Document Database Service

qs-dds

Issue	01
Date	2023-01-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Overview....1

2 Getting Started with Clusters....3

2.1 Buying a Cluster Instance....3

2.1.1 Quick Config....3

2.1.2 Custom Config....9

2.2 Connecting to a Cluster Instance....21

2.2.1 Connection Methods....21

2.2.2 (Recommended) Connecting to Cluster Instances Through DAS....22

2.2.2.1 Overview....22

2.2.2.2 Connecting to a Cluster Instance Through DAS....23

2.2.3 Connecting to a Cluster Instance over a Private Network....23

2.2.3.1 Configuring Security Group Rules....23

2.2.3.2 Connecting to a Cluster Instance Using Mongo Shell (Private Network)....27

2.2.3.3 Connecting to Read Replicas Using Mongo Shell....37

2.2.4 Connecting to a Cluster Instance over a Public Network....42

2.2.4.1 Binding and Unbinding an EIP....42

2.2.4.2 Configuring a Security Group....45

2.2.4.3 Connecting to a Cluster Instance Using Mongo Shell (Public Network)....48

2.2.4.4 Connecting to a Cluster Instance Using Robo 3T....55

2.2.5 Connecting to a Cluster Instance Using Program Code....62

2.2.5.1 Java....62

2.2.5.2 Python....66

3 Getting Started with Replica Sets....67

3.1 Buying a Replica Set Instance....67

3.1.1 Quick Config....67

3.1.2 Custom Config....72

3.2 Connecting to a Replica Set Instance....84

3.2.1 Connection Methods....84

3.2.2 (Recommended) Connecting to Replica Set Instances Through DAS....85

3.2.2.1 Overview....85

3.2.2.2 Connecting to a Replica Set Instance Through DAS....86

3.2.3 Connecting to a Replica Set Instance over a Private Network....86

3.2.3.1 Configuring Security Group Rules 86
3.2.3.2 Connecting to a Replica Set Instance Using Mongo Shell (Private Network) 90
3.2.3.3 Connecting to Read Replicas Using Mongo Shell 102
3.2.4 Connecting to a Replica Set Instance over a Public Network 106
3.2.4.1 Binding and Unbinding an EIP 106
3.2.4.2 Configuring Security Group Rules 109
3.2.4.3 Connecting to a Replica Set Instance Using Mongo Shell (Public Network) 112
3.2.4.4 Connecting to a Replica Set Instance Using Robo 3T 119
3.2.5 Connecting to a Replica Set Instance Using Program Code 125
3.2.5.1 Java 125
3.2.5.2 Python 128
4 Getting Started with Single Nodes 130
4.1 Connecting to a Single Node Instance 130
4.1.1 Connection Methods 130
4.1.2 (Recommended) Connecting to a Single Node Instance Through DAS 131
4.1.2.1 Overview 131
4.1.2.2 Connecting to a Single Node Instance Through DAS 131
4.1.3 Connecting to a Single Node Instance over a Private Network 132
4.1.3.1 Configuring a Security Group 132
4.1.3.2 Connecting to a Single Node Instance Using Mongo Shell (Private Network) 136
4.1.4 Connecting to a Single Node Instance over a Public Network 140
4.1.4.1 Binding and Unbinding an EIP 140
4.1.4.2 Configuring a Security Group 142
4.1.4.3 Connecting to a Single Node Instance Using Mongo Shell (Public Network) 145
4.1.4.4 Connecting to a Single Node Instance Using Robo 3T 150
4.1.5 Connecting to a Single Node Instance Using Program Code 156
4.1.5.1 Java 156
4.1.5.2 Python 160
5 Logging In to and Logging Out of the DDS Console 161
6 Example: Buying and Connecting to a DDS Instance 163
6.1 Connecting to a DB Instance Using Mongo Shell 163
6.2 Connecting to a DDS Instance Through an EIP 180
7 Getting Started with Common Practices 198
A Change History 201

1 Overview

You can create and connect to instances on the management console.

Process

To create and use an instance, you need to perform the operations described in the following flowchart.

Figure 1-1 Process

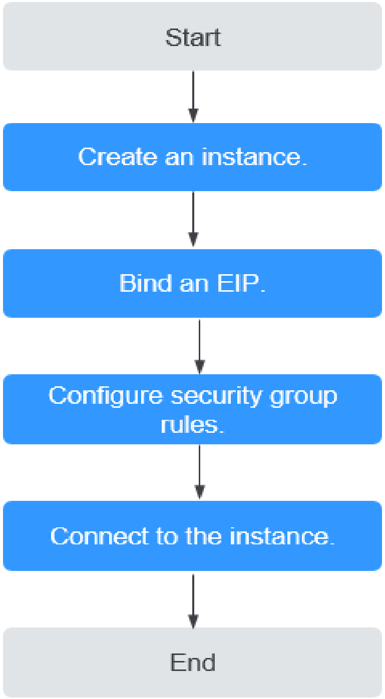


Table 1-1 Operation process

Procedure	Description	Reference
Creating an instance	You can customize the computing resources and storage available to your instance.	• **Buying a Cluster Instance** • **Buying a Replica Set Instance**
Binding an EIP	(Optional) When connecting to an instance from the Internet, you need to configure an EIP.	**Binding and Unbinding an EIP**
Configuring security group rules	(Optional) Add the devices that access the instance to the security group associated with the instance, so you can access the instance from the devices. • If you access the instance from an ECS that is in a different security from the instance over a private network, you need to configure the security group rule. • If you connect to an instance over a public network, you need to configure security group rules.	• **Configuring Security Group Rules (Private Network)** • **Configuring Security Group Rules (Public Network)**
Connecting to an instance	You can connect to instances through DAS, a private network, a public network, or program code.	• **Connecting to a Cluster Instance** • **Connecting to a Replica Set Instance** • **Connecting to a Single Node Instance**

2 Getting Started with Clusters

2.1 Buying a Cluster Instance

2.1.1 Quick Config

This section describes how to quickly purchase a cluster instance on the management console. DDS helps you quickly configure and create a cluster within several minutes.

Precautions

Each account can create up to 10 cluster instances.

Prerequisites

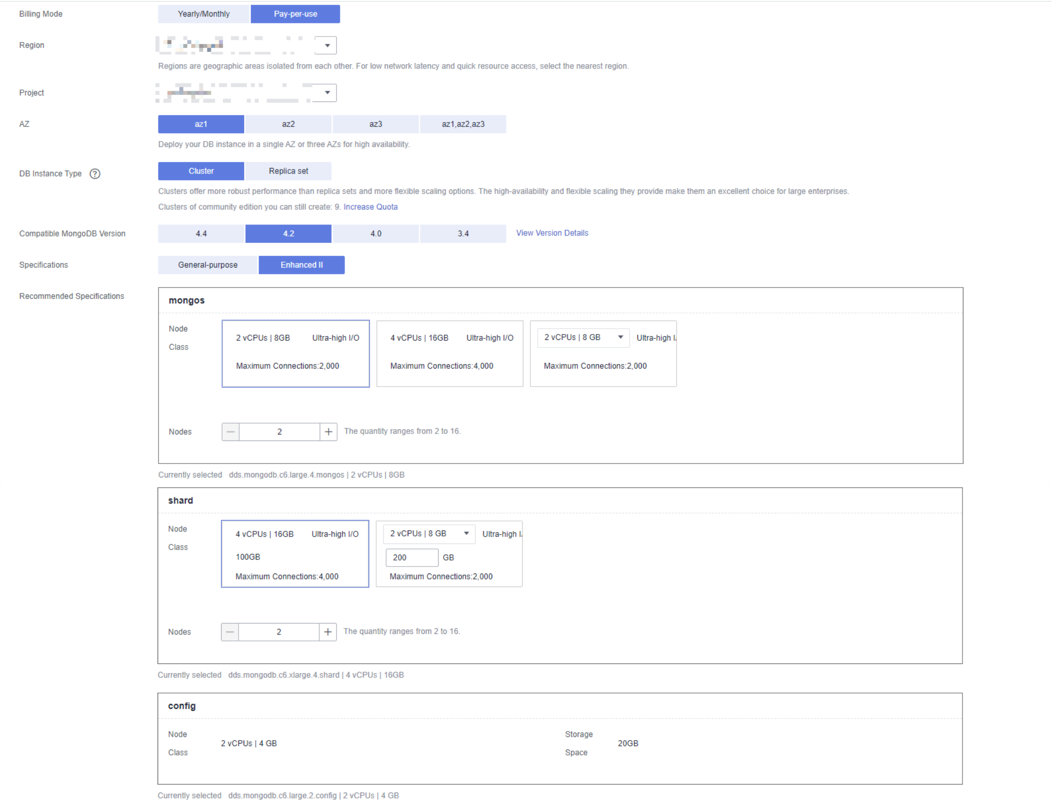
- You have **registered a Huawei ID and enabled Huawei Cloud services**.
- Your account balance is greater than or equal to $0 USD.
- To display whether the disk is encrypted in the DB instance list, submit a service ticket. In the upper right corner of the management console, choose **Service Tickets > Create Service Ticket**.

Procedure

Step 1 Go to the **Guick Config** page.

Step 2 On the displayed page, select a billing mode and configure information about your DB instance. Then, click **Next**.

Figure 2-1 Basic configurations



Billing Mode: Yearly/Monthly [✓ Pay-per-use]

Region: [redacted]

Regions are geographic areas isolated from each other. For low network latency and quick resource access, select the nearest region.

Project: [redacted]

AZ: [✓ az1] az2 az3 az1,az2,az3

Deploy your DB instance in a single AZ or three AZs for high availability.

DB Instance Type: [✓ Cluster] Replica set

Clusters offer more robust performance than replica sets and more flexible scaling options. The high-availability and flexible scaling they provide make them an excellent choice for large enterprises.

Clusters of community edition you can still create: 9. Increase Quota

Compatible MongoDB Version: 4.4 [✓ 4.2] 4.0 3.4 View Version Details

Specifications: General-purpose [✓ Enhanced II]

Recommended Specifications

mongos

Node Class: [✓ 2 vCPUs | 8GB Ultra-high I/O Maximum Connections:2,000] | 4 vCPUs | 16GB Ultra-high I/O Maximum Connections:4,000 | 2 vCPUs | 8 GB Ultra-high I. Maximum Connections:2,000

Nodes: 2 The quantity ranges from 2 to 16.

Currently selected dds.mongodb.c6.large.4.mongos | 2 vCPUs | 8GB

shard

Node Class: [✓ 4 vCPUs | 16GB Ultra-high I/O 100GB Maximum Connections:4,000] | 2 vCPUs | 8 GB Ultra-high I. 200 GB Maximum Connections:2,000

Nodes: 2 The quantity ranges from 2 to 16.

Currently selected dds.mongodb.c6.xlarge.4.shard | 4 vCPUs | 16GB

config

Node Class: 2 vCPUs | 4 GB

Storage Space: 20GB

Currently selected dds.mongodb.c6.large.2.config | 2 vCPUs | 4 GB

Table 2-1 Basic configurations

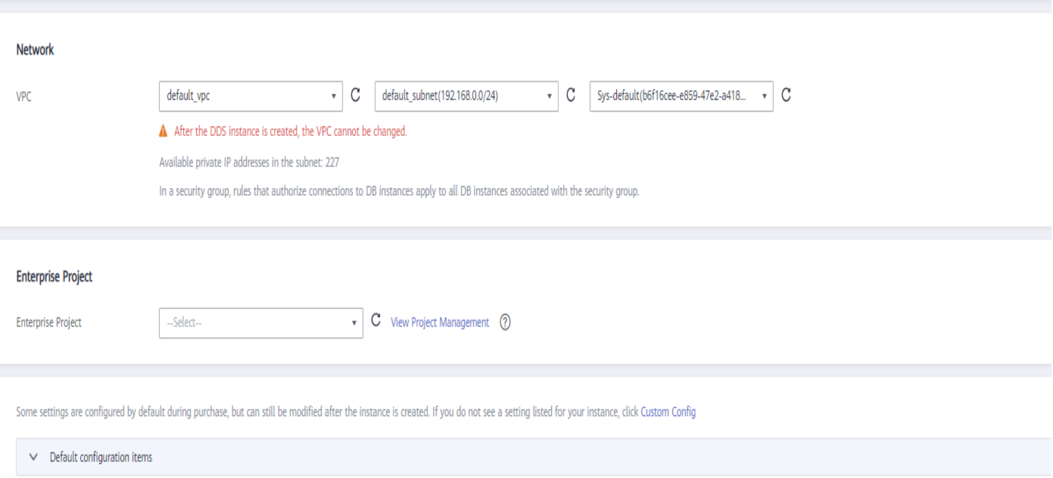
Parameter	Description
Billing Mode	Select a billing mode, **Yearly/Monthly** or **Pay-per-use**. ● For yearly/monthly instances – Specify **Required Duration**, and the system deducts the fees incurred from your account based on the service price. – If you do not expect to continue using the instance much after it expires, you can change the billing mode from yearly/monthly to pay-per-use. For details, see **Changing the Billing Mode from Yearly/Monthly to Pay-per-Use**. **NOTE** Instances billed on a yearly/monthly basis cannot be deleted. They can only be unsubscribed from. For details, see **Unsubscribing from a Yearly/Monthly Instance**. ● For pay-per-use instances – You are billed for usage based on how much time the service is in use. – If you expect to use the service extensively over a long period of time, you can change its billing mode from pay-per-use to yearly/monthly to reduce costs. For details, see **Changing the Billing Mode from Pay-per-Use to Yearly/Monthly**.

Parameter	Description
Region	The region where the resource is located. **NOTE** Instances deployed in different regions cannot communicate with each other through a private network, and you cannot change the region of an instance once it is purchased. Exercise caution when selecting a region.
Project	The project corresponds to the current region and can be changed.
AZ	An AZ is a part of a region with its own independent power supply and network. AZs are physically isolated but can communicate through internal network connections. Instances can be deployed in a single AZ or three AZs. **NOTE** The 3-AZ deployment is not available in all regions. If the 3-AZ option is not displayed on the page for you to buy an instance, try a different region. ● If your service requires low network latency between instances, you deploy the components of the instance in the same AZ. If you select a single AZ to deploy your instance, anti-affinity deployment is used by default. With an anti-affinity deployment, your primary, secondary, and hidden nodes are deployed on different physical machines for high availability. ● If you want to deploy an instance across AZs for disaster recovery, select three AZs. In this deployment mode, the dds mongos, shard, and config nodes are evenly distributed across the three AZs.
DB Instance Type	Select **Cluster**. A cluster instance includes three types of nodes: dds mongos, shard, and config. Each shard and config is a three-node replica set to ensure high availability.
Compatible MongoDB Version	● 4.4 ● 4.2 ● 4.0 ● 3.4

Parameter	Description
CPU Type	DDS supports x86 and Kunpeng CPU architectures. **NOTE** This parameter is available only for MongoDB 4.0 and 3.4. The default value is **Kunpeng**. ● x86 x86 CPUs use the Complex Instruction Set Computing (CISC) instruction set. Each instruction can be used to execute low-level hardware operations. CISC instructions vary in length, and tend to be complicated and slow compared to Reduced Instruction Set Computing (RISC). ● Kunpeng The Kunpeng CPU architecture uses RISC. The RISC instruction set is smaller and faster than CISC, thanks to the simplified architecture. Kunpeng CPUs also offer a better balance between power and performance than x86. Kunpeng CPUs offer a high density, low power option that is more cost effective for heavy workloads.
Specifications	With an x86 architecture, you have the following options: ● General-purpose (s6): S6 instances are suitable for applications that require moderate performance generally but occasional bursts of high performance, such as light-workload web servers, enterprise R&D and testing environments, and low- and medium-performance databases. ● Enhanced II (c6): C6 instances have multiple technologies optimized to provide stable powerful compute performance. 25 GE intelligent high-speed NICs are used to provide ultra-high bandwidth and throughput, making it an excellent choice for heavy-load scenarios. It is suitable for websites, web applications, general databases, and cache servers that have higher performance requirements for compute and network resources; and medium- and heavy-load enterprise applications. For details about the supported instance specifications, see **Cluster Instance Specifications**.
dds mongos Node Class	For details about the dds mongos CPU and memory, see **Cluster Instance Specifications**. You can change the class of an instance after it is created. For details, see **Changing the Instance Class**.
dds mongos Nodes	The value ranges from 2 to 32. You can add nodes to an instance after it is created if necessary. For details, see **Adding Cluster Instance Nodes**.

Parameter	Description
shard Node Class	For details about shard CPU and memory, see **Cluster Instance Specifications**. The shard node stores user data but cannot be accessed directly. You can change the class of an instance after it is created. For details, see **Changing the Instance Class**.
shard Storage Space	The value ranges from 10 GB to 2000 GB and must be a multiple of 10. You can scale up an instance after it is created. For details, see **Scaling Up a Cluster Instance**. **NOTE** ● If the storage space you purchased exceeds 600 GB and the remaining storage space is 18 GB, the instance becomes **Read-only**. ● If the storage space you purchased is less than 600 GB and the storage space usage reaches 97%, the instance becomes **Read-only**. In these cases, delete unnecessary resources or expand the capacity.
shard Nodes	The value ranges from 2 to 32. You can add nodes to an instance after it is created if necessary. For details, see **Adding Cluster Instance Nodes**.
config Node Class	For details about the CPU and memory of the config node, see **Cluster Instance Specifications**. You can change the class of an instance after it is created. For details, see **Changing the Instance Class**.
config Storage Space	Based on the functions and minimum requirements of the config node, the storage space of the config node is set to 20 GB by default. You cannot scale up the storage of the node after it is created.

Figure 2-2 Network, Required Duration, and Quantity



Network

VPC: default_vpc ▾ | default_subnet(192.168.0.0/24) ▾ | Sys-default(b6f16cee-e859-47e2-a418... ▾

After the DDS instance is created, the VPC cannot be changed.

Available private IP addresses in the subnet: 227

In a security group, rules that authorize connections to DB instances apply to all DB instances associated with the security group.

Enterprise Project

Enterprise Project: --Select-- ▾

Some settings are configured by default during purchase, but can still be modified after the instance is created. If you do not see a setting listed for your instance, click Custom Config

Table 2-2 Network settings

Parameter	Description
VPC	The VPC where your DB instances are located. A VPC isolates networks for different services. It allows you to easily manage and configure private networks and change network configurations. You need to create or select the required VPC. For details, see **Creating a VPC** in the *Virtual Private Cloud User Guide*. For details about the constraints on the use of VPCs, see **Connection Methods**. If there are no VPCs available, DDS creates one for you by default. **NOTE** After the DDS instance is created, the VPC cannot be changed.
Enterprise Project	Only enterprise users can use this function. To use this function, contact customer service. An enterprise project is a cloud resource management mode, in which cloud resources and members are centrally managed by project. Select an enterprise project from the drop-down list. The default project is **default**. For more information about enterprise project, see **Project Management** in *Enterprise Management User Guide*. To customize an enterprise project, click **Enterprise** in the upper right corner of the console. The **Enterprise Management** page is displayed. For details, see **Creating an Enterprise Project** in *Enterprise Management User Guide*.

Table 2-3 Required duration and quantity

Parameter	Description
Required Duration	The length of your subscription if you select **Yearly/Monthly** billing. Subscription lengths range from one month to three years.
Auto-renew	● By default, this option is not selected. ● If you select this option, the auto-renew cycle is determined by the length of the subscription.
Quantity	The purchase quantity depends on the cluster instance quota. If your current quota does not allow you to purchase the required number of instances, you can apply for an increased quota. Yearly/Monthly instances that were purchased in batches have the same specifications except for the instance name and ID.

Step 3 On the displayed page, confirm the instance details.

- For yearly/monthly instances

  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, read and agree to the service agreement and click **Pay Now** to go to the payment page and complete the payment.
- For pay-per-use instances
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, read and agree to the service agreement and click **Submit** to start creating the instance.

Step 4 Click **Back to Instance List**. After a DDS instance is created, you can view and manage it on the **Instances** page.

- When an instance is being created, the status displayed in the **Status** column is **Creating**. This process takes about 15 minutes. After the creation is complete, the status changes to **Available**.
- DDS enables the automated backup policy by default. After an instance is created, you can modify or disable the automated backup policy. An automated full backup is immediately triggered after the creation of an instance.

----End

2.1.2 Custom Config

This section describes how to purchase a cluster instance in custom mode on the management console. You can customize the computing resources and storage space of a cluster instance based on your service requirements. In addition, you can configure advanced settings, such as slow query log and automated backup.

Precautions

Each account can create up to 10 cluster instances.

Prerequisites

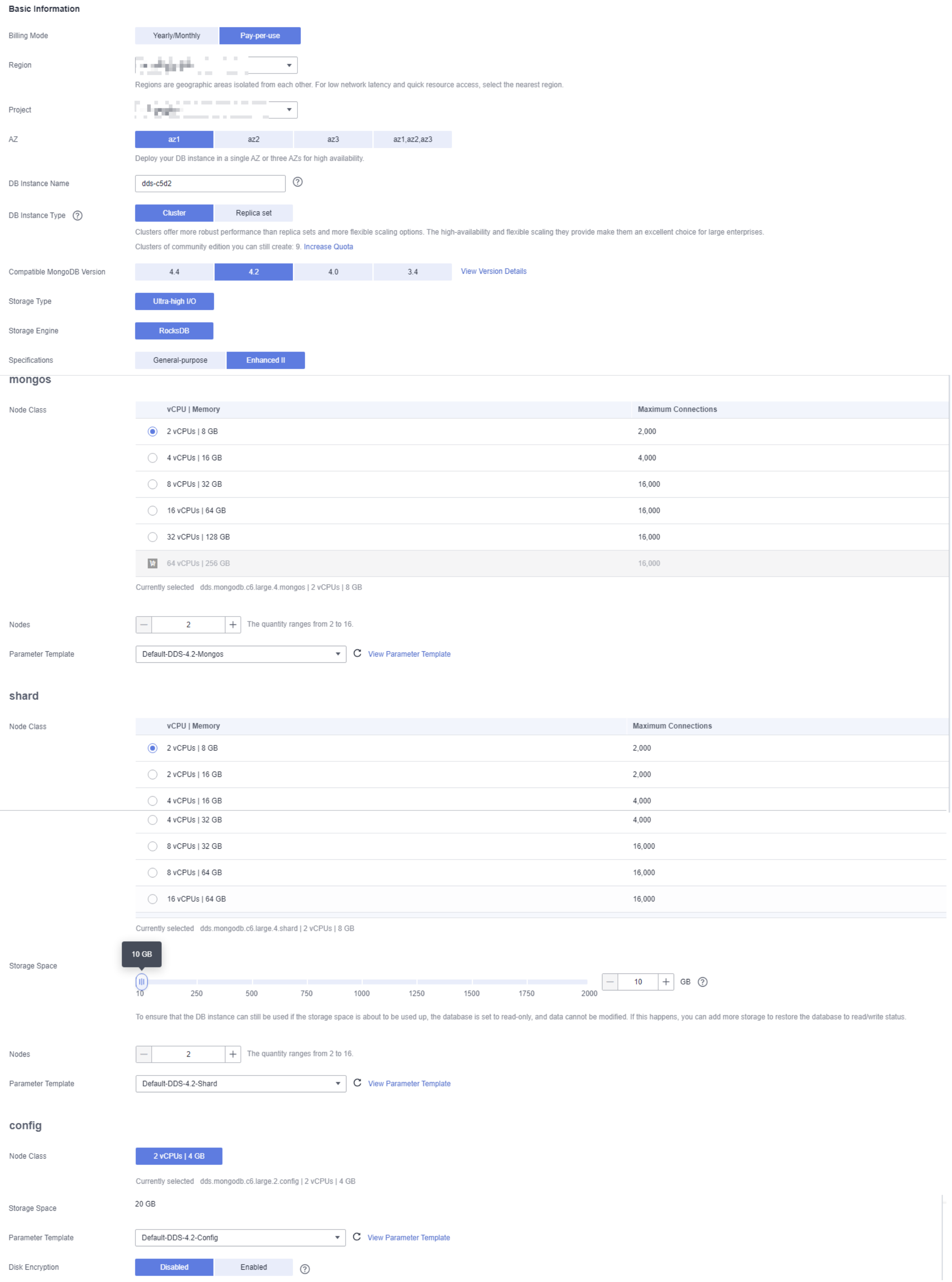
- You have **registered a Huawei ID and enabled Huawei Cloud services**.
- Your account balance is greater than or equal to $0 USD.
- To display whether the disk is encrypted in the DB instance list, submit a service ticket. In the upper right corner of the management console, choose **Service Tickets > Create Service Ticket**.

Procedure

Step 1 Go to the **Custom Config** page.

Step 2 On the displayed page, select a billing mode and configure information about your DB instance. Then, click **Next**.

Figure 2-3 Basic configurations



Basic Information

Billing Mode: Yearly/Monthly | [Pay-per-use]

Region: [redacted]

Regions are geographic areas isolated from each other. For low network latency and quick resource access, select the nearest region.

Project: [redacted]

AZ: [az1] | az2 | az3 | az1,az2,az3

Deploy your DB instance in a single AZ or three AZs for high availability.

DB Instance Name: dds-c5d2

DB Instance Type: [Cluster] | Replica set

Clusters offer more robust performance than replica sets and more flexible scaling options. The high-availability and flexible scaling they provide make them an excellent choice for large enterprises.

Clusters of community edition you can still create: 9. Increase Quota

Compatible MongoDB Version: 4.4 | [4.2] | 4.0 | 3.4 View Version Details

Storage Type: [Ultra-high I/O]

Storage Engine: [RocksDB]

Specifications: General-purpose | [Enhanced II]

mongos

Node Class

	vCPU | Memory	Maximum Connections
●	2 vCPUs | 8 GB	2,000
○	4 vCPUs | 16 GB	4,000
○	8 vCPUs | 32 GB	16,000
○	16 vCPUs | 64 GB	16,000
○	32 vCPUs | 128 GB	16,000
	64 vCPUs | 256 GB	16,000

Currently selected dds.mongodb.c6.large.4.mongos | 2 vCPUs | 8 GB

Nodes: 2 The quantity ranges from 2 to 16.

Parameter Template: Default-DDS-4.2-Mongos View Parameter Template

shard

Node Class

	vCPU | Memory	Maximum Connections
●	2 vCPUs | 8 GB	2,000
○	2 vCPUs | 16 GB	2,000
○	4 vCPUs | 16 GB	4,000
○	4 vCPUs | 32 GB	4,000
○	8 vCPUs | 32 GB	16,000
○	8 vCPUs | 64 GB	16,000
○	16 vCPUs | 64 GB	16,000

Currently selected dds.mongodb.c6.large.4.shard | 2 vCPUs | 8 GB

Storage Space: 10 GB

10 GB

To ensure that the DB instance can still be used if the storage space is about to be used up, the database is set to read-only, and data cannot be modified. If this happens, you can add more storage to restore the database to read/write status.

Nodes: 2 The quantity ranges from 2 to 16.

Parameter Template: Default-DDS-4.2-Shard View Parameter Template

config

Node Class: [2 vCPUs | 4 GB]

Currently selected dds.mongodb.c6.large.2.config | 2 vCPUs | 4 GB

Storage Space: 20 GB

Parameter Template: Default-DDS-4.2-Config View Parameter Template

Disk Encryption: [Disabled] | Enabled

Table 2-4 Basic configurations

Parameter	Description
Billing Mode	Select a billing mode, **Yearly/Monthly** or **Pay-per-use**. ● For yearly/monthly instances – Specify **Required Duration**, and the system deducts the fees incurred from your account based on the service price. – If you do not expect to continue using the instance much after it expires, you can change the billing mode from yearly/monthly to pay-per-use. For details, see **Changing the Billing Mode from Yearly/Monthly to Pay-per-Use**.. **NOTE** Instances billed on a yearly/monthly basis cannot be deleted. They can only be unsubscribed from. For details, see **Unsubscribing from a Yearly/Monthly Instance**. ● For pay-per-use instances – You are billed for usage based on how much time the service is in use. – If you expect to use the service extensively over a long period of time, you can change its billing mode from pay-per-use to yearly/monthly to reduce costs. For details, see **Changing the Billing Mode from Pay-per-Use to Yearly/Monthly**..
Region	The region where the resource is located. **NOTE** Instances deployed in different regions cannot communicate with each other through a private network, and you cannot change the region of an instance once it is purchased. Exercise caution when selecting a region.
Project	The project corresponds to the current region and can be changed.

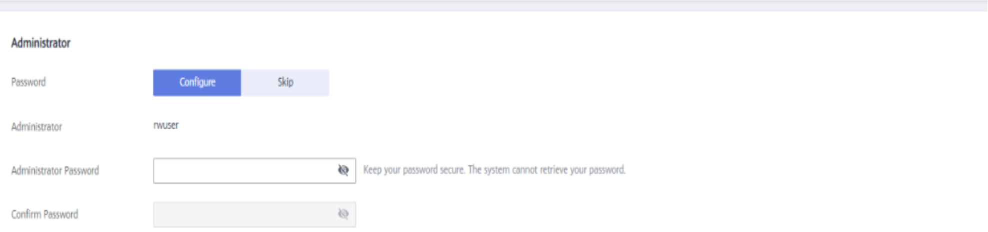
Parameter	Description
AZ	An AZ is a part of a region with its own independent power supply and network. AZs are physically isolated but can communicate through internal network connections. Instances can be deployed in a single AZ or three AZs. ● If your service requires low network latency between instances, you deploy the components of the instance in the same AZ. If you select a single AZ to deploy your instance, anti-affinity deployment is used by default. With an anti-affinity deployment, your primary, secondary, and hidden nodes are deployed on different physical machines for high availability. ● If you want to deploy an instance across AZs for disaster recovery, select three AZs. In this deployment mode, the dds mongos, shard, and config nodes are evenly distributed across the three AZs. **NOTE** The 3-AZ deployment is not available in all regions. If the 3-AZ option is not displayed on the page for you to buy an instance, try a different region.
DB Instance Name	● The instance name that you specify after the purchase. The instance name must contain 4 to 64 characters and must start with a letter. It is case sensitive and can contain letters, digits, hyphens (-), and underscores (_). It cannot contain other special characters. ● The instance name can be the same as an existing instance name. ● If you buy a batch of instances at once, a 4-digit numerical suffix will be added to the instance names, starting with **-0001**. If you later make another batch purchase, the new instance names will be numbered first using any suffixes missing from the sequence of your existing instances, and then continuing on from where your last batch purchase left off. For example, a batch of 3 instances get the suffixes **-0001**, **-0002**, and **-0003**. If you deleted instance **0002** and then bought 3 more instances, the new instances would get the suffixes **-0002**, **-0004**, and **-0005**. ● After the DB instance is created, you can change its name. For details, see **Changing an Instance Name**.
DB Instance Type	Select **Cluster**. A cluster instance includes three types of nodes: dds mongos, shard, and config. Each shard and config is a three-node replica set to ensure high availability.

Parameter	Description
Compatible MongoDB Version	● 4.4 ● 4.2 ● 4.0 ● 3.4
CPU Type	DDS supports x86 and Kunpeng CPU architectures. **NOTE** This parameter is available only for MongoDB 4.0 and 3.4. The default value is **Kunpeng**. ● x86 x86 CPUs use the Complex Instruction Set Computing (CISC) instruction set. Each instruction can be used to execute low-level hardware operations. CISC instructions vary in length, and tend to be complicated and slow compared to Reduced Instruction Set Computing (RISC). ● Kunpeng The Kunpeng CPU architecture uses RISC. The RISC instruction set is smaller and faster than CISC, thanks to the simplified architecture. Kunpeng CPUs also offer a better balance between power and performance than x86. Kunpeng CPUs offer a high density, low power option that is more cost effective for heavy workloads.
Storage Type	The storage type can be **Ultra-high I/O** and **Extreme SSD** for non-DeC users. For DeC users, the supported storage types depend on the selected resource type. ● If you select **EVS** for **Resource Type**, **Storage Type** is set to **Cloud SSD**. ● If you select **DSS** for **Resource Type**, **Storage Type** can be set to **Common I/O**, **High I/O**, or **Cloud SSD**.
Storage Engine	● WiredTiger WiredTiger is the default storage engine of DDS 3.4 and 4.0. WiredTiger provides different granularity concurrency control and compression mechanism for data management. It can provide the best performance and storage efficiency for different kinds of applications. ● RocksDB RocksDB is the default storage engine of DDS 4.2 and 4.4. RocksDB supports efficient point lookup, range scan, and high-speed write. RocksDB can be used as the underlying data storage engine of MongoDB and is suitable for scenarios with a large number of write operations.

Parameter	Description
Specifications	With an x86 architecture, you have the following options: ● General-purpose (s6): S6 instances are suitable for applications that require moderate performance generally but occasional bursts of high performance, such as light-workload web servers, enterprise R&D and testing environments, and low- and medium-performance databases. ● Enhanced II (c6): C6 instances have multiple technologies optimized to provide stable powerful compute performance. 25 GE intelligent high-speed NICs are used to provide ultra-high bandwidth and throughput, making it an excellent choice for heavy-load scenarios. It is suitable for websites, web applications, general databases, and cache servers that have higher performance requirements for compute and network resources; and medium- and heavy-load enterprise applications. For details about the supported instance specifications, see **Cluster Instance Specifications**.
dds mongos Node Class	For details about the dds mongos CPU and memory, see **Cluster Instance Specifications**. You can change the class of an instance after it is created. For details, see **Changing the Instance Class**.
dds mongos Nodes	The value ranges from 2 to 32. You can add nodes to an instance after it is created if necessary. For details, see **Adding Cluster Instance Nodes**.
dds mongos Parameter Template	The parameters that apply to the dds mongos nodes. After an instance is created, you can change the parameter template of a node to bring out the best performance. For details, see **Editing a Parameter Template**.
shard Node Class	For details about shard CPU and memory, see **Cluster Instance Specifications**. The shard node stores user data but cannot be accessed directly. You can change the class of an instance after it is created. For details, see **Changing the Instance Class**.
shard Storage Space	The value ranges from 10 GB to 2000 GB and must be a multiple of 10. You can scale up an instance after it is created. For details, see **Scaling Up a Cluster Instance**. **NOTE** ● If the storage space you purchased exceeds 600 GB and the remaining storage space is 18 GB, the instance becomes **Read-only**. ● If the storage space you purchased is less than 600 GB and the storage space usage reaches 97%, the instance becomes **Read-only**. In these cases, delete unnecessary resources or expand the capacity.

Parameter	Description
shard Nodes	The value ranges from 2 to 32. You can add nodes to an instance after it is created if necessary. For details, see **Adding Cluster Instance Nodes**.
shard Parameter Template	The parameters that apply to the shard nodes. After an instance is created, you can change the parameter template of a node to bring out the best performance. For details, see **Editing a Parameter Template**.
config Node Class	For details about the CPU and memory of the config node, see **Cluster Instance Specifications**. You can change the class of an instance after it is created. For details, see **Changing the Instance Class**.
config Storage Space	Based on the functions and minimum requirements of the config node, the storage space of the config node is set to 20 GB by default. You cannot scale up the storage of the node after it is created.
config Parameter Template	The parameters that apply to the config nodes. After an instance is created, you can change the parameter template of a node to bring out the best performance. For details, see **Editing a Parameter Template**.
Disk Encryption	● **Disabled**: Disable encryption. ● **Enabled**: Enable encryption. This feature improves data security but slightly affects read/write performance. **Key Name**: Select or create a private key, which is the tenant key. **NOTE** – After an instance is created, the disk encryption status and the key cannot be changed. Disk encryption will not encrypt backup data stored in OBS. To enable backup data encryption, contact customer service. – To check whether the disk is encrypted, you can view **Disk Encrypted** in the DB instance list. – If disk encryption or backup data encryption is enabled, keep the key properly. Once the key is disabled, deleted, or frozen, the database will be unavailable and data may not be restored. If disk encryption is enabled but backup data encryption is not enabled, you can **restore data to a new instance from backups**. If both disk encryption and backup data encryption are enabled, data cannot be restored. – For details about how to create a key, see "**Creating a CMK**" in *Data Encryption Workshop User Guide*.

Figure 2-4 Administrator settings



Administrator

Password Configure Skip

Administrator rwuser

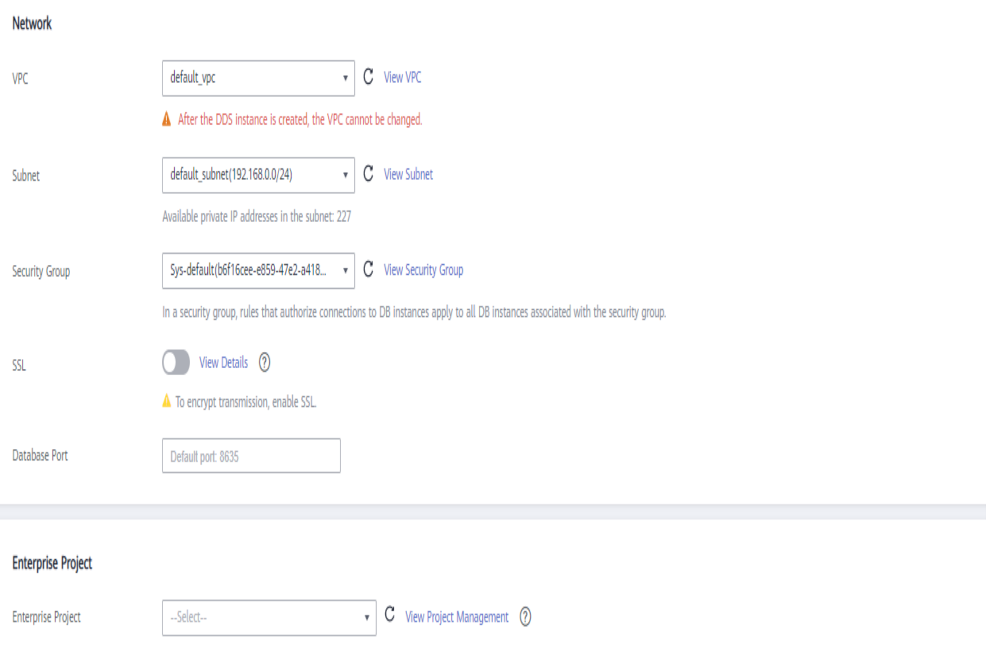
Administrator Password Keep your password secure. The system cannot retrieve your password.

Confirm Password

Table 2-5 Administrator settings

Parameter	Description
Password	● Configure Enter and confirm the new administrator password. After an instance is created, you can connect to the instance using the password. ● Skip To log in, you will have to reset the password later on the **Basic Information** page. If you need to connect to an instance after it is created, locate the instance and choose **More** > **Reset Password** in the **Operation** column to set a password for the instance first.
Administrator	The default account is **rwuser**.
Administrator Password	Set a password for the administrator. The password must be 8 to 32 characters in length and contain uppercase letters, lowercase letters, digits, and at least one of the following special characters: ~!@#%^*-_=+?()$ Keep this password secure. If lost, the system cannot retrieve it for you.
Confirm Password	Enter the administrator password again.

Figure 2-5 Network and required duration



Network

VPC: default_vpc ▾ C View VPC

⚠ After the DDS instance is created, the VPC cannot be changed.

Subnet: default_subnet(192.168.0.0/24) ▾ C View Subnet

Available private IP addresses in the subnet: 227

Security Group: Sys-default(b6f16cee-e859-47e2-a418... ▾ C View Security Group

In a security group, rules that authorize connections to DB instances apply to all DB instances associated with the security group.

SSL: ○ View Details ?

⚠ To encrypt transmission, enable SSL.

Database Port: Default port: 8635

Enterprise Project

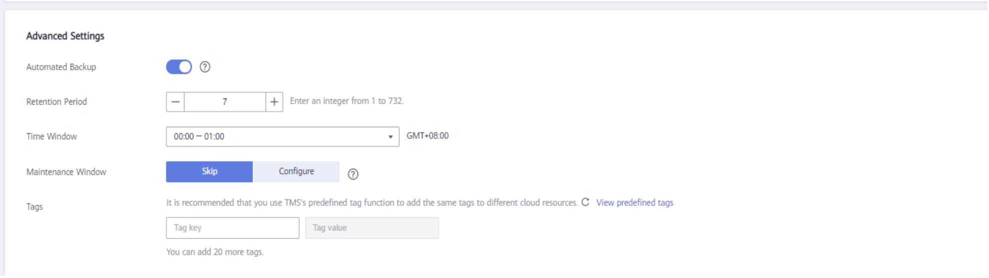
Enterprise Project: --Select-- ▾ C View Project Management ?

Table 2-6 Network settings

Parameter	Description
VPC	The VPC where your DB instances are located. A VPC isolates networks for different services. It allows you to easily manage and configure private networks and change network configurations. You will need to create or select the required VPC. For details about how to create a VPC, see "Creating a VPC" in *Virtual Private Cloud User Guide*. For details about the constraints on the use of VPCs, see **Connection Methods**. If there are no VPCs available, DDS creates one for you by default. **NOTE** After the DDS instance is created, the VPC cannot be changed.
Subnet	A subnet provides dedicated network resources that are logically isolated from other networks for security reasons. After the instance is created, you can change the private IP address assigned by the subnet. For details, see **Changing a Private IP Address**. **NOTE** Both IPv4 and IPv6 subnets are supported.

Parameter	Description
Security Group	A security group controls access between DDS and other services. If there are no security groups available, DDS creates one for you by default. **NOTE** ● Ensure that there is a security group rule configured that allows clients to access instances. For example, select an inbound TCP rule with the default port 8635, and enter a subnet IP address or select a security group that the instance belongs to. ● When creating a DB instance, you can select multiple security groups. For better network performance, you are advised to select no more than five security groups. In such a case, the access rules of all the selected security groups apply on the instance.
SSL	Secure Sockets Layer (SSL) encrypts connections between clients and servers, preventing data from being tampered with or stolen during transmission. You can enable SSL to improve data security. After an instance is created, you can connect to it using SSL.
Database Port	The default DDS port is 8635, but this port can be modified if necessary. If you change the port, add a corresponding security group rule to allow access to the instance. **NOTE** ● The database port is the port of the dds mongos node. The default port is 8635. To change the port, see **Changing a Database Port**. ● The shard node port is 8637, and the config node port is 8636, which cannot be changed. For details about how to connect to the shard and config nodes, see **Enabling IP Addresses of Shard and Config Nodes**.
Enterprise Project	Only enterprise users can use this function. To use this function, contact customer service. An enterprise project is a cloud resource management mode, in which cloud resources and members are centrally managed by project. Select an enterprise project from the drop-down list. The default project is **default**. For more information about enterprise project, see *Enterprise Management User Guide*.

Figure 2-6 Advanced settings



Advanced Settings

Automated Backup ●

Retention Period 7 Enter an integer from 1 to 732.

Time Window 00:00 – 01:00 GMT+08:00

Maintenance Window Skip Configure

Tags It is recommended that you use TMS's predefined tag function to add the same tags to different cloud resources. View predefined tags

Tag key Tag value

You can add 20 more tags.

Table 2-7 Advanced settings

Parameter	Description
Automated Backup	DDS enables an automated backup policy by default, but you can disable it after an instance is created. An automated full backup is immediately triggered after the creation of an instance. For details, see **Configuring an Automated Backup Policy**.
Retention Period (days)	**Retention Period** refers to the number of days that data is kept. You can increase the retention period to improve data reliability. The backup retention period is from 1 to 732 days.
Time Window	A one-hour period the backup will be scheduled within 24 hours, such as 01:00-02:00. The backup time is in UTC format.

Parameter	Description
Tags	(Optional) You can add tags to DDS instances so that you can quickly search for and filter specified instances by tag. Each DDS instance can have up to 20 tags. If your organization has configured tag policies for DDS, add tags to DB instances based on the policies. If a tag does not comply with the policies, DB instance creation may fail. Contact your organization administrator to learn more about tag policies. ● Create a tag. You can create tags on the DDS console and configure the tag **key** and **value**. Key: This parameter is mandatory. – Each tag key must be unique for each instance. – A tag key consists of up to 36 characters. – The key must consist of only digits, letters, underscores (_), and hyphens (-). Value: This parameter is optional. – The value consists of up to 43 characters. – The value must consist of only digits, letters, underscores (_), periods (.), and hyphens (-). ● Add a predefined tag. Predefined tags can be used to identify multiple cloud resources. To tag a cloud resource, you can select a created predefined tag from the drop-down list, without entering a key and value for the tag. For example, if a predefined tag has been created, its key is Usage and value is Project1. When you configure the key and value for a cloud resource, the created predefined tag will be displayed on the page. After an instance is created, you can click the instance name to view its tags. On the **Tags** page, you can also **modify or delete the tags**. In addition, you can quickly **search for and filter specified instances by tag**. You can add a tag to an instance after the instance is created. For details, see **Adding a Tag**.

If you have any question about the price, click **Price Details**.

NOTE

Instance performance depends on the specifications you select during creation. The hardware configuration items that can be selected include the node class and storage space.

Step 3 On the displayed page, confirm the instance details.

- For yearly/monthly instances
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, read and agree to the service agreement and click **Pay Now** to go to the payment page and complete payment.
- For pay-per-use instances
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, read and agree to the service agreement and click **Submit** to start creating the instance.

Step 4 Click **Back to Instance List**. After a DDS instance is created, you can view and manage it on the **Instances** page.

- When an instance is being created, the status displayed in the **Status** column is **Creating**. This process takes about 15 minutes. After the creation is complete, the status changes to **Available**.
- Yearly/Monthly instances that were purchased in batches have the same specifications except for the instance name and ID.

----End

2.2 Connecting to a Cluster Instance

2.2.1 Connection Methods

You can access DDS over private or public networks.

Table 2-8 Connection methods

Method	IP Address	Scenario	Description
DAS	Not required	DAS provides a GUI and allows you to perform visualized operations on the console. SQL execution, advanced database management, and intelligent O&M are all available to make database management simple, secure, and intelligent. By default, the permission to connect to DAS is enabled.	● Easy to use, secure, advanced, and intelligent ● Recommended

Method	IP Address	Scenario	Description
Private network	Private IP address	DDS provides a private IP address by default. If your applications are running on an ECS in the same region and VPC as your DDS instance, you are advised to use a private IP address to connect the ECS to your DDS instances.	● Secure and excellent performance ● For faster transmission and improved security, you are advised to migrate your applications to an ECS that is in the same subnet as your DDS instance and use a private IP address to access the instance.
Public network	EIP	● If your applications are running on an ECS that is in a different region from the one where the DDS instance is located, use an EIP to connect the ECS to your DDS instances. ● If you use a third-party device or your local device to connect to a DDS instance, you can use an EIP to connect to the DB instance.	● Low security

2.2.2 (Recommended) Connecting to Cluster Instances Through DAS

2.2.2.1 Overview

DAS provides a GUI and allows you to perform visualized operations on the console. SQL execution, advanced database management, and intelligent O&M are all available to make database management simple, secure, and intelligent. You are advised to use DAS to connect to instances.

This section describes how to buy a cluster instance on the management console and how to connect to the cluster instance through DAS.

Process

To purchase and connect to a cluster instance, perform the following steps:

1. **Buy a cluster instance.**
2. **Connect to the cluster instance through DAS.**

2.2.2.2 Connecting to a Cluster Instance Through DAS

Data Admin Service (DAS) enables you to manage DB instances on a web-based console, simplifying database management and improving working efficiency. You can connect and manage instances through DAS. By default, you have the permission required for remote login. It is recommended that you use the DAS service to connect to DB instances. DAS is secure and convenient.

Procedure

Step 1 **Log in to the management console**.

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

If you want compute and network resources dedicated to your exclusive use, **enable a DeC** and **apply for DCC resources**. After enabling a DeC, you can select the DeC region and project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, locate the target DB instance and click **Log In** in the **Operation** column.

Alternatively, click the target instance on the **Instances** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner of the page.

Step 5 In the **Instance Login** dialog box, enter the correct information and click **Log In** to access and manage your database.

Step 6 After the login is successful, you can perform operations such as creating a database, managing accounts, and managing databases.

For details, see **Data Management**.

----End

2.2.3 Connecting to a Cluster Instance over a Private Network

2.2.3.1 Configuring Security Group Rules

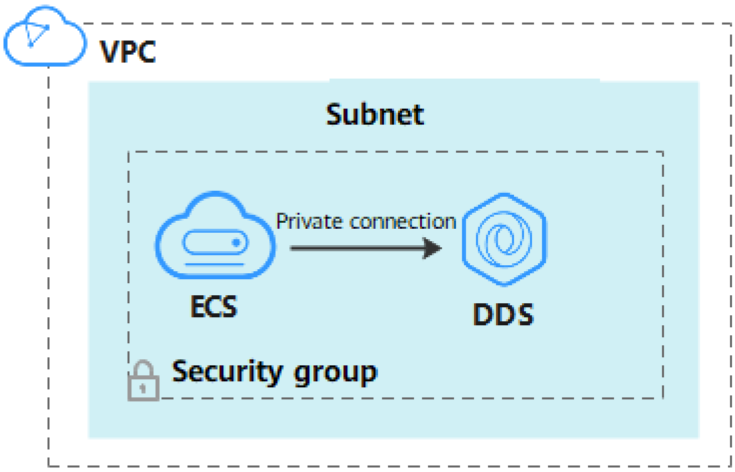
A security group is a collection of access control rules for ECSs and DDS instances that have the same security protection requirements and are mutually trusted in a VPC.

To ensure database security and reliability, you need to configure security group rules to allow specific IP addresses and ports to access DDS instances.

You can connect to an instance by configuring security group rules in following two ways:

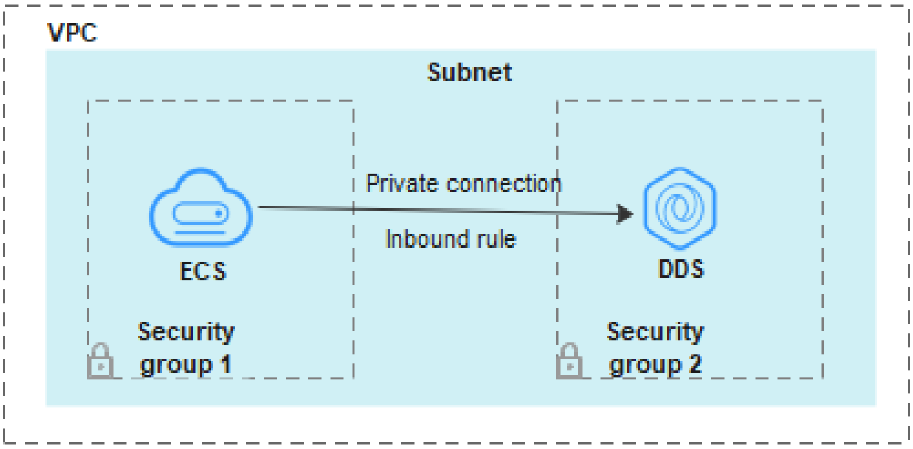
- If the ECS and instance are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to **Connecting to a Cluster Instance Using Mongo Shell (Private Network)**.

Figure 2-7 Same security group



- If the ECS and instance are in different security groups, you need to configure security group rules for them, separately.

Figure 2-8 Different security groups



  - Instance: Configure an **inbound rule** for the security group associated with the instance.
  - ECS: The default security group rule allows all outbound data packets. In this case, you do not need to configure a security group rule for the ECS. If not all traffic is allowed to reach the instance, configure an **outbound** rule for the ECS.

This section describes how to configure an **inbound** rule for an instance.

Precautions

- By default, an account can create up to 500 security group rules.

- Too many security group rules will increase the first packet latency, so a maximum of 50 rules for each security group is recommended.
- By default, one DDS instance is associated with only one security group.
- DDS allows you to associate multiple security groups to a DB instance. You can apply for the service based on your service requirements. For better network performance, you are advised to select no more than five security groups.

Procedure

Step 1 Log in to the management console.

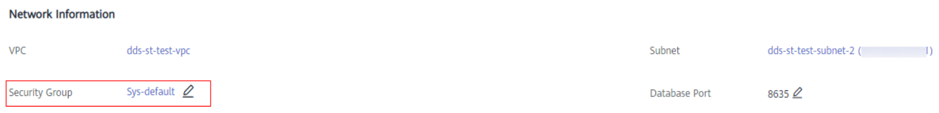
Step 2 Click 📍 in the upper left corner and select a region and a project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the instance name. The **Basic Information** page is displayed.

Step 5 In the **Network Information** area on the **Basic Information** page, click the security group.

Figure 2-9 Security Group

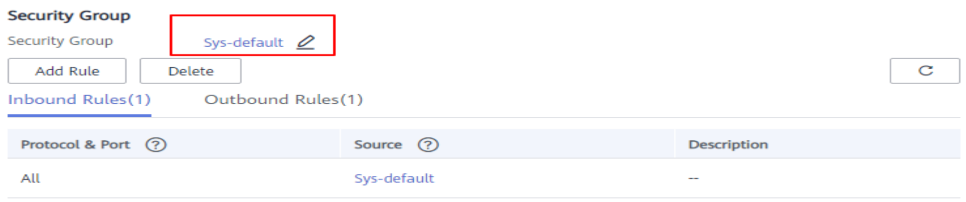


Network Information

VPC	dds-st-test-vpc	Subnet	dds-st-test-subnet-2 ([redacted])
Security Group	Sys-default	Database Port	8635

You can also choose **Connections** in the navigation pane on the left. On the **Private Connection** tab, in the **Security Group** area, click the security group name.

Figure 2-10 Security Group



Security Group

Security Group Sys-default

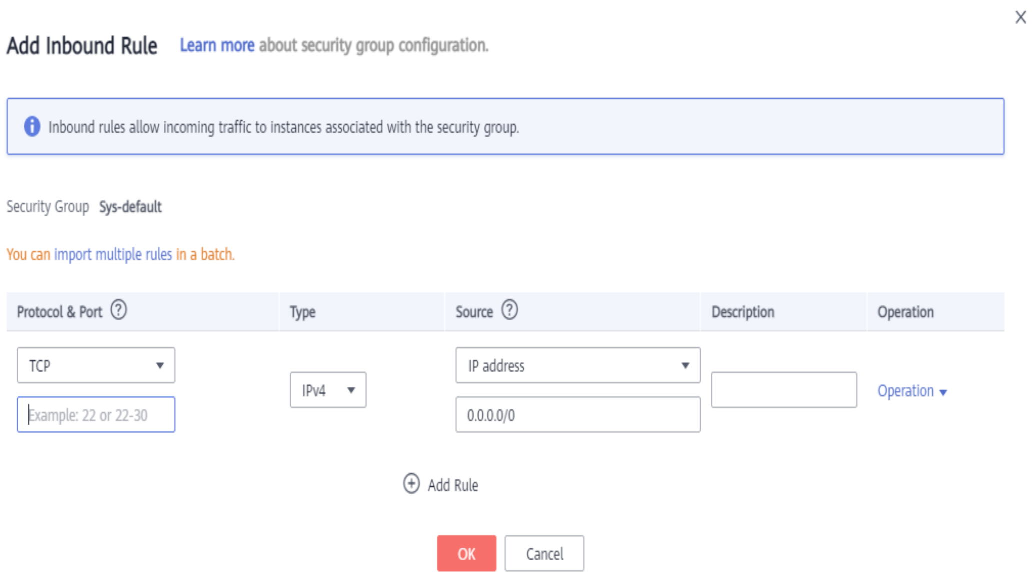
Protocol & Port	Source	Description
All	Sys-default	--

Step 6 On the **Security Group** page, locate the target security group and click **Manage Rule** in the **Operation** column.

Step 7 On the **Inbound Rules** tab, click **Add Rule**. The **Add Inbound Rule** dialog box is displayed.

Step 8 Add a security group rule as prompted.

Figure 2-11 Add Inbound Rule



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group Sys-default

You can import multiple rules in a batch.

Protocol & Port	Type	Source	Description	Operation
TCP Example: 22 or 22-30	IPv4	IP address 0.0.0.0/0		Operation

Table 2-9 Inbound rule settings

Parameter	Description	Example
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	The security group rule actions. A rule with a deny action overrides another with an allow action if the two rules have the same priority.	Allow
Protocol & Port	The network protocol required for access. Available options: **TCP**, **UDP**, **ICMP**, or **GRE**	TCP
	Port: the port on which you wish to allow access to DDS. The default port is 8635. The port ranges from 2100 to 9500 or can be 27017, 27018, or 27019.	8635
Type	IP address type. Only **IPv4** and **IPv6** are supported.	IPv4

Parameter	Description	Example
Source	Specifies the supported IP address, security group, and IP address group, which allow access from IP addresses or instances in other security group. Example: ● Single IP address: 192.168.10.10/32 ● IP address segment: 192.168.1.0/24 ● All IP addresses: 0.0.0.0/0 ● Security group: sg-abc ● IP address group: ipGroup-test If you enter a security group, all ECSs associated with the security group comply with the created rule. For more information about IP address groups, see **IP Address Group**.	0.0.0.0/0
Description	(Optional) Provides supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

Step 9 Click **OK**.

----End

2.2.3.2 Connecting to a Cluster Instance Using Mongo Shell (Private Network)

Mongo shell is the default client for the MongoDB database server. You can use Mongo Shell to connect to DB instances, and query, update, and manage data in databases. DDS is compatible with MongoDB. Mongo Shell is a part of the MongoDB client. To use Mongo Shell, download and install the MongoDB client first, and then use the Mongo shell to connect to the DB instance.

By default, a DDS instance provides a private IP address. If your applications are deployed on an ECS and are in the same region and VPC as DDS instances, you can connect to DDS instances using a private IP address to achieve a fast transmission rate and high security.

This section describes how to use Mongo Shell to connect to a cluster instance over a private network.

You can connect to an instance using an SSL connection or an unencrypted connection. The SSL connection is encrypted and more secure. To improve data transmission security, connect to instances using SSL.

Prerequisites

1. For details about how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.
2. Install the MongoDB client on the ECS. To ensure successful authentication, install the MongoDB client of the same version as the target instance.

   For details about how to install a MongoDB client, see **How Can I Install a MongoDB Client?**
3. The ECS can communicate with the DDS instance. For details, see **Configuring Security Group Rules**.

SSL Connection

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

Step 1 **Log in to the management console**.

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

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the instance name.

Step 5 In the navigation pane on the left, choose **Connections**.

Step 6 In the **Basic Information** area, click ⭳ next to the **SSL** field.

Step 7 Upload the root certificate to the ECS to be connected to the instance.

The following describes how to upload the certificate to a Linux and Window ECS:

- In Linux, run the following command:

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

  NOTE

  – **IDENTITY_FILE** is the directory where the root certificate resides. The file access permission is 600.

  – **REMOTE_USER** is the ECS OS user.

  – **REMOTE_ADDRESS** is the ECS address.

  – **REMOTE_DIR** is the directory of the ECS to which the root certificate is uploaded.
- In Windows, upload the root certificate using a remote connection tool.

Step 8 Connect to the instance in the directory where the MongoDB client is located.

Method 1: Using the private HA connection address (recommended)

DDS provides a private HA connection address that consists of IP addresses and ports of all dds mongos nodes in a cluster instance. You can use this address to connect to the cluster instance to improve availability of the cluster instance.

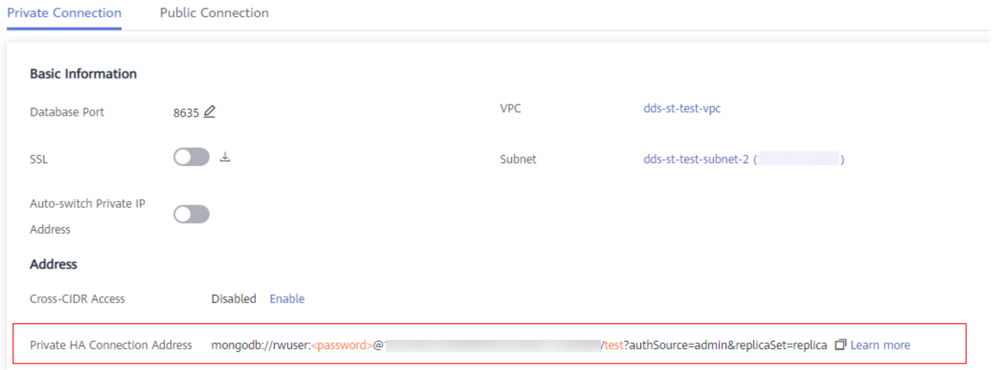
Example command:

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

Parameter description:

- **Private HA Connection Address**: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 2-12 Obtaining the private HA connection address



Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet-2 ([redacted])

Auto-switch Private IP Address

Address

Cross-CIDR Access Disabled Enable

Private HA Connection Address mongodb://rwuser:<password>@[redacted]/test?authSource=admin&replicaSet=replica Learn more

The format of the private HA connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

Pay attention to the following parameters in the private HA address:

Table 2-10 Parameter information

Parameter	Description
rwuser	Database username
<password>	Password for the database username. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.

Parameter	Description
192.168.***.***:8635,192.168.***.***:8635	IP addresses and ports of the dds mongos nodes of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user **rwuser** must be **admin**. **authSource=admin** is fixed in the command.

- **FILE_PATH** is the path for storing the root certificate.
- **--sslAllowInvalidHostnames**: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and bandwidth, the cluster certificate is generated using the internal management IP address. **--sslAllowInvalidHostnames** is needed for the SSL connection through a private network.

Command example:

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

Method 2: Using the private HA connection address (user-defined database and account)

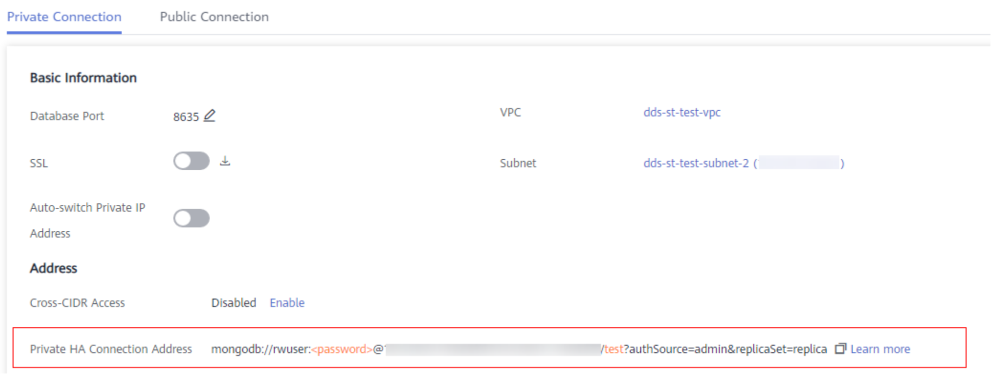
Example command:

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

Parameter description:

- **Private HA Connection Address**: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 2-13 Obtaining the private HA connection address



Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet-2 ([redacted])

Auto-switch Private IP Address

Address

Cross-CIDR Access Disabled Enable

Private HA Connection Address mongodb://rwuser:<password>@[redacted]/test?authSource=admin&replicaSet=replica Learn more

The format of the obtained private HA connection address is as follows:

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

The following table lists the required parameters in the private HA address.

Table 2-11 Parameter information

Parameter	Description
rwuser	Database username. The default value is **rwuser**. You can change the value to the username based on your service requirements.
<password>	Password for the database username. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.
192.168.***.***:8635,192.168.***.***:8635	IP addresses and ports of the dds mongos nodes of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user **rwuser** is **admin**. **NOTE** If you use a user-defined database for authentication, change the authentication database in the HA connection address to the name of the user-defined database. In addition, replace **rwuser** with the username created in the user-defined database.

- **FILE_PATH** is the path for storing the root certificate.
- **--sslAllowInvalidHostnames**: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and bandwidth, the cluster certificate is generated using the internal management IP address. **--sslAllowInvalidHostnames** is needed for the SSL connection through a private network.

For example, if you create a user-defined database **Database** and user **test1** in the database, the connection command is as follows:

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

Method 3: Using a private IP address

Example command:

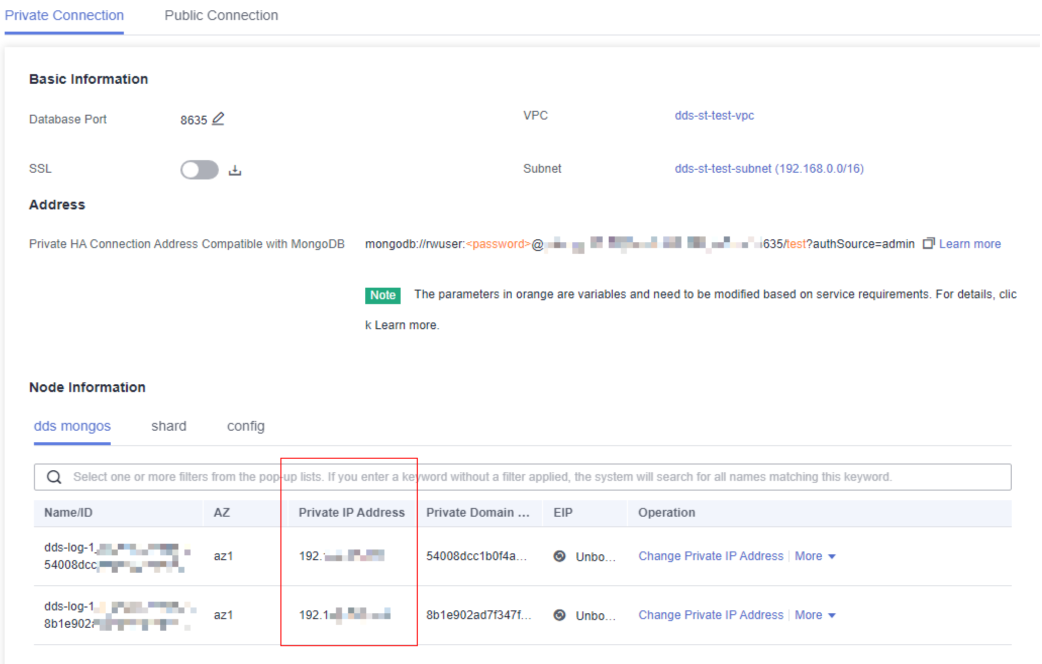
./mongo --host <*DB_HOST*> **--port** <*DB_PORT*> **-u** <*DB_USER*> **-p --authenticationDatabase admin --ssl --sslCAFile** <*FILE_PATH*> **--sslAllowInvalidHostnames**

Parameter description:

- **DB_HOST** is the IP address of the dds mongos node of the cluster instance to be connected.

  Click the instance name. On the **Basic Information** page, choose **Connections** > **Private Connection**, obtain the private IP address of the dds mongos node on the **dds mongos** tab in the **Node Information** area.

  Figure 2-14 Obtaining the private IP address



Private Connection | Public Connection

Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet (192.168.0.0/16)

Address

Private HA Connection Address Compatible with MongoDB mongodb://rwuser:<password>@[redacted]635/test?authSource=admin Learn more

Note The parameters in orange are variables and need to be modified based on service requirements. For details, click Learn more.

Node Information

dds mongos | shard | config

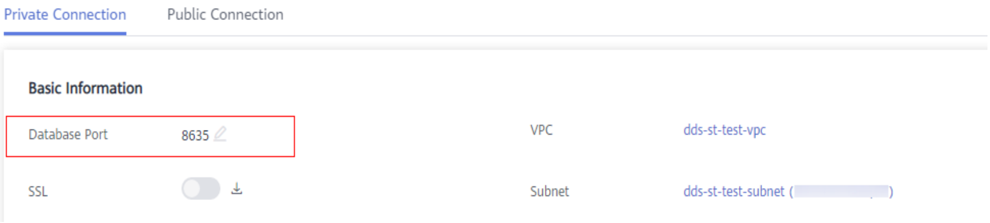
Select one or more filters from the pop-up lists. If you enter a keyword without a filter applied, the system will search for all names matching this keyword.

Name/ID	AZ	Private IP Address	Private Domain ...	EIP	Operation
dds-log-1[redacted] 54008dcc[redacted]	az1	192.[redacted]	54008dcc1b0f4a...	Unbo...	Change Private IP Address | More
dds-log-1[redacted] 8b1e902[redacted]	az1	192.1[redacted]	8b1e902ad7f347f...	Unbo...	Change Private IP Address | More

- **DB_PORT** is the port of the instance to be connected. The default port is 8635.

  Click the instance name. On the **Basic Information** page, choose **Connections**. On the **Private Connection** tab, obtain the database port information in the **Database Port** field in the **Basic Information** area.

  Figure 2-15 Obtaining the port



Private Connection | Public Connection

Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet ([redacted])

- **DB_USER** is the database user. The default value is **rwuser**.
- **FILE_PATH** is the path for storing the root certificate.
- **--sslAllowInvalidHostnames**: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and

bandwidth, the cluster certificate is generated using the internal management IP address. **--sslAllowInvalidHostnames** is needed for the SSL connection through a private network.

Enter the database account password when prompted:

```
Enter password:
```

Command example:

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

Step 9 Check the connection result. If the following information is displayed, the connection is successful.

```
mongos>
```

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

Step 1 Connect to the ECS.

Step 2 Connect to the instance in the directory where the MongoDB client is located.

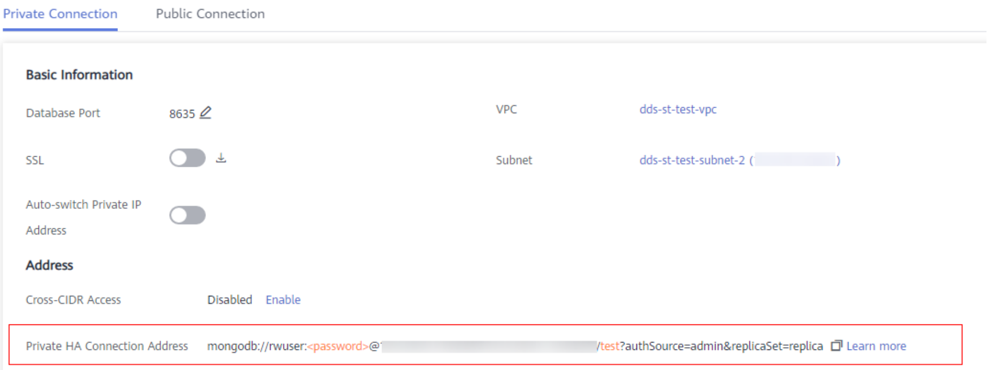
Method 1: Private HA connection address (recommended)

Example command:

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

Private HA Connection Address: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 2-16 Obtaining the private HA connection address



Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet-2 ([redacted])

Auto-switch Private IP Address

Address

Cross-CIDR Access Disabled Enable

Private HA Connection Address mongodb://rwuser:<password>@[redacted]/test?authSource=admin&replicaSet=replica Learn more

The format of the private HA connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

The following table lists the required parameters in the private HA address.

Table 2-12 Parameter information

Parameter	Description
rwuser	Database username
<password>	Password for the database username. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.
192.168.***.***:8635,192.168.***.***:8635	IP addresses and ports of the dds mongos nodes of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user **rwuser** must be **admin**. **authSource=admin** is fixed in the command.

Command example:

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

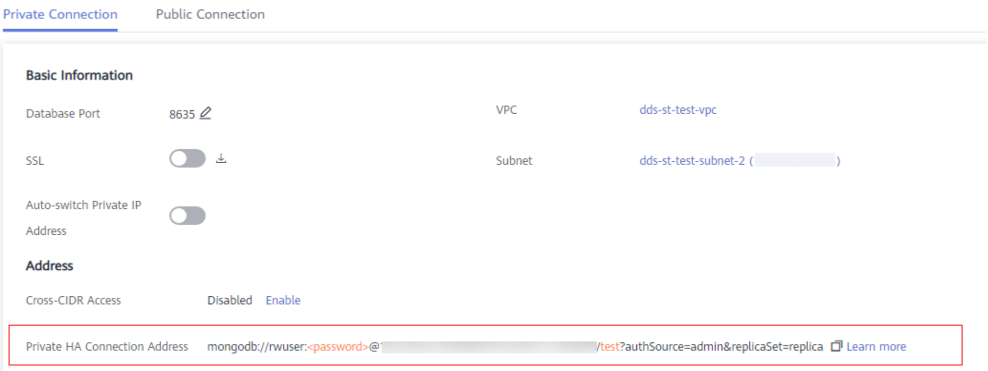
Method 2: Private HA connection (user-defined database and account)

Example command:

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

Private HA Connection Address: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 2-17 Obtaining the private HA connection address



Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet-2 ([redacted])

Auto-switch Private IP Address

Address

Cross-CIDR Access Disabled Enable

Private HA Connection Address mongodb://rwuser:<password>@[redacted]/test?authSource=admin&replicaSet=replica Learn more

The format of the obtained private HA connection address is as follows:

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

The following table lists the required parameters in the private HA address.

Table 2-13 Parameter information

Parameter	Description
rwuser	Database username. The default value is **rwuser**. You can change the value to the username based on your service requirements.
<password>	Password for the database username. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.
192.168.***.***:8635,192.168.***.***:8635	IP addresses and ports of the dds mongos nodes of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user **rwuser** is **admin**. **NOTE** If you use a user-defined database for authentication, change the authentication database in the HA connection address to the name of the user-defined database. In addition, replace **rwuser** with the username created in the user-defined database.

For example, if you create a user-defined database **Database** and user **test1** in the database, the connection command is as follows:

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

Method 3: Using a private IP address

Example command:

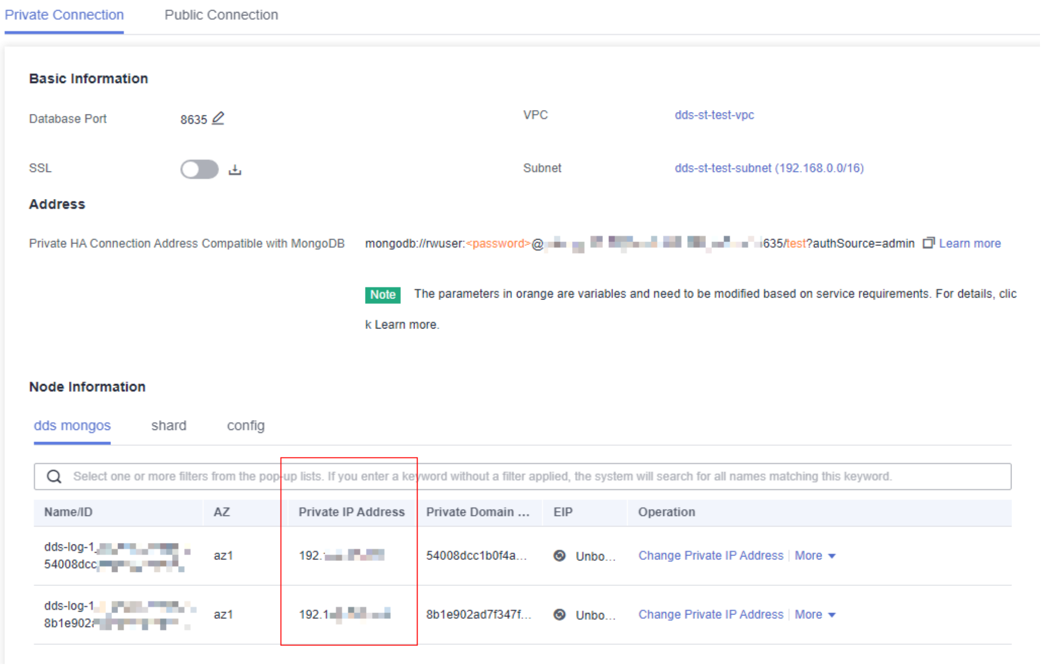
./mongo --host *<DB_HOST>* **--port** *<DB_PORT>* **-u** *<DB_USER>* **-p --authenticationDatabase admin**

Parameter description:

- **DB_HOST** is the IP address of the dds mongos node of the cluster instance to be connected.

  Click the instance name. On the **Basic Information** page, choose **Connections** > **Private Connection**, obtain the private IP address of the dds mongos node on the **dds mongos** tab in the **Node Information** area.

  Figure 2-18 Obtaining the private IP address

  Basic Information

  Database Port 8635

  VPC dds-st-test-vpc

  SSL

  Subnet dds-st-test-subnet (192.168.0.0/16)

  Address

  Private HA Connection Address Compatible with MongoDB mongodb://rwuser:<password>@[redacted]635/test?authSource=admin Learn more

  Note The parameters in orange are variables and need to be modified based on service requirements. For details, clic k Learn more.

  Node Information

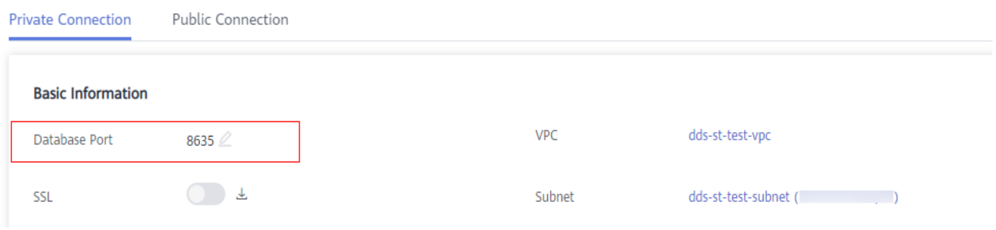
  Select one or more filters from the pop-up lists. If you enter a keyword without a filter applied, the system will search for all names matching this keyword.

Name/ID	AZ	Private IP Address	Private Domain ...	EIP	Operation
dds-log-1[redacted] 54008dcc[redacted]	az1	192.[redacted]	54008dcc1b0f4a...	Unbo...	Change Private IP Address | More
dds-log-1[redacted] 8b1e902[redacted]	az1	192.1[redacted]	8b1e902ad7f347f...	Unbo...	Change Private IP Address | More

- **DB_PORT** is the port of the instance to be connected. The default port is 8635.

  Click the instance name. On the **Basic Information** page, choose **Connections**. On the **Private Connection** tab, obtain the database port information in the **Database Port** field in the **Basic Information** area.

Figure 2-19 Obtaining the port



Private Connection Public Connection

Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet ([redacted])

- **DB_USER** is the database user. The default value is **rwuser**.

Enter the database password when prompted:

```
Enter password:
```

Command example:

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

Step 3 Check the connection result. If the following information is displayed, the connection is successful.

```
mongos>
```

----End

2.2.3.3 Connecting to Read Replicas Using Mongo Shell

Mongo shell is the default client for the MongoDB database server. You can use Mongo Shell to connect to DB instances, and query, update, and manage data in databases. DDS is compatible with MongoDB. Mongo Shell is a part of the MongoDB client. To use Mongo Shell, download and install the MongoDB client first, and then use the Mongo shell to connect to the DB instance.

By default, a DDS instance provides a private IP address. If your applications are deployed on an ECS and are in the same region and VPC as DDS instances, you can connect to DDS instances using a private IP address to achieve a fast transmission rate and high security.

This section describes how to use Mongo Shell to connect to a read replica over a private network.

You can connect to a read replica using an SSL connection or an unencrypted connection. The SSL connection is encrypted and more secure. To improve data transmission security, connect to instances using SSL.

Prerequisites

1. For details about how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.
2. Install the MongoDB client on the ECS. To ensure successful authentication, install the MongoDB client of the same version as the target instance.

   For details about how to install a MongoDB client, see **How Can I Install a MongoDB Client?**
3. The ECS can communicate with the DDS instance. For details, see **Configuring Security Group Rules**.

SSL Connection

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

Step 1 On the **Instances** page, click the instance name.

Step 2 In the navigation pane on the left, choose **Connections**.

Step 3 In the **Basic Information** area, click ⤓ next to the **SSL** field.

Step 4 Upload the root certificate to the ECS to be connected to the instance.

The following describes how to upload the certificate to a Linux and Window ECS:

- In Linux, run the following command:

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

  NOTE

  – **IDENTITY_FILE** is the directory where the root certificate resides. The file access permission is 600.
  – **REMOTE_USER** is the ECS OS user.
  – **REMOTE_ADDRESS** is the ECS address.
  – **REMOTE_DIR** is the directory of the ECS to which the root certificate is uploaded.

- In Windows, upload the root certificate using a remote connection tool.

Step 5 Connect to a DDS instance. The DDS console provides the read replica connection address. You can use this address to connect to the read replica.

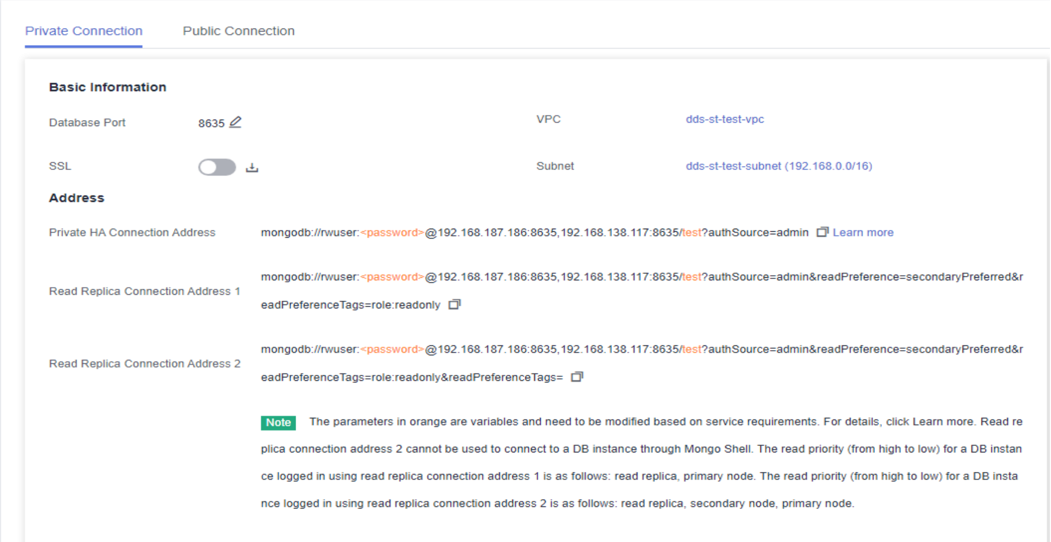
Example command:

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

Parameter description:

- **Read Replica Connection Address**: On the **Instances** page, click the instance to go to the **Basic Information** page. Choose **Connections**. Click the **Private Connection** tab. In the **Address** area, obtain the connection address of the read replica instance.

Figure 2-20 Obtaining the read replica connection address



Private Connection | Public Connection

Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet (192.168.0.0/16)

Address

Private HA Connection Address mongodb://rwuser:<password>@192.168.187.186:8635,192.168.138.117:8635/test?authSource=admin Learn more

Read Replica Connection Address 1 mongodb://rwuser:<password>@192.168.187.186:8635,192.168.138.117:8635/test?authSource=admin&readPreference=secondaryPreferred&readPreferenceTags=role:readonly

Read Replica Connection Address 2 mongodb://rwuser:<password>@192.168.187.186:8635,192.168.138.117:8635/test?authSource=admin&readPreference=secondaryPreferred&readPreferenceTags=role:readonly&readPreferenceTags=

Note The parameters in orange are variables and need to be modified based on service requirements. For details, click Learn more. Read replica connection address 2 cannot be used to connect to a DB instance through Mongo Shell. The read priority (from high to low) for a DB instance logged in using read replica connection address 1 is as follows: read replica, primary node. The read priority (from high to low) for a DB instance logged in using read replica connection address 2 is as follows: read replica, secondary node, primary node.

The format of the read replica connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

mongodb://rwuser:<password>@*192.168.xx.xx:8635,192.168.xx.xx:8635*/**test?authSource=admin&readPreference=secondaryPreferred&readPreferenceTags=role:readonly**

Pay attention to the following parameters in the read replica connection address:

Table 2-14 Parameter description

Parameter	Description
rwuser	Account name, that is, the database username.
<password>	Password for the database account. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.
192.168.xx.xx:8635,192.168.xx.xx:8635	IP address and port of the mongos node of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user **rwuser** must be **admin**. **authSource=admin** is fixed in the command.

- **FILE_PATH** is the path for storing the root certificate.
- **--sslAllowInvalidHostnames**: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and bandwidth, the cluster certificate is generated using the internal management IP address. **--sslAllowInvalidHostnames** is needed for the SSL connection through a private network.

Command example:

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

NOTE

When connecting to an instance using the read replica connection address, add double quotation marks (") before and after the connection information.

If the following information is displayed, the instance is successfully connected:

```
mongos>
```

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

Step 1 Log in to the ECS.

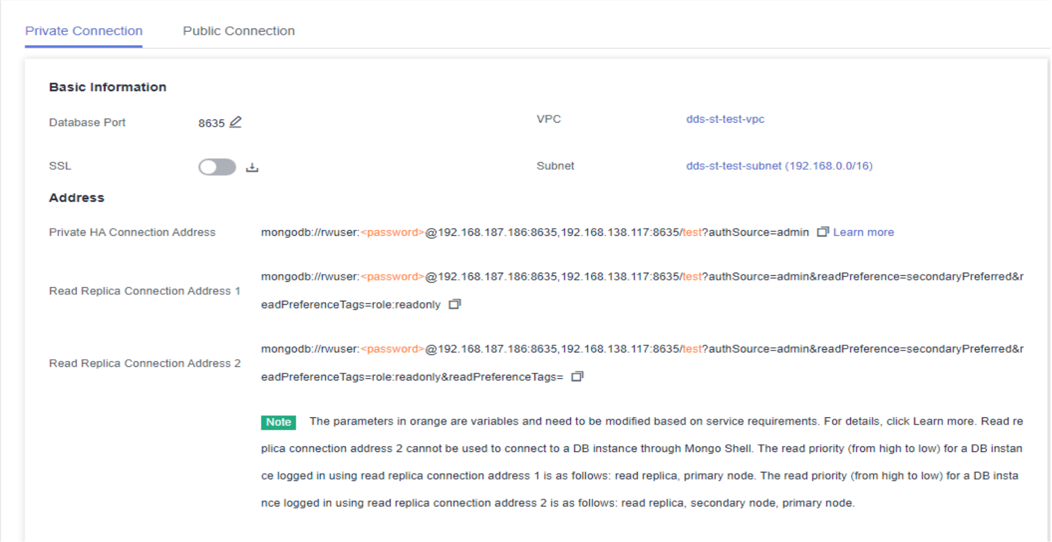
Step 2 Connect to a DDS instance. The DDS console provides the read replica connection address. You can use this address to connect to the read replica.

Example command:

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

Read Replica Connection Address: On the **Instances** page, click the instance to go to the **Basic Information** page. Choose **Connections**. Click the **Private Connection** tab. In the **Address** area, obtain the connection address of the read replica instance.

Figure 2-21 Obtaining the read replica connection address



Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet (192.168.0.0/16)

Address

Private HA Connection Address mongodb://rwuser:<password>@192.168.187.186:8635,192.168.138.117:8635/test?authSource=admin Learn more

Read Replica Connection Address 1 mongodb://rwuser:<password>@192.168.187.186:8635,192.168.138.117:8635/test?authSource=admin&readPreference=secondaryPreferred&readPreferenceTags=role:readonly

Read Replica Connection Address 2 mongodb://rwuser:<password>@192.168.187.186:8635,192.168.138.117:8635/test?authSource=admin&readPreference=secondaryPreferred&readPreferenceTags=role:readonly&readPreferenceTags=

Note The parameters in orange are variables and need to be modified based on service requirements. For details, click Learn more. Read replica connection address 2 cannot be used to connect to a DB instance through Mongo Shell. The read priority (from high to low) for a DB instance logged in using read replica connection address 1 is as follows: read replica, primary node. The read priority (from high to low) for a DB instance logged in using read replica connection address 2 is as follows: read replica, secondary node, primary node.

The format of the read replica connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

mongodb://rwuser:<password>@*192.168.xx.xx:8635,192.168.xx.xx:8635***/test?authSource=admin&readPreference=secondaryPreferred&readPreferenceTags=role:readonly**

Pay attention to the following parameters in the private HA address:

Table 2-15 Parameter description

Parameter	Description
rwuser	Account name, that is, the database username.
<password>	Password for the database account. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ********@%***!$**, the corresponding URL code is ******%40%25***%21%24**.
192.168.xx.xx:8635,192.168.xx.xx:8635	IP address and port of the mongos node of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user **rwuser** must be **admin**. **authSource=admin** is fixed in the command.

Command example:

./mongo "mongodb:// rwuser:<password>@*192.168.xx.xx:8635,192.168.xx.xx:8635***/test?authSource=admin&readPreference=secondaryPreferred&readPreferenceTags=role:readonly"**

If the following information is displayed, the instance is successfully connected:

```
mongos>
```

----End

2.2.4 Connecting to a Cluster Instance over a Public Network

2.2.4.1 Binding and Unbinding an EIP

After you create a Cluster instance, you can bind an EIP to it to allow external access. If later you want to prohibit external access, you can also unbind the EIP from the instance.

Precautions

- Deleting a bound EIP does not mean that the EIP is unbound.
- Before accessing a database, apply for an EIP on the VPC console. Then, add an inbound rule to allow the IP addresses or IP address ranges of ECSs. For details, see **Configuring a Security Group**.
- In the cluster instance, only dds mongos can have an EIP bound. To change the EIP that has been bound to a node, you need to unbind it from the node first.

Binding an EIP

Step 1 **Log in to the management console**.

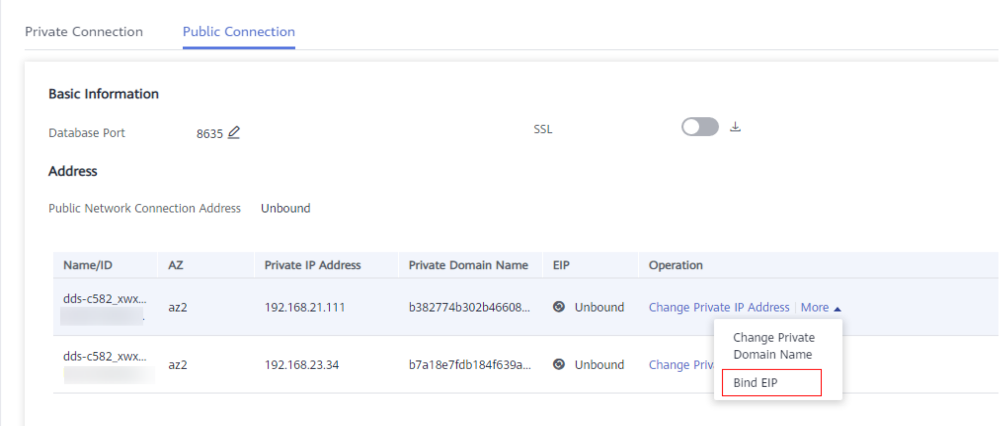
Step 2 Click 📍 in the upper left corner and select a region and a project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the cluster instance name.

Step 5 In the navigation pane on the left, choose **Connections**. Click the **Public Connection** tab. In the **Basic Information** area, locate the dds mongos node and click **Bind EIP** in the **Operation** column.

Figure 2-22 Binding an EIP



Basic Information

Database Port 8635

SSL

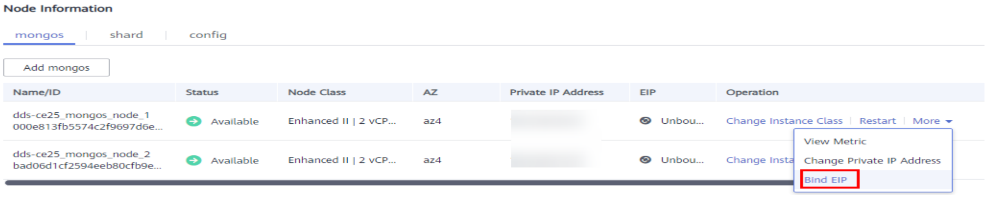
Address

Public Network Connection Address Unbound

Name/ID	AZ	Private IP Address	Private Domain Name	EIP	Operation
dds-c582_xwx... [redacted]	az2	192.168.21.111	b382774b302b46608...	Unbound	Change Private IP Address More
dds-c582_xwx... [redacted]	az2	192.168.23.34	b7a18e7fdb184f639a...	Unbound	Change Priv

Alternatively, in the **Node Information** area on the **Basic Information** page, locate the dds mongos node and choose **More** > **Bind EIP** in the **Operation** column.

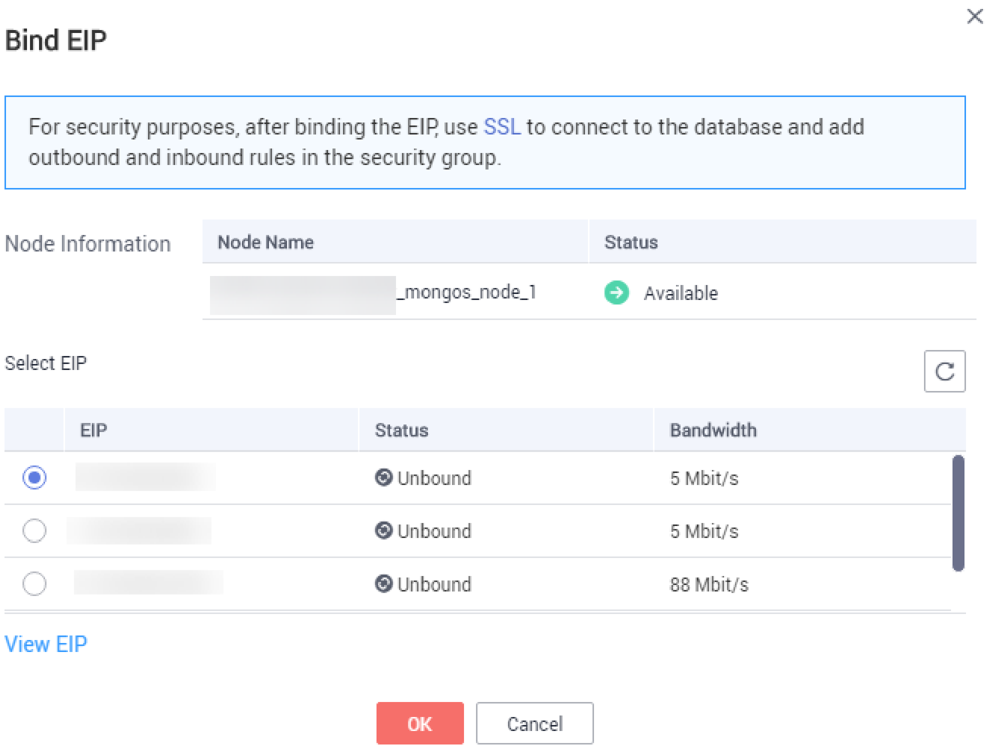
Figure 2-23 Binding an EIP


Node Information

Name/ID	Status	Node Class	AZ	Private IP Address	EIP	Operation
dds-ce25_mongos_node_1 000e813fb5574c2f9697d6e...	Available	Enhanced II | 2 vCP...	az4	[redacted]	Unbou...	Change Instance Class | Restart | More
dds-ce25_mongos_node_2 bad06d1cf2594eeb80cfb9e...	Available	Enhanced II | 2 vCP...	az4	[redacted]	Unbou...	Change Insta

Step 6 In the displayed dialog box, all available unbound EIPs are listed. Select the required EIP and click **OK**. If no available EIPs are displayed, click **View EIP** and create an EIP on the VPC console.

Figure 2-24 Selecting an EIP



Bind EIP

For security purposes, after binding the EIP, use SSL to connect to the database and add outbound and inbound rules in the security group.

Node Information

Node Name	Status
[redacted]_mongos_node_1	Available

Select EIP

	EIP	Status	Bandwidth
●	[redacted]	Unbound	5 Mbit/s
○	[redacted]	Unbound	5 Mbit/s
○	[redacted]	Unbound	88 Mbit/s

Step 7 In the **EIP** column on the **dds mongos** tab, you can view the EIP that was bound.

To unbind an EIP from the instance, see **Unbinding an EIP**.

----End

Unbinding an EIP

Step 1 **Log in to the management console**.

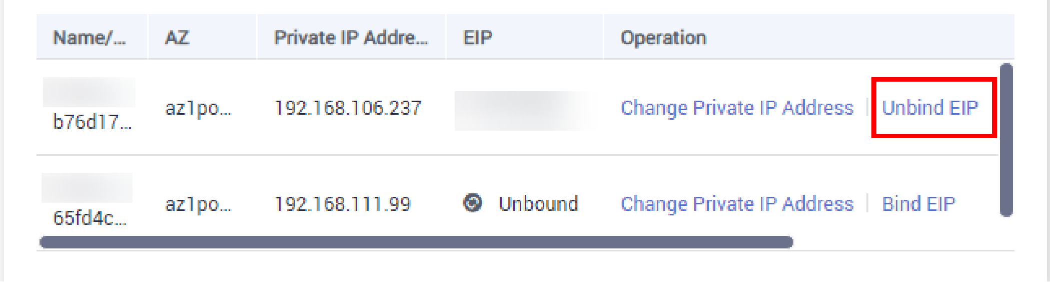
Step 2 Click 📍 in the upper left corner and select a region and a project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the cluster instance name.

Step 5 In the navigation pane on the left, choose **Connections**. Click the **Public Connection** tab. In the **Basic Information** area, locate the dds mongos node and click **Unbind EIP** in the **Operation** column.

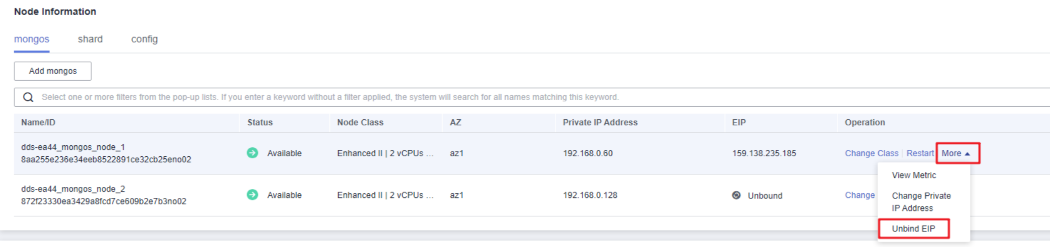
Figure 2-25 Unbinding an EIP



Name/...	AZ	Private IP Addre...	EIP	Operation
[redacted] b76d17...	az1po...	192.168.106.237	[redacted]	Change Private IP Address | Unbind EIP
[redacted] 65fd4c...	az1po...	192.168.111.99	Unbound	Change Private IP Address | Bind EIP

Alternatively, in the **Node Information** area on the **Basic Information** page, locate the dds mongos node and choose **More** > **Unbind EIP** in the **Operation** column.

Figure 2-26 Unbinding an EIP



Node Information

mongos shard config

Add mongos

Select one or more filters from the pop-up lists. If you enter a keyword without a filter applied, the system will search for all names matching this keyword.

Name/ID	Status	Node Class	AZ	Private IP Address	EIP	Operation
dds-ea44_mongos_node_1 8aa255e236e34eeb8522891ce32cb25eno02	Available	Enhanced II | 2 vCPUs ...	az1	192.168.0.60	159.138.235.185	Change Class | Restart | More ▲
dds-ea44_mongos_node_2 872f23330ea3429a8fcd7ce609b2e7b3no02	Available	Enhanced II | 2 vCPUs ...	az1	192.168.0.128	Unbound	Change

Step 6 In the displayed dialog box, click **Yes**.

To bind an EIP to the instance again, see **Binding an EIP**.

----End

2.2.4.2 Configuring a Security Group

A security group is a collection of access control rules for ECSs and DDS instances that have the same security protection requirements and are mutually trusted in a VPC.

To ensure database security and reliability, you need to configure security group rules to allow specific IP addresses and ports to access DDS instances.

To access an instance from the Internet, add an inbound rule for the security group associated with the instance.

Precautions

- By default, an account can create up to 500 security group rules.
- Too many security group rules will increase the first packet latency, so a maximum of 50 rules for each security group is recommended.
- By default, one DDS instance is associated with only one security group.
- DDS allows you to associate multiple security groups to a DB instance. You can apply for the service based on your service requirements. For better network performance, you are advised to select no more than five security groups.

Procedure

Step 1 Log in to the management console.

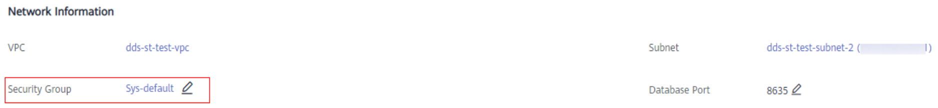
Step 2 Click 📍 in the upper left corner and select a region and a project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the instance name. The **Basic Information** page is displayed.

Step 5 In the **Network Information** area on the **Basic Information** page, click the security group.

Figure 2-27 Security Group



Network Information

VPC dds-st-test-vpc

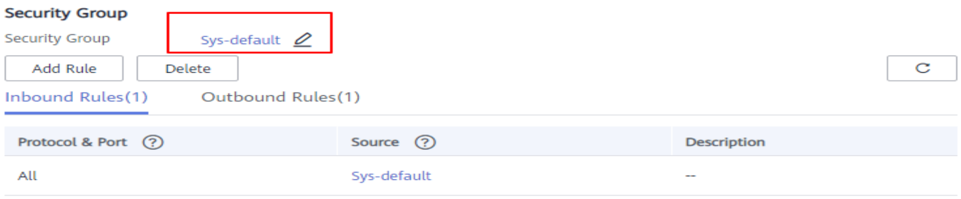
Subnet dds-st-test-subnet-2 ([redacted])

Security Group Sys-default

Database Port 8635

You can also choose **Connections** in the navigation pane on the left. On the **Public Connection** tab, in the **Security Group** area, click the security group name.

Figure 2-28 Security Group



Security Group

Security Group Sys-default

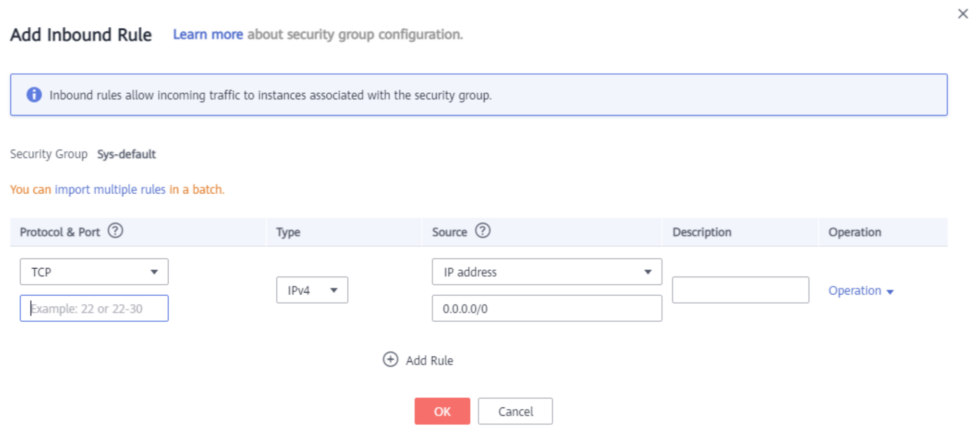
Protocol & Port	Source	Description
All	Sys-default	--

Step 6 On the **Security Group** page, locate the target security group and click **Manage Rule** in the **Operation** column.

Step 7 On the **Inbound Rules** tab, click **Add Rule**. The **Add Inbound Rule** dialog box is displayed.

Step 8 Add a security group rule as prompted.

Figure 2-29 Add Inbound Rule



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group Sys-default

You can import multiple rules in a batch.

Protocol & Port	Type	Source	Description	Operation
TCP Example: 22 or 22-30	IPv4	IP address 0.0.0.0/0		Operation

Table 2-16 Inbound rule settings

Paramete r	Description	Example Value
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	The security group rule actions. A rule with a deny action overrides another with an allow action if the two rules have the same priority.	Allow
Protocol & Port	The network protocol required for access. The option can be **All**, **TCP**, **UDP**, **ICMP**, or **GRE**.	TCP
	Port: the port on which you wish to allow access to DDS. The default port is 8635. The port ranges from 2100 to 9500 or can be 27017, 27018, or 27019.	8635
Type	IP address type. Only **IPv4** and **IPv6** are supported.	IPv4

Parameter	Description	Example Value
Source	Specifies the supported IP address, security group, and IP address group, which allow access from IP addresses or instances in other security group. Example: ● Single IP address: 192.168.10.10/32 ● IP address segment: 192.168.1.0/24 ● All IP addresses: 0.0.0.0/0 ● Security group: sg-abc ● IP address group: ipGroup-test If you enter a security group, all ECSs associated with the security group comply with the created rule. For more information about IP address groups, see **IP Address Group**.	0.0.0.0/0
Description	(Optional) Provides supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

Step 9 Click **OK**.

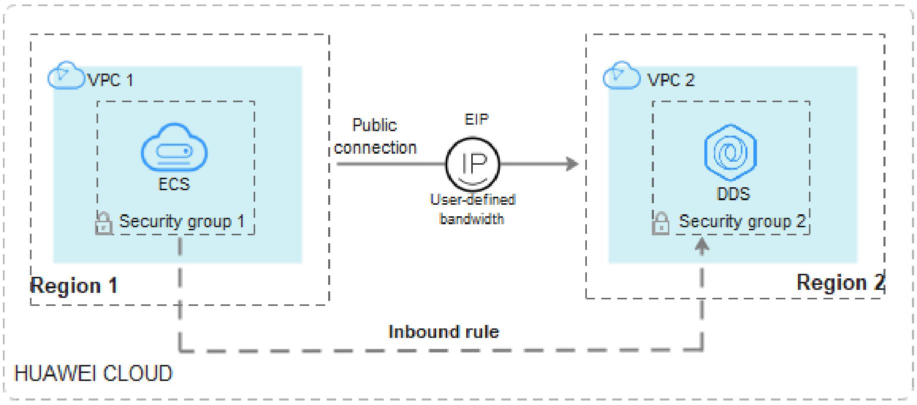
----End

2.2.4.3 Connecting to a Cluster Instance Using Mongo Shell (Public Network)

In the following scenarios, you can access a DDS instance from the Internet by binding an EIP to the instance.

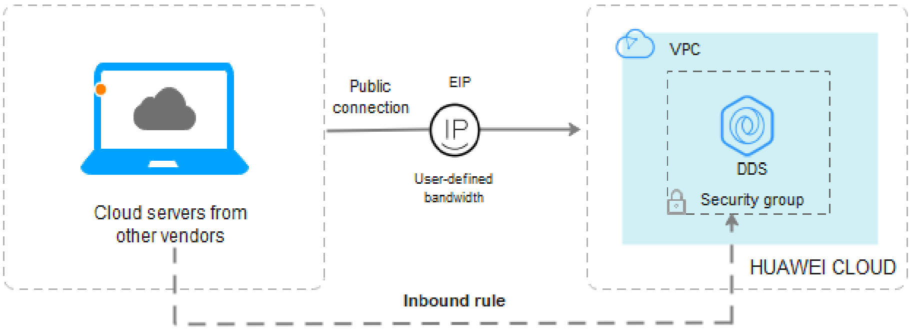
Scenario 1: Your applications are deployed on an ECS and are not in the same region as the DDS instance.

Figure 2-30 Accessing DDS from ECS across regions



Scenario 2: Your applications are deployed on a cloud server provided by other vendors.

Figure 2-31 Accessing DDS from other cloud servers



This section describes how to use Mongo Shell to connect to a cluster instance over a public network.

You can connect to an instance using an SSL connection or an unencrypted connection. The SSL connection is encrypted and more secure. To improve data transmission security, connect to instances using SSL.

Prerequisites

1. For details about how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.
2. **Bind an EIP** to the cluster instance and **set security group rules** to ensure that the instance can be accessed from the ECS.
3. Install the MongoDB client on the ECS.

   For details about how to install a MongoDB client, see **How Can I Install a MongoDB Client?**

SSL

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

Step 1 **Log in to the management console**.

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

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the instance name.

Step 5 In the navigation pane on the left, choose **Connections**.

Step 6 In the **Basic Information** area, click ⤓ next to the **SSL** field.

Step 7 Upload the root certificate obtained in **Step 6** to the ECS.

The following describes how to upload the certificate to a Linux and Window ECS:

- In Linux, run the following command:

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

  NOTE

  - **IDENTITY_FILE** is the directory where the root certificate resides. The file access permission is 600.
  - **REMOTE_USER** is the ECS OS user.
  - **REMOTE_ADDRESS** is the ECS address.
  - **REMOTE_DIR** is the directory of the ECS to which the root certificate is uploaded.

- In Windows, upload the root certificate using a remote connection tool.

Step 8 Connect to the instance in the directory where the MongoDB client is located.

Method 1: Using a public network connection address

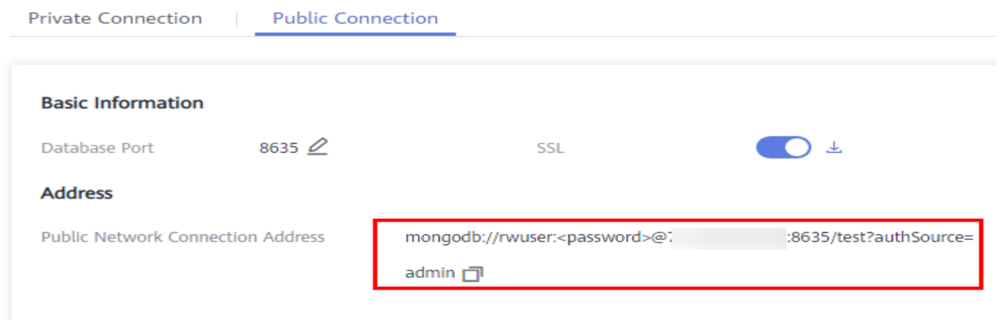
Example command:

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

Parameter description:

- **Public Network Connection Address**: On the **Instances** page, click the instance to switch to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Public Connection** tab. In the **Address** area, obtain the instance connection address from the **Public Network Connection Address** field.

Figure 2-32 Obtaining the public network connection address



Basic Information

Database Port 8635

SSL

Address

Public Network Connection Address

mongodb://rwuser:<password>@[redacted]:8635/test?authSource=admin

The format of the public connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

Pay attention to the following parameters in the public connection address:

Table 2-17 Parameter description

Parameter	Description
rwuser	Account name, that is, the database username.
<password>	Password for the database account. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.
192.168.*xx.xx*:8635	EIP and port bound to the dds mongos node of the cluster instance
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user **rwuser** must be **admin**. **authSource=admin** is fixed in the command.

- **FILE_PATH** is the path for storing the root certificate.
- **--sslAllowInvalidHostnames**: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and bandwidth, the cluster certificate is generated using the internal management IP address. **--sslAllowInvalidHostnames** is needed for the SSL connection through a public network.

Command example:

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

Method 2: Connect to an instance using an EIP.

Example command:

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

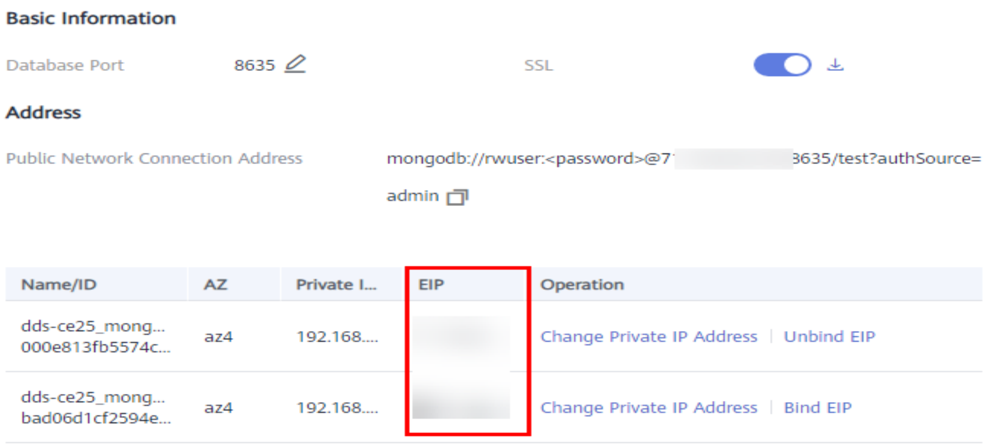
Parameter description:

- **DB_HOST** is the EIP bound to the instance to be connected.

  You can click the instance name to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the **Public Connection** tab, obtain the EIP bound to the dds mongos node in the **EIP** column.

  If there are multiple dds mongos nodes, the EIP of any node can be used to connect to the instance.

  Figure 2-33 Obtaining an EIP



Basic Information

Database Port 8635

SSL

Address

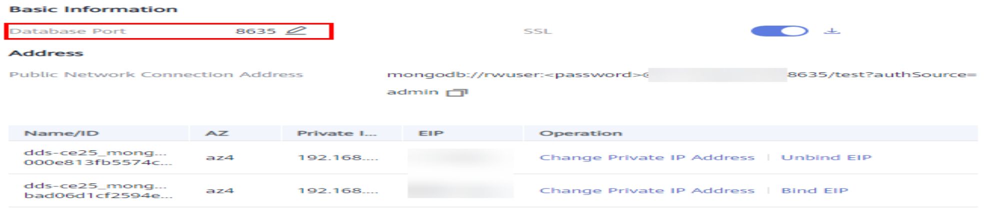
Public Network Connection Address mongodb://rwuser:<password>@7[redacted]3635/test?authSource=admin

Name/ID	AZ	Private I...	EIP	Operation
dds-ce25_mong... 000e813fb5574c...	az4	192.168....	[redacted]	Change Private IP Address | Unbind EIP
dds-ce25_mong... bad06d1cf2594e...	az4	192.168....	[redacted]	Change Private IP Address | Bind EIP

- **DB_PORT** is the port of the instance to be connected. The default port number is 8635.

  You can click the instance to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Public Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

  Figure 2-34 Obtaining the port



Basic Information

Database Port 8635

SSL

Address

Public Network Connection Address mongodb://rwuser:<password>[redacted]8635/test?authSource=admin

Name/ID	AZ	Private I...	EIP	Operation
dds-ce25_mong... 000e813fb5574c...	az4	192.168....	[redacted]	Change Private IP Address | Unbind EIP
dds-ce25_mong... bad06d1cf2594e...	az4	192.168....	[redacted]	Change Private IP Address | Bind EIP

- **DB_USER** is the database user. The default value is **rwuser**.
- **FILE_PATH** is the path for storing the root certificate.
- **--sslAllowInvalidHostnames**: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and

bandwidth, the cluster certificate is generated using the internal management IP address. **--sslAllowInvalidHostnames** is needed for the SSL connection through a public network.

Enter the database account password when prompted:

```
Enter password:
```

Command example:

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

Step 9 Check the connection result. If the following information is displayed, the connection is successful.

```
mongos>
```

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

Step 1 Log in to the ECS.

Step 2 Connect to the instance in the directory where the MongoDB client is located.

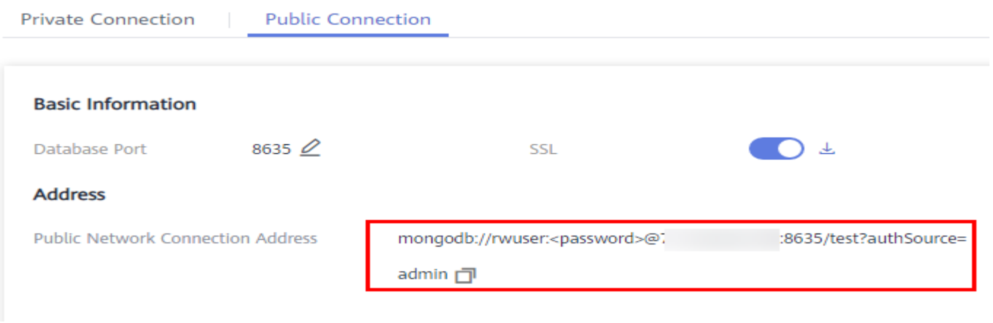
Method 1: Using a public network connection address

Example command:

./mongo *<Public network address>*

Public Network Connection Address: You can click the instance name to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Public Connection** tab. In the **Address** area, obtain the instance connection address from the **Public Network Connection Address** field.

Figure 2-35 Obtaining the public network connection address



Basic Information

Database Port 8635

SSL

Address

Public Network Connection Address mongodb://rwuser:<password>@[redacted]:8635/test?authSource=admin

The format of the public connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

The following table describes the required parameters in the public connection address.

Table 2-18 Parameter description

Parameter	Description
rwuser	Account name, that is, the database username.
<password>	Password for the database account. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.
192.168.*xx.xx*:8635	EIP and port bound to the dds mongos node of the cluster instance
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user **rwuser** must be **admin**. **authSource=admin** is fixed in the command.

Command example:

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

Method 2: Using an EIP

Example command:

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

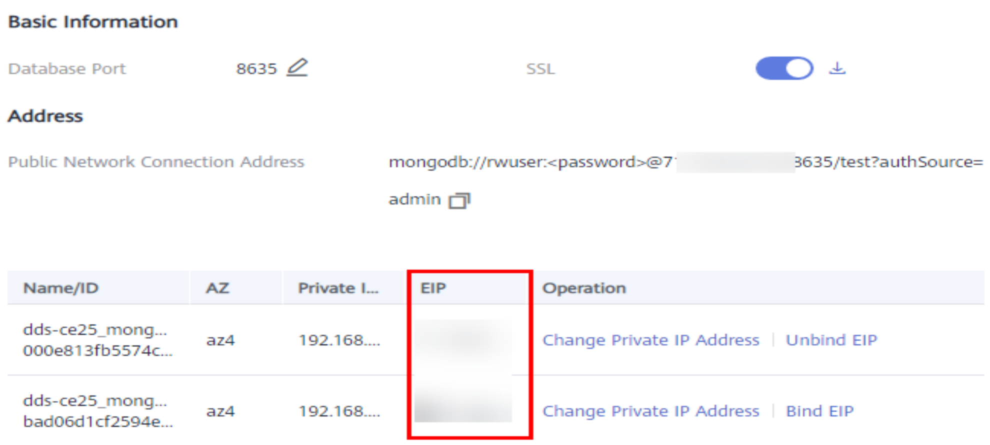
Parameter description:

- **DB_HOST** is the EIP bound to the instance to be connected.

  You can click the instance name to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the **Public Connection** tab, obtain the EIP bound to the dds mongos node in the **EIP** column.

  If there are multiple dds mongos nodes, the EIP of any node can be used to connect to the instance.

Figure 2-36 Obtaining an EIP



Basic Information

Database Port 8635

SSL

Address

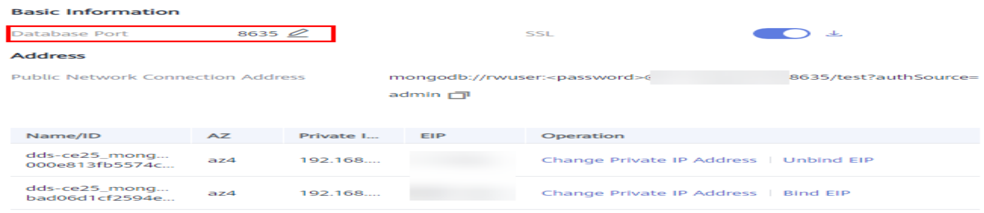
Public Network Connection Address mongodb://rwuser:<password>@7[redacted]3635/test?authSource=admin

Name/ID	AZ	Private I...	EIP	Operation
dds-ce25_mong... 000e813fb5574c...	az4	192.168....	[redacted]	Change Private IP Address | Unbind EIP
dds-ce25_mong... bad06d1cf2594e...	az4	192.168....	[redacted]	Change Private IP Address | Bind EIP

- **DB_PORT** is the port of the instance to be connected. The default port number is 8635.

  You can click the instance to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Public Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

Figure 2-37 Obtaining the port



Basic Information

Database Port 8635

SSL

Address

Public Network Connection Address mongodb://rwuser:<password>@[redacted]8635/test?authSource=admin

Name/ID	AZ	Private I...	EIP	Operation
dds-ce25_mong... 000e813fb5574c...	az4	192.168....	[redacted]	Change Private IP Address | Unbind EIP
dds-ce25_mong... bad06d1cf2594e...	az4	192.168....	[redacted]	Change Private IP Address | Bind EIP

- **DB_USER** is the database user. The default value is **rwuser**.

Enter the database account password when prompted:

```
Enter password:
```

Command example:

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

Step 3 Check the connection result. If the following information is displayed, the connection is successful.

```
mongos>
```

----End

2.2.4.4 Connecting to a Cluster Instance Using Robo 3T

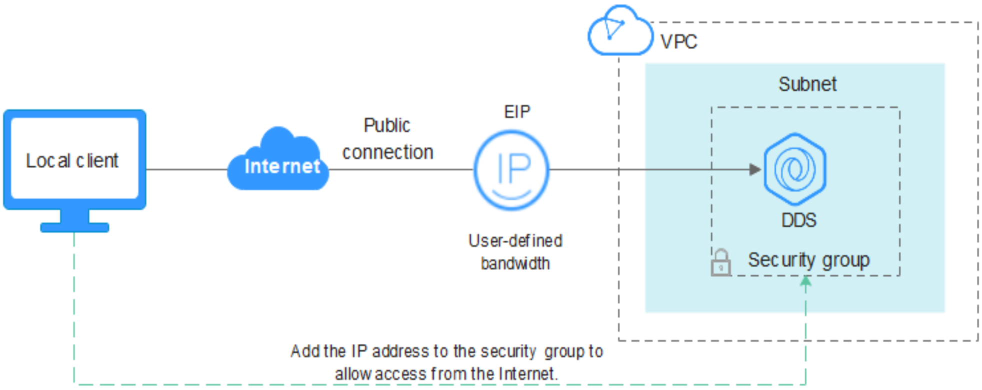
To connect to an instance from a local device, you can use Robo 3T to access the instance from the Internet.

This section describes how to use Robo 3T to connect to a cluster instance from a local device. In this section, the Windows operating system (OS) used by the client is used as an example.

Robo 3T can connect to an instance with an unencrypted connection or an encrypted connection (SSL). To improve data transmission security, connect to instances using SSL.

Connection Diagram

Figure 2-38 Connection diagram



Prerequisites

1. **Bind an EIP** to the cluster instance and **configure security group rules** to ensure that the instance can be accessed using Robo 3T.
2. Install Robo 3T.

   For details, see **Installing Robo 3T**.

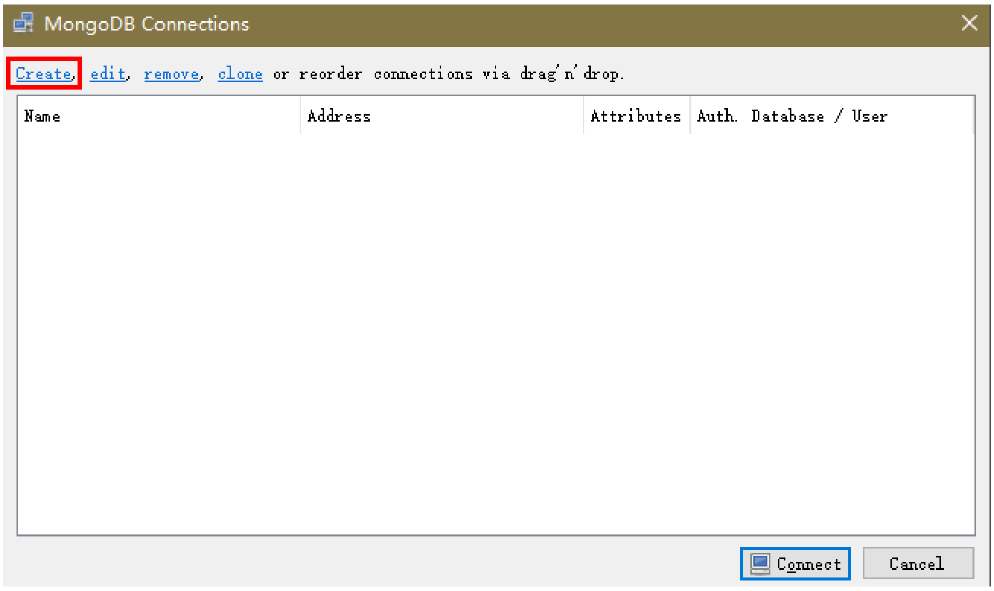
SSL

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

Step 1 Run the installed Robo 3T. On the displayed dialog box, click **Create**.

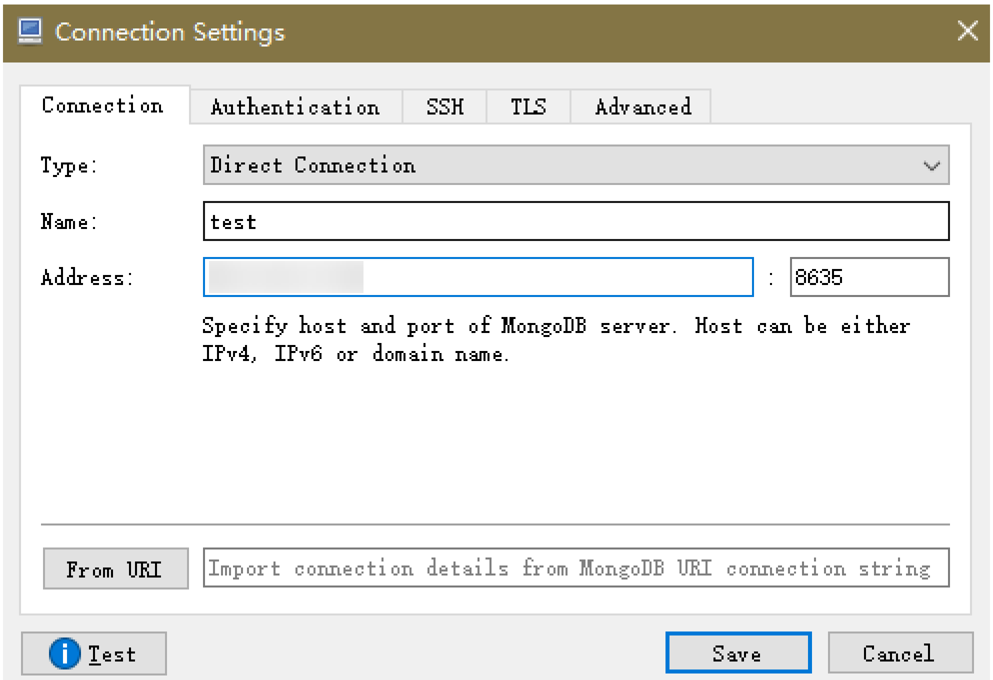
Figure 2-39 Connections



Step 2 In the **Connection Settings** dialog box, set the parameters of the new connection.

1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the DDS DB instance in the **Address** text box.

Figure 2-40 Connection



Type: Direct Connection

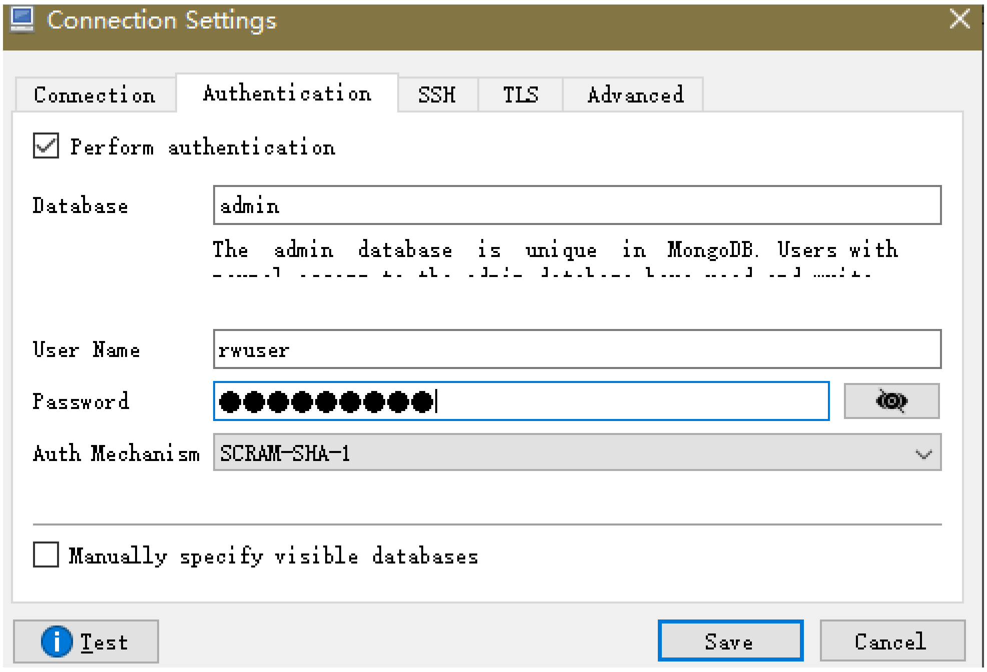
Name: test

Address: [redacted] : 8635

Specify host and port of MongoDB server. Host can be either IPv4, IPv6 or domain name.

2. On the **Authentication** tab, set **Database** to **admin**, **User Name** to **rwuser**, and **Password** to the administrator password you set during the creation of the cluster instance.

Figure 2-41 Authentication



☑ Perform authentication

Database: admin

The admin database is unique in MongoDB. Users with

User Name: rwuser

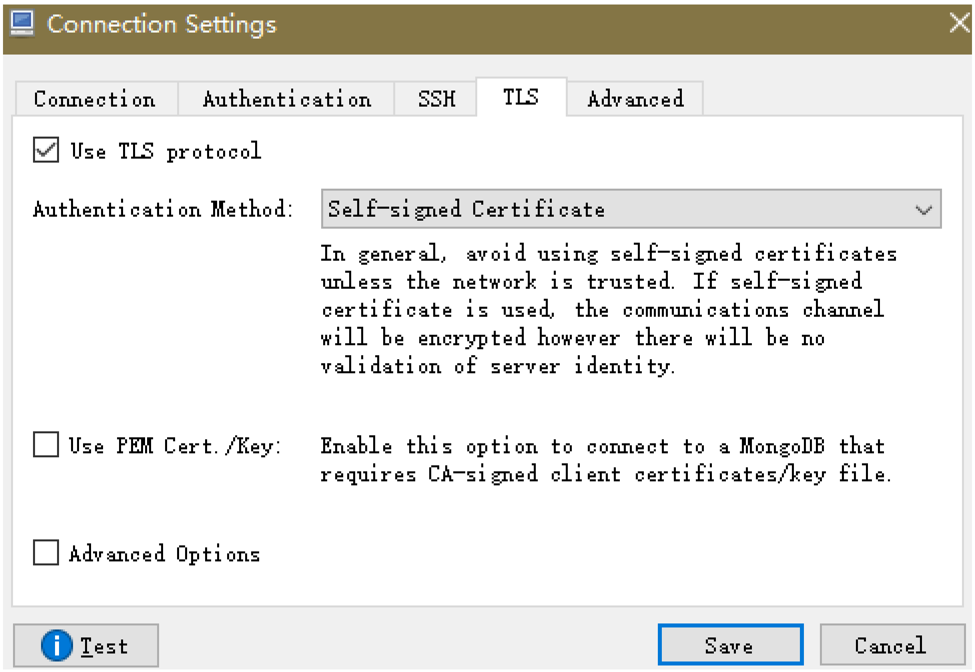
Password: ●●●●●●●●●●

Auth Mechanism: SCRAM-SHA-1

□ Manually specify visible databases

3. On the **TLS** tab, select **Use TLS protocol** and select **Self-signed Certificate** for **Authentication Method**.

Figure 2-42 SSL



☑ Use TLS protocol

Authentication Method: Self-signed Certificate

In general, avoid using self-signed certificates unless the network is trusted. If self-signed certificate is used, the communications channel will be encrypted however there will be no validation of server identity.

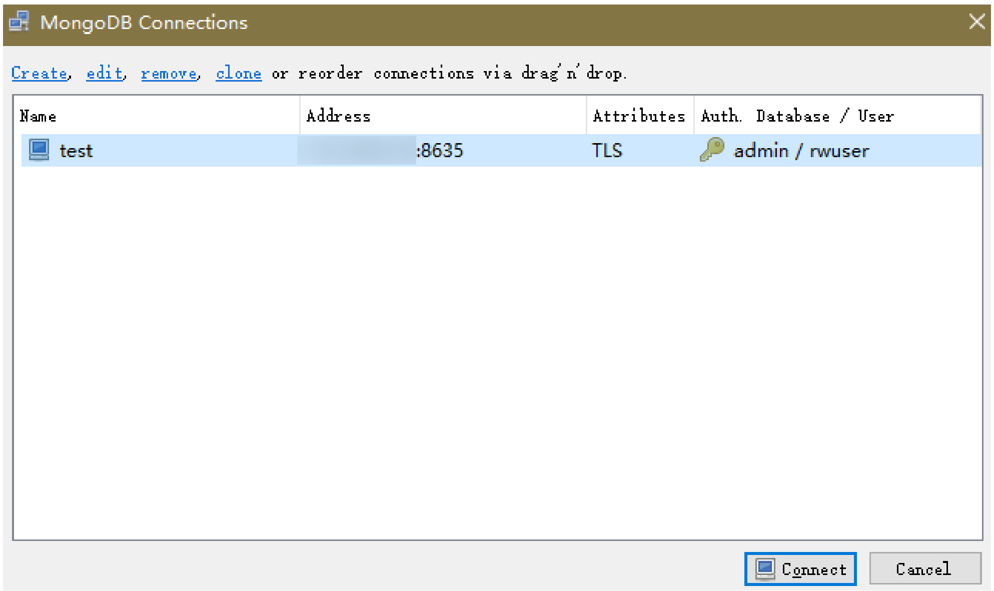
□ Use PEM Cert./Key: Enable this option to connect to a MongoDB that requires CA-signed client certificates/key file.

□ Advanced Options

4. Click **Save**.

Step 3 On the **MongoDB Connections** page, click **Connect** to connect to the cluster instance.

Figure 2-43 Cluster connection information

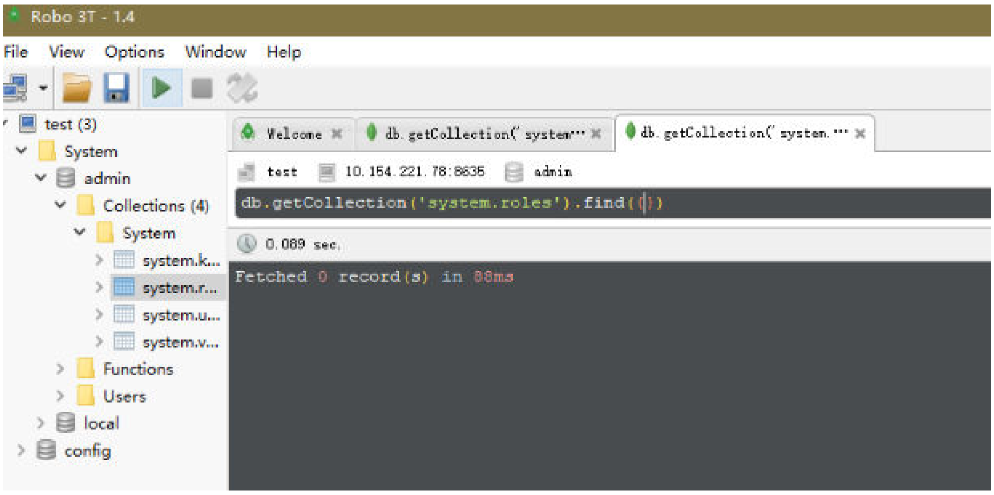


Create, edit, remove, clone or reorder connections via drag'n'drop.

Name	Address	Attributes	Auth. Database / User
test	[redacted]:8635	TLS	admin / rwuser

Step 4 If the cluster instance is successfully connected, the page shown in **Figure 2-44** is displayed.

Figure 2-44 Cluster connected successfully.



```
db.getCollection('system.roles').find({})
```

```
0.089 sec.
Fetched 0 record(s) in 88ms
```

----End

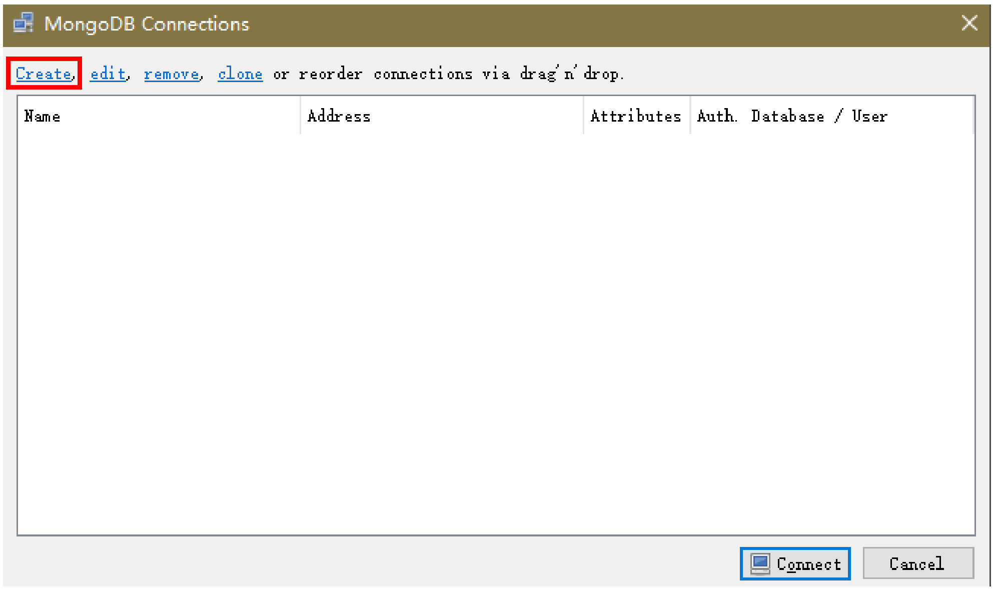
Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details, see **Enabling and Disabling SSL**.

Step 1 Run the installed Robo 3T. On the displayed dialog box, click **Create**.

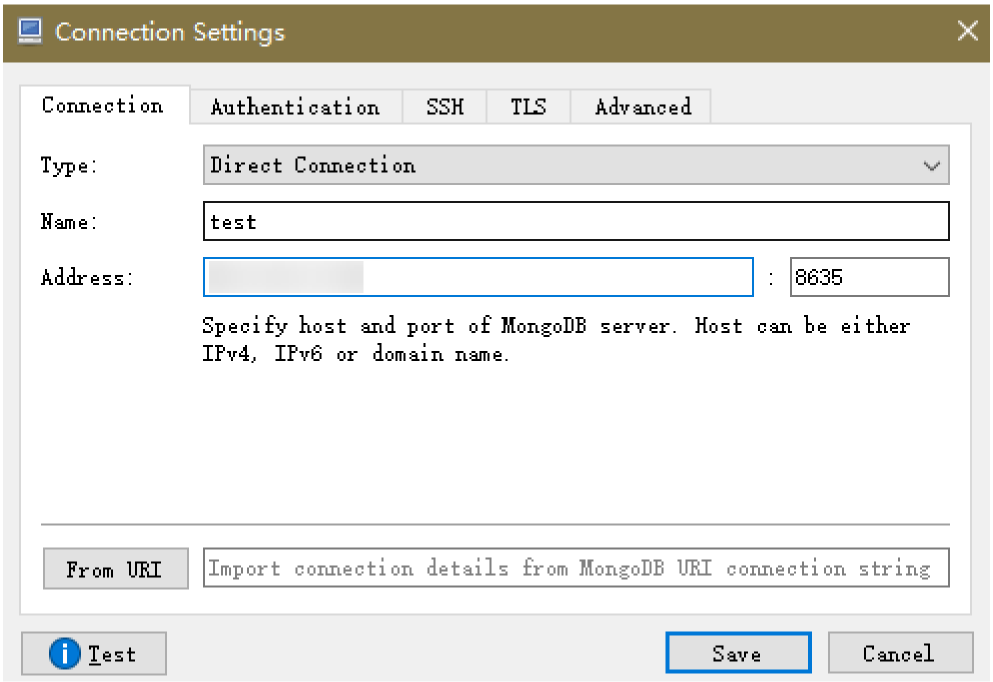
Figure 2-45 Connections



Step 2 In the **Connection Settings** dialog box, set the parameters of the new connection.

1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the DDS DB instance in the **Address** text box.

Figure 2-46 Connection



Type: Direct Connection

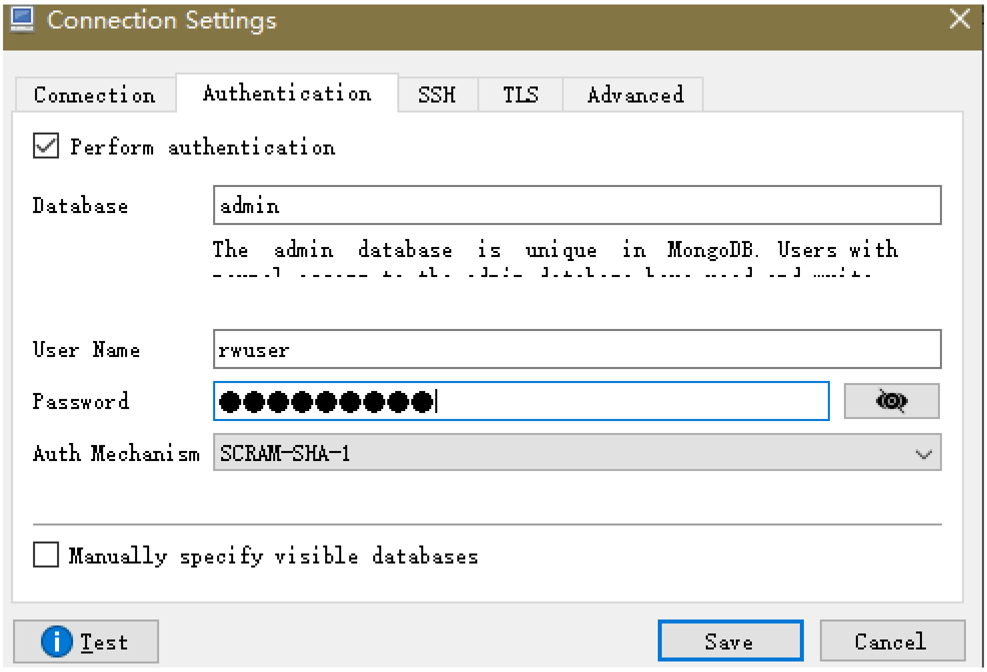
Name: test

Address: [redacted] : 8635

Specify host and port of MongoDB server. Host can be either IPv4, IPv6 or domain name.

2. On the **Authentication** tab, set **Database** to **admin**, **User Name** to **rwuser**, and **Password** to the administrator password you set during the creation of the cluster instance.

Figure 2-47 Authentication



Connection Settings

☑ Perform authentication

Database: admin

The admin database is unique in MongoDB. Users with

User Name: rwuser

Password: ●●●●●●●●●●

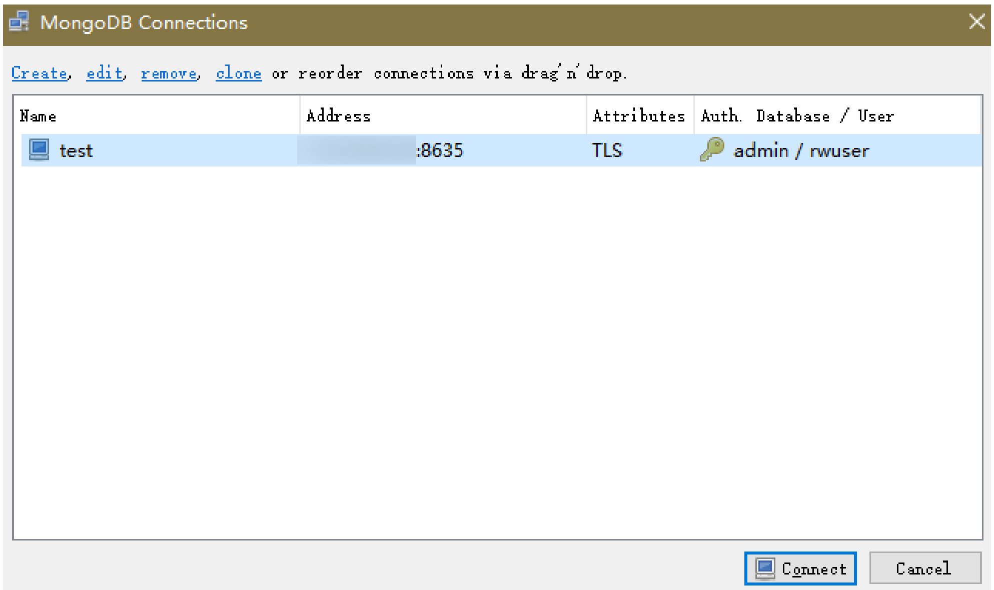
Auth Mechanism: SCRAM-SHA-1

□ Manually specify visible databases

3. Click **Save**.

Step 3 On the **MongoDB Connections** page, click **Connect** to connect to the cluster instance.

Figure 2-48 Cluster connection information



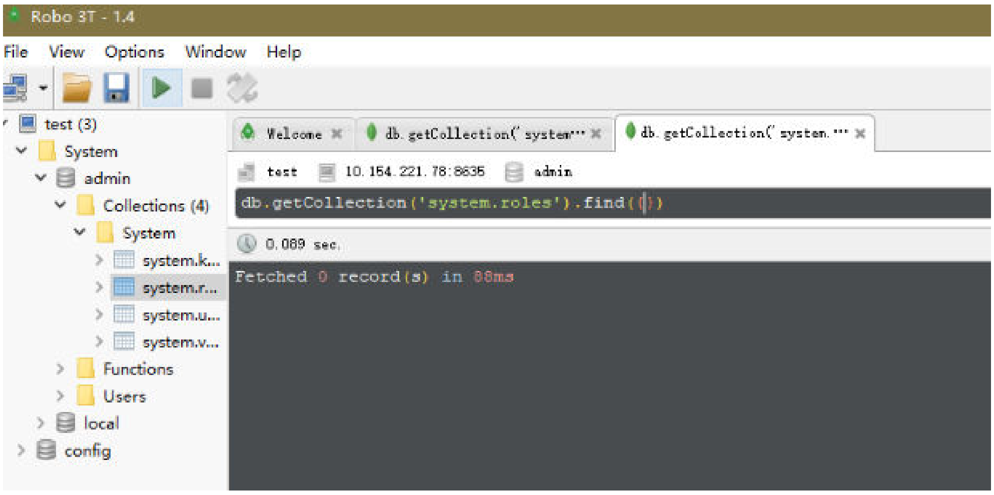
MongoDB Connections

Create, edit, remove, clone or reorder connections via drag'n'drop.

Name	Address	Attributes	Auth. Database / User
test	[redacted]:8635	TLS	admin / rwuser

Step 4 If the cluster instance is successfully connected, the page shown in **Figure 2-49** is displayed.

Figure 2-49 Cluster connected successfully



```
db.getCollection('system.roles').find({})
```

```
Fetched 0 record(s) in 88ms
```

----End

2.2.5 Connecting to a Cluster Instance Using Program Code

2.2.5.1 Java

If you are connecting to an instance using Java, an SSL certificate is optional, but downloading an SSL certificate and encrypting the connection will improve the security of your instance. SSL is disabled by default for newly created instances, but you can enable SSL by referring to **Enabling or Disabling SSL**. SSL encrypts connections to databases but it increases the connection response time and CPU usage. For this reason, enabling SSL is not recommended.

Prerequisites

Familiarize yourself with:

- Computer basics
- Java code

Obtaining and Using Java

- Download the Jar driver from: **https://repo1.maven.org/maven2/org/mongodb/mongo-java-driver/3.0.4/**
- To view the usage guide, visit **https://mongodb.github.io/mongo-java-driver/4.2/driver/getting-started/installation/**.

Using an SSL Certificate

NOTE

- Download the SSL certificate and verify the certificate before connecting to databases.
- On the **Instances** page, click the target DB instance name. In the **DB Information** area on the **Basic Information** page, click ⤓ in the **SSL** field to download the root certificate or certificate bundle.
- For details about how to set up an SSL connection, see the MongoDB Java Driver official document at **https://www.mongodb.com/docs/drivers/java/sync/current/fundamentals/connection/tls/#std-label-tls-ssl**.

If you connect to a cluster instance using Java, the format of code is as follows:

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

Table 2-19 Parameter description

Parameter	Description
<username>	Current username.
<password>	Password for the current username
<instance_ip>	If you attempt to access the instance from an ECS, set *instance_ip* to the private IP address displayed on the **Basic Information** page of the instance to which you intend to connect.
	If you intend to access the instance through an EIP, set *instance_ip* to the EIP that has been bound to the instance.
	If multiple host addresses are required, list the addresses in the format of <instance_ip1>:<instance_port1>,<instance_ip2>:<instance_port2>....... Example: mongodb://username:*****@127.***.***.1:8635,127.***.***.2:8635/?authSource=admin
<instance_port>	Database port displayed on the **Basic Information** page. Default value: **8635**
<database_name>	Name of the database to be connected.
authSource	Authentication user database. The value is **admin**.
ssl	Connection mode. **true** indicates that the SSL connection mode is used.

Use the keytool to configure the CA certificate. For details about the parameters, see **Table 2-20**.

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

Table 2-20 Parameter description

Parameter	Description
<path to certificate authority file>	Path for storing the SSL certificate.
<path to trust store>	Path for storing the truststore. Set this parameter as required, for example, **./trust/certs.keystore**.
<password>	Custom password.

Set the JVM system properties in the program to point to the correct truststore and keystore:

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

For details about the Java code, see the following example:

```
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)
                    .applyToSslSettings(builder -> builder.enabled(true))
                    .applyToSslSettings(builder -> builder.invalidHostNameAllowed(true))
                    .build();
            MongoClient mongoClient = MongoClients.create(settings);
            MongoDatabase database = mongoClient.getDatabase("admin");
            //Ping the database. If the operation fails, an exception occurs.
            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");
        }
    }
}
```

Connection Without the SSL Certificate

NOTE

You do not need to download the SSL certificate because certificate verification on the server is not required.

If you connect to a cluster instance using Java, the format of code is as follows:

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

Table 2-21 Parameter description

Parameter	Description
<username>	Current username.
<password>	Password for the current username
<instance_ip>	If you attempt to access the instance from an ECS, set *instance_ip* to the private IP address displayed on the **Basic Information** page of the instance to which you intend to connect.
	If you intend to access the instance through an EIP, set *instance_ip* to the EIP that has been bound to the instance.
	If multiple host addresses are required, list the addresses in the format of <instance_ip1>:<instance_port1>,<instance_ip2>:<instance_port2>....... Example: mongodb://username:*****@127.***.***.1:8635,127.***.***.2:8635/?authSource=admin
<instance_port>	Database port displayed on the **Basic Information** page. Default value: **8635**
<database_name>	Name of the database to be connected.
authSource	Authentication user database. The value is **admin**.

For details about the Java code, see the following example:

```
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)
                    .retryWrites(true)
                    .build();
            MongoClient mongoClient = MongoClients.create(settings);
            MongoDatabase database = mongoClient.getDatabase("admin");
            //Ping the database. If the operation fails, an exception occurs.
            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

This section describes how to use the MongoDB client in Python to connect to a cluster instance.

Prerequisites

1. To connect an ECS to an instance, the ECS must be able to communicate with the DDS instance. You can run the following command to connect to the IP address and port of the instance server to test the network connectivity.

   curl *ip:port*

   If the message **It looks like you are trying to access MongoDB over HTTP on the native driver port** is displayed, the network connectivity is normal.
2. Install Python and third-party installation package **pymongo** on the ECS. Pymongo 2.8 is recommended.
3. If SSL is enabled, you need to download the root certificate and upload it to the ECS.

Connection Code

- Enabling 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
```

- Disabling 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
```

NOTE

- The authentication database in the URL must be **admin**. That means setting **authSource** to **admin**.
- In SSL mode, you need to manually generate the trustStore file.
- The authentication database must be **admin**, and then switch to the service database.

3 Getting Started with Replica Sets

3.1 Buying a Replica Set Instance

3.1.1 Quick Config

This section describes how to quickly purchase a replica set instance on the management console. DDS provides several recommended configurations to help you purchase a replica set instance within several minutes.

Prerequisites

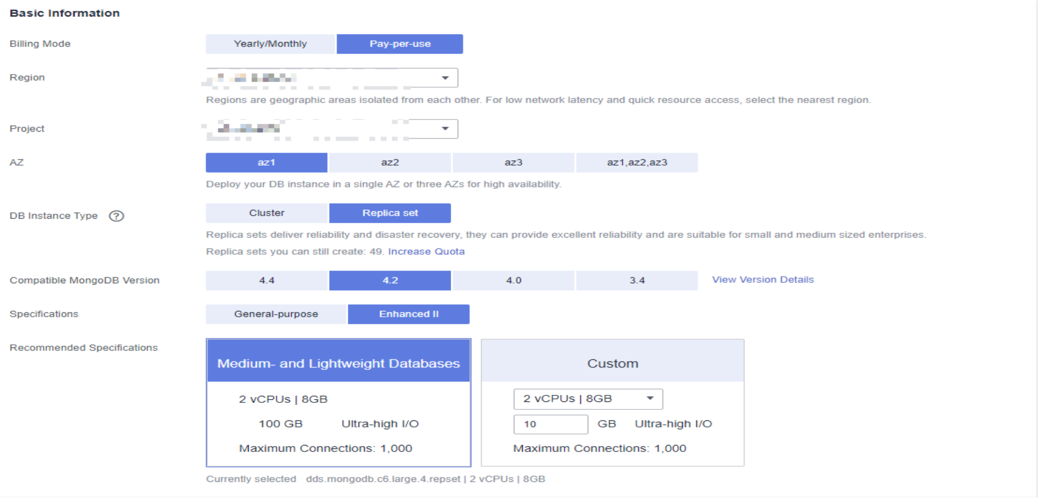
- You have **registered a Huawei ID and enabled Huawei Cloud services**.
- Your account balance is greater than or equal to $0 USD.

Procedure

Step 1 Go to the **Guick Config** page.

Step 2 On the displayed page, select a billing mode and configure information about your DB instance. Then, click **Next**.

Figure 3-1 Basic configurations



Basic Information

Billing Mode: Yearly/Monthly | **Pay-per-use**

Region: [redacted]

Regions are geographic areas isolated from each other. For low network latency and quick resource access, select the nearest region.

Project: [redacted]

AZ: **az1** | az2 | az3 | az1,az2,az3

Deploy your DB instance in a single AZ or three AZs for high availability.

DB Instance Type ?: Cluster | **Replica set**

Replica sets deliver reliability and disaster recovery, they can provide excellent reliability and are suitable for small and medium sized enterprises.

Replica sets you can still create: 49. Increase Quota

Compatible MongoDB Version: 4.4 | **4.2** | 4.0 | 3.4 View Version Details

Specifications: General-purpose | **Enhanced II**

Recommended Specifications:

Medium- and Lightweight Databases
2 vCPUs | 8GB
100 GB Ultra-high I/O
Maximum Connections: 1,000

Custom
2 vCPUs | 8GB
10 GB Ultra-high I/O
Maximum Connections: 1,000

Currently selected dds.mongodb.c6.large.4.repset | 2 vCPUs | 8GB

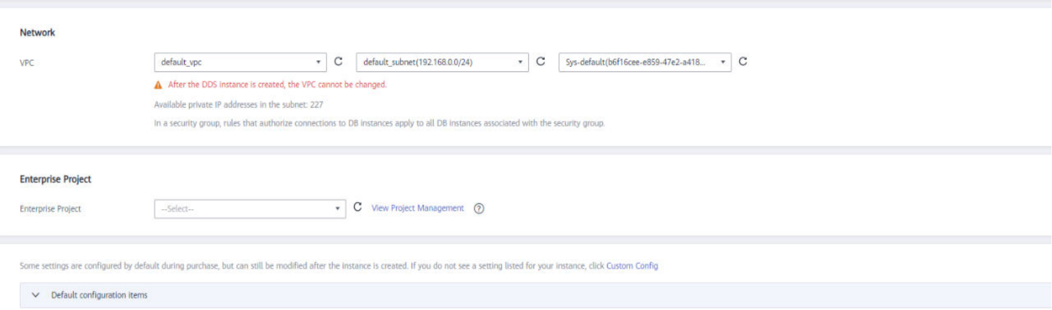
Table 3-1 Basic configurations

Parameter	Description
Billing Mode	Select a billing mode, **Yearly/Monthly** or **Pay-per-use**. ● For yearly/monthly instances – Specify **Required Duration**, and the system deducts the fees incurred from your account based on the service price. – If you do not expect to continue using the instance much after it expires, you can change the billing mode from yearly/monthly to pay-per-use. For details, see **Changing the Billing Mode from Yearly/Monthly to Pay-per-Use**. **NOTE** Instances billed on a yearly/monthly basis cannot be deleted. They can only be unsubscribed from. For details, see **Unsubscribing from a Yearly/Monthly Instance**. ● For pay-per-use instances – You are billed for usage based on how much time the service is in use. – If you expect to use the service extensively over a long period of time, you can change its billing mode from pay-per-use to yearly/monthly to reduce costs. For details, see **Changing the Billing Mode from Pay-per-Use to Yearly/Monthly**.
Region	The region where the resource is located. **NOTE** Instances deployed in different regions cannot communicate with each other through a private network, and you cannot change the region of an instance once it is purchased. Exercise caution when selecting a region.
Project	The project corresponds to the current region and can be changed.

Parameter	Description
AZ	An AZ is a part of a region with its own independent power supply and network. AZs are physically isolated but can communicate through internal network connections. Instances can be deployed in a single AZ or three AZs. ● If your service requires low network latency between instances, you deploy the components of the instance in the same AZ. If you select a single AZ to deploy your instance, anti-affinity deployment is used by default. With an anti-affinity deployment, your primary, secondary, and hidden nodes are deployed on different physical machines for high availability. ● If you want to deploy an instance across AZs for disaster recovery, select three AZs. In this deployment mode, the primary, secondary, and hidden nodes are evenly distributed across three AZs. **NOTE** The 3-AZ deployment is not available in all regions. If the 3-AZ option is not displayed on the page for you to buy an instance, try a different region.
DB Instance Type	Select **Replica set**. A replica set consists of the primary node, secondary node, and hidden node. If a primary node goes down or becomes faulty, a secondary node is automatically assigned to the primary role and continues normal operation. If a secondary node is unavailable, a hidden node will take the role of the secondary to ensure high availability.
Compatible MongoDB Version	● 4.4 ● 4.2 ● 4.0 ● 3.4

Parameter	Description
CPU Type	DDS supports x86 and Kunpeng CPU architectures. **NOTE** This parameter is available only for MongoDB 4.0 and 3.4. The default value is **Kunpeng**. ● x86 x86 CPUs use the Complex Instruction Set Computing (CISC) instruction set. Each instruction can be used to execute low-level hardware operations. CISC instructions vary in length, and tend to be complicated and slow compared to Reduced Instruction Set Computing (RISC). ● Kunpeng The Kunpeng CPU architecture uses RISC. The RISC instruction set is smaller and faster than CISC, thanks to the simplified architecture. Kunpeng CPUs also offer a better balance between power and performance than x86. Kunpeng CPUs offer a high density, low power option that is more cost effective for heavy workloads.
Specifications	With an x86 architecture, you have the following options: ● General-purpose (s6): S6 instances are suitable for applications that require moderate performance generally but occasional bursts of high performance, such as light-workload web servers, enterprise R&D and testing environments, and low- and medium-performance databases. ● Enhanced II (c6): C6 instances have multiple technologies optimized to provide stable powerful compute performance. 25 GE intelligent high-speed NICs are used to provide ultra-high bandwidth and throughput, making it an excellent choice for heavy-load scenarios. It is suitable for websites, web applications, general databases, and cache servers that have higher performance requirements for compute and network resources; and medium- and heavy-load enterprise applications.
Recommended Specifications	Currently, medium- and lightweight database specifications and customized specifications are supported. **NOTE** ● If an instance has less than 16 vCPUs, the storage space ranges from 10 GB to 2000 GB. ● If an instance has more than 16 vCPUs, the storage space ranges from 10 GB to 4000 GB.

Figure 3-2 Network, Required Duration, and Quantity



Network

VPC: default_vpc | default_subnet(192.168.0.0/24) | Sys-default(b6f16cee-e859-47e2-a418...

⚠ After the DDS instance is created, the VPC cannot be changed.

Available private IP addresses in the subnet: 227

In a security group, rules that authorize connections to DB instances apply to all DB instances associated with the security group.

Enterprise Project

Enterprise Project: --Select-- | View Project Management

Some settings are configured by default during purchase, but can still be modified after the instance is created. If you do not see a setting listed for your instance, click Custom Config

Default configuration items

Table 3-2 Network settings

Parameter	Description
VPC	The VPC where your DB instances are located. A VPC isolates networks for different services. It allows you to easily manage and configure private networks and change network configurations. You need to create or select the required VPC. For details, see **Creating a VPC** in the *Virtual Private Cloud User Guide*. For details about the constraints on the use of VPCs, see **Connection Methods**. If there are no VPCs available, DDS creates one for you by default. **NOTE** After the DDS instance is created, the VPC cannot be changed.
Enterprise Project	Only enterprise users can use this function. To use this function, contact customer service. An enterprise project is a cloud resource management mode, in which cloud resources and members are centrally managed by project. Select an enterprise project from the drop-down list. The default project is **default**. For more information about enterprise project, see **Project Management** in *Enterprise Management User Guide*. To customize an enterprise project, click **Enterprise** in the upper right corner of the console. The **Enterprise Management** page is displayed. For details, see **Creating an Enterprise Project** in *Enterprise Management User Guide*.

Table 3-3 Required duration and quantity

Parameter	Description
Required Duration	The system will automatically calculate the fee based on the validity period you have selected.

Parameter	Description
Auto-renew	● By default, this option is not selected. ● If you select this option, the auto-renew cycle is determined by the length of the subscription.
Quantity	The purchase quantity depends on the replica set instance quota. If your current quota does not allow you to purchase the required number of instances, you can apply for increasing the quota as prompted. Yearly/Monthly instances that were purchased in batches have the same specifications except for the instance name and ID.

Step 3 On the displayed page, confirm the instance details.

- For yearly/monthly instances
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, read and agree to the service agreement and click **Pay Now** to go to the payment page and complete the payment.
- For pay-per-use instances
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, read and agree to the service agreement and click **Submit** to start creating the instance.

Step 4 Click **Back to Instance List**. After a DDS instance is created, you can view and manage it on the **Instances** page.

- When an instance is being created, the status displayed in the **Status** column is **Creating**. This process takes about 15 minutes. After the creation is complete, the status changes to **Available**.
- DDS enables the automated backup policy by default. After an instance is created, you can modify or disable the automated backup policy. An automated full backup is immediately triggered after the creation of an instance.

----End

3.1.2 Custom Config

This section describes how to purchase a replica set instance in custom mode on the management console. You can customize the computing resources and storage space of a replica set instance based on your service requirements. In addition, you can configure advanced settings, such as slow query log and automated backup.

Precautions

Each account can create up to 50 replica set instances.

Prerequisites

- You have **registered a Huawei ID and enabled Huawei Cloud services**.
- Your account balance is greater than or equal to $0 USD.
- To display whether the disk is encrypted in the DB instance list, submit a service ticket. In the upper right corner of the management console, choose **Service Tickets > Create Service Ticket**.
- If you want compute and network resources dedicated to your exclusive use, **enable a DeC** and **apply for DCC resources**. Then, you can create DDS instances. Click in the upper left corner and select a region and a project.

NOTE

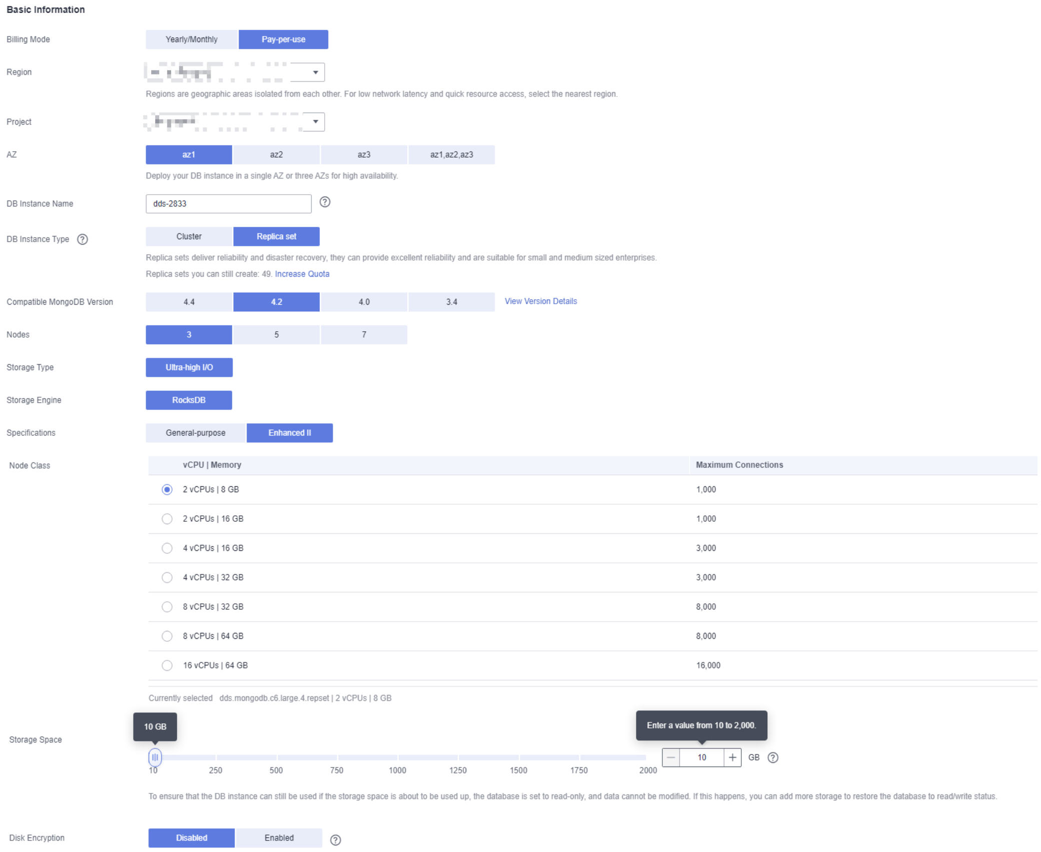
You will be additionally charged for using DeC. Only pay-per-use replica set instances can be purchased through DeC.

Procedure

Step 1 Go to the **Custom Config** page.

Step 2 On the displayed page, select a billing mode and configure information about your DB instance. Then, click **Next**.

Figure 3-3 Basic configurations



Basic Information

Billing Mode: Yearly/Monthly [✓ Pay-per-use]

Region: [redacted]

Regions are geographic areas isolated from each other. For low network latency and quick resource access, select the nearest region.

Project: [redacted]

AZ: [✓ az1] az2 az3 az1,az2,az3

Deploy your DB instance in a single AZ or three AZs for high availability.

DB Instance Name: dds-2833

DB Instance Type: Cluster [✓ Replica set]

Replica sets deliver reliability and disaster recovery, they can provide excellent reliability and are suitable for small and medium sized enterprises.

Replica sets you can still create: 49. Increase Quota

Compatible MongoDB Version: 4.4 [✓ 4.2] 4.0 3.4 View Version Details

Nodes: [✓ 3] 5 7

Storage Type: [✓ Ultra-high I/O]

Storage Engine: [✓ RocksDB]

Specifications: General-purpose [✓ Enhanced II]

Node Class

	vCPU | Memory	Maximum Connections
●	2 vCPUs | 8 GB	1,000
○	2 vCPUs | 16 GB	1,000
○	4 vCPUs | 16 GB	3,000
○	4 vCPUs | 32 GB	3,000
○	8 vCPUs | 32 GB	8,000
○	8 vCPUs | 64 GB	8,000
○	16 vCPUs | 64 GB	16,000

Currently selected dds.mongodb.c6.large.4.repset | 2 vCPUs | 8 GB

Storage Space: 10 GB

Enter a value from 10 to 2,000.

To ensure that the DB instance can still be used if the storage space is about to be used up, the database is set to read-only, and data cannot be modified. If this happens, you can add more storage to restore the database to read/write status.

Disk Encryption: [✓ Disabled] Enabled

Table 3-4 Billing Mode

Parameter	Description
Billing Mode	Select a billing mode, **Yearly/Monthly** or **Pay-per-use**. ● For yearly/monthly instances – Specify **Required Duration**, and the system deducts the fees incurred from your account based on the service price. – If you do not expect to continue using the instance much after it expires, you can change the billing mode from yearly/monthly to pay-per-use. For details, see **Changing the Billing Mode from Yearly/Monthly to Pay-per-Use**.. **NOTE** Instances billed on a yearly/monthly basis cannot be deleted. They can only be unsubscribed from. For details, see **Unsubscribing from a Yearly/Monthly Instance**. ● For pay-per-use instances – You are billed for usage based on how much time the service is in use. – If you expect to use the service extensively over a long period of time, you can change its billing mode from pay-per-use to yearly/monthly to reduce costs. For details, see **Changing the Billing Mode from Pay-per-Use to Yearly/Monthly**..
Region	The region where the resource is located. **NOTE** Instances deployed in different regions cannot communicate with each other through a private network, and you cannot change the region of an instance once it is purchased. Exercise caution when selecting a region.
Project	The project corresponds to the current region and can be changed.

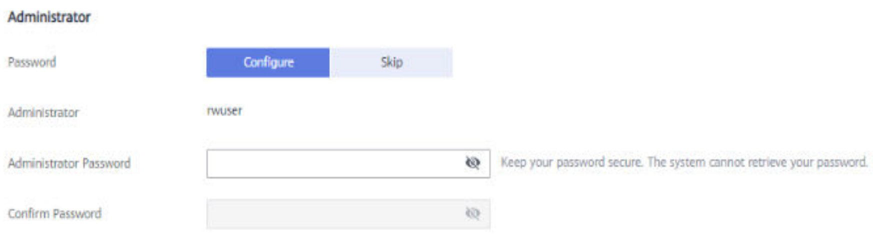
Parameter	Description
AZ	An AZ is a part of a region with its own independent power supply and network. AZs are physically isolated but can communicate through internal network connections. Instances can be deployed in a single AZ or three AZs. ● If your service requires low network latency between instances, you deploy the components of the instance in the same AZ. If you select a single AZ to deploy your instance, anti-affinity deployment is used by default. With an anti-affinity deployment, your primary, secondary, and hidden nodes are deployed on different physical machines for high availability. ● If you want to deploy an instance across AZs for disaster recovery, select three AZs. In this deployment mode, the primary, secondary, and hidden nodes are evenly distributed across three AZs. **NOTE** The 3-AZ deployment is not available in all regions. If the 3-AZ option is not displayed on the page for you to buy an instance, try a different region.
DB Instance Name	● The instance name that you specify after the purchase. The instance name must contain 4 to 64 characters and must start with a letter. It is case sensitive and can contain letters, digits, hyphens (-), and underscores (_). It cannot contain other special characters. ● The instance name can be the same as an existing instance name. ● If you buy a batch of instances at once, a 4-digit numerical suffix will be added to the instance names, starting with **-0001**. If you later make another batch purchase, the new instance names will be numbered first using any suffixes missing from the sequence of your existing instances, and then continuing on from where your last batch purchase left off. For example, a batch of 3 instances get the suffixes **-0001**, **-0002**, and **-0003**. If you deleted instance **0002** and then bought 3 more instances, the new instances would get the suffixes **-0002**, **-0004**, and **-0005**. ● After the DB instance is created, you can change its name. For details, see **Changing an Instance Name**.
DB Instance Type	Select **Replica set**. A replica set consists of the primary node, secondary node, and hidden node. If a primary node goes down or becomes faulty, a secondary node is automatically assigned to the primary role and continues normal operation. If a secondary node is unavailable, a hidden node will take the role of the secondary to ensure high availability.

Parameter	Description
Compatible MongoDB Version	● 4.4 ● 4.2 ● 4.0 ● 3.4
Nodes	You can create a three-node, five-node, or seven-node replica set instance.
CPU Type	DDS supports x86 and Kunpeng CPU architectures. **NOTE** This parameter is available only for MongoDB 4.0 and 3.4. The default value is **Kunpeng**. ● x86 x86 CPUs use the Complex Instruction Set Computing (CISC) instruction set. Each instruction can be used to execute low-level hardware operations. CISC instructions vary in length, and tend to be complicated and slow compared to Reduced Instruction Set Computing (RISC). ● Kunpeng The Kunpeng CPU architecture uses RISC. The RISC instruction set is smaller and faster than CISC, thanks to the simplified architecture. Kunpeng CPUs also offer a better balance between power and performance than x86. Kunpeng CPUs offer a high density, low power option that is more cost effective for heavy workloads.
Storage Type	The storage type can be **Ultra-high I/O** and **Extreme SSD** for non-DeC users. For DeC users, the supported storage types depend on the selected resource type. ● If you select **EVS** for **Resource Type**, **Storage Type** is set to **Cloud SSD**. ● If you select **DSS** for **Resource Type**, **Storage Type** can be set to **Common I/O**, **High I/O**, or **Cloud SSD**.
Storage Engine	● WiredTiger WiredTiger is the default storage engine of DDS 3.4 and 4.0. WiredTiger provides different granularity concurrency control and compression mechanism for data management. It can provide the best performance and storage efficiency for different kinds of applications. ● RocksDB RocksDB is the default storage engine of DDS 4.2. RocksDB supports efficient point lookup, range scan, and high-speed write. RocksDB can be used as the underlying data storage engine of MongoDB and is suitable for scenarios with a large number of write operations.

Parameter	Description
Specifications	With an x86 architecture, you have the following options: ● General-purpose (s6): S6 instances are suitable for applications that require moderate performance generally but occasional bursts of high performance, such as light-workload web servers, enterprise R&D and testing environments, and low- and medium-performance databases. ● Enhanced II (c6): C6 instances have multiple technologies optimized to provide stable powerful compute performance. 25 GE intelligent high-speed NICs are used to provide ultra-high bandwidth and throughput, making it an excellent choice for heavy-load scenarios. It is suitable for websites, web applications, general databases, and cache servers that have higher performance requirements for compute and network resources; and medium- and heavy-load enterprise applications.
Node Class	For details about the instance specifications, see **Instance Specifications**. For details about the performance data of DB instances of different specifications, see **Performance White Paper**. If the CPU or memory of a created DB instance cannot meet service requirements, you can change it on the management console. For details, see **Changing a Replica Set Instance Class**.
Storage Space	If an instance has less than 16 vCPUs, the storage space ranges from 10 GB to 2000 GB. If an instance has more than 16 vCPUs, the storage space ranges from 10 GB to 4000 GB. The value must be an integer multiple of 10. You can scale up an instance after it is created. For details, see **Scaling Up a Replica Set Instance**. **NOTE** ● If the storage space you purchased exceeds 600 GB and the remaining storage space is 18 GB, the instance becomes **Read-only**. ● If the storage space you purchased is less than 600 GB and the storage space usage reaches 97%, the instance becomes **Read-only**. In these cases, delete unnecessary resources or expand the capacity.

Parameter	Description
Disk Encryption	● **Disabled**: Disable encryption. ● **Enabled**: Enable encryption. This feature improves data security but slightly affects read/write performance. **Key Name**: Select or create a private key, which is the tenant key. **NOTE** ● After an instance is created, the disk encryption status and the key cannot be changed. Disk encryption will not encrypt backup data stored in OBS. To enable backup data encryption, contact customer service. ● To check whether the disk is encrypted, you can view **Disk Encrypted** in the DB instance list. ● If disk encryption or backup data encryption is enabled, keep the key properly. Once the key is disabled, deleted, or frozen, the database will be unavailable and data may not be restored. If disk encryption is enabled but backup data encryption is not enabled, you can **restore data to a new instance from backups**. If both disk encryption and backup data encryption are enabled, data cannot be restored. ● For details about how to create a key, see "**Creating a CMK**" in *Data Encryption Workshop User Guide*.

Figure 3-4 Administrator settings



Administrator

Password: Configure | Skip

Administrator: rwuser

Administrator Password: Keep your password secure. The system cannot retrieve your password.

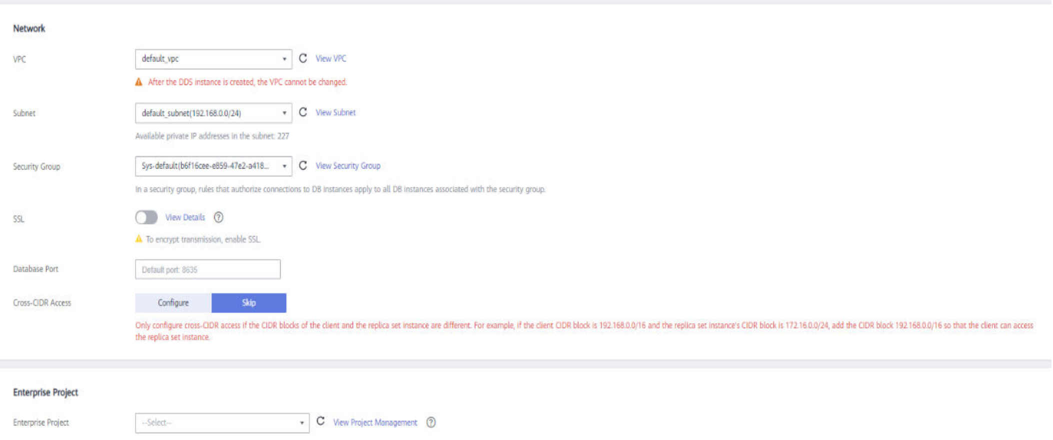
Confirm Password

Table 3-5 Administrator settings

Parameter	Description
Password	● Configure Enter and confirm the new administrator password. After an instance is created, you can connect to the instance using the password. ● Skip To log in, you will have to reset the password later on the **Basic Information** page. If you need to connect to an instance after it is created, locate the instance and choose **More** > **Reset Password** in the **Operation** column to set a password for the instance first.
Administrator	The default account is **rwuser**.

Parameter	Description
Administrator Password	Set a password for the administrator. The password must be 8 to 32 characters in length and contain uppercase letters, lowercase letters, digits, and at least one of the following special characters: ~!@#%^*-_=+?()$ Keep this password secure. If lost, the system cannot retrieve it for you.
Confirm Password	Enter the administrator password again.

Figure 3-5 Network, Required Duration, and Quantity



Network

VPC: default_vpc

After the DDS instance is created, the VPC cannot be changed.

Subnet: default_subnet(192.168.0.0/24)

Available private IP addresses in the subnet: 227

Security Group: Sys-default(b6f16cee-e859-47e2-a418...

In a security group, rules that authorize connections to DB instances apply to all DB instances associated with the security group.

SSL

To encrypt transmission, enable SSL.

Database Port: Default port: 8635

Cross-CIDR Access: Configure / Skip

Only configure cross-CIDR access if the CIDR blocks of the client and the replica set instance are different. For example, if the client CIDR block is 192.168.0.0/16 and the replica set instance's CIDR block is 172.16.0.0/24, add the CIDR block 192.168.0.0/16 so that the client can access the replica set instance.

Enterprise Project

Enterprise Project: --Select--

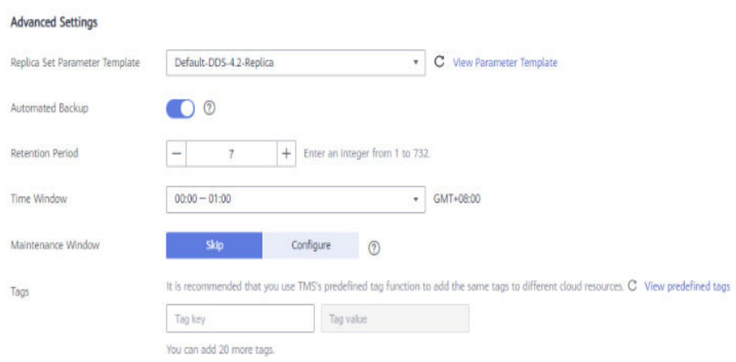
Table 3-6 Network

Parameter	Description
VPC	The VPC where your DB instances are located. A VPC isolates networks for different services. It allows you to easily manage and configure private networks and change network configurations. You will need to create or select the required VPC. For details about how to create a VPC, see "Creating a VPC" in *Virtual Private Cloud User Guide*. For details about the constraints on the use of VPCs, see **Connection Methods**. If there are no VPCs available, DDS creates one for you by default. **NOTE** After the DDS instance is created, the VPC cannot be changed.

Parameter	Description
Subnet	A subnet provides dedicated network resources that are logically isolated from other networks for security reasons. After the instance is created, you can change the private IP address assigned by the subnet. For details, see **Changing a Private IP Address**. **NOTE** IPv6 subnets are not supported. You are advised to create and select IPv4 subnets.
Security Group	A security group controls access between DDS and other services. If there are no security groups available, DDS creates one for you by default. **NOTE** ● Ensure that there is a security group rule configured that allows clients to access instances. For example, select an inbound TCP rule with the default port 8635, and enter a subnet IP address or select a security group that the instance belongs to. ● When creating a DB instance, you can select multiple security groups. For better network performance, you are advised to select no more than five security groups. In such a case, the access rules of all the selected security groups apply on the instance.
SSL	Secure Sockets Layer (SSL) encrypts connections between clients and servers, preventing data from being tampered with or stolen during transmission. You can enable SSL to improve data security. After an instance is created, you can connect to it using SSL.
Database Port	The default DDS port is 8635, but this port can be modified if necessary. If you change the port, add a corresponding security group rule to allow access to the instance. **NOTE** ● For details about how to change a database port, see **Changing a Database Port**.

Parameter	Description
Cross-CIDR Access	● Configure If a client and a replica set instance are deployed in different CIDR blocks and the client is not in 192.168.0.0/16, 172.16.0.0/24, or 10.0.0.0/8, configure Cross-CIDR Access for the instance to communicate with the client. **NOTE** – To ensure the ECS and the DB instance can communicate with each other, configure the connection by referring to **VPC Peering Connection Overview**. – Up to 30 CIDR blocks can be configured, and each of them can overlap but they cannot be the same. That is, the source CIDR blocks can overlap but cannot be the same. The CIDR blocks cannot start with 127. The allowed IP mask ranges from 8 to 32. ● Skip Configure the CIDR block of the client later. After a DB instance is created, you can configure cross-CIDR access by referring to **Configuring Cross-CIDR Access**.
Enterprise Project	Only enterprise users can use this function. To use this function, contact customer service. An enterprise project is a cloud resource management mode, in which cloud resources and members are centrally managed by project. Select an enterprise project from the drop-down list. The default project is **default**.

Figure 3-6 Advanced settings



Advanced Settings

Replica Set Parameter Template: Default-DDS-4.2-Replica

Automated Backup: ●

Retention Period: 7 Enter an integer from 1 to 732.

Time Window: 00:00 – 01:00 GMT+08:00

Maintenance Window: Skip

Tags: It is recommended that you use TMS's predefined tag function to add the same tags to different cloud resources.

You can add 20 more tags.

Table 3-7 Advanced settings

Parameter	Description
Replica Set Parameter Template	The parameters that apply to the replica set instances. After an instance is created, you can change the parameter template you configured for the instance to bring out the best performance. For details, see **Editing a Parameter Template**.
Automated Backup	DDS enables an automated backup policy by default, but you can disable it after an instance is created. An automated full backup is immediately triggered after the creation of an instance. For details, see **Configuring an Automated Backup Policy**.
Retention Period (days)	**Retention Period** refers to the number of days that data is kept. You can increase the retention period to improve data reliability. The backup retention period is from 1 to 732 days.
Time Window	The backup interval is 1 hour.

Parameter	Description
Tags	(Optional) You can add tags to DDS instances so that you can quickly search for and filter specified instances by tag. Each DDS instance can have up to 20 tags. If your organization has configured tag policies for DDS, add tags to DB instances based on the policies. If a tag does not comply with the policies, DB instance creation may fail. Contact your organization administrator to learn more about tag policies. ● Create a tag. You can create tags on the DDS console and configure the tag **key** and **value**. Key: This parameter is mandatory. – Each tag key must be unique for each instance. – A tag key consists of up to 36 characters. – The key must consist of only digits, letters, underscores (_), and hyphens (-). Value: This parameter is optional. – The value consists of up to 43 characters. – The value must consist of only digits, letters, underscores (_), periods (.), and hyphens (-). ● Add a predefined tag. Predefined tags can be used to identify multiple cloud resources. To tag a cloud resource, you can select a created predefined tag from the drop-down list, without entering a key and value for the tag. For example, if a predefined tag has been created, its key is Usage and value is Project1. When you configure the key and value for a cloud resource, the created predefined tag will be displayed on the page. After an instance is created, you can click the instance name to view its tags. On the **Tags** page, you can also **modify or delete the tags**. In addition, you can quickly **search for and filter specified instances by tag**. You can add a tag to an instance after the instance is created. For details, see **Adding a Tag**.

If you have any question about the price, click **Price Details**.

NOTE

Instance performance depends on the specifications you select during creation. The hardware configuration items that can be selected include the instance class and storage space.

Step 3 On the displayed page, confirm the instance details.

- For yearly/monthly instances
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, read and agree to the service agreement and click **Pay Now** to go to the payment page and complete payment.
- For pay-per-use instances
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, read and agree to the service agreement and click **Submit** to start creating the instance.

Step 4 Click **Back to Instance List**. After a DDS instance is created, you can view and manage it on the **Instances** page.

- When an instance is being created, the status displayed in the **Status** column is **Creating**. This process takes about 15 minutes. After the creation is complete, the status changes to **Available**.
- Yearly/Monthly instances that were purchased in batches have the same specifications except for the instance name and ID.

----End

3.2 Connecting to a Replica Set Instance

3.2.1 Connection Methods

You can access DDS over private or public networks.

Table 3-8 Connection methods

Method	IP Address	Scenario	Description
DAS	Not required	DAS provides a GUI and allows you to perform visualized operations on the console. SQL execution, advanced database management, and intelligent O&M are available to make database management simple, secure, and intelligent.	• Easy to use, secure, advanced, and intelligent • Recommended

Method	IP Address	Scenario	Description
Private network	Private IP address	DDS provides a private IP address by default. If your applications are running on an ECS in the same region, AZ, and VPC subnet as your DDS instance, you are advised to use a private IP address to connect the ECS to your DDS instances.	Secure and excellent performance
Public network	EIP	● If your applications are running on an ECS that is in a different region from the one where the DB instance is located, use an EIP to connect the ECS to your DDS DB instances. ● If your applications are deployed on another cloud platform, EIP is recommended.	● Low security ● For faster transmission and improved security, you are advised to migrate your applications to an ECS that is in the same subnet as your DDS instance and use a private IP address to access the instance.

3.2.2 (Recommended) Connecting to Replica Set Instances Through DAS

3.2.2.1 Overview

DAS provides a GUI and allows you to perform visualized operations on the console. SQL execution, advanced database management, and intelligent O&M are available to make database management simple, secure, and intelligent. You are advised to use DAS to connect to DB instances.

This section describes how to buy a replica set instance on the management console and how to connect to the replica set instance through DAS.

Process

To purchase and connect to a replica set instance, perform the following steps:

1. **Buy a replica set instance.**
2. **Connect to the replica set instance through DAS.**

3.2.2.2 Connecting to a Replica Set Instance Through DAS

Data Admin Service (DAS) enables you to manage DB instances on a web-based console, simplifying database management and improving working efficiency. You can connect and manage instances through DAS. By default, you have the permission required for remote login. It is recommended that you use the DAS service to connect to instances. DAS is secure and convenient.

Procedure

Step 1 Log in to the management console.

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

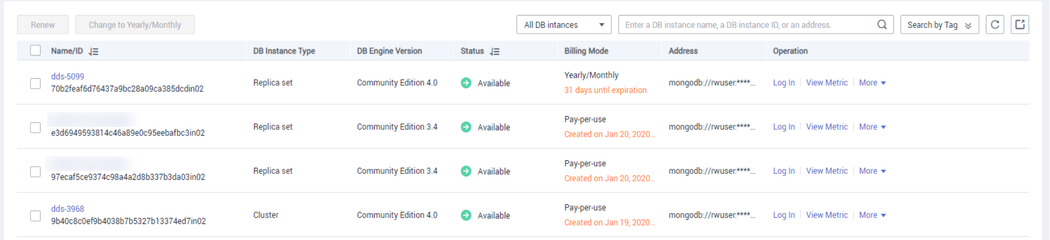
If you want compute and network resources dedicated to your exclusive use, **enable a DeC** and **apply for DCC resources**. After enabling a DeC, you can select the DeC region and project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, locate the target DB instance and click **Log In** in the **Operation** column.

Alternatively, click the target DB instance on the **Instances** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner of the page.

Figure 3-7 Instance management



□	Name/ID	DB Instance Type	DB Engine Version	Status	Billing Mode	Address	Operation
□	dds-5099 70b2feaf6d76437a9bc28a09ca385dcdin02	Replica set	Community Edition 4.0	Available	Yearly/Monthly 31 days until expiration	mongodb://rwuser:****...	Log In | View Metric | More
□	[redacted] e3d6949593814c46a89e0c95eebafbc3in02	Replica set	Community Edition 3.4	Available	Pay-per-use Created on Jan 20, 2020...	mongodb://rwuser:****...	Log In | View Metric | More
□	[redacted] 97ecaf5ce9374c98a4a2d8b337b3da03in02	Replica set	Community Edition 3.4	Available	Pay-per-use Created on Jan 20, 2020...	mongodb://rwuser:****...	Log In | View Metric | More
□	dds-3968 9b40c8c0ef9b4038b7b5327b13374ed7in02	Cluster	Community Edition 4.0	Available	Pay-per-use Created on Jan 19, 2020...	mongodb://rwuser:****...	Log In | View Metric | More

Step 5 On the displayed login page, enter the administrator username and password and click **Log In**.

For details about how to manage databases through DAS, see **DDS Instance Management**.

----End

3.2.3 Connecting to a Replica Set Instance over a Private Network

3.2.3.1 Configuring Security Group Rules

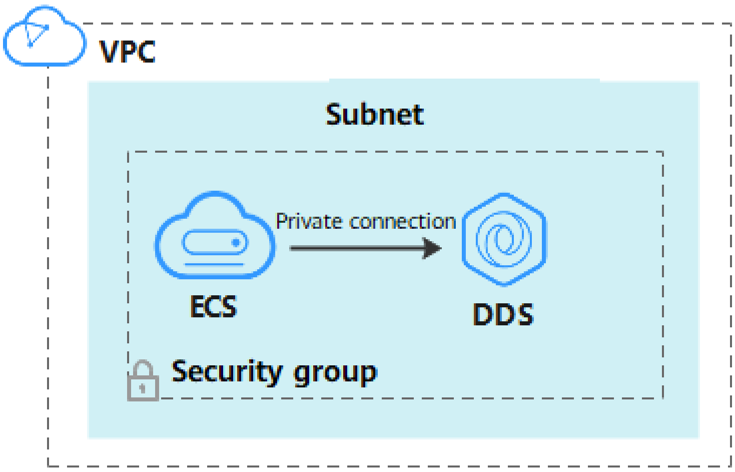
A security group is a collection of access control rules for ECSs and DDS instances that have the same security protection requirements and are mutually trusted in a VPC.

To ensure database security and reliability, you need to configure security group rules to allow specific IP addresses and ports to access DDS instances.

You can connect to an instance by configuring security group rules in following two ways:

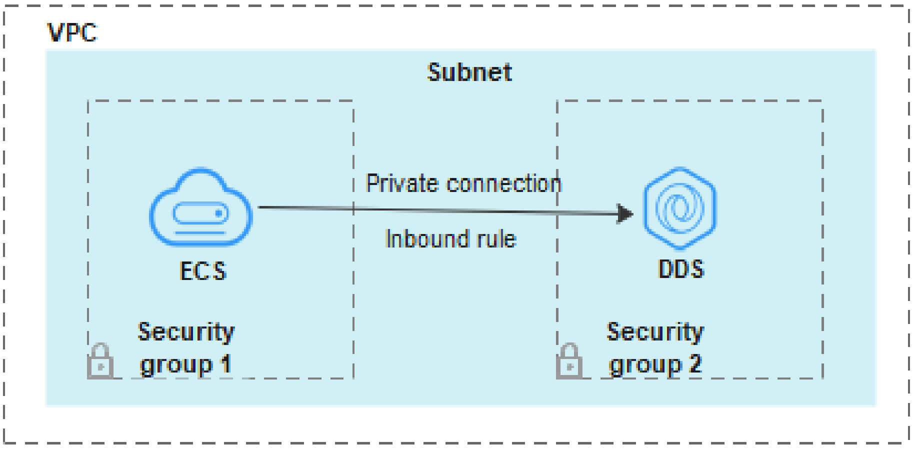
- If the ECS and instance are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to **Connecting to a Replica Set Instance Using Mongo Shell (Private Network)**.

  Figure 3-8 Same security group

- If the ECS and instance are in different security groups, you need to configure security group rules for them, separately.

  Figure 3-9 Different security groups

  – Instance: Configure an **inbound rule** for the security group associated with the instance.
  – ECS: The default security group rule allows all outbound data packets. In this case, you do not need to configure a security group rule for the ECS. If not all traffic is allowed to reach the instance, configure an **outbound** rule for the ECS.

This section describes how to configure an inbound rule for an instance.

Precautions

- By default, an account can create up to 500 security group rules.
- Too many security group rules will increase the first packet latency, so a maximum of 50 rules for each security group is recommended.
- By default, one DDS instance is associated with only one security group.
- DDS allows you to associate multiple security groups to a DB instance. You can apply for the service based on your service requirements. For better network performance, you are advised to select no more than five security groups.

Procedure

Step 1 Log in to the management console.

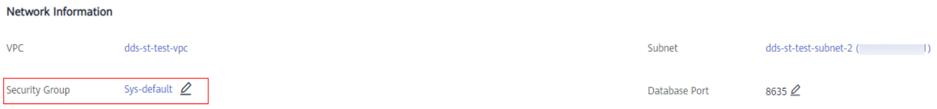
Step 2 Click 📍 in the upper left corner and select a region and a project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the instance name. The **Basic Information** page is displayed.

Step 5 In the **Network Information** area on the **Basic Information** page, click the security group.

Figure 3-10 Security Group

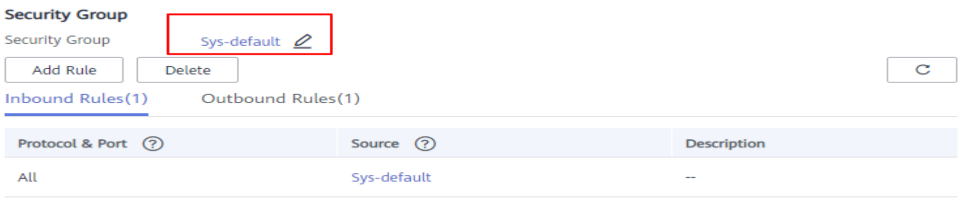


Network Information

VPC	dds-st-test-vpc	Subnet	dds-st-test-subnet-2 ([redacted])
Security Group	Sys-default	Database Port	8635

You can also choose **Connections** in the navigation pane on the left. On the **Private Connection** tab, in the **Security Group** area, click the security group name.

Figure 3-11 Security Group



Security Group

Security Group Sys-default

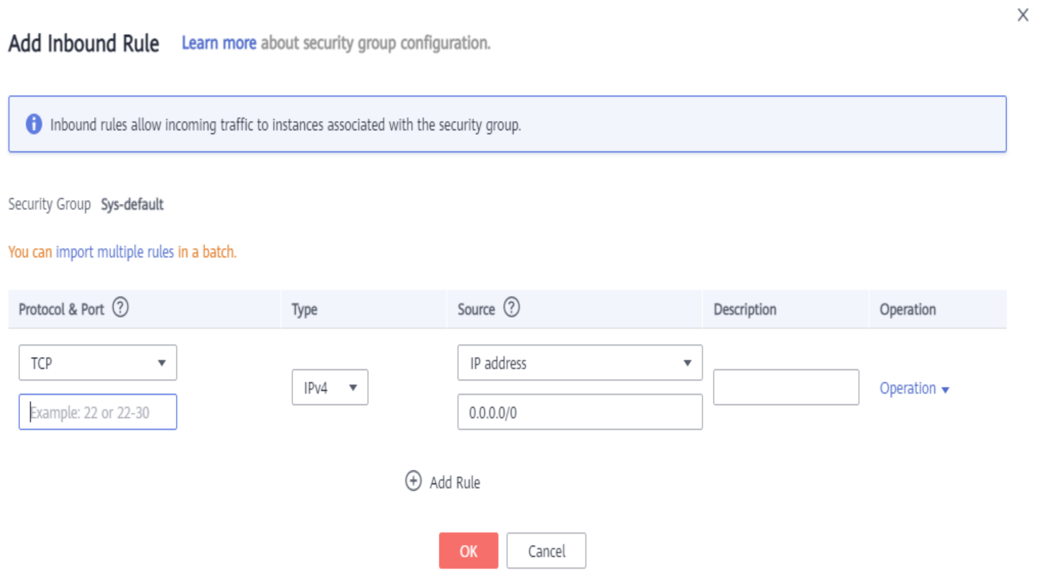
Protocol & Port	Source	Description
All	Sys-default	--

Step 6 On the **Security Group** page, locate the target security group and click **Manage Rule** in the **Operation** column.

Step 7 On the **Inbound Rules** tab, click **Add Rule**. The **Add Inbound Rule** dialog box is displayed.

Step 8 Add a security group rule as prompted.

Figure 3-12 Add Inbound Rule



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group Sys-default

You can import multiple rules in a batch.

Protocol & Port	Type	Source	Description	Operation
TCP Example: 22 or 22-30	IPv4	IP address 0.0.0.0/0		Operation

Table 3-9 Inbound rule settings

Parameter	Description	Example
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	The security group rule actions. A rule with a deny action overrides another with an allow action if the two rules have the same priority.	Allow
Protocol & Port	The network protocol required for access. Available options: **TCP**, **UDP**, **ICMP**, or **GRE**	TCP
	Port: the port on which you wish to allow access to DDS. The default port is 8635. The port ranges from 2100 to 9500 or can be 27017, 27018, or 27019.	8635
Type	IP address type. Only **IPv4** and **IPv6** are supported.	IPv4

Parameter	Description	Example
Source	Specifies the supported IP address, security group, and IP address group, which allow access from IP addresses or instances in other security group. Example: - Single IP address: 192.168.10.10/32 - IP address segment: 192.168.1.0/24 - All IP addresses: 0.0.0.0/0 - Security group: sg-abc - IP address group: ipGroup-test If you enter a security group, all ECSs associated with the security group comply with the created rule. For more information about IP address groups, see **IP Address Group**.	0.0.0.0/0
Description	(Optional) Provides supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

Step 9 Click **OK**.

----End

3.2.3.2 Connecting to a Replica Set Instance Using Mongo Shell (Private Network)

Mongo shell is the default client for the MongoDB database server. You can use Mongo Shell to connect to DB instances, and query, update, and manage data in databases. DDS is compatible with MongoDB. Mongo Shell is a part of the MongoDB client. To use Mongo Shell, download and install the MongoDB client first, and then use the Mongo shell to connect to the DB instance.

By default, a DDS instance provides a private IP address. If your applications are deployed on an ECS and are in the same region and VPC as DDS instances, you can connect to DDS instances using a private IP address to achieve a fast transmission rate and high security.

This section describes how to use Mongo Shell to connect to a replica set instance over a private network.

The MongoDB client can connect to an instance with an unencrypted connection or an encrypted connection (SSL). To improve data transmission security, connect to instances using SSL.

Prerequisites

1. For details about how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.
2. Install the MongoDB client on the ECS. To ensure successful authentication, install the MongoDB client of the same version as the target instance.

   For details about how to install a MongoDB client, see **How Can I Install a MongoDB Client?**
3. The ECS can communicate with the DDS instance. For details, see **Configuring Security Group Rules**.

SSL Connection

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

Step 1 **Log in to the management console**.

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

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the instance name.

Step 5 In the navigation pane on the left, choose **Connections**.

Step 6 In the **Basic Information** area, click ⤓ next to the **SSL** field.

Step 7 Upload the root certificate to the ECS to be connected to the instance.

The following describes how to upload the certificate to a Linux and Window ECS:

- In Linux, run the following command:

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

  NOTE

  - **IDENTITY_FILE** is the directory where the root certificate resides. The file access permission is 600.
  - **REMOTE_USER** is the ECS OS user.
  - **REMOTE_ADDRESS** is the ECS address.
  - **REMOTE_DIR** is the directory of the ECS to which the root certificate is uploaded.
- In Windows, upload the root certificate using a remote connection tool.

Step 8 Connect to a DDS instance.

Method 1: Using the private HA connection address (recommended)

DDS provides the HA connection address. Using this address to connect to a replica set instance improves data read/write performance and prevents errors reported when data is written from the client after a primary/standby switchover.

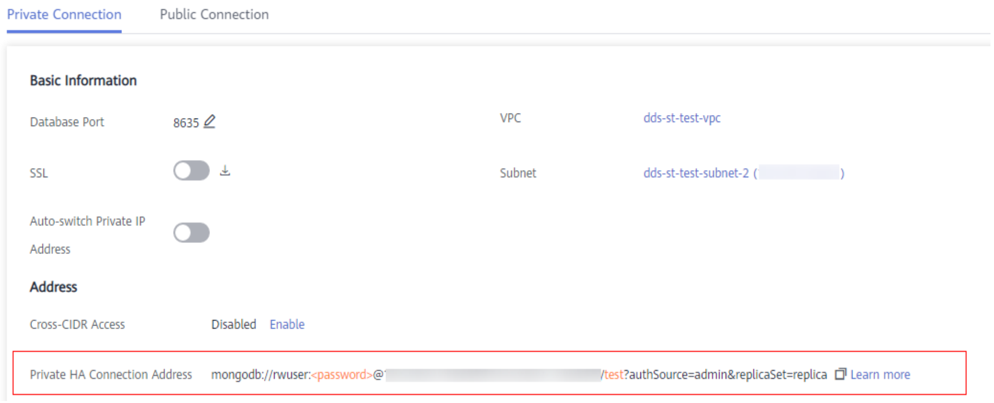
Example command:

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

Parameter description:

- **Private HA Connection Address**: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 3-13 Obtaining the private HA connection address



Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet-2 ([redacted])

Auto-switch Private IP Address

Address

Cross-CIDR Access Disabled Enable

Private HA Connection Address mongodb://rwuser:<password>@[redacted]/test?authSource=admin&replicaSet=replica Learn more

The format of the private HA connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

Pay attention to the following parameters in the private HA address:

Table 3-10 Parameter description

Parameter	Description
rwuser	Account name, that is, the database username.
<password>	Password for the database account. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.

Parameter	Description
192.168.xx.xx:8635,192.168.xx.xx:8635	IP addresses and ports of the nodes of the replica set instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin&replicaSet=replica	– The authentication database of user **rwuser** must be **admin**. **authSource=admin** is fixed in the command. – **replica** in **replicaSet=replica** is the name of a replica set. The default replica set of Huawei Cloud DDS is **replica**.

- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: The replica set certificate is generated using the internal management IP address to ensure that internal communication does not occupy resources such as the user IP address and bandwidth. **--sslAllowInvalidHostnames** is needed for the SSL connection through a private network.

Command example:

./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**

NOTE

- If you connect to an instance over a private HA address, add double quotation marks before and after the connection information.
- For details about the HA connection, see **Connecting to a Replica Set Instance for Read and Write Separation and High Availability**.

If the following information is displayed, the instance is successfully connected:

```
replica:PRIMARY>
```

Run the following command to access the local database:

use local

Information similar to the following is displayed:

```
switched to db local
```

Run the following command to query replica set oplog:

db.oplog.rs.find()

Method 2: Using the private HA connection address (user-defined database and account)

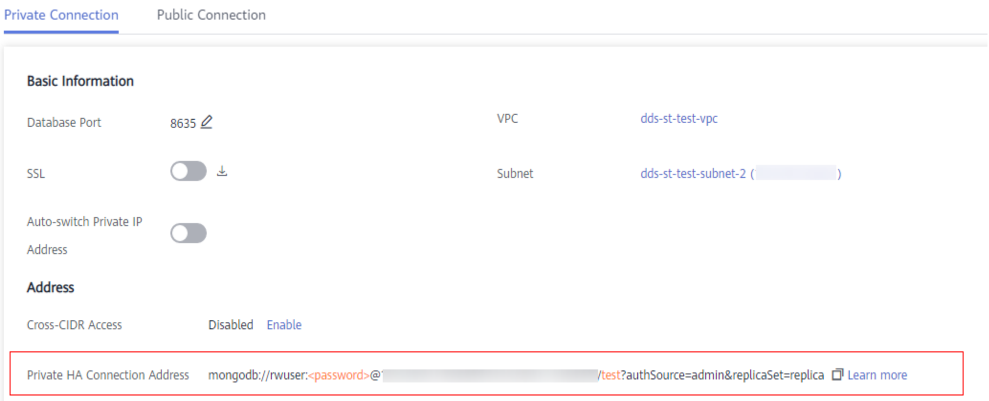
Example command:

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

Parameter description:

- **Private HA Connection Address**: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 3-14 Obtaining the private HA connection address



Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet-2 ([redacted])

Auto-switch Private IP Address

Address

Cross-CIDR Access Disabled Enable

Private HA Connection Address mongodb://rwuser:<password>@[redacted]/test?authSource=admin&replicaSet=replica

The format of the obtained private HA connection address is as follows:

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

The following table lists the required parameters in the private HA address.

Table 3-11 Parameter information

Parameter	Description
rwuser	Database username. The default value is **rwuser**. You can change the value to the username based on your service requirements.
<password>	Password for the database username. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.
192.168.xx.xx:8635,192.168.xx.xx:8635	IP addresses and ports of the nodes of the replica set instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.

Parameter	Description
authSource=admin&replicaSet=replica	– The authentication database of user **rwuser** is **admin**. – In **replica in replicaSet=replica**, **replica** indicates that the instance type is replica set and the format cannot be changed. **NOTE** If you use a user-defined database for authentication, change the authentication database in the HA connection address to the name of the user-defined database. In addition, replace **rwuser** with the username created in the user-defined database.

- **FILE_PATH** is the path for storing the root certificate.
- **--sslAllowInvalidHostnames**: The replica set certificate is generated using the internal management IP address to ensure that internal communication does not occupy resources such as the user IP address and bandwidth. **--sslAllowInvalidHostnames** is needed for the SSL connection through a private network.

For example, if you create a user-defined database **Database** and user **test1** in the database, the connection command is as follows:

./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**

Method 3: Connect to a single node.

You can also use the private IP address of a primary or secondary node to access the replica set instance. This method affects the read/write performance when **a primary/standby switchover** occurs.

Example command:

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

Parameter description:

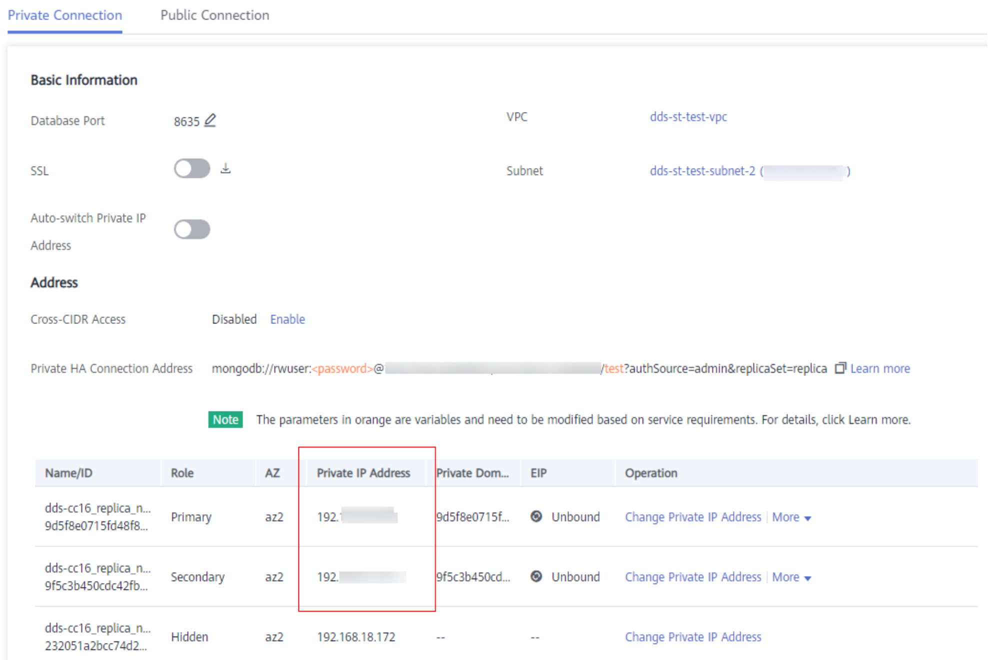
- **DB_HOST** is the private IP address of the primary or standby node of the instance to be connected.

  Primary node: You can read and write data on it.

  Secondary node: You can only read data from it.

  On the **Instances** page, click the instance to go to the **Basic Information** page. Choose **Connections**. On the **Private Connection** tab, obtain the IP address of the corresponding node.

Figure 3-15 Obtaining the IP address of a node



Private Connection Public Connection

Basic Information

Database Port	8635	VPC	dds-st-test-vpc
SSL		Subnet	dds-st-test-subnet-2 ([redacted])
Auto-switch Private IP Address			

Address

Cross-CIDR Access Disabled Enable

Private HA Connection Address mongodb://rwuser:<password>@[redacted]/test?authSource=admin&replicaSet=replica Learn more

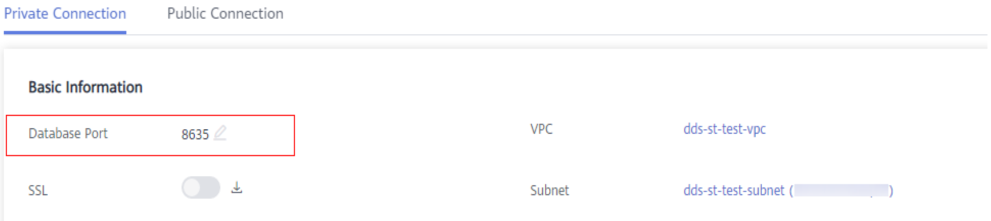
Note The parameters in orange are variables and need to be modified based on service requirements. For details, click Learn more.

Name/ID	Role	AZ	Private IP Address	Private Dom...	EIP	Operation
dds-cc16_replica_n... 9d5f8e0715fd48f8...	Primary	az2	192.[redacted]	9d5f8e0715f...	Unbound	Change Private IP Address | More
dds-cc16_replica_n... 9f5c3b450cdc42fb...	Secondary	az2	192.[redacted]	9f5c3b450cd...	Unbound	Change Private IP Address | More
dds-cc16_replica_n... 232051a2bcc74d2...	Hidden	az2	192.168.18.172	--	--	Change Private IP Address

- **DB_PORT** is the database port. The default value is 8635.

  You can click the instance to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Private Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

  Figure 3-16 Obtaining the port

  Private Connection Public Connection

  Basic Information

Database Port	8635	VPC	dds-st-test-vpc
SSL		Subnet	dds-st-test-subnet ([redacted])

- **DB_USER** is the database user. The default value is **rwuser**.
- **FILE_PATH** is the path for storing the root certificate.
- **--sslAllowInvalidHostnames**: The replica set certificate is generated using the internal management IP address to ensure that internal communication does not occupy resources such as the user IP address and bandwidth. **--sslAllowInvalidHostnames** is needed for the SSL connection through a private network.

Enter the database account password when prompted:

```
Enter password:
```

Command example:

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

If the following information is displayed, the corresponding node is successfully connected:

- The primary node of the replica set is connected.
  ```
  replica:PRIMARY>
  ```
- The standby node of the replica set is connected.
  ```
  replica:SECONDARY>
  ```

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

Step 1 Log in to the ECS.

Step 2 Connect to a DDS instance.

Method 1: High-availability connection (recommended)

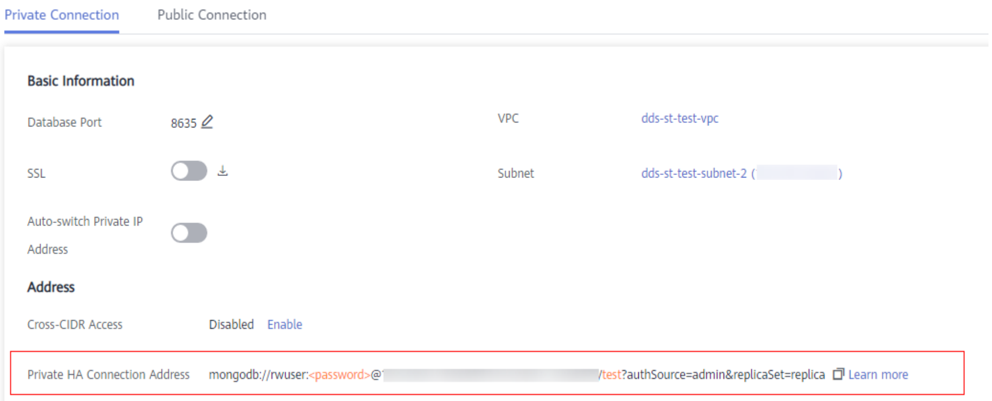
DDS provides the HA connection address. Using this address to connect to a replica set instance improves read/write performance and prevents errors reported when data is written from the client after a primary/standby switchover.

Example command:

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

Private HA Connection Address: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 3-17 Obtaining the private HA connection address



Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet-2 ([redacted])

Auto-switch Private IP Address

Address

Cross-CIDR Access Disabled Enable

Private HA Connection Address mongodb://rwuser:<password>@[redacted]/test?authSource=admin&replicaSet=replica Learn more

The format of the private HA connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

Pay attention to the following parameters in the private HA address:

Table 3-12 Parameter description

Parameter	Description
rwuser	Account name, that is, the database username.
<password>	Password for the database account. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.
192.168.xx.xx:8635,192.168.xx.xx:8635	IP addresses and ports of the nodes of the replica set instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin&replicaSet=replica	● The authentication database of user **rwuser** must be **admin**. **authSource=admin** is fixed in the command. ● **replica** in **replicaSet=replica** is the name of a replica set. The default replica set of Huawei Cloud DDS is **replica**.

Command example:

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

If the following information is displayed, the instance is successfully connected:

```
replica:PRIMARY>
```

Run the following command to access the local database:

use local

Information similar to the following is displayed:

```
switched to db local
```

Run the following command to query replica set oplog:

db.oplog.rs.find()

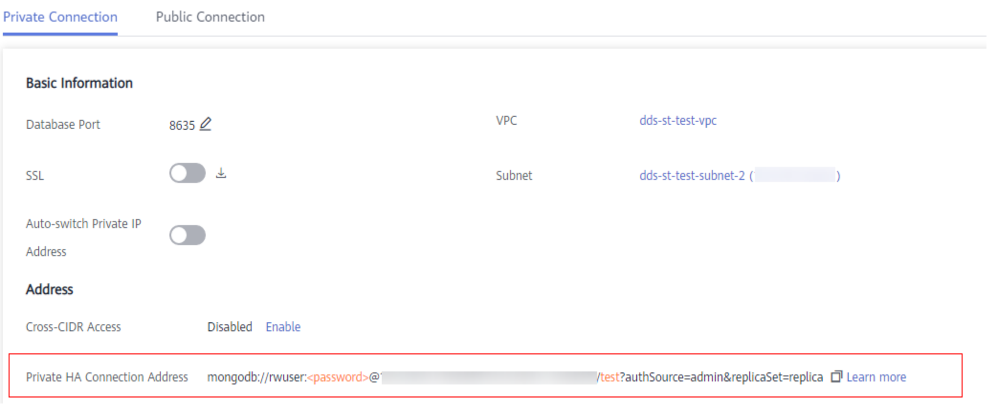
Method 2: Private HA connection (user-defined database and account)

Example command:

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

Private HA Connection Address: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 3-18 Obtaining the private HA connection address



Basic Information

Database Port	8635	VPC	dds-st-test-vpc
SSL		Subnet	dds-st-test-subnet-2 ([redacted])
Auto-switch Private IP Address			

Address

Cross-CIDR Access: Disabled

Private HA Connection Address: mongodb://rwuser:<password>@[redacted]/test?authSource=admin&replicaSet=replica

The format of the obtained private HA connection address is as follows:

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

The following table lists the required parameters in the private HA address.

Table 3-13 Parameter information

Parameter	Description
rwuser	Database username. The default value is **rwuser**. You can change the value to the username based on your service requirements.
<password>	Password for the database username. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.
192.168.xx.xx:8635,192.168.xx.xx:8635	IP addresses and ports of the nodes of the replica set instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.

Parameter	Description
authSource=admin&replicaSet=replica	- The authentication database of user **rwuser** is **admin**. - In **replica in replicaSet=replica**, **replica** indicates that the instance type is replica set and the format cannot be changed. **NOTE** If you use a user-defined database for authentication, change the authentication database in the HA connection address to the name of the user-defined database. In addition, replace **rwuser** with the username created in the user-defined database.

For example, if you create a user-defined database **Database** and user **test1** in the database, the connection command is as follows:

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

Method 3: Connect to a single node.

You can also use the private IP address of a primary or secondary node to access the replica set instance. This method affects the read/write performance when a primary/standby switchover occurs.

Example command:

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

Parameter description:

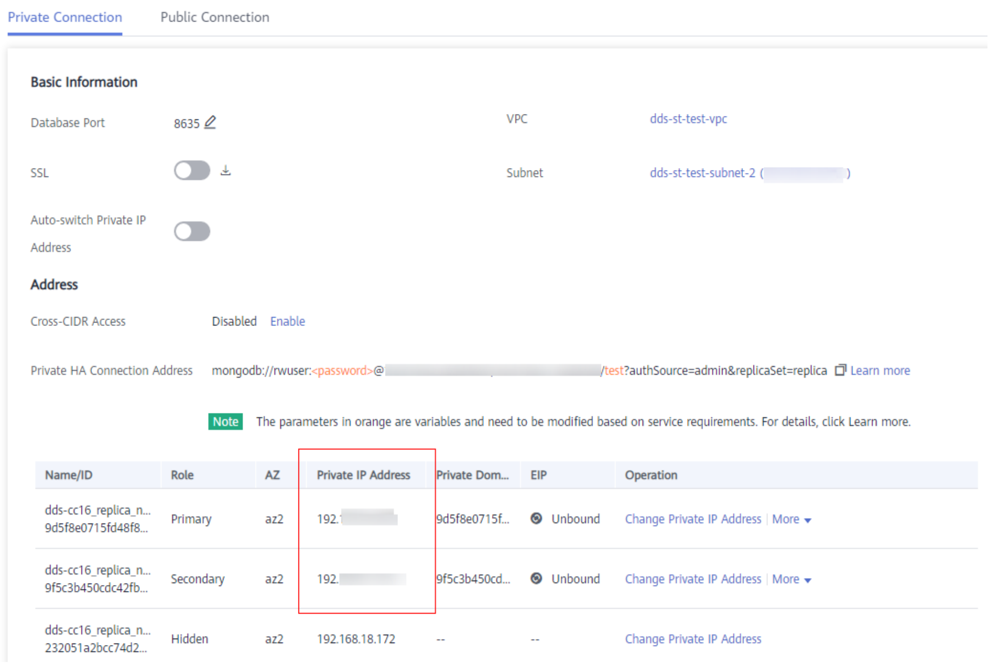
- **DB_HOST** is the private IP address of the primary or standby node of the instance to be connected.

  Primary node: You can read and write data on it.

  Secondary node: You can only read data from it.

  On the **Instances** page, click the instance to go to the **Basic Information** page. Choose **Connections**. On the **Private Connection** tab, obtain the IP address of the corresponding node.

Figure 3-19 Obtaining the IP address of a node



Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet-2 ([redacted])

Auto-switch Private IP Address

Address

Cross-CIDR Access Disabled Enable

Private HA Connection Address mongodb://rwuser:<password>@[redacted]/test?authSource=admin&replicaSet=replica Learn more

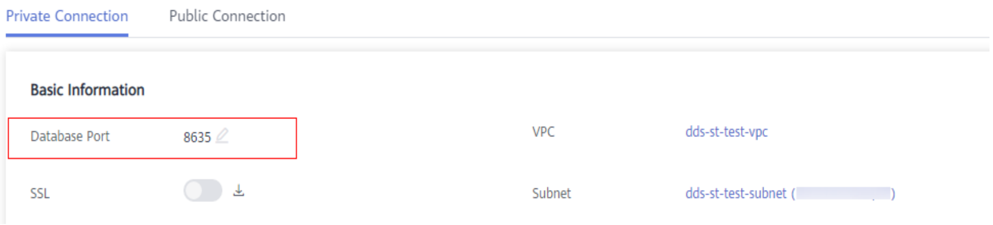
Note The parameters in orange are variables and need to be modified based on service requirements. For details, click Learn more.

Name/ID	Role	AZ	Private IP Address	Private Dom...	EIP	Operation
dds-cc16_replica_n... 9d5f8e0715fd48f8...	Primary	az2	192.[redacted]	9d5f8e0715f...	Unbound	Change Private IP Address | More
dds-cc16_replica_n... 9f5c3b450cdc42fb...	Secondary	az2	192.[redacted]	9f5c3b450cd...	Unbound	Change Private IP Address | More
dds-cc16_replica_n... 232051a2bcc74d2...	Hidden	az2	192.168.18.172	--	--	Change Private IP Address

- **DB_PORT** is the database port. The default value is 8635.

  You can click the instance to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Private Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

Figure 3-20 Obtaining the port



Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet ([redacted])

- **DB_USER** is the database user. The default value is **rwuser**.

Command example:

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

Enter the database account password when prompted:

```
Enter password:
```

If the following information is displayed, the corresponding node is successfully connected:

- The primary node of the replica set is connected.
  ```
  replica:PRIMARY>
  ```
- The standby node of the replica set is connected.

```
replica:SECONDARY>
```

----End

3.2.3.3 Connecting to Read Replicas Using Mongo Shell

Mongo shell is the default client for the MongoDB database server. You can use Mongo Shell to connect to DB instances, and query, update, and manage data in databases. DDS is compatible with MongoDB. Mongo Shell is a part of the MongoDB client. To use Mongo Shell, download and install the MongoDB client first, and then use the Mongo shell to connect to the DB instance.

By default, a DDS instance provides a private IP address. If your applications are deployed on an ECS and are in the same region and VPC as DDS instances, you can connect to DDS instances using a private IP address to achieve a fast transmission rate and high security.

This section describes how to use Mongo Shell to connect to a read replica over a private network.

You can connect to a read replica using an SSL connection or an unencrypted connection. The SSL connection is encrypted and more secure. To improve data transmission security, connect to instances using SSL.

Prerequisites

1. For details about how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.
2. Install the MongoDB client on the ECS. To ensure successful authentication, install the MongoDB client of the same version as the target instance.

   For details about how to install a MongoDB client, see **How Can I Install a MongoDB Client?**
3. The ECS can communicate with the DDS instance. For details, see **Configuring Security Group Rules**.

SSL Connection

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

Step 1 On the **Instances** page, click the instance name.

Step 2 In the navigation pane on the left, choose **Connections**.

Step 3 In the **Basic Information** area, click ⤓ next to the **SSL** field.

Step 4 Upload the root certificate to the ECS to be connected to the instance.

The following describes how to upload the certificate to a Linux and Window ECS:

- In Linux, run the following command:

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

  NOTE

  – **IDENTITY_FILE** is the directory where the root certificate resides. The file access permission is 600.

  – **REMOTE_USER** is the ECS OS user.

  – **REMOTE_ADDRESS** is the ECS address.

  – **REMOTE_DIR** is the directory of the ECS to which the root certificate is uploaded.

- In Windows, upload the root certificate using a remote connection tool.

Step 5 Connect to a DDS instance. The DDS console provides the read replica connection address. You can use this address to connect to the read replica.

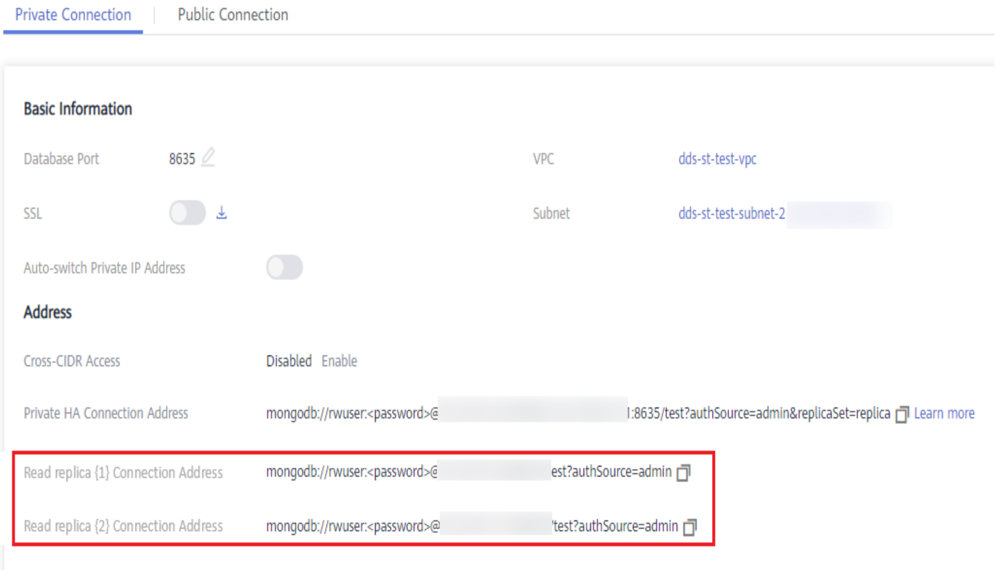
Example command:

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

Parameter description:

- **Read Replica Connection Address**: On the **Instances** page, click the instance to go to the **Basic Information** page. Choose **Connections**. Click the **Private Connection** tab. In the **Address** area, obtain the connection address of the read replica instance.

Figure 3-21 Obtaining the read replica connection address



Private Connection | Public Connection

Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet-2[redacted]

Auto-switch Private IP Address

Address

Cross-CIDR Access Disabled Enable

Private HA Connection Address mongodb://rwuser:<password>@[redacted]:8635/test?authSource=admin&replicaSet=replica Learn more

Read replica {1} Connection Address mongodb://rwuser:<password>@[redacted]est?authSource=admin

Read replica {2} Connection Address mongodb://rwuser:<password>@[redacted]'test?authSource=admin

The format of the read replica connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

Pay attention to the following parameters in the read replica connection address:

Table 3-14 Parameter description

Parameter	Description
rwuser	Account name, that is, the database username.
<password>	Password for the database account. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ****@%***!$, the corresponding URL code is ****%40%25***%21%24.
192.168.xx.xx:8635	IP address and port of the read replica of the replica set instance.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user **rwuser** must be **admin**. **authSource=admin** is fixed in the command.

- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: The replica set certificate is generated using the internal management IP address to ensure that internal communication does not occupy resources such as the user IP address and bandwidth. **--sslAllowInvalidHostnames** is needed for the SSL connection through a private network.

Command example:

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

NOTE

When connecting to an instance using the read replica connection address, add double quotation marks (") before and after the connection information.

If the following information is displayed, the instance is successfully connected:

```
replica:SECONDARY>
```

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

Step 1 Log in to the ECS.

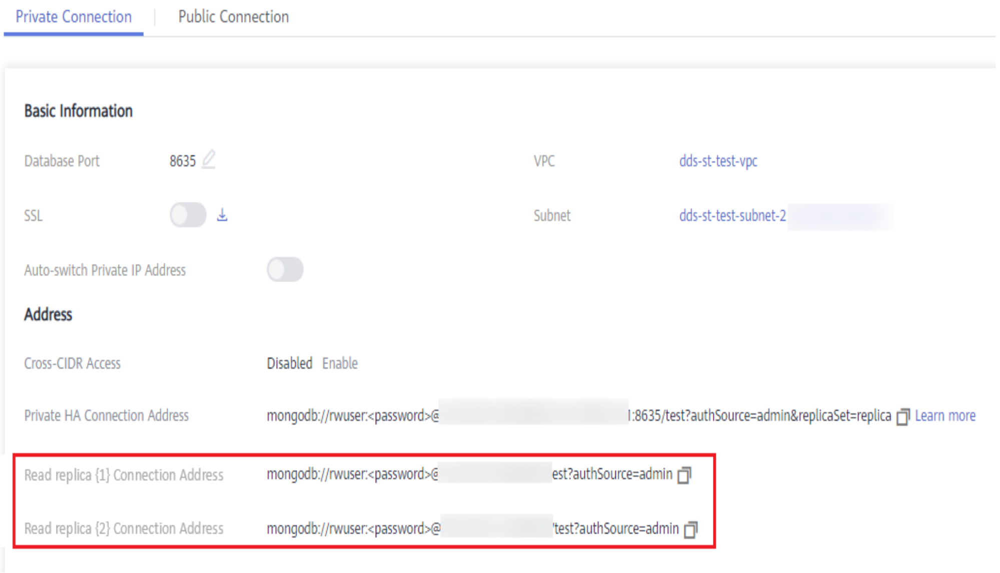
Step 2 Connect to a DDS instance. The DDS console provides the read replica connection address. You can use this address to connect to the read replica.

Example command:

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

Read Replica Connection Address: On the **Instances** page, click the instance to go to the **Basic Information** page. Choose **Connections**. Click the **Private Connection** tab. In the **Address** area, obtain the connection address of the read replica instance.

Figure 3-22 Obtaining the read replica connection address



Private Connection | Public Connection

Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet-2 [redacted]

Auto-switch Private IP Address

Address

Cross-CIDR Access Disabled Enable

Private HA Connection Address mongodb://rwuser:<password>@[redacted]:8635/test?authSource=admin&replicaSet=replica Learn more

Read replica {1} Connection Address mongodb://rwuser:<password>@[redacted]est?authSource=admin

Read replica {2} Connection Address mongodb://rwuser:<password>@[redacted]'test?authSource=admin

The format of the read replica connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

Pay attention to the following parameters in the private HA address:

Table 3-15 Parameter description

Parameter	Description
rwuser	Account name, that is, the database username.
<password>	Password for the database account. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25*** %21%24**.
192.168.xx.xx:8635	IP address and port of the read replica of the replica set instance.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user **rwuser** must be **admin**. **authSource=admin** is fixed in the command.

Command example:

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

If the following information is displayed, the instance is successfully connected:

```
replica:SECONDARY>
```

----End

3.2.4 Connecting to a Replica Set Instance over a Public Network

3.2.4.1 Binding and Unbinding an EIP

After you create an instance, you can bind an EIP to it to allow external access. If later you want to prohibit external access, you can also unbind the EIP from the DB instance.

Precautions

- Deleting a bound EIP does not mean that the EIP is unbound.
- Before accessing a database, apply for an EIP on the VPC console. Then, add an inbound rule to allow the IP addresses or IP address ranges of ECSs. For details, see **Configuring Security Group Rules**.

- In the replica set instance, only primary and secondary nodes can have an EIP bound. To change the EIP that has been bound to a node, you need to unbind it from the node first.

Binding an EIP

Step 1 Log in to the management console.

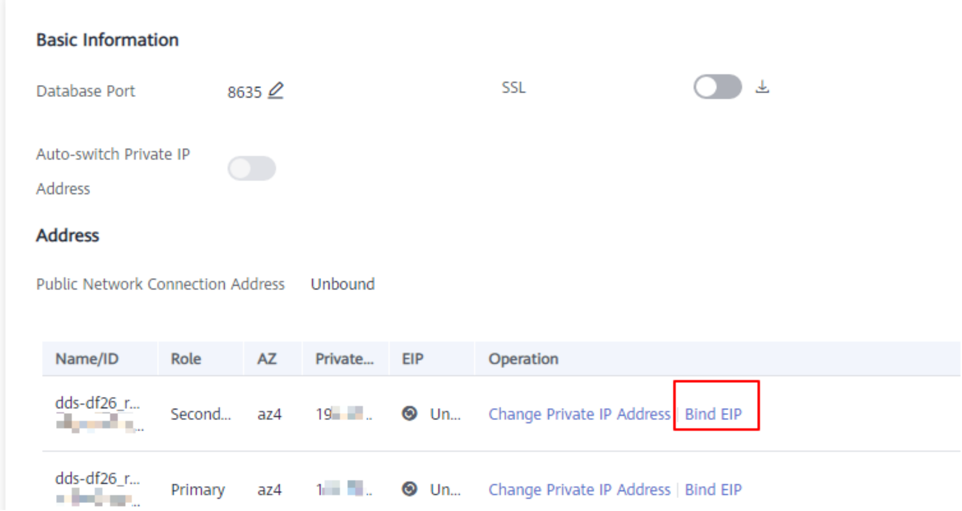
Step 2 Click 📍 in the upper left corner and select a region and a project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the replica set instance name.

Step 5 In the navigation pane on the left, choose **Connections**. Click the **Public Connection** tab. In the **Basic Information** area, locate the node you want to bind an EIP to and click **Bind EIP** in the **Operation** column.

Figure 3-23 Binding an EIP



Basic Information

Database Port 8635

SSL

Auto-switch Private IP Address

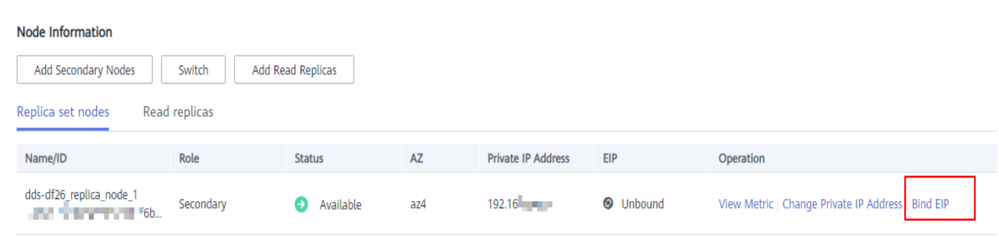
Address

Public Network Connection Address Unbound

Name/ID	Role	AZ	Private...	EIP	Operation
dds-df26_r... [redacted]	Second...	az4	19[redacted]..	Un...	Change Private IP Address | Bind EIP
dds-df26_r... [redacted]	Primary	az4	1[redacted]..	Un...	Change Private IP Address | Bind EIP

You can also locate the node in the **Node Information area** on the **Basic Information** page and click **Bind EIP** in the **Operation** column.

Figure 3-24 Binding an EIP

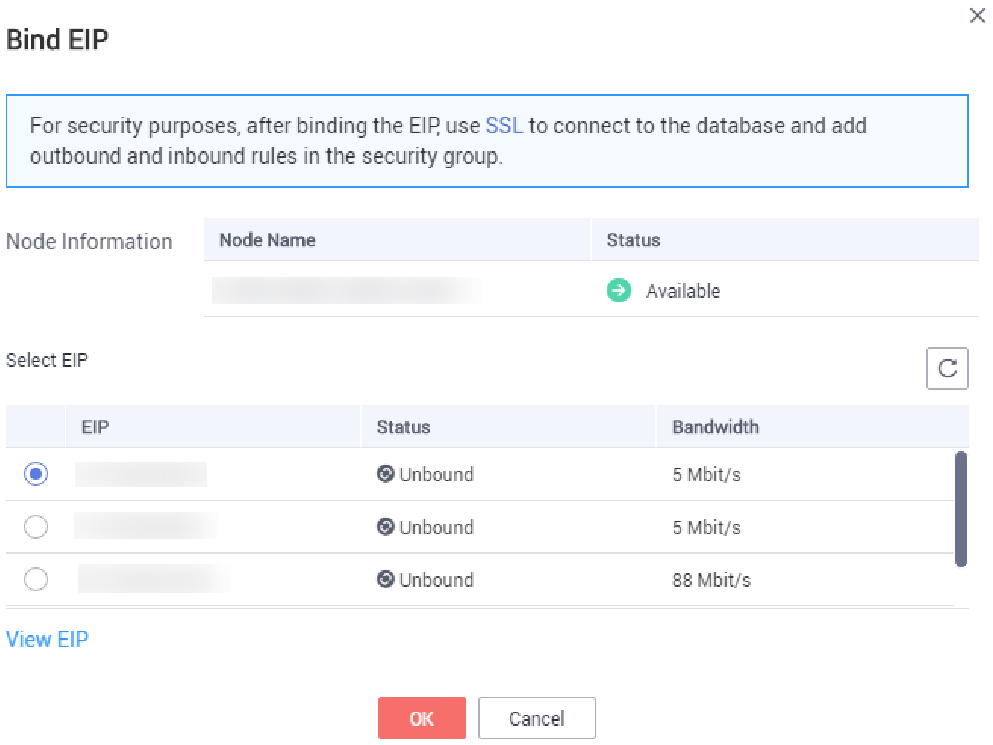


Node Information

Name/ID	Role	Status	AZ	Private IP Address	EIP	Operation
dds-df26_replica_node_1 [redacted]6b...	Secondary	Available	az4	192.16[redacted]	Unbound	View Metric | Change Private IP Address | Bind EIP

Step 6 In the displayed dialog box, all available unbound EIPs are listed. Select the required EIP and click **OK**. If no available EIPs are displayed, click **View EIP** and create an EIP on the VPC console.

Figure 3-25 Selecting an EIP



Bind EIP

For security purposes, after binding the EIP, use SSL to connect to the database and add outbound and inbound rules in the security group.

Node Information

Node Name	Status
[redacted]	Available

Select EIP

	EIP	Status	Bandwidth
●	[redacted]	Unbound	5 Mbit/s
○	[redacted]	Unbound	5 Mbit/s
○	[redacted]	Unbound	88 Mbit/s

Step 7 Locate the target node. In the **EIP** column, you can view the EIP that was bound.

To unbind an EIP from the instance, see **Unbinding an EIP**.

----End

Unbinding an EIP

Step 1 **Log in to the management console**.

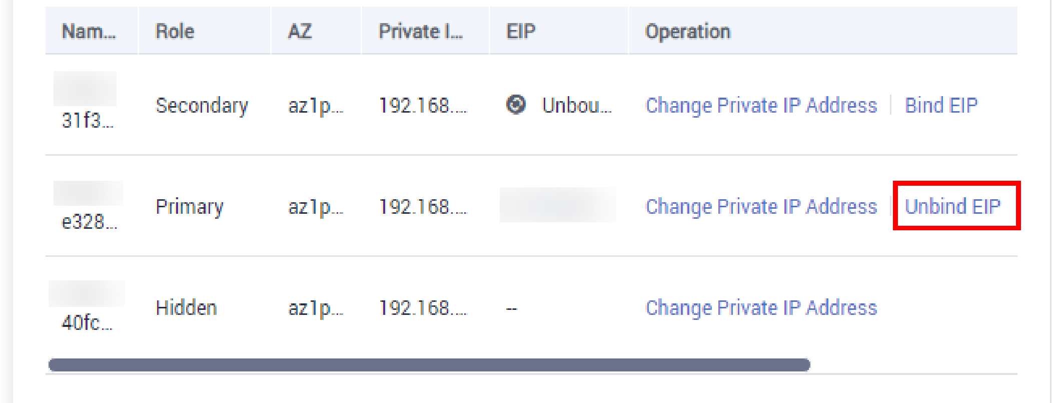
Step 2 Click 📍 in the upper left corner and select a region and a project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the replica set instance that has been bound with an EIP.

Step 5 In the navigation pane on the left, choose **Connections**. Click the **Public Connection** tab. In the **Basic Information** area, locate the node and click **Unbind EIP** in the **Operation** column.

Figure 3-26 Unbinding an EIP



Nam...	Role	AZ	Private I...	EIP	Operation
[redacted] 31f3...	Secondary	az1p...	192.168....	⊘ Unbou...	Change Private IP Address | Bind EIP
[redacted] e328...	Primary	az1p...	192.168....	[redacted]	Change Private IP Address | Unbind EIP
[redacted] 40fc...	Hidden	az1p...	192.168....	--	Change Private IP Address

You can also locate the node in the **Node Information area** on the **Basic Information** page and click **Unbind EIP** in the **Operation** column.

Step 6 In the displayed dialog box, click **Yes**.

To bind an EIP to the instance again, see **Binding an EIP**.

----End

3.2.4.2 Configuring Security Group Rules

A security group is a collection of access control rules for ECSs and DDS instances that have the same security protection requirements and are mutually trusted in a VPC.

To ensure database security and reliability, you need to configure security group rules to allow specific IP addresses and ports to access the instance.

If you attempt to connect to an instance through an EIP, you need to configure an inbound rule for the security group associated with the instance.

Precautions

- By default, an account can create up to 500 security group rules.
- Too many security group rules will increase the first packet latency, so a maximum of 50 rules for each security group is recommended.
- By default, one DDS instance is associated with only one security group.
- DDS allows you to associate multiple security groups to a DB instance. You can apply for the service based on your service requirements. For better network performance, you are advised to select no more than five security groups.

Procedure

Step 1 **Log in to the management console**.

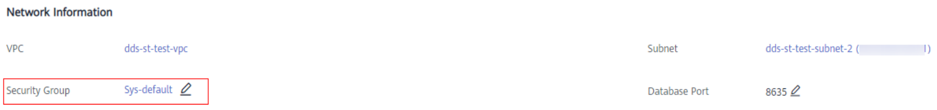
Step 2 Click 📍 in the upper left corner and select a region and a project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the instance name. The **Basic Information** page is displayed.

Step 5 In the **Network Information** area on the **Basic Information** page, click the security group.

Figure 3-27 Security Group

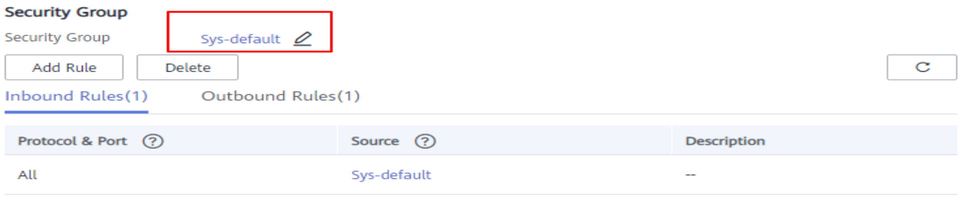


Network Information

VPC	dds-st-test-vpc	Subnet	dds-st-test-subnet-2 ([redacted])
Security Group	Sys-default	Database Port	8635

You can also choose **Connections** in the navigation pane on the left. On the **Public Connection** tab, in the **Security Group** area, click the security group name.

Figure 3-28 Security Group



Security Group

Security Group Sys-default

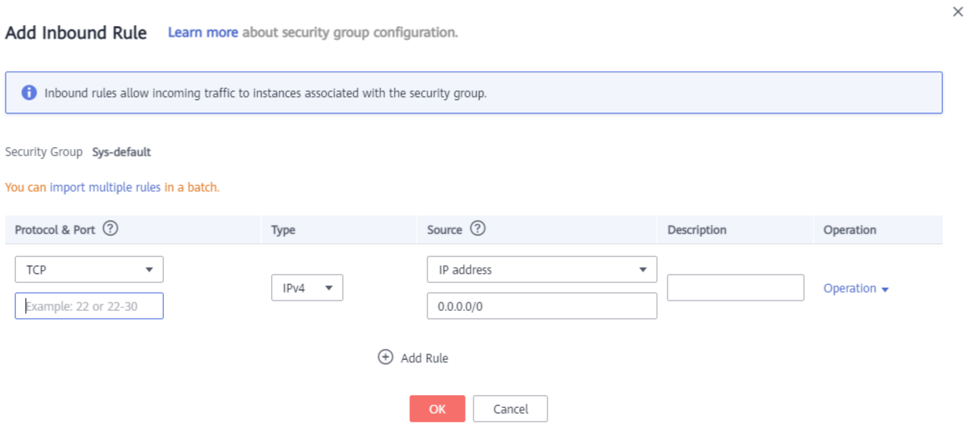
Protocol & Port	Source	Description
All	Sys-default	--

Step 6 On the **Security Group** page, locate the target security group and click **Manage Rule** in the **Operation** column.

Step 7 On the **Inbound Rules** tab, click **Add Rule**. The **Add Inbound Rule** dialog box is displayed.

Step 8 Add a security group rule as prompted.

Figure 3-29 Add Inbound Rule



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group Sys-default

You can import multiple rules in a batch.

Protocol & Port	Type	Source	Description	Operation
TCP Example: 22 or 22-30	IPv4	IP address 0.0.0.0/0		Operation

Table 3-16 Inbound rule settings

Parameter	Description	Example Value
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	The security group rule actions. A rule with a deny action overrides another with an allow action if the two rules have the same priority.	Allow
Protocol & Port	The network protocol required for access. The option can be **All**, **TCP**, **UDP**, **ICMP**, or **GRE**.	TCP
	Port: the port on which you wish to allow access to DDS. The default port is 8635. The port ranges from 2100 to 9500 or can be 27017, 27018, or 27019.	8635
Type	IP address type. Only **IPv4** and **IPv6** are supported.	IPv4
Source	Specifies the supported IP address, security group, and IP address group, which allow access from IP addresses or instances in other security group. Example: ● Single IP address: 192.168.10.10/32 ● IP address segment: 192.168.1.0/24 ● All IP addresses: 0.0.0.0/0 ● Security group: sg-abc ● IP address group: ipGroup-test If you enter a security group, all ECSs associated with the security group comply with the created rule. For more information about IP address groups, see **IP Address Group**.	0.0.0.0/0
Description	(Optional) Provides supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

Step 9 Click **OK**.

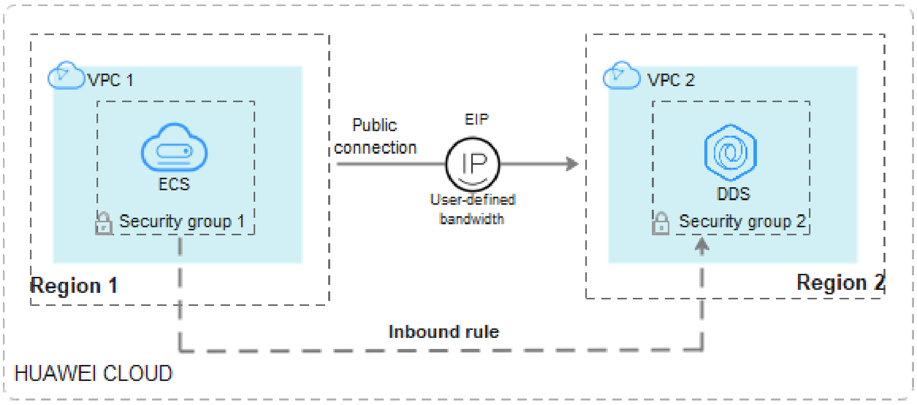
----End

3.2.4.3 Connecting to a Replica Set Instance Using Mongo Shell (Public Network)

In the following scenarios, you can access a DDS instance from the Internet by binding an EIP to the instance.

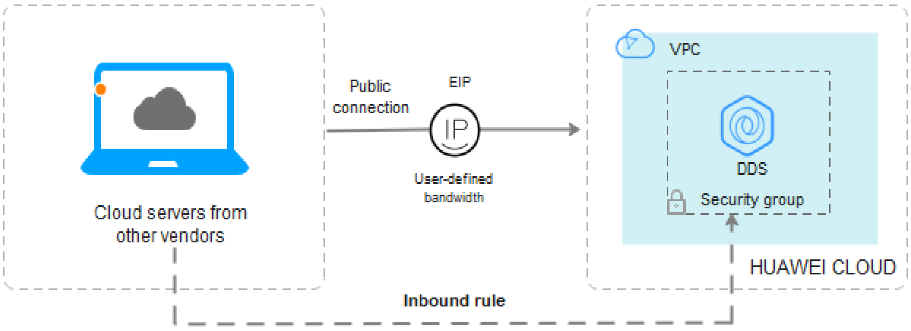
Scenario 1: Your applications are deployed on an ECS and are not in the same region as the DDS instance.

Figure 3-30 Accessing DDS from ECS across regions



Scenario 2: Your applications are deployed on a cloud server provided by other vendors.

Figure 3-31 Accessing DDS from other cloud servers



This section describes how to use Mongo Shell to connect to a replica set instance through an EIP.

You can connect to an instance using an SSL connection or an unencrypted connection. The SSL connection is encrypted and more secure. To improve data transmission security, connect to instances using SSL.

Prerequisites

1. For details about how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.
2. Bind an **EIP** to the replica set instance and configure security group rules to ensure that the replica set instance can be accessed from an ECS.
3. Install the MongoDB client on the ECS.

   For details about how to install a MongoDB client, see **How Can I Install a MongoDB Client?**

   NOTE

   The version of the installed MongoDB client must be the same as the instance version.

SSL Connection

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

Step 1 **Log in to the management console**.

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

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the instance name.

Step 5 In the navigation pane on the left, choose **Connections**.

Step 6 In the **Basic Information** area, click ⤓ next to the **SSL** field.

Step 7 Upload the root certificate to the ECS to be connected to the instance.

The following describes how to upload the certificate to a Linux and Window ECS:

- In Linux, run the following command:

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

  NOTE

  – **IDENTITY_FILE** is the directory where the root certificate resides. The file access permission is 600.

  – **REMOTE_USER** is the ECS OS user.

  – **REMOTE_ADDRESS** is the ECS address.

  – **REMOTE_DIR** is the directory of the ECS to which the root certificate is uploaded.

- In Windows, upload the root certificate using a remote connection tool.

Step 8 Connect to the instance in the directory where the MongoDB client is located.

Method 1: Using a public network connection address

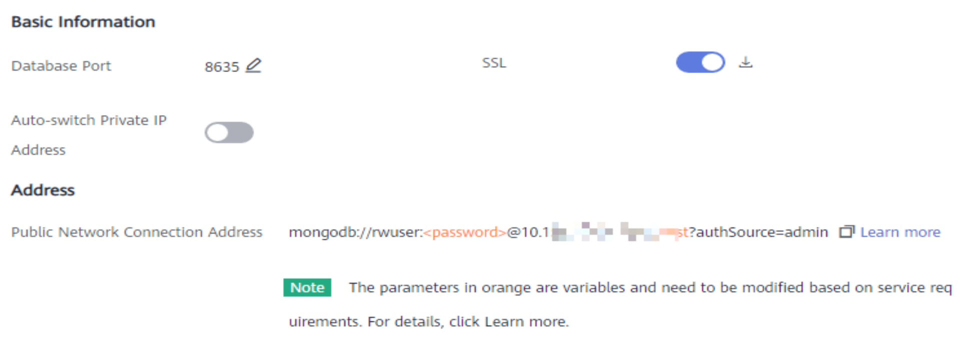
Example command:

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

Parameter description:

- **Public Network Connection Address**: On the **Instances** page, click the instance to switch to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. Click the **Public Connection** tab and obtain the public network connection address.

Figure 3-32 Obtaining the public network connection address



Basic Information

Database Port 8635

SSL

Auto-switch Private IP Address

Address

Public Network Connection Address mongodb://rwuser:<password>@10.1[redacted]st?authSource=admin Learn more

Note The parameters in orange are variables and need to be modified based on service requirements. For details, click Learn more.

The format of the public connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

Pay attention to the following parameters in the public network connection address:

Table 3-17 Parameter description

Parameter	Description
rwuser	Account name, that is, the database username.
<password>	Password for the database account. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.
192.168.xx.xx:8635	The EIP and port bound to the node of the replica set instance.

Parameter	Description
authSource=admin	The authentication database of user **rwuser** must be **admin**. **authSource=admin** is fixed in the command.

- **FILE_PATH** is the path for storing the root certificate.
- **--sslAllowInvalidHostnames**: The replica set certificate is generated using the internal management IP address to ensure that internal communication does not occupy resources such as the user IP address and bandwidth. **--sslAllowInvalidHostnames** is needed for the SSL connection through a public network.

Command example:

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

NOTE

- If you connect to an instance over a public HA address, add double quotation marks before and after the connection information.
- To improve read and write performance and prevent errors from being reported when data is written from the client after a primary/standby switchover. For details about how to connect to an instance in HA mode, see **Connecting to a Replica Set Instance for Read and Write Separation and High Availability**.

Method 2: Using an EIP

Example command:

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

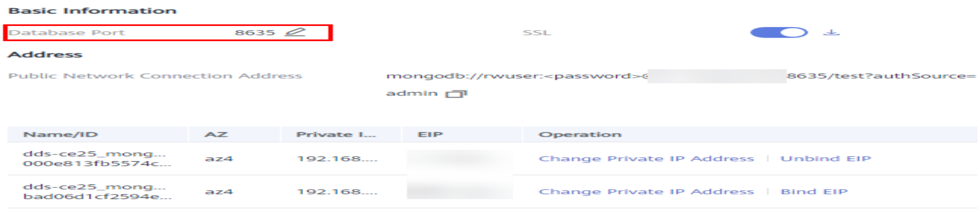
Parameter description:

- **DB_HOST** is the EIP bound to the instance node to be connected.

  On the **Instances** page, click the instance to go to the **Basic Information** page. Choose **Connections**> **Public Connection** and obtain the EIP of the corresponding node.
- **DB_PORT** is the database port. The default port number is 8635.

  You can click the instance to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Public Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

Figure 3-33 Obtaining the port



Basic Information

Database Port 8635

SSL

Address

Public Network Connection Address mongodb://rwuser:<password>@[redacted]8635/test?authSource=admin

Name/ID	AZ	Private I...	EIP	Operation
dds-ce25_mong... 000e813fb5574c...	az4	192.168....	[redacted]	Change Private IP Address | Unbind EIP
dds-ce25_mong... bad06d1cf2594e...	az4	192.168....	[redacted]	Change Private IP Address | Bind EIP

- **DB_USER** is the database user. The default value is **rwuser**.
- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: The replica set certificate is generated using the internal management IP address to ensure that internal communication does not occupy resources such as the user IP address and bandwidth. **--sslAllowInvalidHostnames** is needed for the SSL connection through a public network.

Enter the database account password when prompted:

```
Enter password:
```

Command example:

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

Step 9 Check the connection result. If the following information is displayed, the connection is successful.

- The primary node of the replica set is connected.
  ```
  replica:PRIMARY>
  ```
- The standby node of the replica set is connected.
  ```
  replica:SECONDARY>
  ```

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

Step 1 Log in to the ECS.

Step 2 Connect to a DDS instance.

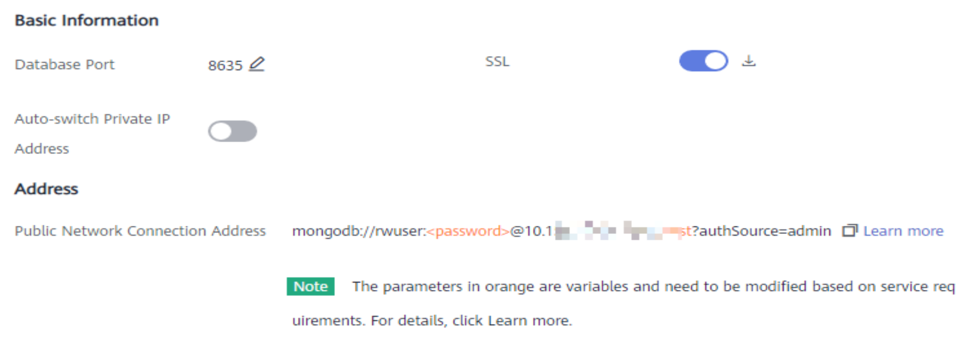
Method 1: Using a public network connection address

Example command:

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

Public Network Connection Address: On the **Instances** page, click the instance to switch to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. Click the **Public Connection** tab and obtain the public network connection address.

Figure 3-34 Obtaining the public network connection address



Basic Information

Database Port 8635

SSL

Auto-switch Private IP Address

Address

Public Network Connection Address mongodb://rwuser:<password>@10.1[redacted]st?authSource=admin Learn more

Note The parameters in orange are variables and need to be modified based on service req uirements. For details, click Learn more.

The format of the public connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

Pay attention to the following parameters in the public connection address:

Table 3-18 Parameter description

Parameter	Description
rwuser	Account name, that is, the database username.
<password>	Password for the database account. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.
192.168.xx.xx:8635	The EIP and port bound to the node of the replica set instance.
authSource=admin	The authentication database of user **rwuser** must be **admin**. **authSource=admin** is fixed in the command.

Command example:

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

NOTE

- If you connect to an instance over a public HA address, add double quotation marks before and after the connection information.
- To improve read and write performance and prevent errors from being reported when data is written from the client after a primary/standby switchover, you are advised to connect to an instance using the HA connection address. For details, see **Connecting to a Replica Set Instance for Read and Write Separation and High Availability**.

Method 2: Using an EIP

Example command:

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

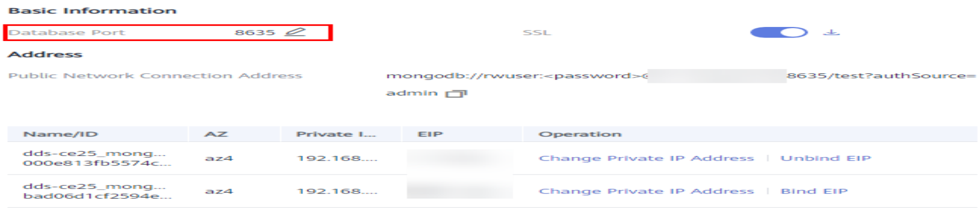
Parameter description:

- **DB_HOST** is the EIP bound to the instance node to be connected.

  On the **Instances** page, click the instance to go to the **Basic Information** page. Choose **Connections**> **Public Connection** and obtain the EIP of the corresponding node.
- **DB_PORT** is the database port. The default port number is 8635.

  You can click the instance to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Public Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

  Figure 3-35 Obtaining the port

  Basic Information

  Database Port 8635

  SSL

  Address

  Public Network Connection Address mongodb://rwuser:<password>@[redacted]8635/test?authSource=admin

Name/ID	AZ	Private I...	EIP	Operation
dds-ce25_mong... 000e813fb5574c...	az4	192.168....	[redacted]	Change Private IP Address | Unbind EIP
dds-ce25_mong... bad06d1cf2594e...	az4	192.168....	[redacted]	Change Private IP Address | Bind EIP

- **DB_USER** is the database user. The default value is **rwuser**.

Enter the database account password when prompted:

```
Enter password:
```

Command example:

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

Step 3 Check the connection result. If the following information is displayed, the connection is successful.

- The primary node of the replica set is connected.
  ```
  replica:PRIMARY>
  ```
- The standby node of the replica set is connected.
  ```
  replica:SECONDARY>
  ```

----End

3.2.4.4 Connecting to a Replica Set Instance Using Robo 3T

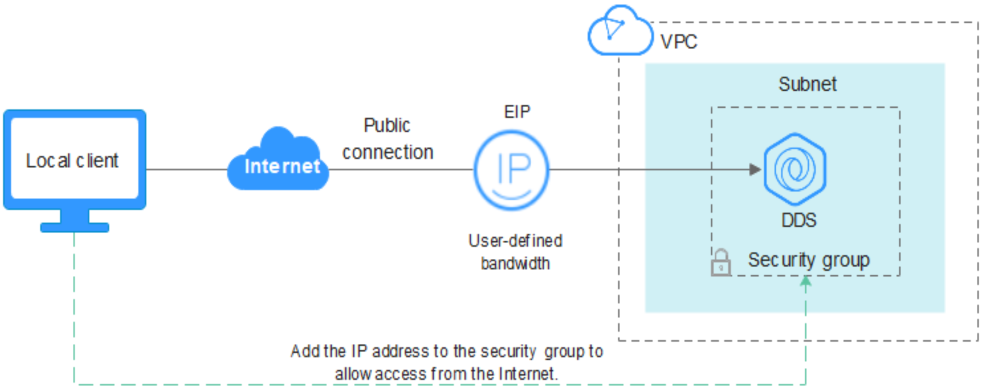
To connect to an instance from a local device, you can use Robo 3T to access the instance from the Internet.

This section describes how to use Robo 3T to connect to a cluster instance from a local device. In this section, the Windows operating system (OS) used by the client is used as an example.

Robo 3T can connect to an instance with an unencrypted connection or an encrypted connection (SSL). To improve data transmission security, connect to instances using SSL.

Connection Diagram

Figure 3-36 Connection diagram



Prerequisites

1. Bind an EIP to the ECS and configure security group rules.
   a. Bind an EIP to the replica set instance.

      For details about how to bind an EIP, see **Binding and Unbinding an EIP**.
   b. Obtain the IP address of a local device.
   c. Configure security group rules.

      Add the IP address obtained in **1.b** and the instance port to the inbound rule of the security group.

      For details about how to configure security group rules, see **Configuring Security Group Rules**.
   d. Run the ping command to ping the EIP bound in **1.a** to ensure that the EIP is accessible through your local device.
2. Install Robo 3T.
   a. For details, see **Installing Robo 3T**.

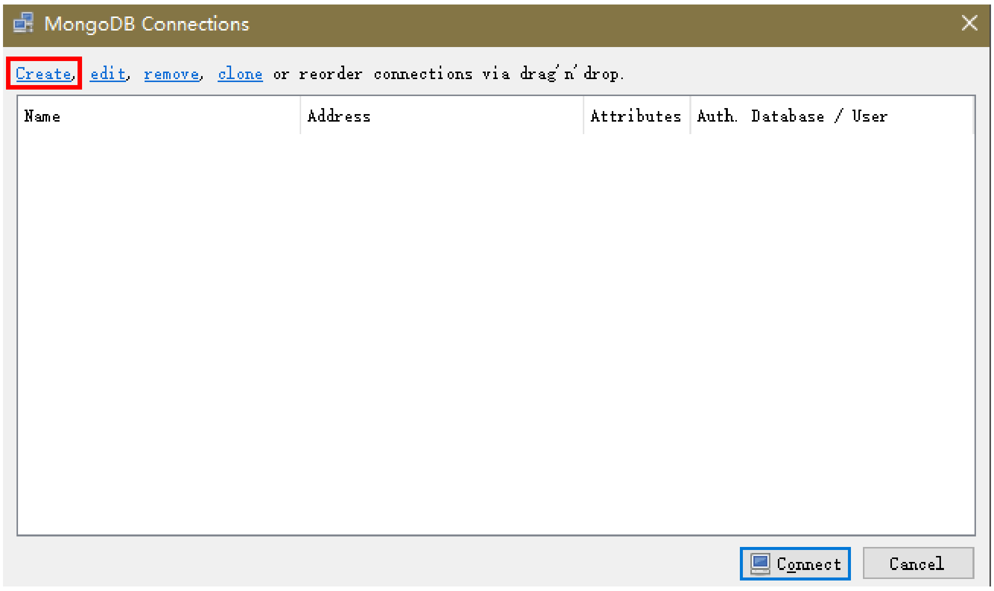
SSL

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

Step 1 Run the installed Robo 3T. On the displayed dialog box, click **Create**.

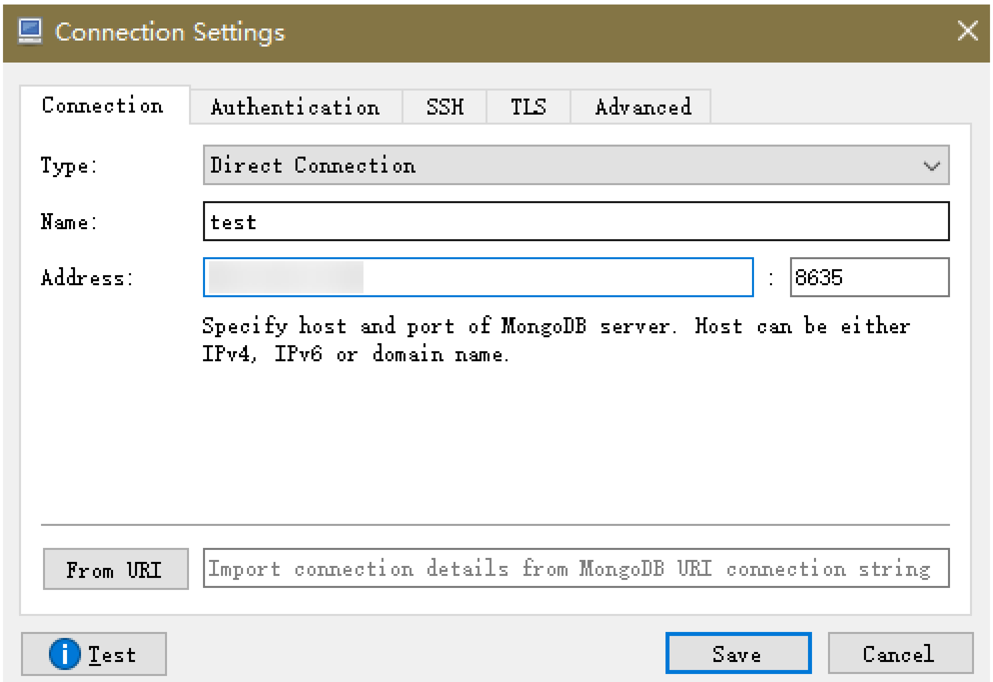
Figure 3-37 Connections



Step 2 In the **Connection Settings** dialog box, set the parameters of the new connection.

1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the DDS DB instance in the **Address** text box.

Figure 3-38 Connection



Connection Settings

Type: Direct Connection

Name: test

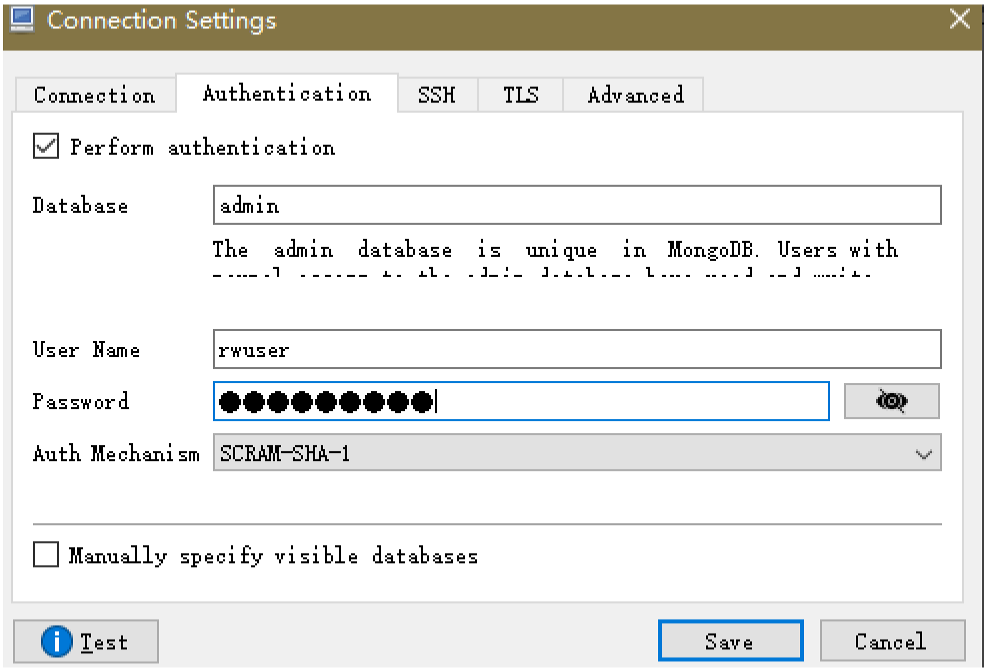
Address: [redacted] : 8635

Specify host and port of MongoDB server. Host can be either IPv4, IPv6 or domain name.

From URI: Import connection details from MongoDB URI connection string

2. On the **Authentication** tab, set **Database** to **admin**, **User Name** to **rwuser**, and **Password** to the administrator password you set during the creation of the cluster instance.

Figure 3-39 Authentication



Connection Settings

☑ Perform authentication

Database: admin

The admin database is unique in MongoDB. Users with

User Name: rwuser

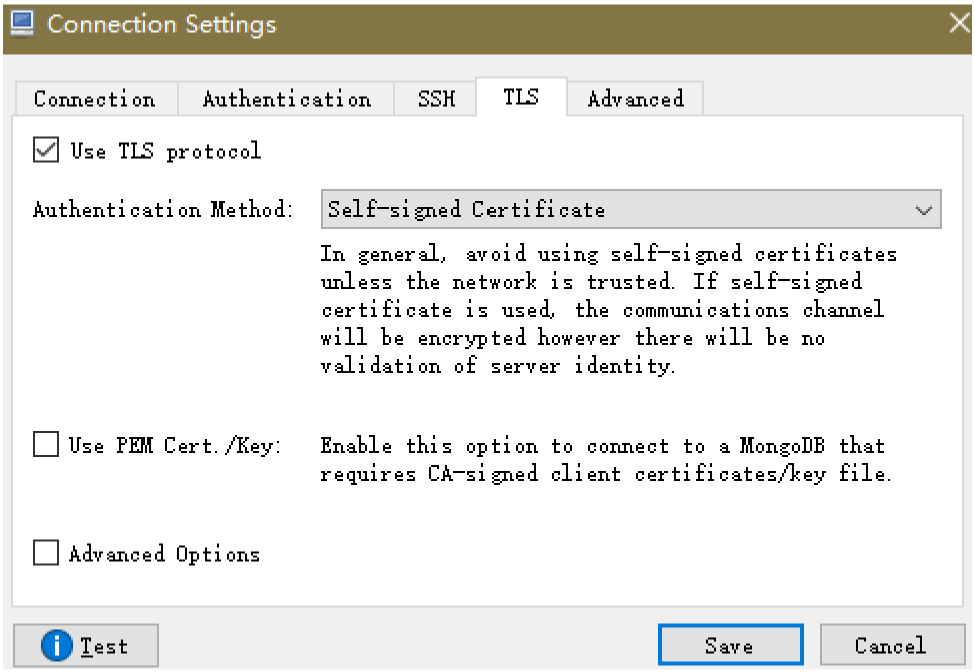
Password: ●●●●●●●●●●

Auth Mechanism: SCRAM-SHA-1

□ Manually specify visible databases

3. On the **TLS** tab, select **Use TLS protocol** and select **Self-signed Certificate** for **Authentication Method**.

Figure 3-40 SSL



☑ Use TLS protocol

Authentication Method: Self-signed Certificate

In general, avoid using self-signed certificates unless the network is trusted. If self-signed certificate is used, the communications channel will be encrypted however there will be no validation of server identity.

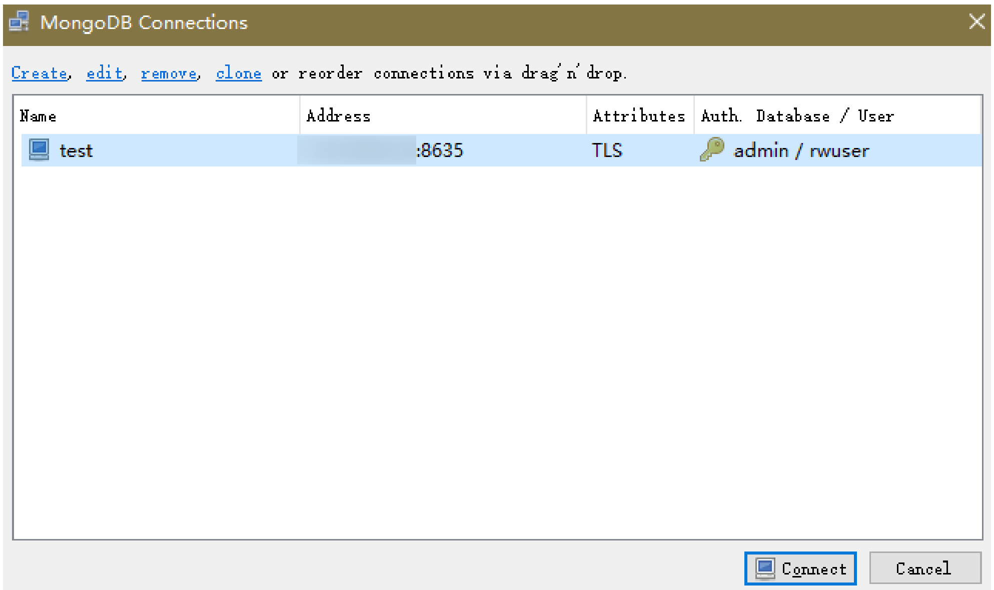
□ Use PEM Cert./Key: Enable this option to connect to a MongoDB that requires CA-signed client certificates/key file.

□ Advanced Options

4. Click **Save**.

Step 3 On the **MongoDB Connections** page, click **Connect** to connect to the replica set instance.

Figure 3-41 Cluster connection information

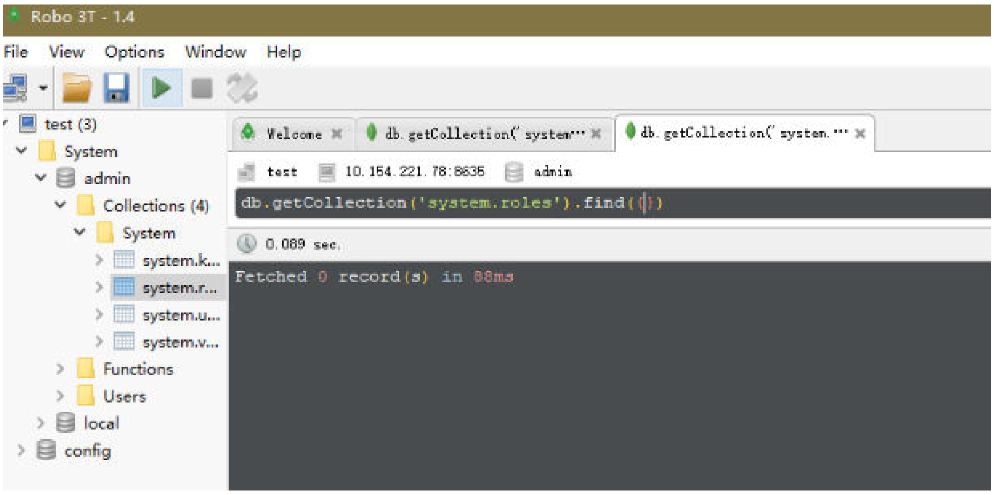


Create, edit, remove, clone or reorder connections via drag'n' drop.

Name	Address	Attributes	Auth. Database / User
test	[redacted]:8635	TLS	admin / rwuser

Step 4 If the replica set instance is successfully connected, the page shown in **Figure 3-42** is displayed.

Figure 3-42 Connection succeeded



```
db.getCollection('system.roles').find({})
```

```
0.089 sec.
Fetched 0 record(s) in 88ms
```

----End

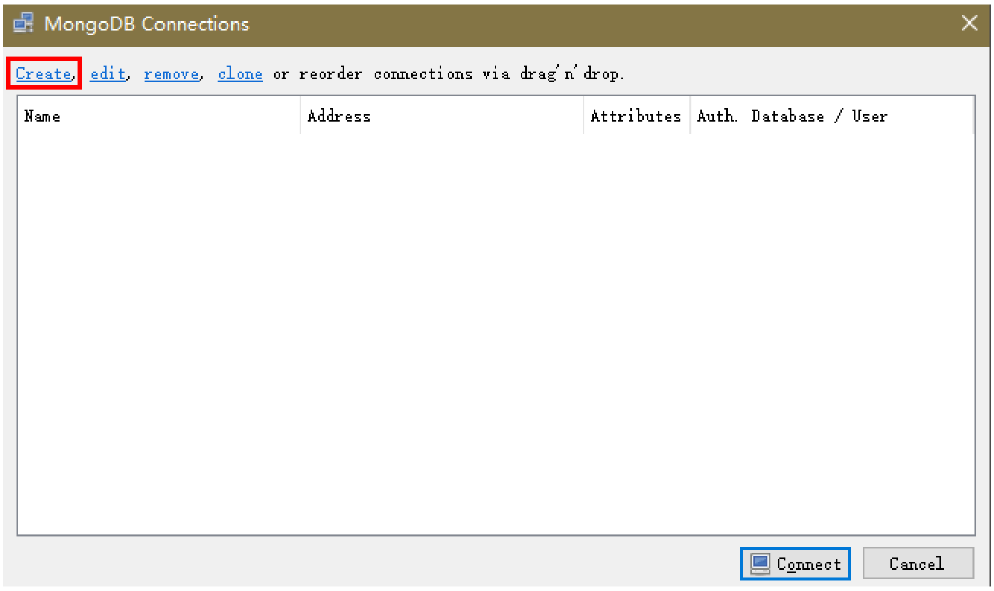
Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details, see **Enabling and Disabling SSL**.

Step 1 Run the installed Robo 3T. On the displayed dialog box, click **Create**.

Figure 3-43 Connections



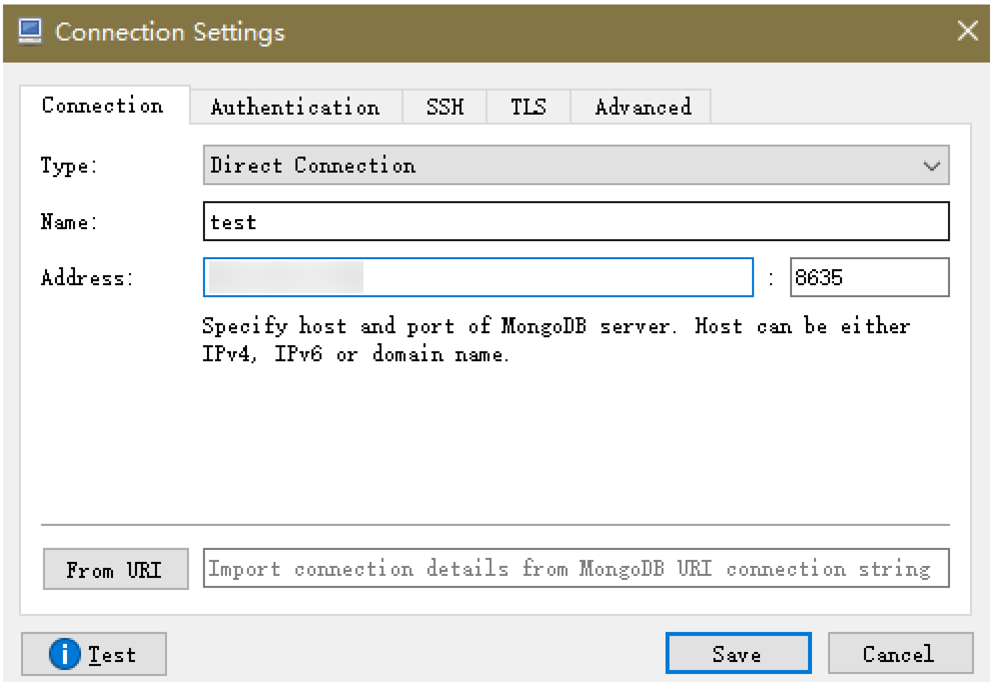
Create, edit, remove, clone or reorder connections via drag'n'drop.

Name	Address	Attributes	Auth. Database / User

Step 2 In the **Connection Settings** dialog box, set the parameters of the new connection.

1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the DDS DB instance in the **Address** text box.

Figure 3-44 Connection



Connection Settings

Type: Direct Connection

Name: test

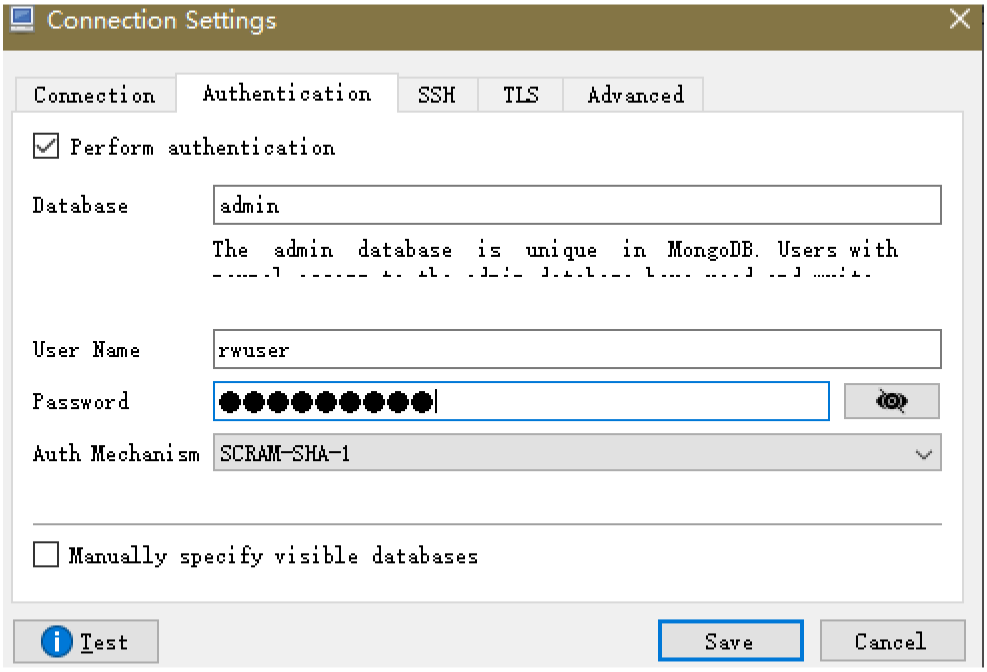
Address: [redacted] : 8635

Specify host and port of MongoDB server. Host can be either IPv4, IPv6 or domain name.

Import connection details from MongoDB URI connection string

2. On the **Authentication** tab, set **Database** to **admin**, **User Name** to **rwuser**, and **Password** to the administrator password you set during the creation of the cluster instance.

Figure 3-45 Authentication



Connection Settings

☑ Perform authentication

Database: admin

The admin database is unique in MongoDB. Users with

User Name: rwuser

Password: ●●●●●●●●●●

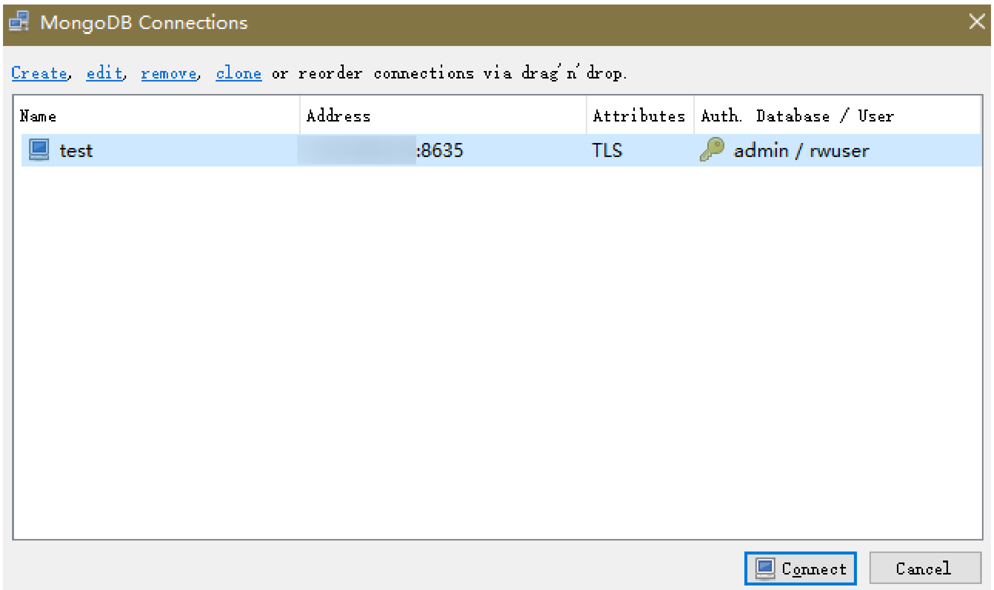
Auth Mechanism: SCRAM-SHA-1

□ Manually specify visible databases

3. Click **Save**.

Step 3 On the **MongoDB Connections** page, click **Connect** to connect to the replica set instance.

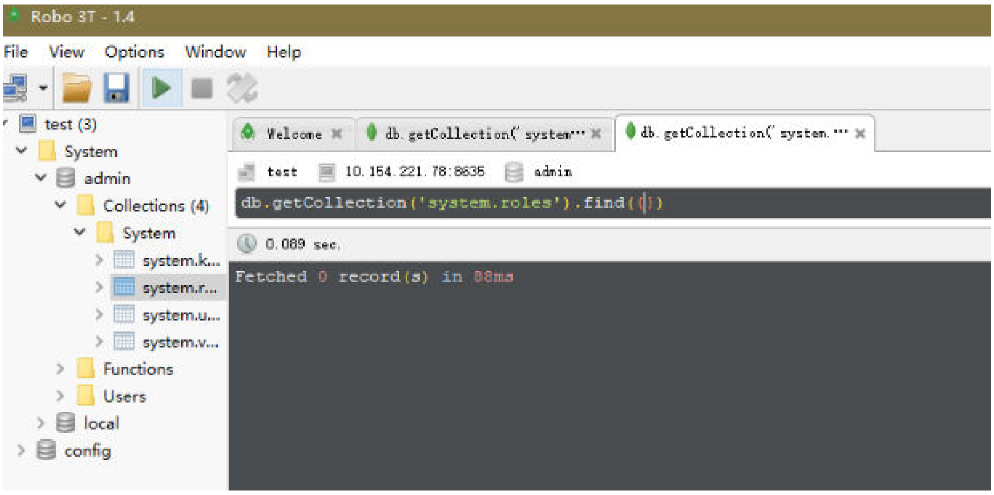
Figure 3-46 Replica set connection information


MongoDB Connections
Create, edit, remove, clone or reorder connections via drag'n'drop.
Connect
Cancel

Name	Address	Attributes	Auth. Database / User
test	[redacted]:8635	TLS	admin / rwuser

Step 4 If the replica set instance is successfully connected, the page shown in **Figure 3-47** is displayed.

Figure 3-47 Connection succeeded



```
db.getCollection('system.roles').find({})
```

0.089 sec.

```
Fetched 0 record(s) in 88ms
```

----End

3.2.5 Connecting to a Replica Set Instance Using Program Code

3.2.5.1 Java

If you are connecting to an instance using Java, an SSL certificate is optional, but downloading an SSL certificate and encrypting the connection will improve the security of your instance. SSL is disabled by default for newly created instances, but you can enable SSL by referring to **Enabling or Disabling SSL**. SSL encrypts connections to databases but it increases the connection response time and CPU usage. For this reason, enabling SSL is not recommended.

Prerequisites

Familiarize yourself with:

- Computer basics
- Java code

Obtaining and Using Java

- Download the Jar driver from: **https://repo1.maven.org/maven2/org/mongodb/mongo-java-driver/3.0.4/**
- To view the usage guide, visit **https://mongodb.github.io/mongo-java-driver/4.2/driver/getting-started/installation/**.

Using an SSL Certificate

NOTE

- Download the SSL certificate and verify the certificate before connecting to databases.
- In the **DB Information** area on the **Basic Information** page, click ⤓ in the **SSL** field to download the root certificate or certificate bundle.
- For details about how to set up an SSL connection, see the MongoDB Java Driver official document at **https://www.mongodb.com/docs/drivers/java/sync/current/fundamentals/connection/tls/#std-label-tls-ssl**.

Use Java to connect to the replica set. The format of the Java code is as follows:

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

Table 3-19 Parameter description

Parameter	Description
<username>	Current username.
<password>	Password for the current username
<instance_ip>	If you attempt to access the instance from an ECS, set *instance_ip* to the private IP address displayed on the **Basic Information** page of the instance to which you intend to connect.
	If you intend to access the instance through an EIP, set *instance_ip* to the EIP that has been bound to the instance.
<instance_port>	Database port displayed on the **Basic Information** page. Default value: **8635**
<database_name>	Name of the database to be connected.
authSource	Authentication user database. The value is **admin**.
ssl	Connection mode. **true** indicates that the SSL connection mode is used.

Use the keytool to configure the CA certificate. For details about the parameters, see **Table 3-20**.

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

Table 3-20 Parameter description

Parameter	Description
<path to certificate authority file>	Path for storing the SSL certificate.
<path to trust store>	Path for storing the truststore. Set this parameter as required, for example, **./trust/certs.keystore**.
<password>	Custom password.

Set the JVM system properties in the program to point to the correct truststore and keystore:

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

For details about the Java code, see the following example:

```
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)
                    .applyToSslSettings(builder -> builder.enabled(true))
                    .applyToSslSettings(builder -> builder.invalidHostNameAllowed(true))
                    .build();
            MongoClient mongoClient = MongoClients.create(settings);
            MongoDatabase database = mongoClient.getDatabase("admin");
            //Ping the database. If the operation fails, an exception occurs.
            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");
        }
    }
}
```

Connection Without the SSL Certificate

NOTE

You do not need to download the SSL certificate because certificate verification on the server is not required.

Connect to a replica set instance using Java. The Java link format is as follows:

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

Table 3-21 Parameter description

Parameter	Description
<username>	Current username.
<password>	Password for the current username
<instance_ip>	If you attempt to access the instance from an ECS, set *instance_ip* to the private IP address displayed on the **Basic Information** page of the instance to which you intend to connect.
	If you intend to access the instance through an EIP, set *instance_ip* to the EIP that has been bound to the instance.
<instance_port>	Database port displayed on the **Basic Information** page. Default value: **8635**
<database_name>	Name of the database to be connected.
authSource	Authentication user database. The value is **admin**.

For details about the Java code, see the following example:

```
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)
                    .retryWrites(true)
                    .build();
            MongoClient mongoClient = MongoClients.create(settings);
            MongoDatabase database = mongoClient.getDatabase("admin");
            //Ping the database. If the operation fails, an exception occurs.
            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

This section describes how to connect to a replica set instance using Python.

Prerequisites

1. To connect an ECS to an instance, the ECS must be able to communicate with the DDS instance. You can run the following command to connect to the IP address and port of the instance server to test the network connectivity.

   curl *ip:port*

   If the message **It looks like you are trying to access MongoDB over HTTP on the native driver port** is displayed, the network connectivity is normal.
2. Install Python and third-party installation package **pymongo** on the ECS. Pymongo 2.8 is recommended.
3. If SSL is enabled, you need to download the root certificate and upload it to the ECS.

Connection Code

- Enabling 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
```

- Disabling 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
```

NOTE

- The authentication database in the URL must be **admin**. That means setting **authSource** to **admin**.
- In SSL mode, you need to manually generate the trustStore file.
- The authentication database must be **admin**, and then switch to the service database.

4 Getting Started with Single Nodes

4.1 Connecting to a Single Node Instance

4.1.1 Connection Methods

You can access DDS over private or public networks.

Table 4-1 Connection methods

Method	IP Address	Scenario	Description
DAS	Not required	DAS provides a GUI and allows you to perform visualized operations on the console. SQL execution, advanced database management, and intelligent O&M are available to make database management simple, secure, and intelligent.	- Easy to use, secure, advanced, and intelligent - Recommended
Private network	Private IP address	DDS provides a private IP address by default. If your applications are running on an ECS in the same region, AZ, and VPC subnet as your DDS instance, you are advised to use a private IP address to connect the ECS to your DDS instances.	Secure and excellent performance

Method	IP Address	Scenario	Description
Public network	EIP	- If your applications are running on an ECS that is in a different region from the one where the DB instance is located, use an EIP to connect the ECS to your DDS DB instances. - If your applications are deployed on another cloud platform, EIP is recommended.	- Low security - For faster transmission and improved security, you are advised to migrate your applications to an ECS that is in the same subnet as your DDS instance and use a private IP address to access the instance.

4.1.2 (Recommended) Connecting to a Single Node Instance Through DAS

4.1.2.1 Overview

DAS provides a GUI and allows you to perform visualized operations on the console. SQL execution, advanced database management, and intelligent O&M are available to make database management simple, secure, and intelligent. You are advised to use DAS to connect to DB instances.

This section decribes how to connect to a single node instance through DAS.

Process

To connect to a single node instance, perform the following steps:

1. **Connect to a single node instance through DAS.**

4.1.2.2 Connecting to a Single Node Instance Through DAS

Data Admin Service (DAS) enables you to manage DB instances on a web-based console, simplifying database management and improving working efficiency. You can connect and manage instances through DAS. By default, you have the permission required for remote login. It is recommended that you use the DAS service to connect to instances. DAS is secure and convenient.

Procedure

Step 1 **Log in to the management console**.

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

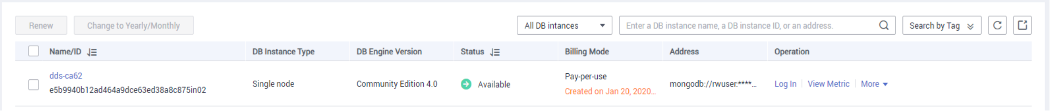
If you want compute and network resources dedicated to your exclusive use, **enable a DeC** and **apply for DCC resources**. After enabling a DeC, you can select the DeC region and project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, locate the target DB instance and click **Log In** in the **Operation** column.

Alternatively, click the target DB instance on the **Instances** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner of the page.

Figure 4-1 Instance management



Name/ID	DB Instance Type	DB Engine Version	Status	Billing Mode	Address	Operation
dds-ca62 e5b9940b12ad464a9dce63ed38a8c875in02	Single node	Community Edition 4.0	Available	Pay-per-use Created on Jan 20, 2020...	mongodb://rwuser:****...	Log In | View Metric | More

Step 5 On the displayed login page, enter the administrator username and password and click **Login**.

For details about how to manage databases through DAS, see **DDS Instance Management**.

----End

4.1.3 Connecting to a Single Node Instance over a Private Network

4.1.3.1 Configuring a Security Group

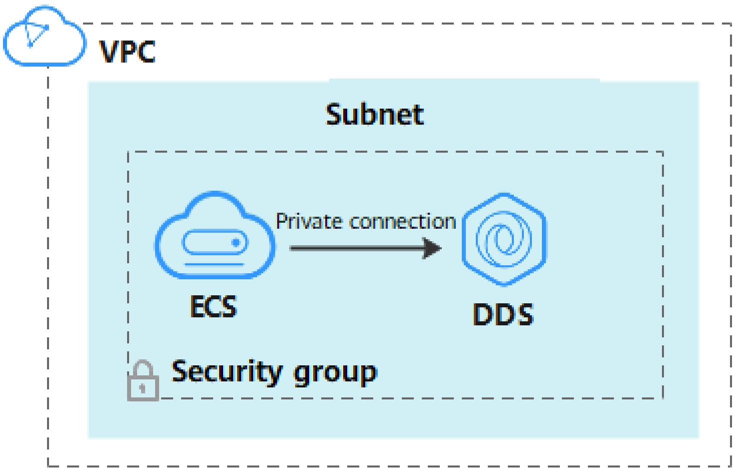
A security group is a logical group. It provides access control policies for the ECSs and instances that have the same security protection requirements and are mutually trusted in a VPC.

To ensure database security and reliability, you need to configure security group rules to allow specific IP addresses and ports to access DDS instances.

You can connect to an instance by configuring security group rules in following two ways:

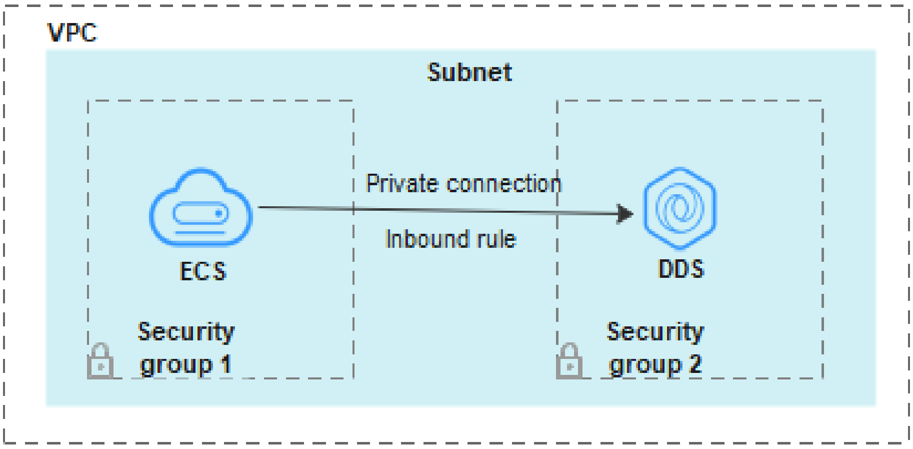
- If the ECS and instance are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to **Connecting to a Single Node Instance Using Mongo Shell (Private Network)**.

Figure 4-2 Same security group



- If the ECS and instance are in different security groups, you need to configure security group rules for them, separately.

Figure 4-3 Different security groups



  – Instance: Configure an **inbound rule** for the security group associated with the instance.
  – ECS: The default security group rule allows all outbound data packets. In this case, you do not need to configure a security group rule for the ECS. If not all traffic is allowed to reach the instance, configure an **outbound** rule for the ECS.

This section describes how to configure an inbound rule for an instance.

Precautions

- By default, an account can create up to 500 security group rules.
- Too many security group rules will increase the first packet latency, so a maximum of 50 rules for each security group is recommended.
- By default, one DDS instance is associated with only one security group.
- DDS allows you to associate multiple security groups to a DB instance. You can apply for the service based on your service requirements. For better

network performance, you are advised to select no more than five security groups.

Procedure

Step 1 Log in to the management console.

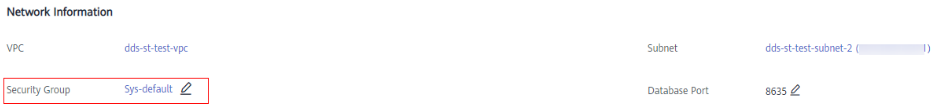
Step 2 Click 📍 in the upper left corner and select a region and a project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the instance name. The **Basic Information** page is displayed.

Step 5 In the **Network Information** area on the **Basic Information** page, click the security group.

Figure 4-4 Security Group



Network Information

VPC dds-st-test-vpc

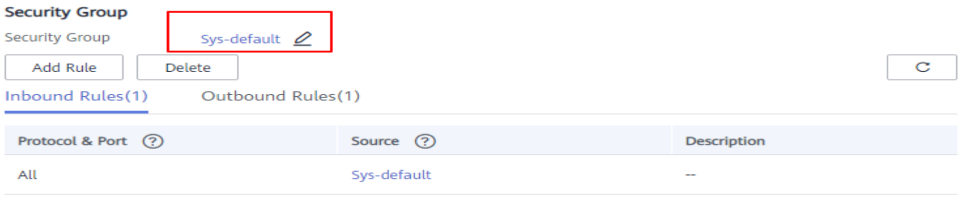
Subnet dds-st-test-subnet-2 ([redacted])

Security Group Sys-default

Database Port 8635

You can also choose **Connections** in the navigation pane on the left. On the **Private Connection** tab, in the **Security Group** area, click the security group name.

Figure 4-5 Security Group



Security Group

Security Group Sys-default

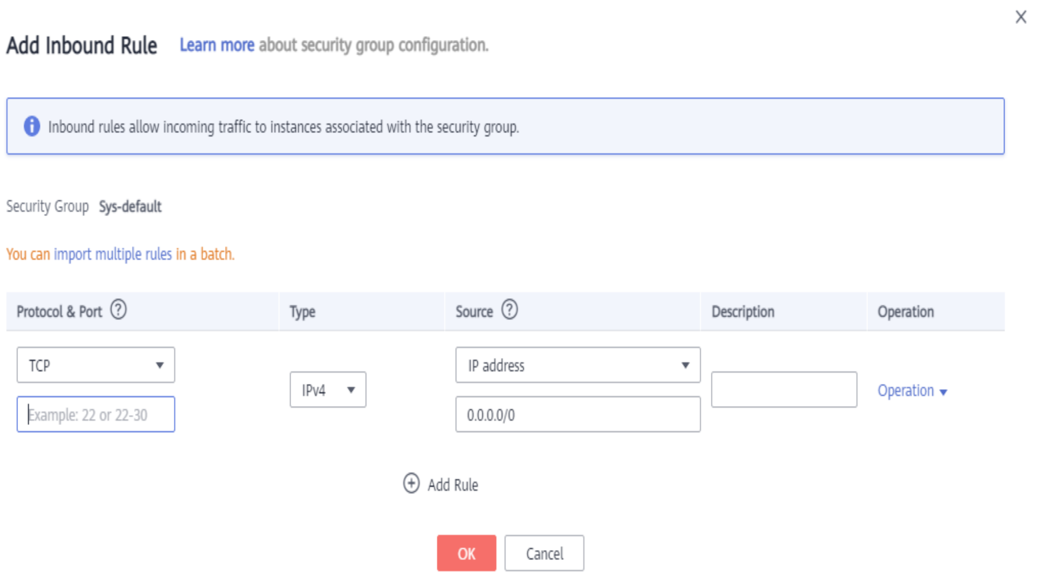
Protocol & Port	Source	Description
All	Sys-default	--

Step 6 On the **Security Group** page, locate the target security group and click **Manage Rule** in the **Operation** column.

Step 7 On the **Inbound Rules** tab, click **Add Rule**. The **Add Inbound Rule** dialog box is displayed.

Step 8 Add a security group rule as prompted.

Figure 4-6 Add Inbound Rule



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group Sys-default

You can import multiple rules in a batch.

Protocol & Port	Type	Source	Description	Operation
TCP Example: 22 or 22-30	IPv4	IP address 0.0.0.0/0		Operation

Table 4-2 Inbound rule settings

Parameter	Description	Example
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	The security group rule actions. A rule with a deny action overrides another with an allow action if the two rules have the same priority.	Allow
Protocol & Port	The network protocol required for access. Available options: **TCP**, **UDP**, **ICMP**, or **GRE**	TCP
	Port: the port on which you wish to allow access to DDS. The default port is 8635. The port ranges from 2100 to 9500 or can be 27017, 27018, or 27019.	8635
Type	IP address type. Only **IPv4** and **IPv6** are supported.	IPv4

Parameter	Description	Example
Source	Specifies the supported IP address, security group, and IP address group, which allow access from IP addresses or instances in other security group. Example: ● Single IP address: 192.168.10.10/32 ● IP address segment: 192.168.1.0/24 ● All IP addresses: 0.0.0.0/0 ● Security group: sg-abc ● IP address group: ipGroup-test If you enter a security group, all ECSs associated with the security group comply with the created rule. For more information about IP address groups, see **IP Address Group**.	0.0.0.0/0
Description	(Optional) Provides supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

Step 9 Click **OK**.

----End

4.1.3.2 Connecting to a Single Node Instance Using Mongo Shell (Private Network)

Mongo shell is the default client for the MongoDB database server. You can use Mongo Shell to connect to DB instances, and query, update, and manage data in databases. DDS is compatible with MongoDB. Mongo Shell is a part of the MongoDB client. To use Mongo Shell, download and install the MongoDB client first, and then use the Mongo shell to connect to the DB instance.

By default, a DDS instance provides a private IP address. If your applications are deployed on an ECS and are in the same region and VPC as DDS instances, you can connect to DDS instances using a private IP address to achieve a fast transmission rate and high security.

This section describes how to use Mongo Shell installed on a Linux ECS to connect to a single node instance over a private network.

You can connect to an instance using an SSL connection or an unencrypted connection. The SSL connection is encrypted and more secure. To improve data transmission security, connect to instances using SSL.

Prerequisites

1. For details about how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.
2. Install the MongoDB client on the ECS.

   For details about how to install a MongoDB client, see **How Can I Install a MongoDB Client?**
3. The ECS can communicate with the DDS instance. For details, see ECS.

SSL

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

Step 1 **Log in to the management console**.

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

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the instance name.

Step 5 In the navigation pane on the left, choose **Connections**.

Step 6 In the **Basic Information** area, click ⤓ next to the **SSL** field.

Step 7 Import the root certificate to the Linux or Windows ECS. For details, see **How Can I Import the Root Certificate to a Windows or Linux OS?**

Step 8 Connect to a DDS instance.

Using a private IP address

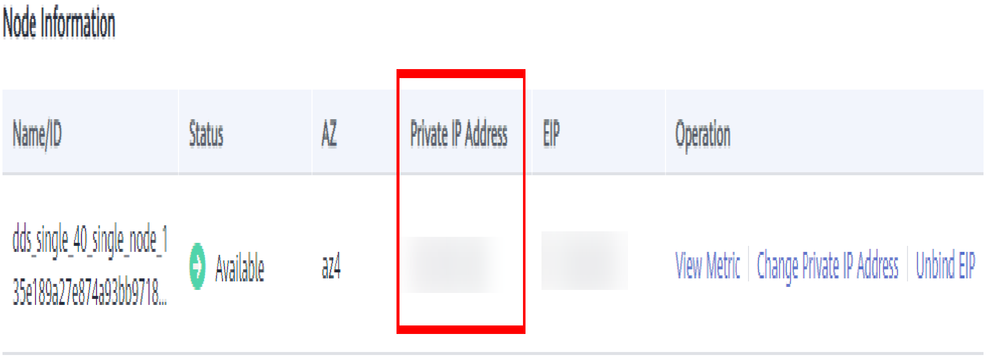
Example command:

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

Parameter description:

- **DB_HOST** is the private IP address of the instance to be connected.

  On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. On the **Private Connection** tab, obtain the IP address of the corresponding node.



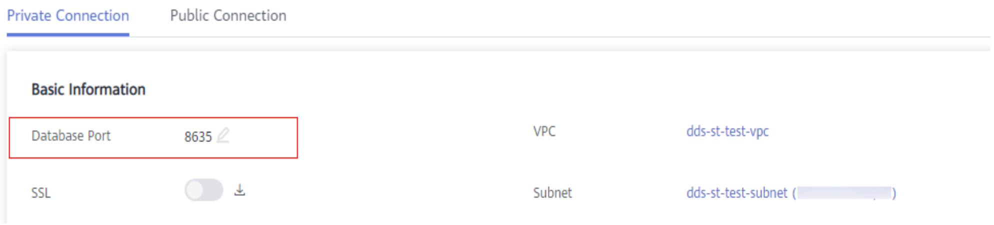
Node Information

Name/ID	Status	AZ	Private IP Address	EIP	Operation
dds_single_40_single_node_1 35e189a27e874a93bb9718...	Available	az4	[redacted]	[redacted]	View Metric | Change Private IP Address | Unbind EIP

- **DB_PORT** is the database port. The default port number is 8635.

  You can click the instance name to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Private Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

  Figure 4-7 Obtaining the port



Basic Information

Database Port	8635	VPC	dds-st-test-vpc
SSL		Subnet	dds-st-test-subnet ([redacted])

- **DB_USER** is the database user. The default value is **rwuser**.
- **FILE_PATH** is the path for storing the root certificate.
- **--sslAllowInvalidHostnames**: To ensure that the internal communication of the single nodes does not occupy resources such as the user IP address and bandwidth, the single node certificate is generated using the internal management IP address. **--sslAllowInvalidHostnames** is needed for the SSL connection over private networks.

Command example:

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

Enter the database password when prompted:

```
Enter password:
```

Step 9 Check the connection result. If the following information is displayed, the connection is successful.

```
replica:PRIMARY>
```

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

Step 1 Log in to the ECS.

Step 2 Connect to a DDS instance.

Using a private IP address

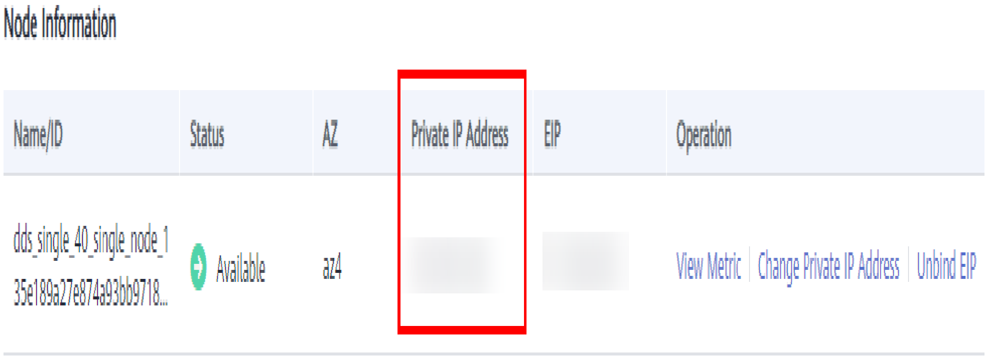
Example command:

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

Parameter description:

- **DB_HOST** is the private IP address of the instance to be connected.

  On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. On the **Private Connection** tab, obtain the IP address of the corresponding node.



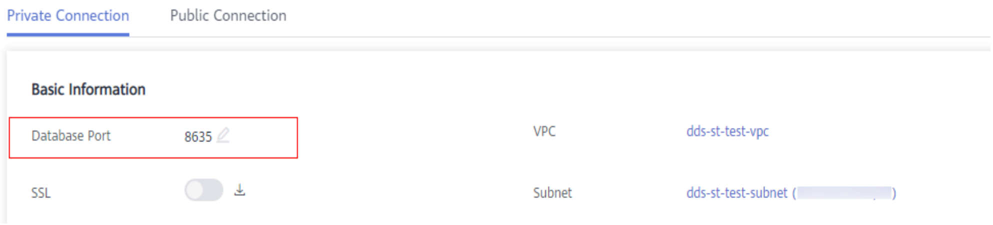
Node Information

Name/ID	Status	AZ	Private IP Address	EIP	Operation
dds_single_40_single_node_1 35e189a27e874a93bb9718...	Available	az4	[redacted]	[redacted]	View Metric | Change Private IP Address | Unbind EIP

- **DB_PORT** is the database port. The default port number is 8635.

  You can click the instance name to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Private Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

Figure 4-8 Obtaining the port



Basic Information

Database Port	8635	VPC	dds-st-test-vpc
SSL		Subnet	dds-st-test-subnet ([redacted])

- **DB_USER** is the database user. The default value is **rwuser**.

Command example:

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

Enter the database password when prompted:

```
Enter password:
```

Step 3 Check the connection result. If the following information is displayed, the connection is successful.

```
replica:PRIMARY>
```

----End

4.1.4 Connecting to a Single Node Instance over a Public Network

4.1.4.1 Binding and Unbinding an EIP

After you create an instance, you can bind an EIP to it to allow external access. If later you want to prohibit external access, you can also unbind the EIP from the instance.

Precautions

- Deleting a bound EIP does not mean that the EIP is unbound.
- Before accessing a database, apply for an EIP on the VPC console. Then, add an inbound rule to allow the IP addresses or IP address ranges of ECSs. For details, see **Configuring a Security Group**.
- To change the EIP that has been bound to a node, unbind it from the node first.

Binding an EIP

Step 1 **Log in to the management console**.

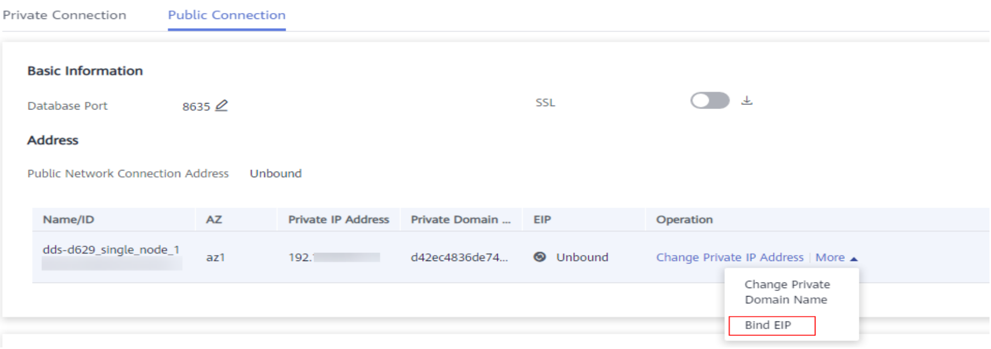
Step 2 Click 📍 in the upper left corner and select a region and a project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the single node instance name.

Step 5 In the navigation pane on the left, choose **Connections**. Click the **Public Connection** tab. In the **Basic Information** area, locate the node you want to bind an EIP to and click **Bind EIP** in the **Operation** column.

Figure 4-9 Binding an EIP



Basic Information

Database Port 8635

SSL

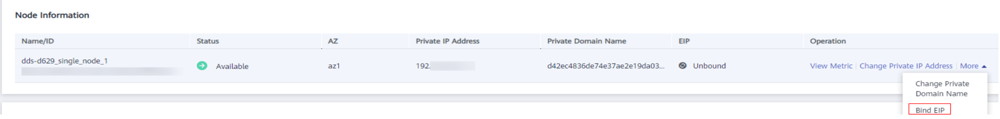
Address

Public Network Connection Address Unbound

Name/ID	AZ	Private IP Address	Private Domain ...	EIP	Operation
dds-d629_single_node_1	az1	192.	d42ec4836de74...	Unbound	Change Private IP Address | More

You can also locate the node in the **Node Information** area on the **Basic Information** page and click **Bind EIP** in the **Operation** column.

Figure 4-10 Binding an EIP

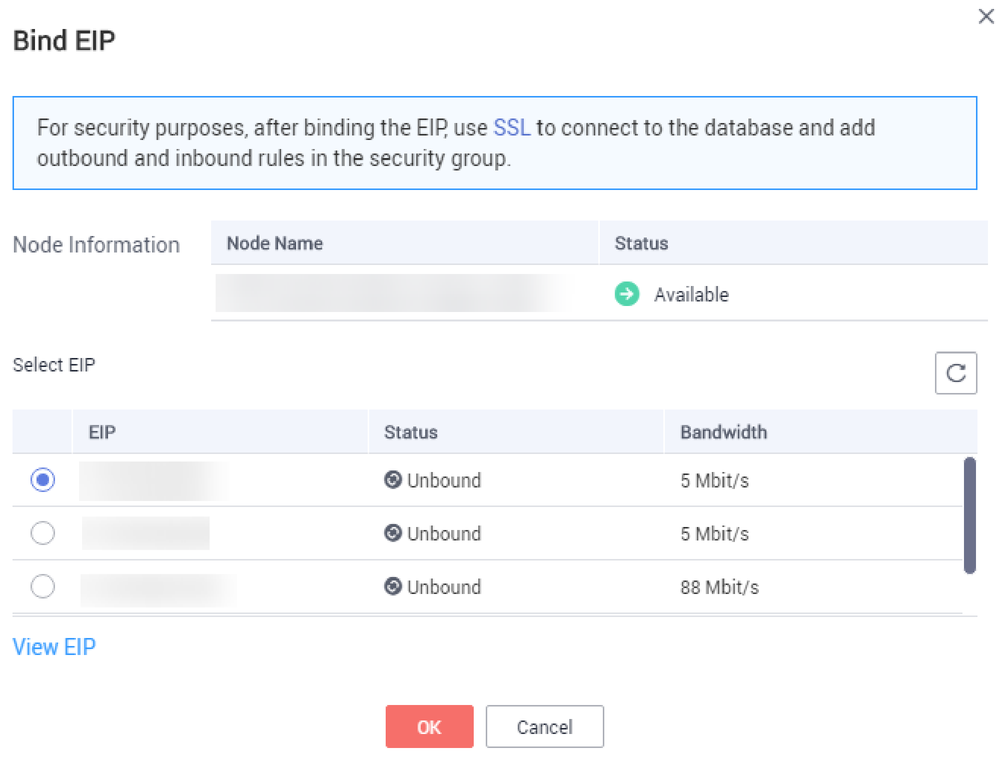


Node Information

Name/ID	Status	AZ	Private IP Address	Private Domain Name	EIP	Operation
dds-d629_single_node_1	Available	az1	192.	d42ec4836de74e37ae2e19da03...	Unbound	View Metric | Change Private IP Address | More

Step 6 In the displayed dialog box, all available unbound EIPs are listed. Select the required EIP and click **OK**. If no available EIPs are displayed, click **View EIP** and create an EIP on the VPC console.

Figure 4-11 Selecting an EIP



Bind EIP

For security purposes, after binding the EIP, use SSL to connect to the database and add outbound and inbound rules in the security group.

Node Information

Node Name	Status
	Available

Select EIP

	EIP	Status	Bandwidth
●		Unbound	5 Mbit/s
○		Unbound	5 Mbit/s
○		Unbound	88 Mbit/s

Step 7 In the **EIP** column, you can view the EIP that was bound.

To unbind an EIP from the instance, see **Unbinding an EIP**.

----End

Unbinding an EIP

Step 1 **Log in to the management console**.

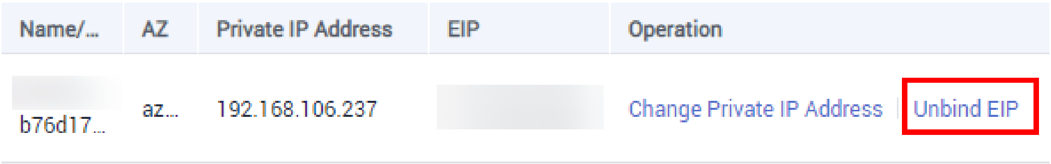
Step 2 Click 📍 in the upper left corner and select a region and a project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the single node instance name.

Step 5 In the navigation pane on the left, choose **Connections**. Click the **Public Connection** tab. In the **Basic Information** area, locate the node and click **Unbind EIP** in the **Operation** column.

Figure 4-12 Unbinding an EIP



Name/...	AZ	Private IP Address	EIP	Operation
[redacted] b76d17...	az...	192.168.106.237	[redacted]	Change Private IP Address | Unbind EIP

You can also locate the node in the **Node Information area** on the **Basic Information** page and click **Unbind EIP** in the **Operation** column.

Step 6 In the displayed dialog box, click **Yes**.

To bind an EIP to the instance again, see **Binding an EIP**.

----End

4.1.4.2 Configuring a Security Group

A security group is a logical group. It provides access control policies for the ECSs and instances that have the same security protection requirements and are mutually trusted in a VPC.

To ensure database security and reliability, you need to configure security group rules to allow specific IP addresses and ports to access DDS instances.

If you attempt to connect to an instance through an EIP, you need to configure an inbound rule for the security group associated with the instance.

Precautions

- By default, an account can create up to 500 security group rules.
- Too many security group rules will increase the first packet latency, so a maximum of 50 rules for each security group is recommended.

- By default, one DDS instance is associated with only one security group.
- DDS allows you to associate multiple security groups to a DB instance. You can apply for the service based on your service requirements. For better network performance, you are advised to select no more than five security groups.

Procedure

Step 1 Log in to the management console.

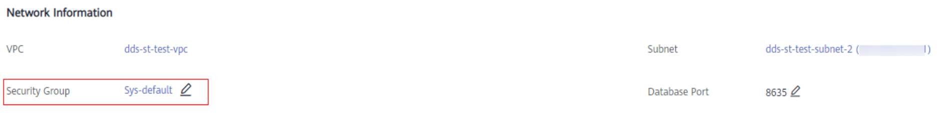
Step 2 Click 📍 in the upper left corner and select a region and a project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the instance name. The **Basic Information** page is displayed.

Step 5 In the **Network Information** area on the **Basic Information** page, click the security group.

Figure 4-13 Security Group



Network Information

VPC dds-st-test-vpc

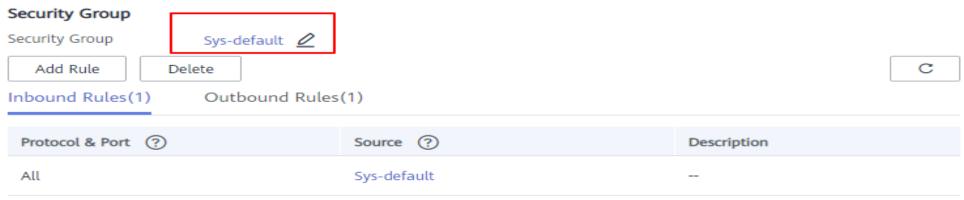
Subnet dds-st-test-subnet-2 ([redacted])

Security Group Sys-default

Database Port 8635

You can also choose **Connections** in the navigation pane on the left. On the **Public Connection** tab, in the **Security Group** area, click the security group name.

Figure 4-14 Security Group



Security Group

Security Group Sys-default

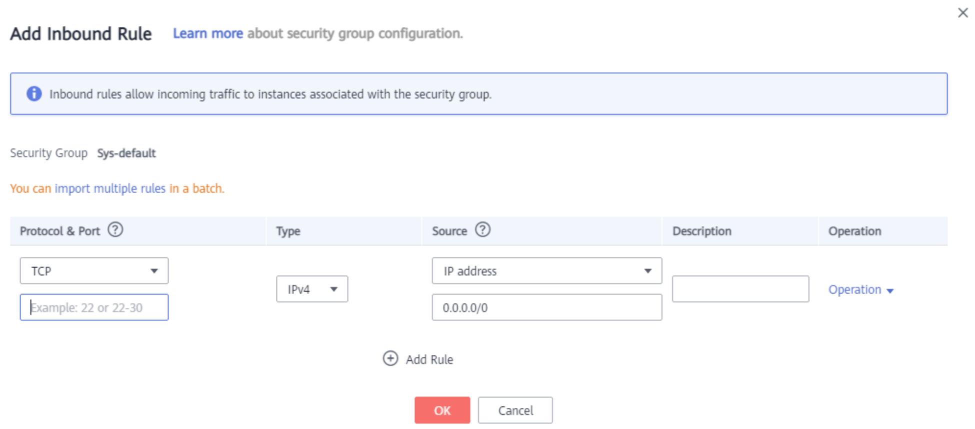
Protocol & Port	Source	Description
All	Sys-default	--

Step 6 On the **Security Group** page, locate the target security group and click **Manage Rule** in the **Operation** column.

Step 7 On the **Inbound Rules** tab, click **Add Rule**. The **Add Inbound Rule** dialog box is displayed.

Step 8 Add a security group rule as prompted.

Figure 4-15 Add Inbound Rule



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group Sys-default

You can import multiple rules in a batch.

Protocol & Port	Type	Source	Description	Operation
TCP Example: 22 or 22-30	IPv4	IP address 0.0.0.0/0		Operation

Table 4-3 Inbound rule settings

Parameter	Description	Example Value
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	The security group rule actions. A rule with a deny action overrides another with an allow action if the two rules have the same priority.	Allow
Protocol & Port	The network protocol required for access. The option can be **All**, **TCP**, **UDP**, **ICMP**, or **GRE**.	TCP
	Port: the port on which you wish to allow access to DDS. The default port is 8635. The port ranges from 2100 to 9500 or can be 27017, 27018, or 27019.	8635
Type	IP address type. Only **IPv4** and **IPv6** are supported.	IPv4

Parameter	Description	Example Value
Source	Specifies the supported IP address, security group, and IP address group, which allow access from IP addresses or instances in other security group. Example: ● Single IP address: 192.168.10.10/32 ● IP address segment: 192.168.1.0/24 ● All IP addresses: 0.0.0.0/0 ● Security group: sg-abc ● IP address group: ipGroup-test If you enter a security group, all ECSs associated with the security group comply with the created rule. For more information about IP address groups, see **IP Address Group**.	0.0.0.0/0
Description	(Optional) Provides supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

Step 9 Click **OK**.

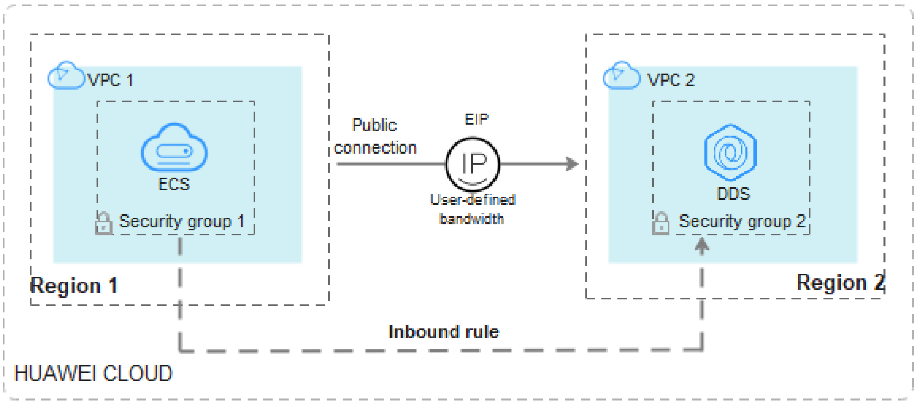
----End

4.1.4.3 Connecting to a Single Node Instance Using Mongo Shell (Public Network)

In the following scenarios, you can access a DDS instance from the Internet by binding an EIP to the instance.

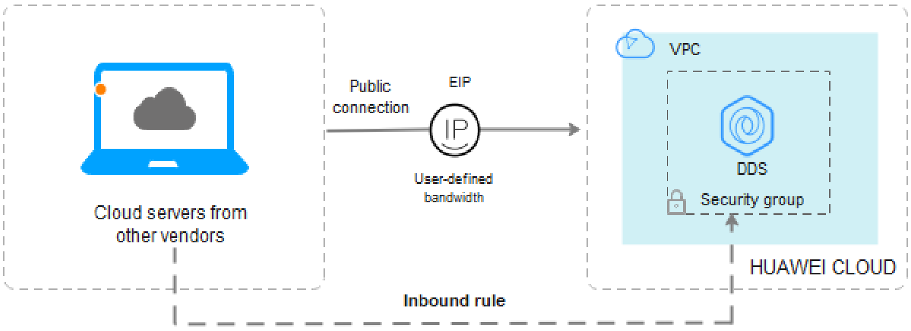
Scenario 1: Your applications are deployed on an ECS and are not in the same region as the DDS instance.

Figure 4-16 Accessing DDS from ECS across regions



Scenario 2: Your applications are deployed on a cloud server provided by other vendors.

Figure 4-17 Accessing DDS from other cloud servers



This section describes how to use Mongo Shell to connect to a single node instance through an EIP.

You can connect to an instance using an SSL connection or an unencrypted connection. The SSL connection is encrypted and more secure. To improve data transmission security, connect to instances using SSL.

Prerequisites

1. For details about how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.
2. **Bind an EIP** to the single node instance and **configure security group rules** to ensure that the EIP can be accessed from the ECS.
3. Install the MongoDB client on the ECS.

   For details about how to install a MongoDB client, see **How Can I Install a MongoDB Client?**

SSL

> **NOTICE**
>
> If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

Step 1 **Log in to the management console**.

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

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the instance name.

Step 5 In the navigation pane on the left, choose **Connections**.

Step 6 In the **Basic Information** area, click ⤓ next to the **SSL** field.

Step 7 Import the root certificate to the Linux or Windows ECS. For details, see **How Can I Import the Root Certificate to a Windows or Linux OS?**

Step 8 Connect to the instance in the directory where the MongoDB client is located.

Using an EIP

Example command:

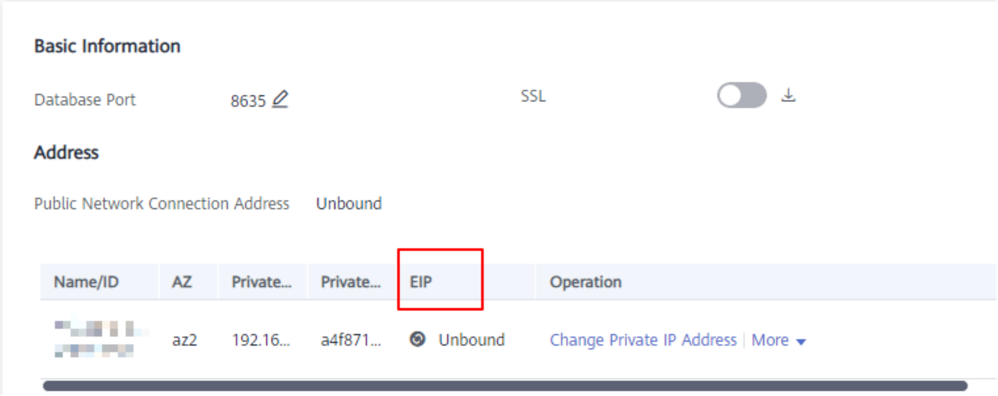
./mongo --host <*DB_HOST*> **--port** <*DB_PORT*> **-u** <*DB_USER*> **-p --authenticationDatabaseadmin --ssl --sslCAFile**<*FILE_PATH*> **--sslAllowInvalidHostnames**

Parameter description:

- **DB_HOST** is the EIP bound to the instance to be connected.

  On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**> **Public Connection** and obtain the EIP of the corresponding node.

Figure 4-18 Obtaining an EIP



Basic Information

Database Port 8635

SSL

Address

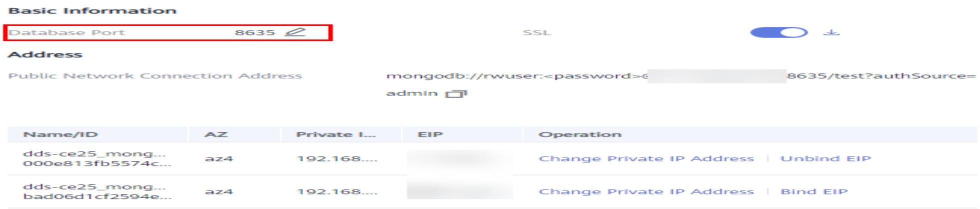
Public Network Connection Address Unbound

Name/ID	AZ	Private...	Private...	EIP	Operation
[redacted]	az2	192.16...	a4f871...	Unbound	Change Private IP Address | More

- **DB_PORT** is the database port. The default port number is 8635.

  You can click the instance name to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Public Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

Figure 4-19 Obtaining the port



Basic Information

Database Port 8635

SSL

Address

Public Network Connection Address mongodb://rwuser:<password>@[redacted]8635/test?authSource=admin

Name/ID	AZ	Private I...	EIP	Operation
dds-ce25_mong... 000e813fb5574c...	az4	192.168....	[redacted]	Change Private IP Address | Unbind EIP
dds-ce25_mong... bad06d1cf2594e...	az4	192.168....	[redacted]	Change Private IP Address | Bind EIP

- **DB_USER** is the database user. The default value is **rwuser**.
- **FILE_PATH** is the path for storing the root certificate.
- **--sslAllowInvalidHostnames**: To ensure that the internal communication of the single nodes does not occupy resources such as the user IP address and bandwidth, the single node certificate is generated using the internal management IP address. **--sslAllowInvalidHostnames** is needed for the SSL connection through a public network.

Command example:

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

Enter the database password when prompted:

```
Enter password:
```

Step 9 Check the connection result. If the following information is displayed, the connection is successful.

```
replica:PRIMARY>
```

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

Step 1 Log in to the ECS.

Step 2 Connect to a DDS instance.

Using an EIP

Example command:

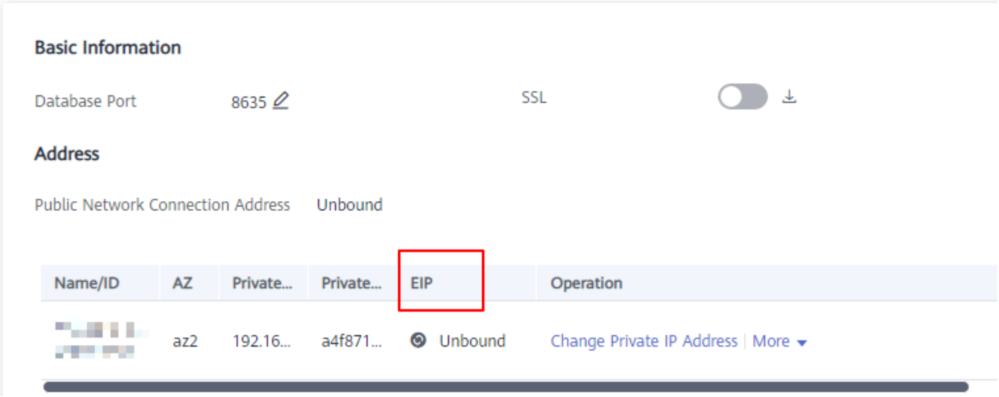
./mongo --host <*DB_HOST*> **--port** <*DB_PORT*> **-u** <*DB_USER*> **-p --authenticationDatabase admin**

Parameter description:

- **DB_HOST** is the EIP bound to the instance to be connected.

  On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**> **Public Connection** and obtain the EIP of the corresponding node.

  Figure 4-20 Obtaining an EIP

  Basic Information

  Database Port 8635

  SSL

  Address

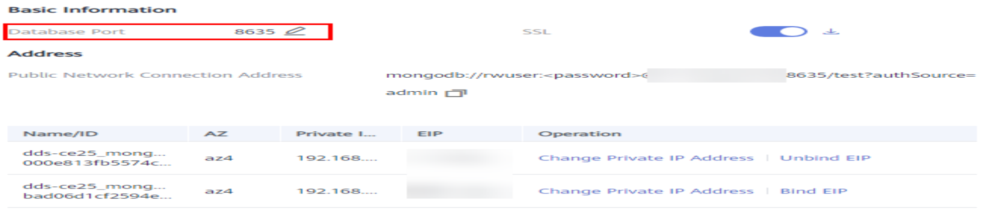
  Public Network Connection Address Unbound

Name/ID	AZ	Private...	Private...	EIP	Operation
[redacted]	az2	192.16...	a4f871...	Unbound	Change Private IP Address | More

- **DB_PORT** is the database port. The default port number is 8635.

  You can click the instance name to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Public Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

  Figure 4-21 Obtaining the port

  Basic Information

  Database Port 8635

  SSL

  Address

  Public Network Connection Address mongodb://rwuser:<password>@[redacted]8635/test?authSource=admin

Name/ID	AZ	Private I...	EIP	Operation
dds-ce25_mong... 000e813fb5574c...	az4	192.168....	[redacted]	Change Private IP Address | Unbind EIP
dds-ce25_mong... bad06d1cf2594e...	az4	192.168....	[redacted]	Change Private IP Address | Bind EIP

- **DB_USER** is the database user. The default value is **rwuser**.

Command example:

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

Enter the database password when prompted:

```
Enter password:
```

Step 3 Check the connection result. If the following information is displayed, the connection is successful.

```
replica:PRIMARY>
```

----End

4.1.4.4 Connecting to a Single Node Instance Using Robo 3T

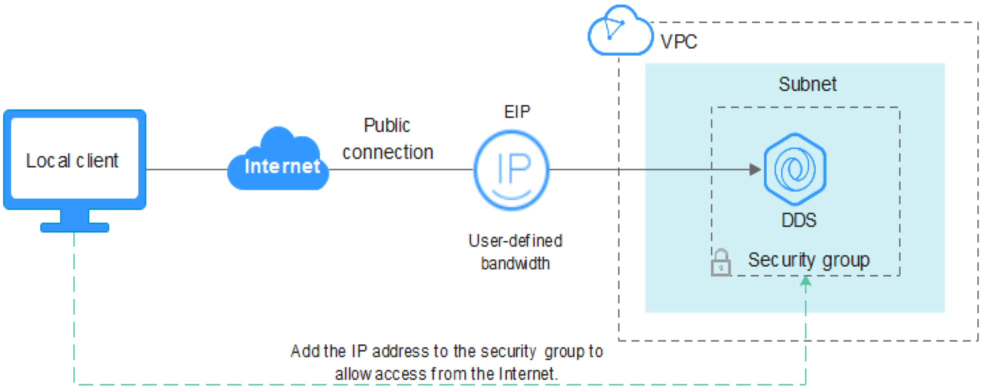
If you want to connect to an instance from a local device, you can bind an EIP to the instance and use Robo 3T to connect to the instance over a public network.

This section describes how to use Robo 3T to connect to a cluster instance from a local device. In this section, the Windows operating system (OS) used by the client is used as an example.

Robo 3T can connect to an instance with an unencrypted connection or an encrypted connection (SSL). To improve data transmission security, connect to instances using SSL.

Connection Diagram

Figure 4-22 Connection diagram



Prerequisites

1. **Bind an EIP** to the single node instance and configure security group rules to ensure that the instance can be accessed using Robo 3T.
2. Install Robo 3T.

   Install Robo 3T. For details, see **How Can I Install Robo 3T?**

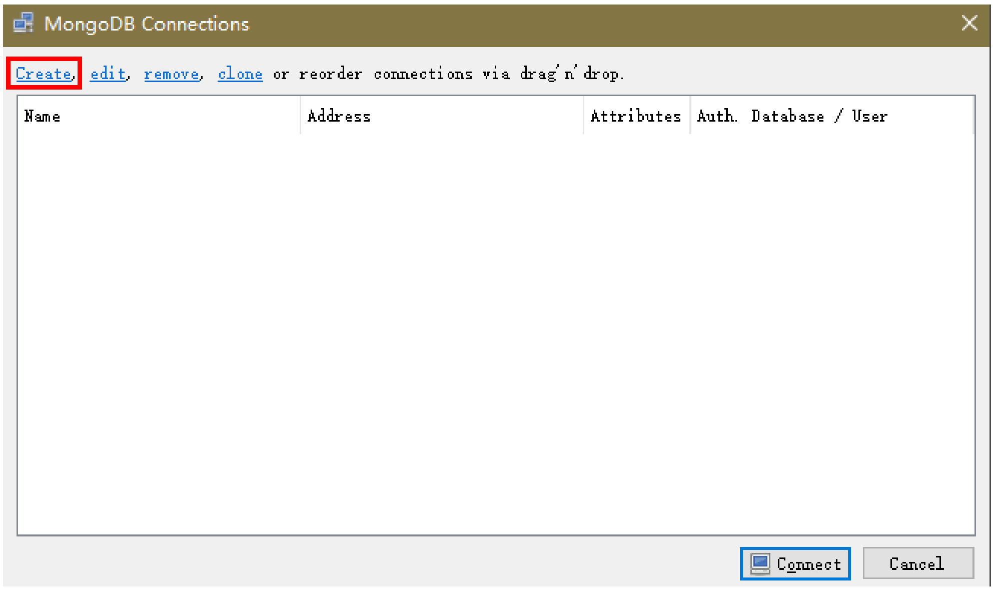
SSL

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

Step 1 Run the installed Robo 3T. On the displayed dialog box, click **Create**.

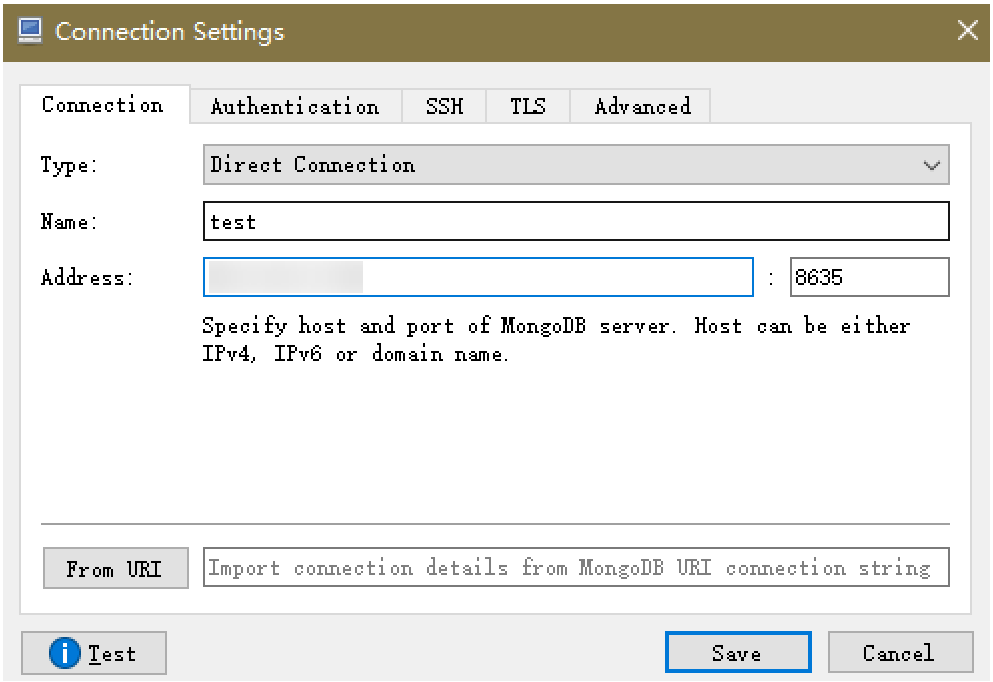
Figure 4-23 Connections



Step 2 In the **Connection Settings** dialog box, set the parameters of the new connection.

1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the DDS DB instance in the **Address** text box.

Figure 4-24 Connection



Type: Direct Connection

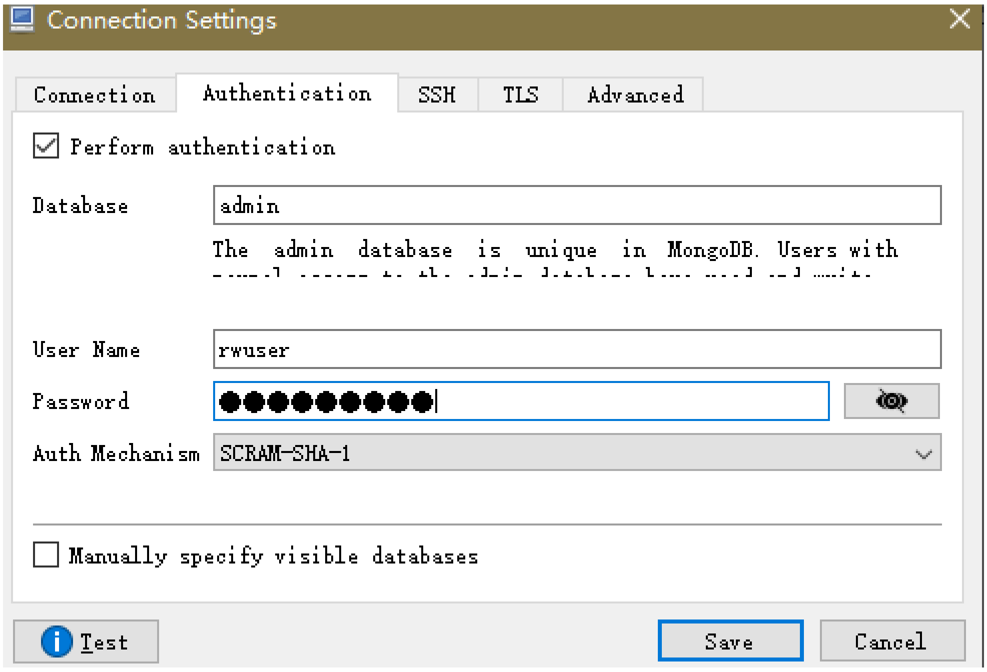
Name: test

Address: [redacted] : 8635

Specify host and port of MongoDB server. Host can be either IPv4, IPv6 or domain name.

2. On the **Authentication** tab, set **Database** to **admin**, **User Name** to **rwuser**, and **Password** to the administrator password you set during the creation of the cluster instance.

Figure 4-25 Authentication



☑ Perform authentication

Database: admin

The admin database is unique in MongoDB. Users with

User Name: rwuser

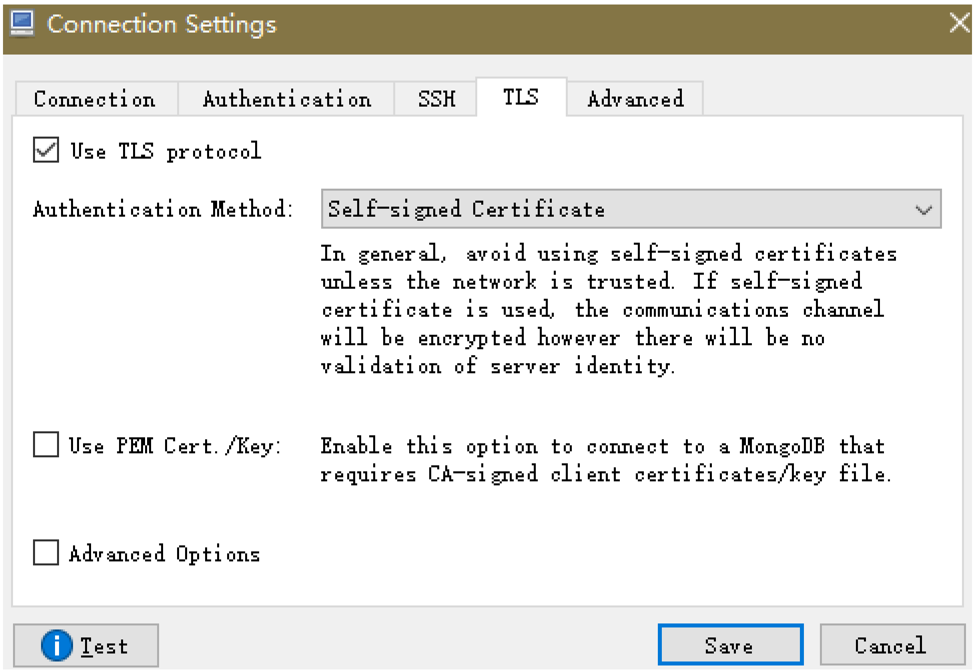
Password: ●●●●●●●●●●

Auth Mechanism: SCRAM-SHA-1

□ Manually specify visible databases

3. On the **TLS** tab, select **Use TLS protocol** and select **Self-signed Certificate** for **Authentication Method**.

Figure 4-26 SSL



☑ Use TLS protocol

Authentication Method: Self-signed Certificate

In general, avoid using self-signed certificates unless the network is trusted. If self-signed certificate is used, the communications channel will be encrypted however there will be no validation of server identity.

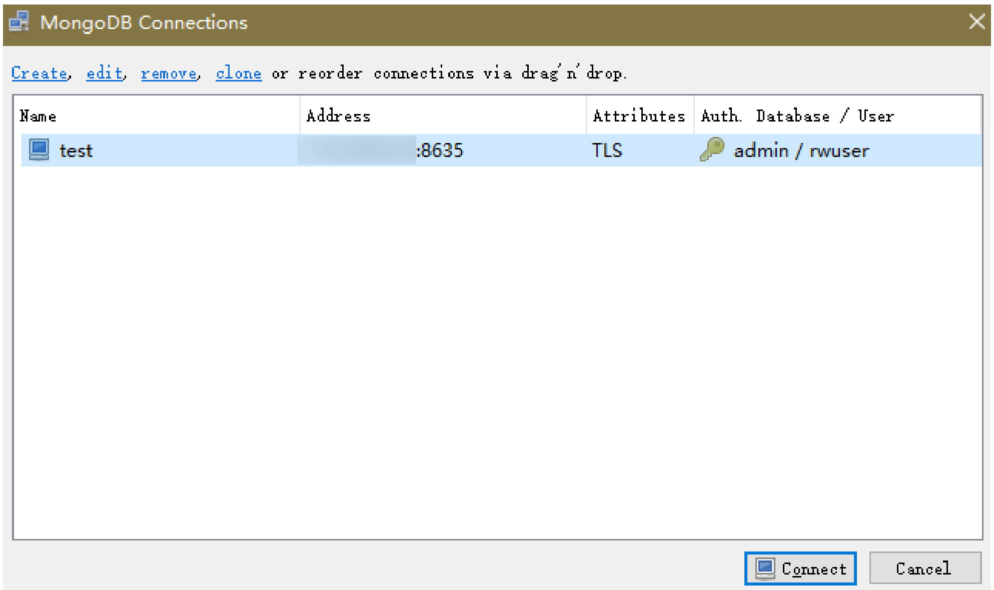
□ Use PEM Cert./Key: Enable this option to connect to a MongoDB that requires CA-signed client certificates/key file.

□ Advanced Options

4. Click **Save**.

Step 3 On the **MongoDB Connections** page, click **Connect** to connect to the single-node instance.

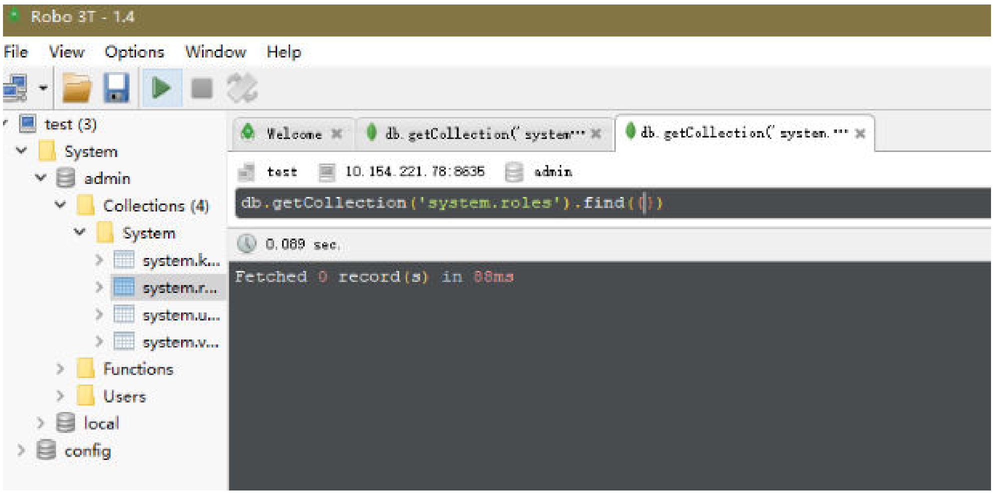
Figure 4-27 Single node connection information


MongoDB Connections
Create, edit, remove, clone or reorder connections via drag'n'drop.
Connect
Cancel

Name	Address	Attributes	Auth. Database / User
test	[redacted]:8635	TLS	admin / rwuser

Step 4 If the single-node instance is successfully connected, the page shown in **Figure 4-28** is displayed.

Figure 4-28 Single node connected



```
db.getCollection('system.roles').find({})
```

```
Fetched 0 record(s) in 88ms
```

----End

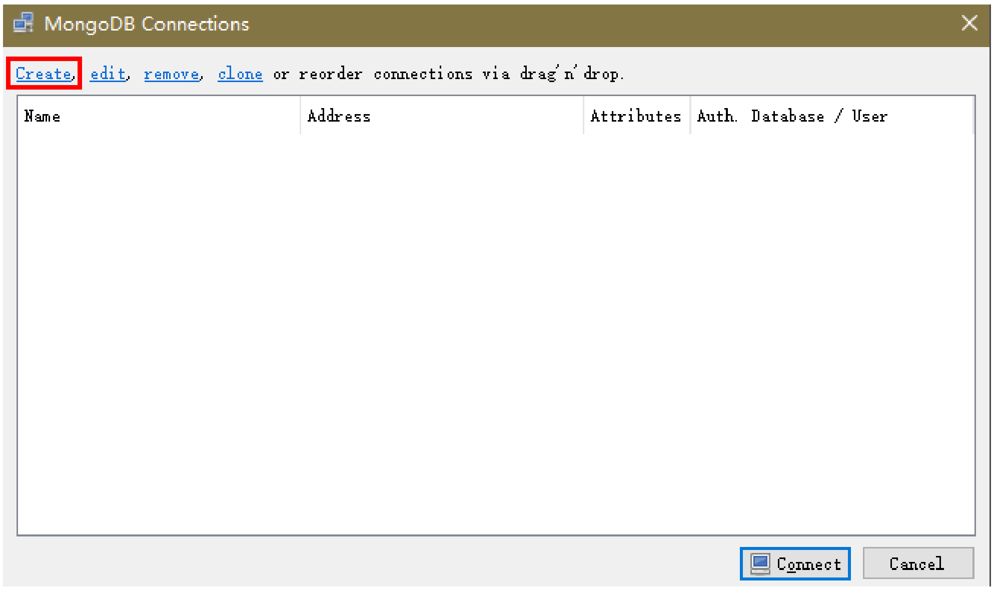
Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

Step 1 Run the installed Robo 3T. On the displayed dialog box, click **Create**.

Figure 4-29 Connections



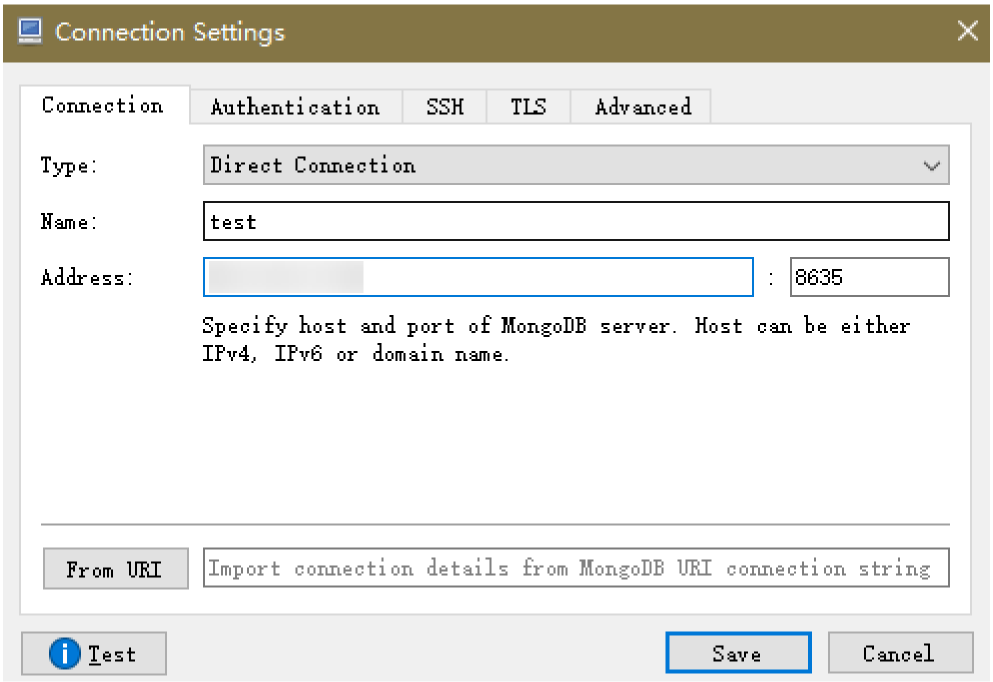
Create, edit, remove, clone or reorder connections via drag'n'drop.

Name	Address	Attributes	Auth. Database / User

Step 2 In the **Connection Settings** dialog box, set the parameters of the new connection.

1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the DDS DB instance in the **Address** text box.

Figure 4-30 Connection



Type: Direct Connection

Name: test

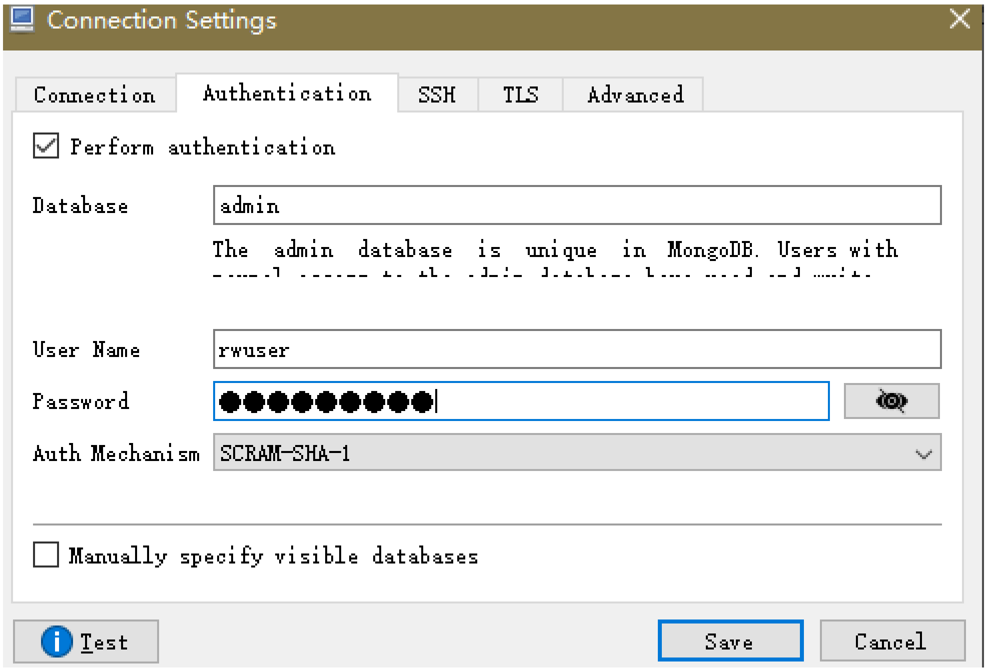
Address: [redacted] : 8635

Specify host and port of MongoDB server. Host can be either IPv4, IPv6 or domain name.

Import connection details from MongoDB URI connection string

2. On the **Authentication** tab, set **Database** to **admin**, **User Name** to **rwuser**, and **Password** to the administrator password you set during the creation of the cluster instance.

Figure 4-31 Authentication



☑ Perform authentication

Database: admin

The admin database is unique in MongoDB. Users with

User Name: rwuser

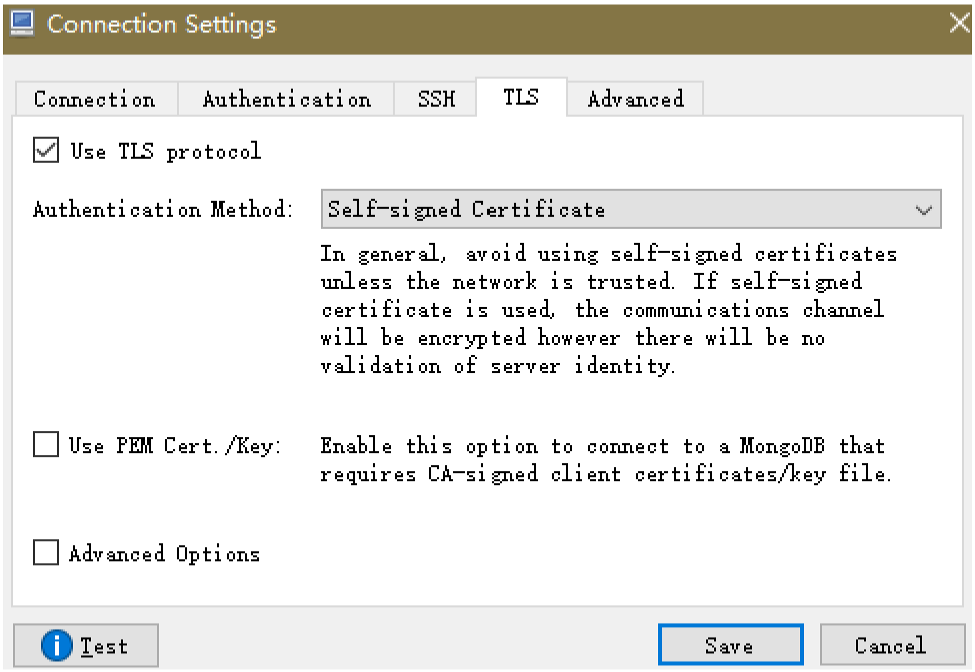
Password: ●●●●●●●●●●

Auth Mechanism: SCRAM-SHA-1

□ Manually specify visible databases

3. On the **TLS** tab, select **Use TLS protocol** and select **Self-signed Certificate** for **Authentication Method**.

Figure 4-32 SSL



☑ Use TLS protocol

Authentication Method: Self-signed Certificate

In general, avoid using self-signed certificates unless the network is trusted. If self-signed certificate is used, the communications channel will be encrypted however there will be no validation of server identity.

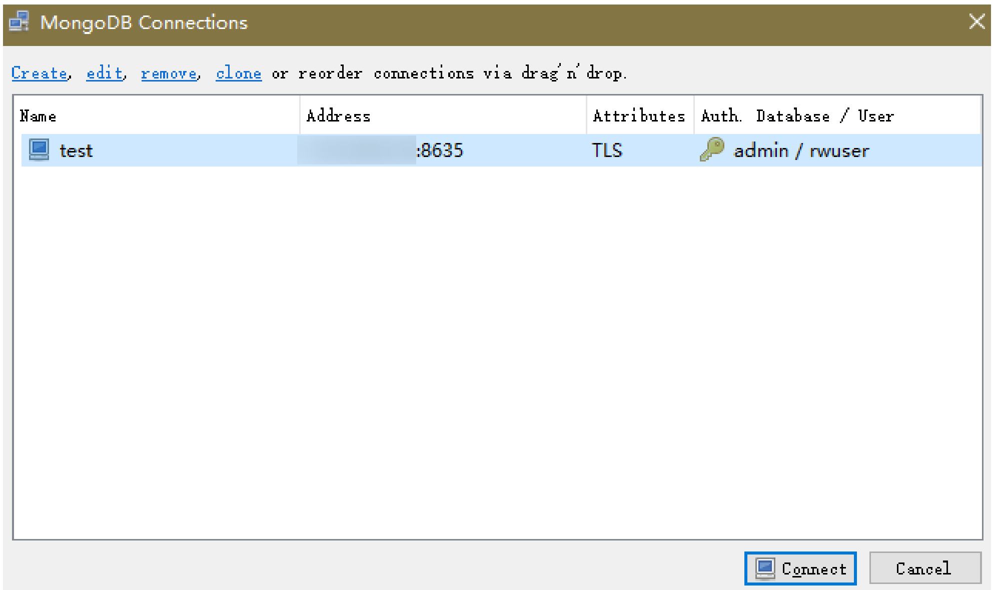
□ Use PEM Cert./Key: Enable this option to connect to a MongoDB that requires CA-signed client certificates/key file.

□ Advanced Options

4. Click **Save**.

Step 3 On the **MongoDB Connections** page, click **Connect** to connect to the single-node instance.

Figure 4-33 Single node connection information

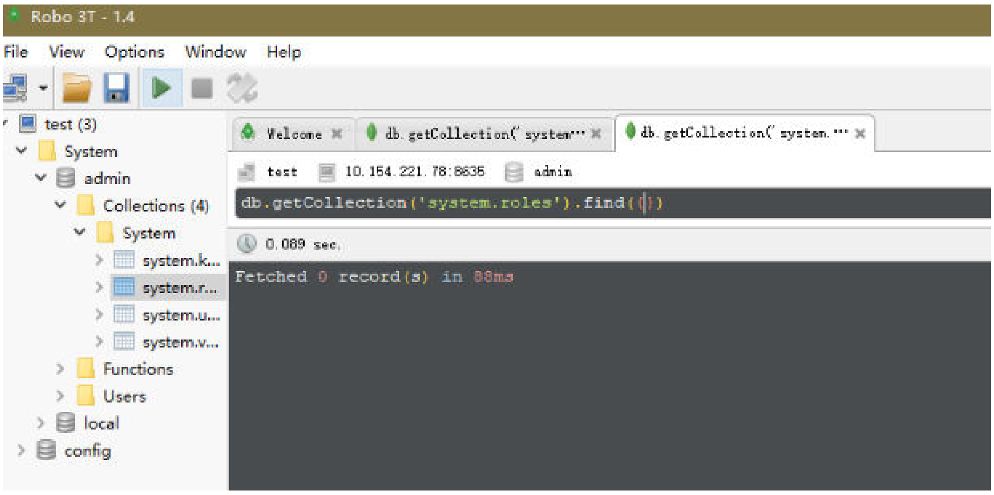


Create, edit, remove, clone or reorder connections via drag'n' drop.

Name	Address	Attributes	Auth. Database / User
test	[redacted]:8635	TLS	admin / rwuser

Step 4 If the single node instance is successfully connected, the page shown in **Figure 4-34** is displayed.

Figure 4-34 Single node connected



```
db.getCollection('system.roles').find({})
```

```
0.089 sec.
Fetched 0 record(s) in 88ms
```

----End

4.1.5 Connecting to a Single Node Instance Using Program Code

4.1.5.1 Java

If you are connecting to an instance using Java, an SSL certificate is optional, but downloading an SSL certificate and encrypting the connection will improve the security of your instance. SSL is disabled by default for newly created DB instances. You can enable SSL by referring to **Enabling or Disabling SSL**. SSL encrypts connections to databases but it increases the connection response time and CPU usage. Therefore, you are advised not to enable SSL.

Prerequisites

Familiarize yourself with:

- Computer basics
- Java code

Obtaining and Using Java

- Download the Jar driver from: **https://repo1.maven.org/maven2/org/mongodb/mongo-java-driver/3.0.4/**
- To view the usage guide, visit **https://mongodb.github.io/mongo-java-driver/4.2/driver/getting-started/installation/**.

Using an SSL Certificate

NOTE

- Download the SSL certificate and verify the certificate before connecting to databases.
- On the **Instances** page, click the target DB instance name. In the **DB Information** area on the **Basic Information** page, click ⤓ in the **SSL** field to download the root certificate or certificate bundle.
- For details about how to set up an SSL connection, see the MongoDB Java Driver official document at **https://www.mongodb.com/docs/drivers/java/sync/current/fundamentals/connection/tls/#std-label-tls-ssl**.

Connect to a single node instance using Java. The format of the Java link is as follows:

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

Table 4-4 Parameter description

Parameter	Description
<username>	Current username.
<password>	Password for the current username
<instance_ip>	If you attempt to access the instance from an ECS, set *instance_ip* to the private IP address displayed on the **Basic Information** page of the instance to which you intend to connect.
	If you intend to access the instance through an EIP, set *instance_ip* to the EIP that has been bound to the instance.
<instance_port>	Database port displayed on the **Basic Information** page. Default value: **8635**
<database_name>	Name of the database to be connected.
authSource	Authentication user database. The value is **admin**.

Parameter	Description
ssl	Connection mode. **true** indicates that the SSL connection mode is used.

Use the keytool to configure the CA certificate. For details about the parameters, see **Table 4-5**.

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

Table 4-5 Parameter description

Parameter	Description
<path to certificate authority file>	Path for storing the SSL certificate.
<path to trust store>	Path for storing the truststore. Set this parameter as required, for example, **./trust/certs.keystore**.
<password>	Custom password.

Set the JVM system properties in the program to point to the correct truststore and keystore:

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

For details about the Java code, see the following example:

```
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)
                    .applyToSslSettings(builder -> builder.enabled(true))
                    .applyToSslSettings(builder -> builder.invalidHostNameAllowed(true))
                    .build();
            MongoClient mongoClient = MongoClients.create(settings);
            MongoDatabase database = mongoClient.getDatabase("admin");
            //Ping the database. If the operation fails, an exception occurs.
            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");
        }
    }
}
```

Connection Without the SSL Certificate

NOTE

You do not need to download the SSL certificate because certificate verification on the server is not required.

Connect a single node using Java. The Java link format is as follows:

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

Table 4-6 Parameter description

Parameter	Description
<username>	Current username.
<password>	Password for the current username
<instance_ip>	If you attempt to access the instance from an ECS, set *instance_ip* to the private IP address displayed on the **Basic Information** page of the instance to which you intend to connect.
	If you intend to access the instance through an EIP, set *instance_ip* to the EIP that has been bound to the instance.
<instance_port>	Database port displayed on the **Basic Information** page. Default value: **8635**
<database_name>	Name of the database to be connected.
authSource	Authentication user database. The value is **admin**.

Example script in 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)
                    .retryWrites(true)
                    .build();
            MongoClient mongoClient = MongoClients.create(settings);
            MongoDatabase database = mongoClient.getDatabase("admin");
            //Ping the database. If the operation fails, an exception occurs.
            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");
        }
    }
}
```

4.1.5.2 Python

This section describes how to connect to a single node instance using Python.

Prerequisites

1. To connect an ECS to an instance, the ECS must be able to communicate with the DDS instance. You can run the following command to connect to the IP address and port of the instance server to test the network connectivity.

   curl *ip:port*

   If the message **It looks like you are trying to access MongoDB over HTTP on the native driver port** is displayed, the network connectivity is normal.
2. Install Python and third-party installation package **pymongo** on the ECS. Pymongo 2.8 is recommended.
3. If SSL is enabled, you need to download the root certificate and upload it to the ECS.

Connection Code

- Enabling 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
```

- Disabling 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
```

NOTE

- The authentication database in the URL must be **admin**. That means setting **authSource** to **admin**.
- In SSL mode, you need to manually generate the trustStore file.
- The authentication database must be **admin**, and then switch to the service database.

5 Logging In to and Logging Out of the DDS Console

Prerequisites

You need to have an account on the cloud platform before you can use DDS

For the first time you use DDS, apply for an account at the official website. After the application is successful, your account has permissions to access the DDS service, as well as all other cloud services.

Logging In to the DDS Console

Step 1 Open **Huawei Cloud official website**

Step 2 Click **Console** on the upper right of the page. The Huawei Cloud management console login page is displayed.

Step 3 Enter account information as prompted and click **Log In**.

The login is successful.

Step 4 Click 📍 in the upper left corner and select a region and a project.

If you want to use computing and network resources exclusively, you need to **Enabling a DeC** and **Applying for DCC Resources**. After enabling a DeC, you can select the DeC region and project.

You will be additionally charged for using DeC.

Step 5 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

----End

Logging Out of the DDS Console

Step 1 On any page of the DDS console, click the username in the upper right corner.

Step 2 In the displayed dialog box, click **Log Out**.

----End

6 Example: Buying and Connecting to a DDS Instance

6.1 Connecting to a DB Instance Using Mongo Shell

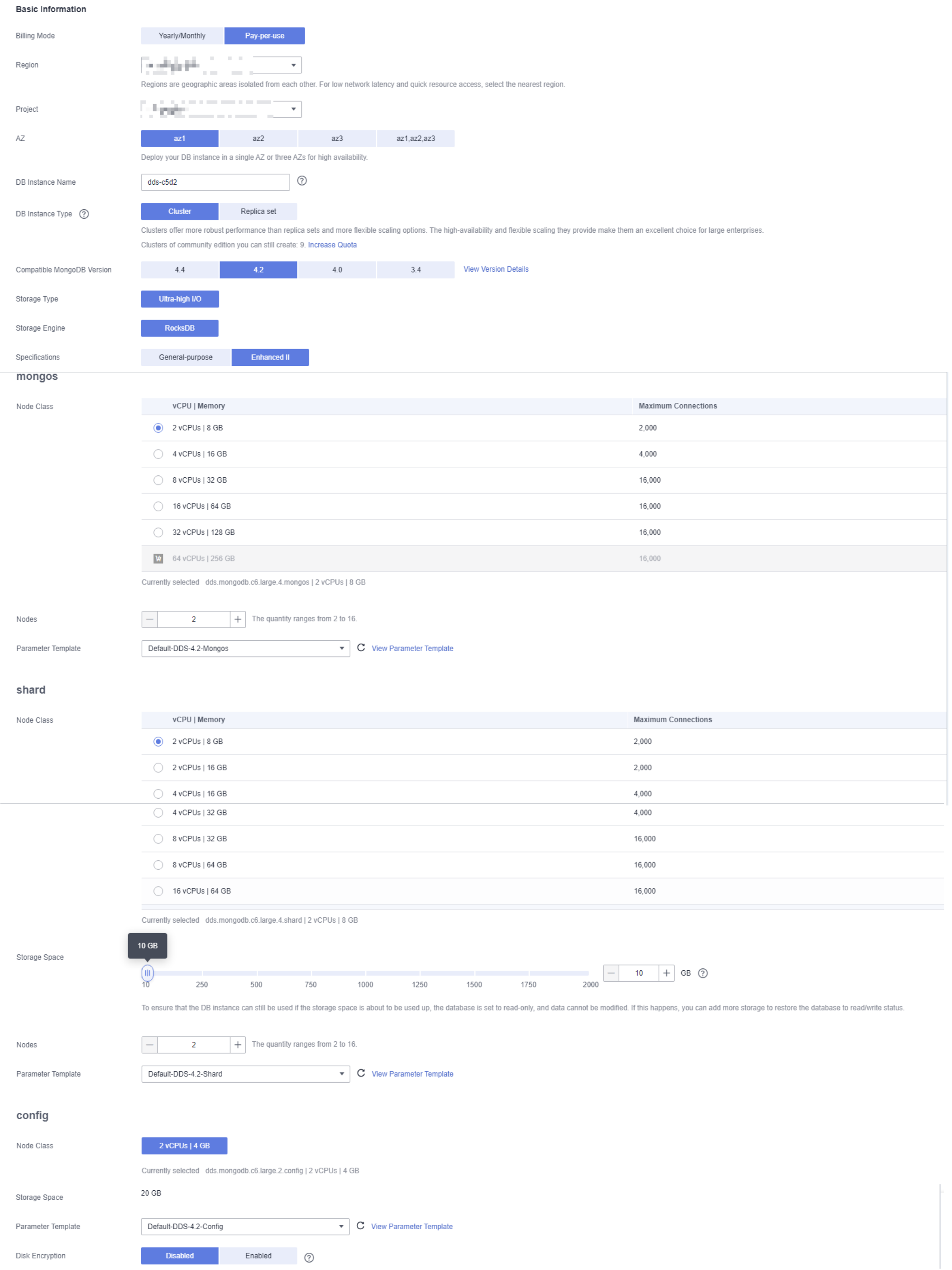
This section describes how to create a DB instance, use Mongo Shell to connect to the DB instance over a private network, and read data from and write data to the DB instance.

- **Step 1: Buy a DB Instance**
- **Step 2: Buy an ECS**
- **Step 3: Configure Security Group Rules**
- **Step 4: Connect to a DDS Cluster Instance Using Mongo Shell**
- **Step 5: Create a Database and Writing Data to the Database**

Step 1: Buy a DB Instance

1. Go to the **Custom Config** page.
2. On the displayed page, select a billing mode and configure information about your DB instance. Then, click **Next**.

Figure 6-1 Basic configurations



Basic Information

Billing Mode: Yearly/Monthly | **Pay-per-use**

Region: [redacted]

Regions are geographic areas isolated from each other. For low network latency and quick resource access, select the nearest region.

Project: [redacted]

AZ: **az1** | az2 | az3 | az1,az2,az3

Deploy your DB instance in a single AZ or three AZs for high availability.

DB Instance Name: dds-c5d2

DB Instance Type: **Cluster** | Replica set

Clusters offer more robust performance than replica sets and more flexible scaling options. The high-availability and flexible scaling they provide make them an excellent choice for large enterprises.

Clusters of community edition you can still create: 9. Increase Quota

Compatible MongoDB Version: 4.4 | **4.2** | 4.0 | 3.4 View Version Details

Storage Type: **Ultra-high I/O**

Storage Engine: **RocksDB**

Specifications: General-purpose | **Enhanced II**

mongos

Node Class

	vCPU | Memory	Maximum Connections
●	2 vCPUs | 8 GB	2,000
○	4 vCPUs | 16 GB	4,000
○	8 vCPUs | 32 GB	16,000
○	16 vCPUs | 64 GB	16,000
○	32 vCPUs | 128 GB	16,000
☒	64 vCPUs | 256 GB	16,000

Currently selected dds.mongodb.c6.large.4.mongos | 2 vCPUs | 8 GB

Nodes: 2 The quantity ranges from 2 to 16.

Parameter Template: Default-DDS-4.2-Mongos View Parameter Template

shard

Node Class

	vCPU | Memory	Maximum Connections
●	2 vCPUs | 8 GB	2,000
○	2 vCPUs | 16 GB	2,000
○	4 vCPUs | 16 GB	4,000
○	4 vCPUs | 32 GB	4,000
○	8 vCPUs | 32 GB	16,000
○	8 vCPUs | 64 GB	16,000
○	16 vCPUs | 64 GB	16,000

Currently selected dds.mongodb.c6.large.4.shard | 2 vCPUs | 8 GB

Storage Space: 10 GB

10 GB

To ensure that the DB instance can still be used if the storage space is about to be used up, the database is set to read-only, and data cannot be modified. If this happens, you can add more storage to restore the database to read/write status.

Nodes: 2 The quantity ranges from 2 to 16.

Parameter Template: Default-DDS-4.2-Shard View Parameter Template

config

Node Class: **2 vCPUs | 4 GB**

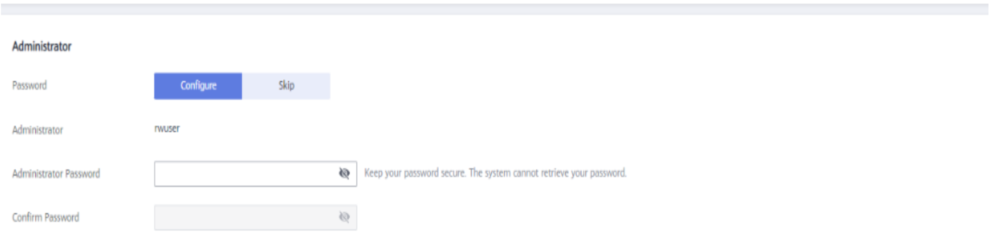
Currently selected dds.mongodb.c6.large.2.config | 2 vCPUs | 4 GB

Storage Space: 20 GB

Parameter Template: Default-DDS-4.2-Config View Parameter Template

Disk Encryption: **Disabled** | Enabled

Figure 6-2 Administrator settings



Administrator

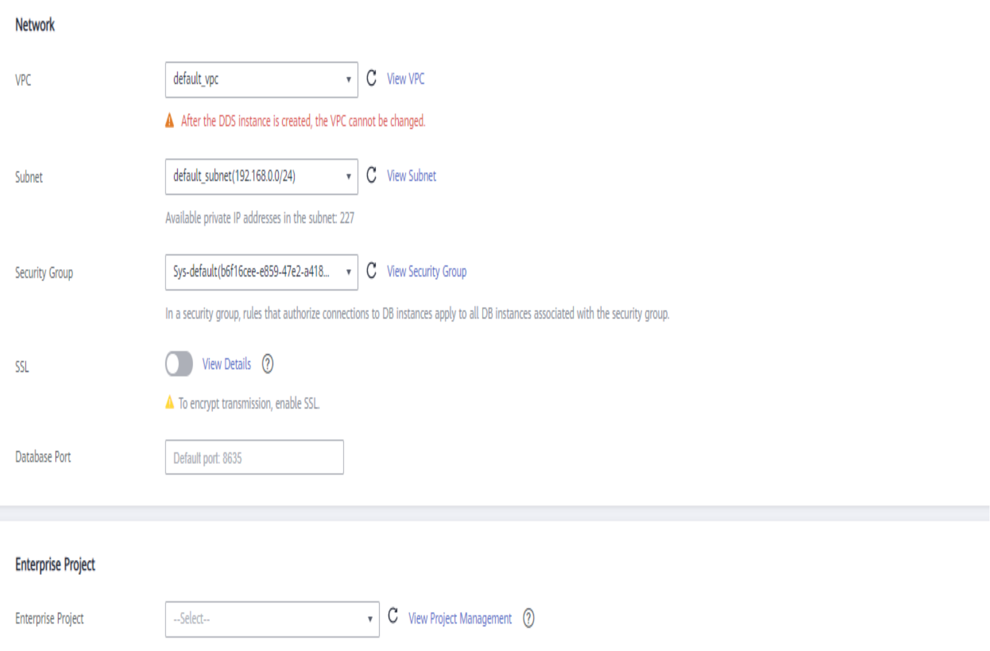
Password: **Configure** | Skip

Administrator: rwuser

Administrator Password: Keep your password secure. The system cannot retrieve your password.

Confirm Password:

Figure 6-3 Network and required duration



Network

VPC: default_vpc ▾ C View VPC

⚠ After the DDS instance is created, the VPC cannot be changed.

Subnet: default_subnet(192.168.0.0/24) ▾ C View Subnet

Available private IP addresses in the subnet: 227

Security Group: Sys-default(b6f16cee-e859-47e2-a418... ▾ C View Security Group

In a security group, rules that authorize connections to DB instances apply to all DB instances associated with the security group.

SSL: ○ View Details ?

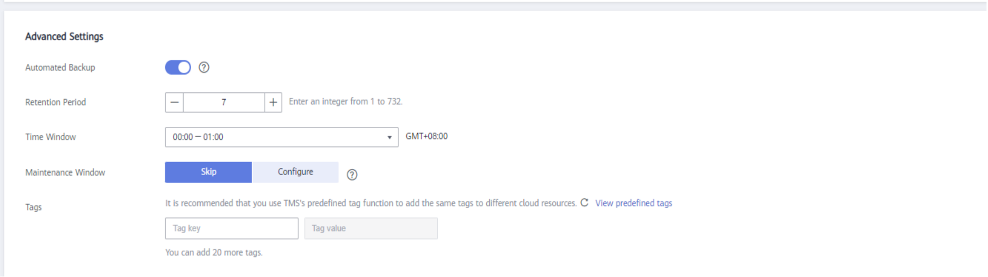
⚠ To encrypt transmission, enable SSL.

Database Port: Default port: 8635

Enterprise Project

Enterprise Project: --Select-- ▾ C View Project Management ?

Figure 6-4 Advanced settings



Advanced Settings

Automated Backup: ● ?

Retention Period: − 7 + Enter an integer from 1 to 732.

Time Window: 00:00 – 01:00 ▾ GMT+08:00

Maintenance Window: Skip | Configure ?

Tags: It is recommended that you use TMS's predefined tag function to add the same tags to different cloud resources. C View predefined tags

Tag key | Tag value

You can add 20 more tags.

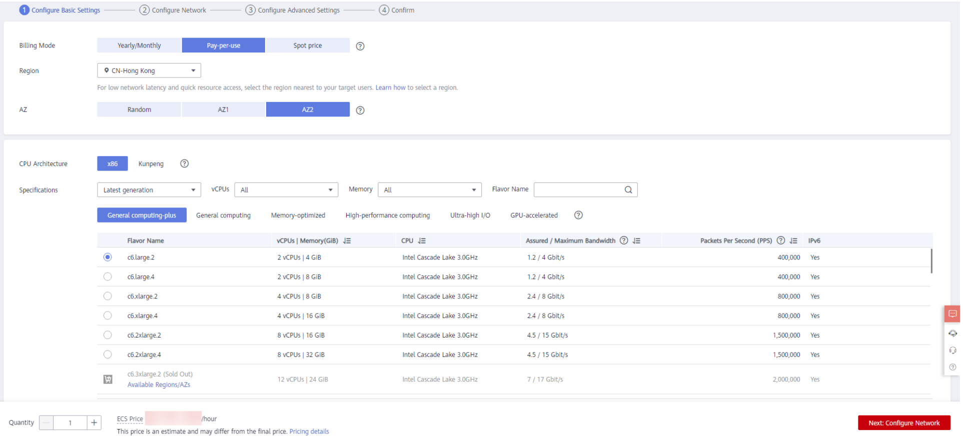
3. On the displayed page, confirm the instance details.
   - For yearly/monthly instances
     - If you need to modify the settings, click **Previous**.
     - If you do not need to modify the settings, read and agree to the service agreement and click **Pay Now** to go to the payment page and complete the payment.
   - For pay-per-use instances
     - If you need to modify the settings, click **Previous**.
     - If you do not need to modify the settings, read and agree to the service agreement and click **Submit** to start creating the instance.
4. Click **Back to Instance List**. Click **Back to Instance List**. You can view and manage the DB instance on the **Instances** page.
   - When a DB instance is being created, the status displayed in the **Status** column is **Creating**. This process takes about 15 minutes. After the creation is complete, the status changes to **Available**.

– Yearly/Monthly instances that were purchased in batches have the same specifications except for the instance name and ID.

Step 2: Buy an ECS

1. Go to the **Buy ECS** page.
2. Configure basic settings and click **Next: Configure Network**. Keep the region and AZ of the ECS the same as those of the DDS instance to be connected.

Figure 6-5 Basic configurations



① Configure Basic Settings ② Configure Network ③ Configure Advanced Settings ④ Confirm

Billing Mode: Yearly/Monthly [✓ Pay-per-use] Spot price

Region: CN-Hong Kong

For low network latency and quick resource access, select the region nearest to your target users. Learn how to select a region.

AZ: Random AZ1 [✓ AZ2]

CPU Architecture: [✓ x86] Kunpeng

Specifications: Latest generation; vCPUs: All; Memory: All; Flavor Name:

[✓ General computing-plus] General computing Memory-optimized High-performance computing Ultra-high I/O GPU-accelerated

	Flavor Name	vCPUs | Memory(GiB)	CPU	Assured / Maximum Bandwidth	Packets Per Second (PPS)	IPv6
●	c6.large.2	2 vCPUs | 4 GiB	Intel Cascade Lake 3.0GHz	1.2 / 4 Gbit/s	400,000	Yes
○	c6.large.4	2 vCPUs | 8 GiB	Intel Cascade Lake 3.0GHz	1.2 / 4 Gbit/s	400,000	Yes
○	c6.xlarge.2	4 vCPUs | 8 GiB	Intel Cascade Lake 3.0GHz	2.4 / 8 Gbit/s	800,000	Yes
○	c6.xlarge.4	4 vCPUs | 16 GiB	Intel Cascade Lake 3.0GHz	2.4 / 8 Gbit/s	800,000	Yes
○	c6.2xlarge.2	8 vCPUs | 16 GiB	Intel Cascade Lake 3.0GHz	4.5 / 15 Gbit/s	1,500,000	Yes
○	c6.2xlarge.4	8 vCPUs | 32 GiB	Intel Cascade Lake 3.0GHz	4.5 / 15 Gbit/s	1,500,000	Yes
	c6.3xlarge.2 (Sold Out) Available Regions/AZs	12 vCPUs | 24 GiB	Intel Cascade Lake 3.0GHz	7 / 17 Gbit/s	2,000,000	Yes

Quantity: 1 ECS Price [redacted]/hour

This price is an estimate and may differ from the final price. Pricing details

Next: Configure Network

Figure 6-6 Selecting an image

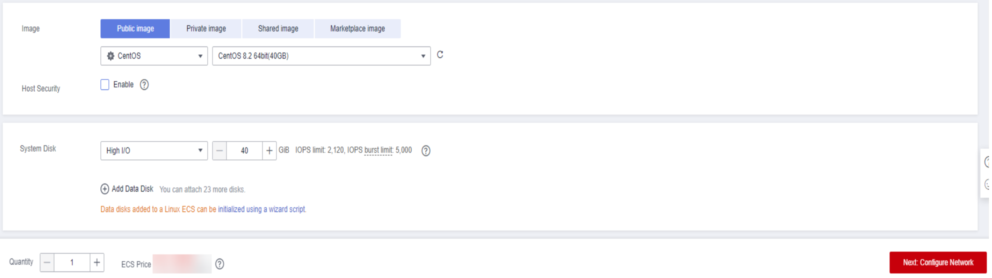


Image: [✓ Public image] Private image Shared image Marketplace image

CentOS; CentOS 8.2 64bit(40GB)

Host Security: □ Enable

System Disk: High I/O; 40 GiB IOPS limit: 2,120, IOPS burst limit: 5,000

Add Data Disk You can attach 23 more disks.

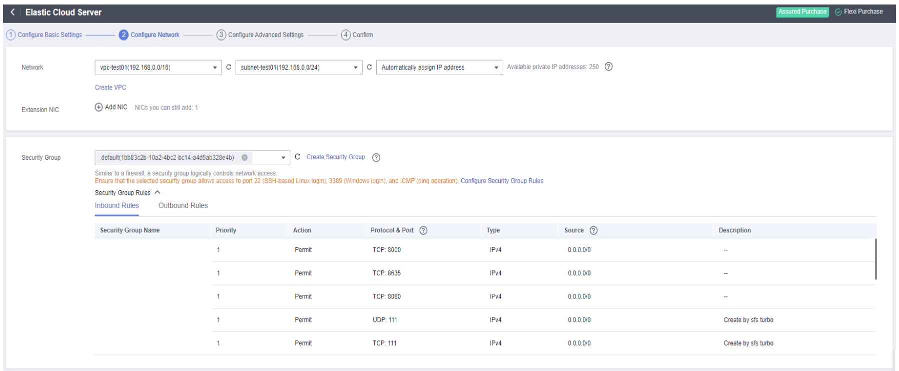
Data disks added to a Linux ECS can be initialized using a wizard script.

Quantity: 1 ECS Price [redacted]

Next: Configure Network

3. Configure the ECS network information and click **Next: Configure Advanced Settings**. Keep the VPC and security group of the ECS the same as those of the DDS instance to be connected.

Figure 6-7 Network settings



Elastic Cloud Server — Assured Purchase · Flexi Purchase

① Configure Basic Settings ② Configure Network ③ Configure Advanced Settings ④ Confirm

Network: vpc-test01(192.168.0.0/16); subnet-test01(192.168.0.0/24); Automatically assign IP address; Available private IP addresses: 250

Create VPC

Extension NIC: Add NIC NICs you can still add: 1

Security Group: default(1bb83c2b-10a2-4bc2-bc14-a4d5ab328e4b) Create Security Group

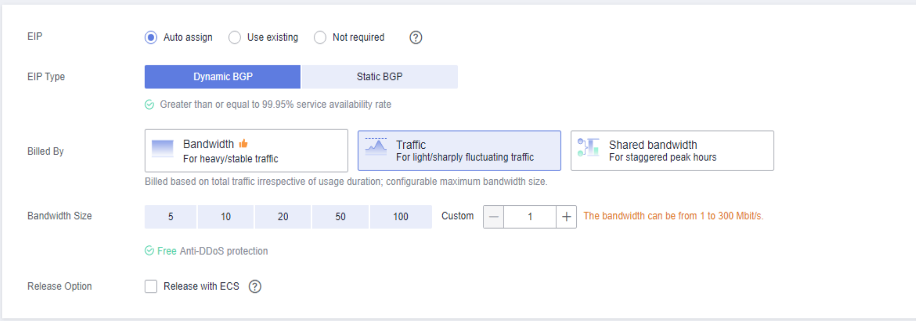
Similar to a firewall, a security group logically controls network access.
Ensure that the selected security group allows access to port 22 (SSH-based Linux login), 3389 (Windows login), and ICMP (ping operation). Configure Security Group Rules

Security Group Rules

[✓ Inbound Rules] Outbound Rules

Security Group Name	Priority	Action	Protocol & Port	Type	Source	Description
	1	Permit	TCP: 8000	IPv4	0.0.0.0/0	--
	1	Permit	TCP: 8635	IPv4	0.0.0.0/0	--
	1	Permit	TCP: 8080	IPv4	0.0.0.0/0	--
	1	Permit	UDP: 111	IPv4	0.0.0.0/0	Create by sfs turbo
	1	Permit	TCP: 111	IPv4	0.0.0.0/0	Create by sfs turbo

Figure 6-8 Selecting an EIP



EIP: ● Auto assign ○ Use existing ○ Not required

EIP Type: Dynamic BGP | Static BGP

Greater than or equal to 99.95% service availability rate

Billed By: Bandwidth – For heavy/stable traffic | Traffic – For light/sharply fluctuating traffic | Shared bandwidth – For staggered peak hours

Billed based on total traffic irrespective of usage duration; configurable maximum bandwidth size.

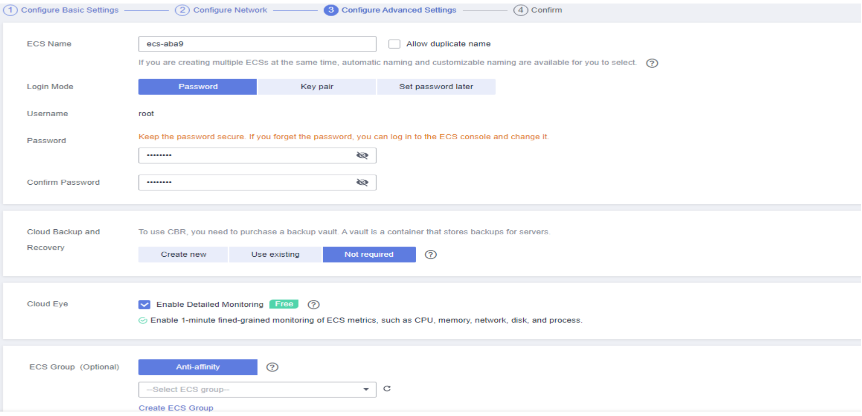
Bandwidth Size: 5 | 10 | 20 | 50 | 100 | Custom – 1 + The bandwidth can be from 1 to 300 Mbit/s.

Free Anti-DDoS protection

Release Option: □ Release with ECS

4. Configure the ECS password and click **Next: Confirm**.

Figure 6-9 Advanced settings



1 Configure Basic Settings — 2 Configure Network — 3 Configure Advanced Settings — 4 Confirm

ECS Name: ecs-aba9 □ Allow duplicate name

If you are creating multiple ECSs at the same time, automatic naming and customizable naming are available for you to select.

Login Mode: Password | Key pair | Set password later

Username: root

Password: Keep the password secure. If you forget the password, you can log in to the ECS console and change it.
•••••••••

Confirm Password: •••••••••

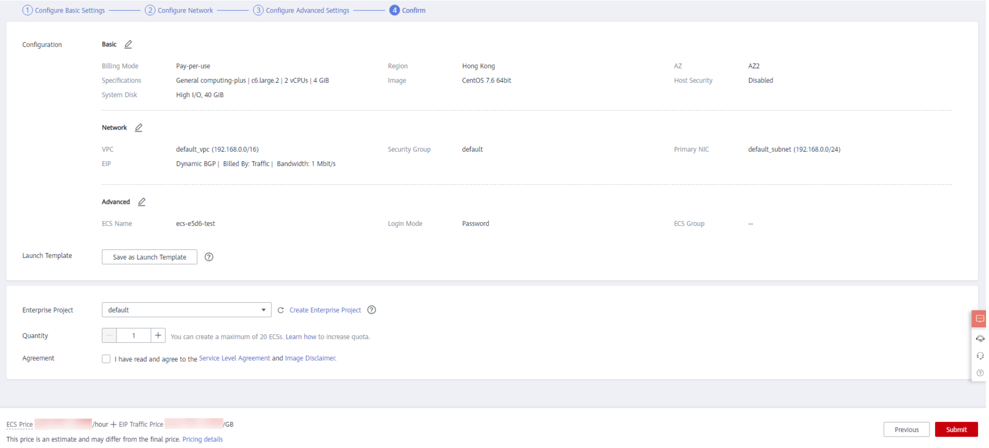
Cloud Backup and Recovery: To use CBR, you need to purchase a backup vault. A vault is a container that stores backups for servers.
Create new | Use existing | Not required

Cloud Eye: ☑ Enable Detailed Monitoring Free
Enable 1-minute fined-grained monitoring of ECS metrics, such as CPU, memory, network, disk, and process.

ECS Group (Optional): Anti-affinity
--Select ECS group--
Create ECS Group

5. Confirm the configurations and click **Submit**.

Figure 6-10 Confirming the configurations



1 Configure Basic Settings — 2 Configure Network — 3 Configure Advanced Settings — 4 Confirm

Configuration

Basic

Billing Mode	Pay-per-use	Region	Hong Kong	AZ	AZ2
Specifications	General computing-plus | c6.large.2 | 2 vCPUs | 4 GiB	Image	CentOS 7.6 64bit	Host Security	Disabled
System Disk	High I/O, 40 GiB				

Network

VPC	default_vpc (192.168.0.0/16)	Security Group	default	Primary NIC	default_subnet (192.168.0.0/24)
EIP	Dynamic BGP | Billed By: Traffic | Bandwidth: 1 Mbit/s				

Advanced

ECS Name	ecs-e5d6-test	Login Mode	Password	ECS Group	--

Launch Template: Save as Launch Template

Enterprise Project: default – Create Enterprise Project

Quantity: 1 You can create a maximum of 20 ECSs. Learn how to increase quota.

Agreement: □ I have read and agree to the Service Level Agreement and Image Disclaimer.

ECS Price [redacted]/hour + EIP Traffic Price [redacted]/GB

This price is an estimate and may differ from the final price. Pricing details

Previous | Submit

6. View the purchased ECS.

Step 3: Configure Security Group Rules

Step 1 Log in to the management console.

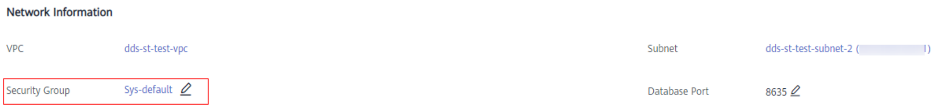
Step 2 Click ⊙ in the upper left corner and select a region and a project.

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the instance name. The **Basic Information** page is displayed.

Step 5 In the **Network Information** area on the **Basic Information** page, click the security group.

Figure 6-11 Security Group

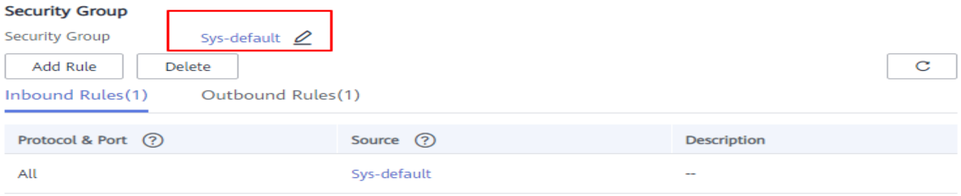


Network Information

VPC	dds-st-test-vpc	Subnet	dds-st-test-subnet-2 ([redacted])
Security Group	Sys-default	Database Port	8635

You can also choose **Connections** in the navigation pane on the left. On the **Private Connection** tab, in the **Security Group** area, click the security group name.

Figure 6-12 Security Group



Security Group

Security Group Sys-default

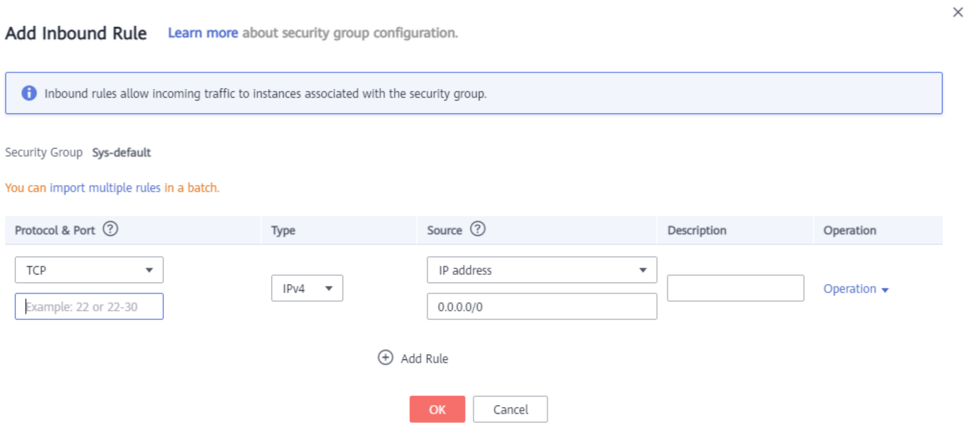
Protocol & Port	Source	Description
All	Sys-default	--

Step 6 On the **Security Group** page, locate the target security group and click **Manage Rule** in the **Operation** column.

Step 7 On the **Inbound Rules** tab, click **Add Rule**. The **Add Inbound Rule** dialog box is displayed.

Step 8 Add a security group rule as prompted.

Figure 6-13 Add Inbound Rule



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group Sys-default

You can import multiple rules in a batch.

Protocol & Port	Type	Source	Description	Operation
TCP Example: 22 or 22-30	IPv4	IP address 0.0.0.0/0		Operation

Table 6-1 Inbound rule settings

Parameter	Description	Example Value
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	The security group rule actions. Deny rules take precedence over allow rules of the same priority.	Allow
Protocol & Port	The network protocol required for access. Available options: **TCP**, **UDP**, **ICMP**, or **GRE**	TCP
	Port: the port on which you wish to allow access to DDS. The default port is 8635. The port ranges from 2100 to 9500 or can be 27017, 27018, or 27019.	8635
Type	IP address type. Only **IPv4** and **IPv6** are supported.	IPv4
Source	Specifies the supported IP address, security group, and IP address group, which allow access from IP addresses or instances in other security groups. Example: ● Single IP address: 192.168.10.10/32 ● IP address segment: 192.168.1.0/24 ● All IP addresses: 0.0.0.0/0 ● Security group: sg-abc ● IP address group: ipGroup-test If you enter a security group, all ECSs associated with the security group comply with the created rule. For more information about IP address groups, see **IP Address Group Overview**.	0.0.0.0/0
Description	(Optional) Provides supplementary information about the security group rule. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

Step 9 Click **OK**.

----End

Step 4: Connect to a DDS Cluster Instance Using Mongo Shell

- **SSL Connection**

Step 1 Log in to the management console.

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

Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.

Step 4 On the **Instances** page, click the instance name.

Step 5 In the navigation pane on the left, choose **Connections**.

Step 6 In the **Basic Information** area, click ⤓ next to the **SSL** field.

Step 7 Upload the root certificate to the ECS to be connected to the instance.

The following describes how to upload the certificate to a Linux and Window ECS:

- In Linux, run the following command:

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

  NOTE

  - **IDENTITY_FILE** is the directory where the root certificate resides. The file access permission is 600.
  - **REMOTE_USER** is the ECS OS user.
  - **REMOTE_ADDRESS** is the ECS address.
  - **REMOTE_DIR** is the directory of the ECS to which the root certificate is uploaded.
- In Windows, upload the root certificate using a remote connection tool.

Step 8 Connect to the instance in the directory where the MongoDB client is located.

Method 1: Using the private HA connection address (recommended)

DDS provides a private HA connection address that consists of IP addresses and ports of all dds mongos nodes in a cluster instance. You can use this address to connect to the cluster instance to improve availability of the cluster instance.

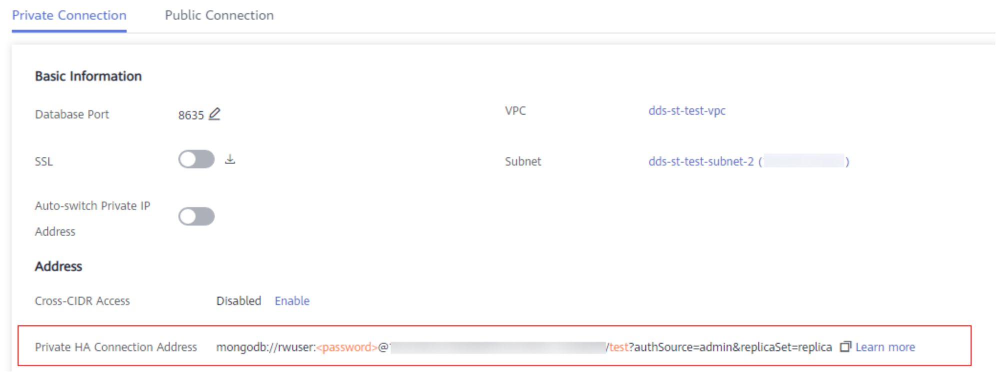
Command:

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

Parameter description:

- **Private HA Connection Address**: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 6-14 Obtaining the private HA connection address



Private Connection Public Connection

Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet-2 ([redacted])

Auto-switch Private IP Address

Address

Cross-CIDR Access Disabled Enable

Private HA Connection Address mongodb://rwuser:<password>@[redacted]/test?authSource=admin&replicaSet=replica Learn more

The format of the private HA connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

The following table lists the required parameters in the private HA address.

Table 6-2 Parameter information

Parameter	Description
rwuser	Database username
<password>	Password for the database username. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.
192.168.***.***:8635,192.168.***.***:8635	IP addresses and ports of the dds mongos nodes of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user **rwuser** must be **admin**. **authSource=admin** is fixed in the command.

- **FILE_PATH** is the path for storing the root certificate.
- **--sslAllowInvalidHostnames**: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and bandwidth, the cluster certificate is generated using the internal management IP address. **--sslAllowInvalidHostnames** is needed for the SSL connection through a private network.

Command example:

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

Method 2: Using the private HA connection address (user-defined database and account)

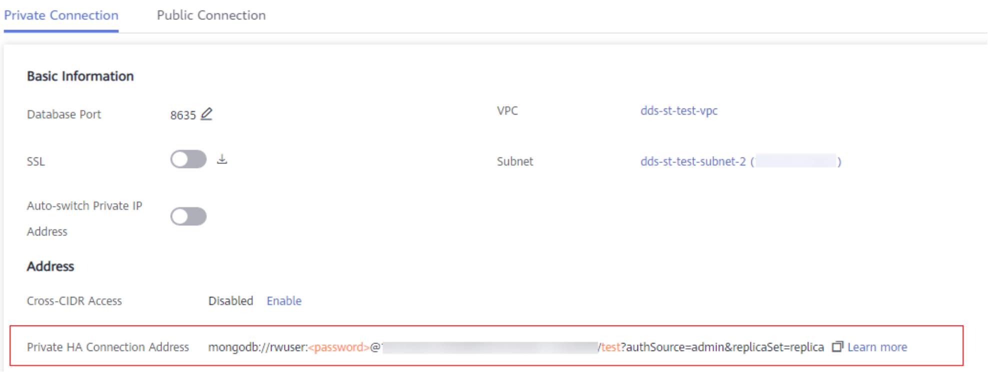
Command:

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

Parameter description:

- **Private HA Connection Address**: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 6-15 Obtaining the private HA connection address



Private Connection | Public Connection

Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet-2 ([redacted])

Auto-switch Private IP Address

Address

Cross-CIDR Access Disabled Enable

Private HA Connection Address mongodb://rwuser:<password>@[redacted]/test?authSource=admin&replicaSet=replica Learn more

The format of the obtained private HA connection address is as follows:

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

The following table lists the required parameters in the private HA address.

Table 6-3 Parameter information

Parameter	Description
rwuser	Database username. The default value is **rwuser**. You can change the value to the username based on your service requirements.

Parameter	Description
<password>	Password for the database username. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.
192.168.***.***:8635,192.168.***.***:8635	IP addresses and ports of the dds mongos nodes of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user **rwuser** is **admin**. **NOTE** If you use a user-defined database for authentication, change the authentication database in the HA connection address to the name of the user-defined database. In addition, replace **rwuser** with the username created in the user-defined database.

- **FILE_PATH** is the path for storing the root certificate.
- **--sslAllowInvalidHostnames**: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and bandwidth, the cluster certificate is generated using the internal management IP address. **--sslAllowInvalidHostnames** is needed for the SSL connection through a private network.

For example, if you create a user-defined database **Database** and user **test1** in the database, the connection command is as follows:

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

Method 3: Using a private IP address

Command:

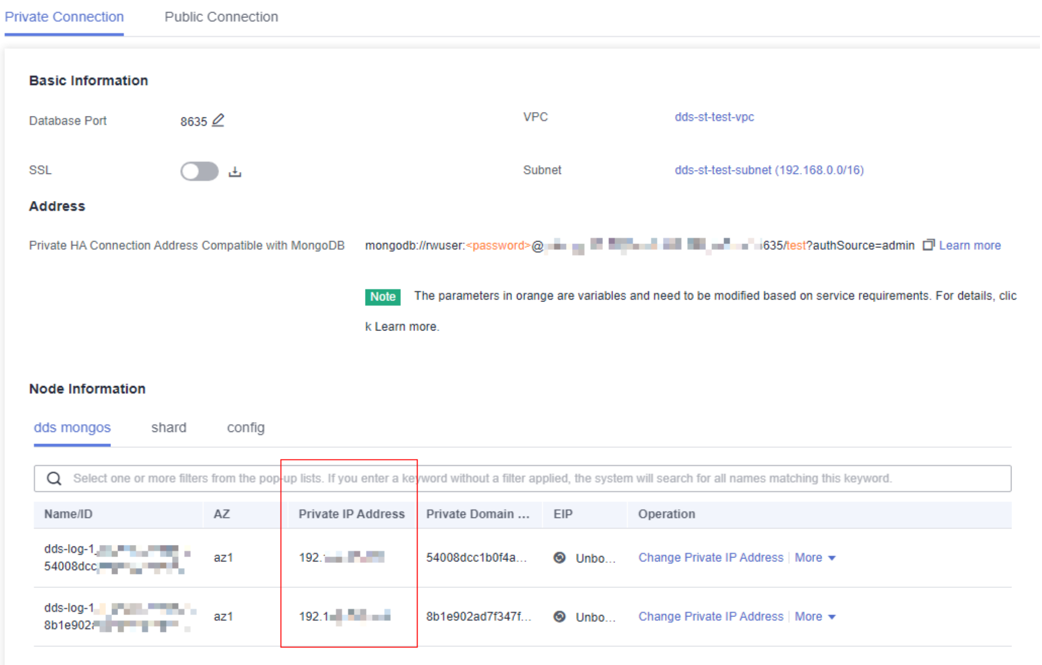
./mongo --host *<DB_HOST>* **--port** *<DB_PORT>* **-u** *<DB_USER>* **-p --authenticationDatabase admin --ssl --sslCAFile** *<FILE_PATH>* **--sslAllowInvalidHostnames**

Parameter description:

- **DB_HOST** is the IP address of the dds mongos node of the cluster instance to be connected.

Click the instance name. On the **Basic Information** page, choose **Connections** > **Private Connection**, obtain the private IP address of the dds mongos node on the **dds mongos** tab in the **Node Information** area.

Figure 6-16 Obtaining the private IP address



Basic Information

Database Port	8635	VPC	dds-st-test-vpc
SSL		Subnet	dds-st-test-subnet (192.168.0.0/16)

Address

Private HA Connection Address Compatible with MongoDB mongodb://rwuser:<password>@[redacted]635/test?authSource=admin Learn more

Note The parameters in orange are variables and need to be modified based on service requirements. For details, click Learn more.

Node Information

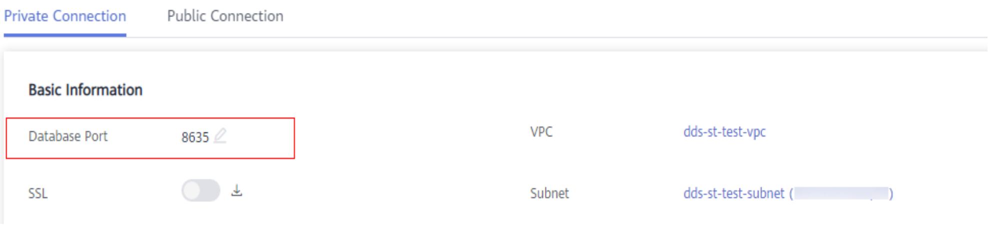
Select one or more filters from the pop-up lists. If you enter a keyword without a filter applied, the system will search for all names matching this keyword.

Name/ID	AZ	Private IP Address	Private Domain ...	EIP	Operation
dds-log-1[redacted] 54008dcc[redacted]	az1	192.[redacted]	54008dcc1b0f4a...	Unbo...	Change Private IP Address | More
dds-log-1[redacted] 8b1e902[redacted]	az1	192.1[redacted]	8b1e902ad7f347f...	Unbo...	Change Private IP Address | More

- **DB_PORT** is the port of the instance to be connected. The default port is 8635.

  Click the instance name. On the **Basic Information** page, choose **Connections**. On the **Private Connection** tab, obtain the database port information in the **Database Port** field in the **Basic Information** area.

  Figure 6-17 Obtaining the port

  Basic Information

Database Port	8635	VPC	dds-st-test-vpc
SSL		Subnet	dds-st-test-subnet ([redacted])

- **DB_USER** is the database user. The default value is **rwuser**.
- **FILE_PATH** is the path for storing the root certificate.
- **--sslAllowInvalidHostnames**: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and bandwidth, the cluster certificate is generated using the internal management IP address. **--sslAllowInvalidHostnames** is needed for the SSL connection through a private network.

Enter the password of the database account if the following information is prompted:

```
Enter password:
```

Command example:

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

Step 9 Check the connection result. If the following information is displayed, the connection is successful.

```
mongos>
```

----End

- **Unencrypted Connection**

Step 1 Connect to the ECS.

Step 2 Connect to the instance in the directory where the MongoDB client is located.

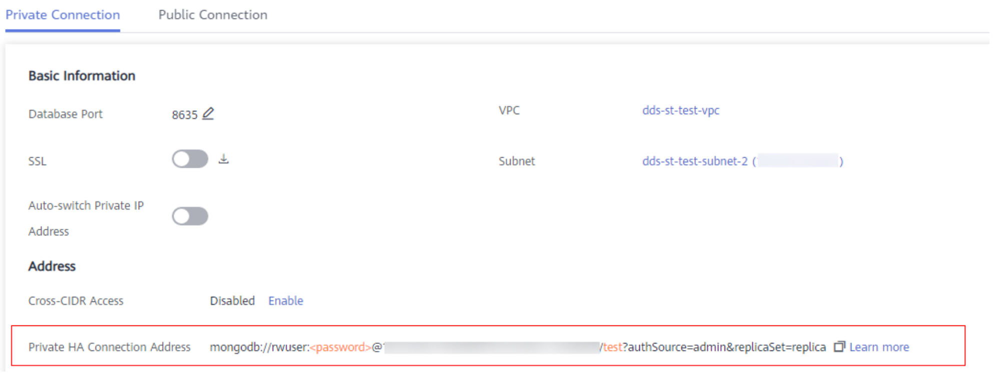
Method 1: Using the private HA connection address (recommended)

Command:

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

Private HA Connection Address: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 6-18 Obtaining the private HA connection address



Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet-2 ([redacted])

Auto-switch Private IP Address

Address

Cross-CIDR Access Disabled Enable

Private HA Connection Address mongodb://rwuser:<password>@[redacted]/test?authSource=admin&replicaSet=replica Learn more

The format of the private HA connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

The following table lists the required parameters in the private HA address.

Table 6-4 Parameter information

Parameter	Description
rwuser	Database username.

Parameter	Description
<password>	Password for the database username. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.
192.168.xx.xx:8635,192.168.xx.xx:8635	IP addresses and ports of the dds mongos nodes of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user **rwuser** must be **admin**. **authSource=admin** is fixed in the command.

Command example:

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

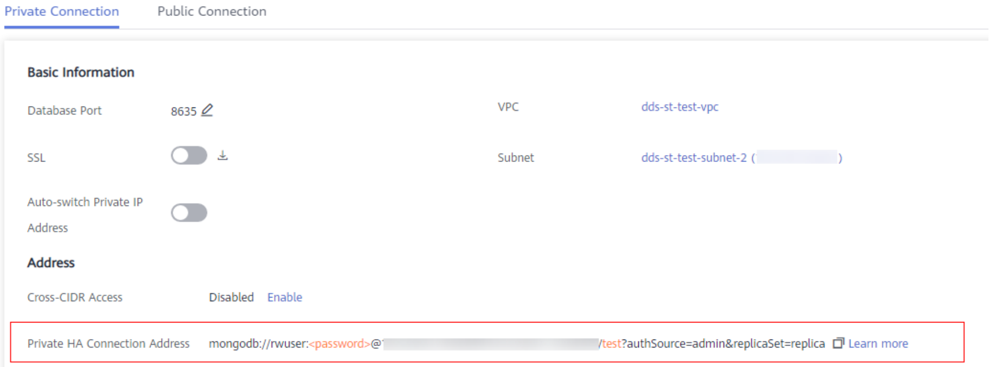
Method 2: Using the private HA connection address (user-defined database and account)

Command:

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

Private HA Connection Address: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 6-19 Obtaining the private HA connection address



Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet-2 ([redacted])

Auto-switch Private IP Address

Address

Cross-CIDR Access Disabled Enable

Private HA Connection Address mongodb://rwuser:<password>@[redacted]/test?authSource=admin&replicaSet=replica Learn more

The format of the obtained private HA connection address is as follows:

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

The following table lists the required parameters in the private HA address.

Table 6-5 Parameter information

Parameter	Description
rwuser	Database username. The default value is **rwuser**. You can change the value to the username based on your service requirements.
<password>	Password for the database username. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs ($), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ******@%***!$**, the corresponding URL code is ******%40%25***%21%24**.
192.168.xx.xx:8635,192.168.xx.xx:8635	IP addresses and ports of the dds mongos nodes of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user **rwuser** is **admin**. **NOTE** If you use a user-defined database for authentication, change the authentication database in the HA connection address to the name of the user-defined database. In addition, replace **rwuser** with the username created in the user-defined database.

For example, if you create a user-defined database **Database** and user **test1** in the database, the connection command is as follows:

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

Method 3: Using a private IP address

Command:

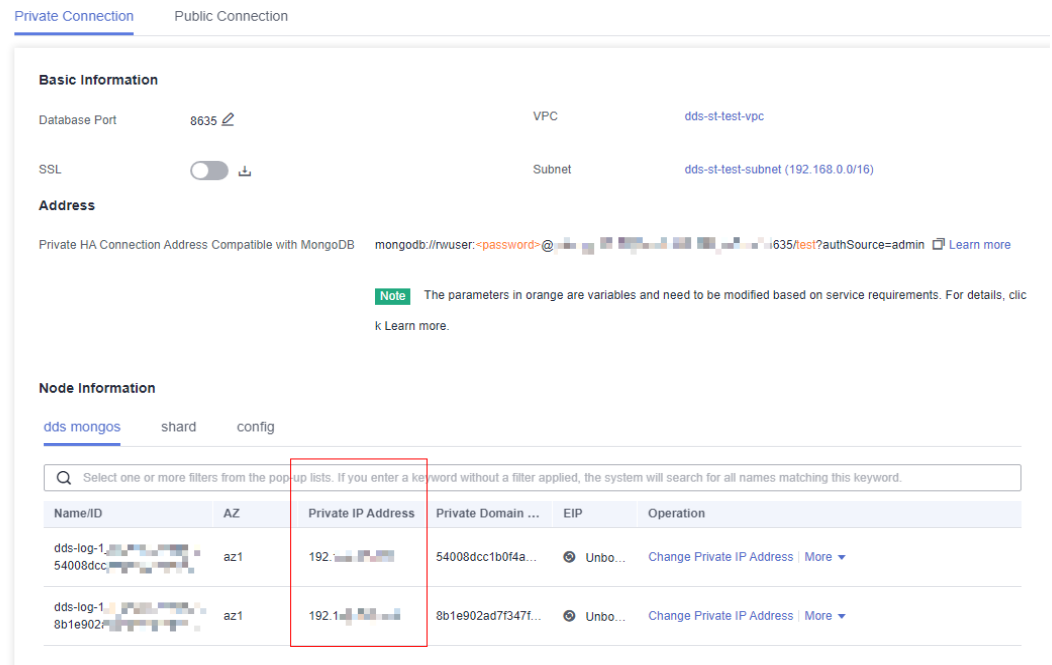
./mongo --host *<DB_HOST>* **--port** *<DB_PORT>* **-u** *<DB_USER>* **-p --authenticationDatabase admin**

Parameter description:

- **DB_HOST** is the IP address of the dds mongos node of the cluster instance to be connected.

Click the instance name. On the **Basic Information** page, choose **Connections** > **Private Connection**, obtain the private IP address of the dds mongos node on the **dds mongos** tab in the **Node Information** area.

Figure 6-20 Obtaining the private IP address



Private Connection | Public Connection

Basic Information

Database Port 8635

VPC dds-st-test-vpc

SSL

Subnet dds-st-test-subnet (192.168.0.0/16)

Address

Private HA Connection Address Compatible with MongoDB mongodb://rwuser:<password>@[redacted]635/test?authSource=admin Learn more

Note The parameters in orange are variables and need to be modified based on service requirements. For details, click Learn more.

Node Information

dds mongos | shard | config

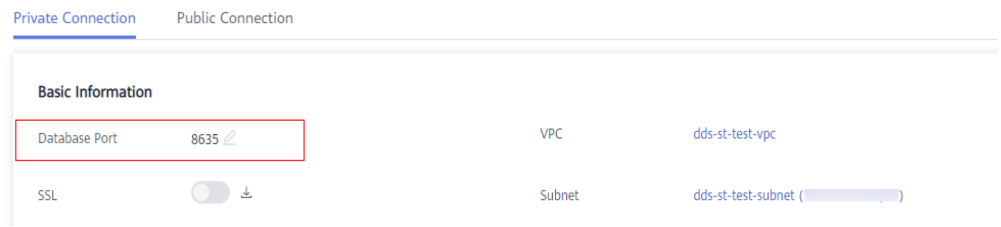
Select one or more filters from the pop-up lists. If you enter a keyword without a filter applied, the system will search for all names matching this keyword.

Name/ID	AZ	Private IP Address	Private Domain ...	EIP	Operation
dds-log-1[redacted] 54008dcc[redacted]	az1	192.[redacted]	54008dcc1b0f4a...	Unbo...	Change Private IP Address | More
dds-log-1[redacted] 8b1e902[redacted]	az1	192.1[redacted]	8b1e902ad7f347f...	Unbo...	Change Private IP Address | More

- **DB_PORT** is the port of the instance to be connected. The default port is 8635.

  Click the instance name. On the **Basic Information** page, choose **Connections**. On the **Private Connection** tab, obtain the database port information in the **Database Port** field in the **Basic Information** area.

  Figure 6-21 Obtaining the port

  Private Connection | Public Connection

  Basic Information

  Database Port 8635

  VPC dds-st-test-vpc

  SSL

  Subnet dds-st-test-subnet ([redacted])

- **DB_USER** is the database user. The default value is **rwuser**.

Enter the password of the database account if the following information is prompted:

```
Enter password:
```

Command example:

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

Step 3 Check the connection result. If the following information is displayed, the connection is successful.

```
mongos>
```

----End

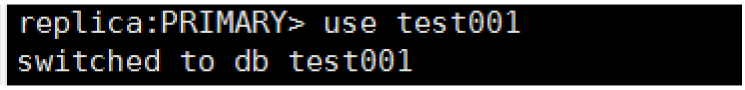
Step 5: Create a Database and Writing Data to the Database

Step 1 Create a database.

use *dbname*

dbname: indicates the name of the database to be created.

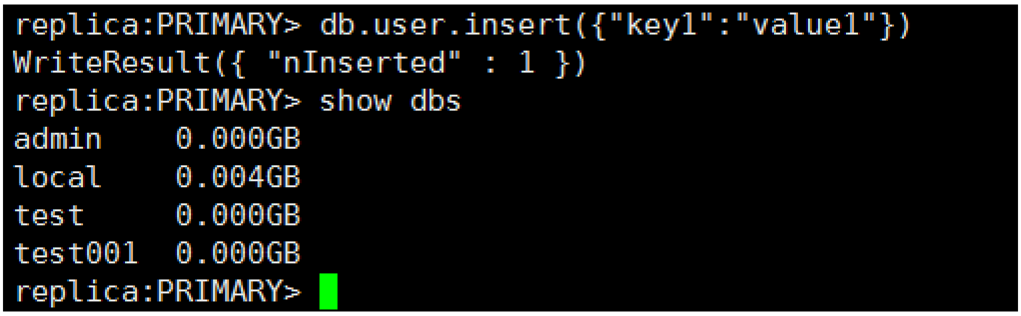
Figure 6-22 Creating a database



```
replica:PRIMARY> use test001
switched to db test001
```

Step 2 After a database is created, insert data into the database so that you can view the database in the database list.

Figure 6-23 Inserting data

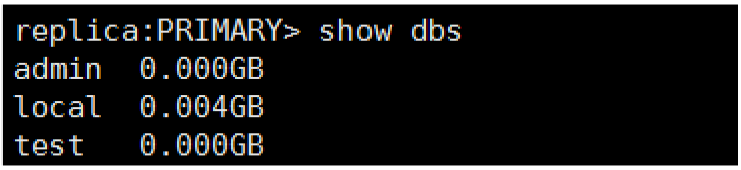


```
replica:PRIMARY> db.user.insert({"key1":"value1"})
WriteResult({ "nInserted" : 1 })
replica:PRIMARY> show dbs
admin    0.000GB
local    0.004GB
test     0.000GB
test001  0.000GB
replica:PRIMARY> 
```

NOTE

There are three system databases created by default: **admin**, **local**, and **test**. If you directly insert data without creating a database, the data is inserted to the **test** database by default.

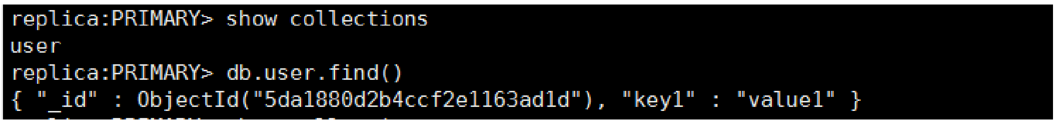
Figure 6-24 Viewing the database



```
replica:PRIMARY> show dbs
admin  0.000GB
local  0.004GB
test   0.000GB
```

Step 3 View data in the database.

Figure 6-25 Viewing data



```
replica:PRIMARY> show collections
user
replica:PRIMARY> db.user.find()
{ "_id" : ObjectId("5da1880d2b4ccf2e1163ad1d"), "key1" : "value1" }
```

----End

6.2 Connecting to a DDS Instance Through an EIP

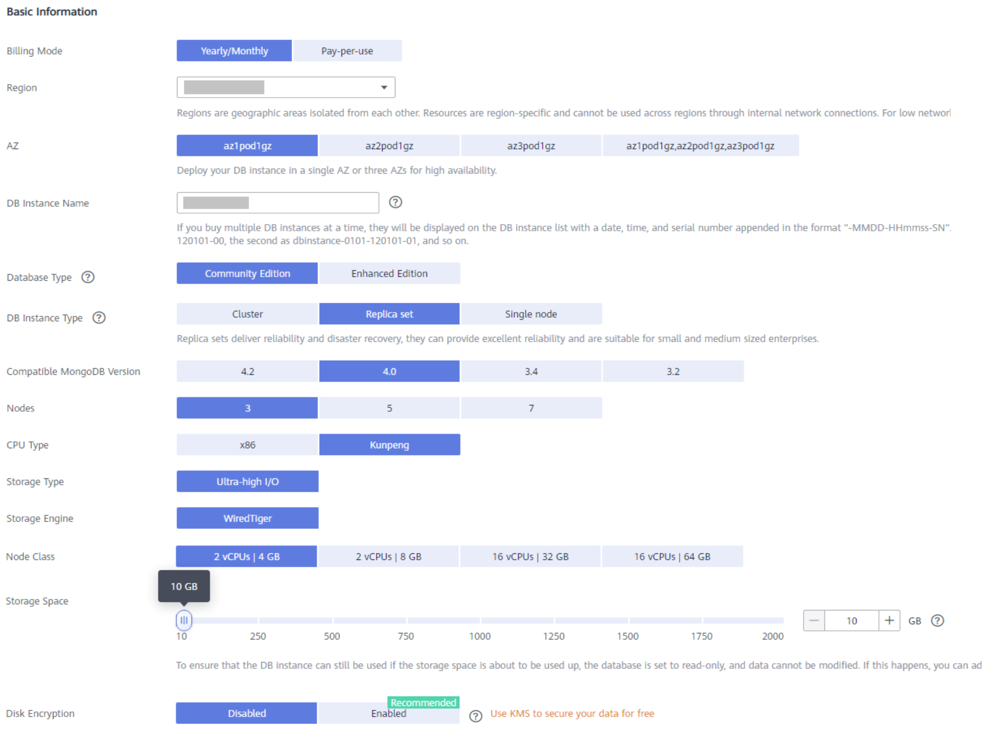
This section uses a DDS replica set instance and Windows operating system as an example to describe how to buy a DDS instance, bind an EIP, set a security group, and connect to the DDS instance using the Robo 3T tool in your local environment. The procedures are as follows:

- Step 1: Buy a DB Instance
- Step 2: Bind an EIP
- Step 3: Configure a Security Group
- Step 4: Connect to a DDS Instance

Step 1: Buy a DB Instance

1. Go to the **Custom Config** page.
2. On the displayed page, select a billing mode and configure information about your DB instance. Then, click **Next**.

Figure 6-26 Basic configurations



Basic Information

Billing Mode: [✓ Yearly/Monthly] Pay-per-use

Region: [redacted]

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low networ

AZ: [✓ az1pod1gz] az2pod1gz az3pod1gz az1pod1gz,az2pod1gz,az3pod1gz

Deploy your DB instance in a single AZ or three AZs for high availability.

DB Instance Name: [redacted]

If you buy multiple DB instances at a time, they will be displayed on the DB instance list with a date, time, and serial number appended in the format "-MMDD-HHmmss-SN". 120101-00, the second as dbinstance-0101-120101-01, and so on.

Database Type: [✓ Community Edition] Enhanced Edition

DB Instance Type: Cluster [✓ Replica set] Single node

Replica sets deliver reliability and disaster recovery, they can provide excellent reliability and are suitable for small and medium sized enterprises.

Compatible MongoDB Version: 4.2 [✓ 4.0] 3.4 3.2

Nodes: [✓ 3] 5 7

CPU Type: x86 [✓ Kunpeng]

Storage Type: [✓ Ultra-high I/O]

Storage Engine: [✓ WiredTiger]

Node Class: [✓ 2 vCPUs | 4 GB] 2 vCPUs | 8 GB 16 vCPUs | 32 GB 16 vCPUs | 64 GB

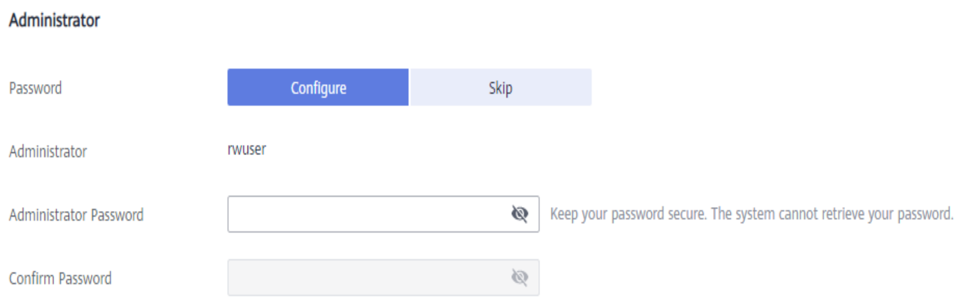
Storage Space: 10 GB

To ensure that the DB instance can still be used if the storage space is about to be used up, the database is set to read-only, and data cannot be modified. If this happens, you can ad

Disk Encryption: [✓ Disabled] Enabled Recommended

Use KMS to secure your data for free

Figure 6-27 Administrator settings



Administrator

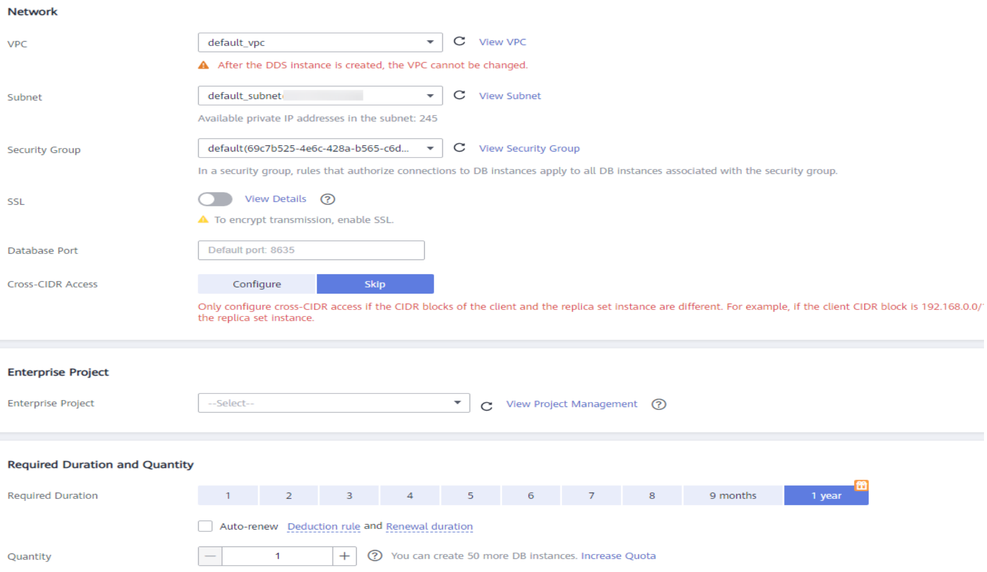
Password: Configure | Skip

Administrator: rwuser

Administrator Password: Keep your password secure. The system cannot retrieve your password.

Confirm Password

Figure 6-28 Network, Required Duration, and Quantity



Network

VPC: default_vpc — View VPC

After the DDS instance is created, the VPC cannot be changed.

Subnet: default_subnet[redacted] — View Subnet

Available private IP addresses in the subnet: 245

Security Group: default(69c7b525-4e6c-428a-b565-c6d... — View Security Group

In a security group, rules that authorize connections to DB instances apply to all DB instances associated with the security group.

SSL: View Details

To encrypt transmission, enable SSL.

Database Port: Default port: 8635

Cross-CIDR Access: Configure | Skip

Only configure cross-CIDR access if the CIDR blocks of the client and the replica set instance are different. For example, if the client CIDR block is 192.168.0.0/
the replica set instance.

Enterprise Project

Enterprise Project: --Select-- — View Project Management

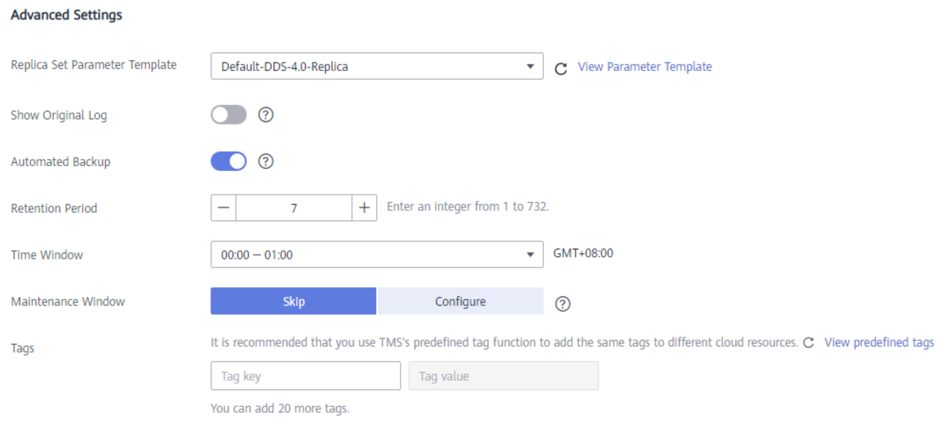
Required Duration and Quantity

Required Duration: 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 months | 1 year

□ Auto-renew Deduction rule and Renewal duration

Quantity: 1 — You can create 50 more DB instances. Increase Quota

Figure 6-29 Advanced settings



Advanced Settings

Replica Set Parameter Template: Default-DDS-4.0-Replica — View Parameter Template

Show Original Log

Automated Backup

Retention Period: 7 — Enter an integer from 1 to 732.

Time Window: 00:00 – 01:00 GMT+08:00

Maintenance Window: Skip | Configure

Tags: It is recommended that you use TMS's predefined tag function to add the same tags to different cloud resources. View predefined tags

Tag key | Tag value

You can add 20 more tags.

3. On the displayed page, confirm the instance details.
   - For yearly/monthly instances
     - If you need to modify the specifications, click **Previous** to return to the previous page.

        - If you do not need to modify the specifications, read and agree to the service agreement and click **Pay Now** to go to the payment page and complete payment.
    - For pay-per-use instances
        - If you need to modify the specifications, click **Previous** to return to the previous page.
        - If you do not need to modify the specifications, read and agree to the service agreement and click **Submit** to start creating the instance.

4. Click **Back to Instance List**. After a DDS instance is created, you can view and manage it on the **Instances** page.
    - When an instance is being created, the status displayed in the **Status** column is **Creating**. This process takes about 15 minutes. After the creation is complete, the status changes to **Available**.
    - Yearly/Monthly instances that were purchased in batches have the same specifications except for the instance name and ID.

Step 2: Bind an EIP

1. Log in to the **management console**.
2. Click 📍 in the upper left corner and select a region and a project.
3. Click ☰ in the upper left corner of the page and choose **Databases** > **Document Database Service**.
4. On the **Instances** page, click the instance. The **Basic Information** page is displayed.
5. In the **Node Information** area, locate the row that contains the primary node and click **Bind EIP**.
6. In the displayed dialog box, select the purchased EIP and click **OK**.
7. After the binding is successful, view the EIP in the **Node Information** area.

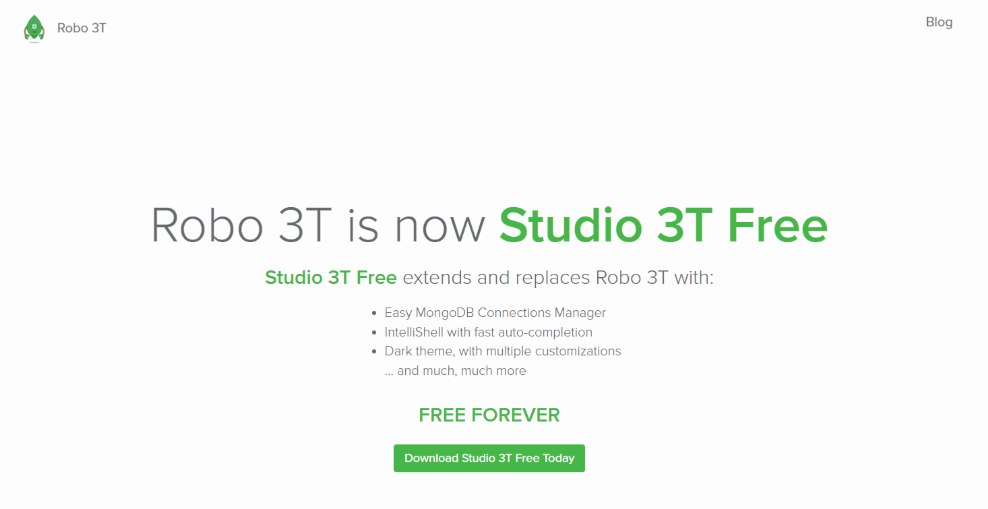
Step 3: Configure a Security Group

1. In the **Network Information** area on the **Basic Information** page, check the database port of the DB instance.
2. In the **Network Information** area, click the security group name.
3. On the **Security Groups** page, click the security group name.
4. Click the **Inbound Rules** tab and click **Add Rule**. In the displayed dialog box, add an inbound rule for the database port.

Step 4: Connect to a DDS Instance

1. Access the Robo 3T download address **https://robomongo.org/download** and click **Download Studio 3T Free Today**.

Figure 6-30 Downloading page



Robo 3T is now Studio 3T Free

Studio 3T Free extends and replaces Robo 3T with:

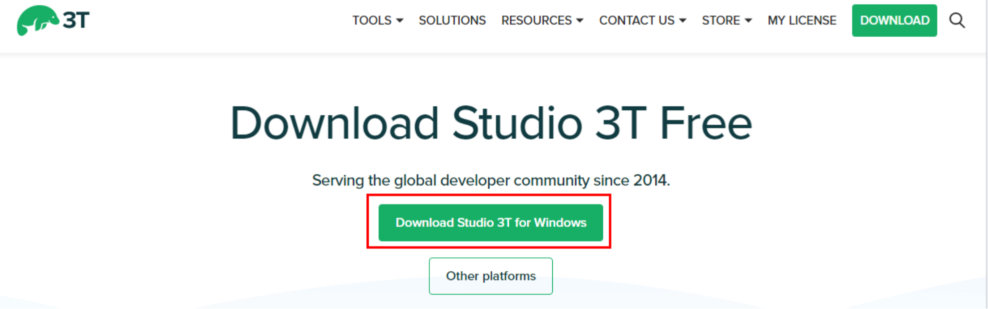
- Easy MongoDB Connections Manager
- IntelliShell with fast auto-completion
- Dark theme, with multiple customizations

... and much, much more

FREE FOREVER

2. In the displayed dialog box, enter required information and click **Download Studio 3T for Windows** to download **studio-3t-x64.zip**.

Figure 6-31 Downloading Robo 3T

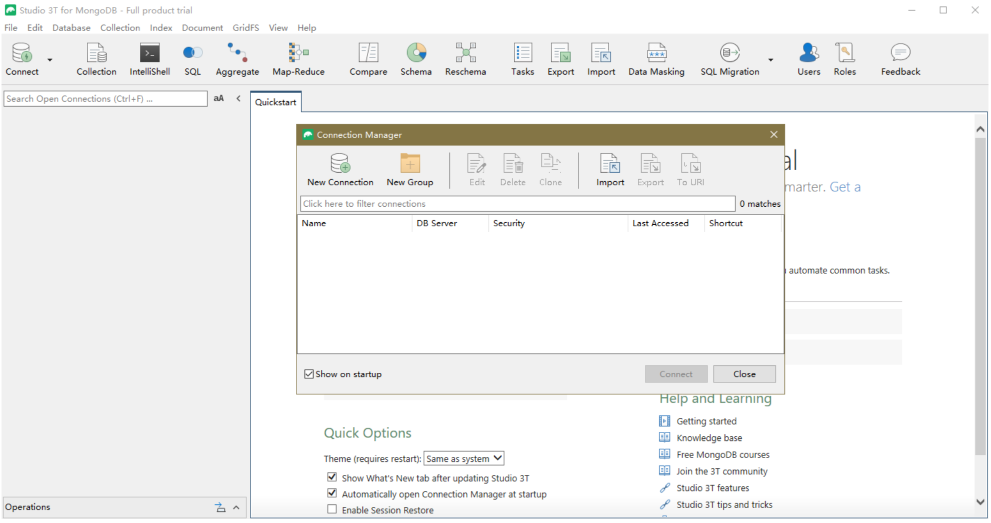


Download Studio 3T Free

Serving the global developer community since 2014.

3. Decompress the downloaded package and double-click the **studio-3t-x64.exe** file in the decompressed directory to start the installation.
4. After the installation is complete, start the tool, as shown in **Figure 6-32**.

Figure 6-32 Main window



Name	DB Server	Security	Last Accessed	Shortcut

☑ Show on startup

Quick Options

Theme (requires restart): Same as system

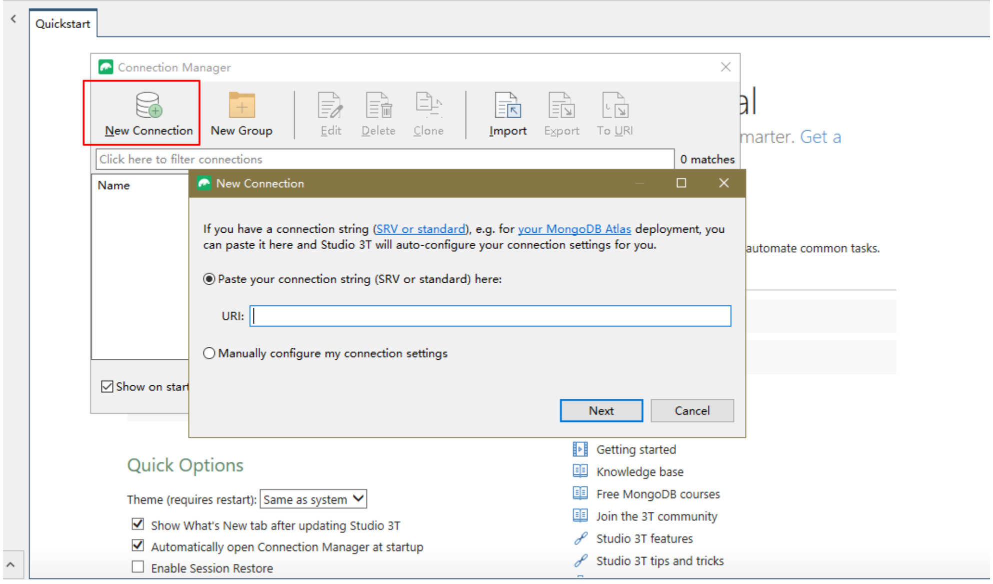
☑ Show What's New tab after updating Studio 3T

☑ Automatically open Connection Manager at startup

☐ Enable Session Restore

5. On the **Connection Manager** page, click **New Connection**.

Figure 6-33 Connection manager



New Connection

If you have a connection string (SRV or standard), e.g. for your MongoDB Atlas deployment, you can paste it here and Studio 3T will auto-configure your connection settings for you.

● Paste your connection string (SRV or standard) here:

URI:

○ Manually configure my connection settings

Theme (requires restart): Same as system

☑ Show What's New tab after updating Studio 3T

☑ Automatically open Connection Manager at startup

□ Enable Session Restore

6. Connect to a DB instance **automatically** or **manually**.

   – Method 1: Connect to a DB instance automatically.

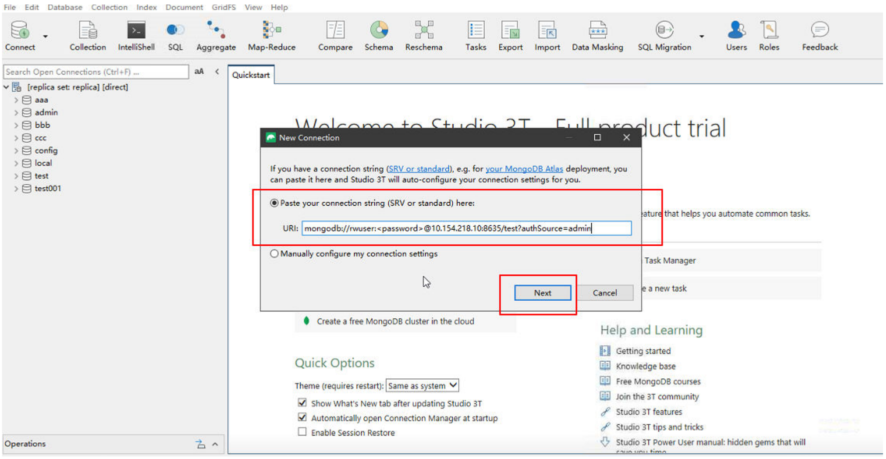
     i. In the dialog box that is displayed, enter the URI, replace **<password>**, and click **Next**.

        NOTE

        How to obtain the URI:

        On the **Instances** page, click the target DB instance name. On the **Basic Information** page, click **Connections**. In the **Public Connection** area, obtain the public connection address from **Address**.

Figure 6-34 Entering the URI



New Connection

If you have a connection string (SRV or standard), e.g. for your MongoDB Atlas deployment, you can paste it here and Studio 3T will auto-configure your connection settings for you.

● Paste your connection string (SRV or standard) here:

URI: mongodb://rwuser:<password>@10.154.218.10:8635/test?authSource=admin

○ Manually configure my connection settings

Theme (requires restart): Same as system

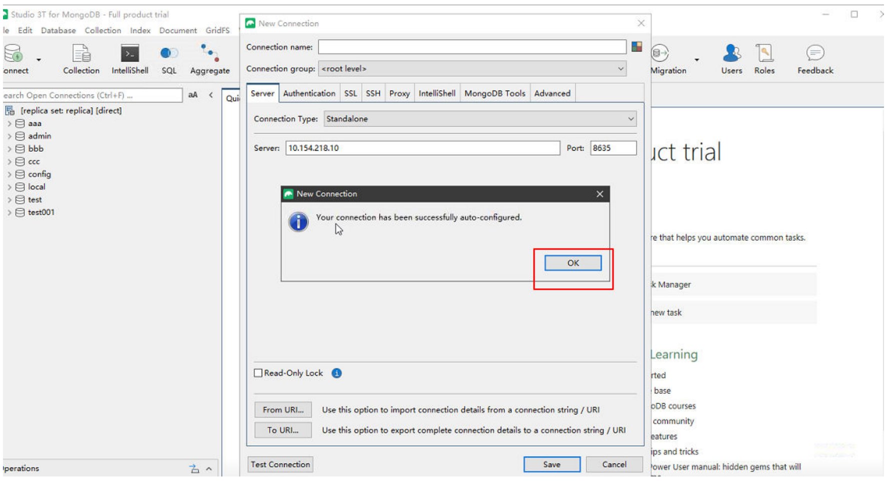
☑ Show What's New tab after updating Studio 3T

☑ Automatically open Connection Manager at startup

□ Enable Session Restore

     ii. On the **Server** tab, click **OK** in the displayed dialog box.

Figure 6-35 Server



Connection Type: Standalone

Server: 10.154.218.10 Port: 8635

New Connection

Your connection has been successfully auto-configured.

OK

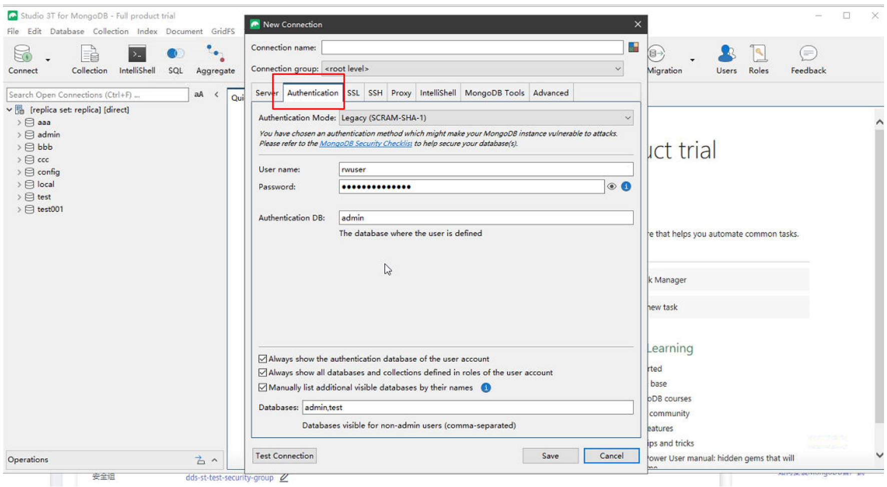
☐ Read-Only Lock

From URI... Use this option to import connection details from a connection string / URI

To URI... Use this option to export complete connection details to a connection string / URI

iii. Click the **Authentication** tab.

Figure 6-36 Authentication



Authentication Mode: Legacy (SCRAM-SHA-1)

You have chosen an authentication method which might make your MongoDB instance vulnerable to attacks. Please refer to the MongoDB Security Checklist to help secure your database(s).

User name: rwuser

Password: ••••••••••••••

Authentication DB: admin

The database where the user is defined

☑ Always show the authentication database of the user account

☑ Always show all databases and collections defined in roles of the user account

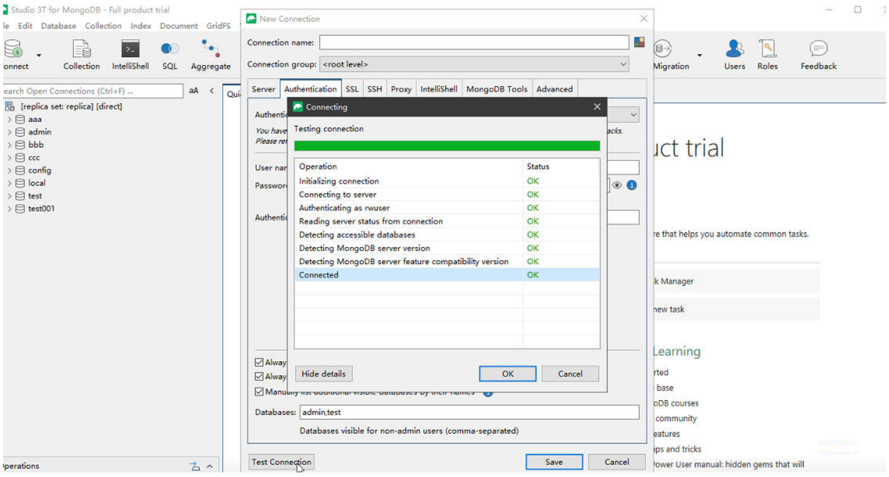
☑ Manually list additional visible databases by their names

Databases: admin,test

Databases visible for non-admin users (comma-separated)

iv. Click **Test Connection** to check whether the connection is successful.

Figure 6-37 Test Connection



Connecting

Testing connection

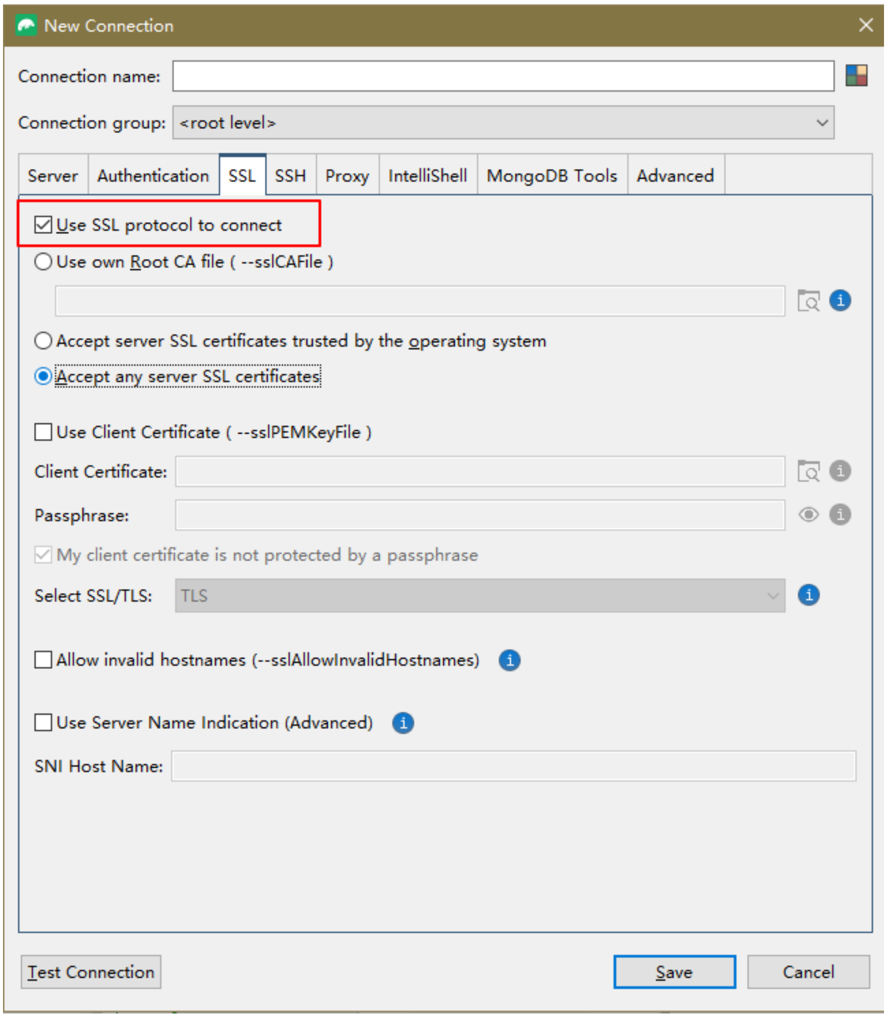
Operation	Status
Initializing connection	OK
Connecting to server	OK
Authenticating as rwuser	OK
Reading server status from connection	OK
Detecting accessible databases	OK
Detecting MongoDB server version	OK
Detecting MongoDB server feature compatibility version	OK
Connected	OK

v. Click the **SSL** tab and select **Use SSL protocol to connect**.

NOTE

If SSL data encryption is disabled, skip this step and go to **6.viii**.

Figure 6-38 SSL



Connection name:

Connection group: <root level>

☑ Use SSL protocol to connect

○ Use own Root CA file (--sslCAFile)

○ Accept server SSL certificates trusted by the operating system

● Accept any server SSL certificates

□ Use Client Certificate (--sslPEMKeyFile)

Client Certificate:

Passphrase:

☑ My client certificate is not protected by a passphrase

Select SSL/TLS: TLS

□ Allow invalid hostnames (--sslAllowInvalidHostnames)

□ Use Server Name Indication (Advanced)

SNI Host Name:

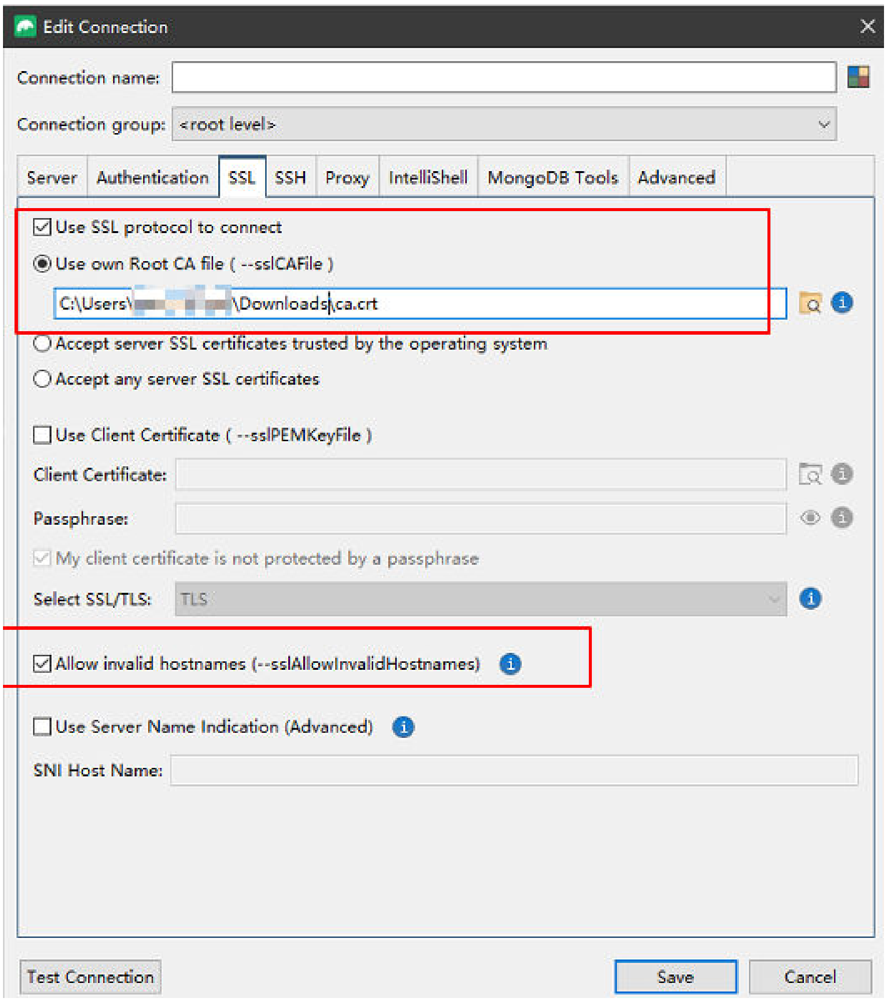
vi. Select **Use own Root CA file (--sslCAFile)**, import the certificate, and select **Allow invalid hostnames**.

NOTE

Download the SSL certificate and verify the certificate before connecting to databases.

On the **Instances** page, click the target DB instance name. In the **DB Information** area on the **Basic Information** page, click ⤓ in the **SSL** field to download the root certificate or certificate bundle.

Figure 6-39 Entering SSL information



Edit Connection

Connection name:

Connection group: <root level>

☑ Use SSL protocol to connect

● Use own Root CA file (--sslCAFile)

C:\Users\[redacted]\Downloads\ca.crt

○ Accept server SSL certificates trusted by the operating system

○ Accept any server SSL certificates

□ Use Client Certificate (--sslPEMKeyFile)

Client Certificate:

Passphrase:

☑ My client certificate is not protected by a passphrase

Select SSL/TLS: TLS

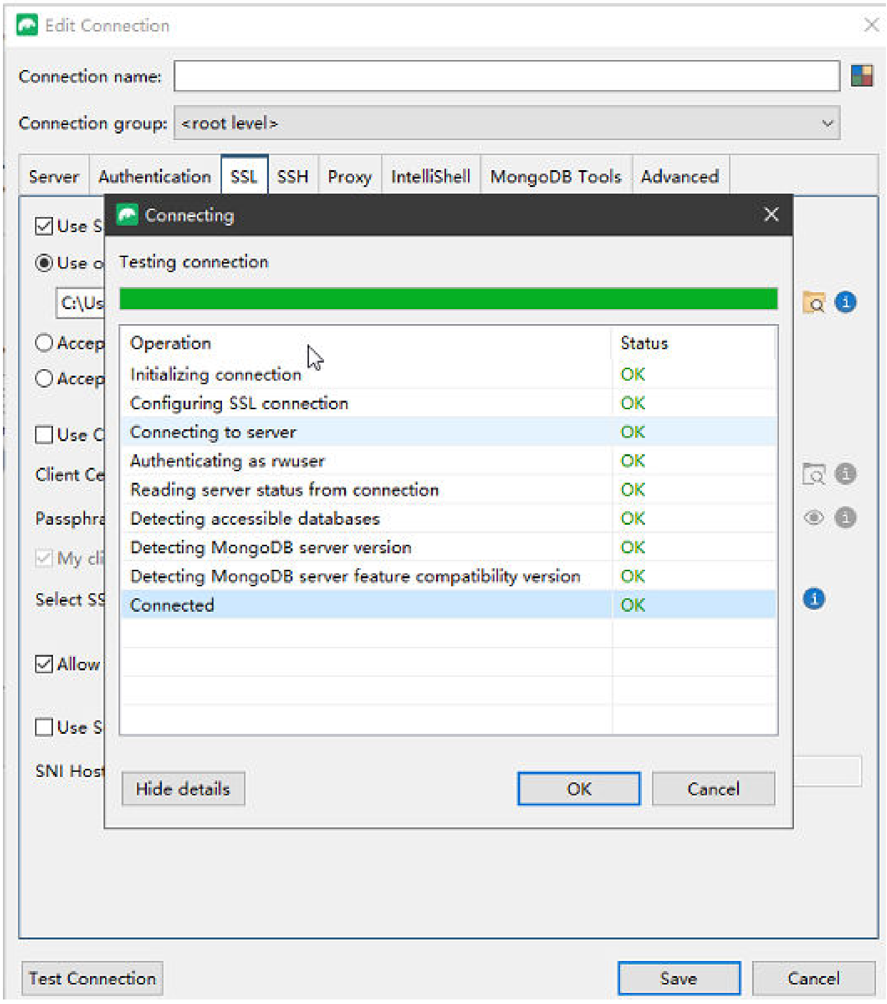
☑ Allow invalid hostnames (--sslAllowInvalidHostnames)

□ Use Server Name Indication (Advanced)

SNI Host Name:

vii. Click **Test Connection** to check whether the connection is successful.

Figure 6-40 Checking the SSL connection



Connection name:

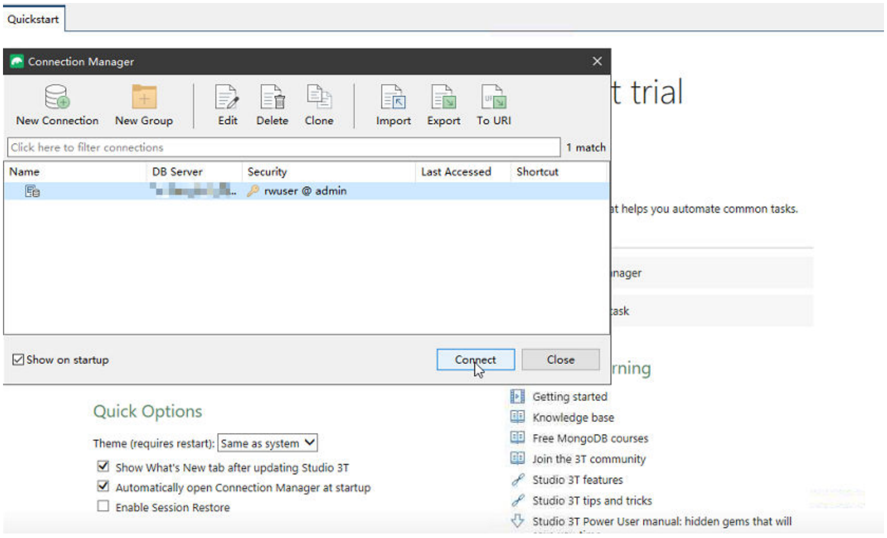
Connection group: <root level>

Testing connection

Operation	Status
Initializing connection	OK
Configuring SSL connection	OK
Connecting to server	OK
Authenticating as rwuser	OK
Reading server status from connection	OK
Detecting accessible databases	OK
Detecting MongoDB server version	OK
Detecting MongoDB server feature compatibility version	OK
Connected	OK

viii. After the check is successful, click **Save**.

Figure 6-41 Connection information



Name	DB Server	Security	Last Accessed	Shortcut
	[redacted]	rwuser @ admin		

Quick Options

Theme (requires restart): Same as system

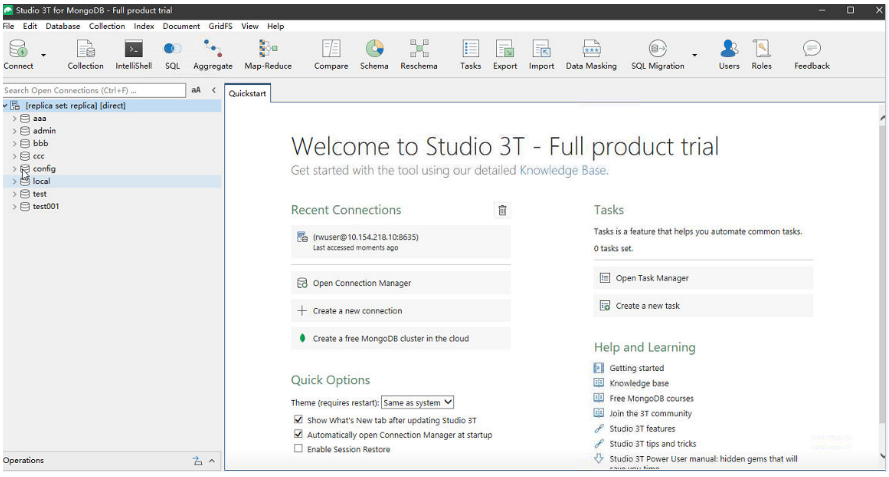
☑ Show What's New tab after updating Studio 3T

☑ Automatically open Connection Manager at startup

□ Enable Session Restore

ix. On the connection information page, click **Connect** to connect to the replica set instance. After the replica set instance is successfully connected, **Figure 6-42** is displayed.

Figure 6-42 Connection succeeded



Welcome to Studio 3T - Full product trial

Get started with the tool using our detailed Knowledge Base.

(rwuser@10.154.218.10:8635)
Last accessed moments ago

Tasks is a feature that helps you automate common tasks.

0 tasks set.

Theme (requires restart): Same as system

☑ Show What's New tab after updating Studio 3T

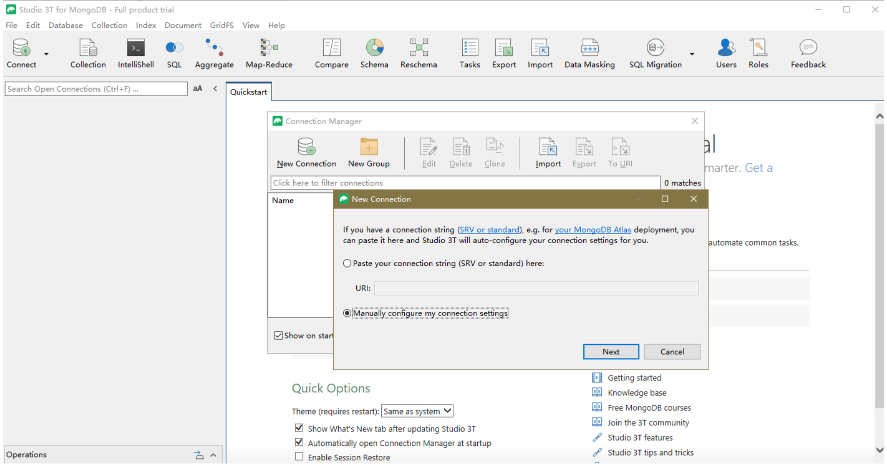
☑ Automatically open Connection Manager at startup

☐ Enable Session Restore

– **Method 2: Manually connect to a DB instance.**

i. In the displayed dialog box, select **Manually configure my connection settings** and click **Next**.

Figure 6-43 Manual connection mode



If you have a connection string (SRV or standard), e.g. for your MongoDB Atlas deployment, you can paste it here and Studio 3T will auto-configure your connection settings for you.

○ Paste your connection string (SRV or standard) here:

URI:

● Manually configure my connection settings

Theme (requires restart): Same as system

☑ Show What's New tab after updating Studio 3T

☑ Automatically open Connection Manager at startup

☐ Enable Session Restore

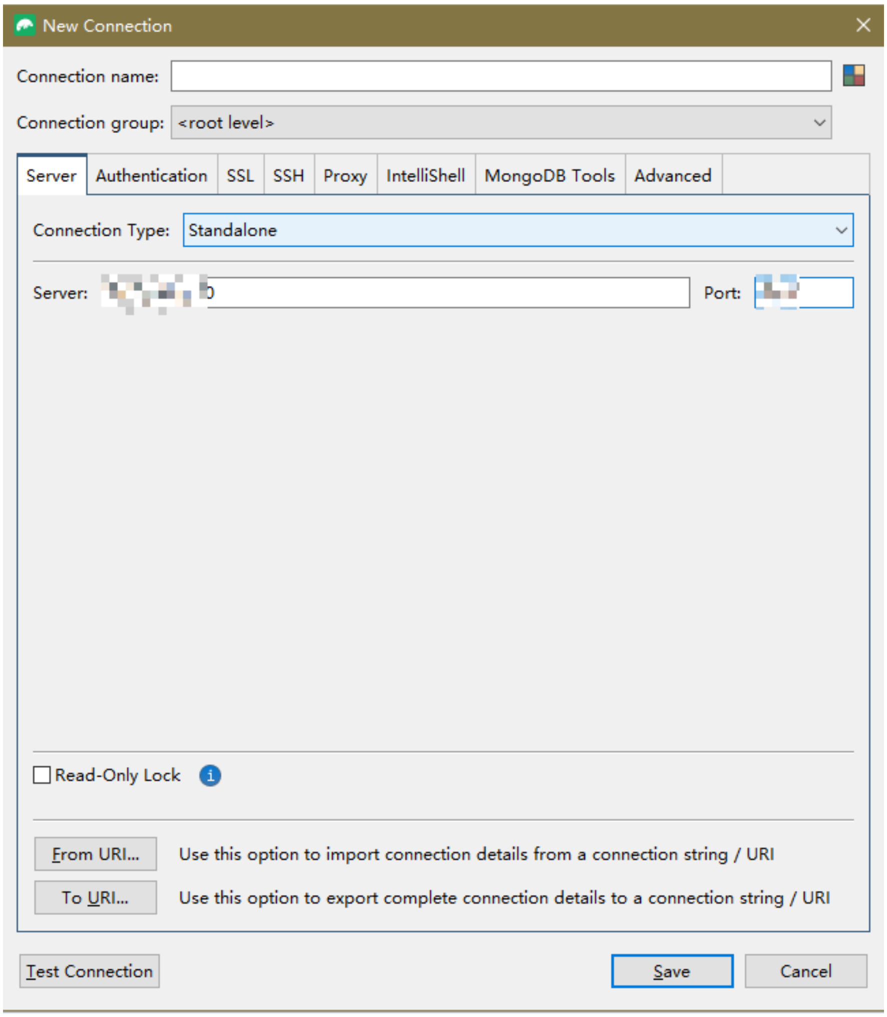
ii. On the **Server** tab, set **Server** and **Port**.

NOTE

Server: EIP.

Port: database port.

Figure 6-44 Server



New Connection

Connection name:

Connection group: <root level>

Connection Type: Standalone

Server: [redacted] Port: [redacted]

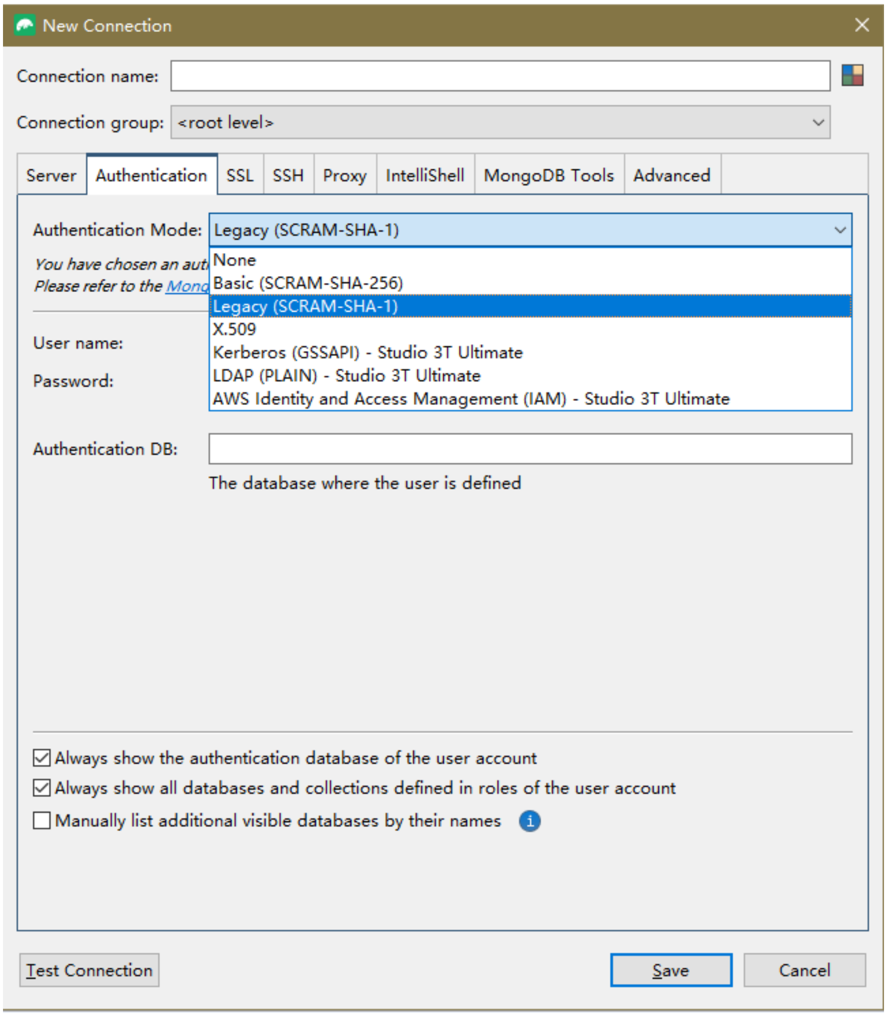
□ Read-Only Lock

Use this option to import connection details from a connection string / URI

Use this option to export complete connection details to a connection string / URI

iii. Click the **Authentication** tab and select **Legacy(SCRAM-SHA-1)**.

Figure 6-45 Authentication



New Connection

Connection name:

Connection group: <root level>

Server
Authentication
SSL
SSH
Proxy
IntelliShell
MongoDB Tools
Advanced

Authentication Mode: Legacy (SCRAM-SHA-1)

You have chosen an auth
Please refer to the Mong

None
Basic (SCRAM-SHA-256)
Legacy (SCRAM-SHA-1)
X.509
Kerberos (GSSAPI) - Studio 3T Ultimate
LDAP (PLAIN) - Studio 3T Ultimate
AWS Identity and Access Management (IAM) - Studio 3T Ultimate

User name:

Password:

Authentication DB:

The database where the user is defined

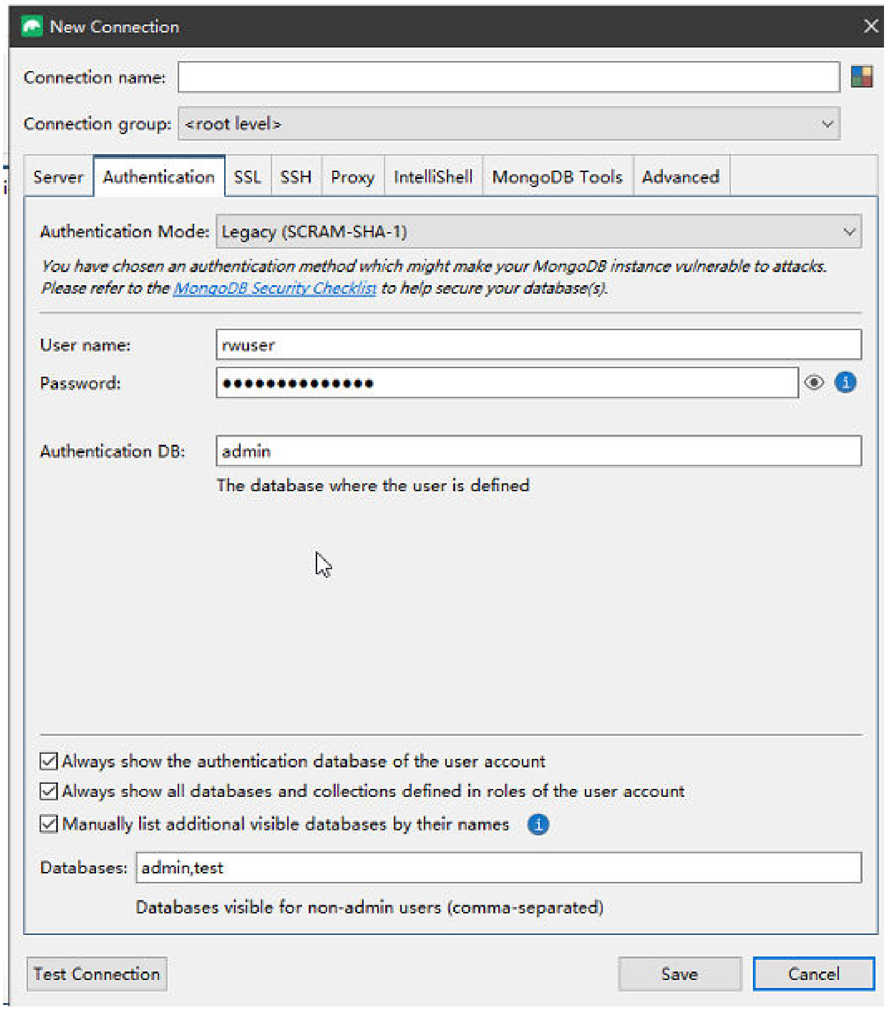
☑ Always show the authentication database of the user account

☑ Always show all databases and collections defined in roles of the user account

□ Manually list additional visible databases by their names

iv. Set **User name**, **Password**, and **Authentication DB**.

Figure 6-46 Authentication



New Connection

Connection name:

Connection group: <root level>

Authentication Mode: Legacy (SCRAM-SHA-1)

You have chosen an authentication method which might make your MongoDB instance vulnerable to attacks. Please refer to the MongoDB Security Checklist to help secure your database(s).

User name: rwuser

Password: ••••••••••••••

Authentication DB: admin

The database where the user is defined

☑ Always show the authentication database of the user account

☑ Always show all databases and collections defined in roles of the user account

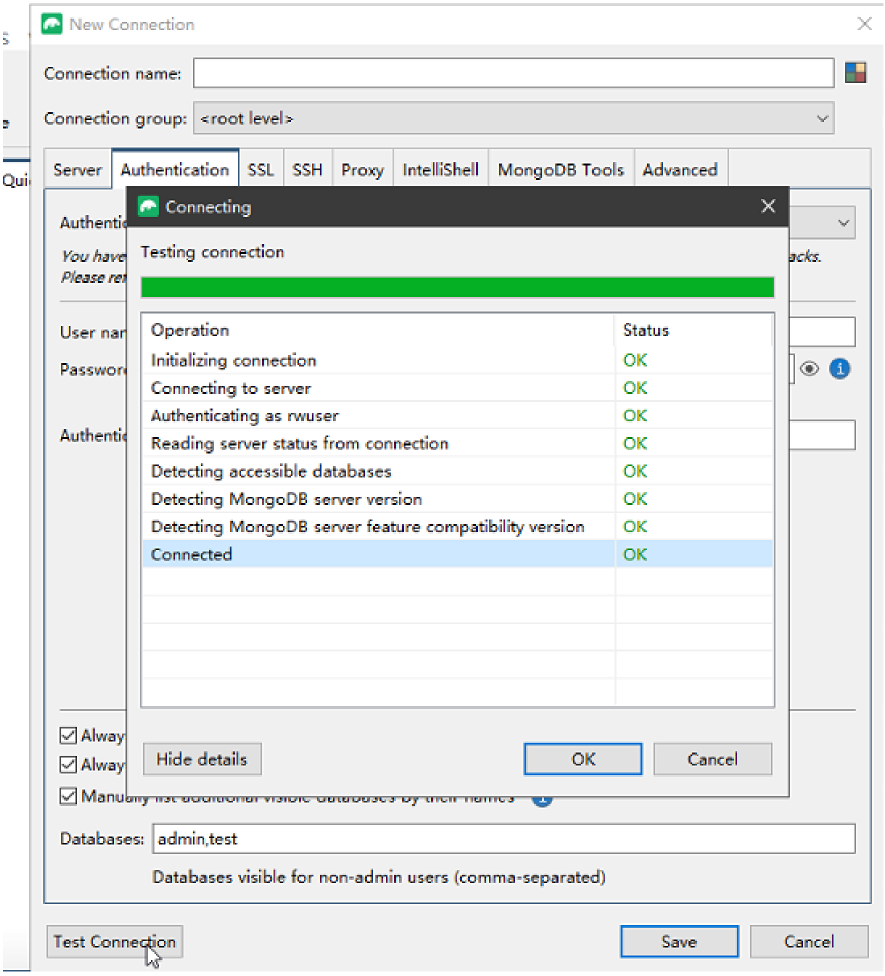
☑ Manually list additional visible databases by their names

Databases: admin,test

Databases visible for non-admin users (comma-separated)

v. Click **Test Connection** to check whether the connection is successful.

Figure 6-47 Test Connection



Connection name:

Connection group: <root level>

Testing connection

Operation	Status
Initializing connection	OK
Connecting to server	OK
Authenticating as rwuser	OK
Reading server status from connection	OK
Detecting accessible databases	OK
Detecting MongoDB server version	OK
Detecting MongoDB server feature compatibility version	OK
Connected	OK

Databases: admin,test

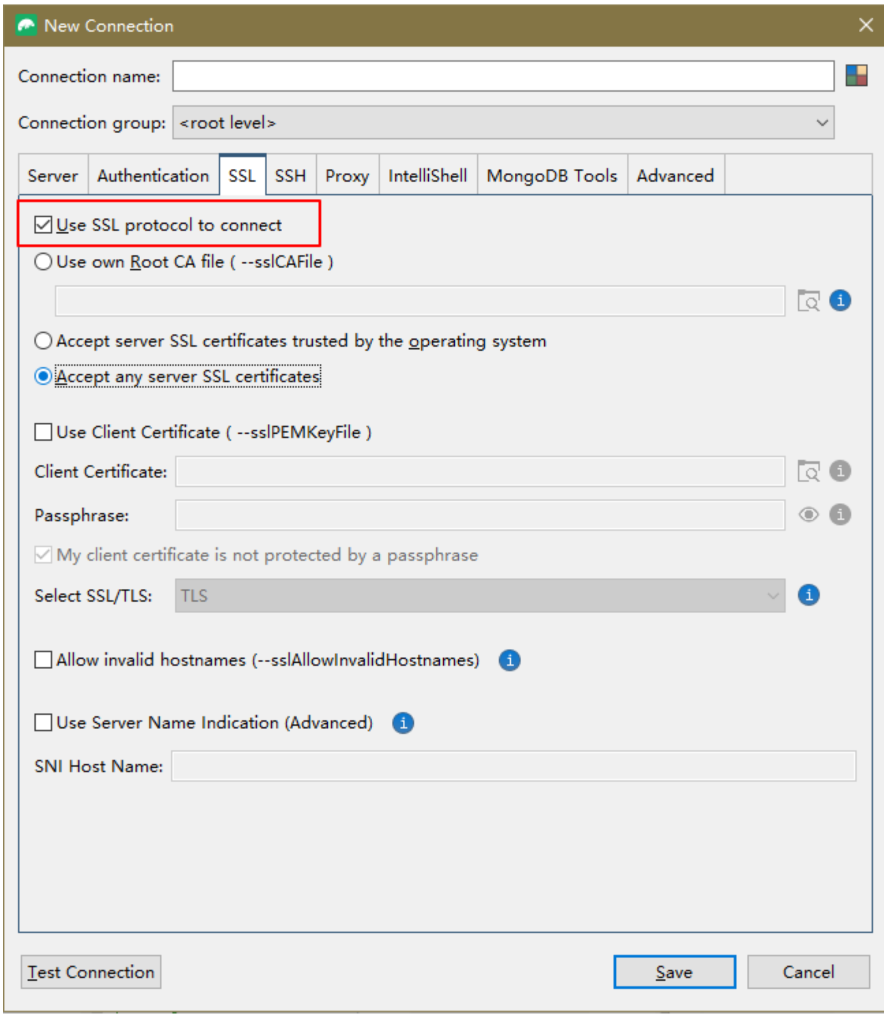
Databases visible for non-admin users (comma-separated)

vi. Click the **SSL** tab and select **Use SSL protocol to connect**.

NOTE

If SSL data encryption is disabled, skip this step and go to **6.ix**.

Figure 6-48 SSL



New Connection

Connection name:

Connection group: <root level>

Server | Authentication | SSL | SSH | Proxy | IntelliShell | MongoDB Tools | Advanced

☑ Use SSL protocol to connect

○ Use own Root CA file (--sslCAFile)

○ Accept server SSL certificates trusted by the operating system

● Accept any server SSL certificates

☐ Use Client Certificate (--sslPEMKeyFile)

Client Certificate:

Passphrase:

☑ My client certificate is not protected by a passphrase

Select SSL/TLS: TLS

☐ Allow invalid hostnames (--sslAllowInvalidHostnames)

☐ Use Server Name Indication (Advanced)

SNI Host Name:

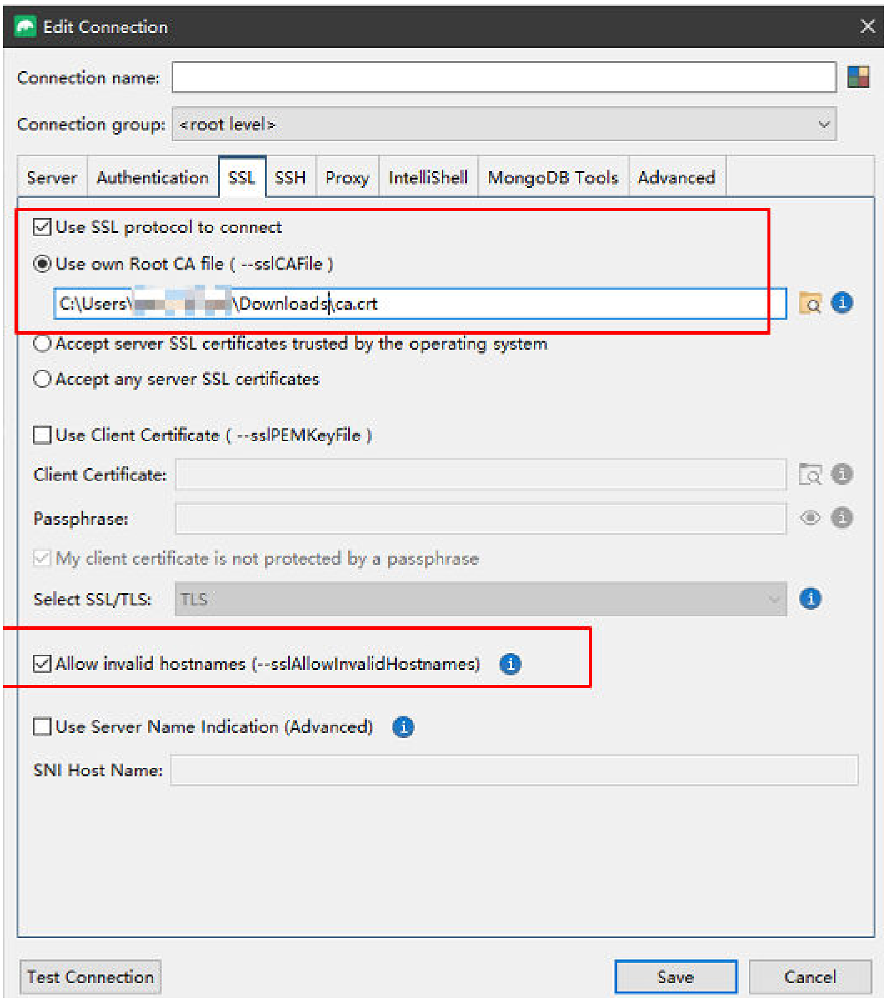
vii. Select **Use own Root CA file (--sslCAFile)**, import the certificate, and select **Allow invalid hostnames**.

NOTE

Download the SSL certificate and verify the certificate before connecting to databases.

On the **Instances** page, click the target DB instance name. In the **DB Information** area on the **Basic Information** page, click ⤓ in the **SSL** field to download the root certificate or certificate bundle.

Figure 6-49 Entering SSL information



Connection name:

Connection group: <root level>

☑ Use SSL protocol to connect

● Use own Root CA file (--sslCAFile)

C:\Users\[redacted]\Downloads\ca.crt

○ Accept server SSL certificates trusted by the operating system

○ Accept any server SSL certificates

☐ Use Client Certificate (--sslPEMKeyFile)

Client Certificate:

Passphrase:

☑ My client certificate is not protected by a passphrase

Select SSL/TLS: TLS

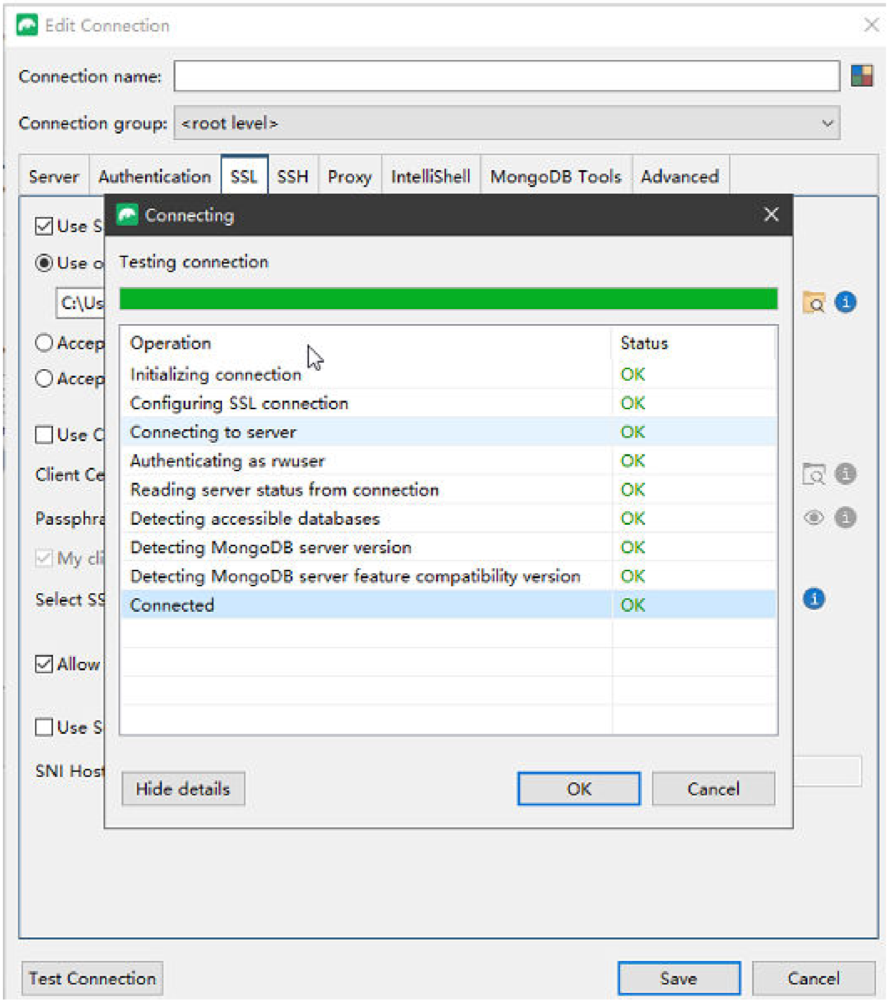
☑ Allow invalid hostnames (--sslAllowInvalidHostnames)

☐ Use Server Name Indication (Advanced)

SNI Host Name:

viii. Click **Test Connection** to check whether the connection is successful.

Figure 6-50 Checking the SSL connection



Edit Connection

Connection name:

Connection group: <root level>

Server | Authentication | SSL | SSH | Proxy | IntelliShell | MongoDB Tools | Advanced

☑ Use S
● Use o
C:\Us
○ Accep
○ Accep
□ Use C
Client Ce
Passphra
☑ My cli
Select SS
☑ Allow
□ Use S
SNI Host

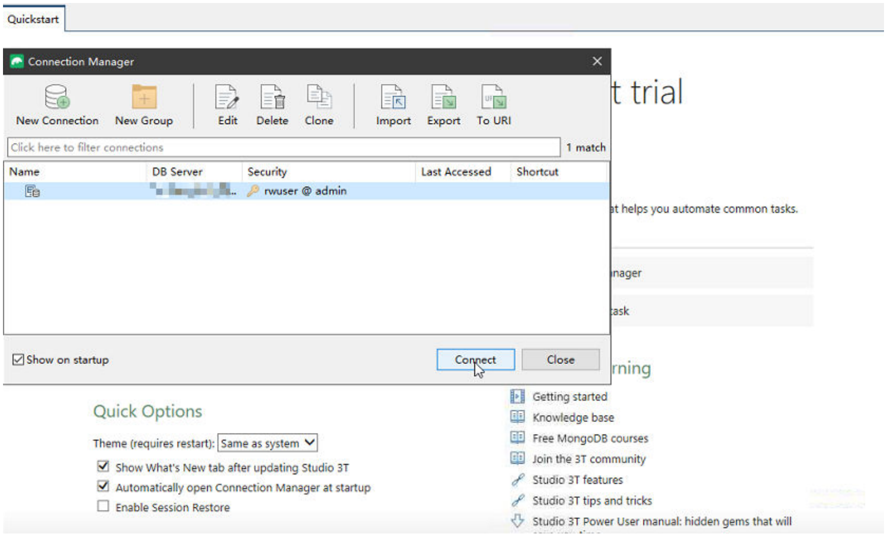
Connecting

Testing connection

Operation	Status
Initializing connection	OK
Configuring SSL connection	OK
Connecting to server	OK
Authenticating as rwuser	OK
Reading server status from connection	OK
Detecting accessible databases	OK
Detecting MongoDB server version	OK
Detecting MongoDB server feature compatibility version	OK
Connected	OK

ix. After the check is successful, click **Save**.

Figure 6-51 Connection information



Name	DB Server	Security	Last Accessed	Shortcut
	[redacted]	rwuser @ admin		

☑ Show on startup

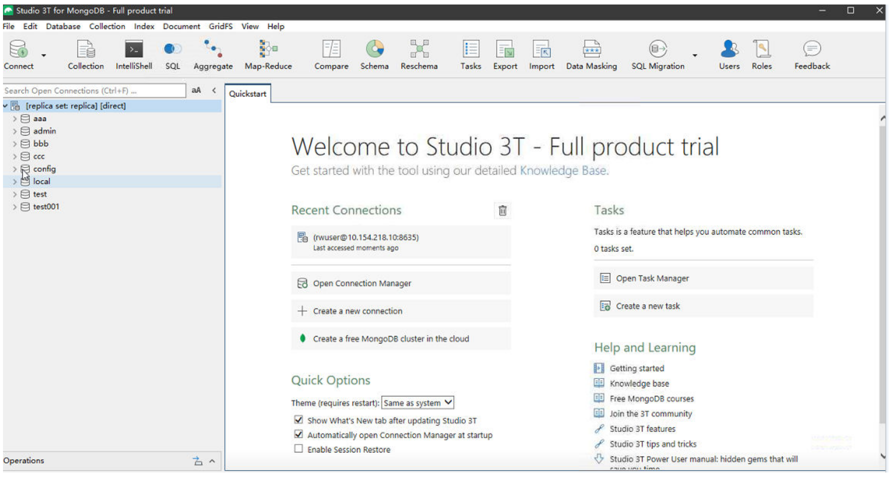
Quick Options

Theme (requires restart): Same as system

☑ Show What's New tab after updating Studio 3T
☑ Automatically open Connection Manager at startup
□ Enable Session Restore

x. On the connection information page, click **Connect** to connect to the replica set instance. After the replica set instance is successfully connected, **Figure 6-52** is displayed.

Figure 6-52 Connection succeeded



Welcome to Studio 3T - Full product trial

Get started with the tool using our detailed Knowledge Base.

Recent Connections

(rwuser@10.154.218.10:8635)
Last accessed moments ago

Quick Options

Theme (requires restart): Same as system

☑ Show What's New tab after updating Studio 3T
☑ Automatically open Connection Manager at startup
☐ Enable Session Restore

Tasks

Tasks is a feature that helps you automate common tasks.

0 tasks set.

Help and Learning

Studio 3T Power User manual: hidden gems that will save you time

7 Getting Started with Common Practices

After purchasing and connecting to a DB instance, you can view common practices to better use DDS.

Table 7-1 Common practices

Practice	Document	Description
Data Backups	**Configuring an Automated Backup Policy**	DDS backs up data automatically based on the automated backup policy you set. Regularly backing up your database is recommended. If your database becomes faulty or data is corrupted, you can restore it from backups. The automated backup policy for DDS is enabled by default.
	Creating a Manual Backup	This practice describes how to create a manual backup. Creating a backup for a DB instance helps ensure data can be restored if needed, ensuring data reliability.
Data Restorations	**Restoring Data to a New Instance**	DDS allows you to restore an existing automated or manual backup to a new instance. The restored data is the same as the backup data. When you restore an instance from a backup file, a full backup file is downloaded from OBS and then restored to the instance at an average speed of 40 MB/s.
	Restoring Data to the Original Instance	DDS allows you to restore an existing automated or manual backup to an original instance. The restored data is the same as the backup data. When you restore an instance from a backup file, a full backup file is downloaded from OBS and then restored to the instance at an average speed of 40 MB/s.

Practice	Document	Description
	Restoring Data to a Point in Time	DDS allows you to restore cluster and replica set instances to a point in time. When you enter the point in time that you want to restore the instance to, DDS downloads the most recent full backup file from OBS to the instance. Then, incremental backups are also restored to the specified point in time on the instance. Data is restored at an average speed of 30 MB/s.
Data Migration	**Migrating Data Using mongoexport and mongoimport**	mongoexport and mongoimport are backup and restoration tools provided by the MongoDB client. You can install a MongoDB client on the local device or ECS and use the mongoexport and mongoimport tools to migrate your on-premises MongoDB databases or other cloud MongoDB databases to DDS instances. Before migrating data from a MongoDB database to DDS, transfer data to a .json file using the mongoexport tool. This practice describes how to import the data from the JSON files to DDS using the mongoimport tool on the ECS or from some other devices that can access DDS.
	Migrating Data Using mongodump and mongorestore	mongodump and mongorestore are backup and restoration tools provided by the MongoDB client. You can install a MongoDB client on the local device or ECS and use the mongodump and mongorestore tools to migrate your on-premises MongoDB databases or other cloud MongoDB databases to DDS instances.
	From Other Cloud MongoDB to DDS	DRS helps you migrate MongoDB databases from other cloud platforms to DDS instances on the current cloud. With DRS, you can perform real-time migration tasks with minimal downtime. Services and databases remain operational during a migration.
	From On-Premises MongoDB to DDS	DRS helps you migrate data from on-premises MongoDB databases to DDS instances on the current cloud. With DRS, you can perform real-time migration tasks with minimal downtime. Services and databases remain operational during a migration.
	From ECS-hosted MongoDB to DDS	DRS helps you migrate data from MongoDB databases on ECSs to DDS instances on the current cloud. With DRS, you can perform real-time migration tasks with minimal downtime. Services and databases remain operational during a migration.
	From DDS to MongoDB	This practice describes how to migrate data from a DDS instance to an on-premises MongoDB database.

Practice	Document	Description
Instance Modifications	**Changing an Instance Name**	This practice describes how to change an instance name to identify different instances.
	Changing an Instance Class	This practice describes how to change the class of a cluster, replica set, or single node instance.
	Scaling Up Storage Space	This practice describes how to scale up the storage space of an instance. If you scale up the storage space of an instance, the backup space increases accordingly.
Data Security	**Enabling or Disabling SSL**	Secure Socket Layer (SSL) is an encryption-based Internet security protocol for establishing an encrypted link between a server and a client. It provides privacy, authentication, and integrity to Internet communications. SSL: ● Authenticates users and servers, ensuring that data is sent to the correct clients and servers. ● Encrypts data to prevent it from being intercepted during transfer. ● Ensures data integrity during transmission. After SSL is enabled, you can establish an encrypted connection between your client and the instance you want to access to improve data security.
	Changing a Security Group	This practice describes how to change a security group for cluster and replica set instances.
Logs	**Error Logs**	DDS log management allows you to view database-level logs, including warning- and error-level logs generated during database running, which help you analyze system problems.
	Slow Query Logs	Slow query logs record statements that exceed **operationProfiling.slowOpThresholdMs** (500 seconds by default). You can view log details and statistics to identify statements that are executing slowly and optimize the statements. You can also download slow query logs for service analysis.
	Audit Logs	An audit log records operations performed on your databases and collections. The generated log files are stored in OBS. Auditing logs can enhance your database security and help you analyze the cause of failed operations.

A Change History

Released On	Description
2021-12-30	This issue is the thirtieth official release, which incorporates the following changes: ● Added **Connecting to a Cluster Instance Using Program Code**. ● Added **Connecting to a Replica Set Instance Using Program Code**. ● Added **Connecting to a Single Node Instance Using Program Code**.
2021-10-30	This issue is the twenty-ninth official release, which incorporates the following change: Added **Overview**.
2021-05-30	This issue is the twenty-eighth official release, which incorporates the following change: Supported quick purchase and custom purchase.
2021-04-30	This issue is the twenty-seventh official release, which incorporates the following change: Changed parameter group to parameter template.
2020-10-30	This issue is the twenty-sixth official release, which incorporates the following change: Supported up to 20 tags per instance.
2020-09-30	This issue is the twenty-fifth official release, which incorporates the following changes: Supported Kunpeng-based instances of Community Edition 4.0.

Released On	Description
2020-08-30	This issue is the twenty-fourth official release, which incorporates the following changes: ● Supported up to 32 dds mongos nodes and 32 shard nodes in each Community Edition cluster instance. ● Supported up to 3,000 GB of the replica set storage space.
2020-07-30	This issue is the twenty-third official release, which incorporates the following changes: Supported cross-CIDR access to replica set instances.
2020-07-15	This issue is the twenty-second official release, which incorporates the following change: Supported DCC.
2020-05-30	This issue is the twenty-first official release, which incorporates the following change: Supported enterprise projects for the Enhanced cluster instance.
2020-04-30	This issue is the twentieth official release, which incorporates the following changes: ● Updated the IAM permission template. ● Supported the purchase of multi-AZ Community Edition DB instances.
2020-04-15	This issue is the nineteenth official release, which incorporates the following change: Supported cross-subnet access for replica set instances in the same VPC.
2020-03-31	This issue is the eighteenth official release, which incorporates the following changes: ● Supported changing billing mode from yearly/monthly to pay-per-use. ● Allowed users to set a password after the DB instance is created. ● Supported enabling IP addresses of shard and config nodes of Community Edition cluster instances.
2020-02-14	This issue is the seventeenth official release, which incorporates the following change: Optimized the procedures for creating a DB instance.
2020-01-07	This issue is the sixteenth official release, which incorporates the following changes: ● Adjusted the structure of section Getting Started.

Released On	Description
2019-11-11	This issue is the fifteenth official release, which incorporates the following change: Supported the Community Edition cluster instance with up to 2,000 GB of storage.
2019-10-18	This issue is the fourteenth official release, which incorporates the following changes: ● Supported the selection of s6 specifications. ● Added the procedures for using Robo 3T to connect to the DDS instance.
2019-09-11	This issue is the thirteenth official release, which incorporates the following changes: Supported a maximum of 16 dds mongos nodes and 16 shards for a Community Edition cluster instance.
2019-08-13	This issue is the twelfth official release, which incorporates the following change: Supported selecting a CPU type for the pay-per-use DB instance of Community Edition 3.4.
2019-07-07	This issue is the eleventh official release, which incorporates the following changes: Supported selecting a parameter group during DB instance creation.
2019-06-13	This issue is the tenth official release, which incorporates the following change: Supported DeC.
2019-04-19	This issue is the ninth official release, which incorporates the following changes: ● Optimized the procedures for creating and connecting to a DB instance.
2019-02-15	This issue is the eighth official release, which incorporates the following changes: Supported the modification of the node private IP address.
2019-01-07	This issue is the seventh official release, which incorporates the following changes: ● Added the **Tags** configuration item on the page for buying a DB instance of Community Edition.
2018-11-02	This issue is the sixth official release, which incorporates the following changes: ● Supported buying yearly/monthly DB instances in batches. ● Added the command for connecting to DB instances through connection addresses.

Released On	Description
2018-09-06	This issue is the fifth official release, which incorporates the following change: Optimized the section for guiding a purchase of DB instances.
2018-08-03	This issue is the fourth official release, which incorporates the following changes: ● Optimized the page for purchasing a DB instance. ● Supported creation of yearly/monthly cluster instances. ● Supported automatic renewal of yearly/monthly replica set instances.
2018-07-02	This issue is the third official release, which incorporates the following change: ● Supported creating a replica set instance in multiple AZs. ● Adjusted the position of **HA Type** displayed on the console page. ● Changed the maximum storage capacity of replica sets to 2,000 GB.
2018-06-01	This issue is the second official release, which incorporates the following change: ● Supported DB instances that are compatible with MongoDB 3.4 Community Edition. ● Supported allocation of default VPC resources during the DB instance creation.
2018-05-04	This issue is the first official release.