HA privado, adicione aspas duplas antes e depois das informações de conexão.
- Para obter detalhes sobre a conexão HA, consulte **Conexão a uma instância de conjunto de réplicas para separação de leitura e gravação e alta disponibilidade**.

Se as seguintes informações forem exibidas, a instância será conectada com êxito:

```
replica:PRIMARY>
```

Execute o seguinte comando para acessar o banco de dados local:

**use local**

Informação semelhante à seguinte foi exibida:

```
switched to db local
```

Execute o seguinte comando para consultar oplog de conjunto de réplicas:

**db.oplog.rs.find()**

Método 2: conexão HA privada (banco de dados e conta definidos pelo usuário)

Exemplo de comando:

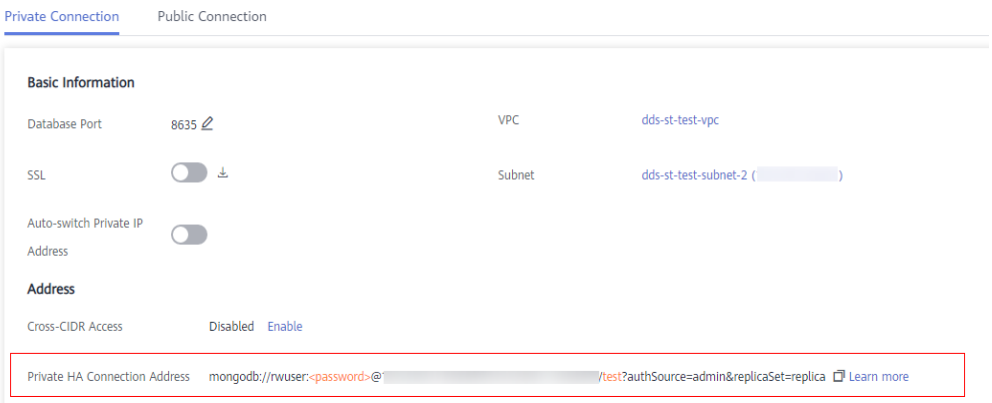
**./mongo "**<*Private HA connection address*>**" --ssl --sslCAFile**<*FILE_PATH*> **--sslAllowInvalidHostnames**

Descrição do parâmetro:

- **Private HA Connection Address**: na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida. Escolha **Connections**. Clique na guia **Private Connection** e obtenha o endereço de conexão da instância atual do campo **Private HA Connection Address**.

**Figura 3-14** Obter o endereço de conexão HA privada




O formato do endereço de conexão HA privada obtido é o seguinte:

**mongodb://rwuser:***<password>*@*192.168.xx.xx:8635,192.168.xx.xx:8635*/test?authSource=admin&replicaSet=replica**

A tabela a seguir lista os parâmetros necessários no endereço HA privado.

**Tabela 3-12** Informações de parâmetro

| Parâmetro | Descrição |
| --- | --- |
| rwuser | Nome de usuário do banco de dados. O valor padrão é **rwuser**. Você pode alterar o valor para o nome de usuário com base em seus requisitos de serviço. |
| *<password>* | Senha para o nome de usuário do banco de dados. Substitua-a pela senha atual.<br>Se a senha contiver sinais de arroba (@), pontos de exclamação (!) ou sinais de porcentagem (%), substitua-os por códigos de URL hexadecimais (ASCII) %40, %21 e %25, respectivamente.<br>Por exemplo, se a senha for ****@ %***!, o código de URL correspondente será **** %40%25*** %21. |
| *192.168.xx.xx:8635,192.168.xx.xx:8635* | Endereço IP e porta do nó da instância do conjunto de réplicas |
| test | O nome do banco de dados de teste. Você pode definir esse parâmetro com base em seus requisitos de serviço. |

| Parâmetro | Descrição |
| --- | --- |
| authSource=admin&replicaSet=replica | – O banco de dados de autenticação do usuário **rwuser** é **admin**.<br>– Em **replica in replicaSet=replica**, **replica** indica que o tipo de instância é conjunto de réplicas e o formato não pode ser alterado.<br>**NOTA**<br>Se você usar um banco de dados definido pelo usuário para autenticação, altere o banco de dados de autenticação no endereço de conexão de alta disponibilidade para o nome do banco de dados definido pelo usuário. Além disso, substitua **rwuser** pelo nome de usuário criado no banco de dados definido pelo usuário. |

- **FILE_PATH** é o caminho para armazenar o certificado raiz.
- **--sslAllowInvalidHostnames**: o certificado do conjunto de réplicas é gerado usando o endereço IP de gerenciamento interno para garantir que a comunicação interna não ocupe recursos como o endereço IP do usuário e a largura de banda. **--sslAllowInvalidHostnames** é necessário para a conexão SSL por meio de uma rede privada.

Por exemplo, se você criar um banco de dados definido pelo usuário **Database** e um usuário **test1** no banco de dados, o comando de conexão será o seguinte:

**./mongo "mongodb://test1:***<password>***@192.168.xx.xx:8635,192.168.xx.xx:8635/Database?authSource=Database&replicaSet=replica" --ssl --sslCAFile/tmp/ca.crt --sslAllowInvalidHostnames**

**Método 3**: conectar a um único nó.

Você também pode usar o endereço IP privado de um nó primário ou secundário para acessar a instância do conjunto de réplicas. Este método afeta o desempenho de leitura/gravação quando ocorre **uma alternância primária/em espera**.

Exemplo de comando:

**./mongo --host** *<DB_HOST>* **--port** *<DB_PORT>* **-u** *<DB_USER>* **-p --authenticationDatabase admin --ssl --sslCAFile***<FILE_PATH>* **--sslAllowInvalidHostnames**

Descrição do parâmetro:

- **DB_HOST** é o endereço IP privado do nó primário ou em espera da instância a ser conectada.

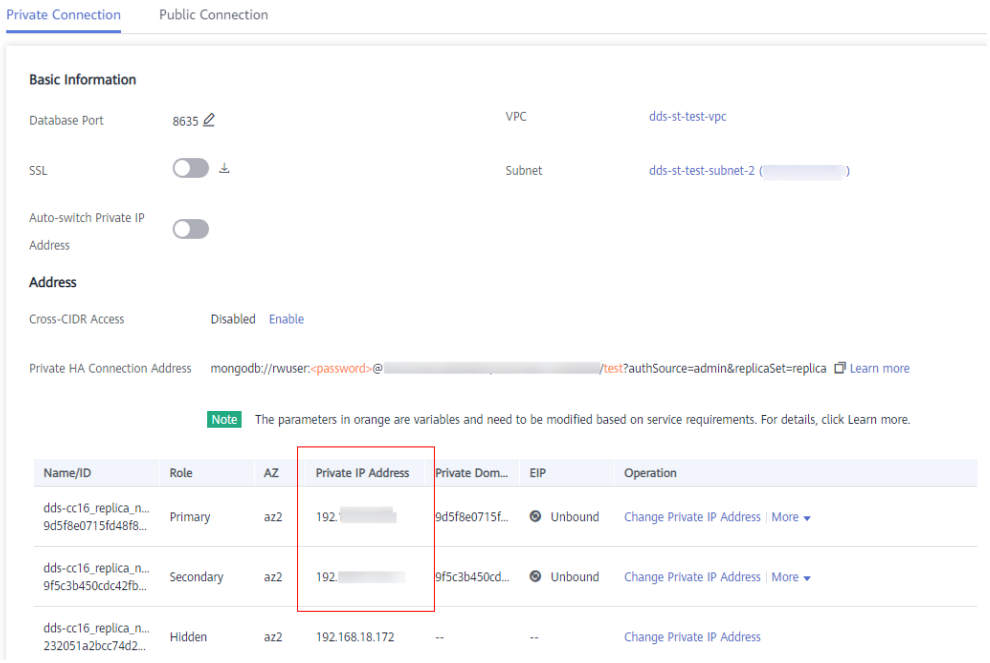
  Nó primário: você pode ler e escrever dados nele.

  Nó secundário: você só pode ler dados dele.

  Na página **Instances**, clique na instância para ir para a página **Basic Information**. Escolha **Connections**. Na guia **Private Connection**, obtenha o endereço IP do nó correspondente.

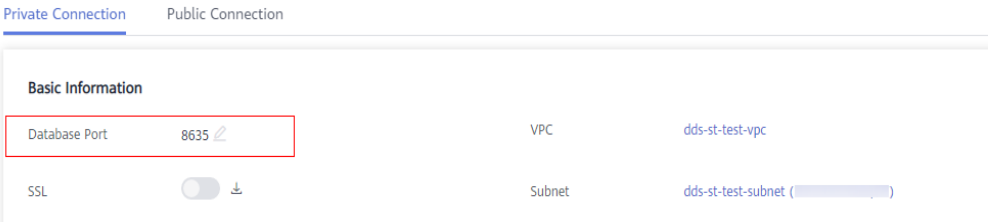
**Figura 3-15** Obter o endereço IP de um nó




- **DB_PORT** é a porta do banco de dados. O valor padrão é 8635.

  Você pode clicar na instância para ir para a página **Basic Information**. No painel de navegação à esquerda, escolha **Connections**. Na página exibida, clique na guia **Private Connection** e obtenha a porta no campo **Database Port** na área **Basic Information**.

  **Figura 3-16** Obter a porta

- **DB_USER** é o usuário do banco de dados. O valor padrão é **rwuser**.
- **FILE_PATH** é o caminho para armazenar o certificado raiz.
- **--sslAllowInvalidHostnames**: o certificado do conjunto de réplicas é gerado usando o endereço IP de gerenciamento interno para garantir que a comunicação interna não ocupe recursos como o endereço IP do usuário e a largura de banda. **--sslAllowInvalidHostnames** é necessário para a conexão SSL por meio de uma rede privada.

Digite a senha da conta do banco de dados quando solicitado:

```
Enter password:
```

Exemplo de comando:

**./mongo --host** *192.168.xx.xx* **--port 8635 -u rwuser -p --authenticationDatabase admin --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames**

Se as seguintes informações forem exibidas, o nó correspondente será conectado com sucesso:

- O nó primário do conjunto de réplicas está conectado.
  ```
  replica:PRIMARY>
  ```
- O nó em espera do conjunto de réplicas está conectado.
  ```
  replica:SECONDARY>
  ```

**----Fim**

## Conexão não criptografada

**AVISO**

Se você se conectar a uma instância por meio de uma conexão não criptografada, desative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como desabilitar SSL, consulte **Ativação e desativação de SSL**.

**Passo 1** Efetue logon no ECS.

**Passo 2** Conecte-se a uma instância do DDS.

Método 1: conexão de alta disponibilidade (recomendada)

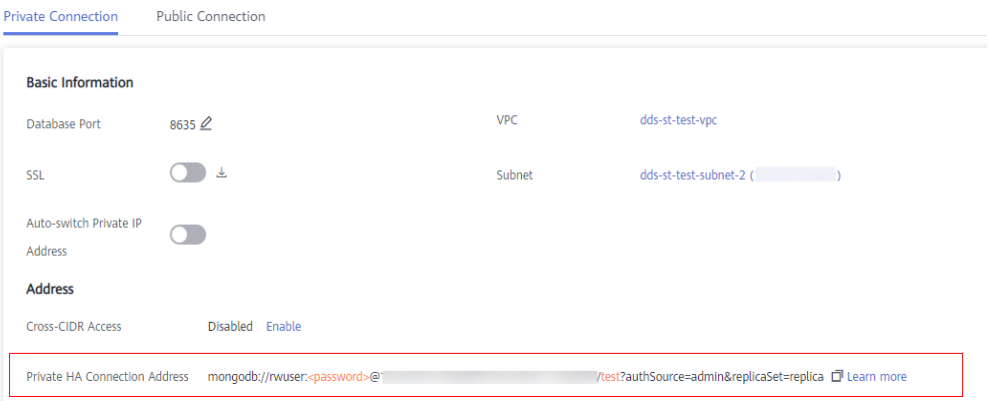
O DDS fornece o endereço de conexão HA. O uso desse endereço para se conectar a uma instância do conjunto de réplicas melhora o desempenho de leitura/gravação e evita erros relatados quando os dados são gravados do cliente após uma alternância primária/em espera.

Exemplo de comando:

**./mongo "***<Private HA Connection Address>***"**

**Private HA Connection Address**: na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida. Escolha **Connections**. Clique na guia **Private Connection** e obtenha o endereço de conexão da instância atual do campo **Private HA Connection Address**.

**Figura 3-17** Obter o endereço de conexão HA privada




O formato do endereço de conexão privada é o seguinte. O nome de usuário do banco de dados **rwuser** e o banco de dados de autenticação **admin** não podem ser alterados.

**mongodb://rwuser:***<password>*@*192.168.xx.xx:8635,192.168.xx.xx:8635*/**test?authSource=admin&replicaSet=replica**

Preste atenção aos seguintes parâmetros no endereço HA privado:

**Tabela 3-13** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| rwuser | Nome da conta, ou seja, o nome de usuário do banco de dados. |
| *<password>* | Senha da conta do banco de dados. Substitua-a pela senha atual.<br>Se a senha contiver sinais de arroba (@), pontos de exclamação (!) ou sinais de porcentagem (%), substitua-os por códigos de URL hexadecimais (ASCII) %40, %21 e %25, respectivamente.<br>Por exemplo, se a senha for ****@ %***!, o código de URL correspondente será **** %40%25*** %21. |
| *192.168.xx.xx:8635,192.168.xx.xx:8635* | Endereço IP e porta do nó da instância do conjunto de réplicas |
| test | O nome do banco de dados de teste. Você pode definir esse parâmetro com base em seus requisitos de serviço. |
| authSource=admin&replicaSet=replica | ● O banco de dados de autenticação do usuário **rwuser** deve ser **admin**. **authSource=admin** é corrigido no comando.<br>● **replica** em **replicaSet=replica** é o nome de um conjunto de réplicas. O conjunto de réplicas padrão do DDS da Huawei Cloud é **replica**. |

Exemplo de comando:

**./mongo "mongodb://rwuser:***<password>*@192.168.xx.xx:8635,192.168.xx.xx:8635/**test?authSource=admin&replicaSet=replica"**

Se as seguintes informações forem exibidas, a instância será conectada com êxito:

```
replica:PRIMARY>
```

Execute o seguinte comando para acessar o banco de dados local:

**use local**

Informação semelhante à seguinte foi exibida:

```
switched to db local
```

Execute o seguinte comando para consultar oplog de conjunto de réplicas:

**db.oplog.rs.find()**

Método 2: conexão HA privada (banco de dados e conta definidos pelo usuário)

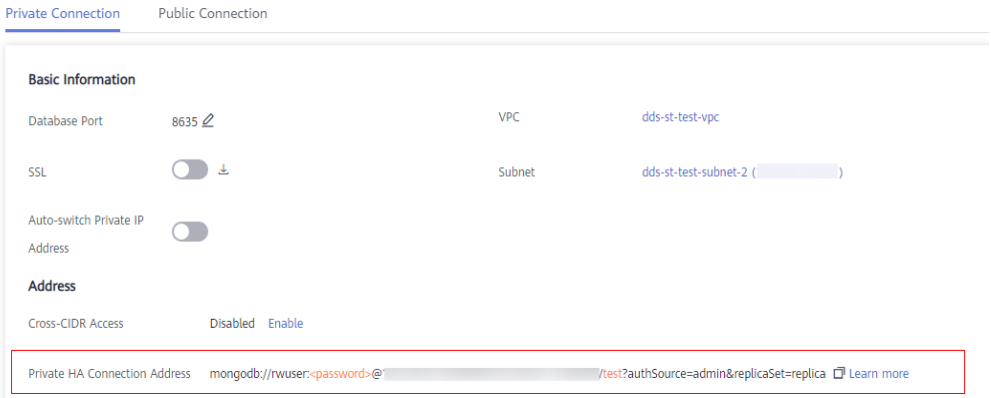
Exemplo de comando:

**./mongo "***<Private HA Connection Address>***"**

**Private HA Connection Address**: na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida. Escolha **Connections**. Clique na guia **Private Connection** e obtenha o endereço de conexão da instância atual do campo **Private HA Connection Address**.

**Figura 3-18** Obter o endereço de conexão HA privada




O formato do endereço de conexão HA privada obtido é o seguinte:

**mongodb://rwuser:***<password>*@*192.168.xx.xx:8635,192.168.xx.xx:8635*/**test?authSource=admin&replicaSet=replica**

A tabela a seguir lista os parâmetros necessários no endereço HA privado.

**Tabela 3-14** Informações de parâmetro

| Parâmetro | Descrição |
| --- | --- |
| rwuser | Nome de usuário do banco de dados. O valor padrão é **rwuser**. Você pode alterar o valor para o nome de usuário com base em seus requisitos de serviço. |
| *<password>* | Senha para o nome de usuário do banco de dados. Substitua-a pela senha atual.<br>Se a senha contiver sinais de arroba (@), pontos de exclamação (!) ou sinais de porcentagem (%), substitua-os por códigos de URL hexadecimais (ASCII) %40, %21 e %25, respectivamente.<br>Por exemplo, se a senha for ****@ %***!, o código de URL correspondente será **** %40%25*** %21. |
| *192.168.xx.xx:8635,192.168.xx.xx:8635* | Endereço IP e porta do nó da instância do conjunto de réplicas |
| test | O nome do banco de dados de teste. Você pode definir esse parâmetro com base em seus requisitos de serviço. |

| Parâmetro | Descrição |
| --- | --- |
| authSource=admin&replicaSet=replica | ● O banco de dados de autenticação do usuário **rwuser** é **admin**.<br>● Em **replica in replicaSet=replica**, **replica** indica que o tipo de instância é conjunto de réplicas e o formato não pode ser alterado.<br>**NOTA**<br>Se você usar um banco de dados definido pelo usuário para autenticação, altere o banco de dados de autenticação no endereço de conexão de alta disponibilidade para o nome do banco de dados definido pelo usuário. Além disso, substitua **rwuser** pelo nome de usuário criado no banco de dados definido pelo usuário. |

Por exemplo, se você criar um banco de dados definido pelo usuário **Database** e um usuário **test1** no banco de dados, o comando de conexão será o seguinte:

**./mongo "mongodb://test1:***<password>***@192.168.xx.xx:8635,192.168.xx.xx:8635/Database?authSource=Database&replicaSet=replica"**

**Método 3**: conectar-se a um único nó.

Você também pode usar o endereço IP privado de um nó primário ou secundário para acessar a instância do conjunto de réplicas. Este método afeta o desempenho de leitura/gravação quando ocorre uma alternância primária/em espera.

Exemplo de comando:

**./mongo --host** *<DB_HOST>* **--port** *<DB_PORT>* **-u** *<DB_USER>* **-p --authenticationDatabase admin**

Descrição do parâmetro:

- **DB_HOST** é o endereço IP privado do nó primário ou em espera da instância a ser conectada.

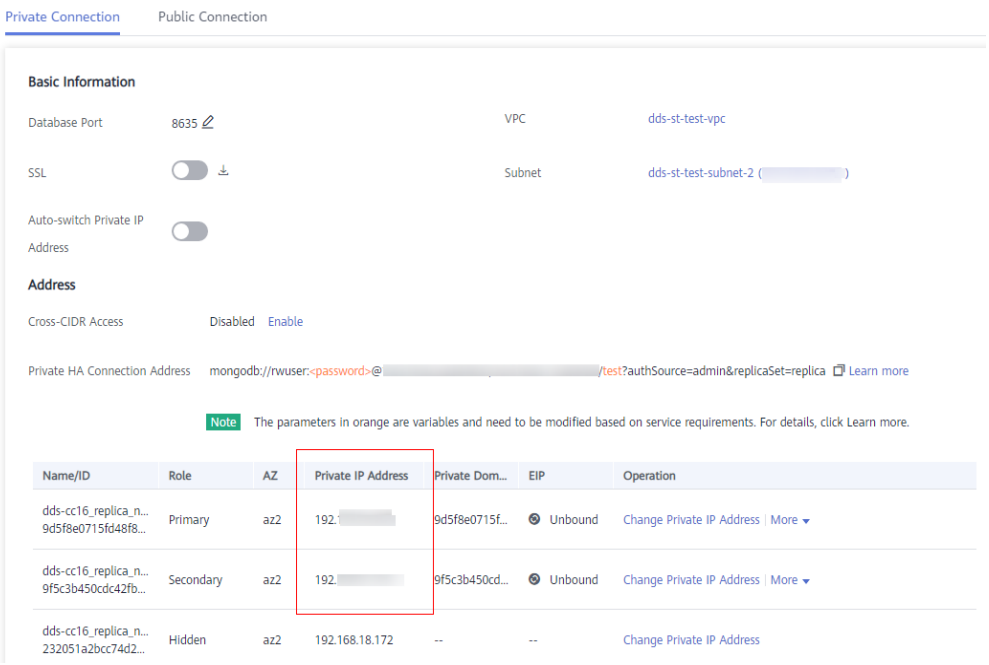
  Nó primário: você pode ler e escrever dados nele.

  Nó secundário: você só pode ler dados dele.

  Na página **Instances**, clique na instância para ir para a página **Basic Information**. Escolha **Connections**. Na guia **Private Connection**, obtenha o endereço IP do nó correspondente.

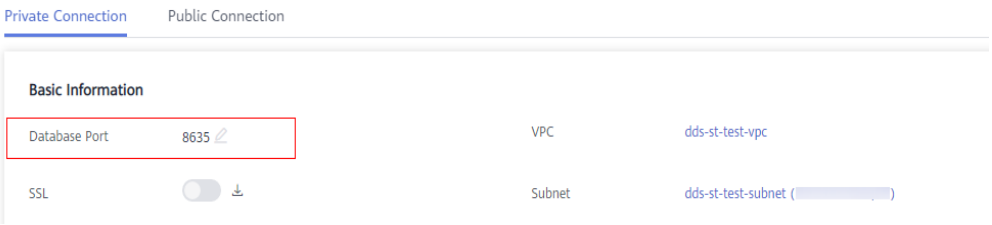
**Figura 3-19** Obter o endereço IP de um nó




- **DB_PORT** é a porta do banco de dados. O valor padrão é 8635.

  Você pode clicar na instância para ir para a página **Basic Information**. No painel de navegação à esquerda, escolha **Connections**. Na página exibida, clique na guia **Private Connection** e obtenha a porta no campo **Database Port** na área **Basic Information**.

**Figura 3-20** Obter a porta




- **DB_USER** é o usuário do banco de dados. O valor padrão é **rwuser**.

Exemplo de comando:

**./mongo --host** *192.168.xx.xx* **--port 8635 -u rwuser -p --authenticationDatabase admin**

Digite a senha da conta do banco de dados quando solicitado:

```
Enter password:
```

Se as seguintes informações forem exibidas, o nó correspondente será conectado com sucesso:

- O nó primário do conjunto de réplicas está conectado.
  ```
  replica:PRIMARY>
  ```
- O nó em espera do conjunto de réplicas está conectado.
  ```
  replica:SECONDARY>
  ```

**----Fim**

### 3.2.3.3 Conexão a réplicas de leitura usando Mongo Shell

O Mongo shell é o cliente padrão para o servidor de banco de dados MongoDB. Você pode usar o Mongo Shell para se conectar a instâncias de BD e consultar, atualizar e gerenciar dados em bancos de dados. Para usar o Mongo Shell, baixe e instale o cliente de MongoDB primeiro e, em seguida, use o Mongo shell para se conectar à instância de BD.

Por padrão, uma instância do DDS fornece um endereço IP privado. Se suas aplicações forem implementadas em um ECS e estiverem na mesma região e VPC que as instâncias do DDS, você poderá se conectar a instâncias do DDS usando um endereço IP privado para obter uma taxa de transmissão rápida e alta segurança.

Esta seção descreve como usar o Mongo Shell para se conectar a uma réplica de leitura em uma rede privada.

Você pode se conectar a uma réplica de leitura usando uma conexão SSL ou uma conexão não criptografada. A conexão SSL é criptografada e mais segura. Para melhorar a segurança da transmissão de dados, conecte-se a instâncias usando SSL.

## Pré-requisitos

1. Para obter detalhes sobre como criar e fazer logon em um ECS, consulte **Compra de um ECS** e **Logon em um ECS**.
2. Instale o cliente de MongoDB no ECS. Para garantir a autenticação bem-sucedida, instale o cliente de MongoDB da mesma versão da instância de destino.

   Para obter detalhes sobre como instalar um cliente de MongoDB, consulte **Como instalar um cliente de MongoDB?**
3. O ECS pode se comunicar com a instância do DDS. Para mais detalhes, consulte **Configuração de regras de grupo de segurança**.

## Conexão SSL

**AVISO**

Se você se conectar a uma instância por meio da conexão SSL, ative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como ativar SSL, consulte **Ativação e desativação de SSL**.

**Passo 1** Na página **Instances**, clique no nome da instância.

**Passo 2** No painel de navegação à esquerda, escolha **Connections**.

**Passo 3** Na área **Basic Information**, clique em ao lado do campo **SSL**.

**Passo 4** Faça upload do certificado raiz para o ECS a ser conectado à instância.

A seguir, descrevemos como fazer upload do certificado para um ECS do Linux e Window:

- No Linux, execute o seguinte comando:

  **scp***<IDENTITY_FILE>**<REMOTE_USER>@<REMOTE_ADDRESS>:<REMOTE_DIR>*

NOTA

- **IDENTITY_FILE** é o diretório onde o certificado raiz reside. A permissão de acesso ao arquivo é 600.
- **REMOTE_USER** é o usuário do sistema operacional ECS.
- **REMOTE_ADDRESS** é o endereço do ECS.
- **REMOTE_DIR** é o diretório do ECS no qual o certificado raiz é carregado.

- No Windows, carregue o certificado raiz usando uma ferramenta de conexão remota.

**Passo 5** Conecte-se a uma instância do DDS. O console do DDS fornece o endereço de conexão da réplica de leitura. Você pode usar esse endereço para se conectar à réplica de leitura.

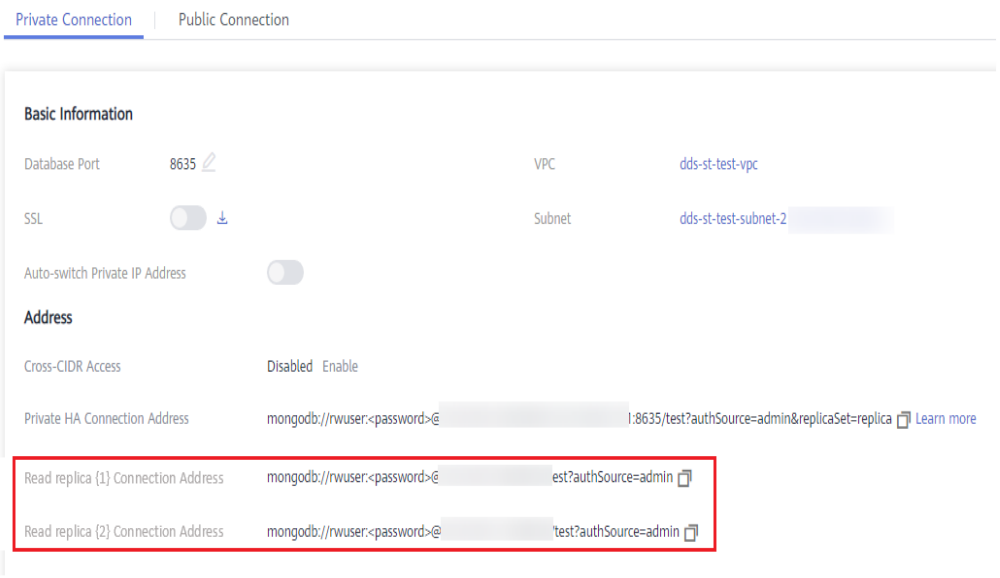
Exemplo de comando:

**./mongo "***<Read replica connection address>***" --ssl --sslCAFile***<FILE_PATH>* **--sslAllowInvalidHostnames**

Descrição do parâmetro:

- **Read Replica Connection Address**: na página **Instances**, clique na instância para ir para a página **Basic Information**. Escolha **Connections**. Clique na guia **Private Connection** Na área **Address**, obtenha o endereço de conexão da instância de réplica de leitura.

**Figura 3-21** Obter o endereço de conexão de réplica de leitura




O formato do endereço de conexão de réplica de leitura é o seguinte. O nome de usuário do banco de dados **rwuser** e o banco de dados de autenticação **admin** não podem ser alterados.

**mongodb://rwuser:***<password>@192.168.xx.xx:8635***/test?authSource=admin**

Preste atenção aos seguintes parâmetros no endereço de conexão de réplica de leitura:

**Tabela 3-15** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| rwuser | Nome da conta, ou seja, o nome de usuário do banco de dados. |
| *<password>* | Senha da conta do banco de dados. Substitua-a pela senha atual.<br>Se a senha contiver sinais de arroba (@), pontos de exclamação (!) ou sinais de porcentagem (%), substitua-os por códigos de URL hexadecimais (ASCII) %40, %21 e %25, respectivamente.<br>Por exemplo, se a senha for ****@ %***!, o código de URL correspondente será **** %40%25*** %21. |
| *192.168.xx.xx:8635* | Endereço IP e porta da réplica de leitura da instância do conjunto de réplicas |
| test | O nome do banco de dados de teste. Você pode definir esse parâmetro com base em seus requisitos de serviço. |
| authSource=admin | O banco de dados de autenticação do usuário **rwuser** deve ser **admin**. **authSource=admin** é corrigido no comando. |

- **FILE_PATH** é o caminho para armazenar o certificado raiz.
- --sslAllowInvalidHostnames: o certificado do conjunto de réplicas é gerado usando o endereço IP de gerenciamento interno para garantir que a comunicação interna não ocupe recursos como o endereço IP do usuário e a largura de banda. **--sslAllowInvalidHostnames** é necessário para a conexão SSL por meio de uma rede privada.

Exemplo de comando:

**./mongo "mongodb://rwuser:***<password>***@*192.168.xx.xx:8635*/test?authSource=admin" --ssl --sslCAFile/tmp/ca.crt --sslAllowInvalidHostnames**

NOTA

Ao se conectar a uma instância usando o endereço de conexão de réplica de leitura, adicione aspas duplas (") antes e depois das informações de conexão.

Se as seguintes informações forem exibidas, a instância será conectada com êxito:

```
replica:SECONDARY>
```

**----Fim**

## Conexão não criptografada

**AVISO**

Se você se conectar a uma instância por meio de uma conexão não criptografada, desative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como desabilitar SSL, consulte **Ativação e desativação de SSL**.

**Passo 1** Efetue logon no ECS.

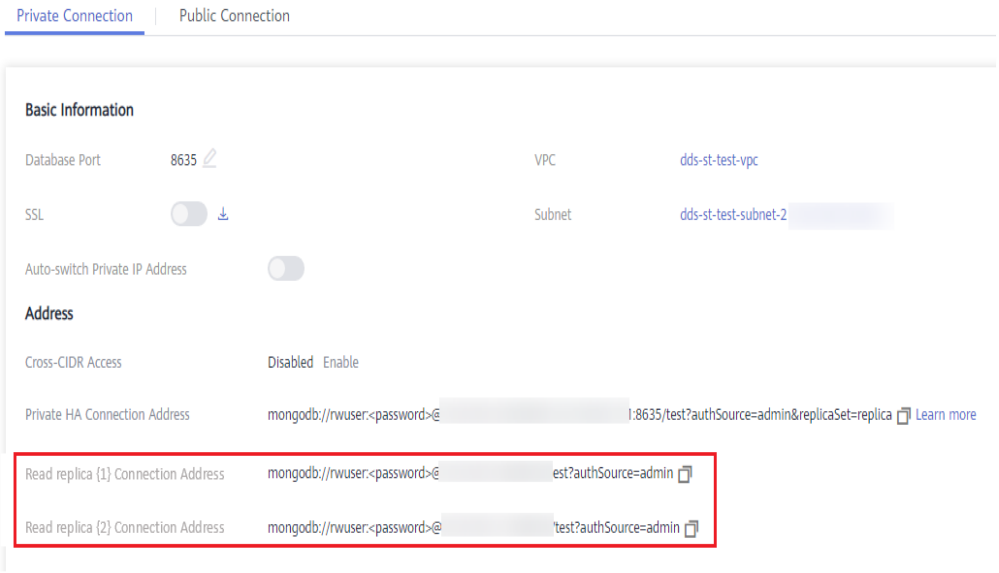
**Passo 2** Conecte-se a uma instância do DDS. O console do DDS fornece o endereço de conexão da réplica de leitura. Você pode usar esse endereço para se conectar à réplica de leitura.

Exemplo de comando:

**./mongo "***<Read replica connection address>***"**

**Read Replica Connection Address**: na página **Instances**, clique na instância para ir para a página **Basic Information**. Escolha **Connections**. Clique na guia **Private Connection** Na área **Address**, obtenha o endereço de conexão da instância de réplica de leitura.

**Figura 3-22** Obter o endereço de conexão de réplica de leitura




O formato do endereço de conexão de réplica de leitura é o seguinte. O nome de usuário do banco de dados **rwuser** e o banco de dados de autenticação **admin** não podem ser alterados.

**mongodb://rwuser:***<password>@192.168.xx.xx:8635***/test?authSource=admin**

Preste atenção aos seguintes parâmetros no endereço HA privado:

**Tabela 3-16** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| rwuser | Nome da conta, ou seja, o nome de usuário do banco de dados. |
| *<password>* | Senha da conta do banco de dados. Substitua-a pela senha atual.<br>Se a senha contiver sinais de arroba (@), pontos de exclamação (!) ou sinais de porcentagem (%), substitua-os por códigos de URL hexadecimais (ASCII) %40, %21 e %25, respectivamente.<br>Por exemplo, se a senha for ****@ %***!, o código de URL correspondente será **** %40%25*** %21. |
| *192.168.xx.xx:8635* | Endereço IP e porta da réplica de leitura da instância do conjunto de réplicas |
| test | O nome do banco de dados de teste. Você pode definir esse parâmetro com base em seus requisitos de serviço. |
| authSource=admin | O banco de dados de autenticação do usuário **rwuser** deve ser **admin**. **authSource=admin** é corrigido no comando. |

Exemplo de comando:

**./mongo "mongodb://rwuser:***<password>*@*192.168.xx.xx:8635*/test?authSource=admin"**

Se as seguintes informações forem exibidas, a instância será conectada com êxito:

```
replica:SECONDARY>
```

**----Fim**

# 3.2.4 Conexão a uma instância de conjunto de réplicas em numa rede pública

## 3.2.4.1 Vinculação ou desvinculação de um EIP

Depois de criar uma instância, você pode vincular um EIP a ela para permitir acesso externo. Se mais tarde você quiser proibir o acesso externo, você também pode desvincular o EIP da instância de BD.

## Precauções

- A exclusão de um EIP vinculado não significa que o EIP não esteja vinculado.
- Antes de acessar um banco de dados, solicite um EIP no console da VPC. Em seguida, adicione uma regra de entrada para permitir os endereços IP ou intervalos de endereços IP de ECSs. Para mais detalhes, consulte **Configuração de regras de grupo de segurança**.

- Na instância do conjunto de réplicas, apenas os nós primários e secundários podem ter um EIP vinculado. Para alterar o EIP que foi vinculado a um nó, você precisa desvinculá-lo do nó primeiro.

## Vincular um EIP

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

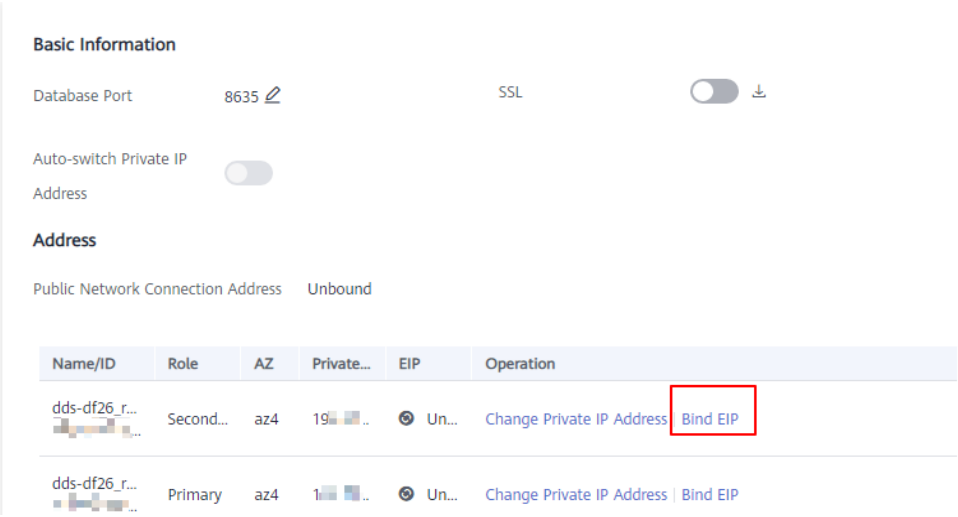
**Passo 2** Clique em no canto superior esquerdo e selecione uma região e um projeto.

**Passo 3** Clique em no canto superior esquerdo da página e escolha **Databases** > **Document Database Service**.

**Passo 4** Na página **Instances**, clique no nome da instância do conjunto de réplicas.

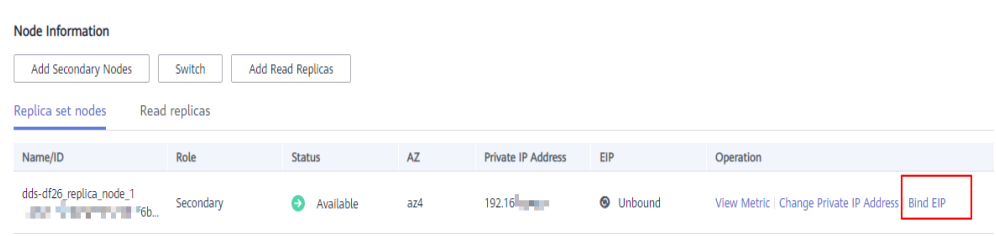
**Passo 5** No painel de navegação à esquerda, escolha **Connections**. Clique na guia **Public Connection**. Na área **Basic Information**, localize o nó ao qual deseja vincular um EIP e clique em **Bind EIP** na coluna **Operation**.

**Figura 3-23** Vincular um EIP




Você também pode localizar o nó na área **Node Information area** na página **Basic Information** e clicar em **Bind EIP** na coluna **Operation**.

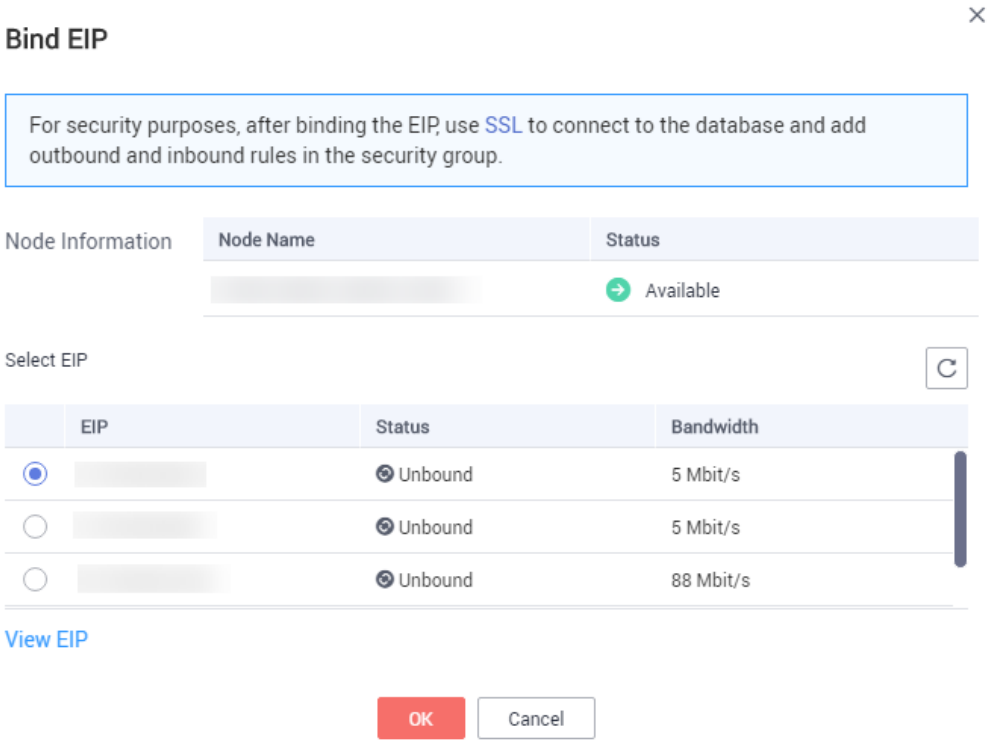
**Figura 3-24** Vincular um EIP




**Passo 6** Na caixa de diálogo exibida, todos os EIPs não vinculados e disponíveis são listados. Selecione o EIP necessário e clique em **OK**. Se nenhum EIP disponível for exibido, clique em **View EIP** e crie um EIP no console da VPC.

**Figura 3-25** Selecionar um EIP




**Passo 7** Localize o nó de destino. Na coluna **EIP**, você pode exibir o EIP vinculado.

Para desvincular um EIP da instância, consulte **Desvincular um EIP**.

**----Fim**

## Desvincular um EIP

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

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

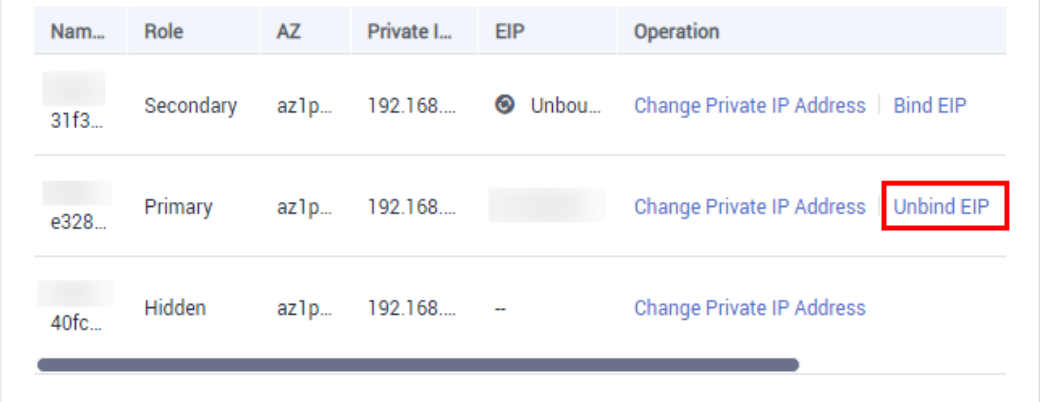
**Passo 3** Clique em no canto superior esquerdo da página e escolha **Databases** > **Document Database Service**.

**Passo 4** Na página **Instances**, clique na instância do conjunto de réplicas vinculada a um EIP.

**Passo 5** No painel de navegação à esquerda, escolha **Connections**. Clique na guia **Public Connection**. Na área **Basic Information**, localize o nó e clique em **Unbind EIP** na coluna **Operation**.

**Figura 3-26** Desvincular um EIP




Você também pode localizar o nó na área **Node Information area** na página **Basic Information** e clicar em **Unbind EIP** na coluna **Operation**.

**Passo 6** Na caixa de diálogo exibida, clique em **Yes**.

Para vincular um EIP à instância novamente, consulte **Vincular um EIP**.

**----Fim**

## 3.2.4.2 Configuração de regras de grupo de segurança

Um grupo de segurança é uma coleção de regras de controle de acesso para ECSs e instâncias do DDS que têm os mesmos requisitos de proteção de segurança e são mutuamente confiáveis em uma VPC.

Para garantir a segurança e a confiabilidade do banco de dados, é necessário configurar regras de grupo de segurança para permitir que endereços IP e portas específicos acessem a instância.

Quando você tenta se conectar a uma instância por meio de um EIP, é necessário configurar uma regra de entrada para o grupo de segurança associado à instância.

### Precauções

- Por predefinição, uma conta pode criar até 500 regras de grupo de segurança.
- Muitas regras de grupo de segurança aumentarão a latência do primeiro pacote, portanto, recomenda-se um máximo de 50 regras para cada grupo de segurança.
- Uma instância do DDS só pode ser associada a um grupo de segurança.

### 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 e escolha **Databases** > **Document Database Service**.

**Passo 4** Na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida.

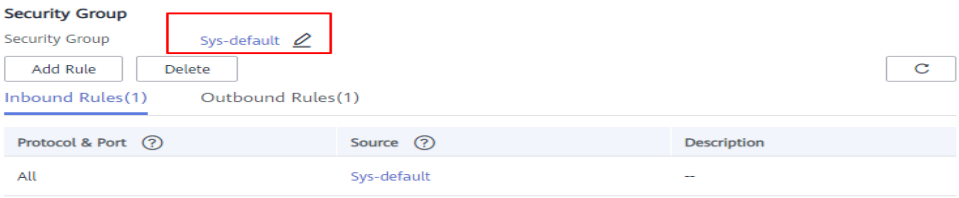
  

**Passo 5** Na área **Network Information** da página **Basic Information**, clique no nome do grupo de segurança.

**Figura 3-27** Grupo de segurança


Você também pode escolher **Connections** no painel de navegação à esquerda. Na guia **Public Connection**, na área **Security Group**, clique no nome do grupo de segurança.

**Figura 3-28** Grupo de segurança




**Passo 6** Na página **Security Group**, localize o grupo de segurança de destino e clique em **Manage Rule** na coluna **Operation**.

**Passo 7** Na guia **Inbound Rules**, clique em **Add Rule**. A caixa de diálogo **Add Inbound Rule** é exibida.

**Passo 8** Adicione uma regra de grupo de segurança conforme solicitado.

**Figura 3-29** Adicionar regra de entrada

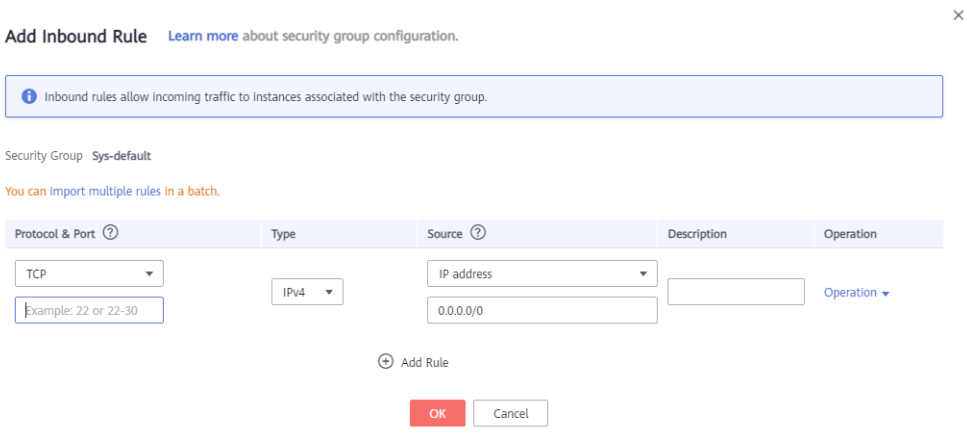


**Tabela 3-17** Configurações da regra de entrada

| Parâmetro | Descrição | Exemplo de valor |
| --- | --- | --- |
| Priority | A prioridade da regra do grupo de segurança.<br>O valor de prioridade varia de 1 a 100. A prioridade padrão é 1 e tem a prioridade mais alta. A regra de grupo de segurança com um valor menor tem uma prioridade mais alta. | 1 |
| Action | As ações de regra do grupo de segurança.<br>Uma regra com uma ação de negação substitui outra com uma ação de permitir se as duas regras tiverem a mesma prioridade. | Allow |
| Protocol & Port | O protocolo de rede necessário para o acesso. A opção pode ser **All**, **TCP**, **UDP**, **ICMP** ou **GRE**. | TCP |
| | Porta: a porta na qual você deseja permitir o acesso ao DDS. A porta padrão é 8635. A porta varia de 2100 a 9500 ou pode ser 27017, 27018 ou 27019. | 8635 |
| Type | Tipo do endereço IP. Apenas **IPv4** e **IPv6** são suportados. | IPv4 |
| Source | Especifica o endereço IP, o grupo de segurança e o grupo de endereços IP suportados, que permitem o acesso de endereços IP ou instâncias em outro grupo de segurança. Exemplo:<br>● Endereço IP único: 192.168.10.10/32<br>● Segmento do endereço IP: 192.168.1.0/24<br>● Todos os endereços IP: 0.0.0.0/0<br>● Grupo de segurança: sg-abc<br>● Grupo de endereço IP: ipGroup-test<br>Se você inserir um grupo de segurança, todos os ECSs associados ao grupo de segurança estarão em conformidade com a regra criada.<br>Para obter mais informações sobre grupos de endereços IP, consulte **Grupo de endereços IP**. | 0.0.0.0/0 |
| Description | (Opcional) Fornece informações complementares sobre a regra de grupo de segurança. Este parâmetro é opcional.<br>A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >). | - |

**Passo 9** Clique em **OK**.

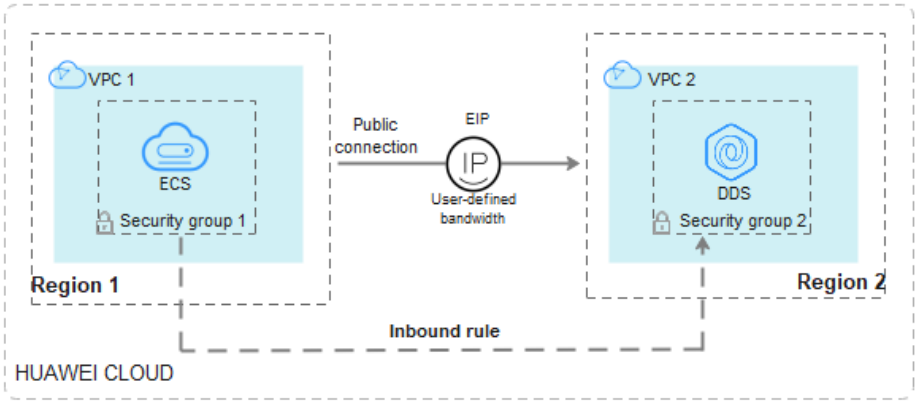
**----Fim**

## 3.2.4.3 Conexão a uma instância de conjunto de réplicas usando Mongo Shell (rede pública)

Nos cenários a seguir, você pode acessar uma instância do DDS da Internet vinculando um EIP à instância.

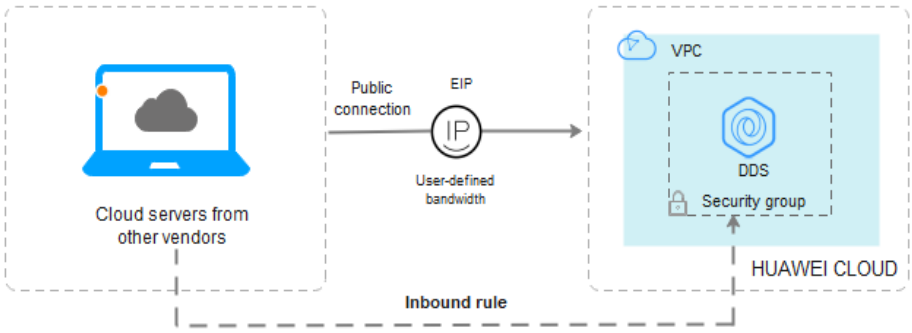
Cenário 1: suas aplicações são implementadas em um ECS e não estão na mesma região que a instância do DDS.

**Figura 3-30** Acessar o DDS a partir do ECS em todas as regiões




Cenário 2: suas aplicações são implementadas em um servidor de nuvem fornecido por outros fornecedores.

**Figura 3-31** Acessar o DDS de outros servidores em nuvem




Esta seção descreve como usar o Mongo Shell para se conectar a uma instância do conjunto de réplicas por meio de um EIP.

Você pode se conectar a uma instância usando uma conexão SSL ou uma conexão não criptografada. A conexão SSL é criptografada e mais segura. Para melhorar a segurança da transmissão de dados, conecte-se a instâncias usando SSL.

## Pré-requisitos

1. Para obter detalhes sobre como criar e fazer logon em um ECS, consulte **Compra de um ECS** e **Logon em um ECS**.
2. Vincule um **EIP** à instância de conjunto de réplicas e configure regras de grupo de segurança para garantir que a instância de conjunto de réplicas possa ser acessada a partir de um ECS.
3. Instale o cliente de MongoDB no ECS.

   Para obter detalhes sobre como instalar um cliente de MongoDB, consulte **Como instalar um cliente de MongoDB?**

   NOTA

   A versão do cliente de MongoDB instalado deve ser a mesma que a versão da instância.

## Conexão SSL

AVISO

Se você se conectar a uma instância por meio da conexão SSL, ative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como ativar SSL, consulte **Ativação e desativação de SSL**.

**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 e escolha **Databases** > **Document Database Service**.

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

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

**Passo 6** Na área **Basic Information**, clique em ao lado do campo **SSL**.

**Passo 7** Carregue o certificado raiz para o ECS a ser conectado à instância.

A seguir, descrevemos como fazer upload do certificado para um ECS do Linux e Window:

- No Linux, execute o seguinte comando:

  **scp**<*IDENTITY_FILE*><*REMOTE_USER*>**@**<*REMOTE_ADDRESS*>**:**<*REMOTE_DIR*>

  NOTA

  - **IDENTITY_FILE** é o diretório onde o certificado raiz reside. A permissão de acesso ao arquivo é 600.
  - **REMOTE_USER** é o usuário do sistema operacional ECS.
  - **REMOTE_ADDRESS** é o endereço do ECS.
  - **REMOTE_DIR** é o diretório do ECS no qual o certificado raiz é carregado.

- No Windows, carregue o certificado raiz usando uma ferramenta de conexão remota.

**Passo 8** Conecte-se à instância no diretório em que o cliente de MongoDB está localizado.

Método 1: utilizar um endereço de conexão de rede pública

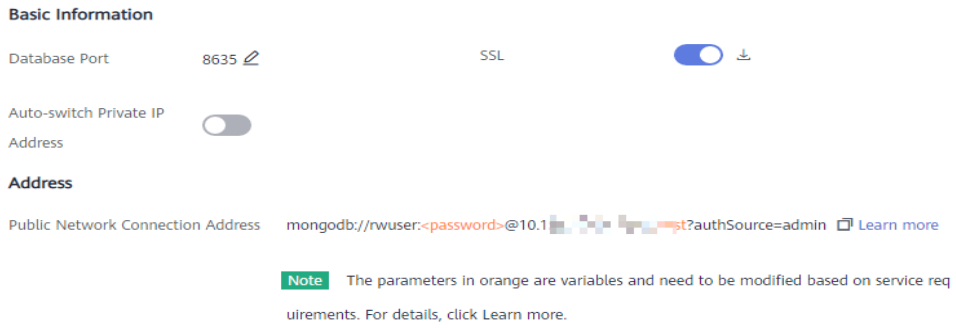
Exemplo de comando:

**./mongo "***<Public network connection address>***" --ssl --sslCAFile***<FILE_PATH>* **--sslAllowInvalidHostnames**

Descrição do parâmetro:

- **Public Network Connection Address**: na página **Instances**, clique na instância para navegar até a página **Basic Information**. No painel de navegação à esquerda, escolha **Connections**. Clique na guia **Public Connection** e obtenha o endereço de conexão de rede pública.

  **Figura 3-32** Obter o endereço de conexão de rede pública




O formato do endereço de conexão pública é o seguinte. O nome de usuário do banco de dados **rwuser** e o banco de dados de autenticação **admin** não podem ser alterados.

**mongodb://rwuser:***<password>*@*192.168.xx.xx:8635*/**test?authSource=admin**

Preste atenção aos seguintes parâmetros no endereço de conexão de rede pública:

**Tabela 3-18** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| rwuser | Nome da conta, ou seja, o nome de usuário do banco de dados. |
| *<password>* | Senha da conta do banco de dados. Substitua-a pela senha atual.<br>Se a senha contiver sinais de arroba (@), pontos de exclamação (!) ou sinais de porcentagem (%), substitua-os por códigos de URL hexadecimais (ASCII) %40, %21 e %25, respectivamente.<br>Por exemplo, se a senha for ****@ %***!, o código de URL correspondente será **** %40%25*** %21. |

| Parâmetro | Descrição |
| --- | --- |
| *192.168.xx.xx:8635* | O EIP e a porta vinculados ao nó da instância do conjunto de réplicas. |
| authSource=admin | O banco de dados de autenticação do usuário **rwuser** deve ser **admin**. **authSource=admin** é corrigido no comando. |

- **FILE_PATH** é o caminho para armazenar o certificado raiz.
- **--sslAllowInvalidHostnames**: o certificado do conjunto de réplicas é gerado usando o endereço IP de gerenciamento interno para garantir que a comunicação interna não ocupe recursos como o endereço IP do usuário e a largura de banda. **--sslAllowInvalidHostnames** é necessário para a conexão SSL por meio de uma rede pública.

Exemplo de comando:

**./mongo "mongodb://rwuser:**<*password*>**@***192.168.xx.xx:8635*/**test?authSource=admin" --ssl --sslCAFile/tmp/ca.crt --sslAllowInvalidHostnames**

NOTA

- Se você se conectar a uma instância por meio de um endereço HA público, adicione aspas duplas antes e depois das informações de conexão.
- Para melhorar o desempenho de leitura e gravação e evitar que erros sejam relatados quando os dados são gravados do cliente após uma alternância primária/em espera. Para obter detalhes sobre como se conectar a uma instância no modo HA, consulte **Conexão a uma instância de conjunto de réplicas para separação de leitura e gravação e alta disponibilidade**.

Método 2: usar um EIP

Exemplo de comando:

**./mongo --host** <*DB_HOST*> **--port** <*DB_PORT*> **-u** <*DB_USER*> **-p --authenticationDatabaseadmin --ssl --sslCAFile**<*FILE_PATH*> **--sslAllowInvalidHostnames**

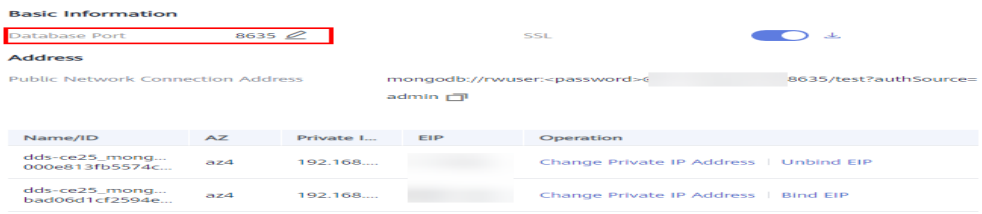
Descrição do parâmetro:

- **DB_HOST** é o EIP vinculado ao nó da instância a ser conectada.

  Na página **Instances**, clique na instância para ir para a página **Basic Information**. Escolha **Connections**> **Public Connection** e obtenha o EIP do nó correspondente.
- **DB_PORT** é a porta do banco de dados. O número de porta padrão é 8635.

  Você pode clicar na instância para ir para a página **Basic Information**. No painel de navegação à esquerda, escolha **Connections**. Na página exibida, clique na guia **Public Connection** e obtenha a porta no campo **Database Port** na área **Basic Information**.

**Figura 3-33** Obter a porta



- **DB_USER** é o usuário do banco de dados. O valor padrão é **rwuser**.
- **FILE_PATH** é o caminho para armazenar o certificado raiz.
- --sslAllowInvalidHostnames: o certificado do conjunto de réplicas é gerado usando o endereço IP de gerenciamento interno para garantir que a comunicação interna não ocupe recursos como o endereço IP do usuário e a largura de banda. **--sslAllowInvalidHostnames** é necessário para a conexão SSL por meio de uma rede pública.

Digite a senha da conta do banco de dados quando solicitado:

```
Enter password:
```

Exemplo de comando:

**./mongo --host** *192.168.xx.xx* **--port 8635 -u rwuser -p --authenticationDatabase admin --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames**

**Passo 9** Verifique o resultado da conexão. Se as informações a seguir forem exibidas, a conexão será bem-sucedida.

- O nó primário do conjunto de réplicas está conectado.
  ```
  replica:PRIMARY>
  ```
- O nó em espera do conjunto de réplicas está conectado.
  ```
  replica:SECONDARY>
  ```

**----Fim**

## Conexão não criptografada

**AVISO**

Se você se conectar a uma instância por meio de uma conexão não criptografada, desative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como desabilitar SSL, consulte **Ativação e desativação de SSL**.

**Passo 1** Efetue logon no ECS.

**Passo 2** Conecte-se a uma instância do DDS.

Método 1: utilizar um endereço de conexão de rede pública

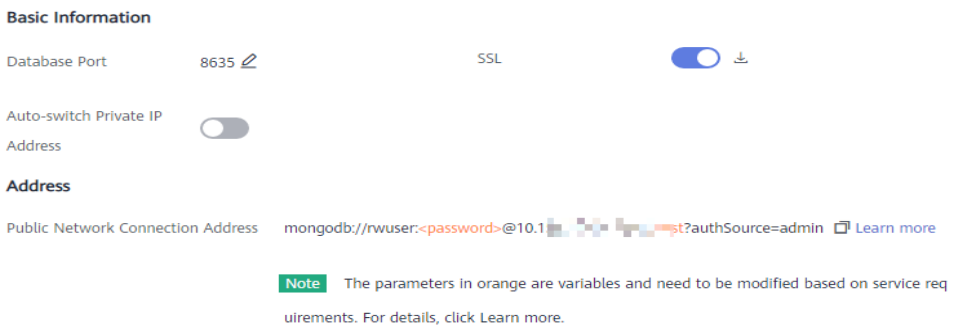
Exemplo de comando:

**./mongo "**<*Public network address*>**"**

**Public Network Connection Address**: na página **Instances**, clique na instância para navegar até a página **Basic Information**. No painel de navegação à esquerda, escolha **Connections**. Clique na guia **Public Connection** e obtenha o endereço de conexão de rede pública.

**Figura 3-34** Obter o endereço de conexão de rede pública




O formato do endereço de conexão pública é o seguinte. O nome de usuário do banco de dados **rwuser** e o banco de dados de autenticação **admin** não podem ser alterados.

**mongodb://rwuser:***<password>*@*192.168.xx.xx:8635*/**test?authSource=admin**

Preste atenção aos seguintes parâmetros no endereço de conexão pública:

**Tabela 3-19** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| rwuser | Nome da conta, ou seja, o nome de usuário do banco de dados. |
| *<password>* | Senha da conta do banco de dados. Substitua-a pela senha atual.<br>Se a senha contiver sinais de arroba (@), pontos de exclamação (!) ou sinais de porcentagem (%), substitua-os por códigos de URL hexadecimais (ASCII) %40, %21 e %25, respectivamente.<br>Por exemplo, se a senha for ****@ %***!, o código de URL correspondente será **** %40%25*** %21. |
| *192.168.xx.xx:8635* | O EIP e a porta vinculados ao nó da instância do conjunto de réplicas. |
| authSource=admin | O banco de dados de autenticação do usuário **rwuser** deve ser **admin**. **authSource=admin** é corrigido no comando. |

Exemplo de comando:

**./mongo "mongodb://rwuser:***<password>*@*192.168.xx.xx:8635*/**test?authSource=admin"**

**NOTA**

- Se você se conectar a uma instância por meio de um endereço HA público, adicione aspas duplas antes e depois das informações de conexão.
- Para melhorar o desempenho de leitura e gravação e impedir que erros sejam relatados quando os dados são gravados do cliente após uma alternância primária/em espera, é aconselhável conectar-se a uma instância usando o endereço de conexão HA. Para obter detalhes, consulte **Conexão a uma instância de conjunto de réplicas para separação de leitura e gravação e alta disponibilidade**.

Método 2: usar um EIP

Exemplo de comando:

**./mongo --host** <*DB_HOST*> **--port** <*DB_PORT*> **-u** <*DB_USER*> **-p --authenticationDatabase admin**

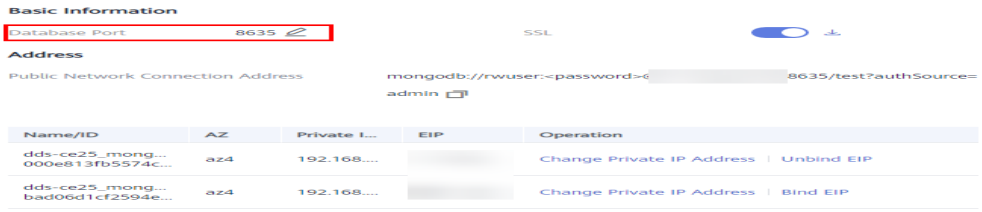
Descrição do parâmetro:

- **DB_HOST** é o EIP vinculado ao nó da instância a ser conectada.

  Na página **Instances**, clique na instância para ir para a página **Basic Information**. Escolha **Connections**> **Public Connection** e obtenha o EIP do nó correspondente.
- **DB_PORT** é a porta do banco de dados. O número de porta padrão é 8635.

  Você pode clicar na instância para ir para a página **Basic Information**. No painel de navegação à esquerda, escolha **Connections**. Na página exibida, clique na guia **Public Connection** e obtenha a porta no campo **Database Port** na área **Basic Information**.

  **Figura 3-35** Obter a porta




- **DB_USER** é o usuário do banco de dados. O valor padrão é **rwuser**.

Digite a senha da conta do banco de dados quando solicitado:

```
Enter password:
```

Exemplo de comando:

**./mongo --host** *192.168.xx.xx* **--port 8635 -u rwuser -p --authenticationDatabase admin**

**Passo 3** Verifique o resultado da conexão. Se as informações a seguir forem exibidas, a conexão será bem-sucedida.

- O nó primário do conjunto de réplicas está conectado.
  ```
  replica:PRIMARY>
  ```
- O nó em espera do conjunto de réplicas está conectado.
  ```
  replica:SECONDARY>
  ```

**----Fim**

## 3.2.4.4 Conexão a uma instância de conjunto de réplicas usando Robo 3T

Para se conectar a uma instância a partir de um dispositivo local, você pode usar o Robo 3T para acessar a instância a partir da Internet.

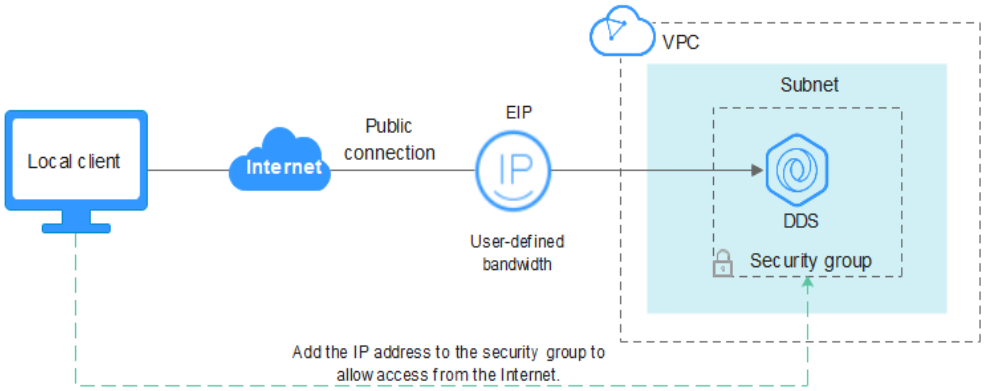
  

Esta seção descreve como usar o Robo 3T para se conectar a uma instância de cluster a partir de um dispositivo local. Nesta seção, o sistema operacional (SO) Windows usado pelo cliente é usado como um exemplo.

O Robo 3T pode se conectar a uma instância com uma conexão não criptografada ou uma conexão criptografada (SSL). Para melhorar a segurança da transmissão de dados, conecte-se a instâncias usando SSL.

## Diagrama de conexão

**Figura 3-36** Diagrama de conexão




## Pré-requisitos

1. Vincule um EIP ao ECS e configure regras de grupo de segurança.
   a. Vincule um EIP à instância do conjunto de réplicas.

      Para obter detalhes sobre como vincular um EIP, consulte **Vinculação ou desvinculação de um EIP**.
   b. Obtenha o endereço IP de um dispositivo local.
   c. Configure regras de grupos de segurança.

      Adicione o endereço IP obtido em **1.b** e a porta da instância à regra de entrada do grupo de segurança.

      Para obter detalhes sobre como configurar regras de grupo de segurança, consulte **Configuração de regras de grupo de segurança**.
   d. Execute o comando ping para fazer ping do EIP vinculado em **1.a** para garantir que o EIP esteja acessível através do seu dispositivo local.
2. Instale o Robo 3T.
   a. Para obter detalhes, consulte **Instalação do Robo 3T**.

## SSL

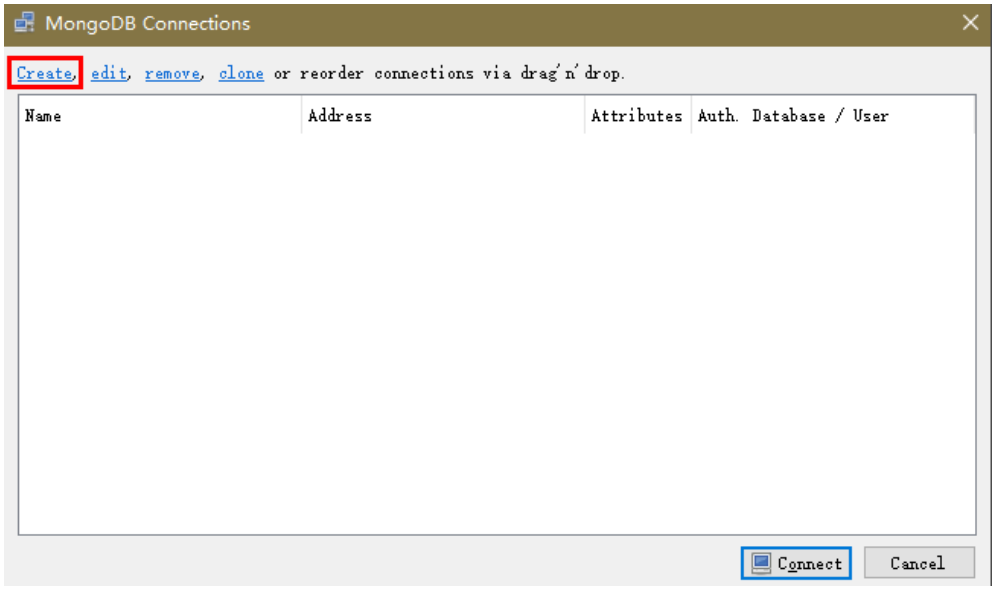
**AVISO**

Se você se conectar a uma instância por meio da conexão SSL, ative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como ativar SSL, consulte **Ativação e desativação de SSL**.

**Passo 1** Execute o Robo 3T instalado. Na caixa de diálogo exibida, clique em **Create**.

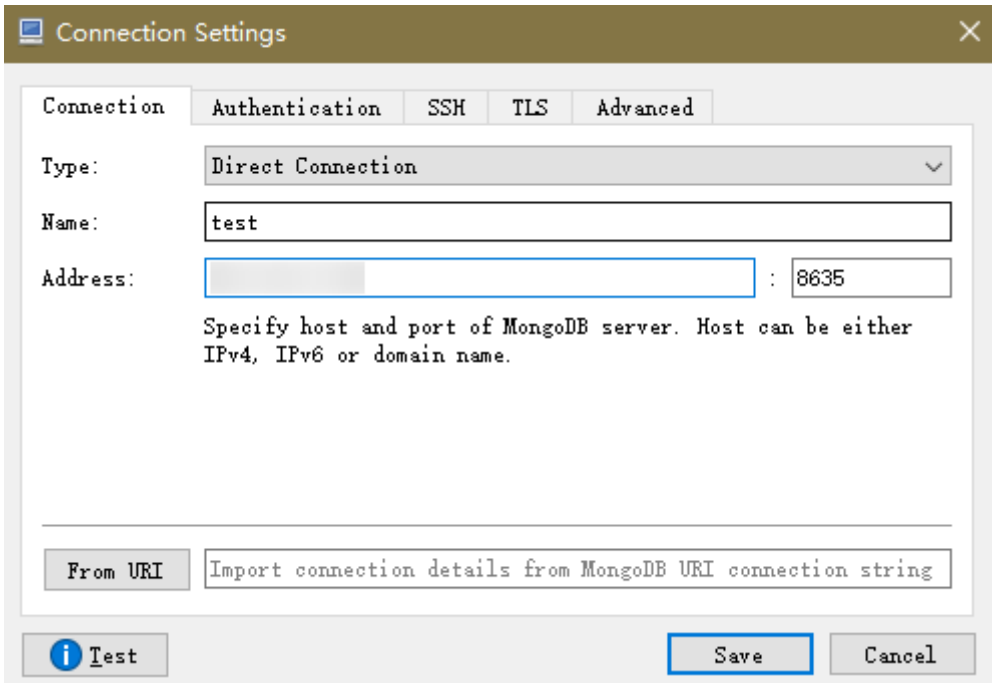
**Figura 3-37** Conexões




**Passo 2** Na caixa de diálogo **Connection Settings**, defina os parâmetros da nova conexão.

1. Na guia **Connection**, digite o nome da nova conexão na caixa de texto **Name** e insira o EIP e a porta do banco de dados vinculada à instância de BD do DDS na caixa de texto **Address**.

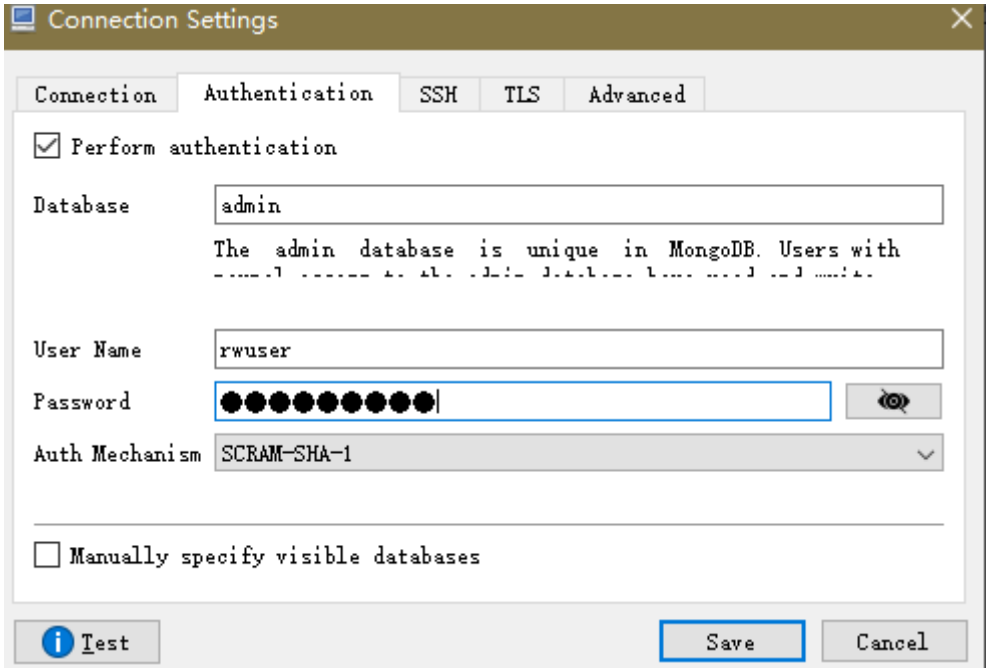
   **Figura 3-38** Conexão

2. Na guia **Authentication**, defina **Database** como **admin**, **User Name** como **rwuser** e **Password** como a senha de administrador definida durante a criação da instância de cluster.

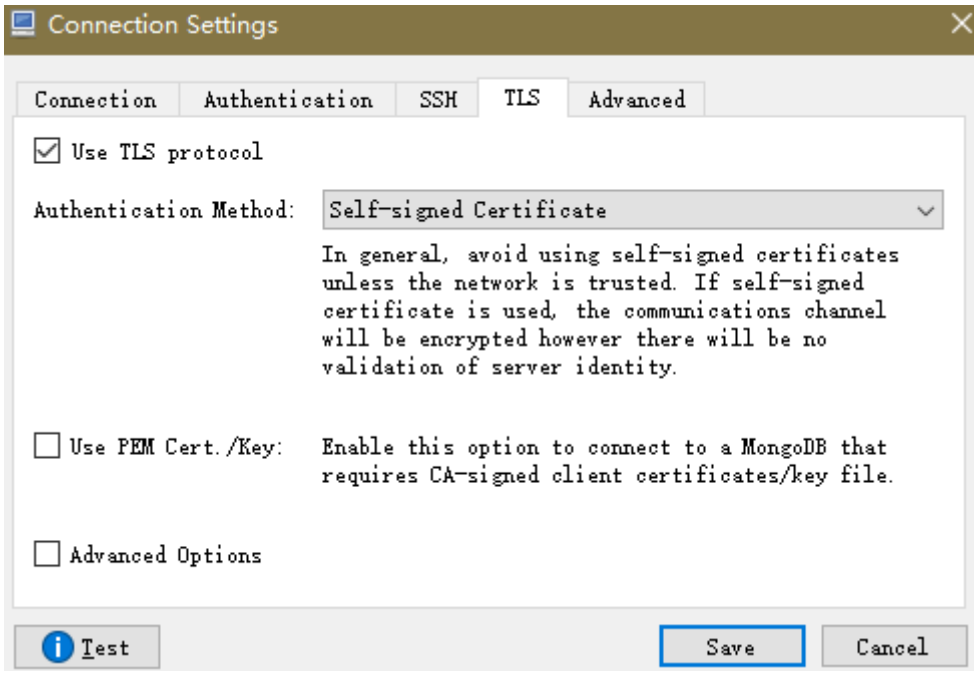
  

**Figura 3-39** Autenticação




3. Na guia **TLS**, selecione **Use TLS protocol** e selecione **Self-signed Certificate** para **Authentication Method**.

**Figura 3-40** SSL

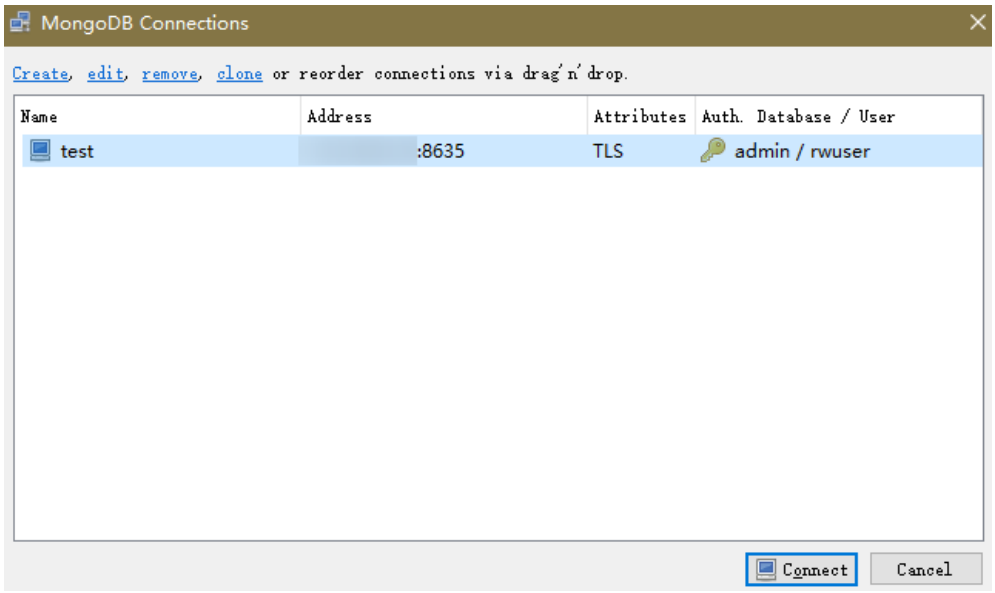



4. Clique em **Save**.

**Passo 3** Na página **MongoDB Connections**, clique em **Connect** para se conectar à instância do conjunto de réplicas.

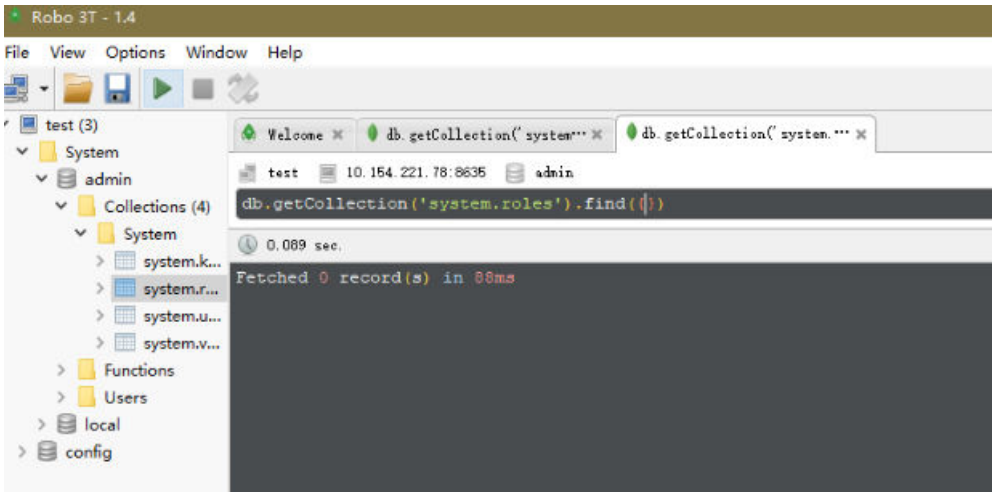
  

**Figura 3-41** Informações de conexão do cluster




**Passo 4** Se a instância de conjunto de réplicas for conectada com êxito, a página mostrada em **Figura 3-42** será exibida.

**Figura 3-42** Conexão bem-sucedida




**----Fim**

## Conexão não criptografada

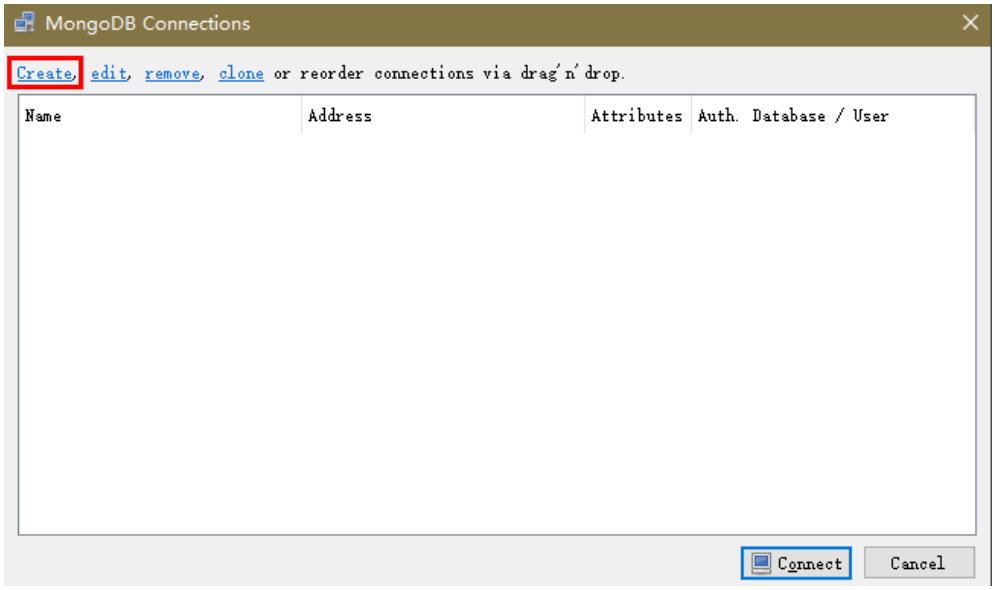
**AVISO**

Se você se conectar a uma instância por meio de uma conexão não criptografada, desative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes, consulte **Ativação e desativação de SSL**.

**Passo 1** Execute o Robo 3T instalado. Na caixa de diálogo exibida, clique em **Create**.

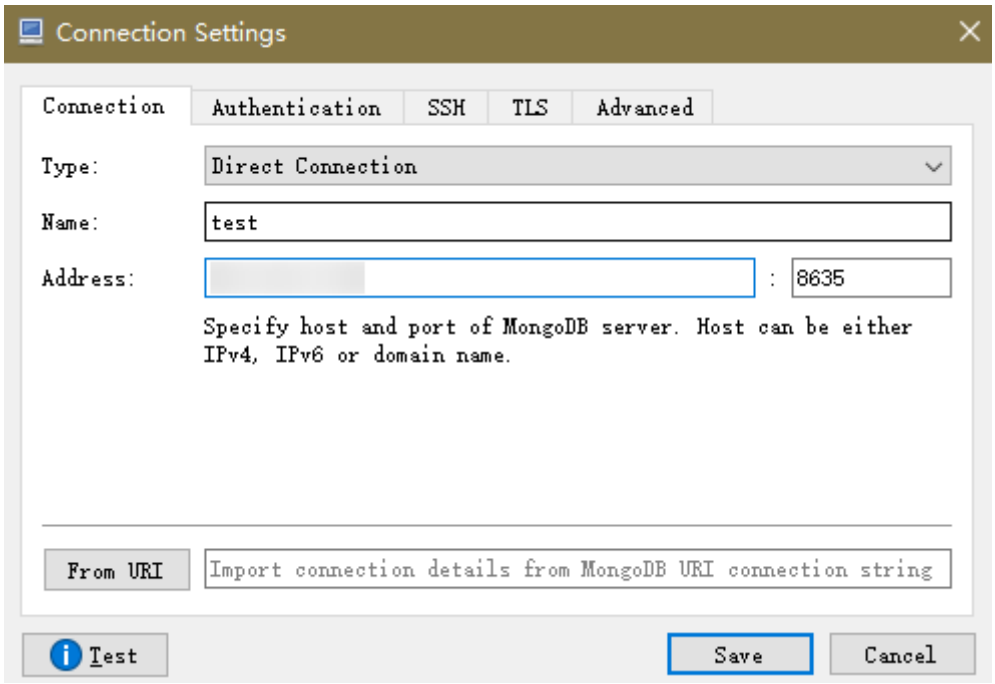
**Figura 3-43** Conexões




**Passo 2** Na caixa de diálogo **Connection Settings**, defina os parâmetros da nova conexão.

1. Na guia **Connection**, digite o nome da nova conexão na caixa de texto **Name** e insira o EIP e a porta do banco de dados vinculada à instância de BD do DDS na caixa de texto **Address**.

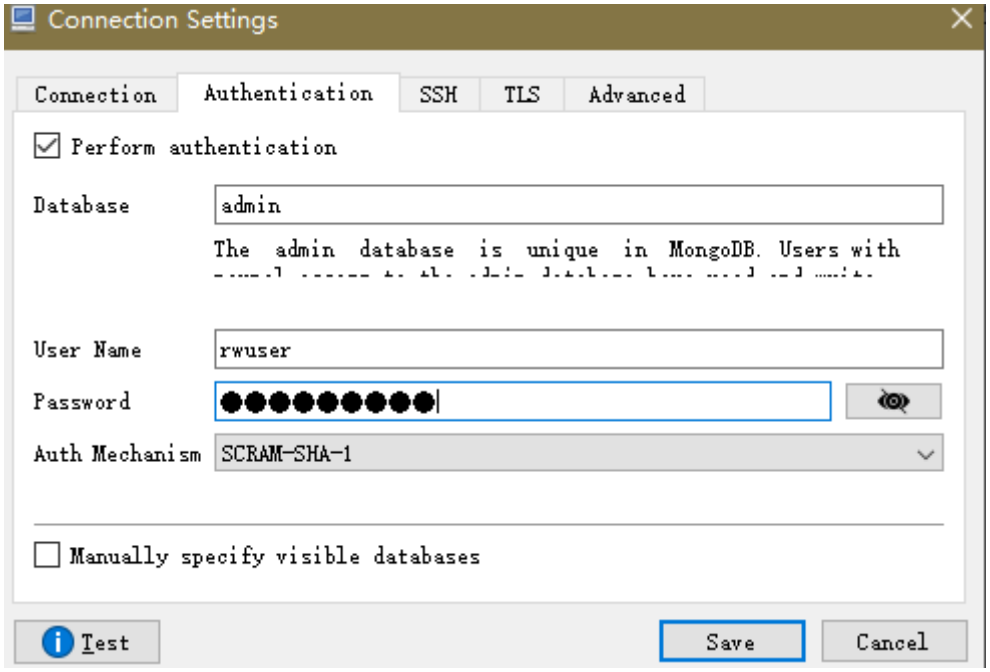
**Figura 3-44** Conexão




2. Na guia **Authentication**, defina **Database** como **admin**, **User Name** como **rwuser** e **Password** como a senha de administrador definida durante a criação da instância de cluster.

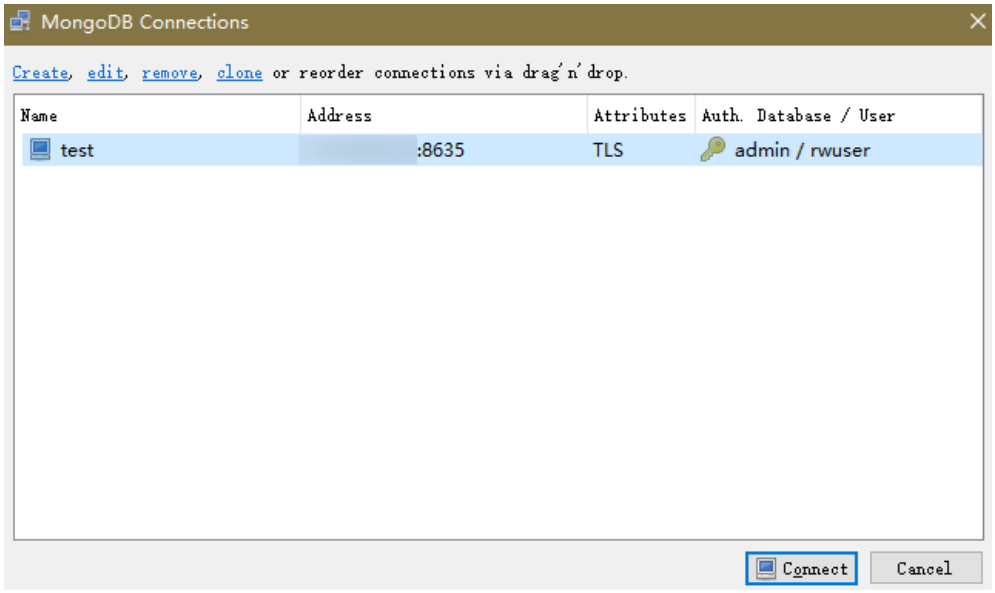
**Figura 3-45** Autenticação




3. Clique em **Save**.

**Passo 3** Na página **MongoDB Connections**, clique em **Connect** para se conectar à instância do conjunto de réplicas.

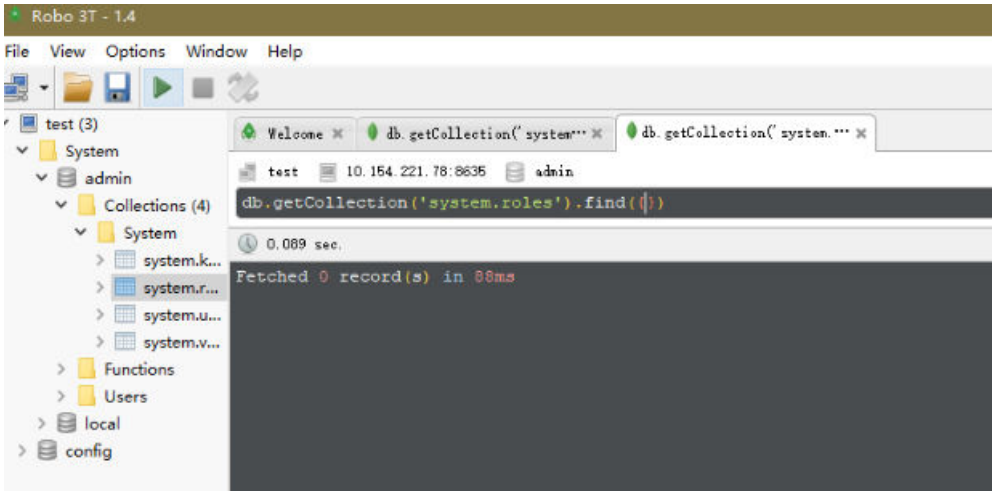
**Figura 3-46** Informações de conexão do conjunto de réplicas




**Passo 4** Se a instância de conjunto de réplicas for conectada com êxito, a página mostrada em **Figura 3-47** será exibida.

**Figura 3-47** Conexão bem sucedida




**----Fim**

# 3.2.5 Conexão a uma instância de conjunto de réplicas usando código do programa

## 3.2.5.1 Java

Se você estiver se conectando a uma instância usando Java, um certificado SSL é opcional, mas baixar um certificado SSL e criptografar a conexão melhorarão a segurança de sua instância. SSL é desativado por padrão para instâncias recém-criadas, mas você pode ativar SSL consultando **Ativação ou desativação de SSL**. SSL criptografa conexões com bancos de dados, mas aumenta o tempo de resposta da conexão e o uso da CPU. Por esse motivo, a ativação de SSL não é recomendada.

### Pré-requisitos

Familiarize-se com:

- Noções básicas de computador
- Código Java

### Obter e utilizar Java

- Baixe o driver do Jar em **https://repo1.maven.org/maven2/org/mongodb/mongo-java-driver/3.0.4/**
- Para ver o guia de uso, visite **https://mongodb.github.io/mongo-java-driver/4.2/driver/getting-started/installation/**.

## Usar um certificado SSL

NOTA

- Baixe o certificado SSL e verifique o certificado antes de se conectar aos bancos de dados.
- Na área **DB Information** da página **Basic Information**, clique em no campo **SSL** para baixar certificado raiz ou do pacote de certificados.
- Para obter detalhes sobre como configurar uma conexão SSL, consulte o documento oficial do driver Java do MongoDB em **https://www.mongodb.com/docs/drivers/java/sync/current/fundamentals/connection/tls/#std-label-tls-ssl**.

Use Java para conectar-se ao conjunto de réplicas. O formato do código Java é o seguinte:

```
mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>?authSource=admin&replicaSet=replica&ssl=true
```

**Tabela 3-20** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| <username> | Nome de usuário atual. |
| <password> | Senha para o nome de usuário atual |
| <instance_ip> | Se você tentar acessar a instância de um ECS, defina *instance_ip* como o endereço IP privado exibido na página **Basic Information** da instância à qual você pretende se conectar. |
| | Se você tentar acessar a instância por meio de um EIP, defina *instance_ip* como o EIP vinculado à instância. |
| <instance_port> | Porta do banco de dados exibida na página **Basic Information**. Valor padrão: **8635** |
| <database_name> | Nome do banco de dados a ser conectado. |
| authSource | Base de dados de utilizadores de autenticação. O valor é **admin**. |
| ssl | Modo de conexão. **true** indica que o modo de conexão SSL é usado. |

Use a keytool para configurar o certificado CA. Para obter detalhes sobre os parâmetros, consulte **Tabela 3-21**.

```
keytool -importcert -trustcacerts -file <path to certificate authority file> -keystore <path to trust store> -storepass <password>
```

**Tabela 3-21** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| <path to certificate authority file> | Caminho para armazenar o certificado SSL. |
| <path to trust store> | Caminho para armazenar o repositório confiável. Defina este parâmetro conforme necessário, por exemplo, **./trust/certs.keystore**. |

| Parâmetro | Descrição |
| --- | --- |
| <password> | Senha personalizada. |

Defina as propriedades do sistema JVM no programa para apontar para o repositório confiável e repositório de chaves corretos:

- System.setProperty("javax.net.ssl.trustStore","<path to trust store>");
- System.setProperty("javax.net.ssl.trustStorePassword","<password>");

Para obter detalhes sobre o código Java, consulte o exemplo a seguir:

```
public class Connector { public static void main(String[] args) { try
{ System.setProperty("javax.net.ssl.trustStore", "./trust/
certs.keystore"); System.setProperty("javax.net.ssl.trustStorePassword",
"123456"); ConnectionString connString = new ConnectionString("mongodb://
<username>:<password>@<instance_ip>:<instance_port>/<database_name>?
authSource=admin&replicaSet=replica&ssl=true"); MongoClientSettings
settings =
MongoClientSettings.builder() .applyConnectionString(connString) .applyTo
SslSettings(builder ->
builder.enabled(true)) .applyToSslSettings(builder ->
builder.invalidHostNameAllowed(true)) .build(); MongoClient mongoClient
= MongoClients.create(settings); MongoDatabase database =
mongoClient.getDatabase("admin"); //Ping the database. Se a operação
falhar, ocorre uma exceção. BsonDocument command = new
BsonDocument("ping", new BsonInt64(1)); Document commandResult =
database.runCommand(command); System.out.println("Connect to database
successfully"); } catch (Exception e) { e.printStackTrace();
System.out.println("Test failed"); } } }
```

## Conexão sem o certificado SSL

NOTA

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

Conecte-se a uma instância do conjunto de réplicas usando Java. O formato do link de Java é o seguinte:

```
mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>?
authSource=admin&replicaSet=replica
```

**Tabela 3-22** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| <username> | Nome de usuário atual. |
| <password> | Senha para o nome de usuário atual |
| <instance_ip> | Se você tentar acessar a instância de um ECS, defina *instance_ip* como o endereço IP privado exibido na página **Basic Information** da instância à qual você pretende se conectar. |

| Parâmetro | Descrição |
| --- | --- |
| | Se você tentar acessar a instância por meio de um EIP, defina *instance_ip* como o EIP vinculado à instância. |
| <instance_port> | Porta do banco de dados exibida na página **Basic Information**. Valor padrão: **8635** |
| <database_name> | Nome do banco de dados a ser conectado. |
| authSource | Base de dados de utilizadores de autenticação. O valor é **admin**. |

Para obter detalhes sobre o código Java, consulte o exemplo a seguir:

```
public class Connector { public static void main(String[] args) { try
{ ConnectionString connString = new ConnectionString("mongodb://
<username>:<password>@<instance_ip>:<instance_port>/<database_name>?
authSource=admin&replicaSet=replica"); MongoClientSettings settings =
MongoClientSettings.builder() .applyConnectionString(connString) .retryWr
ites(true) .build(); MongoClient mongoClient =
MongoClients.create(settings); MongoDatabase database =
mongoClient.getDatabase("admin"); //Ping the database. Se a operação
falhar, ocorre uma exceção. BsonDocument command = new
BsonDocument("ping", new BsonInt64(1)); Document commandResult =
database.runCommand(command); System.out.println("Connect to database
successfully"); } catch (Exception e) { e.printStackTrace();
System.out.println("Test failed"); } }
```

}

### 3.2.5.2 Python

Esta seção descreve como se conectar a uma instância de conjunto de réplicas usando Python.

## Pré-requisitos

1. Para conectar um ECS a uma instância, o ECS deve ser capaz de se comunicar com a instância do DDS. Você pode executar o seguinte comando para conectar-se ao endereço IP e à porta do servidor de instância para testar a conectividade de rede.

   **curl** *ip:port*

   Se a mensagem **It looks like you are trying to access MongoDB over HTTP on the native driver port** for exibida, a conectividade de rede é normal.
2. Instale Python e o pacote de instalação de terceiros **pymongo** no ECS. Pymongo 2.8 é recomendado.
3. Se SSL estiver ativado, você precisará baixar o certificado raiz e carregá-lo no ECS.

## Código de conexão

- Ativar SSL

  ```
  import ssl
  from pymongo import MongoClient
  conn_urls="mongodb://rwuser:rwuserpassword@ip:port/{mydb}?
  authSource=admin&replicaSet=replica"
  connection = MongoClient(conn_urls,connectTimeoutMS=5000,ssl=True,
  ```

```
ssl_cert_reqs=ssl.CERT_REQUIRED,ssl_match_hostname=False,ssl_ca_certs
=${path to certificate authority file})
dbs = connection.database_names()
print "connect database success! database names is %s" % dbs
```

- Desativar SSL

```
import ssl
from pymongo import MongoClient
conn_urls="mongodb://rwuser:rwuserpassword@ip:port/{mydb}?
authSource=admin&replicaSet=replica"
connection = MongoClient(conn_urls,connectTimeoutMS=5000)
dbs = connection.database_names()
print "connect database success! database names is %s" % dbs
```

NOTA

- O banco de dados de autenticação no URL deve ser **admin**. Isso significa definir **authSource** como **admin**.
- No modo SSL, você precisa gerar manualmente o arquivo trustStore.
- A base de dados de autenticação tem de ser **admin** e, em seguida, mudar para a base de dados de serviço.

# 4 Primeiros passos com nós únicos

## 4.1 Compra de uma instância de nó único

### 4.1.1 Configuração rápida

Esta seção descreve como comprar uma instância de nó único no console de gerenciamento. O DDS ajuda você a configurar e criar rapidamente um único nó em poucos minutos.

#### Precauções

Cada conta pode criar até 20 nós únicos no total.

#### Pré-requisitos

- Você registrou uma conta da Huawei Cloud.

#### Procedimento

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

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

Se você quiser recursos de computação e rede dedicados ao seu uso exclusivo, **ative uma DeC** e **solicite recursos do DCC**. Depois de ativar uma DeC, você pode selecionar a região da DeC e o projeto.

**Passo 3** Clique em no canto superior esquerdo da página e escolha **Databases** > **Document Database Service**.

**Passo 4** Na página **Instances**, clique em **Comprar instância de BD**. A página **Quick Config** é exibida por padrão.

**Passo 5** Selecione um modo de cobrança. Especifique os detalhes da instância e clique em **Próximo**.

**Figura 4-1** Configuração básica

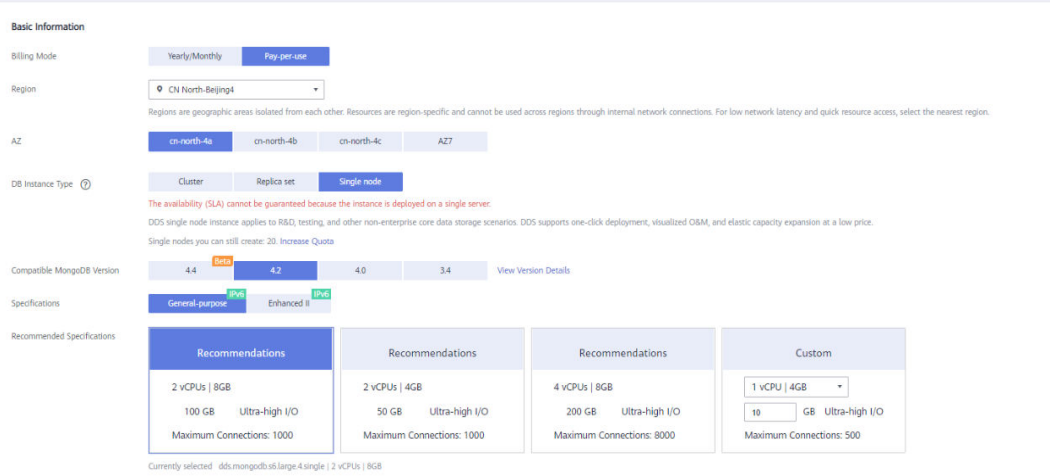



**Tabela 4-1** Modo de cobrança

| Parâmetro | Descrição |
| --- | --- |
| Billing Mode | Selecione um modo de cobrança, **Yearly/Monthly** ou **Pay-per-use**.<br>● **Yearly/Monthly**<br>– Especifique a **Required Duration** e o sistema deduz as taxas incorridas da sua conta com base no preço do serviço.<br>– Se você não espera continuar usando a instância muito depois que ela expirar, altere o modo de cobrança de anual/mensal para pagamento por uso. Para obter detalhes, consulte **Alteração do modo de cobrança de anual/mensal para pagamento por uso**.<br>**NOTA**<br>As instâncias cobradas anualmente/mensalmente não podem ser excluídas. Elas só podem ser canceladas. Para obter detalhes, consulte **Cancelamento da assinatura de uma instância anual/mensal**.<br>● **Pay-per-use**<br>– Você é cobrado pelo uso com base em quanto tempo o serviço está em uso.<br>– Se você espera usar o serviço extensivamente durante um longo período de tempo, você pode alterar seu modo de cobrança de pagamento por uso para anual/mensal para reduzir os custos. Para obter detalhes, consulte **Alteração do modo de cobrança de pagamento por uso para anual/mensal**.. |
| Region | A região onde o recurso está localizado.<br>**NOTA**<br>As instâncias implementadas em diferentes regiões não podem se comunicar entre si por meio de uma rede privada, e você não pode alterar a região de uma instância depois que ela for comprada. Tenha cuidado ao selecionar uma região. |
| AZ | Uma AZ é uma parte de uma região com sua própria fonte de alimentação e rede independentes. As AZs são fisicamente isoladas, mas podem se comunicar através de conexões de rede internas. |

| Parâmetro | Descrição |
| --- | --- |
| DB Instance Type | Selecione **Single Node**.<br>A arquitetura de nó único é outra opção para você, ajudando você a reduzir custos e, ao mesmo tempo, garantir a confiabilidade dos dados. |
| Compatible MongoDB Version | ● 4.2<br>● 4.0<br>● 3.4 |
| CPU Type | O DDS suporta arquiteturas de CPU x86 e Kunpeng.<br>● x86<br>As CPUs x86 usam o conjunto de instruções CISC (Complex Instruction Set Computing). Cada instrução pode ser usada para executar operações de hardware de baixo nível. As instruções CISC variam em comprimento e tendem a ser complicadas e lentas em comparação com RISC (Reductiond Instruction Set Computing).<br>● Kunpeng<br>A arquitetura de CPU Kunpeng usa RISC. O conjunto de instruções RISC é menor e mais rápido que CISC, graças à arquitetura simplificada. CPUs Kunpeng também oferecem um melhor equilíbrio entre energia e desempenho do que x86.<br>As CPUs Kunpeng oferecem uma opção de alta densidade e baixo consumo de energia que é mais econômica para cargas de trabalho pesadas. |
| Especificações | Com uma arquitetura x86, você tem as seguintes opções:<br>● Uso geral (s6): as instâncias S6 são adequadas para aplicações que exigem desempenho moderado em geral, mas explosões ocasionais de alto desempenho, como servidores Web de carga leve, ambientes corporativos de P&D e testes e bancos de dados de baixo e médio desempenho.<br>● Aprimorada II (c6): as instâncias C6 têm várias tecnologias otimizadas para fornecer desempenho computacional robusto e estável. NICs inteligentes de alta velocidade de 25 GE são usadas para fornecer largura de banda e taxa de transferência ultra-altas, o que as torna uma excelente opção para cenários de carga pesada. É adequada para sites, aplicações Web, bancos de dados gerais e servidores de cache que têm requisitos de desempenho mais altos para recursos de computação e rede; e aplicações corporativas de carga média e pesada. |
| Recommended Specifications | Atualmente, são fornecidas especificações recomendadas e personalizadas. |

**Figura 4-2** Rede, duração necessária e quantidade

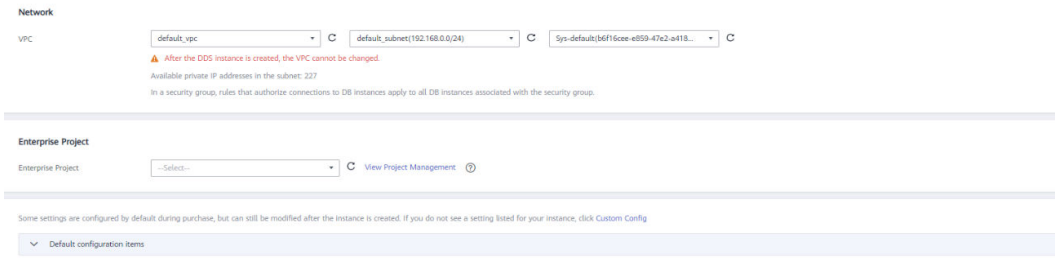



**Tabela 4-2** Configurações da rede

| Parâmetro | Descrição |
| --- | --- |
| VPC | A VPC onde suas instâncias de BD estão localizadas. Uma VPC isola redes para diferentes serviços. Ela permite que você gerencie e configure facilmente redes privadas e altere as configurações de rede.<br>Você precisará criar ou selecionar a VPC necessária. Para obter detalhes, consulte **Criação de uma VPC** no *Guia de usuário da Virtual Private Cloud*. Para obter detalhes sobre as restrições sobre o uso de VPCs, consulte **Métodos de conexão**.<br>Se não houver VPCs disponíveis, o DDS criará uma para você por padrão. |
| Enterprise Project | Somente usuários empresariais podem usar essa função. Para usar essa função, entre em contato com o atendimento ao cliente.<br>Um projeto empresarial é um modo de gerenciamento de recursos em nuvem, no qual os recursos e os membros da nuvem são gerenciados centralmente pelo projeto.<br>Selecione um projeto empresarial na lista suspensa. O projeto padrão é **default**.<br>Para personalizar um projeto empresarial, clique em **Enterprise** no canto superior direito do console. A página **Enterprise Management** é exibida. Para obter detalhes, consulte **Criação de um projeto empresarial** no *Guia de usuário do Enterprise Management*. |

**Tabela 4-3** Duração solicitada e quantidade

| Parâmetro | Descrição |
| --- | --- |
| Required Duration | O sistema calculará automaticamente a taxa com base no período de validade selecionado. |
| Auto-renew | ● Por padrão, essa opção não está selecionada.<br>● Se você selecionar essa opção, o ciclo de renovação automática será determinado pela duração da assinatura. |

| Parâmetro | Descrição |
| --- | --- |
| Quantity | A quantidade de compra depende da cota de instância de nó único. Se sua cota atual não permitir que você compre o número necessário de instâncias, você poderá solicitar uma cota aumentada. As instâncias anuais/mensais que foram compradas em lotes têm as mesmas especificações, exceto o nome e o ID da instância. |

**Tabela 4-4** Itens de configuração padrão

| Especificações | Valor | Editável após a criação da instância |
| --- | --- | --- |
| Nome da instância de BD | dds-d168 | Sim |
| Tipo de CPU | x86 | Não |
| Mecanismo de armazenamento | WiredTiger | Não |
| Configurações de senha | Não configurado | Sim |
| SSL | Desabilitado | Sim |
| Porta do banco de dados | 8635 | Sim |
| Modelo de parâmetro de nó único | Default-DDS-4.0-Single | Sim |
| Tags | Não configurado | Sim |
| Configurações avançadas | Não configurado | Sim |

NOTA

- Algumas configurações são configuradas por padrão durante a compra, mas ainda podem ser modificadas após a criação da instância. Se você não vir uma configuração listada para sua instância, clique em **Configuração personalizada**.
- O desempenho da instância depende das especificações selecionadas durante a criação. Os itens de configuração de hardware que podem ser selecionados incluem a classe de nó e o espaço de armazenamento.

**Passo 6** Na página exibida, confirme os detalhes da instância.

- **Yearly/Monthly**
  - Se você precisar modificar as especificações, clique em **Previous** para retornar à página anterior.

  - Se você não precisar modificar as especificações, leia e concorde com o contrato de serviço e clique em **Pay Now** para ir para a página de pagamento e concluir o pagamento.
- **Pay-per-use**
  - Se você precisar modificar as especificações, clique em **Previous** para retornar à página anterior.
  - Se você não precisar modificar as especificações, leia e concorde com o contrato de serviço e clique em **Submit** para começar a criar a instância.

**Passo 7** Depois que uma instância do DDS for criada, você poderá exibi-la e gerenciá-la na página **Instances**.

- Quando uma instância está sendo criada, o status exibido na coluna **Status** é **Creating**. Este processo leva cerca de 15 minutos. Após a conclusão da criação, o status muda para **Available**.
- O DDS ativa a política de backup automatizado por padrão. Depois que uma instância é criada, você pode modificar ou desativar a política de backup automatizado. Um backup completo automatizado é acionado imediatamente após a criação de uma instância.
- As instâncias anuais/mensais que foram compradas em lotes têm as mesmas especificações, exceto o nome e o ID da instância.

**----Fim**

## 4.1.2 Configuração personalizada

Esta seção descreve como comprar uma instância de nó único no modo personalizado no console de gerenciamento. Você pode personalizar os recursos de computação e o espaço de armazenamento de uma instância de nó único com base em seus requisitos de serviço. Além disso, você pode definir configurações avançadas, como log de consultas lentas e backup automatizado.

### Precauções

Cada conta pode criar até 20 instâncias de nó único.

### Pré-requisitos

- Você registrou uma conta da Huawei Cloud.

### Procedimento

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

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

Se você quiser recursos de computação e rede dedicados ao seu uso exclusivo, **ative uma DeC** e **solicite recursos do DCC**. Depois de ativar uma DeC, você pode selecionar a região da DeC e o projeto.

**Passo 3** Clique em no canto superior esquerdo da página e escolha **Databases** > **Document Database Service**.

**Passo 4** Na página **Instances**, clique em **Comprar instância de BD**.

**Passo 5** Clique na guia **Custom Config**.

**Passo 6** Selecione um modo de cobrança. Especifique os detalhes da instância e clique em **Próximo**.

**Figura 4-3** Configuração básica

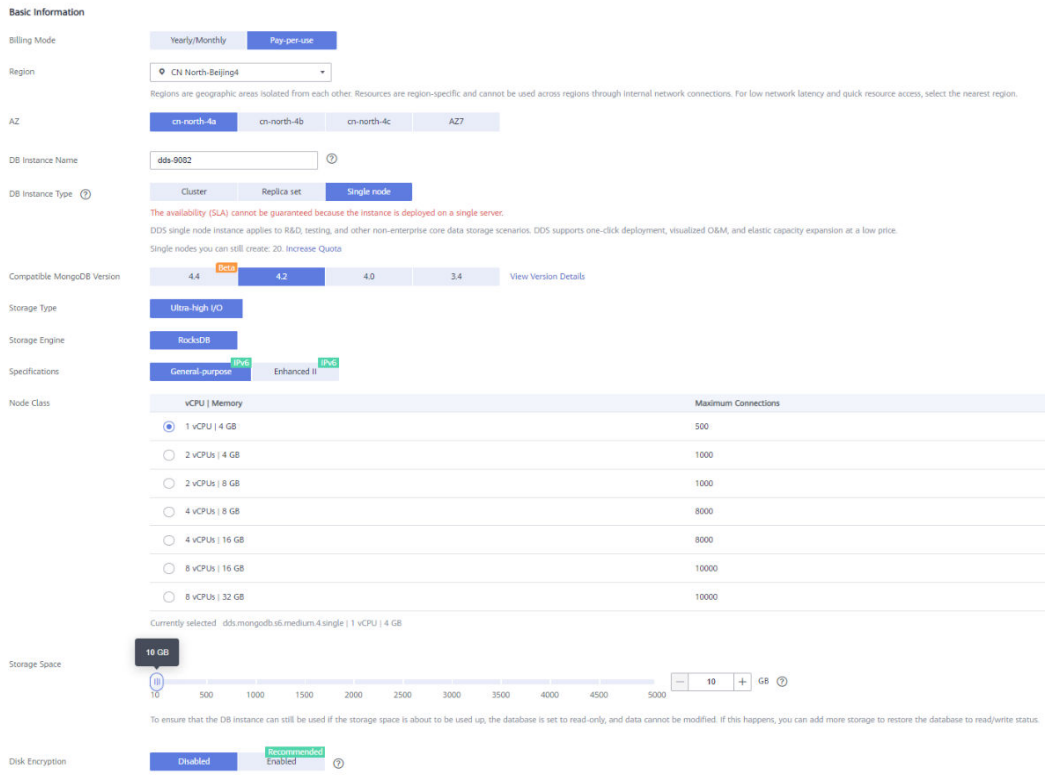


**Tabela 4-5** Modo de cobrança

| Parâmetro | Descrição |
| --- | --- |
| Billing Mode | Selecione um modo de cobrança, **Yearly/Monthly** ou **Pay-per-use**.<br>● **Yearly/Monthly**<br>– Especifique a **Required Duration** e o sistema deduz as taxas incorridas da sua conta com base no preço do serviço.<br>– Se você não espera continuar usando a instância muito depois que ela expirar, altere o modo de cobrança de anual/mensal para pagamento por uso. Para obter detalhes, consulte **Alteração do modo de cobrança de anual/mensal para pagamento por uso**..<br>**NOTA**<br>As instâncias cobradas anualmente/mensalmente não podem ser excluídas. Elas só podem ser canceladas. Para obter detalhes, consulte **Cancelamento da assinatura de uma instancia anual/mensal**.<br>● **Pay-per-use**<br>– Você é cobrado pelo uso com base em quanto tempo o serviço está em uso.<br>– Se você espera usar o serviço extensivamente durante um longo período de tempo, você pode alterar seu modo de cobrança de pagamento por uso para anual/mensal para reduzir os custos. Para obter detalhes, consulte **Alteração do modo de cobrança de pagamento por uso para anual/mensal**. |
| Region | A região onde o recurso está localizado.<br>**NOTA**<br>As instâncias implementadas em diferentes regiões não podem se comunicar entre si por meio de uma rede privada, e você não pode alterar a região de uma instância depois que ela for comprada. Tenha cuidado ao selecionar uma região. |
| AZ | Uma AZ é uma parte de uma região com sua própria fonte de alimentação e rede independentes. As AZs são fisicamente isoladas, mas podem se comunicar através de conexões de rede interna. |

| Parâmetro | Descrição |
| --- | --- |
| DB Instance Name | ● O nome da instância pode ser igual a um nome de instância existente.<br>● O nome da instância que você especificar após a compra. O nome da ocorrência deve conter de 4 a 64 caracteres e deve começar com uma letra. Ele diferencia maiúsculas de minúsculas e minúsculas e pode conter letras, dígitos, hifens (-) e sublinhados (_). Não pode conter outros caracteres especiais.<br>● Se você comprar um lote de instâncias de uma só vez, um sufixo numérico de 4 dígitos será adicionado aos nomes das instâncias, começando com **-0001**. Se mais tarde você fizer outra compra em lote, os novos nomes de instância serão numerados primeiro usando quaisquer sufixos ausentes da sequência de suas instâncias existentes e, em seguida, continuando a partir de onde sua última compra em lote parou. Por exemplo, um lote de 3 instâncias obtém os sufixos **-0001**, **-0002** e **-0003**. Se você excluir a instância **0002** e depois comprar mais 3 instâncias, as novas instâncias receberão os sufixos **-0002**, **-0004** e **-0005**.<br>● Depois que a instância de BD for criada, você poderá alterar seu nome. Para mais detalhes, consulte **Alteração de um nome de instância**. |
| DB Instance Type | Selecione **Single Node**.<br>A arquitetura de nó único é outra opção para você, ajudando você a reduzir custos e, ao mesmo tempo, garantir a confiabilidade dos dados. |
| Compatible MongoDB Version | ● 4.2<br>● 4.0<br>● 3.4 |
| CPU Type | O DDS suporta arquiteturas de CPU x86 e Kunpeng.<br>● x86<br>As CPUs x86 usam o conjunto de instruções CISC (Complex Instruction Set Computing). Cada instrução pode ser usada para executar operações de hardware de baixo nível. As instruções CISC variam em comprimento e tendem a ser complicadas e lentas em comparação com RISC (Reductiond Instruction Set Computing).<br>● Kunpeng<br>A arquitetura de CPU Kunpeng usa RISC. O conjunto de instruções RISC é menor e mais rápido que CISC, graças à arquitetura simplificada. CPUs Kunpeng também oferecem um melhor equilíbrio entre energia e desempenho do que x86.<br>As CPUs Kunpeng oferecem uma opção de alta densidade e baixo consumo de energia que é mais econômica para cargas de trabalho pesadas. |
| Storage Type | O tipo de armazenamento padrão é I/O ultra-alta. |

| Parâmetro | Descrição |
| --- | --- |
| Storage Engine | ● WiredTiger<br>O WiredTiger é o mecanismo de armazenamento padrão do DDS 3.4 e 4.0. O WiredTiger fornece controle de simultaneidade de granularidade diferente e mecanismo de compactação para gerenciamento de dados. Ele pode fornecer o melhor desempenho e eficiência de armazenamento para diferentes tipos de aplicações.<br>● RocksDB<br>RocksDB é o mecanismo de armazenamento padrão do DDS 4.2. O RocksDB suporta pesquisa de pontos eficiente, varredura de alcance e gravação de alta velocidade. O RocksDB pode ser usado como o mecanismo de armazenamento de dados subjacente do MongoDB e é adequado para cenários com um grande número de operações de gravação. |
| Specifications | Com uma arquitetura x86, você tem as seguintes opções:<br>● Uso geral (s6): as instâncias S6 são adequadas para aplicações que exigem desempenho moderado em geral, mas explosões ocasionais de alto desempenho, como servidores da Web de carga leve, ambientes corporativos de P&D e testes e bancos de dados de baixo e médio desempenho.<br>● Aprimorada II (c6): as instâncias C6 têm várias tecnologias otimizadas para fornecer desempenho computacional robusto e estável. NICs inteligentes de alta velocidade de 25 GE são usadas para fornecer largura de banda e taxa de transferência ultra-altas, o que as torna uma excelente opção para cenários de carga pesada. É adequada para sites, aplicações Web, bancos de dados gerais e servidores de cache que têm requisitos de desempenho mais altos para recursos de computação e rede; e aplicações corporativos de carga média e pesada. |
| Node Class | Para obter detalhes sobre as especificações da instância, consulte **Especificações da instância**. |
| Storage Space | Intervalo de valores: 10 GB a 1.000 GB (deve ser um múltiplo de 10)<br>Você pode expandir uma instância depois que ela é criada. Para obter detalhes, consulte **Expansão de uma instância de nó único**.<br>**NOTA**<br>● Se o espaço de armazenamento comprado exceder 600 GB e o espaço de armazenamento restante for 18 GB, a instância se tornará **Read-only**.<br>● Se o espaço de armazenamento comprado for inferior a 600 GB e o uso do espaço de armazenamento atingir 97%, a instância se tornará **Read-only**.<br>Nesses casos, exclua recursos desnecessários ou expanda a capacidade. |

| Parâmetro | Descrição |
| --- | --- |
| Criptografia de disco | ● **Disabled**: desativar a criptografia.<br>● **Enabled**: ativar a criptografia. Esse recurso melhora a segurança dos dados, mas afeta um pouco o desempenho de leitura/gravação. **Key Name**: selecione ou crie uma chave privada, que é a chave do locatário.<br>**NOTA**<br>● Depois que uma instância é criada, o status de criptografia de disco e a chave não podem ser alterados. Os dados de backup armazenados no OBS não são criptografados.<br>● A chave não pode ser desativada, excluída ou congelada ao ser usada. Caso contrário, o banco de dados ficará indisponível.<br>● For details about how to create a key, see "Creating a CMK" in *Data Encryption Workshop User Guide*. |

**Figura 4-4** Configurações do administrador

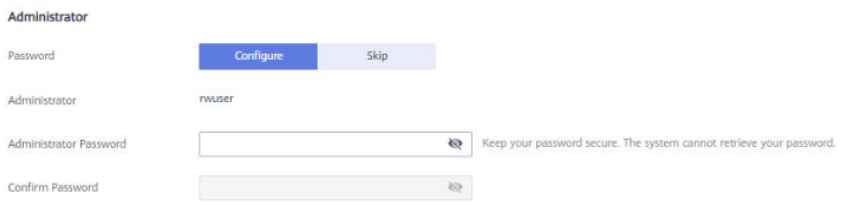



**Tabela 4-6** Configurações do administrador

| Parâmetro | Descrição |
| --- | --- |
| Password | ● Configure<br>Digite e confirme a nova senha de administrador. Depois que uma instância é criada, você pode se conectar à instância usando a senha.<br>● Skip<br>Para fazer logon, você terá que redefinir a senha mais tarde na página **Basic Information**. Se você precisar se conectar a uma instância depois que ela for criada, localize a instância e clique em **Reset Password** na coluna **Operation** para definir uma senha para a instância primeiro. |
| Administrator | A conta padrão é **rwuser**. |
| Administrator Password | Defina uma senha para o administrador. A senha deve ter de 8 a 32 caracteres e conter letras maiúsculas, minúsculas, dígitos e pelo menos um dos seguintes caracteres especiais: ~!@#%^*-_=+?<br>Mantenha esta senha segura. Se for perdida, o sistema não poderá recuperá-la para você. |
| Confirm Password | Digite a senha do administrador novamente. |

**Figura 4-5** Rede, duração necessária e quantidade

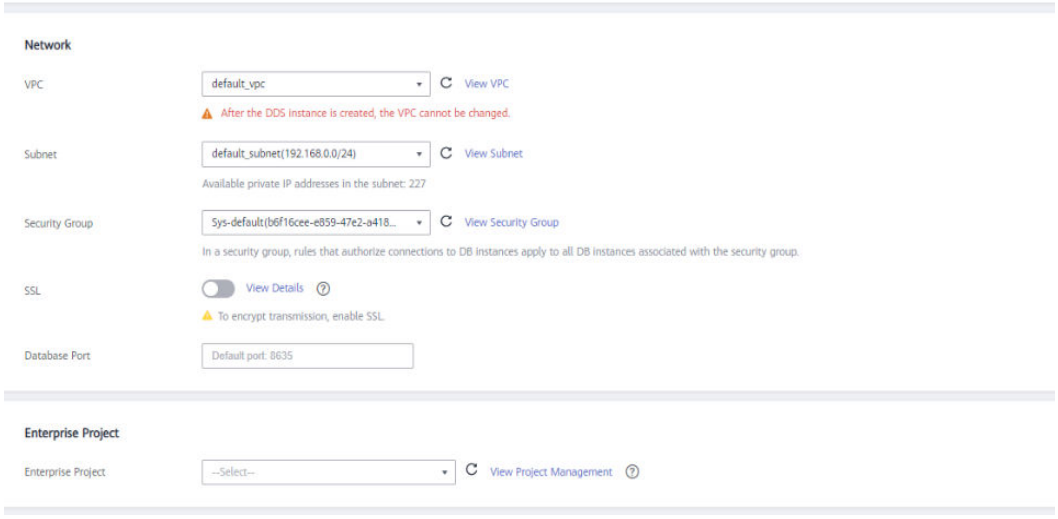



**Tabela 4-7** Rede

| Parâmetro | Descrição |
| --- | --- |
| VPC | A VPC onde suas instâncias de BD estão localizadas. Uma VPC isola redes para diferentes serviços. Ela permite que você gerencie e configure facilmente redes privadas e altere as configurações de rede.<br>Você precisará criar ou selecionar a VPC necessária. Para obter detalhes sobre como criar uma VPC, consulte "Criação de uma VPC" no *Guia de usuário da Virtual Private Cloud*. Para obter detalhes sobre as restrições sobre o uso de VPCs, consulte **Métodos de conexão**.<br>Se não houver VPCs disponíveis, o DDS criará uma para você por padrão. |
| Sub-rede | Uma sub-rede fornece recursos de rede dedicados que são logicamente isolados de outras redes por razões de segurança.<br>Depois que a instância é criada, você pode alterar o endereço IP privado atribuído pela sub-rede. Para obter detalhes, consulte **Alteração um endereço IP privado**.<br>**NOTA**<br>As sub-redes IPv6 não são suportadas. Recomendamos que você crie e selecione sub-redes IPv4. |
| Grupo de segurança | Um grupo de segurança controla o acesso entre o DDS e outros serviços.<br>Se não houver grupos de segurança disponíveis, o DDS criará um para você por padrão.<br>**NOTA**<br>Certifique-se de que haja uma regra de grupo de segurança configurada que permita que os clientes acessem instâncias. Por exemplo, selecione uma regra TCP de entrada com a porta padrão 8635 e insira um endereço IP de sub-rede ou selecione um grupo de segurança ao qual a instância pertence. |

| Parâmetro | Descrição |
| --- | --- |
| SSL | A Camada de soquete seguro (SSL) criptografa as conexões entre clientes e servidores, impedindo que os dados sejam adulterados ou roubados durante a transmissão.<br>Você pode ativar SSL para melhorar a segurança dos dados. Depois que uma instância é criada, você pode se conectar a ela usando SSL. |
| Porta do banco de dados | A porta do DDS padrão é 8635, mas esta porta pode ser modificada se necessário. Se você alterar a porta, adicione uma regra de grupo de segurança correspondente para permitir o acesso à instância. |
| Projeto empresarial | Somente usuários empresariais podem usar essa função. Para usar essa função, entre em contato com o atendimento ao cliente.<br>Um projeto empresarial é um modo de gerenciamento de recursos em nuvem, no qual os recursos e os membros da nuvem são gerenciados centralmente pelo projeto.<br>Selecione um projeto da empresa na lista suspensa. O projeto padrão é **default**. |

**Figura 4-6** Configurações avançadas

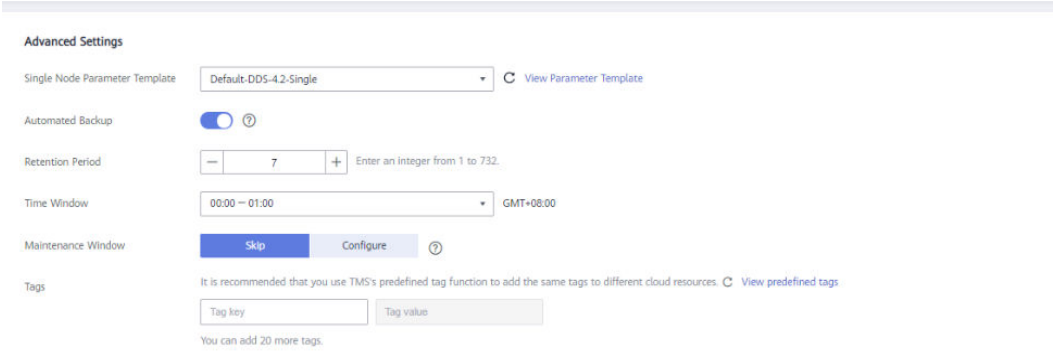
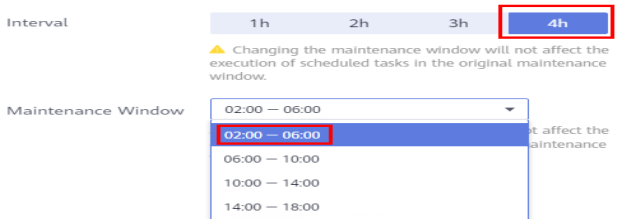



**Tabela 4-8** Configurações avançadas

| Parâmetro | Descrição |
| --- | --- |
| Single Node Parameter Template | Os parâmetros que se aplicam a instâncias de nó único. Depois que uma instância é criada, você pode alterar o modelo de parâmetro configurado para a instância para obter o melhor desempenho.<br>Para obter detalhes, consulte **Editação de um modelo de parâmetro**. |
| Automated Backup | O DDS ativa uma política de backup automatizado por padrão, mas você pode desativá-la após a criação de uma instância. Um backup completo automatizado é acionado imediatamente após a criação de uma instância.<br>Para obter detalhes, consulte **Configuração de uma política de backup automatizado**. |

| Parâmetro | Descrição |
| --- | --- |
| Retention Period (days) | **Retention Period** refere-se ao número de dias que os dados são mantidos. Você pode aumentar o período de retenção para melhorar a confiabilidade dos dados.<br>O período de retenção do backup é de 1 a 732 dias. |
| Time Window | O intervalo de backup é de 1 hora. |
| Maintenance Window | Um período de manutenção refere-se ao período durante o qual um usuário tem permissão para iniciar uma tarefa que afeta a execução de uma instância de banco de dados, por exemplo, uma atualização do sistema operacional ou atualização do software do banco de dados.<br>● Skip<br>A janela de manutenção é 02:00–06:00 por padrão e você pode alterá-la conforme necessário. Para obter detalhes, consulte **Configuração da janela de manutenção**.<br>● Configure<br>É aconselhável definir o período de manutenção para fora do horário de pico para evitar a interrupção do serviço durante a manutenção. Você pode alterar a janela de manutenção após a criação de uma instância. Para obter detalhes, consulte **Configuração da janela de manutenção**.<br>**Figura 4-7** Configurar janelas de manutenção<br>  |

| Parâmetro | Descrição |
| --- | --- |
| Tags | (Opcional) Você pode adicionar tags a instâncias do DDS para que possa pesquisar rapidamente e filtrar instâncias especificadas por tag. Cada instância do DDS pode ter até 20 tags.<br>● Criar uma tag.<br>Você pode criar tags no console do DDS e configurar a **chave** e o **valor** da tag.<br>Key: este parâmetro é obrigatório.<br>– Cada chave de tag deve ser exclusiva para cada instância.<br>– Uma chave de tag consiste em até 36 caracteres.<br>– A chave só pode consistir em dígitos, letras, sublinhados (_) e hifens (-).<br>Value: este parâmetro é opcional.<br>– O valor consiste em até 43 caracteres.<br>– O valor deve consistir apenas em dígitos, letras, sublinhados (_), pontos (.) e hifens (-).<br>● Adicionar uma tag predefinida.<br>Tags predefinidas podem ser usadas para identificar vários recursos de nuvem.<br>Para marcar um recurso de nuvem, você pode selecionar uma tag predefinida criada na lista suspensa, sem inserir uma chave e um valor para a tag.<br>Por exemplo, se uma tag predefinida tiver sido criada, sua chave será Usage e o valor será Project1. Quando você configura a chave e o valor para um recurso de nuvem, a tag predefinida criada será exibida na página.<br>Depois que uma instância é criada, você pode clicar no nome da instância para exibir suas tags. Na página **Tags**, você também pode **modificar ou excluir as tags**. Além disso, você pode **pesquisar e filtrar rapidamente instâncias especificadas por tag**.<br>Você pode adicionar uma tag a uma instância depois que ela for criada. Para obter detalhes, consulte **Adição de uma tag**. |

Se você tiver alguma dúvida sobre o preço, clique em **Price Details**.

NOTA

O desempenho da instância depende das especificações selecionadas durante a criação. Os itens de configuração de hardware que podem ser selecionados incluem a classe de nó e o espaço de armazenamento.

**Passo 7** Na página exibida, confirme os detalhes da instância.

- **Yearly/Monthly**
  - Se você precisar modificar as especificações, clique em **Previous** para retornar à página anterior.

  - Se você não precisar modificar as especificações, leia e concorde com o contrato de serviço e clique em **Pay Now** para ir para a página de pagamento e concluir o pagamento.
- **Pay-per-use**
  - Se você precisar modificar as especificações, clique em **Previous** para retornar à página anterior.
  - Se você não precisar modificar as especificações, leia e concorde com o contrato de serviço e clique em **Submit** para começar a criar a instância.

**Passo 8** Depois que uma instância do DDS for criada, você poderá exibi-la e gerenciá-la na página **Instances**.

- Quando uma instância está sendo criada, o status exibido na coluna **Status** é **Creating**. Este processo leva cerca de 15 minutos. Após a conclusão da criação, o status muda para **Available**.
- As instâncias anuais/mensais que foram compradas em lotes têm as mesmas especificações, exceto o nome e o ID da instância.

**----Fim**

# 4.2 Conexão a uma instância de nó único

## 4.2.1 Métodos de conexão

Você pode acessar o DDS em redes privadas ou públicas.

**Tabela 4-9** Métodos de conexão

| Método | Endereço IP | Cenário | Descrição |
| --- | --- | --- | --- |
| DAS | Não necessário | O DAS fornece uma GUI e permite que você execute operações visualizadas no console. Execução SQL, gerenciamento avançado de banco de dados e O&M inteligente estão disponíveis para tornar o gerenciamento de banco de dados simples, seguro e inteligente. | ● Fácil de usar, seguro, avançado e inteligente<br>● Recomendado |
| Rede privada | Endereço IP privado | O DDS fornece um endereço IP privado por padrão.<br>Se suas aplicações estiverem sendo executadas em um ECS na mesma região, AZ e sub-rede da VPC que sua instância do DDS, recomendamos que você use um endereço IP privado para conectar o ECS às instâncias do DDS. | Seguro e desempenho excelente |

| Método | Endereço IP | Cenário | Descrição |
| --- | --- | --- | --- |
| **Rede pública** | EIP | • Se suas aplicações estiverem sendo executadas em um ECS que esteja em uma região diferente daquela em que a instância de BD está localizada, use um EIP para conectar o ECS às instâncias de BD do DDS.<br>• Se suas aplicações forem implementadas em outra plataforma de nuvem, o EIP é recomendado. | • Baixa segurança<br>• Para uma transmissão mais rápida e segurança aprimorada, é recomendável migrar suas aplicações para um ECS que esteja na mesma sub-rede da instância do DDS e usar um endereço IP privado para acessar a instância. |

# 4.2.2 (Recomendada) Conexão a uma instância de nó único por meio do DAS

## 4.2.2.1 Visão geral

O DAS fornece uma GUI e permite que você execute operações visualizadas no console. Execução SQL, gerenciamento avançado de banco de dados e O&M inteligente estão disponíveis para tornar o gerenciamento de banco de dados simples, seguro e inteligente. Recomendamos que você use o DAS para se conectar a instâncias de BD.

Esta seção descreve como comprar uma instância de nó único no console de gerenciamento e como se conectar à instância de nó único por meio do DAS.

## Processo

Para comprar e se conectar a uma instância de nó único, execute as seguintes etapas:

1. **Compre uma única instância de nó.**
2. **Conecte-se a uma instância de nó único por meio do DAS.**

## 4.2.2.2 Conexão a uma instância de nó único por meio do DAS.

Data Admin Service (DAS) permite que você gerencie instâncias de BD em um console baseado na Web, simplificando o gerenciamento de banco de dados e melhorando a eficiência do trabalho. Você pode se conectar e gerenciar instâncias por meio do DAS. Por padrão, você tem a permissão necessária para o logon remoto. Recomenda-se que você use o serviço DAS para se conectar a instâncias. O DAS é seguro e conveniente.

## Procedimento

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

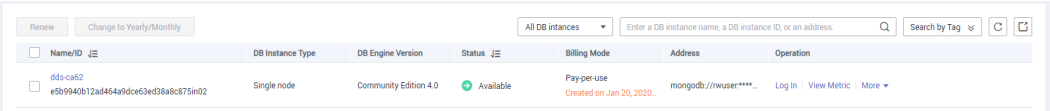
**Passo 2** Clique em no canto superior esquerdo e selecione uma região e um projeto.

**Passo 3** Clique em no canto superior esquerdo da página e escolha **Databases** > **Document Database Service**.

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

Como alternativa, clique na instância de BD de destino na página **Instances**. Na página **Basic Information** exibida, clique em **Log In** no canto superior direito da página.

**Figura 4-8** Gerenciamento de instâncias




**Passo 5** Na página de logon exibida, insira o nome de usuário e a senha do administrador e clique em **Login**.

Para obter detalhes sobre como gerenciar bancos de dados por meio do DAS, consulte **Gerenciamento de instância do DDS**.

**----Fim**

# 4.2.3 Conexão a uma instância de nó único em uma rede privada

## 4.2.3.1 Configuração de um grupo de segurança

Um grupo de segurança é um grupo lógico. Ele fornece políticas de controle de acesso para ECSs e instâncias que têm os mesmos requisitos de proteção de segurança e são mutuamente confiáveis em uma VPC.

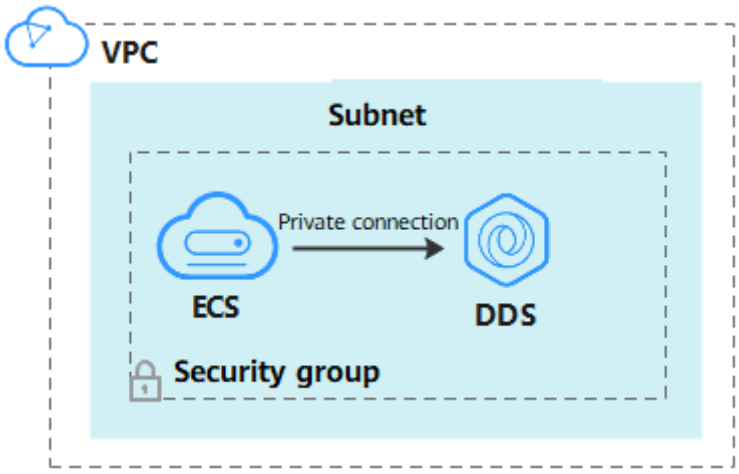
Para garantir a segurança e a confiabilidade do banco de dados, é necessário configurar regras de grupo de segurança para permitir que endereços IP e portas específicos acessem instâncias do DDS.

Você pode se conectar a uma instância configurando regras de grupo de segurança de duas maneiras:

- Se o ECS e a instância de BD estiverem no mesmo grupo de segurança, eles poderão se comunicar entre si por padrão. Nenhuma regra de grupo de segurança precisa ser configurada. Vá para **Conexão a uma instância de nó único usando Mongo Shell (rede privada)**.

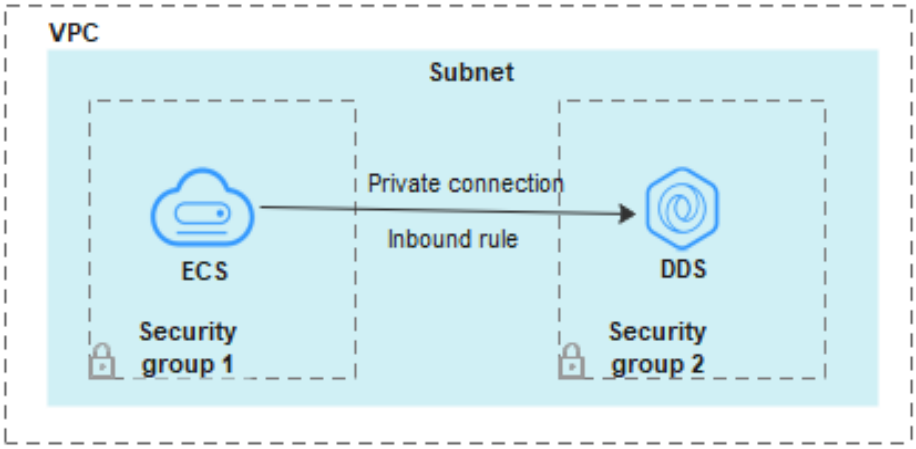
  

**Figura 4-9** Mesmo grupo de segurança




- Se o ECS e a instância estiverem em grupos de segurança diferentes, será necessário configurar as regras de grupo de segurança para eles separadamente.

**Figura 4-10** Diferentes grupos de segurança




  - Instância: configure uma **inbound rule** para o grupo de segurança associado à instância.
  - 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 puder chegar à instância, configure uma regra **de saída** para o ECS.

Esta seção descreve como configurar uma regra de entrada para uma instância.

## Precauções

- Por predefinição, uma conta pode criar até 500 regras de grupo de segurança.
- Muitas regras de grupo de segurança aumentarão a latência do primeiro pacote, portanto, recomenda-se um máximo de 50 regras para cada grupo de segurança.
- Uma instância do DDS só pode ser associada a um grupo de segurança.

## 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 e escolha **Databases** > **Document Database Service**.

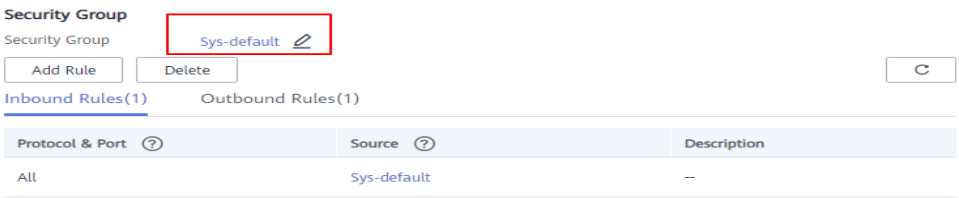
**Passo 4** Na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida.

**Passo 5** Na área **Network Information** da página **Basic Information**, clique no grupo de segurança.

**Figura 4-11** Grupo de segurança


Você também pode escolher **Connections** no painel de navegação à esquerda. Na guia **Private Connection**, na área **Security Group**, clique no nome do grupo de segurança.

**Figura 4-12** Grupo de segurança




**Passo 6** Na página **Security Group**, localize o grupo de segurança de destino e clique em **Manage Rule** na coluna **Operation**.

**Passo 7** Na guia **Inbound Rules**, clique em **Add Rule**. A caixa de diálogo **Add Inbound Rule** é exibida.

**Passo 8** Adicione uma regra de grupo de segurança conforme solicitado.

**Figura 4-13** Adicionar regra de entrada

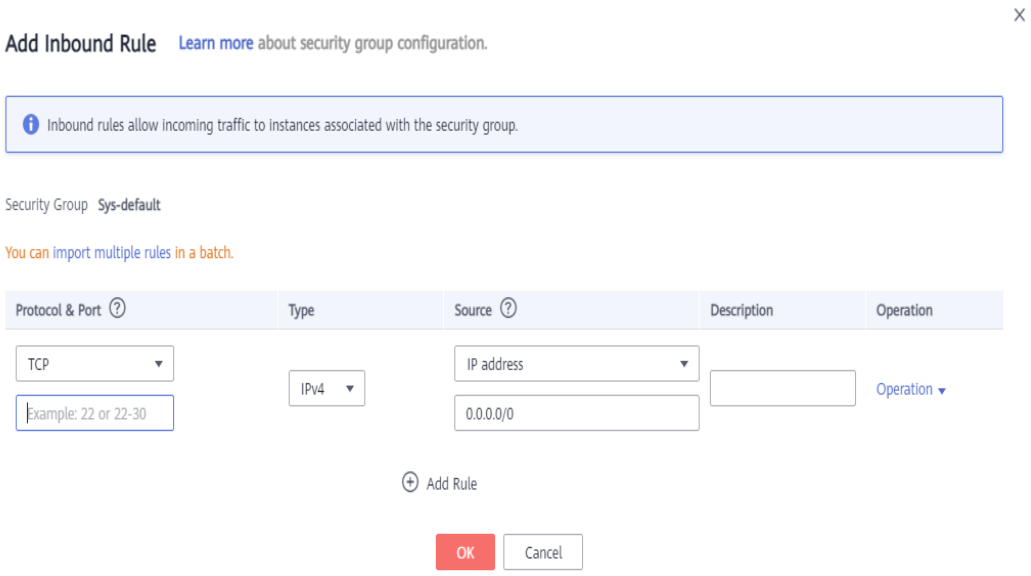



**Tabela 4-10** Configurações da regra de entrada

| Parâmetro | Descrição | Exemplo |
| --- | --- | --- |
| Priority | A prioridade da regra do grupo de segurança.<br>O valor de prioridade varia de 1 a 100. A prioridade padrão é 1 e tem a prioridade mais alta. A regra de grupo de segurança com um valor menor tem uma prioridade mais alta. | 1 |
| Action | As ações de regra do grupo de segurança.<br>Uma regra com uma ação de negação substitui outra com uma ação de permitir se as duas regras tiverem a mesma prioridade. | Allow |
| Protocol & Port | O protocolo de rede necessário para o acesso. Opções disponíveis: **TCP**, **UDP**, **ICMP** ou **GRE** | TCP |
| | Porta: a porta na qual você deseja permitir o acesso ao DDS. A porta padrão é 8635. A porta varia de 2100 a 9500 ou pode ser 27017, 27018 ou 27019. | 8635 |
| Type | Tipo do endereço IP. Apenas **IPv4** e I**IPv6** são suportados. | IPv4 |

| Parâmetro | Descrição | Exemplo |
| --- | --- | --- |
| Source | Especifica o endereço IP, o grupo de segurança e o grupo de endereços IP suportados, que permitem o acesso de endereços IP ou instâncias em outro grupo de segurança. Exemplo:<br>● Endereço IP único: 192.168.10.10/32<br>● Segmento do endereço IP: 192.168.1.0/24<br>● Todos os endereços IP: 0.0.0.0/0<br>● Grupo de segurança: sg-abc<br>● Grupo de endereço IP: ipGroup-test<br>Se você inserir um grupo de segurança, todos os ECSs associados ao grupo de segurança estarão em conformidade com a regra criada.<br>Para obter mais informações sobre grupos de endereços IP, consulte **Grupo de endereços IP**. | 0.0.0.0/0 |
| Description | (Opcional) Fornece informações complementares sobre a regra de grupo de segurança. Este parâmetro é opcional.<br>A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >). | - |

**Passo 9** Clique em **OK**.

**----Fim**

## 4.2.3.2 Conexão a uma instância de nó único usando Mongo Shell (rede privada)

O Mongo shell é o cliente padrão para o servidor de banco de dados MongoDB. Você pode usar o Mongo Shell para se conectar a instâncias de BD e consultar, atualizar e gerenciar dados em bancos de dados. Para usar o Mongo Shell, baixe e instale o cliente de MongoDB primeiro e, em seguida, use o Mongo shell para se conectar à instância de BD.

Por padrão, uma instância do DDS fornece um endereço IP privado. Se suas aplicações forem implementadas em um ECS e estiverem na mesma região e VPC que as instâncias do DDS, você poderá se conectar a instâncias do DDS usando um endereço IP privado para obter uma taxa de transmissão rápida e alta segurança.

Esta seção descreve como usar o Mongo Shell instalado em um ECS do Linux para se conectar a uma instância de nó único em uma rede privada.

Você pode se conectar a uma instância usando uma conexão SSL ou uma conexão não criptografada. A conexão SSL é criptografada e mais segura. Para melhorar a segurança da transmissão de dados, conecte-se a instâncias usando SSL.

## Pré-requisitos

1. Para obter detalhes sobre como criar e fazer logon em um ECS, consulte **Compra de um ECS** e **Logon em um ECS**.
2. Instale o cliente de MongoDB no ECS.

   Para obter detalhes sobre como instalar um cliente de MongoDB, consulte **Como instalar um cliente de MongoDB?**
3. O ECS pode se comunicar com a instância do DDS. Para mais detalhes, consulte ECS.

## SSL

AVISO

Se você se conectar a uma instância por meio da conexão SSL, ative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como ativar SSL, consulte **Ativação e desativação de SSL**.

**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 e escolha **Databases** > **Document Database Service**.

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

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

**Passo 6** Na área **Basic Information**, clique em  ao lado do campo **SSL**.

**Passo 7** Importe o certificado raiz para o Linux ou Windows ECS. Para obter detalhes, consulte **Como importar o certificado raiz para o sistema operacional Windows ou Linux?**

**Passo 8** Conecte-se a uma instância do DDS.

Usar um endereço IP privado

Exemplo de comando:

**./mongo --host** <*DB_HOST*> **--port** <*DB_PORT*> **-u** <*DB_USER*> **-p --authenticationDatabase admin --ssl --sslCAFile**<*FILE_PATH*> **--sslAllowInvalidHostnames**

Descrição do parâmetro:

- **DB_HOST** é o endereço IP privado da instância a ser conectada.

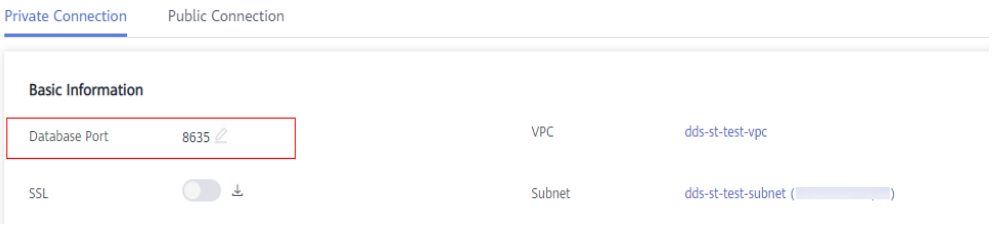
  Na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida. Escolha **Connections**. Na guia **Private Connection**, obtenha o endereço IP do nó correspondente.


- **DB_PORT** é a porta do banco de dados. O número de porta padrão é 8635.

  você pode clicar no nome da instância para ir para a página **Basic Information**. No painel de navegação à esquerda, escolha **Connections**. Na página exibida, clique na guia **Private Connection** e obtenha a porta no campo **Database Port** na área **Basic Information**.

  **Figura 4-14** Obter a porta




- **DB_USER** é o usuário do banco de dados. O valor padrão é **rwuser**.
- **FILE_PATH** é o caminho para armazenar o certificado raiz.
- **--sslAllowInvalidHostnames**: para garantir que a comunicação interna dos nós únicos não ocupe recursos como o endereço IP do usuário e a largura de banda, o certificado de nó único é gerado usando o endereço IP de gerenciamento interno. **--sslAllowInvalidHostnames** é necessário para a conexão SSL em redes privadas.

Exemplo de comando:

**./mongo --host** *192.168.xx.xx* **--port 8635 -u rwuser -p --authenticationDatabase admin --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames**

Digite a senha do banco de dados quando solicitado:

```
Enter password:
```

**Passo 9** Verifique o resultado da conexão. Se as informações a seguir forem exibidas, a conexão será bem-sucedida.

```
replica:PRIMARY>
```

**----Fim**

## Conexão não criptografada

**AVISO**

Se você se conectar a uma instância por meio de uma conexão não criptografada, desative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como desabilitar SSL, consulte **Ativação e desativação de SSL**.

**Passo 1** Efetue logon no ECS.

**Passo 2** Conecte-se a uma instância do DDS.

Usar um endereço IP privado

Exemplo de comando:

**./mongo --host**<*DB_HOST*>**--port**<*DB_PORT*>**-u**<*DB_USER*>**-p --authenticationDatabase admin**

Descrição do parâmetro:

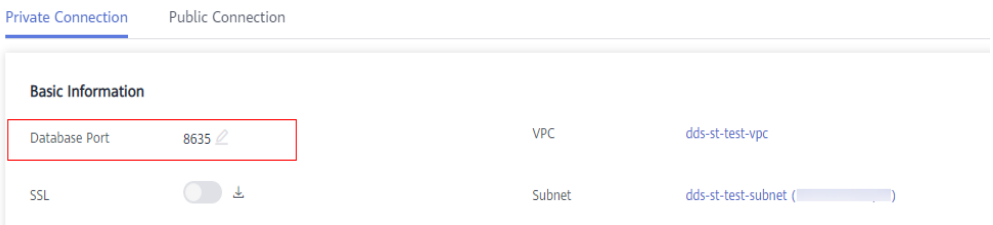
- **DB_HOST** é o endereço IP privado da instância a ser conectada.

  Na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida. Escolha **Connections**. Na guia **Private Connection**, obtenha o endereço IP do nó correspondente.


- **DB_PORT** é a porta do banco de dados. O número de porta padrão é 8635.

  você pode clicar no nome da instância para ir para a página **Basic Information**. No painel de navegação à esquerda, escolha **Connections**. Na página exibida, clique na guia **Private Connection** e obtenha a porta no campo **Database Port** na área **Basic Information**.

**Figura 4-15** Obter a porta



- **DB_USER** é o usuário do banco de dados. O valor padrão é **rwuser**.

Exemplo de comando:

**./mongo --host** *192.168.xx.xx* **--port 8635 -u rwuser -p --authenticationDatabase admin**

Digite a senha do banco de dados quando solicitado:

```
Enter password:
```

**Passo 3** Verifique o resultado da conexão. Se as informações a seguir forem exibidas, a conexão será bem-sucedida.

```
replica:PRIMARY>
```

**----Fim**

# 4.2.4 Conexão a uma instância de nó único em uma rede pública

## 4.2.4.1 Vinculação ou desvinculação de um EIP

Depois de criar uma instância, você pode vincular um EIP a ela para permitir acesso externo. Se mais tarde você quiser proibir o acesso externo, você também pode desvincular o EIP da instância.

## Precauções

- A exclusão de um EIP vinculado não significa que o EIP não esteja vinculado.
- Antes de acessar um banco de dados, solicite um EIP no console da VPC. Em seguida, adicione uma regra de entrada para permitir os endereços IP ou intervalos de endereços IP de ECSs. Para mais detalhes, consulte **Configuração de um grupo de segurança**.
- Para alterar o EIP que foi vinculado a um nó, desvincule-o do nó primeiro.

## Vincular um EIP

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

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

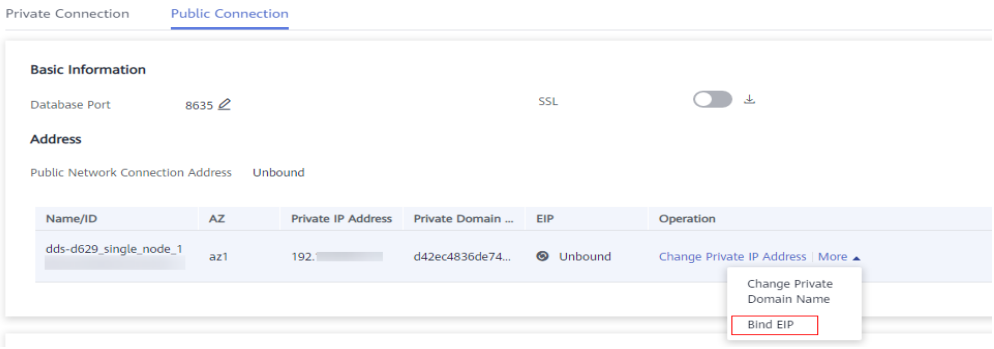
**Passo 3** Clique em  no canto superior esquerdo da página e escolha **Databases** > **Document Database Service**.

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

**Passo 5** No painel de navegação à esquerda, escolha **Connections**. Clique na guia **Public Connection**. Na área **Basic Information**, localize o nó ao qual deseja vincular um EIP e clique em **Bind EIP** na coluna **Operation**.

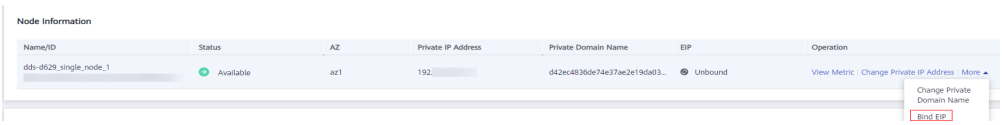
  

**Figura 4-16** Vincular um EIP



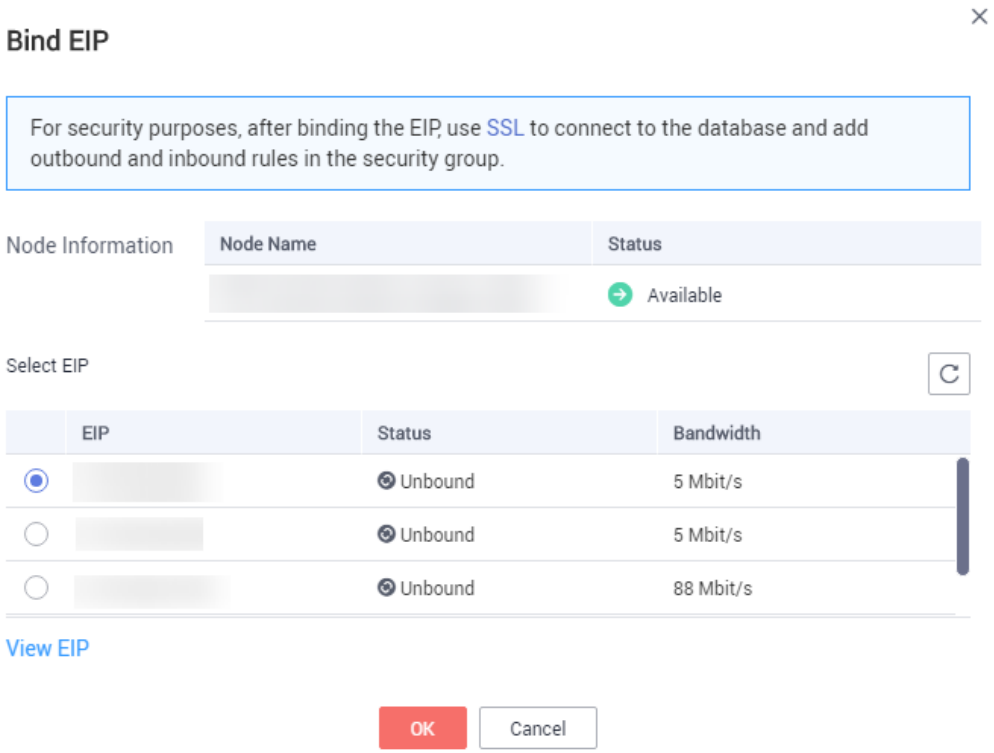

Você também pode localizar o nó na área **Node Information** na página **Basic Information** e clicar em **Bind EIP** na coluna **Operation**.

**Figura 4-17** Vincular um EIP




**Passo 6** Na caixa de diálogo exibida, todos os EIPs não vinculados e disponíveis são listados. Selecione o EIP necessário e clique em **OK**. Se nenhum EIP disponível for exibido, clique em **View EIP** e crie um EIP no console da VPC.

**Figura 4-18** Selecionar um EIP



**Passo 7** Na coluna **EIP**, você pode exibir o EIP vinculado.

Para desvincular um EIP da instância, consulte **Desvincular um EIP**.

**----Fim**

## Desvincular um EIP

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

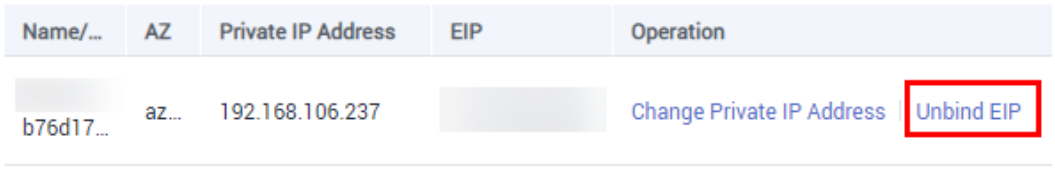
**Passo 2** Clique em no canto superior esquerdo e selecione uma região e um projeto.

**Passo 3** Clique em no canto superior esquerdo da página e escolha **Databases** > **Document Database Service**.

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

**Passo 5** No painel de navegação à esquerda, escolha **Connections**. Clique na guia **Public Connection**. Na área **Basic Information**, localize o nó e clique em **Unbind EIP** na coluna **Operation**.

**Figura 4-19** Desvincular um EIP




Você também pode localizar o nó na área **Node Information area** na página **Basic Information** e clicar em **Unbind EIP** na coluna **Operation**.

**Passo 6** Na caixa de diálogo exibida, clique em **Yes**.

Para vincular um EIP à instância novamente, consulte **Vincular um EIP**.

**----Fim**

## 4.2.4.2 Configuração de um grupo de segurança

Um grupo de segurança é um grupo lógico. Ele fornece políticas de controle de acesso para ECSs e instâncias que têm os mesmos requisitos de proteção de segurança e são mutuamente confiáveis em uma VPC.

Para garantir a segurança e a confiabilidade do banco de dados, você precisa configurar regras de grupo de segurança para permitir que endereços IP e portas específicos acessem instâncias do DDS.

Quando você tenta se conectar a uma instância por meio de um EIP, é necessário configurar uma regra de entrada para o grupo de segurança associado à instância.

## Precauções

- Por predefinição, uma conta pode criar até 500 regras de grupo de segurança.

- Muitas regras de grupo de segurança aumentarão a latência do primeiro pacote, portanto, recomenda-se um máximo de 50 regras para cada grupo de segurança.
- Uma instância do DDS só pode ser associada a um grupo de segurança.

## 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 e escolha **Databases** > **Document Database Service**.

**Passo 4** Na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida.

**Passo 5** Na área **Network Information** da página **Basic Information**, clique no nome do grupo de segurança.

**Figura 4-20** Grupo de segurança


Você também pode escolher **Connections** no painel de navegação à esquerda. Na guia **Public Connection**, na área **Security Group**, clique no nome do grupo de segurança.

**Figura 4-21** Grupo de segurança


**Passo 6** Na página **Security Group**, localize o grupo de segurança de destino e clique em **Manage Rule** na coluna **Operation**.

**Passo 7** Na guia **Inbound Rules**, clique em **Add Rule**. A caixa de diálogo **Add Inbound Rule** é exibida.

**Passo 8** Adicione uma regra de grupo de segurança conforme solicitado.

**Figura 4-22** Adicionar regra de entrada

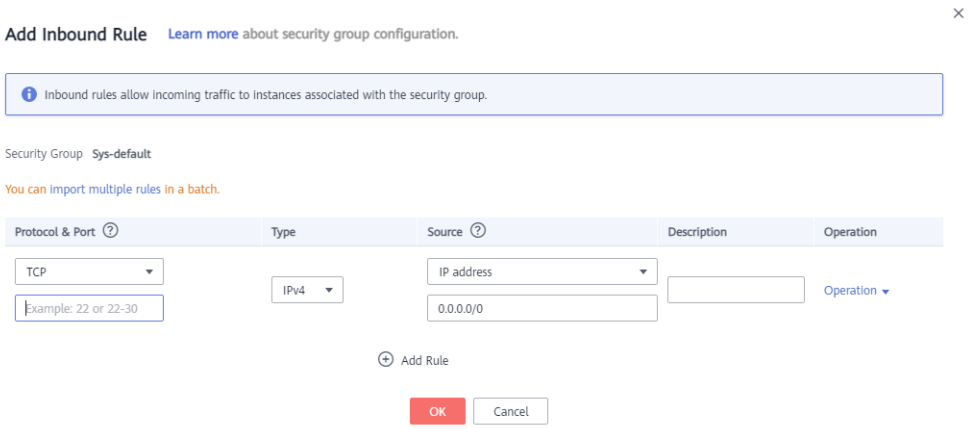



**Tabela 4-11** Configurações da regra de entrada

| Parâmetro | Descrição | Exemplo de valor |
| --- | --- | --- |
| Priority | A prioridade da regra do grupo de segurança.<br>O valor de prioridade varia de 1 a 100. A prioridade padrão é 1 e tem a prioridade mais alta. A regra de grupo de segurança com um valor menor tem uma prioridade mais alta. | 1 |
| Action | As ações de regra do grupo de segurança.<br>Uma regra com uma ação de negação substitui outra com uma ação de permitir se as duas regras tiverem a mesma prioridade. | Allow |
| Protocol & Port | O protocolo de rede necessário para o acesso. A opção pode ser **All**, **TCP**, **UDP**, **ICMP** ou **GRE**. | TCP |
| | Porta: a porta na qual você deseja permitir o acesso ao DDS. A porta padrão é 8635. A porta varia de 2100 a 9500 ou pode ser 27017, 27018 ou 27019. | 8635 |
| Type | Tipo do endereço IP. Apenas **IPv4** e **IPv6** são suportados. | IPv4 |

| Parâmetro | Descrição | Exemplo de valor |
| --- | --- | --- |
| Source | Especifica o endereço IP, o grupo de segurança e o grupo de endereços IP suportados, que permitem o acesso de endereços IP ou instâncias em outro grupo de segurança. Exemplo:<br>● Endereço IP único: 192.168.10.10/32<br>● Segmento do endereço IP: 192.168.1.0/24<br>● Todos os endereços IP: 0.0.0.0/0<br>● Grupo de segurança: sg-abc<br>● Grupo de endereço IP: ipGroup-test<br>Se você inserir um grupo de segurança, todos os ECSs associados ao grupo de segurança estarão em conformidade com a regra criada.<br>Para obter mais informações sobre grupos de endereços IP, consulte **Grupo de endereços IP**. | 0.0.0.0/0 |
| Description | (Opcional) Fornece informações complementares sobre a regra de grupo de segurança. Este parâmetro é opcional.<br>A descrição pode conter no máximo 255 caracteres e não pode conter colchetes angulares (< ou >). | - |

**Passo 9** Clique em **OK**.

**----Fim**

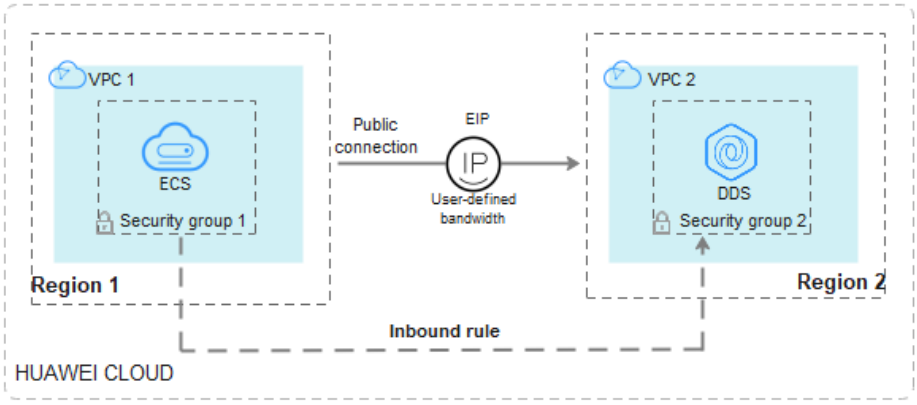
## 4.2.4.3 Conexão a uma instância de nó único usando Mongo Shell (rede pública)

Nos cenários a seguir, você pode acessar uma instância do DDS da Internet vinculando um EIP à instância.

Cenário 1: suas aplicações são implementadas em um ECS e não estão na mesma região que a instância do DDS.

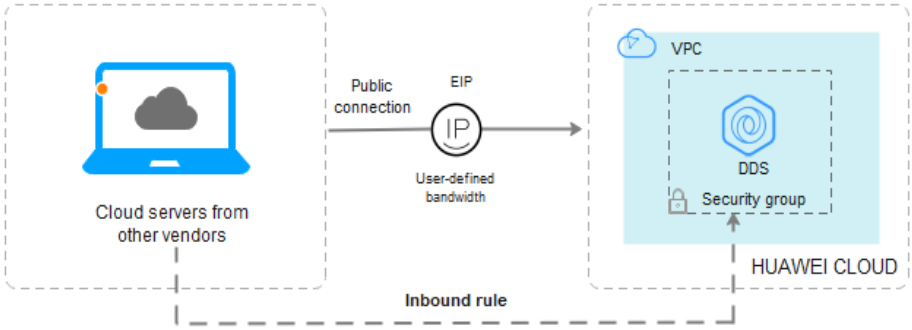
  

**Figura 4-23** Acessar o DDS a partir do ECS em todas as regiões




Cenário 2: suas aplicações são implementadas em um servidor de nuvem fornecido por outros fornecedores.

**Figura 4-24** Acessar o DDS de outros servidores em nuvem




Esta seção descreve como usar o Mongo Shell para se conectar a uma instância de nó único por meio de um EIP.

Você pode se conectar a uma instância usando uma conexão SSL ou uma conexão não criptografada. A conexão SSL é criptografada e mais segura. Para melhorar a segurança da transmissão de dados, conecte-se a instâncias usando SSL.

## Pré-requisitos

1. Para obter detalhes sobre como criar e fazer logon em um ECS, consulte **Compra de um ECS** e **Logon em um ECS**.
2. **Vincule um EIP** à instância de nó único e **configure regras de grupo de segurança** para garantir que o EIP possa ser acessado a partir do ECS.
3. Instale o cliente de MongoDB no ECS.

   Para obter detalhes sobre como instalar um cliente de MongoDB, consulte **Como instalar um cliente de MongoDB?**

## SSL

**AVISO**

Se você se conectar a uma instância por meio da conexão SSL, ative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como ativar SSL, consulte **Ativação e desativação de SSL**.

**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 e escolha **Databases** > **Document Database Service**.

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

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

**Passo 6** Na área **Basic Information**, clique em ao lado do campo **SSL**.

**Passo 7** Importe o certificado raiz para o Linux ou WindowsECS. Para obter detalhes, consulte **Como importar o certificado raiz para o sistema operacional Windows ou Linux?**

**Passo 8** Conecte-se à instância no diretório em que o cliente de MongoDB está localizado.

Usar um EIP

Exemplo de comando:

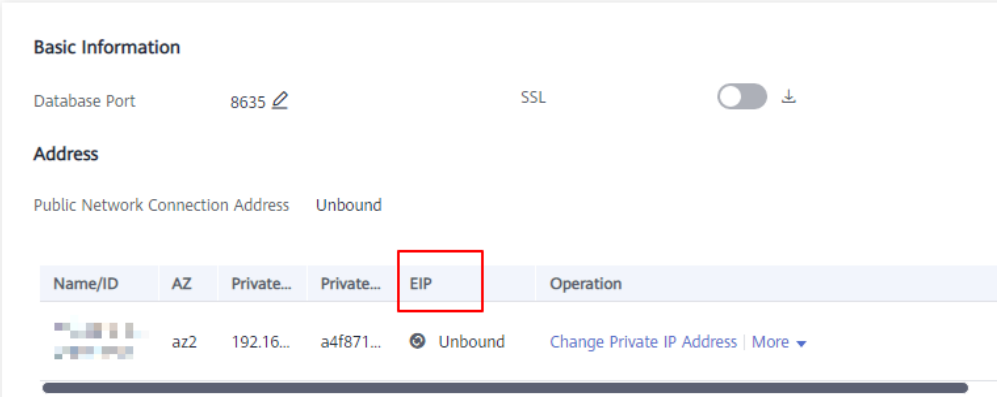
**./mongo --host** <*DB_HOST*> **--port** <*DB_PORT*> **-u** <*DB_USER*> **-p --authenticationDatabaseadmin --ssl --sslCAFile**<*FILE_PATH*> **--sslAllowInvalidHostnames**

Descrição do parâmetro:

- **DB_HOST** é o EIP vinculado à instância a ser conectada.

  Na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida. Escolha **Connections**> **Public Connection** e obtenha o EIP do nó correspondente.

  **Figura 4-25** Obter um EIP

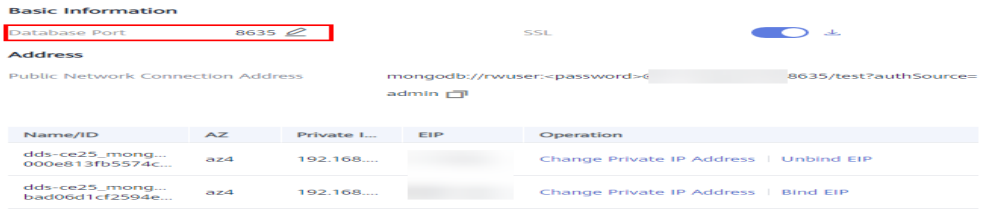


- **DB_PORT** é a porta do banco de dados. O número de porta padrão é 8635.

  você pode clicar no nome da instância para ir para a página **Basic Information**. No painel de navegação à esquerda, escolha **Connections**. Na página exibida, clique na guia **Public Connection** e obtenha a porta no campo **Database Port** na área **Basic Information**.

  **Figura 4-26** Obter a porta

- **DB_USER** é o usuário do banco de dados. O valor padrão é **rwuser**.
- **FILE_PATH** é o caminho para armazenar o certificado raiz.
- **--sslAllowInvalidHostnames**: para garantir que a comunicação interna dos nós únicos não ocupe recursos como o endereço IP do usuário e a largura de banda, o certificado de nó único é gerado usando o endereço IP de gerenciamento interno. **--sslAllowInvalidHostnames** é necessário para a conexão SSL por meio de uma rede pública.

Exemplo de comando:

**./mongo --host** *192.168.xx.xx* **--port 8635 -u rwuser -p --authenticationDatabase admin --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames**

Digite a senha do banco de dados quando solicitado:

```
Enter password:
```

**Passo 9** Verifique o resultado da conexão. Se as informações a seguir forem exibidas, a conexão será bem-sucedida.

```
replica:PRIMARY>
```

**----Fim**

## Conexão não criptografada

**AVISO**

Se você se conectar a uma instância por meio de uma conexão não criptografada, desative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como desativar SSL, consulte **Ativação e desativação de SSL**.

**Passo 1** Efetue logon no ECS.

**Passo 2** Conecte-se a uma instância do DDS.

Usar um EIP

Exemplo de comando:

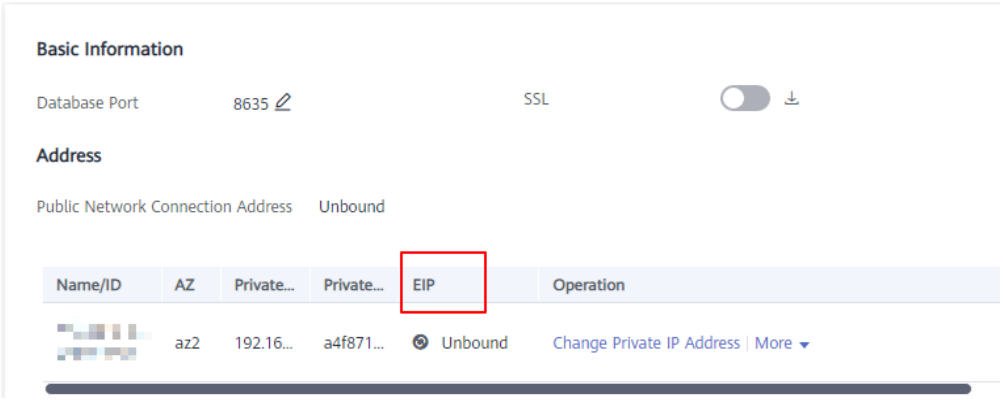
**./mongo --host** *<DB_HOST>* **--port** *<DB_PORT>* **-u** *<DB_USER>* **-p --authenticationDatabase admin**

Descrição do parâmetro:

- **DB_HOST** é o EIP vinculado à instância a ser conectada.

  Na página **Instances**, clique no nome da instância. A página **Basic Information** é exibida. Escolha **Connections**> **Public Connection** e obtenha o EIP do nó correspondente.

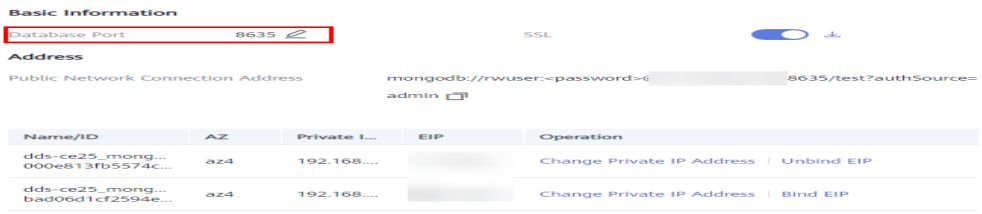
  **Figura 4-27** Obter um EIP

- **DB_PORT** é a porta do banco de dados. O número de porta padrão é 8635.

  você pode clicar no nome da instância para ir para a página **Basic Information**. No painel de navegação à esquerda, escolha **Connections**. Na página exibida, clique na guia **Public Connection** e obtenha a porta no campo **Database Port** na área **Basic Information**.

  **Figura 4-28** Obter a porta

- **DB_USER** é o usuário do banco de dados. O valor padrão é **rwuser**.

Exemplo de comando:

**./mongo --host** *192.168.xx.xx* **--port 8635 -u rwuser -p --authenticationDatabase admin**

Digite a senha do banco de dados quando solicitado:

```
Enter password:
```

**Passo 3** Verifique o resultado da conexão. Se as informações a seguir forem exibidas, a conexão será bem-sucedida.

```
replica:PRIMARY>
```

**----Fim**

## 4.2.4.4 Conexão a uma instância de nó único usando Robo 3T

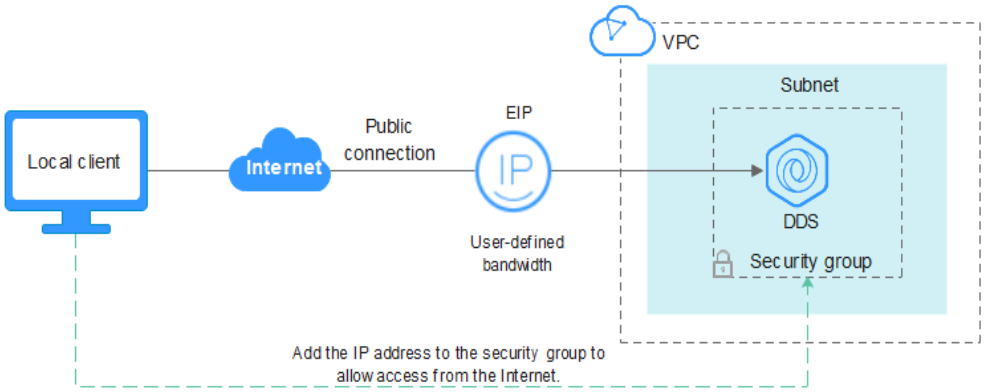
Se quiser se conectar a uma instância de um dispositivo local, você pode vincular um EIP à instância e usar o Robo 3T para se conectar à instância por meio de uma rede pública.

Esta seção descreve como usar o Robo 3T para se conectar a uma instância de cluster a partir de um dispositivo local. Nesta seção, o sistema operacional (SO) Windows usado pelo cliente é usado como um exemplo.

O Robo 3T pode se conectar a uma instância com uma conexão não criptografada ou uma conexão criptografada (SSL). Para melhorar a segurança da transmissão de dados, conecte-se a instâncias usando SSL.

## Diagrama de conexão

**Figura 4-29** Diagrama de conexão




## Pré-requisitos

1. **Vincule um EIP** à instância de nó único e configure regras de grupo de segurança para garantir que a instância possa ser acessada usando Robo 3T.
2. Instale o Robo 3T.

   Instale o Robo 3T. Para obter detalhes, consulte **Como instalar o Robo 3T?**

## SSL

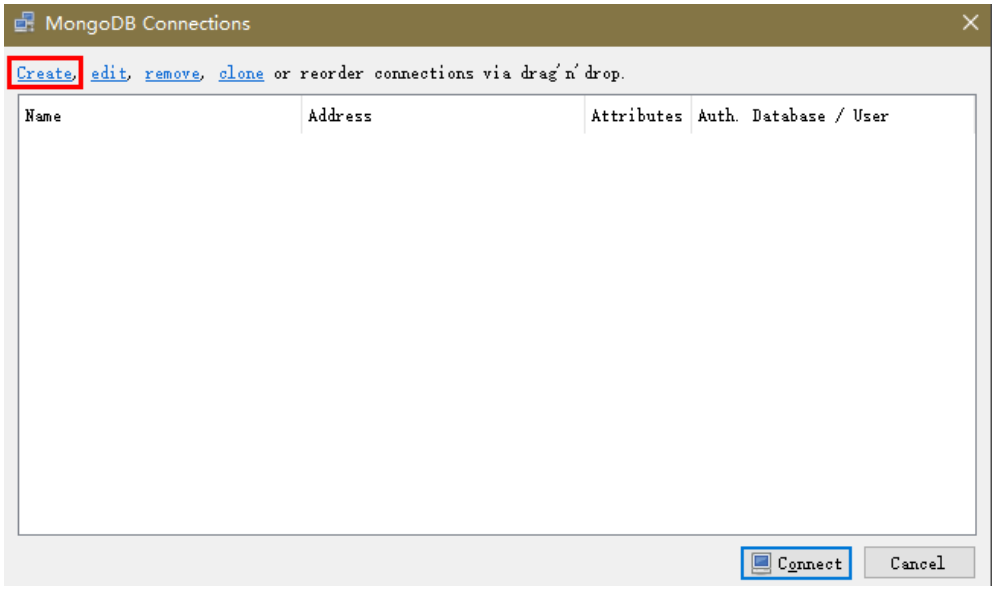
**AVISO**

Se você se conectar a uma instância por meio da conexão SSL, ative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como ativar SSL, consulte **Ativação e desativação de SSL**.

**Passo 1** Execute o Robo 3T instalado. Na caixa de diálogo exibida, clique em **Create**.

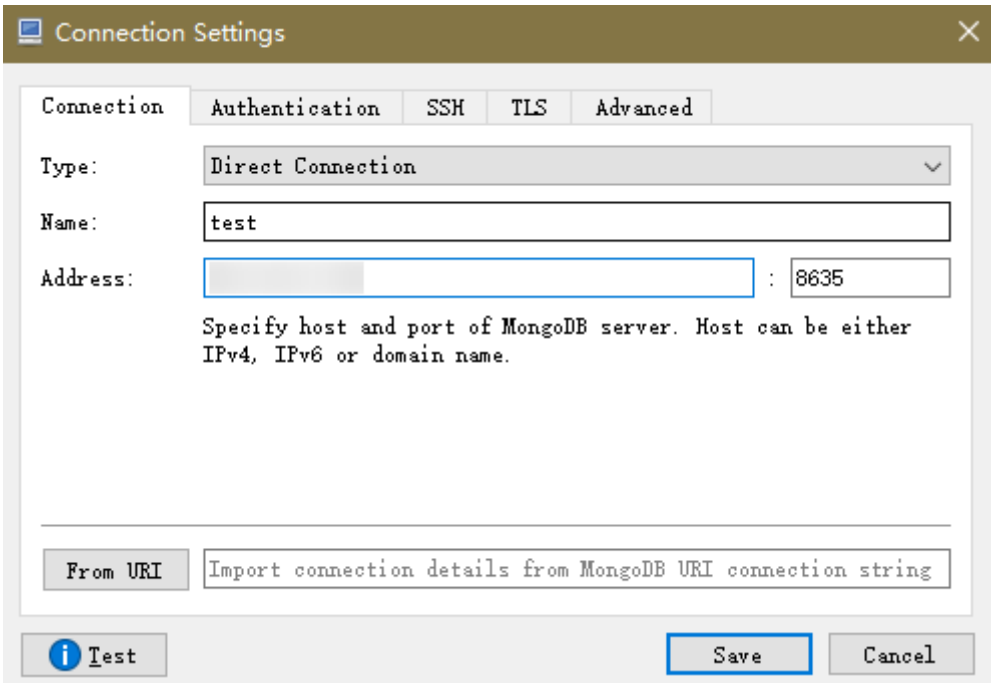
**Figura 4-30** Conexões




**Passo 2** Na caixa de diálogo **Connection Settings**, defina os parâmetros da nova conexão.

1. Na guia **Connection**, digite o nome da nova conexão na caixa de texto **Name** e insira o EIP e a porta do banco de dados vinculada à instância de BD do DDS na caixa de texto **Address**.

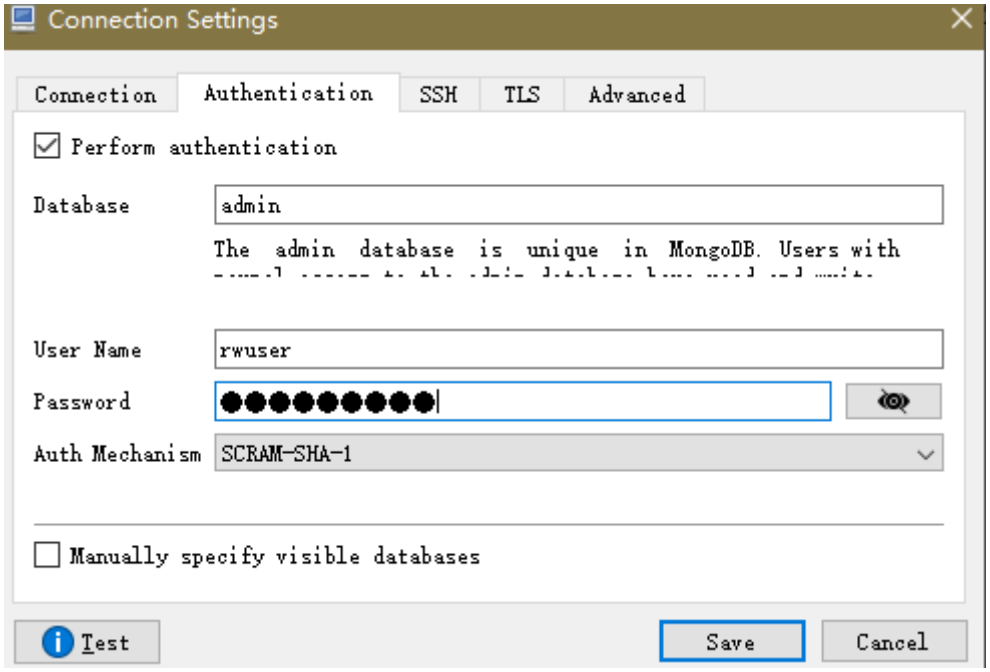
**Figura 4-31** Conexão




2. Na guia **Authentication**, defina **Database** como **admin**, **User Name** como **rwuser** e **Password** como a senha de administrador definida durante a criação da instância de cluster.

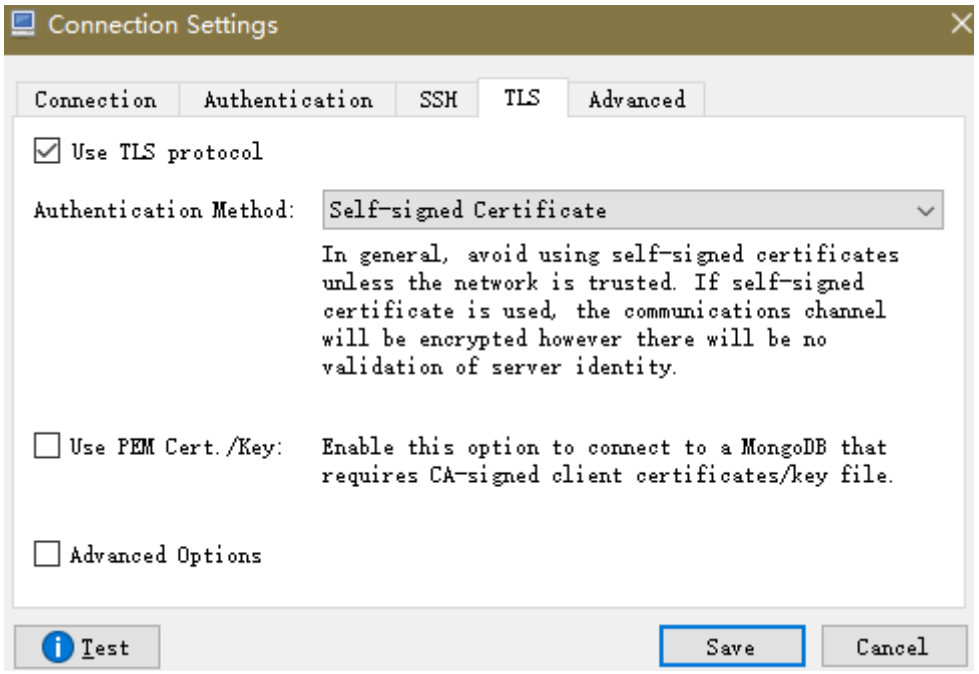
  

**Figura 4-32** Autenticação




3. Na guia **TLS**, selecione **Use TLS protocol** e selecione **Self-signed Certificate** para **Authentication Method**.

**Figura 4-33** SSL

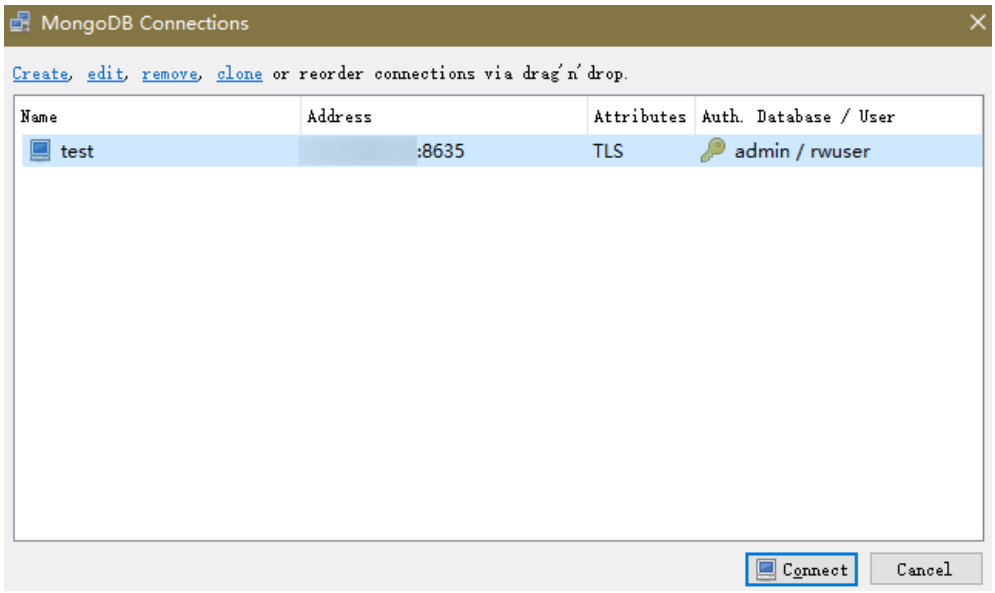



4. Clique em **Save**.

**Passo 3** Na página **MongoDB Connections**, clique em **Connect** para se conectar à instância do nó único.

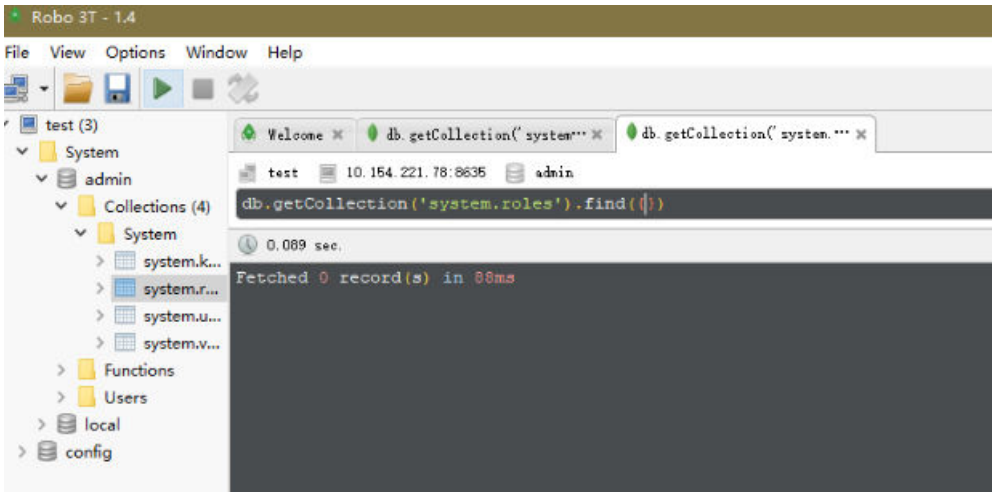
  

**Figura 4-34** Informações de conexão de nó único




**Passo 4** Se a instância de nó único for conectada com êxito, a página mostrada em **Figura 4-35** será exibida.

**Figura 4-35** Nó único conectado




**----Fim**

## Conexão não criptografada

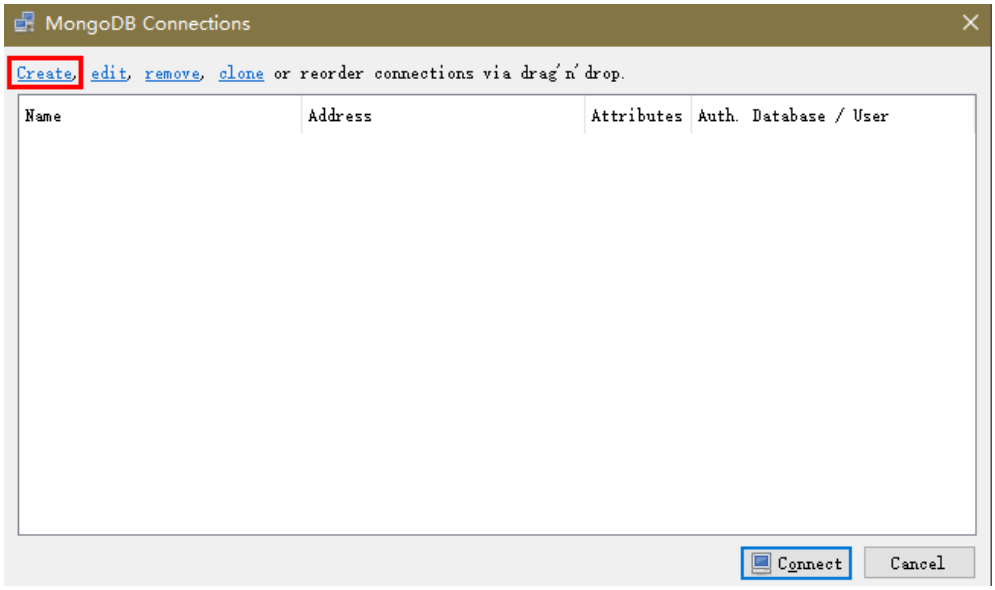
**AVISO**

Se você se conectar a uma instância por meio de uma conexão não criptografada, desative SSL primeiro. Caso contrário, um erro é relatado. Para obter detalhes sobre como desativar SSL, consulte **Ativação e desativação de SSL**.

**Passo 1** Execute o Robo 3T instalado. Na caixa de diálogo exibida, clique em **Create**.

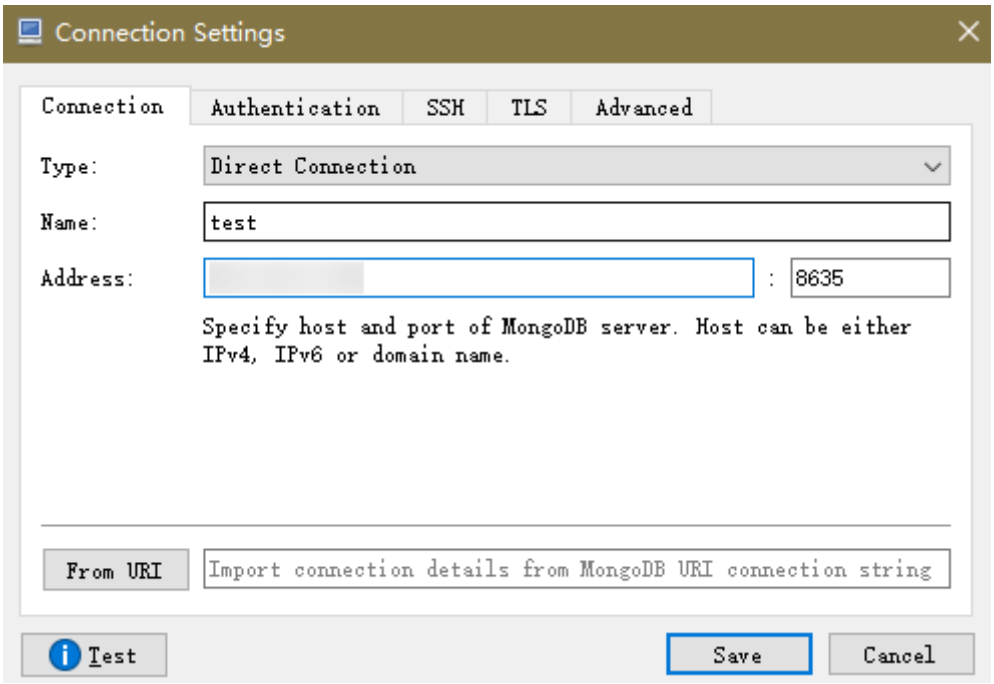
**Figura 4-36** Conexões




**Passo 2** Na caixa de diálogo **Connection Settings**, defina os parâmetros da nova conexão.

1. Na guia **Connection**, digite o nome da nova conexão na caixa de texto **Name** e insira o EIP e a porta do banco de dados vinculada à instância de BD do DDS na caixa de texto **Address**.

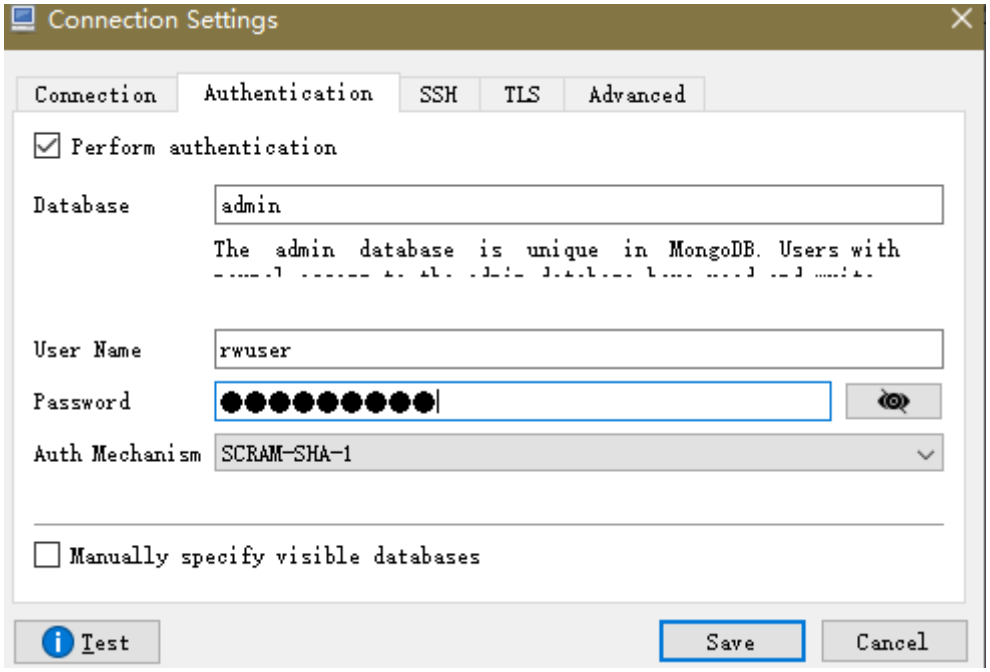
   **Figura 4-37** Conexão

2. Na guia **Authentication**, defina **Database** como **admin**, **User Name** como **rwuser** e **Password** como a senha de administrador definida durante a criação da instância de cluster.

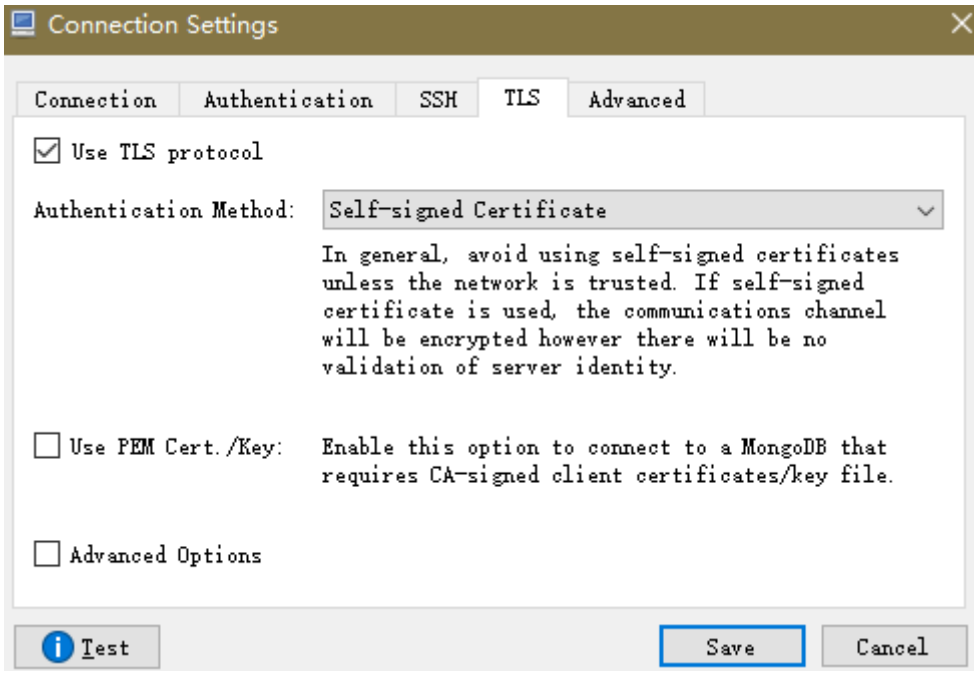
  

**Figura 4-38** Autenticação




3. Na guia **TLS**, selecione **Use TLS protocol** e selecione **Self-signed Certificate** para **Authentication Method**.

**Figura 4-39** SSL

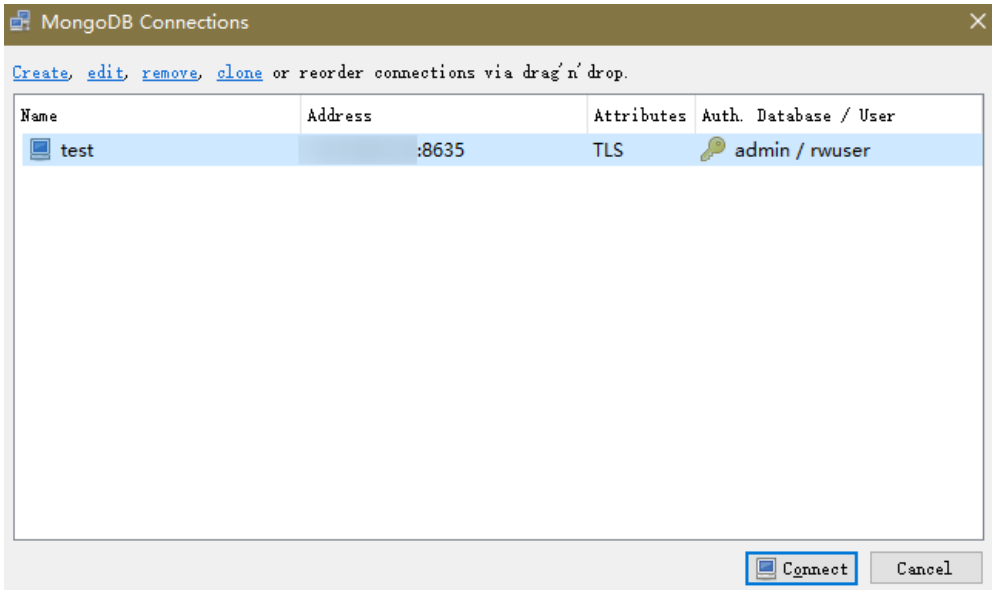



4. Clique em **Save**.

**Passo 3** Na página **MongoDB Connections**, clique em **Connect** para se conectar à instância do nó único.

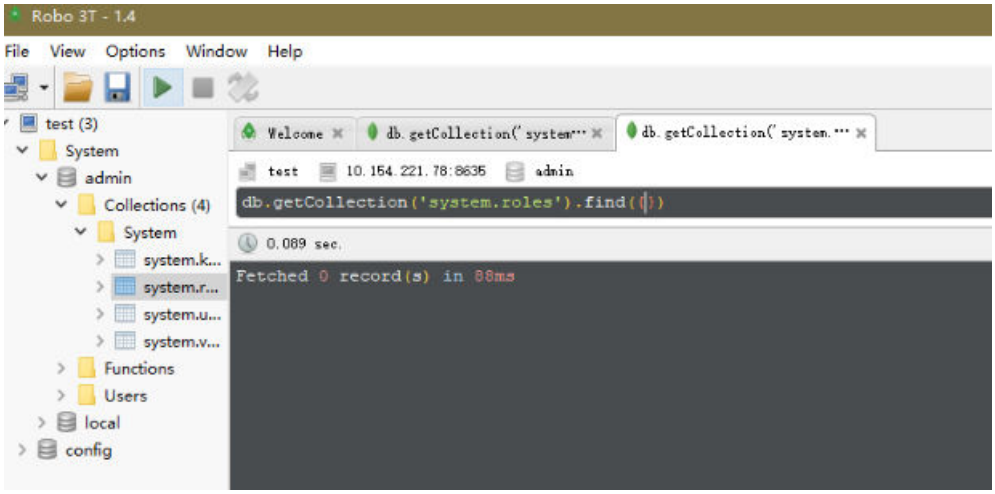
  

**Figura 4-40** Informações de conexão de nó único




**Passo 4** Se a instância de nó único for conectada com êxito, a página mostrada em **Figura 4-41** será exibida.

**Figura 4-41** Nó único conectado




**----Fim**

## 4.2.5 Conexão a uma instância de nó único usando código do programa

### 4.2.5.1 Java

Se você estiver se conectando a uma instância usando Java, um certificado SSL é opcional, mas baixar um certificado SSL e criptografar a conexão melhorarão a segurança de sua instância. SSL é desativado por padrão para instâncias de BD recém-criadas. Você pode ativar SSL consultando **Ativação ou desativação de SSL**. SSL criptografa conexões com bancos de

dados, mas aumenta o tempo de resposta da conexão e o uso da CPU. Portanto, é aconselhável não ativar o SSL.

## Pré-requisitos

Familiarize-se com:

- Noções básicas de computador
- Código Java

## Obter e utilizar Java

- Baixe o driver do Jar em **https://repo1.maven.org/maven2/org/mongodb/mongo-java-driver/3.0.4/**
- Para ver o guia de uso, visite **https://mongodb.github.io/mongo-java-driver/4.2/driver/getting-started/installation/**.

## Usar um certificado SSL

NOTA

- Baixe o certificado SSL e verifique o certificado antes de se conectar aos bancos de dados.
- Na página **Instances**, clique no nome da instância de BD de destino. Na área **DB Information** da página **Basic Information**, clique em no campo **SSL** para baixar certificado raiz ou do pacote de certificados.
- Para obter detalhes sobre como configurar uma conexão SSL, consulte o documento oficial do driver Java do MongoDB em **https://www.mongodb.com/docs/drivers/java/sync/current/fundamentals/connection/tls/#std-label-tls-ssl**.

Conecte-se a uma instância de nó único usando Java. O formato do link de Java é o seguinte:

```
mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>?authSource=admin&ssl=true
```

**Tabela 4-12** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| <username> | Nome de usuário atual. |
| <password> | Senha para o nome de usuário atual |
| <instance_ip> | Se você tentar acessar a instância de um ECS, defina *instance_ip* como o endereço IP privado exibido na página **Basic Information** da instância à qual você pretende se conectar. |
| | Se você tentar acessar a instância por meio de um EIP, defina *instance_ip* como o EIP vinculado à instância. |
| <instance_port> | Porta do banco de dados exibida na página **Basic Information**. Valor padrão: **8635** |
| <database_name> | Nome do banco de dados a ser conectado. |
| authSource | Base de dados de utilizadores de autenticação. O valor é **admin**. |
| ssl | Modo de conexão. **true** indica que o modo de conexão SSL é usado. |

Use keytool para configurar o certificado de AC. Para obter detalhes sobre os parâmetros, consulte **Tabela 4-13**.

```
keytool -importcert -trustcacerts -file <path to certificate authority file> -
keystore <path to trust store> -storepass <password>
```

**Tabela 4-13** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| <path to certificate authority file> | Caminho para armazenar o certificado SSL. |
| <path to trust store> | Caminho para armazenar o repositório confiável. Defina este parâmetro conforme necessário, por exemplo, **./trust/certs.keystore**. |
| <password> | Senha personalizada. |

Defina as propriedades do sistema JVM no programa para apontar para o repositório confiável e repositório de chaves corretos:

- System.setProperty("javax.net.ssl.trustStore","<path to trust store>");
- System.setProperty("javax.net.ssl.trustStorePassword","<password>");

Para obter detalhes sobre o código Java, consulte o exemplo a seguir:

```
public class Connector { public static void main(String[] args) { try
{ System.setProperty("javax.net.ssl.trustStore", "./trust/
certs.keystore"); System.setProperty("javax.net.ssl.trustStorePassword",
"123456"); ConnectionString connString = new ConnectionString("mongodb://
<username>:<password>@<instance_ip>:<instance_port>/<database_name>?
authSource=admin&ssl=true"); MongoClientSettings settings =
MongoClientSettings.builder() .applyConnectionString(connString) .applyTo
SslSettings(builder ->
builder.enabled(true)) .applyToSslSettings(builder ->
builder.invalidHostNameAllowed(true)) .build(); MongoClient mongoClient
= MongoClients.create(settings); MongoDatabase database =
mongoClient.getDatabase("admin"); //Ping the database. Se a operação
falhar, ocorre uma exceção. BsonDocument command = new
BsonDocument("ping", new BsonInt64(1)); Document commandResult =
database.runCommand(command); System.out.println("Connect to database
successfully"); } catch (Exception e) { e.printStackTrace();
System.out.println("Test failed"); } } }
```

## Conexão sem o certificado SSL

NOTA

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

Conecte um único nó usando Java. O formato do link Java é o seguinte:

```
mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>?
authSource=admin
```

**Tabela 4-14** Descrição do parâmetro

| Parâmetro | Descrição |
| --- | --- |
| <username> | Nome de usuário atual. |
| <password> | Senha para o nome de usuário atual |
| <instance_ip> | Se você tentar acessar a instância de um ECS, defina *instance_ip* como o endereço IP privado exibido na página **Basic Information** da instância à qual você pretende se conectar. |
| | Se você tentar acessar a instância por meio de um EIP, defina *instance_ip* como o EIP vinculado à instância. |
| <instance_port> | Porta do banco de dados exibida na página **Basic Information**. Valor padrão: **8635** |
| <database_name> | Nome do banco de dados a ser conectado. |
| authSource | Base de dados de utilizadores de autenticação. O valor é **admin**. |

Script de exemplo em Java:

```
public class Connector { public static void main(String[] args) { try
{ ConnectionString connString = new ConnectionString("mongodb://
<username>:<password>@<instance_ip>:<instance_port>/<database_name>?
authSource=admin"); MongoClientSettings settings =
MongoClientSettings.builder() .applyConnectionString(connString) .retryWr
ites(true) .build(); MongoClient mongoClient =
MongoClients.create(settings); MongoDatabase database =
mongoClient.getDatabase("admin"); //Ping the database. Se a operação
falhar, ocorre uma exceção. BsonDocument command = new
BsonDocument("ping", new BsonInt64(1)); Document commandResult =
database.runCommand(command); System.out.println("Connect to database
successfully"); } catch (Exception e) { e.printStackTrace();
System.out.println("Test failed"); } } }
```

### 4.2.5.2 Python

Esta seção descreve como se conectar a uma instância de nó único usando Python.

## Pré-requisitos

1. Para conectar um ECS a uma instância, o ECS deve ser capaz de se comunicar com a instância do DDS. Você pode executar o seguinte comando para conectar-se ao endereço IP e à porta do servidor de instância para testar a conectividade de rede.

   **curl** *ip:port*

   Se a mensagem **It looks like you are trying to access MongoDB over HTTP on the native driver port** for exibida, a conectividade de rede é normal.
2. Instale Python e o pacote de instalação de terceiros **pymongo** no ECS. Pymongo 2.8 é recomendado.
3. Se SSL estiver ativado, você precisará baixar o certificado raiz e carregá-lo no ECS.

## Código de conexão

- Ativar SSL

```
import ssl
from pymongo import MongoClient
conn_urls="mongodb://rwuser:rwuserpassword@ip:port/{mydb}?
authSource=admin"
connection = MongoClient(conn_urls,connectTimeoutMS=5000,ssl=True,
ssl_cert_reqs=ssl.CERT_REQUIRED,ssl_match_hostname=False,ssl_ca_certs
=${path to certificate authority file})
dbs = connection.database_names()
print "connect database success! database names is %s" % dbs
```

- Desativar SSL

```
import ssl
from pymongo import MongoClient
conn_urls="mongodb://rwuser:rwuserpassword@ip:port/{mydb}?
authSource=admin"
connection = MongoClient(conn_urls,connectTimeoutMS=5000)
dbs = connection.database_names()
print "connect database success! database names is %s" % dbs
```

NOTA

- O banco de dados de autenticação no URL deve ser **admin**. Isso significa definir **authSource** como **admin**.
- No modo SSL, você precisa gerar manualmente o arquivo trustStore.
- A base de dados de autenticação tem de ser **admin** e, em seguida, mudar para a base de dados de serviço.

# 5 Logon no console do DDS

## Pré-requisitos

Você precisa ter uma conta na plataforma de nuvem antes de poder usar o DDS

Pela primeira vez que você usa o DDS, solicite uma conta no site oficial. Depois que a aplicação for bem-sucedida, sua conta terá permissões para acessar o serviço DDS, bem como todos os outros serviços em nuvem.

## Procedimento

**Passo 1** Abre **site oficial da Huawei Cloud**

**Passo 2** Clique em **Console** no canto superior direito da página. A página de logon do console de gerenciamento da Huawei Cloud é exibida.

**Passo 3** Insira as informações da conta conforme solicitado e clique em **Log In**.

O logon foi bem-sucedido.

**Passo 4** Clique em no no canto superior esquerdo e selecione uma região e um projeto.

Se você quiser usar exclusivamente recursos de computação e rede, você precisa **ativar uma DeC** e **solicitar recursos do DCC**. Depois de ativar uma DeC, você pode selecionar a região da DeC e o projeto.

Você será cobrado adicionalmente pelo uso da DeC.

**Passo 5** Clique em no canto superior esquerdo da página e escolha **Databases** > **Document Database Service**.

**----Fim**

# 6 Exemplo: comprar e conectar-se a uma instância do DDS

## 6.1 Conexão a uma instância de um ECS

Esta seção usa o sistema operacional Linux como exemplo para descrever como comprar e se conectar a uma instância de cluster em uma rede privada.

**Passo 1: criar um ECS**

**Passo 2: criar uma instância de cluster**

**Passo 3: conectar a uma instância de cluster**

### Passo 1: criar um ECS

1. Acesse o **console de gerenciamento**.
2. Em **Compute**, escolha **Elastic Cloud Server**. Na página **Elastic Cloud Server** exibida, clique em **Buy ECS**.
3. Defina as configurações básicas e clique em **Next: Configure Network**. A região e AZ do ECS são as mesmas da instância do cluster a ser conectada.

**Figura 6-1** Configurações básicas

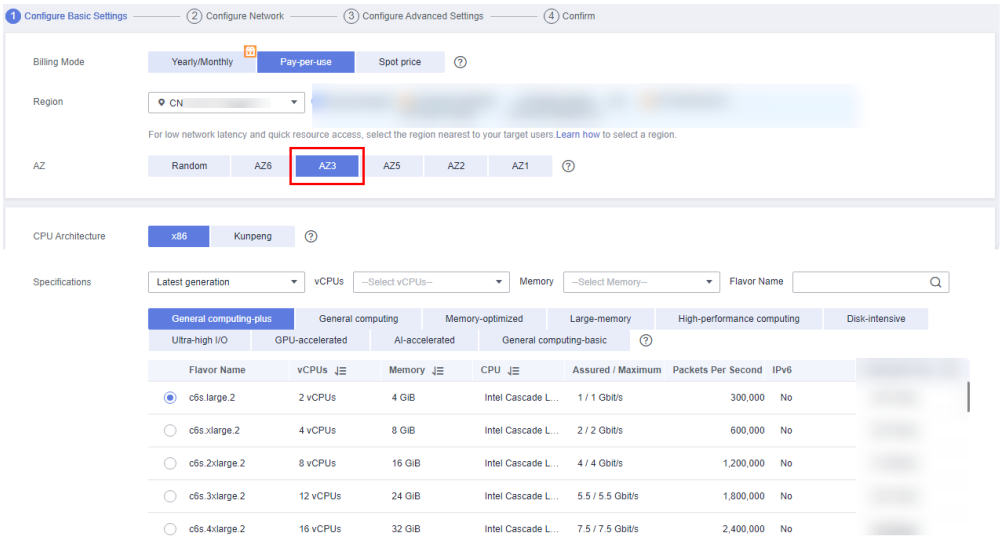
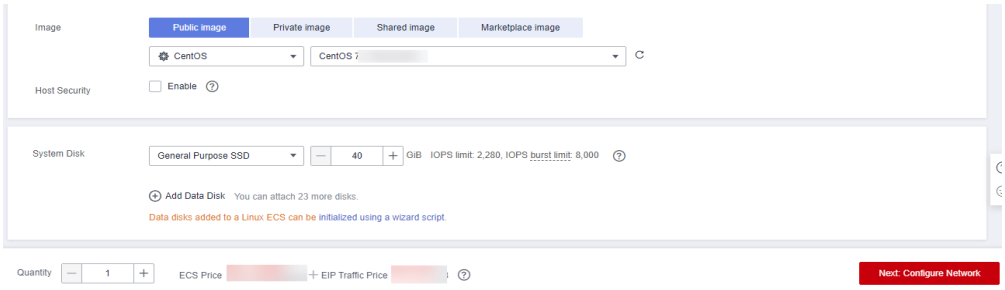
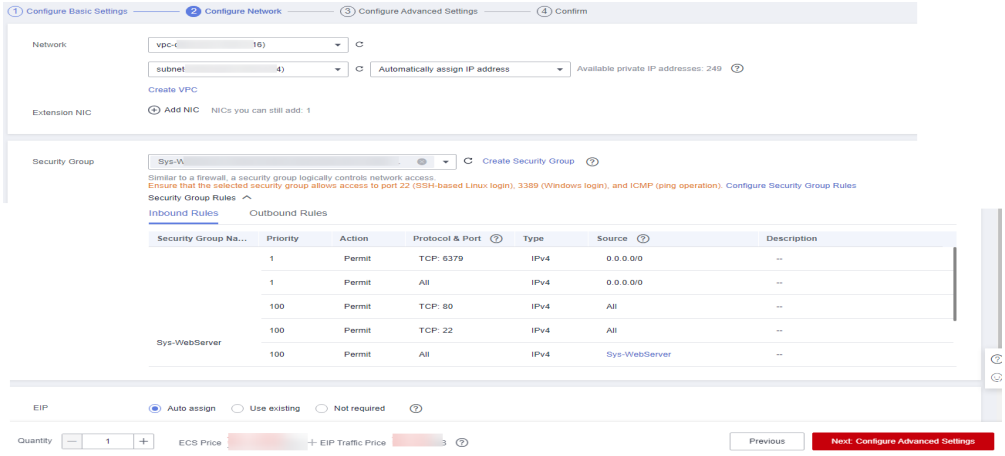



**Figura 6-2** Selecionar uma imagem




4. Configure as informações de rede do ECS e clique em **Next: Configure Advanced Settings**. A VPC e o grupo de segurança do ECS são os mesmos da instância de cluster a ser conectada.

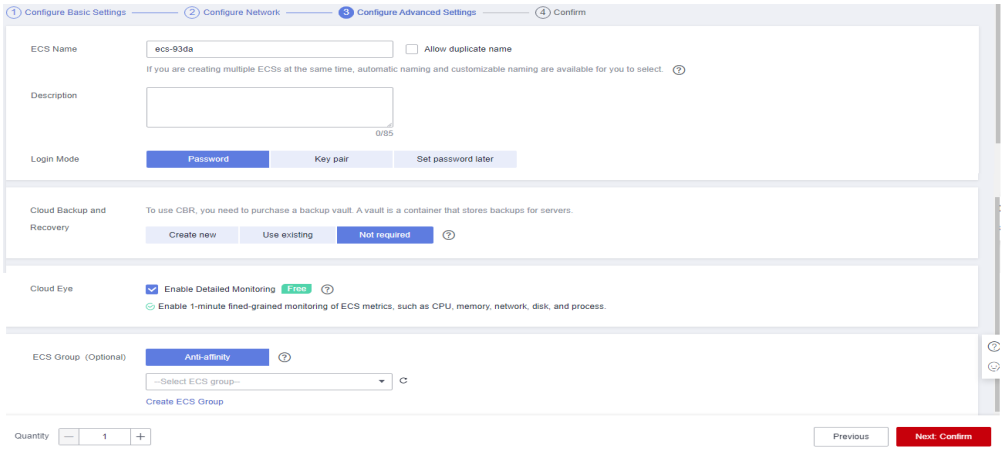
**Figura 6-3** Configurações da rede




5. Configure a senha do ECS e clique em **Next: Confirm**.

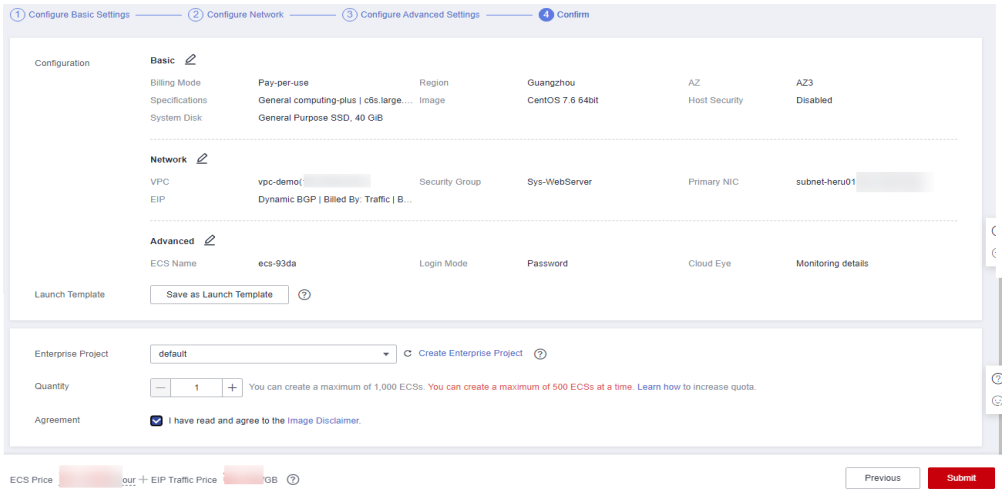
  

**Figura 6-4** Configurações avançadas




6. Confirme as configurações e clique em **Submit**.

**Figura 6-5** Confirmar as configurações




7. Veja o ECS comprado.

**Figura 6-6** Compra bem-sucedida


## Passo 2: criar uma instância de cluster

1. Acesse o **console de gerenciamento**.
2. Escolha **Databases** > **Document Database Service**. Na página exibida, clique em **Buy DB Instance**.
3. Na página exibida, clique em **Custom Config**.
4. Configure as informações da instância e clique em **Submit**. A região, a AZ, a VPC e o grupo de segurança do ECS são os mesmos da instância de cluster a ser conectada.

**Figura 6-7** Configurações básicas

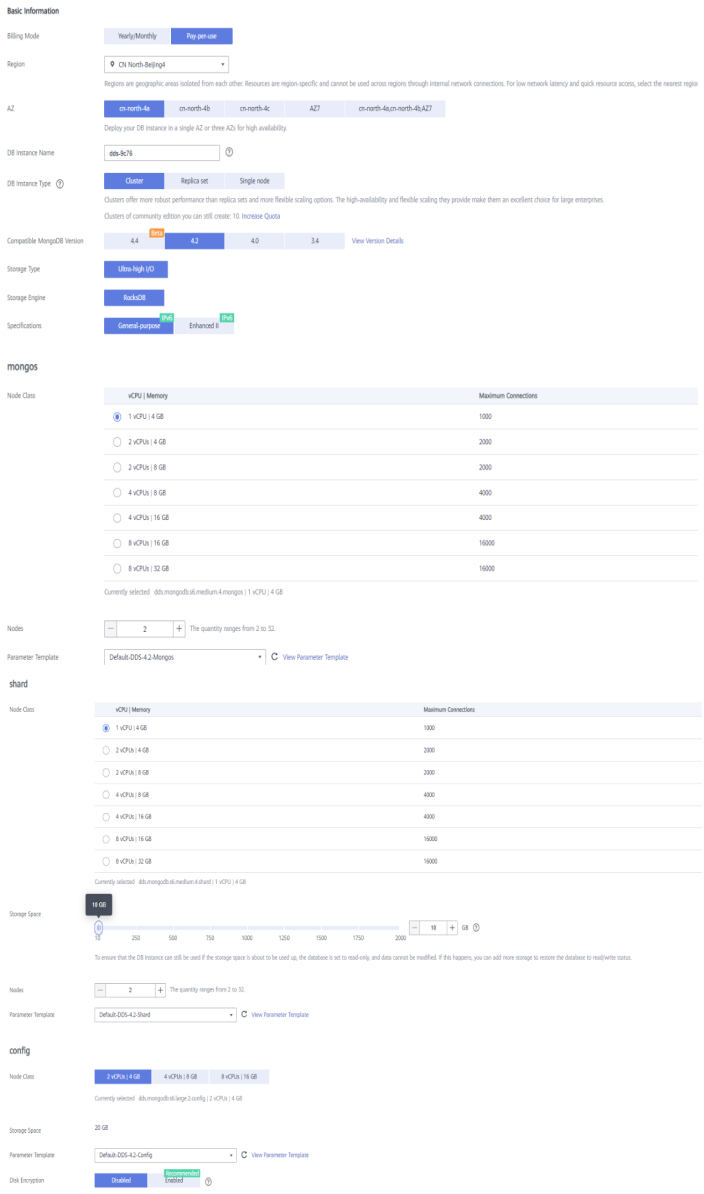



**Figura 6-8** Configurações do administrador

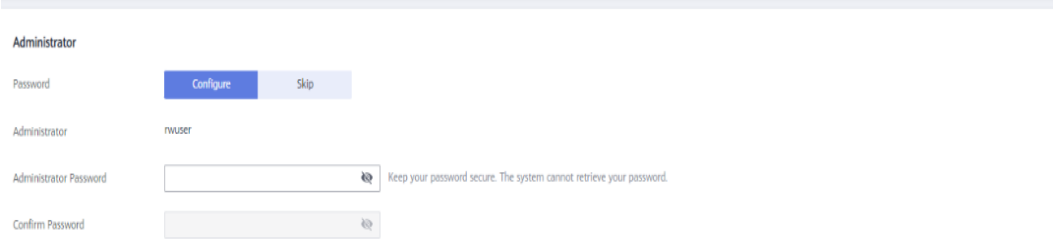


**Figura 6-9** Rede e duração necessária

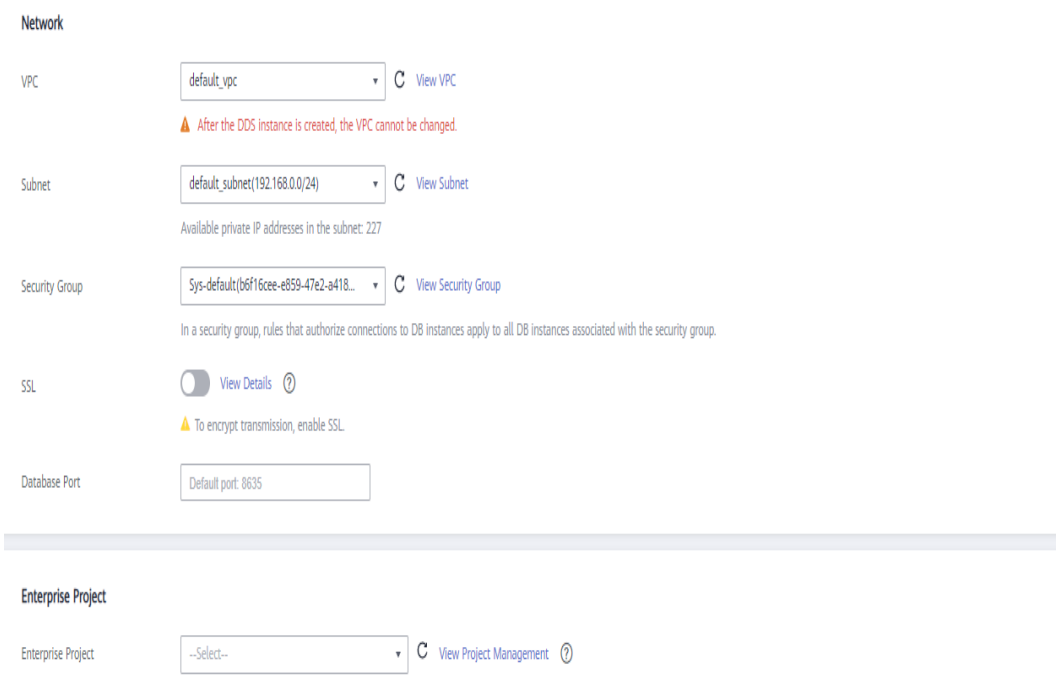
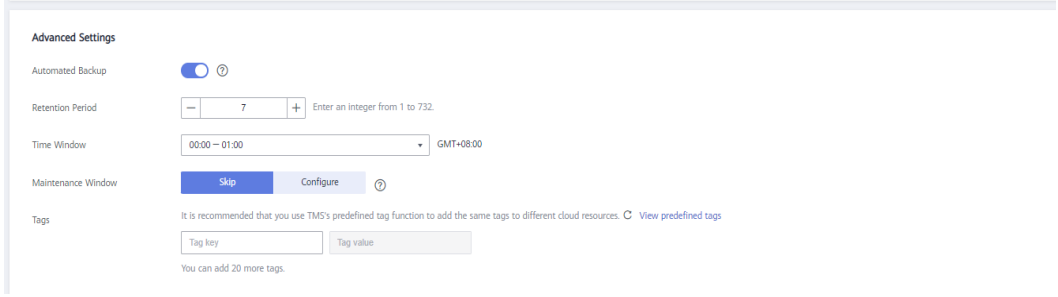
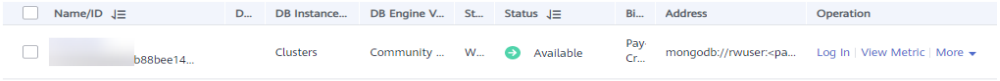



**Figura 6-10** Configurações avançadas




5. Visualize a instância do DDS comprada.

**Figura 6-11** Compra bem-sucedida

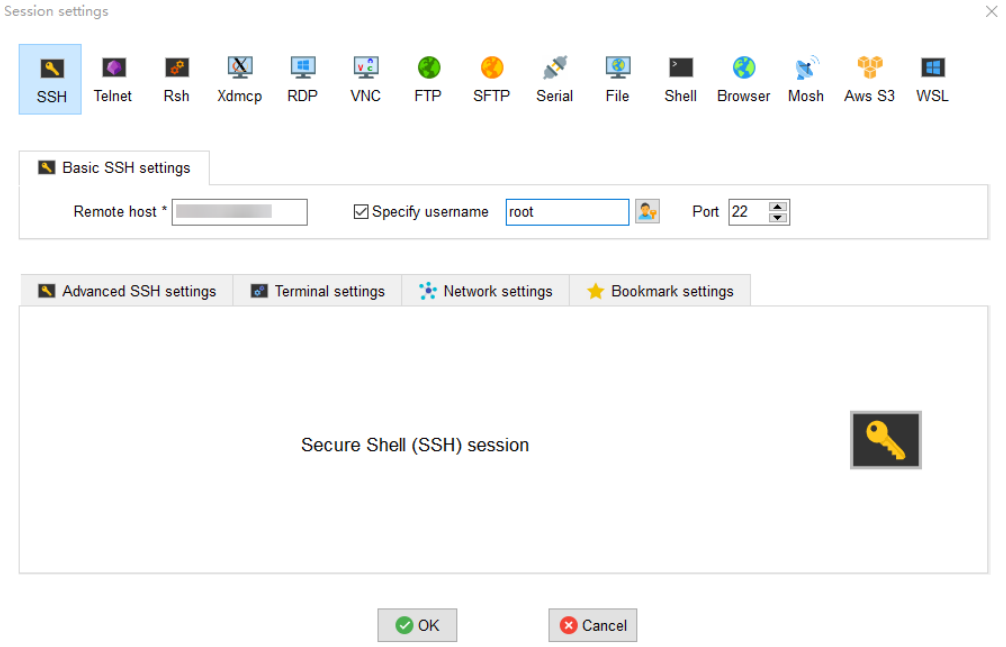



## Passo 3: conectar a uma instância de cluster

1. Use a ferramenta de conexão remota do Linux para efetuar logon no ECS. **Remote host** é o EIP vinculado ao ECS.

**Figura 6-12** Criar uma sessão




2. Digite a senha do ECS.

**Figura 6-13** Digitar a palavra-passe

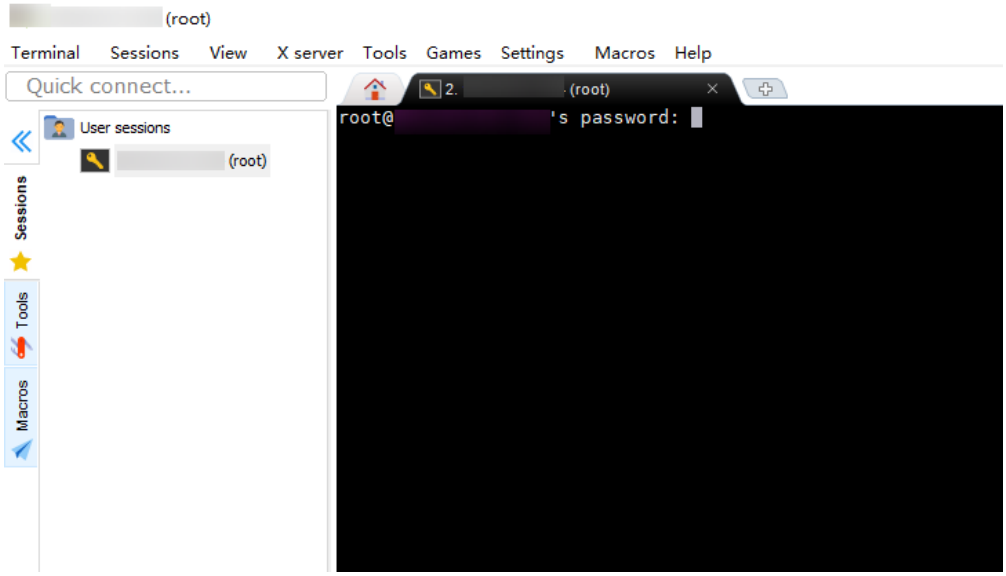
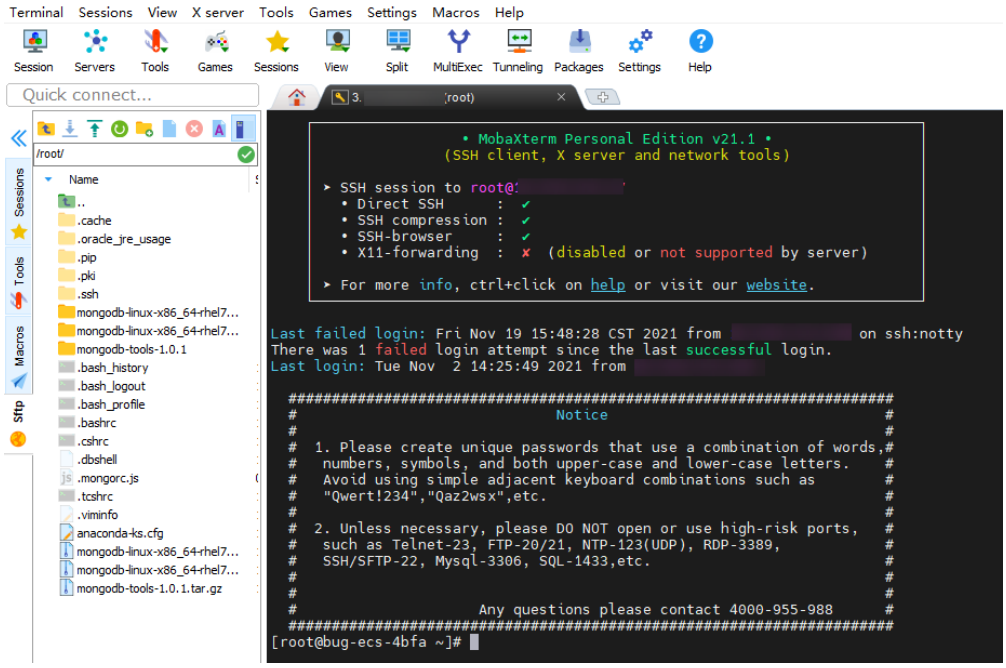


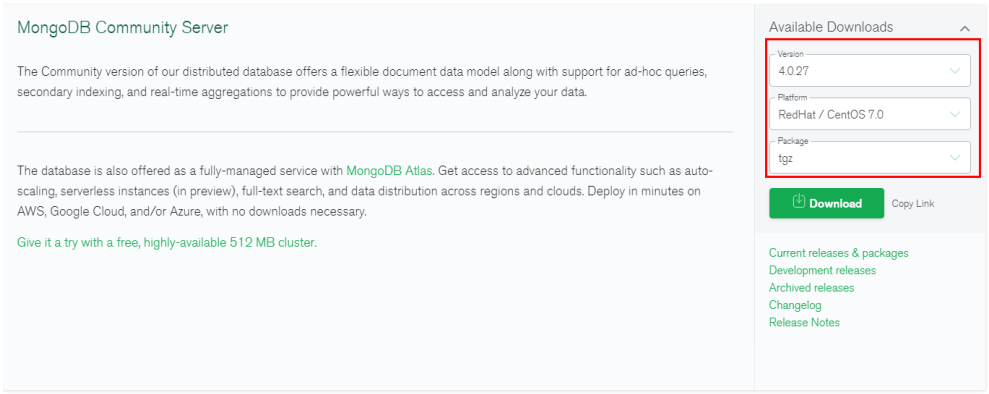

  

**Figura 6-14** Logon bem-sucedido




3. Baixe o pacote de instalação do cliente **mongodb-linux-x86_64-rhel70-4.0.27.tgz**.

**Figura 6-15** Baixar o cliente




4. Faça upload do pacote de instalação do cliente no ECS.

**Figura 6-16** Upload do pacote do cliente

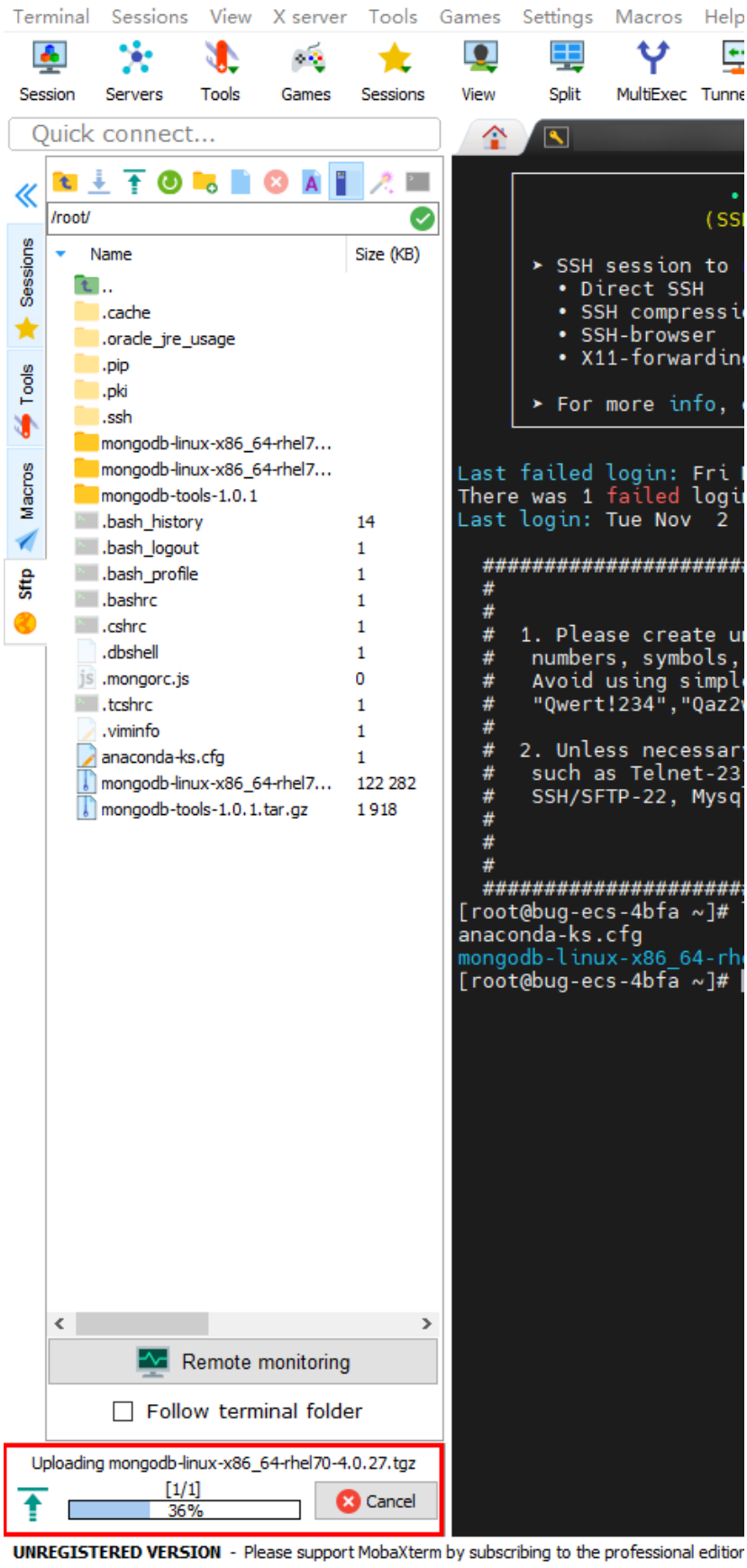
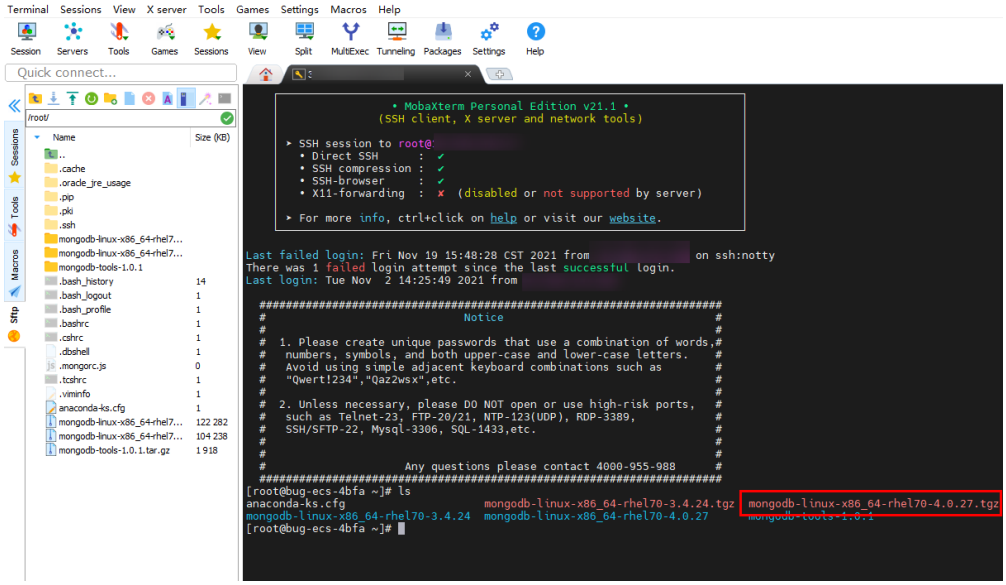


**Figura 6-17** Pacote carregado




5. Descompacte o pacote de instalação no ECS.

   **tar zxvf mongodb-linux-x86_64-rhel70-4.0.27.tgz**

6. Obtenha a ferramenta cliente do diretório **bin** do pacote de instalação.

   **cd mongodb-linux-x86_64-rhel70-4.0.27/bin**

   As ferramentas comuns são as seguintes:

   – Cliente de MongoDB mongo
   – Ferramenta de exportação de dados mongoexport
   – Ferramenta de importação de dados mongoimport

7. Antes de usar uma ferramenta cliente, atribua a permissão de execução a ela.
   – Execute o comando **chmod +x mongo** para conceder a um cliente permissão para se conectar a uma instância de BD.
   – Execute o comando **chmod +x mongoexport** para conceder a um cliente permissão para exportar dados.
   – Execute o comando **chmod +x mongoimport** para conceder a um cliente permissão para importar dados.

8. Conecte-se à instância de DDS.

   **./mongo mongodb://**
   **rwuser:**<*password*>**@**<*DB_HOST1*>**:**<*DB_PORT1*>**,**<*DB_HOST2*>**:**<*DB_PORT2*>**/test?authSource=admin**

   NOTA

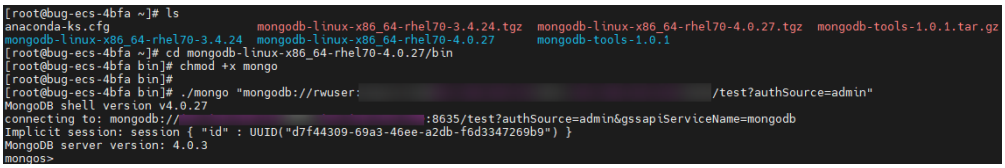
   <*password*> é a senha para o nome de usuário do banco de dados. Substitua-a pela senha atual.

   Se a senha contiver sinais de arroba (@), pontos de exclamação (!) ou sinais de porcentagem (%), substitua-os por códigos de URL hexadecimais (ASCII) %40, %21 e %25, respectivamente.

   Por exemplo, se a senha for ****@ %***!, o código de URL correspondente será **** %40%25*** %21.

**Figura 6-18** Conexão bem sucedida




9. Crie um banco de dados e uma coleção.

**Figura 6-19** Criar um banco de dados

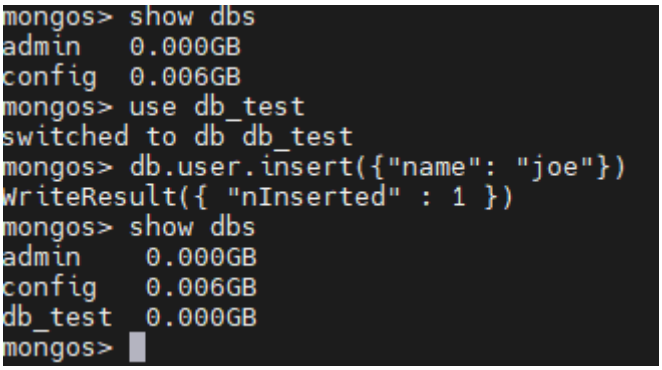
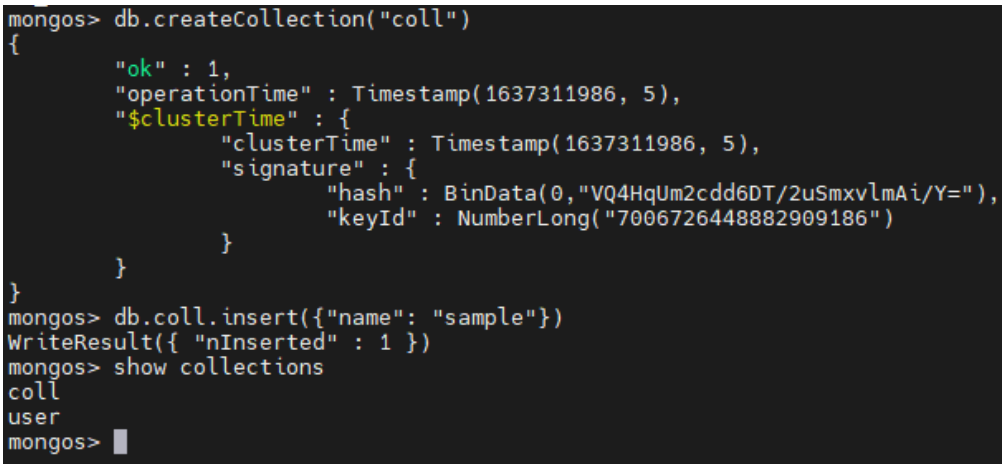



**Figura 6-20** Criar uma coleção




# 6.2 Conexão a uma instância do DDS por meio de um EIP

Esta seção usa uma instância do conjunto de réplicas do DDS e o sistema operacional Windows como exemplo para descrever como comprar uma instância do DDS, vincular um EIP, definir um grupo de segurança e conectar-se à instância do DDS usando a ferramenta Robo 3T em seu ambiente local. Os procedimentos são os seguintes:

- **Passo 1: comprar uma instância de BD**
- **Passo 2: vincular um EIP**
- **Passo 3: configurar um grupo de segurança**
- **Passo 4: conectar-se a uma instância do DDS**

## Passo 1: comprar uma instância de BD

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione uma região e um projeto.
3. Clique em no canto superior esquerdo da página e escolha **Databases** > **Document Database Service**.
4. Na página **Instances**, clique em **Comprar instância de BD**.
5. Na página exibida, clique em **Custom Config**.
6. Selecione um modo de cobrança. Especifique os detalhes da instância e clique em **Próximo**.

**Figura 6-21** Configurações básicas

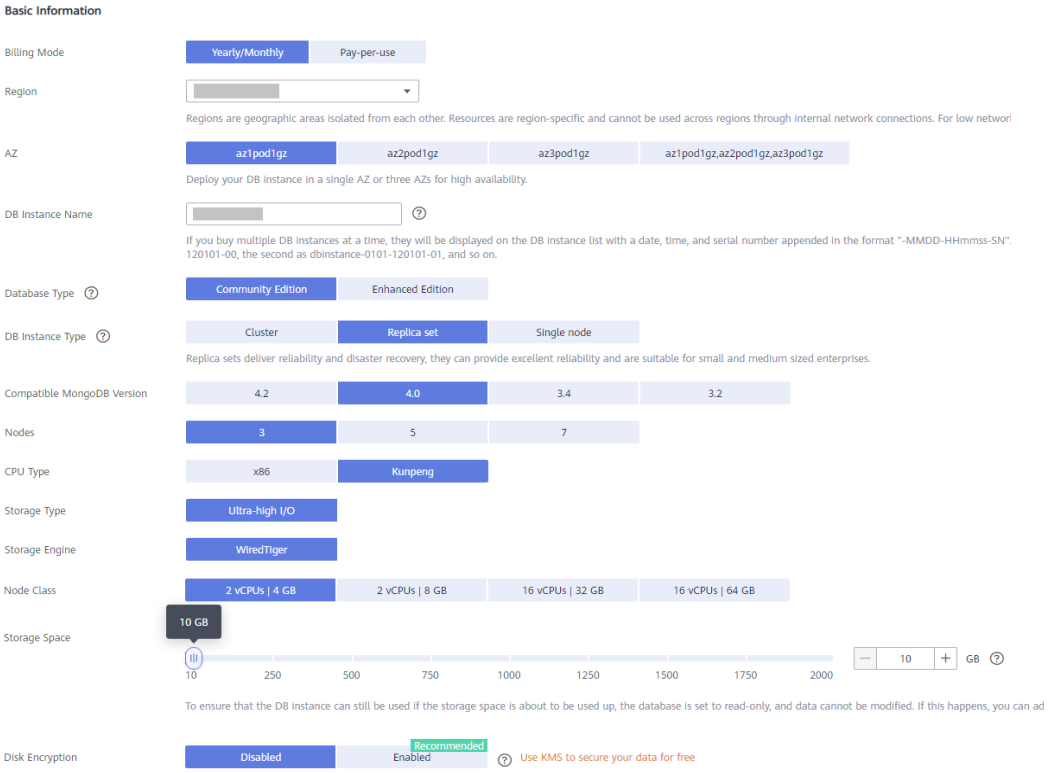



**Figura 6-22** Configurações do administrador

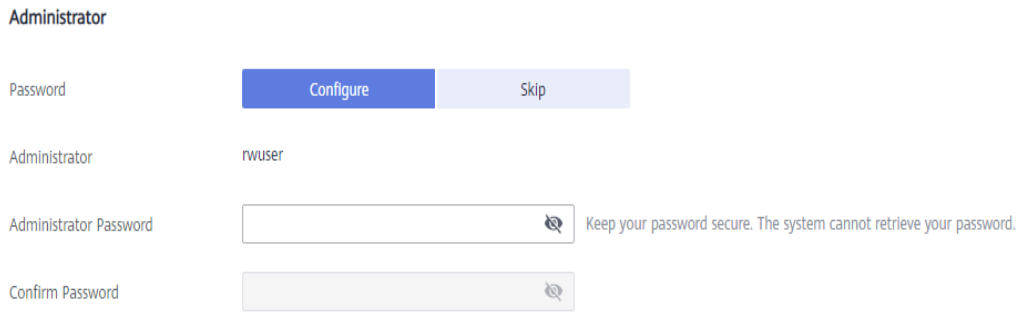


**Figura 6-23** Rede, duração necessária e quantidade

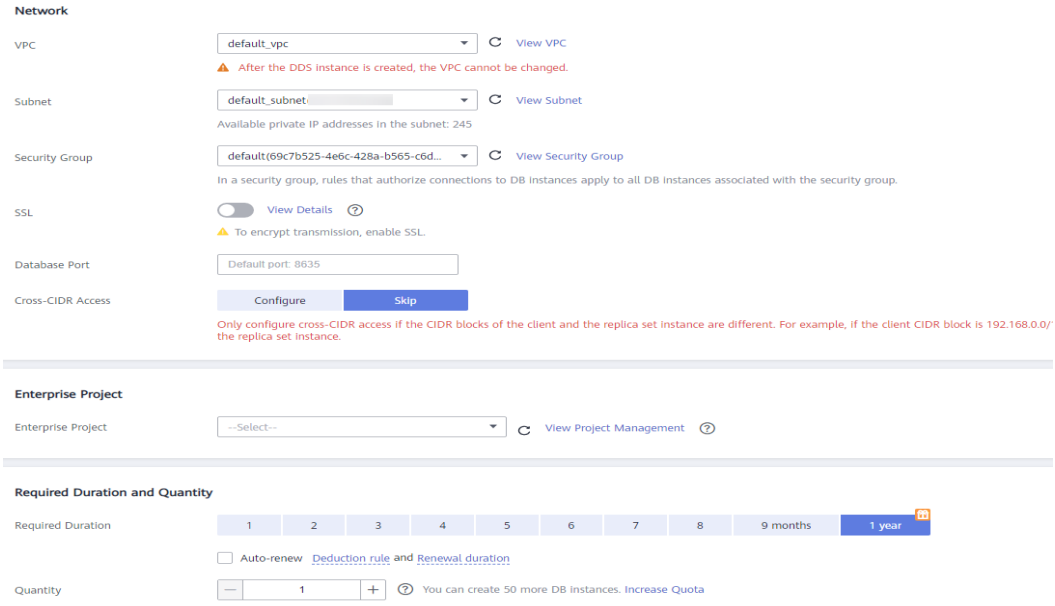
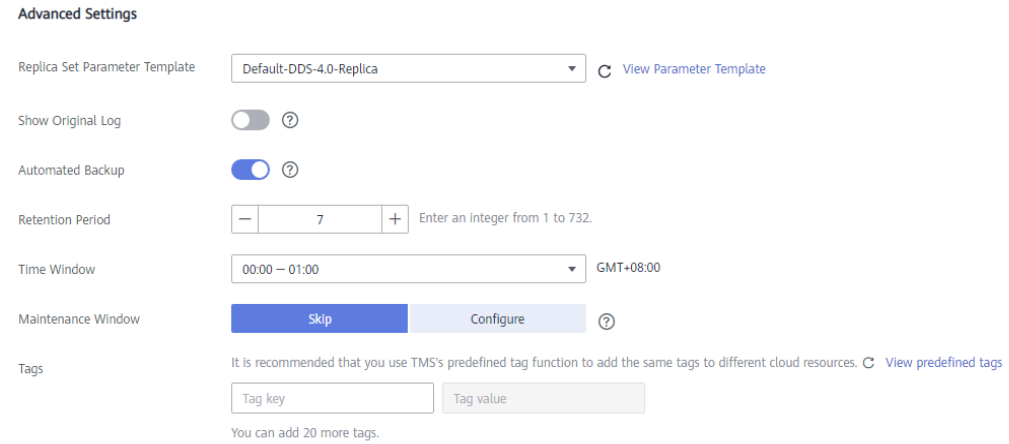



**Figura 6-24** Configurações avançadas




7. Na página exibida, confirme os detalhes da instância.
   - Para instâncias anuais/mensais
     - Se você precisar modificar as especificações, clique em **Previous** para retornar à página anterior.
     - Se você não precisar modificar as especificações, leia e concorde com o contrato de serviço e clique em **Pay Now** para ir para a página de pagamento e concluir o pagamento.
   - Para instâncias de pagamento por uso
     - Se você precisar modificar as especificações, clique em **Previous** para retornar à página anterior.
     - Se você não precisar modificar as especificações, leia e concorde com o contrato de serviço e clique em **Submit** para começar a criar a instância.
8. Depois que uma instância DDS for criada, você poderá exibi-la e gerenciá-la na página **Instances**.

- Quando uma instância está sendo criada, o status exibido na coluna **Status** é **Creating**. Este processo leva cerca de 15 minutos. Após a conclusão da criação, o status muda para **Available**.
- As instâncias anuais/mensais que foram compradas em lotes têm as mesmas especificações, exceto o nome e o ID da instância.

## Passo 2: vincular um EIP

1. Acesse o **console de gerenciamento**.
2. Clique em no canto superior esquerdo e selecione uma região e um projeto.
3. Clique em no canto superior esquerdo da página e escolha **Databases** > **Document Database Service**.
4. Na página **Instances**, clique na instância. A página **Basic Information** é exibida.
5. Na área **Node Information**, localize a linha que contém o nó principal e clique em **Bind EIP**.
6. Na caixa de diálogo exibida, selecione o EIP comprado e clique em **OK**.
7. Depois que a vinculação for bem-sucedida, visualize o EIP na área **Node Information**.

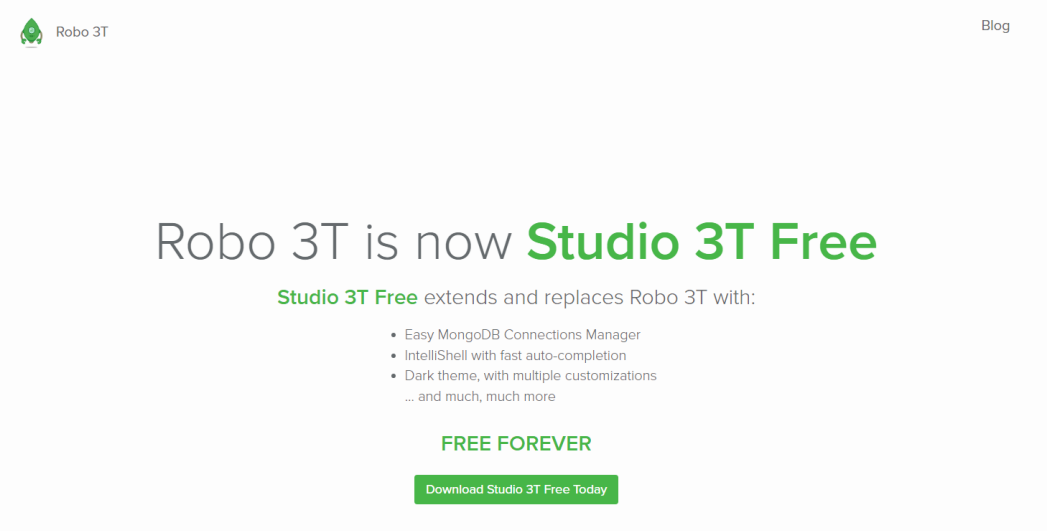
## Passo 3: configurar um grupo de segurança

1. Na área **Network Information** na página **Basic Information**, verifique a porta do banco de dados da instância de BD.
2. Na área **Network Information**, clique no nome do grupo de segurança.
3. Na página **Security Groups**, clique no nome do grupo de segurança.
4. Clique na guia **Inbound Rules** e clique em **Add Rule**. Na caixa de diálogo exibida, adicione uma regra de entrada para a porta do banco de dados.

## Passo 4: conectar-se a uma instância do DDS.

1. Acesse o endereço de download do Robo 3T **https://robomongo.org/download** e clique em **Download Studio 3T Free Today**.

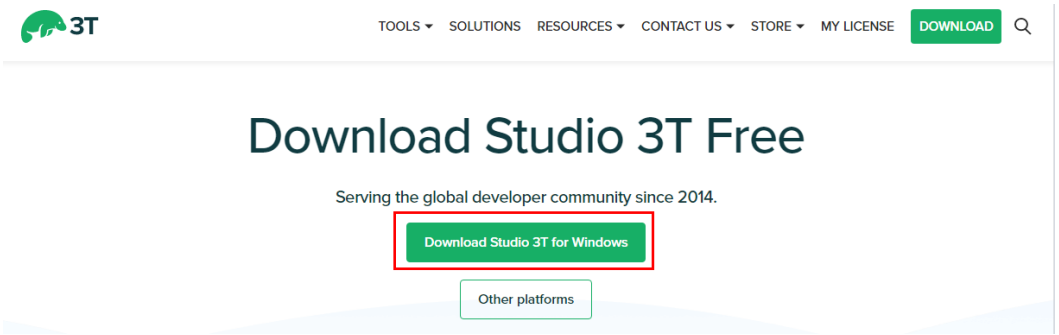
**Figura 6-25** Página de download



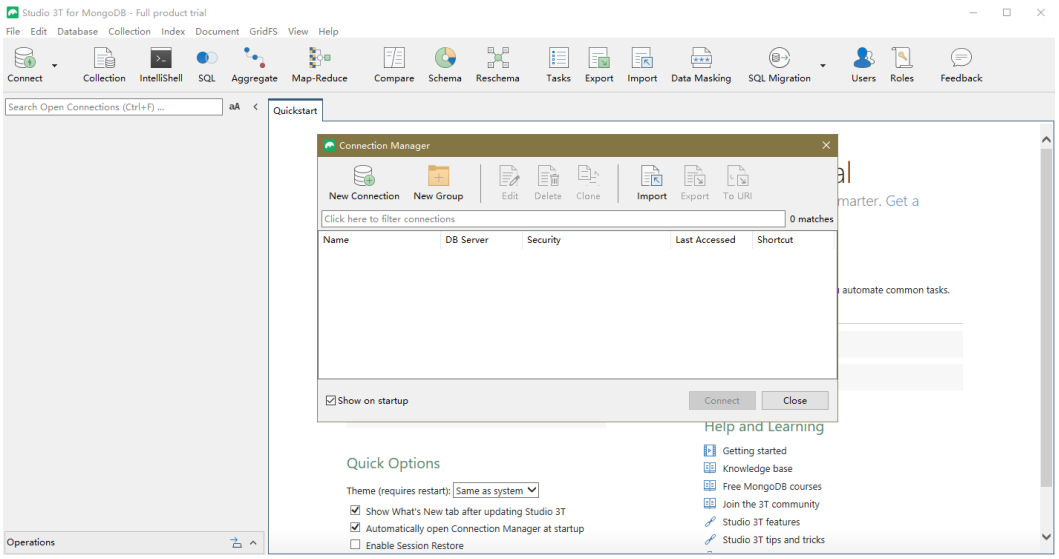
2. Na caixa de diálogo exibida, insira as informações necessárias e clique em **Download Studio 3T for Windows** para baixar **studio-3t-x64.zip**.

**Figura 6-26** Baixar Robo 3T




3. Descompacte o pacote baixado e clique duas vezes no arquivo **studio-3t-x64.exe** no diretório descompactado para iniciar a instalação.
4. Após a conclusão da instalação, inicie a ferramenta, conforme mostrado na **Figura 6-27**.

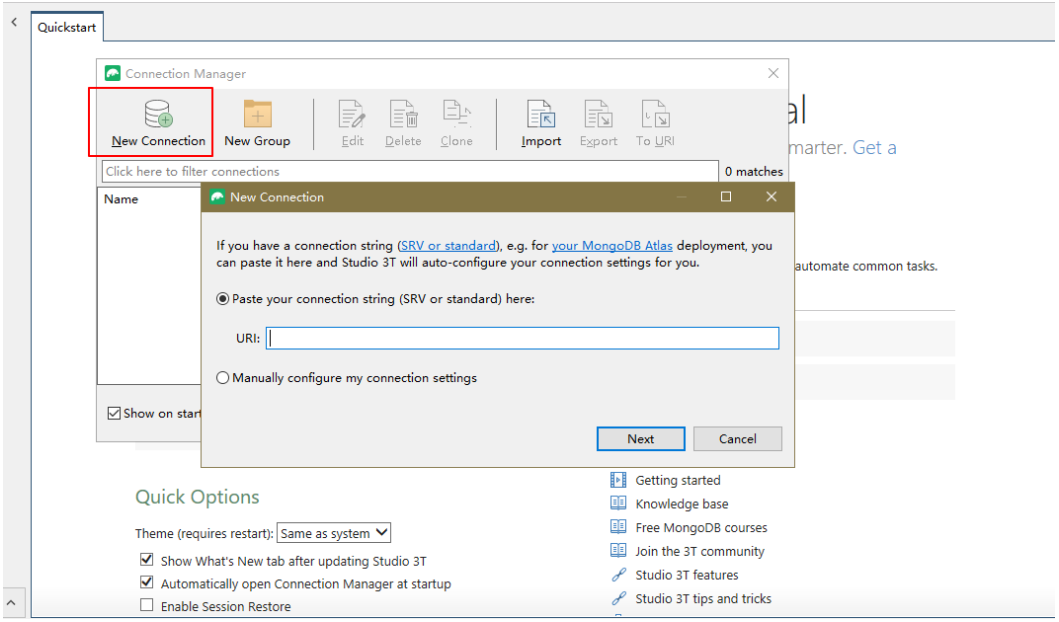
**Figura 6-27** Janela principal




5. Na página **Connection Manager**, clique em **New Connection**.

**Figura 6-28** Gerenciador de conexões




6. Conecte-se a uma instância de BD **automaticamente** ou **manualmente**.

– Método 1: conectar-se a uma instância de BD automaticamente.

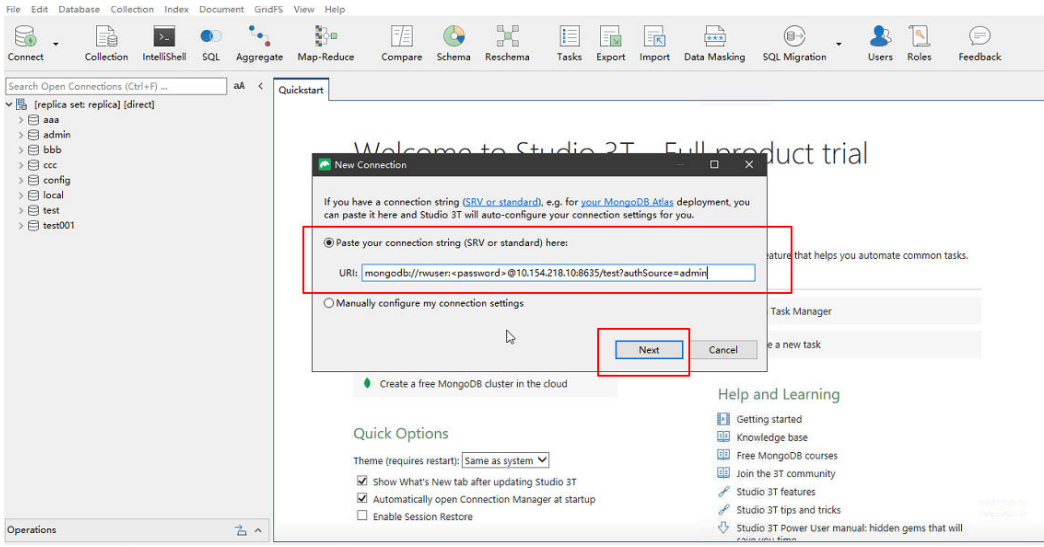
i. Na caixa de diálogo exibida, insira o URI, substitua **<password>** e clique em **Next**.

NOTA

Como obter o URI:

Na página **Instances**, clique no nome da instância de BD de destino. Na página **Basic Information**, clique em **Connections**. Na área **Public Connection**, obtenha o endereço de conexão pública a partir de **Address**.

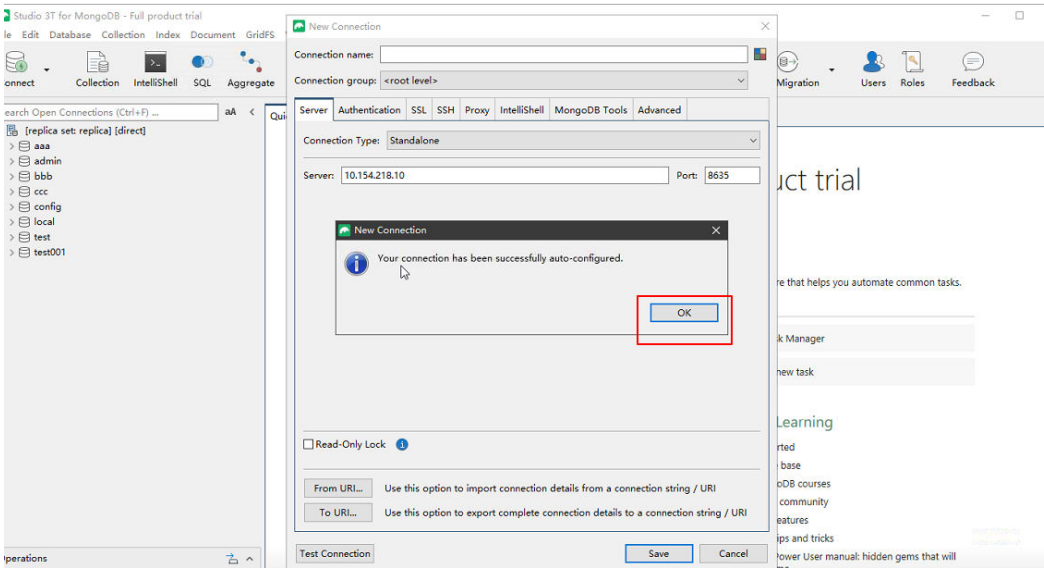
**Figura 6-29** Inserir o URI




ii. Na guia **Server**, clique em **OK** na caixa de diálogo exibida.

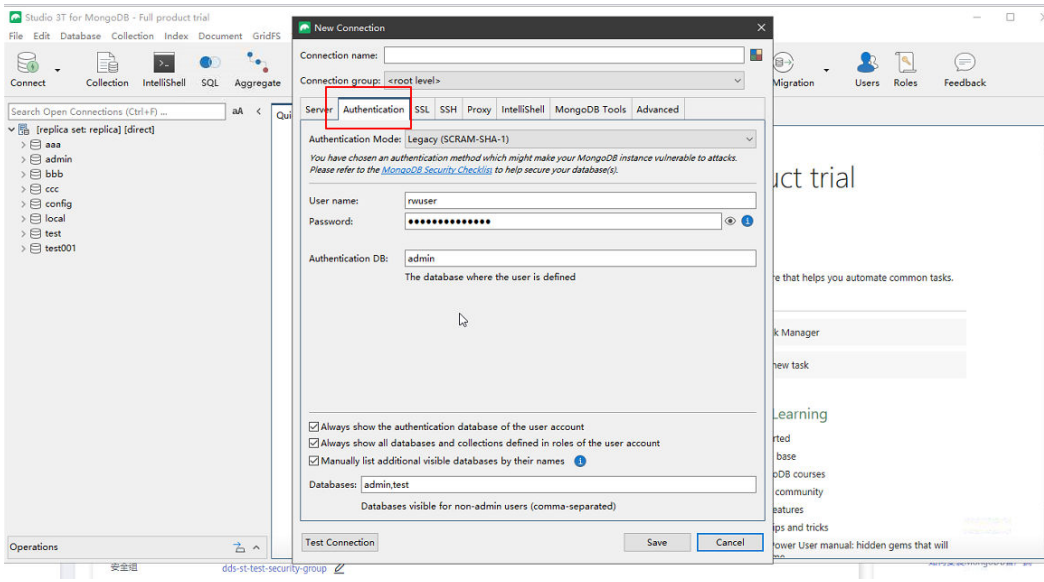
  

**Figura 6-30** Servidor




iii. Clique na guia **Authentication**.

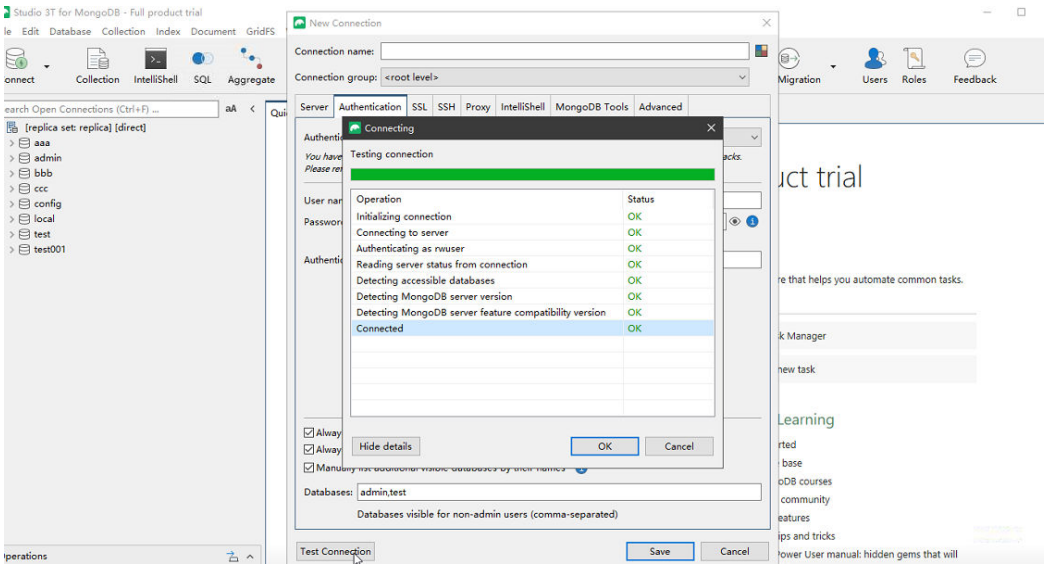
**Figura 6-31** Autenticação




iv. Clique em **Test Connection** para verificar se a conexão foi bem-sucedida.

**Figura 6-32** Conexão de teste



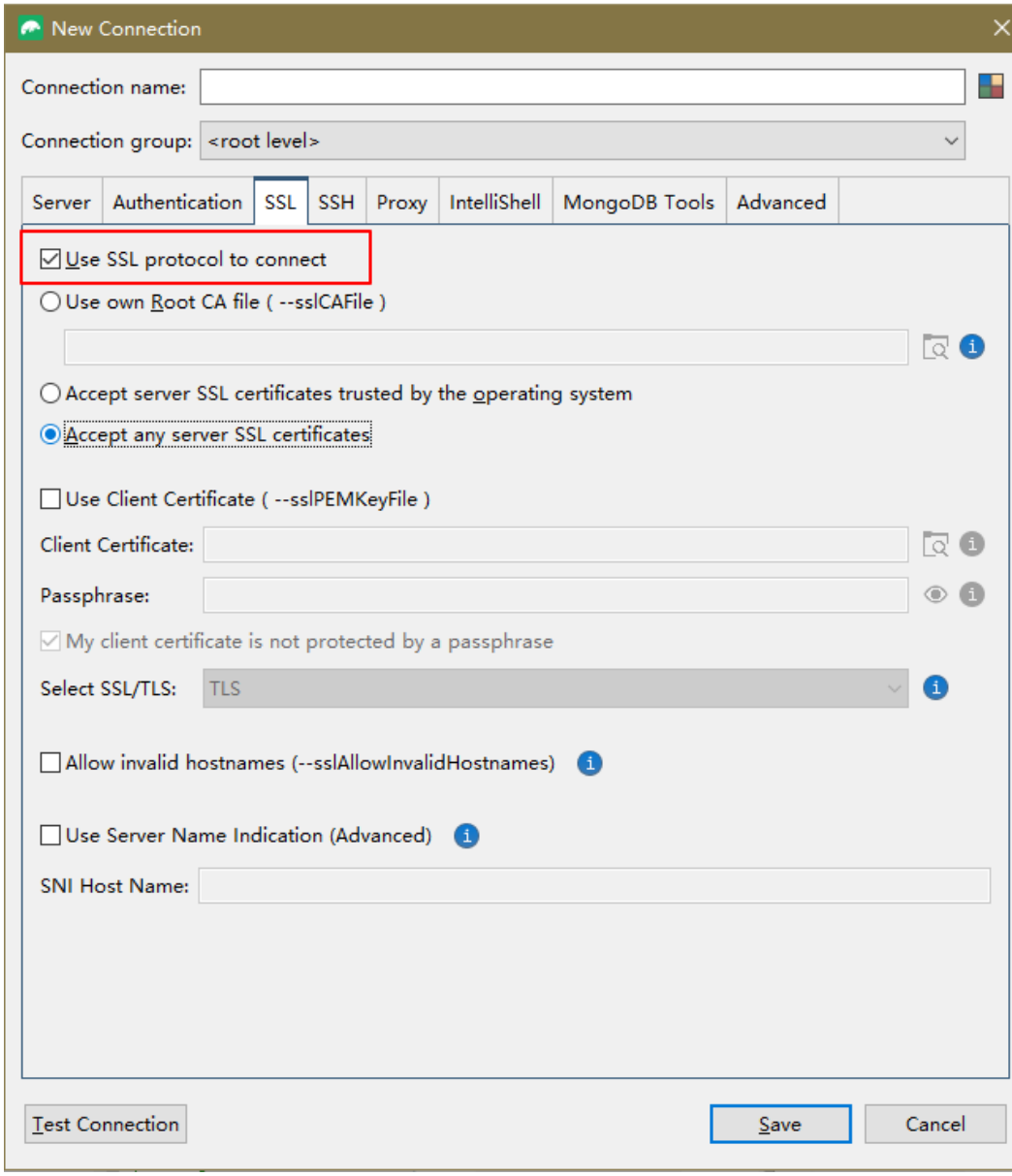

v. Clique na guia **SSL** e selecione **Use SSL protocol to connect**.

NOTA

Se a criptografia de dados SSL estiver desativada, pule esta etapa e vá para **6.viii**.

**Figura 6-33** SSL




vi. Selecione **Use own Root CA file (--sslCAFile)**, importe o certificado e selecione **Allow invalid hostnames**.

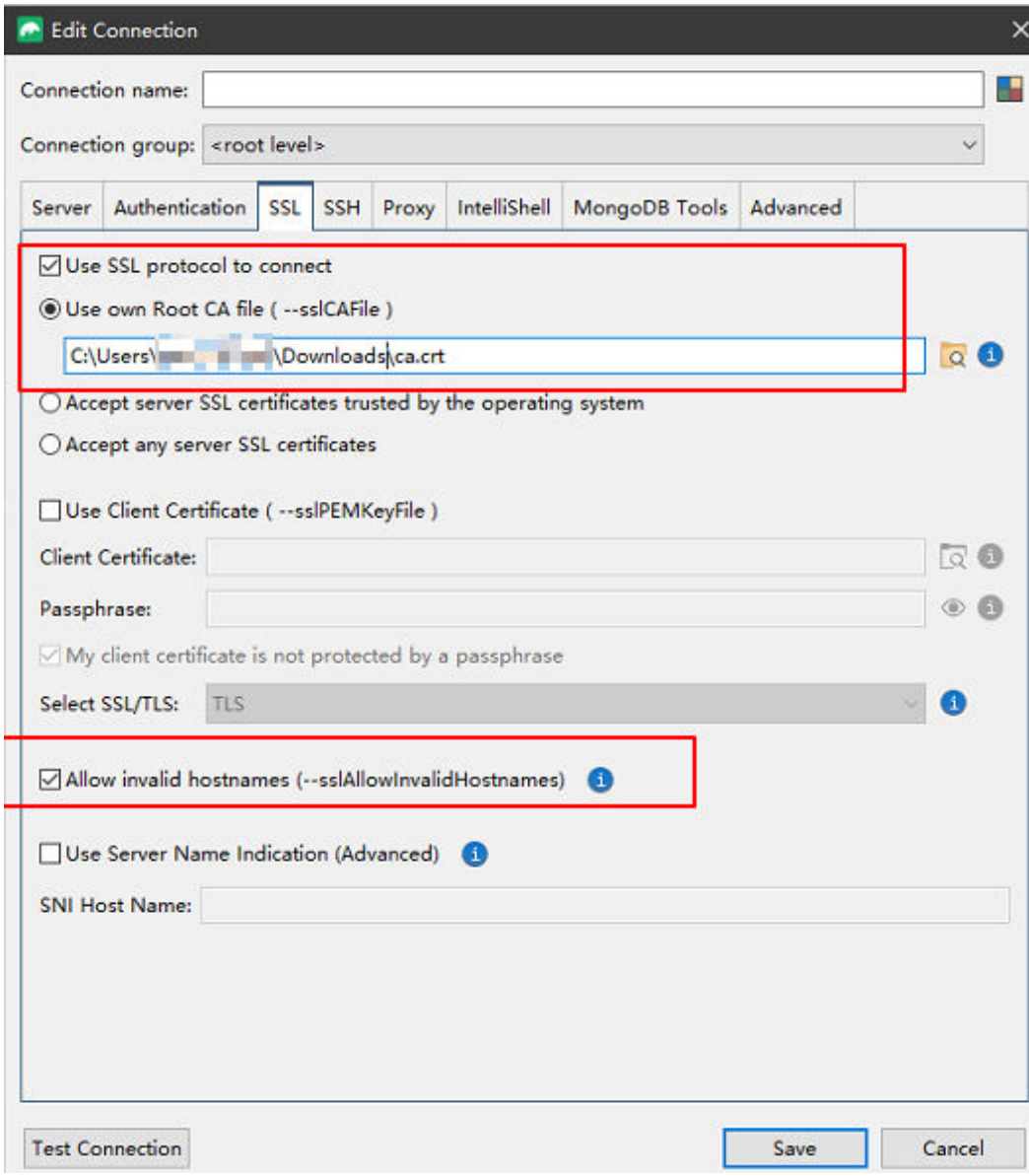
NOTA

Baixe o certificado SSL e verifique o certificado antes de se conectar aos bancos de dados.

Na página **Instances**, clique no nome da instância de BD de destino. Na área **DB Information** da página **Basic Information**, clique em no campo **SSL** para baixar certificado raiz ou do pacote de certificados.

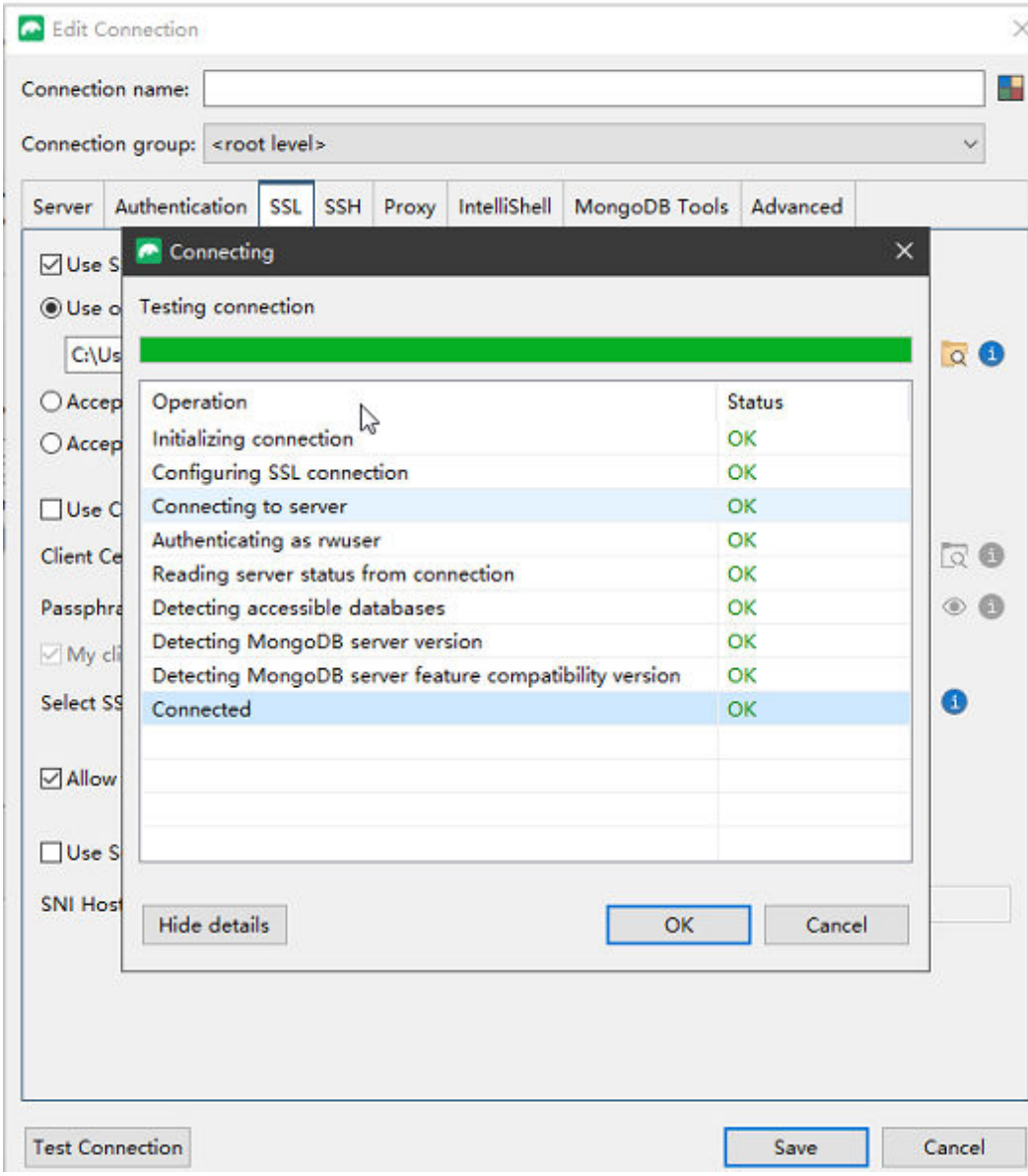
**Figura 6-34** Inserir informações de SSL




vii. Clique em **Test Connection** para verificar se a conexão foi bem-sucedida.

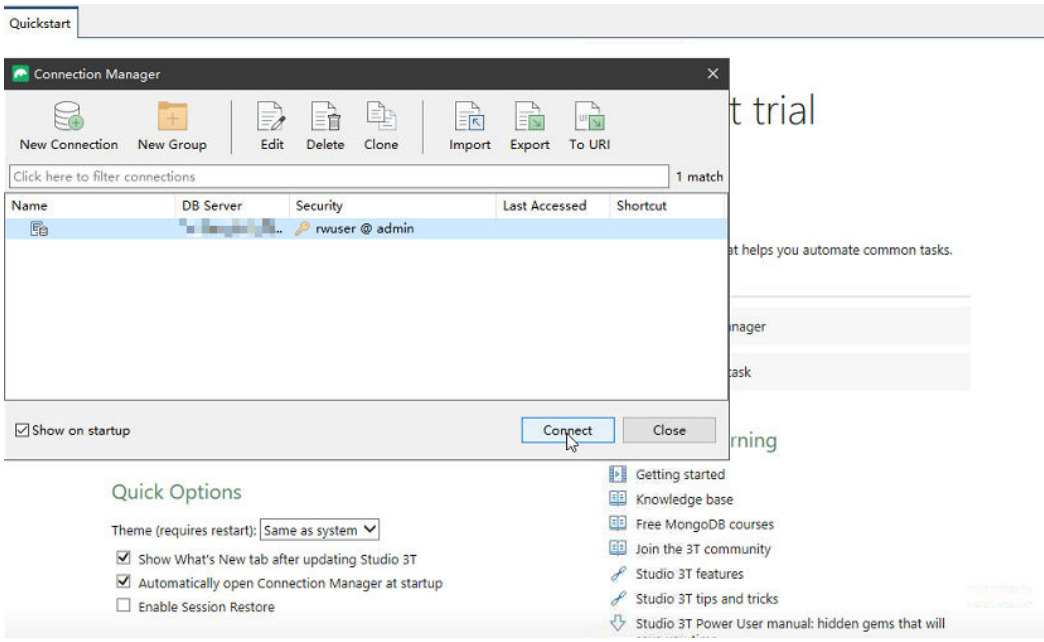
**Figura 6-35** Verificar a conexão SSL




viii. Depois que a verificação for bem-sucedida, clique em **Save**.

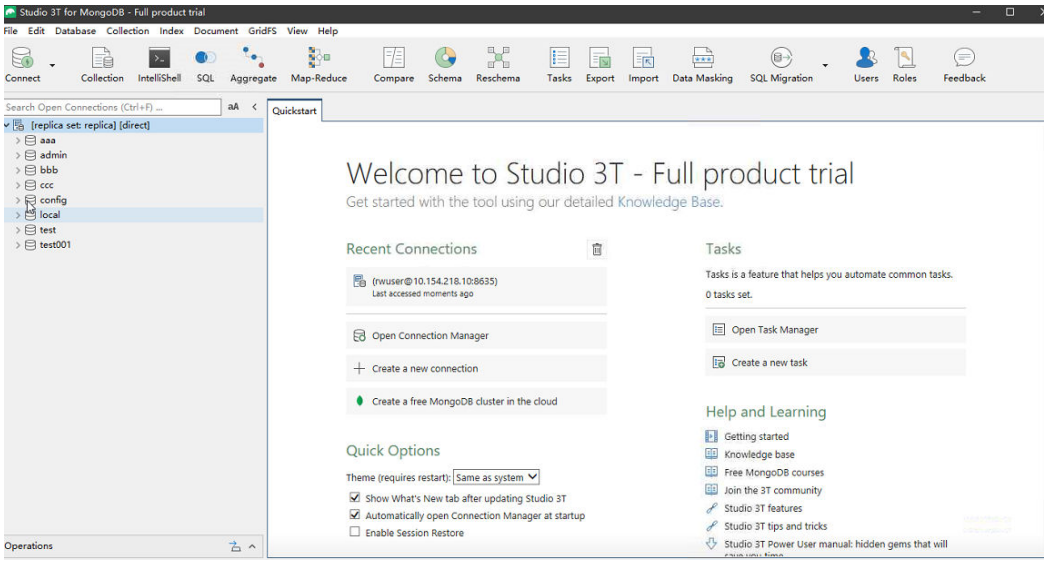
  

**Figura 6-36** Informações de conexão




ix. Na página de informações de conexão, clique em **Connect** para se conectar à instância do conjunto de réplicas. Depois que a instância do conjunto de réplicas for conectada com êxito, **Figura 6-37** é exibida.

**Figura 6-37** Conexão bem sucedida

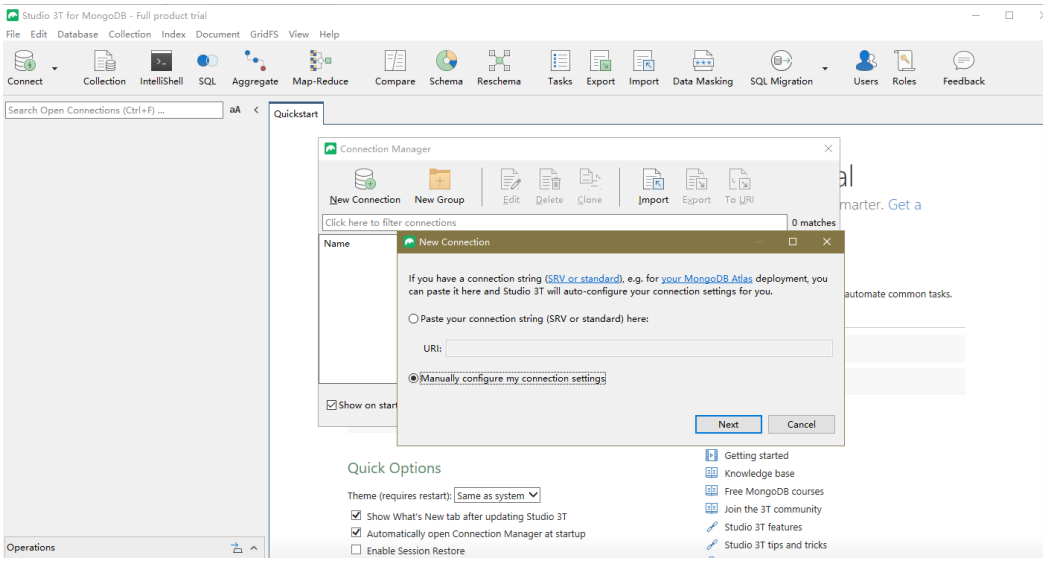



– **Método 2: conectar-se a uma instância de BD manualmente.**

i. Na caixa de diálogo exibida, selecione **Manually configure my connection settings** e clique em **Next**.

**Figura 6-38** Modo de conexão manual




ii. Na guia **Server**, defina **Server** e **Port**.

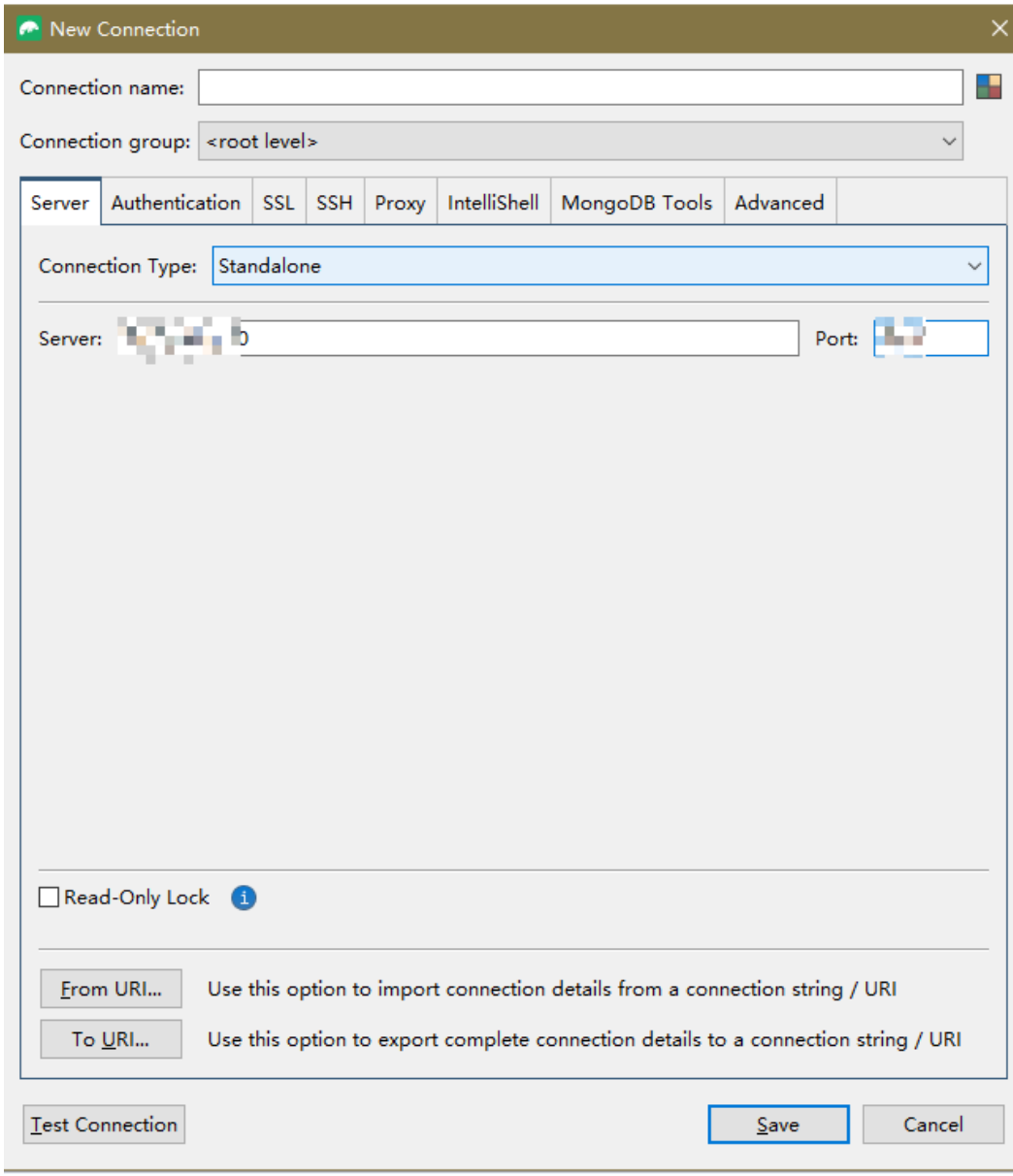
NOTA

**Server**: EIP.

**Port**: porta do banco de dados.

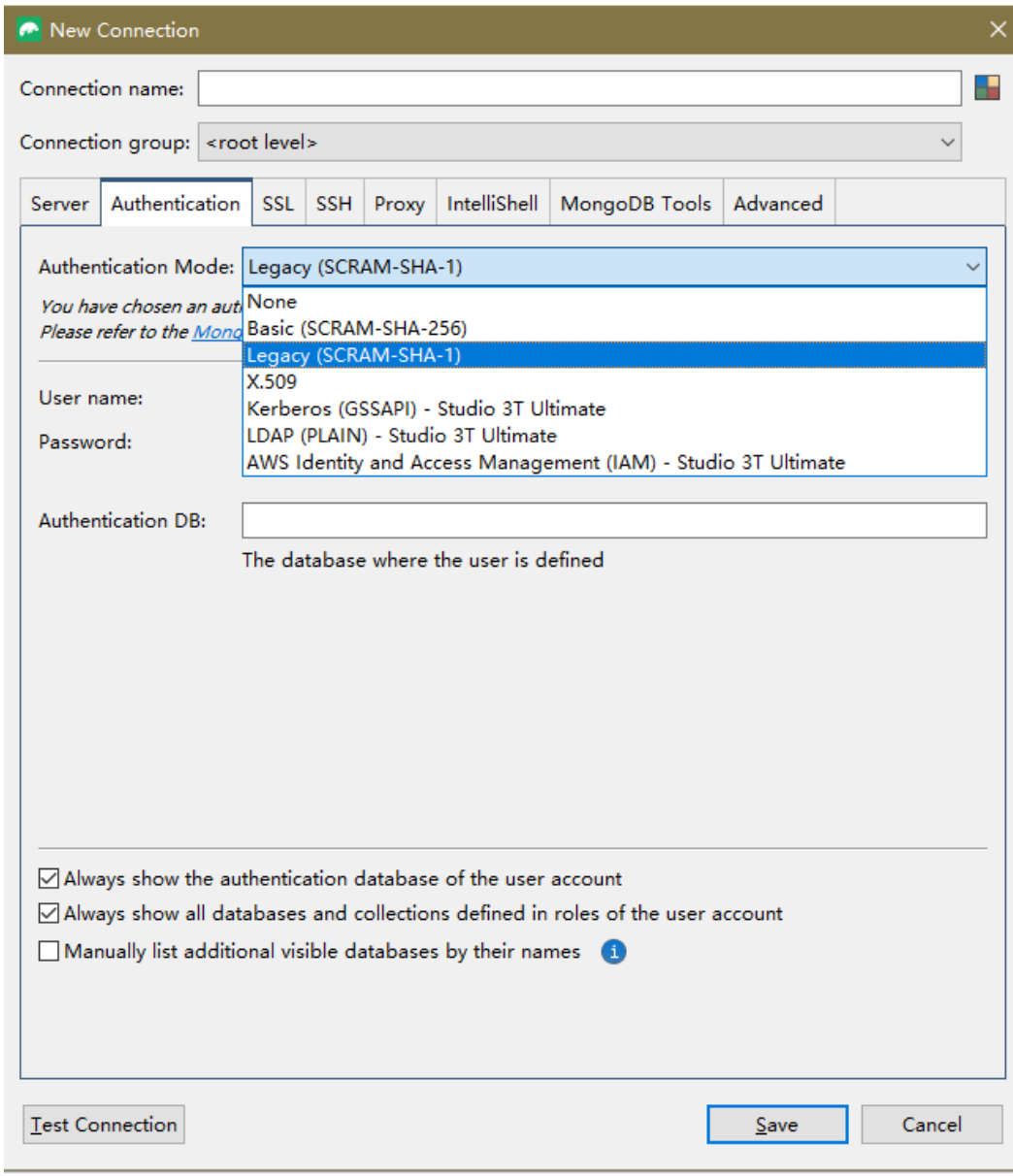
**Figura 6-39** Servidor




iii. Clique na guia **Authentication** e selecione **Legacy(SCRAM-SHA-1)**.

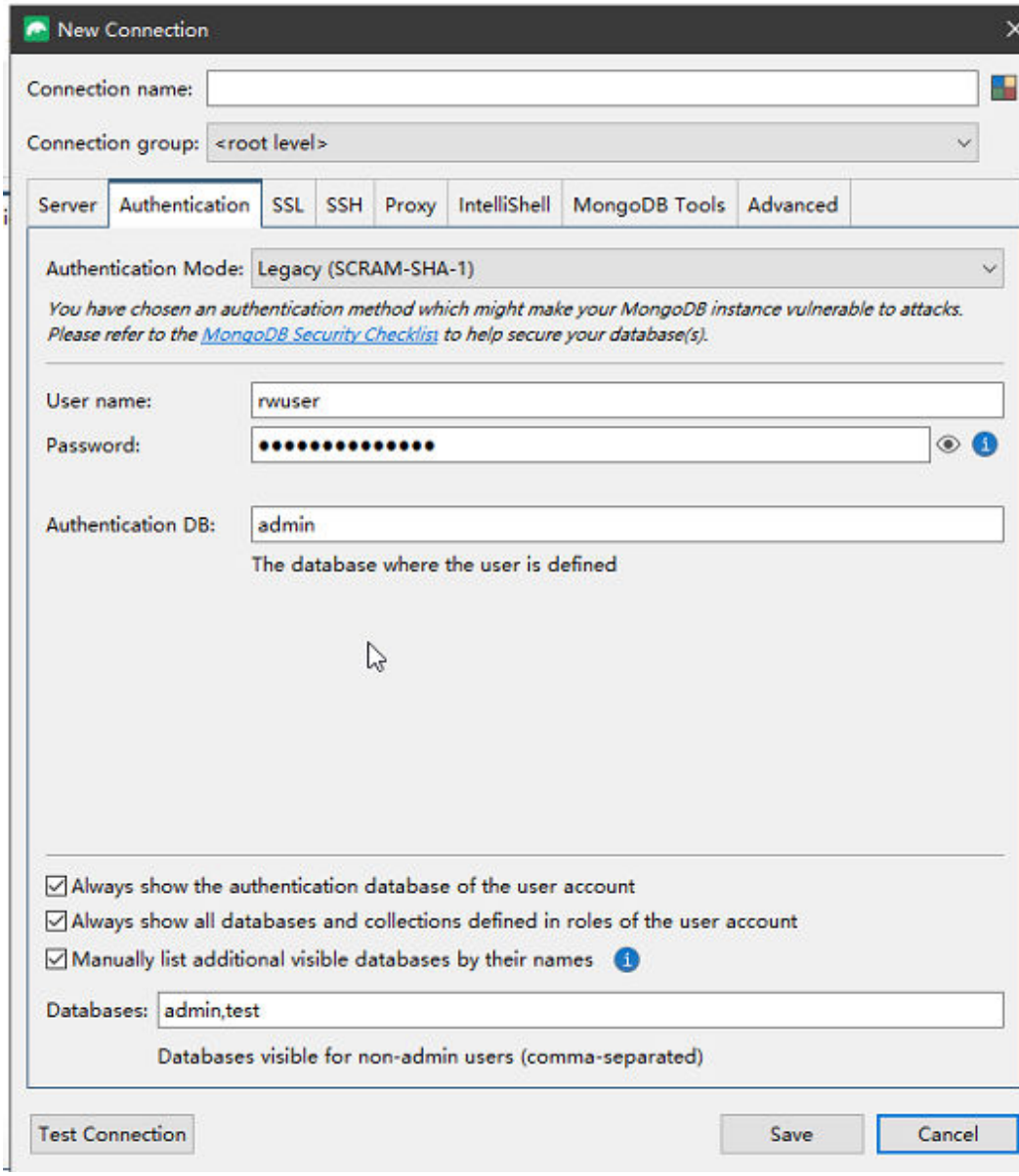
**Figura 6-40** Autenticação




iv. Defina **User name**, **Password** e **Authentication DB**.

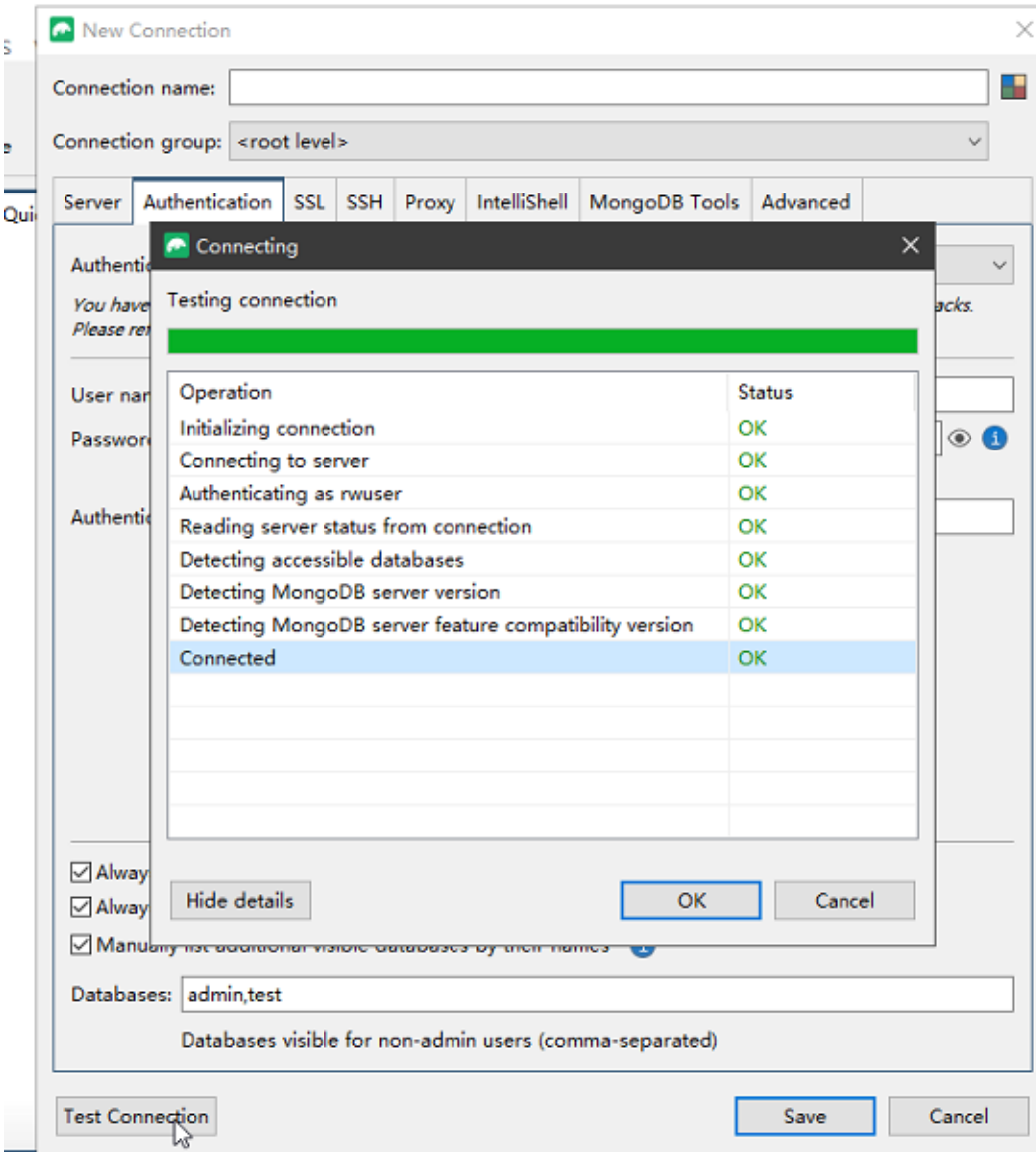
**Figura 6-41** Autenticação




v. Clique em **Test Connection** para verificar se a conexão foi bem-sucedida.

**Figura 6-42** Conexão de teste



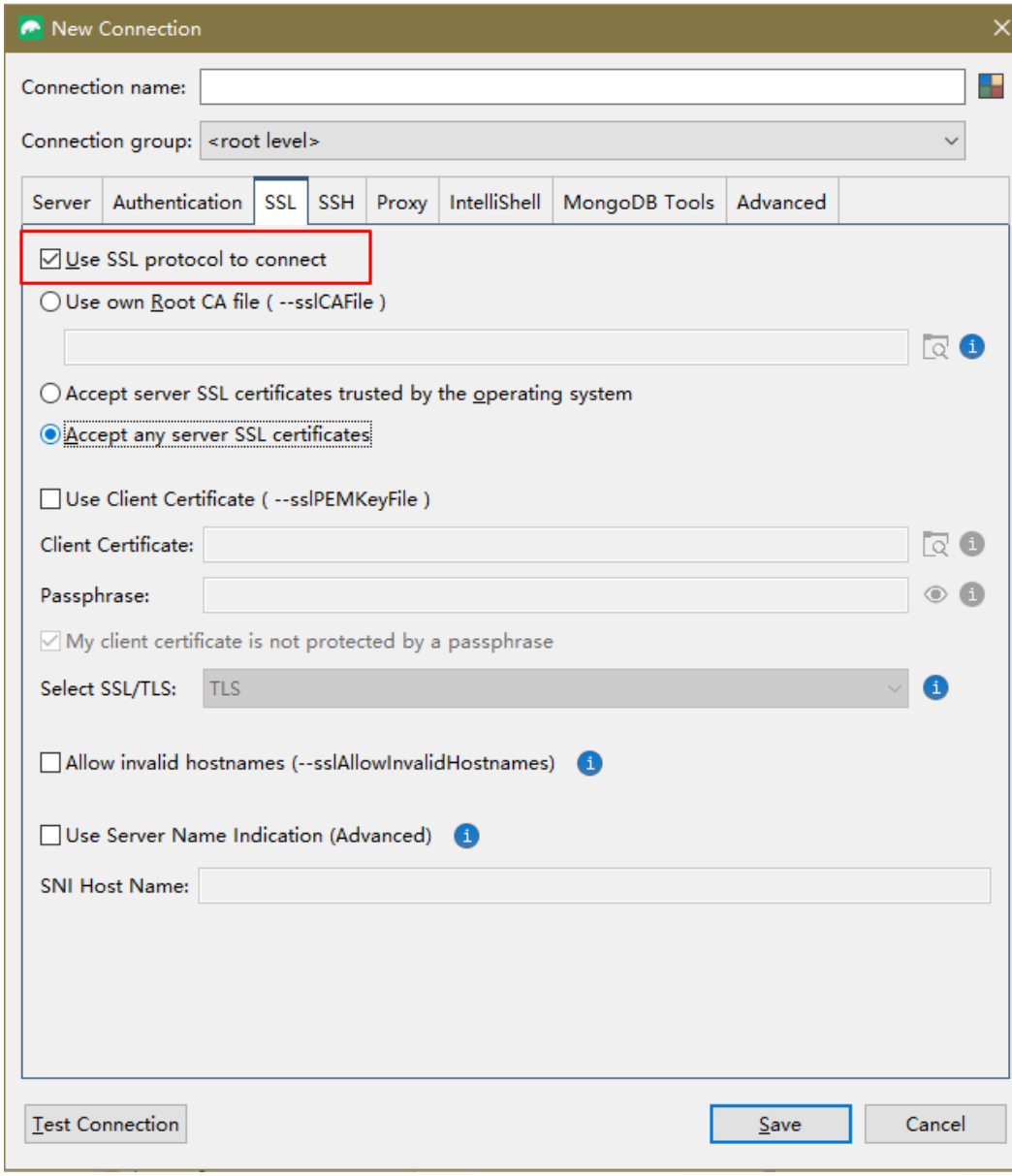

vi. Clique na guia **SSL** e selecione **Use SSL protocol to connect**.

NOTA

Se a criptografia de dados SSL estiver desativada, pule esta etapa e vá para **6.ix**.

**Figura 6-43** SSL




vii. Selecione **Use own Root CA file (--sslCAFile)**, importe o certificado e selecione **Allow invalid hostnames**.

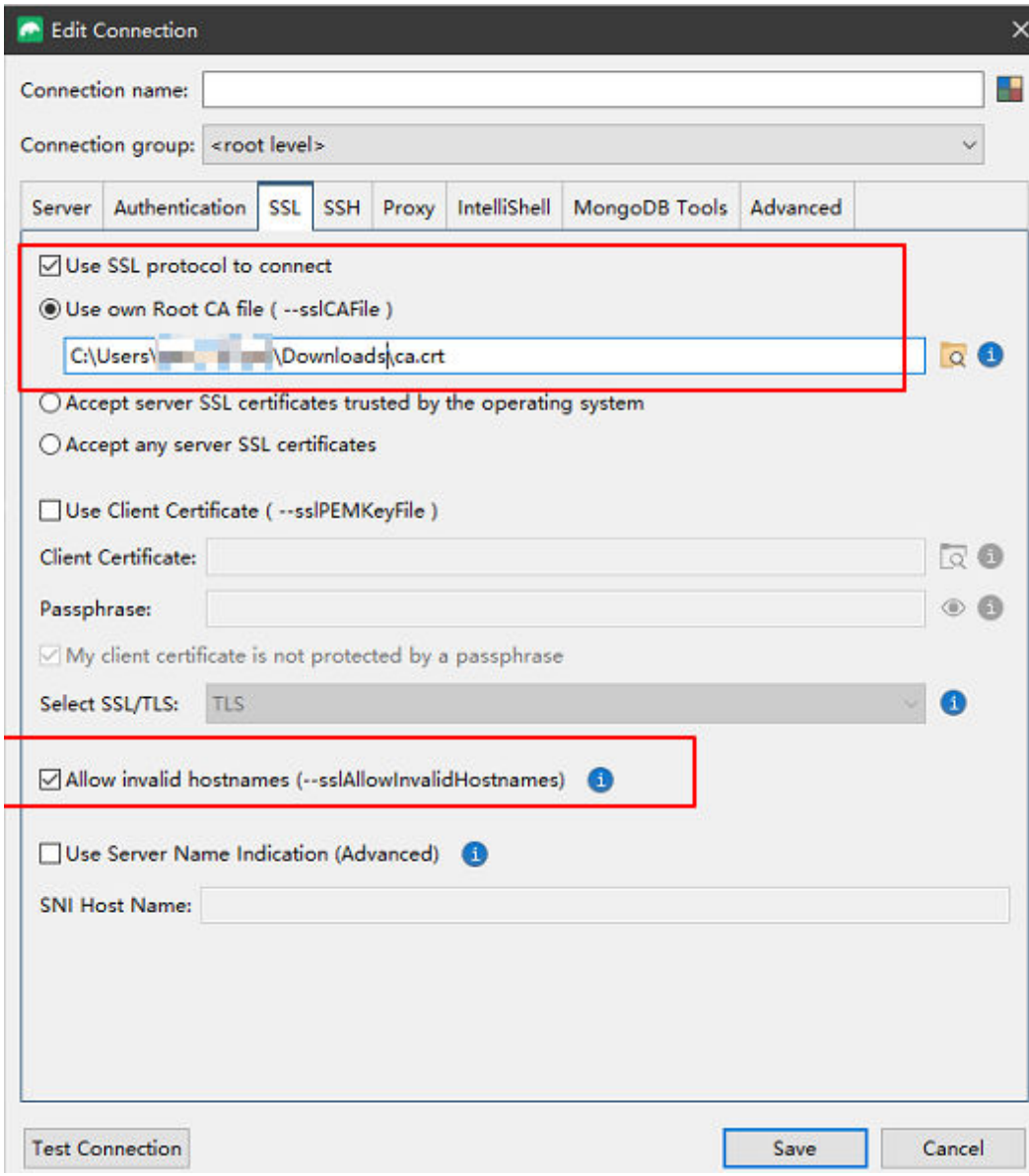
NOTA

Baixe o certificado SSL e verifique o certificado antes de se conectar aos bancos de dados.

Na página **Instances**, clique no nome da instância de BD de destino. Na área **DB Information** da página **Basic Information**, clique em no campo **SSL** para baixar certificado raiz ou do pacote de certificados.

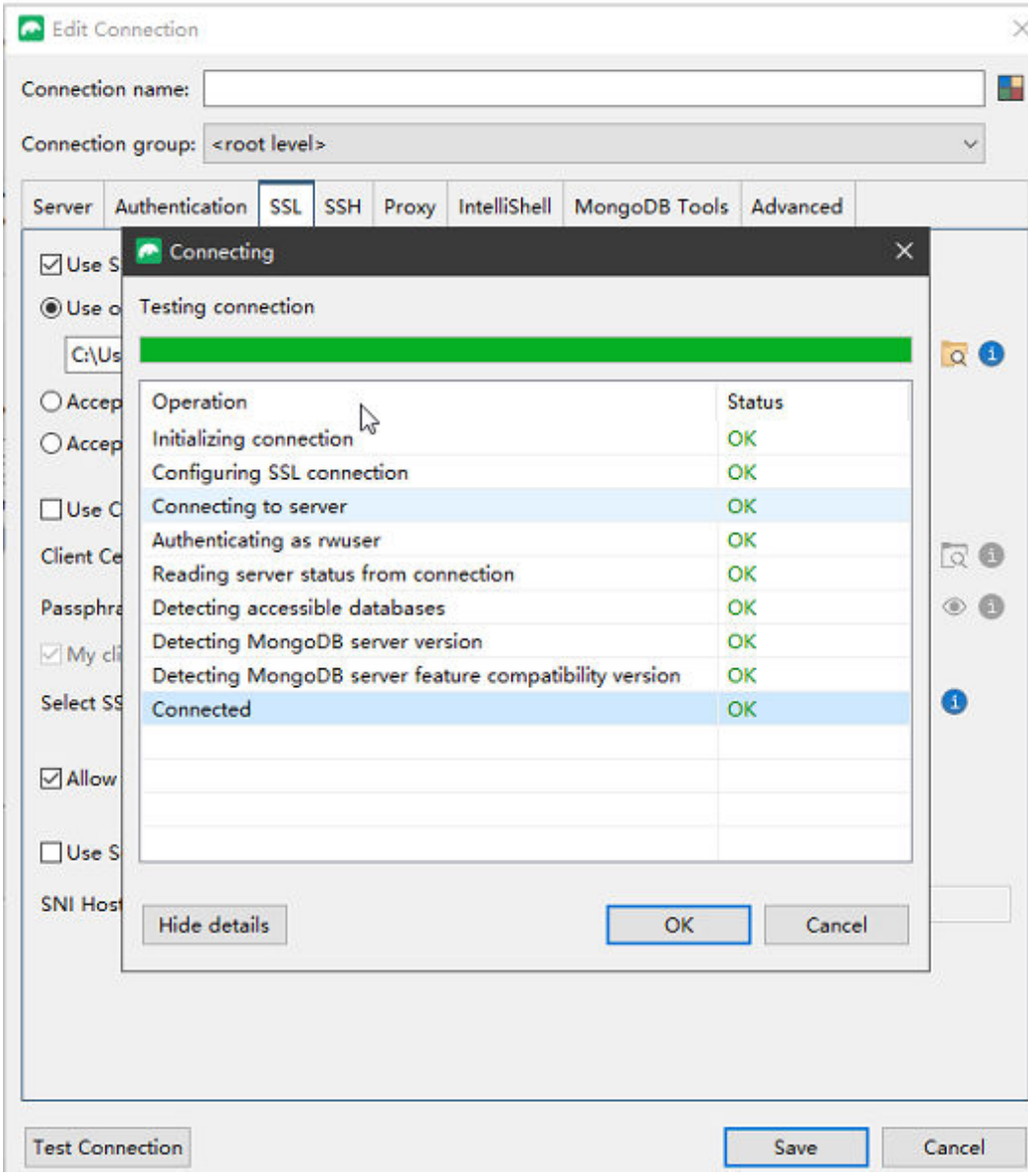
**Figura 6-44** Inserir informações de SSL




viii. Clique em **Test Connection** para verificar se a conexão foi bem-sucedida.

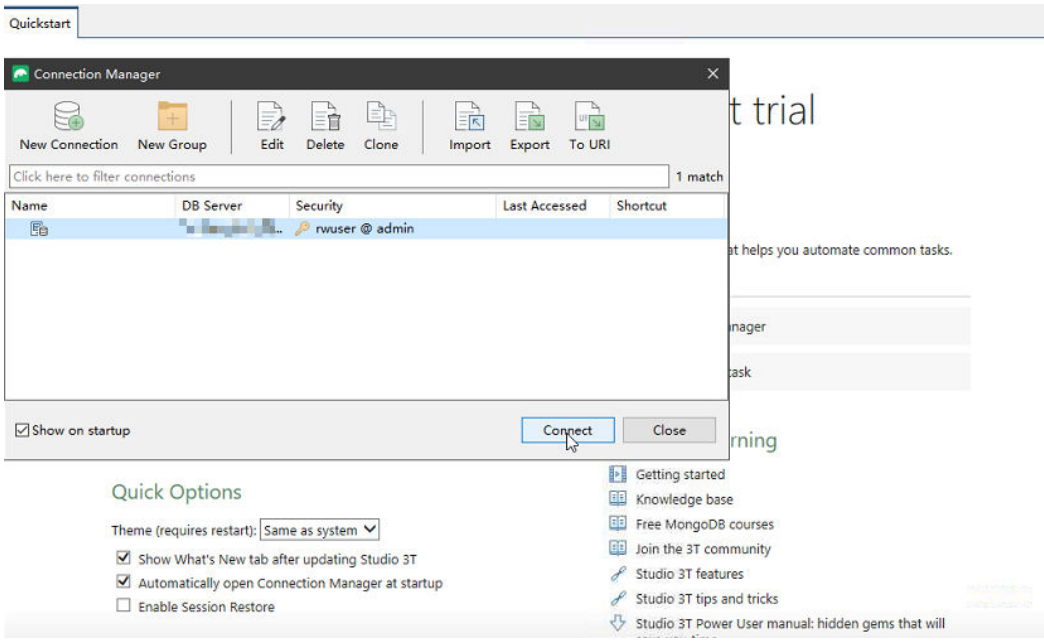
**Figura 6-45** Verificar a conexão SSL




ix. Depois que a verificação for bem-sucedida, clique em **Save**.

**Figura 6-46** Informações de conexão




x. Na página de informações de conexão, clique em **Connect** para se conectar à instância do conjunto de réplicas. Depois que a instância do conjunto de réplicas for conectada com êxito, **Figura 6-47** é exibida.

**Figura 6-47** Conexão bem sucedida