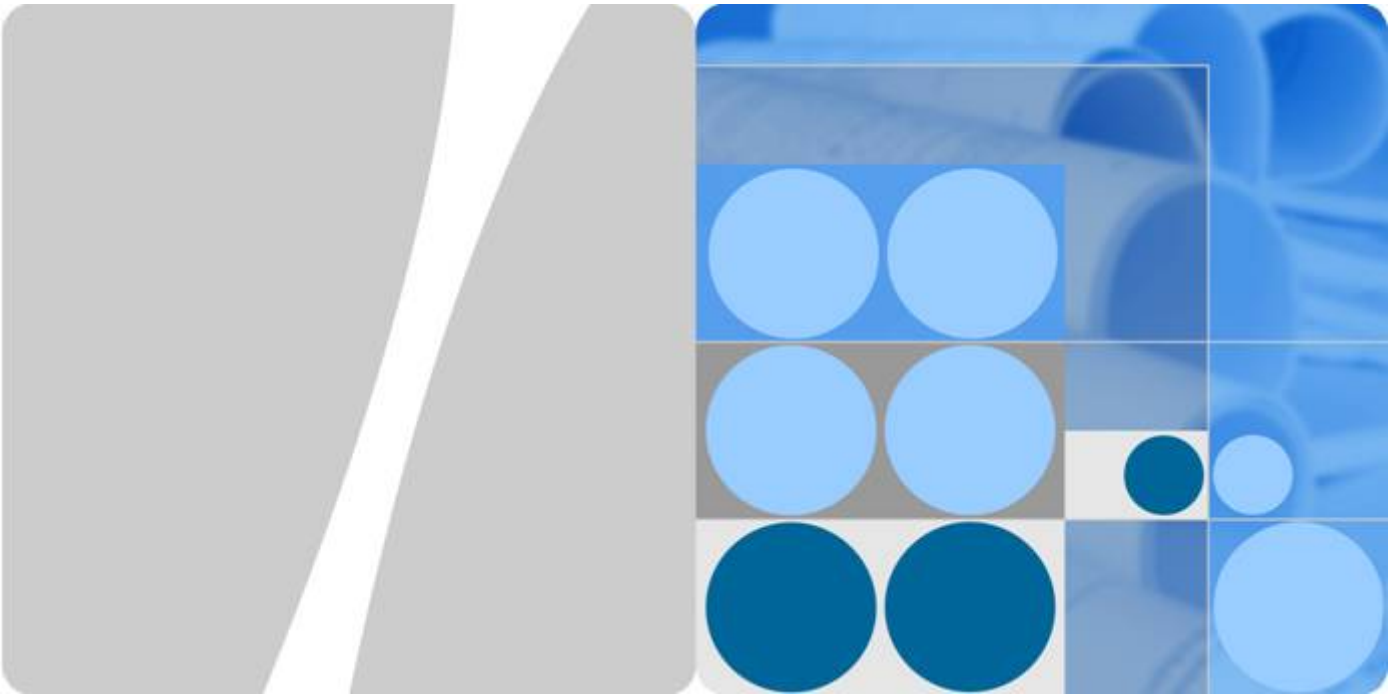


Document Database Service

Getting Started

Issue 27

Date 2020-10-30

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

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.

Contents

1 Logging In to the DDS Console

Prerequisites

You have registered a HUAWEI CLOUD account.

If you have not registered with HUAWEI CLOUD, follow the instructions provided in **Common Operations** to register an account at **HUAWEI CLOUD official website**. After the registration, your account has permissions to access the DDS service, as well as all other HUAWEI CLOUD services.

NOTE

After the registration, you can use your account to create a user, add the user to a user group, and authorize the user group. For details, see **Quick Start with IAM**.

Procedure

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 charged for purchasing DDS DB instances through DeC.

Step 5 Click **Service List**. Under **Database**, click **Document Database Service** to go to the DDS console.

----End

2 Getting Started with Clusters

2.1 Connection Methods

HUAWEI CLOUD DDS can be accessed using Data Admin Service (DAS), private networks, and public networks.

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. For details, see **Step 2: Connect to a Cluster Instance Through DAS**.

Table 2-1 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 all 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 that is in the same region, AZ, and VPC subnet as your DDS DB instance, you are advised to use a private IP address to connect the ECS to your DDS DB instances. • By default, DDS is not accessible from ECSs that are not in the same security group. If the ECS is not in the same group, you need to add an inbound rule to enable access. • The default DDS port is 8635, but this port can be modified if necessary.	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, you are advised to 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.

2.2 Connecting to Cluster Instances Using DAS

2.2.1 Overview

Scenarios

DAS provides a graphical user interface (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 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:

- **Step 1: Buy a Cluster Instance**
- **Step 2: Connect to a Cluster Instance Through DAS**

2.2.2 Step 1: Buy a Cluster Instance

Scenarios

This section describes how to create a Community Edition cluster instance on the DDS management console. Currently, DDS cluster instance of Community Edition supports the yearly/monthly and pay-per-use billing modes. DDS allows you to tailor your compute resources and storage space to your business needs.

You can use your account to create up to 10 cluster instances.

Prerequisites

- You have registered a HUAWEI CLOUD account.
- Your account balance is greater than or equal to ¥0.

Procedure

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

Step 2 On the **Instance Management** page, click Buy DB Instance.

Step 3 On the displayed page, select a billing mode, select your DB instance specifications and click **Next**.

Figure 2-1 Billing mode and basic information

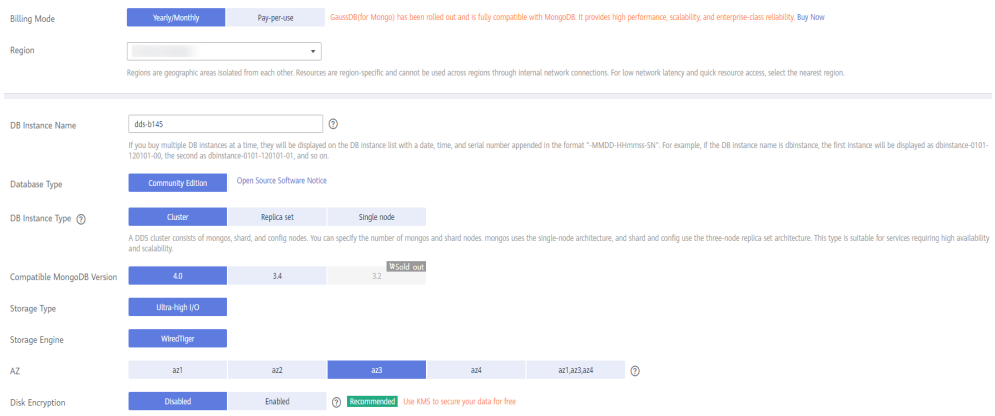


Table 2-2 Billing mode

Parameter	Description
Billing Mode	Select a billing mode, **Yearly/Monthly** or **Pay-per-use**. • Yearly/Monthly – You need to set **Validity Period** as required. Then, the system deducts the fees incurred at one time from your account based on the service price. – When you renew a yearly/monthly DB instance, you can change its billing mode from yearly/monthly to pay-per-use based on your service requirements. For details, see **Changing Yearly/Monthly Instances to a Pay-per-Use**. **NOTE** DB instances paid in yearly/monthly mode cannot be deleted. They support only resource unsubscription. For details, see section **Unsubscribing from a Yearly/Monthly DB Instance**. • Pay-per-use – You do not need to set **Validity Period** because the system deducts the fees incurred from your account based on the service duration. – If you want to use a DB instance at a low cost for a long period of time, you can change its billing mode from pay-per-use to yearly/monthly. For details, see **Changing the Billing Mode in Batches**.

Table 2-3 Basic information

Parameter	Description
Region	A region where the tenant is located. It can be changed in the upper left corner. **NOTE** DB instances deployed in different regions cannot communicate with each other through a private network, and you cannot change the region of a DB instance once it is purchased. Exercise caution when selecting a region.

Parameter	Description
DB Instance Name	The DB instance name can be 4 to 64 characters long. It must start with a letter and can contain only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_). If you buy multiple DB instances, you can only enter 4 to 49 characters to set the DB instance name, and then the system automatically appends a date, time, and serial number to the end of the instance names (format: *instance_name-MMDD-HHmmss-SN*). After the DB instance is created, you can change its name. For details, see **Modifying the DB Instance Name**.
Database Type	Community Edition
DB Instance Type	Select **Cluster**. A cluster instance includes three types of nodes: mongos, shard, and config. Each shard and config is a three-node replica set to ensure high availability.
Compatible MongoDB Version	• 4.0 • 3.4 • 3.2
CPU Type	Currently, DDS supports two CPU architectures: x86 and Kunpeng. The two architectures have similar capabilities and performance, both of which can meet your service requirements. For details about the instance types, versions, and specifications supported by the two CPU architectures, see **DB Instance Specifications**.
Resource Type	If you use DeC, this parameter is displayed. EVS and DSS disks are provided based on whether storage resources are exclusively used. DSS disks provide dedicated storage resources. • If you have applied for a storage pool on the DSS page, click the **DSS** tab and create disks in the obtained storage pool. • If you have not applied for an exclusive storage pool, click the **EVS** disk tab. Then, the created disks use public storage resources.

Parameter	Description
Storage Type	If you do not use DeC, the storage type is ultra-high I/O by default. For DeC users, the supported storage types vary depending on the selected resource type. ● If you select **EVS** for **Resource Type**, **Storage Type** is set to **Ultra-high I/O**. ● If you select **DSS** for **Resource Type**, **Storage Type** can be set to **Common I/O**, **High I/O**, or **Ultra-high I/O**.
Storage Pool	This option is displayed only when you select **DSS** for **Resource Type**. The storage pool is physically isolated from other pools and is secure.
Storage Engine	WiredTiger
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 an internal network. Currently, instances can be deployed in a single AZ or three AZs. ● If you want to deploy an instance in a single AZ, select one AZ. ● If you want to deploy an instance across AZs for disaster recovery, select three AZs. In this deployment mode, the nodes are evenly distributed in the three AZs.
Disk Encryption	● **Disabled**: Disable the encryption function. ● **Enabled**: Enable the encryption function. 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 a DB instance is created, the disk encryption status and the key cannot be changed. The backup data stored in OBS is not encrypted. – The key cannot be disabled, deleted, or frozen when being used. Otherwise, the database becomes unavailable. – For details about how to create a key, see the "Creating a CMK" section in the *Data Encryption Workshop User Guide*.

Figure 2-2 Instance specifications

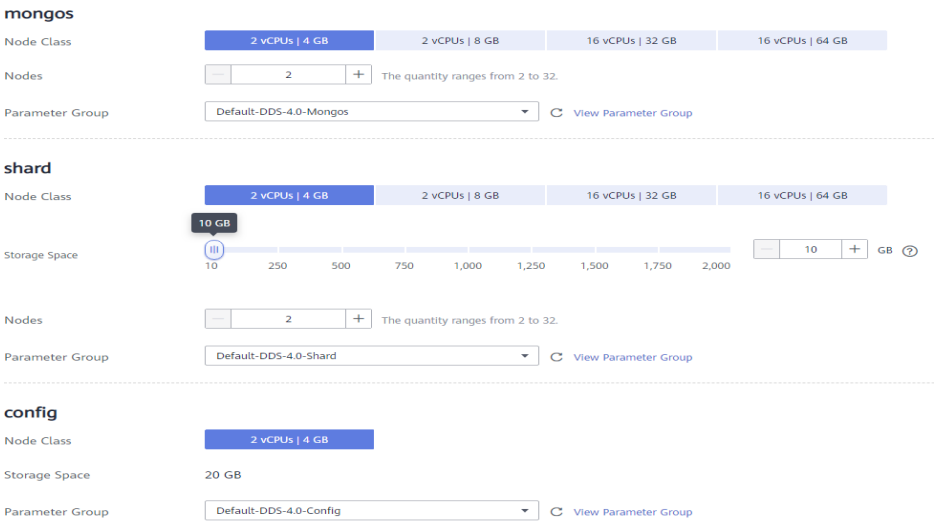


Table 2-4 Specifications

Parameter	Description
Specifications	In the x86 CPU architecture, the following specifications can be selected to suit different application scenarios: General-purpose (s6), Enhanced (c3), and Enhanced II (c6). For details about the supported DB instance specifications, see **DB Instance Specifications**.
Dedicated Cloud	If you use DeC, this parameter is displayed. For details about DB instance specifications in your DeC, see **Database Instance Specifications**.
mongos class	For details about the mongos CPU and memory, see **DB Instance Specifications**. After a DB instance is created, you can change its CPU and memory. For details, see **Changing the CPU or Memory of a Cluster DB Instance**.
mongos quantity	The number of mongos nodes. The value ranges from 2 to 32. After a DB instance is created, you can add mongos nodes if necessary. For details, see section **Adding Cluster Instance Nodes**.
mongos parameter group	The parameters that apply to the mongos nodes. After a DB instance is created, you can change the parameter group of a node to bring out the best performance. For details, see **Editing a Parameter Group**.

Parameter	Description
shard class	For details about the shard CPU and memory, see **DB Instance Specifications**. After a DB instance is created, you can change its CPU and memory. For details, see **Changing the CPU or Memory of a Cluster DB Instance**.
shard storage space	The value ranges from 10 GB to 2000 GB and must be a multiple of 10. After a DB instance is created, you can scale up its storage space. For details, see **Scaling Up Storage Space**.
shard quantity	The number of shard nodes. The shard node stores user data but cannot be accessed directly. The value ranges from 2 to 32. After a DB instance is created, you can add shard nodes if necessary. For details, see **Adding Cluster Instance Nodes**.
shard parameter group	The parameters that apply to the shard nodes. After a DB instance is created, you can change the parameter group of a node to bring out the best performance. For details, see **Editing a Parameter Group**.
config class	The CPU and memory of a config node. The config node stores the DB instance configurations but cannot be accessed directly. For details, see **DB Instance Specifications**.
config storage space	The storage space is 20 GB and cannot be scaled up.
config parameter group	The parameters that apply to the config nodes. After a DB instance is created, you can change the parameter group of a node to bring out the best performance. For details, see **Editing a Parameter Group**.

Figure 2-3 Network and database configuration

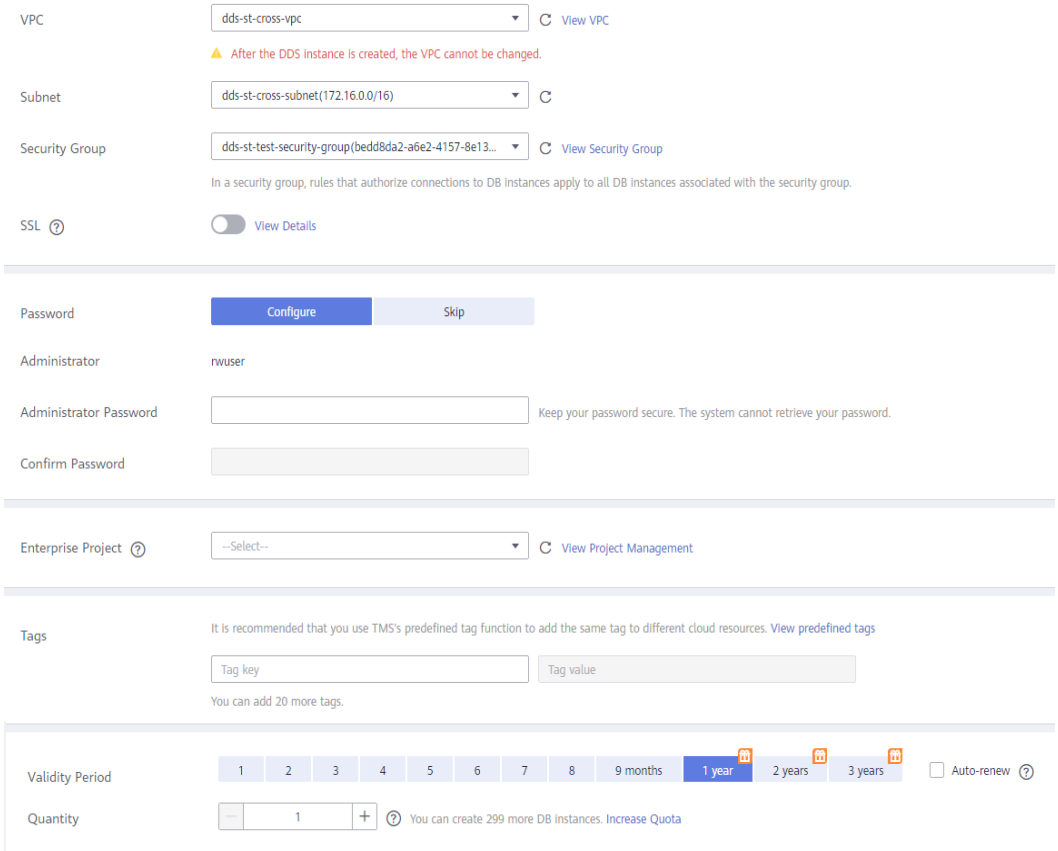


Table 2-5 Network

Parameter	Description
VPC	The VPC where your DB instances are located. A VPC isolates networks for different services, so you can easily manage and configure internal networks and change network configuration. For details about how to create a VPC, see section "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 allocates resources to 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 network security. After the instance is created, you can change the private IP address assigned by the subnet. For details, see **Changing a Private IP Address**.

Parameter	Description
Security Group	A security group controls access between DDS and other services for security. If there are no security groups available, DDS allocates resources to you by default. **NOTE** Ensure that the security group rule you set allows clients to access DB instances. For example, select the TCP protocol with inbound direction, input the default port number **8635**, and enter a subnet IP address or select a security group that the DB instance belongs to.
SSL	Secure Sockets Layer (SSL) certificates set up encrypted connections between clients and servers, preventing data from being tampered with or stolen during transmission. You can enable SSL to improve data security. After a DB instance is created, you can connect to it using SSL.
IPv6	Before enabling IPv6, ensure that IPv6 has been enabled for the VPC and subnet where the DB instance is located. For details about the application scenarios and procedures for enabling IPv6 for the VPC and subnet, see **IPv4 and IPv6 Dual-Stack Network**. After IPv6 is enabled, the DB instance can run in dual-stack mode. It means that the DB instance can use both the IPv4 address and IPv6 address. The DB instance can access the Internet using either IPv4 or IPv6 addresses, and the communications are independent of each other.

Table 2-6 Database configuration

Parameter	Description
Password	• Configure Enter and confirm the administrator password for connecting to the DB instance. • Skip Set the administrator password later. When you need to connect to the DB instance, locate the DB instance and click **Reset Password** in the **Operation** column to set a password for connecting to the DB instance.
Administrator	The default account is **rwuser**.
Administrator Password	Set a password for the administrator. The password is a string of 8 to 32 characters. It must be a combination of uppercase letters, lowercase letters, digits, and special characters. You can also use the following special characters: ~!@#%^*-_=+? Keep this password secure. If lost, the system cannot retrieve it for you.

Parameter	Description
Confirm Password	Enter the administrator password again.
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**. 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 the *Enterprise Management User Guide*.

Table 2-7 Tag

Parameter	Description
Tags	This setting is optional. Adding tags helps you better identify and manage your DB instances. Up to 20 tags can be added for a DB instance. A tag is composed of a key-value pair. • Key: Mandatory if the DB instance is going to be tagged – Each tag key must be unique for each DB instance. – A tag key consists of up to 36 characters. – The key can only consist of digits, letters, underscores (_), and hyphens (-). • Value: Optional if the DB instance is going to be tagged – The value consists of up to 43 characters. – The value can only consist of digits, letters, underscores (_), dots (.), and hyphens (-). After a DB instance is created, you can view its tag details on the **Tags** tab. In addition, you can add, modify, and delete tags for existing DB instances. For details, see **Tag**.

Table 2-8 Required duration and quantity

Parameter	Description
Validity Period	Sets the service duration if you select the **Yearly/Monthly** billing mode. The service duration ranges from one month to three years.

Parameter	Description
Auto-renew	• By default, this option is not selected. • If you select this option, the auto-renew cycle is determined by the selected required duration.
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 increasing the quota as prompted. The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

NOTE

DB instance performance is determined by how you configure it during the creation. The hardware configuration items that can be selected include the node class and storage space.

Step 4 On the displayed page, confirm the DB instance information.

- Yearly/Monthly
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify your settings, click **Pay Now** to go to the payment page and complete the payment.
- Pay-per-use
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, click **Submit** to start the instance creation.

Step 5 After a DDS DB instance is created, you can view and manage it on the **Instance Management** 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**.
- DDS enables the automated backup policy by default. After a DB instance is created, you can modify or disable the automated backup policy. An automated full backup is immediately triggered after the creation of a DB instance.
- The default DDS port is 8635, but this port can be modified if necessary. If you change the port, you need to add the security group rule to enable access.
- The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

----End

2.2.3 Step 2: Connect to a Cluster Instance Through DAS

Scenarios

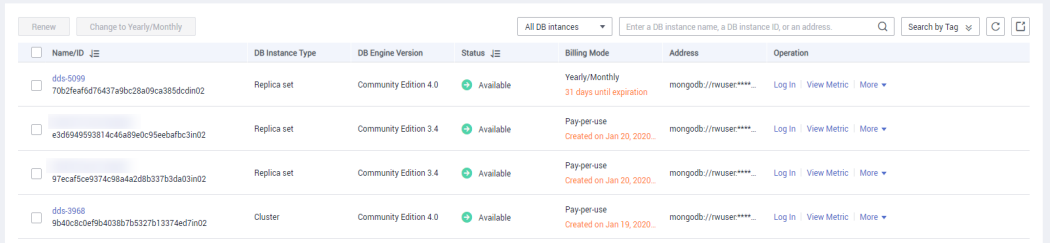
Data Admin Service (DAS) enables you to manage DB instances on a web-based console, simplifying database management and improving working efficiency. By default, you have the remote login permission. It is recommended that you use the DAS service to connect to DB instances, which is more secure and convenient.

Procedure

Step 1 On the **Instance Management** page, locate the target DB instance and click **Log In** in the **Operation** column.

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

Figure 2-4 Instance management



Step 2 On the displayed login page, enter the administrator username and password and click **Login**.

For details about how to manage databases through DAS, see **User Interface Overview**.

----End

2.3 Connecting to a Cluster Instance Over Private Networks

2.3.1 Overview

Scenarios

This section describes how to buy a cluster instance on the management console, set a security group, and connect to a cluster instance over private networks.

Process

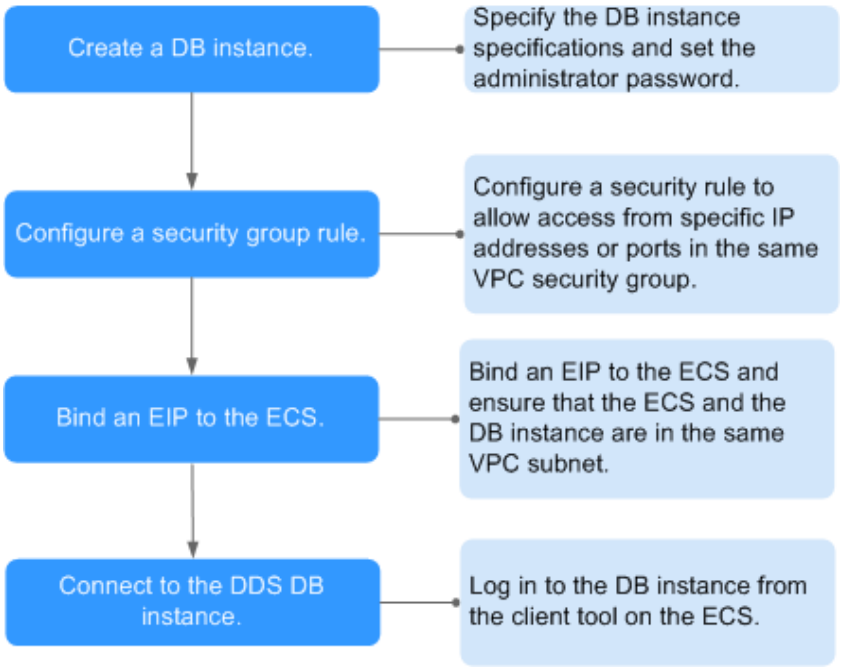
To purchase and connect to a cluster instance, perform the following steps:

- **Step 1: Buy a Cluster Instance**

- **Step 2: Set a Security Group**
- **Step 3: Connect to a Cluster Instance Over Private Networks**

The following describes the steps from creating a DB instance to using it.

Figure 2-5 Accessing DB instances from a private network



2.3.2 Step 1: Buy a Cluster Instance

Scenarios

This section describes how to create a Community Edition cluster instance on the DDS management console. Currently, DDS cluster instance of Community Edition supports the yearly/monthly and pay-per-use billing modes. DDS allows you to tailor your compute resources and storage space to your business needs.

You can use your account to create up to 10 cluster instances.

Prerequisites

- You have registered a HUAWEI CLOUD account.
- Your account balance is greater than or equal to ¥0.

Procedure

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

Step 2 On the **Instance Management** page, click Buy DB Instance.

Step 3 On the displayed page, select a billing mode, select your DB instance specifications and click **Next**.

Figure 2-6 Billing mode and basic information

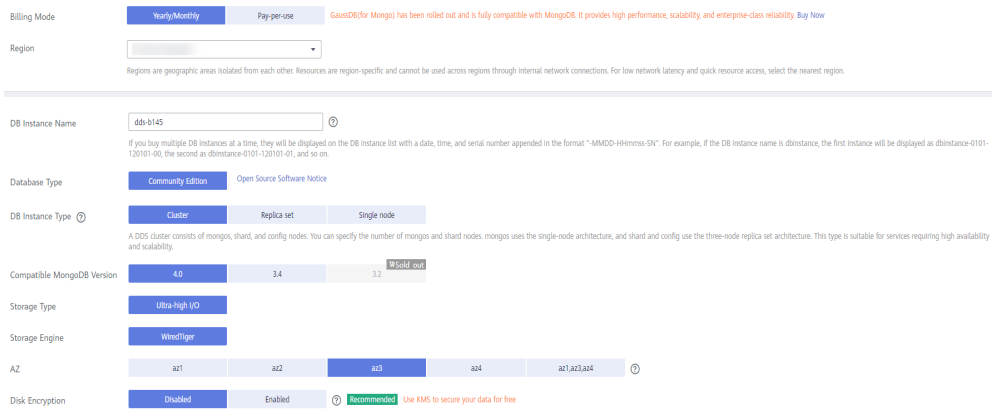


Table 2-9 Billing mode

Parameter	Description
Billing Mode	Select a billing mode, **Yearly/Monthly** or **Pay-per-use**. • Yearly/Monthly – You need to set **Validity Period** as required. Then, the system deducts the fees incurred at one time from your account based on the service price. – When you renew a yearly/monthly DB instance, you can change its billing mode from yearly/monthly to pay-per-use based on your service requirements. For details, see **Changing Yearly/Monthly Instances to a Pay-per-Use**. **NOTE** DB instances paid in yearly/monthly mode cannot be deleted. They support only resource unsubscription. For details, see section **Unsubscribing from a Yearly/Monthly DB Instance**. • Pay-per-use – You do not need to set **Validity Period** because the system deducts the fees incurred from your account based on the service duration. – If you want to use a DB instance at a low cost for a long period of time, you can change its billing mode from pay-per-use to yearly/monthly. For details, see **Changing the Billing Mode in Batches**.

Table 2-10 Basic information

Parameter	Description
Region	A region where the tenant is located. It can be changed in the upper left corner. **NOTE** DB instances deployed in different regions cannot communicate with each other through a private network, and you cannot change the region of a DB instance once it is purchased. Exercise caution when selecting a region.
DB Instance Name	The DB instance name can be 4 to 64 characters long. It must start with a letter and can contain only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_). If you buy multiple DB instances, you can only enter 4 to 49 characters to set the DB instance name, and then the system automatically appends a date, time, and serial number to the end of the instance names (format: *instance_name-MMDD-HHmmss-SN*). After the DB instance is created, you can change its name. For details, see **Modifying the DB Instance Name**.
Database Type	Community Edition
DB Instance Type	Select **Cluster**. A cluster instance includes three types of nodes: mongos, shard, and config. Each shard and config is a three-node replica set to ensure high availability.
Compatible MongoDB Version	• 4.0 • 3.4 • 3.2
CPU Type	Currently, DDS supports two CPU architectures: x86 and Kunpeng. The two architectures have similar capabilities and performance, both of which can meet your service requirements. For details about the instance types, versions, and specifications supported by the two CPU architectures, see **DB Instance Specifications**.

Parameter	Description
Resource Type	If you use DeC, this parameter is displayed. EVS and DSS disks are provided based on whether storage resources are exclusively used. DSS disks provide dedicated storage resources. ● If you have applied for a storage pool on the DSS page, click the **DSS** tab and create disks in the obtained storage pool. ● If you have not applied for an exclusive storage pool, click the **EVS** disk tab. Then, the created disks use public storage resources.
Storage Type	If you do not use DeC, the storage type is ultra-high I/O by default. For DeC users, the supported storage types vary depending on the selected resource type. ● If you select **EVS** for **Resource Type**, **Storage Type** is set to **Ultra-high I/O**. ● If you select **DSS** for **Resource Type**, **Storage Type** can be set to **Common I/O**, **High I/O**, or **Ultra-high I/O**.
Storage Pool	This option is displayed only when you select **DSS** for **Resource Type**. The storage pool is physically isolated from other pools and is secure.
Storage Engine	WiredTiger
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 an internal network. Currently, instances can be deployed in a single AZ or three AZs. ● If you want to deploy an instance in a single AZ, select one AZ. ● If you want to deploy an instance across AZs for disaster recovery, select three AZs. In this deployment mode, the nodes are evenly distributed in the three AZs.

Parameter	Description
Disk Encryption	• **Disabled**: Disable the encryption function. • **Enabled**: Enable the encryption function. 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 a DB instance is created, the disk encryption status and the key cannot be changed. The backup data stored in OBS is not encrypted. – The key cannot be disabled, deleted, or frozen when being used. Otherwise, the database becomes unavailable. – For details about how to create a key, see the "Creating a CMK" section in the *Data Encryption Workshop User Guide*.

Figure 2-7 Instance specifications

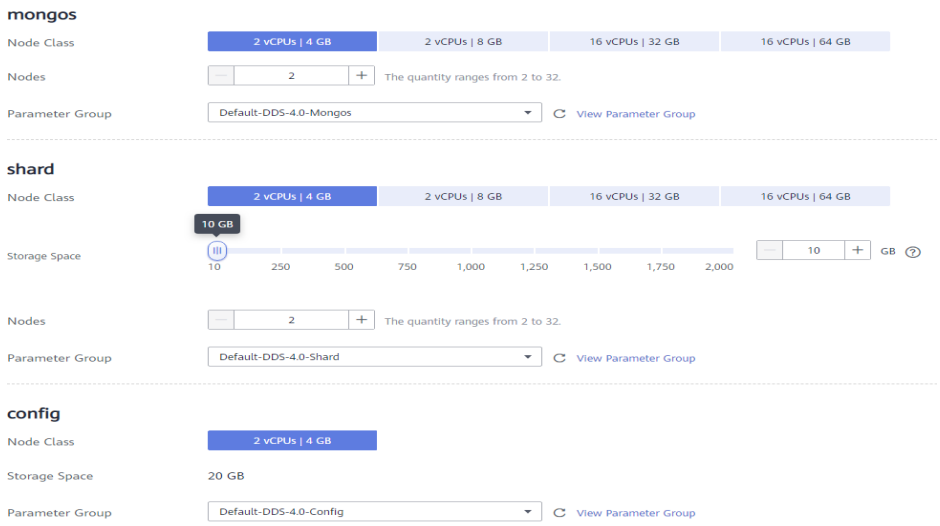


Table 2-11 Specifications

Parameter	Description
Specifications	In the x86 CPU architecture, the following specifications can be selected to suit different application scenarios: General-purpose (s6), Enhanced (c3), and Enhanced II (c6). For details about the supported DB instance specifications, see **DB Instance Specifications**.
Dedicated Cloud	If you use DeC, this parameter is displayed. For details about DB instance specifications in your DeC, see **Database Instance Specifications**.

Parameter	Description
mongos class	For details about the mongos CPU and memory, see **DB Instance Specifications**. After a DB instance is created, you can change its CPU and memory. For details, see **Changing the CPU or Memory of a Cluster DB Instance**.
mongos quantity	The number of mongos nodes. The value ranges from 2 to 32. After a DB instance is created, you can add mongos nodes if necessary. For details, see section **Adding Cluster Instance Nodes**.
mongos parameter group	The parameters that apply to the mongos nodes. After a DB instance is created, you can change the parameter group of a node to bring out the best performance. For details, see **Editing a Parameter Group**.
shard class	For details about the shard CPU and memory, see **DB Instance Specifications**. After a DB instance is created, you can change its CPU and memory. For details, see **Changing the CPU or Memory of a Cluster DB Instance**.
shard storage space	The value ranges from 10 GB to 2000 GB and must be a multiple of 10. After a DB instance is created, you can scale up its storage space. For details, see **Scaling Up Storage Space**.
shard quantity	The number of shard nodes. The shard node stores user data but cannot be accessed directly. The value ranges from 2 to 32. After a DB instance is created, you can add shard nodes if necessary. For details, see **Adding Cluster Instance Nodes**.
shard parameter group	The parameters that apply to the shard nodes. After a DB instance is created, you can change the parameter group of a node to bring out the best performance. For details, see **Editing a Parameter Group**.
config class	The CPU and memory of a config node. The config node stores the DB instance configurations but cannot be accessed directly. For details, see **DB Instance Specifications**.
config storage space	The storage space is 20 GB and cannot be scaled up.
config parameter group	The parameters that apply to the config nodes. After a DB instance is created, you can change the parameter group of a node to bring out the best performance. For details, see **Editing a Parameter Group**.

Figure 2-8 Network and database configuration

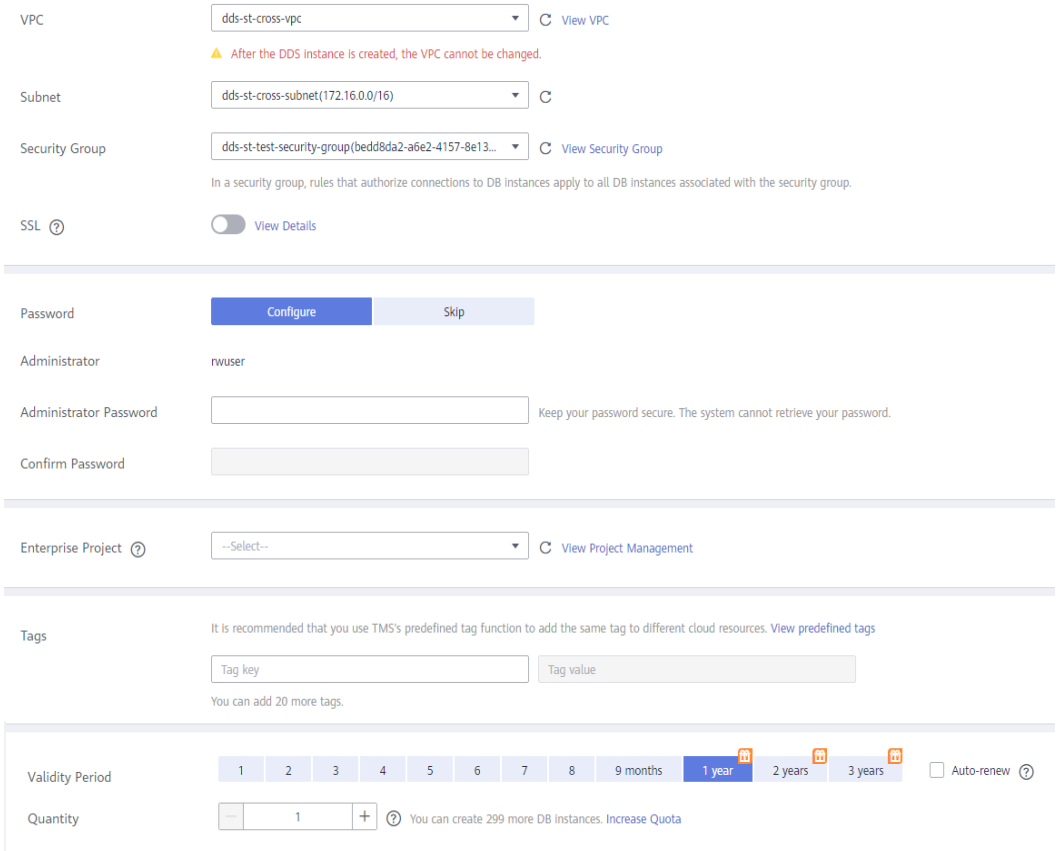


Table 2-12 Network

Parameter	Description
VPC	The VPC where your DB instances are located. A VPC isolates networks for different services, so you can easily manage and configure internal networks and change network configuration. For details about how to create a VPC, see section "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 allocates resources to 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 network security. After the instance is created, you can change the private IP address assigned by the subnet. For details, see **Changing a Private IP Address**.

Parameter	Description
Security Group	A security group controls access between DDS and other services for security. If there are no security groups available, DDS allocates resources to you by default. **NOTE** Ensure that the security group rule you set allows clients to access DB instances. For example, select the TCP protocol with inbound direction, input the default port number **8635**, and enter a subnet IP address or select a security group that the DB instance belongs to.
SSL	Secure Sockets Layer (SSL) certificates set up encrypted connections between clients and servers, preventing data from being tampered with or stolen during transmission. You can enable SSL to improve data security. After a DB instance is created, you can connect to it using SSL.
IPv6	Before enabling IPv6, ensure that IPv6 has been enabled for the VPC and subnet where the DB instance is located. For details about the application scenarios and procedures for enabling IPv6 for the VPC and subnet, see **IPv4 and IPv6 Dual-Stack Network**. After IPv6 is enabled, the DB instance can run in dual-stack mode. It means that the DB instance can use both the IPv4 address and IPv6 address. The DB instance can access the Internet using either IPv4 or IPv6 addresses, and the communications are independent of each other.

Table 2-13 Database configuration

Parameter	Description
Password	• Configure Enter and confirm the administrator password for connecting to the DB instance. • Skip Set the administrator password later. When you need to connect to the DB instance, locate the DB instance and click **Reset Password** in the **Operation** column to set a password for connecting to the DB instance.
Administrator	The default account is **rwuser**.
Administrator Password	Set a password for the administrator. The password is a string of 8 to 32 characters. It must be a combination of uppercase letters, lowercase letters, digits, and special characters. You can also use the following special characters: ~!@#%^*-_=+? Keep this password secure. If lost, the system cannot retrieve it for you.

Parameter	Description
Confirm Password	Enter the administrator password again.
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**. 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 the *Enterprise Management User Guide*.

Table 2-14 Tag

Parameter	Description
Tags	This setting is optional. Adding tags helps you better identify and manage your DB instances. Up to 20 tags can be added for a DB instance. A tag is composed of a key-value pair. • Key: Mandatory if the DB instance is going to be tagged – Each tag key must be unique for each DB instance. – A tag key consists of up to 36 characters. – The key can only consist of digits, letters, underscores (_), and hyphens (-). • Value: Optional if the DB instance is going to be tagged – The value consists of up to 43 characters. – The value can only consist of digits, letters, underscores (_), dots (.), and hyphens (-). After a DB instance is created, you can view its tag details on the **Tags** tab. In addition, you can add, modify, and delete tags for existing DB instances. For details, see **Tag**.

Table 2-15 Required duration and quantity

Parameter	Description
Validity Period	Sets the service duration if you select the **Yearly/Monthly** billing mode. The service duration ranges from one month to three years.

Parameter	Description
Auto-renew	• By default, this option is not selected. • If you select this option, the auto-renew cycle is determined by the selected required duration.
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 increasing the quota as prompted. The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

NOTE

DB instance performance is determined by how you configure it during the creation. The hardware configuration items that can be selected include the node class and storage space.

Step 4 On the displayed page, confirm the DB instance information.

- Yearly/Monthly
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify your settings, click **Pay Now** to go to the payment page and complete the payment.
- Pay-per-use
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, click **Submit** to start the instance creation.

Step 5 After a DDS DB instance is created, you can view and manage it on the **Instance Management** 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**.
- DDS enables the automated backup policy by default. After a DB instance is created, you can modify or disable the automated backup policy. An automated full backup is immediately triggered after the creation of a DB instance.
- The default DDS port is 8635, but this port can be modified if necessary. If you change the port, you need to add the security group rule to enable access.
- The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

----End

2.3.3 Step 2: Set a Security Group

Scenarios

This section explains how to add a security group rule to control access to and from the DDS DB instances associated with a security group.

Precautions

The default security group rule allows all outgoing data packets. ECSs and DDS DB instances in the same security group can access each other. After a security group is created, you can create different rules for that security group, which allows you to control access to the DB instances that are in it.

To access a DB instance in a security group from a source outside of that group, you need to create an inbound rule.

For details about the constraints on using security groups, see **Security Group Overview**.

Procedure

Step 1 On the **Instance Management** page, click the target cluster instance.

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

Step 3 In the **Security Group** area, on the **Inbound Rules** tab, click **Add Rule**. In the displayed **Add Inbound Rule** dialog box, set required parameters to add inbound rules. On the **Outbound Rules** tab, click **Add Rule**. In the displayed **Add Outbound Rule** dialog box, set required parameters to add outbound rules.

You can click ⊕ to add more rules.

Figure 2-9 Add Inbound Rule

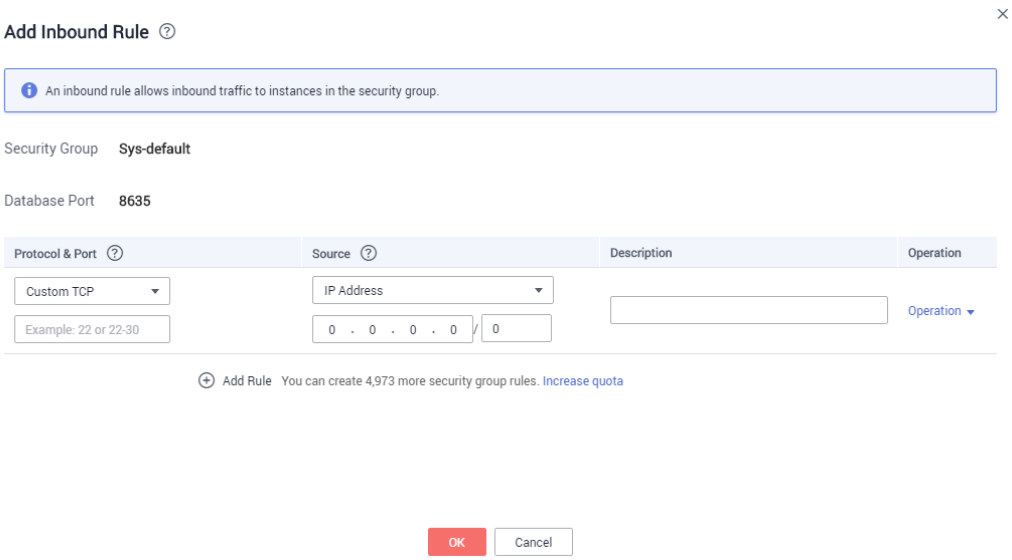
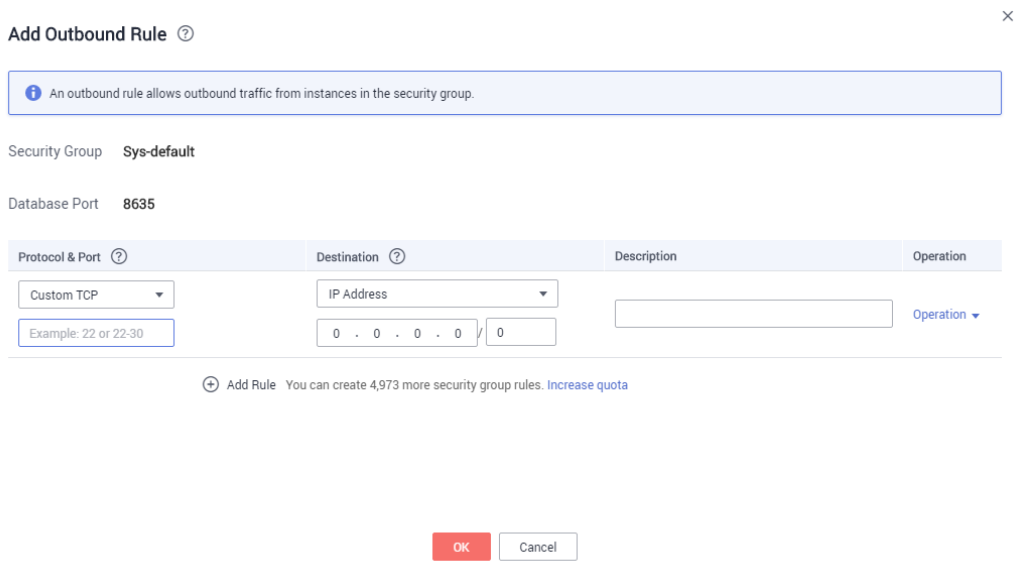


Figure 2-10 Add Outbound Rule



Step 4 Add a security group rule as prompted.

Table 2-16 Parameter description

Parameter	Description	Value Example
Protocol	The network protocol required for access. You can allow all protocols or specify a specific protocol, TCP, UDP, ICMP, and SSH.	TCP
Port	Specifies the port that allows the access to ECSs or external devices. Common ports are listed in **Common Ports Used by ECSs**.	8635
Source/ Destination	Specifies the supported IP address and security group that the rule applies to. • **IP address**: The IP address or subnet that the rule applies to. Single IP addresses must be expressed using slash notation. – Single IP address: xxx.xxx.xxx.xxx/32 (IPv4) – Subnet: xxx.xxx.xxx.0/24 – All IP addresses: 0.0.0.0/0 • **Security group**: A security group that access will be allowed from. ECSs in this security group will be granted access to DDS instance in the current security group.	• 192.168.10.0/24 • default

Step 5 Click **OK**.

----End

2.3.4 Step 3: Connect to a Cluster Instance Over Private Networks

Scenarios

This section describes how to connect to a cluster instance using the MongoDB client over private networks.

The MongoDB client can connect to a DB instance with a common connection or an encrypted connection (SSL). To improve data transmission security, you are advised to connect to DB instances using the SSL connection.

Different OS scenarios: The following uses Linux ECS and Window client as an example.

For best practices about connections to DB instances over private networks, see **Connecting to a DB Instance Through an ECS**.

Constraints

For details about constraints on connecting to a cluster DB instance over private networks, see **Constraints**.

Prerequisites

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

   NOTE

   If you use a **connection address** to connect to a cluster instance, download the MongoDB client of version later than 4.0.

Connecting to a DB Instance Using the MongoDB Client (SSL)

Step 1 On the **Instance Management** page, click the target DB instance.

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

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

Step 5 Connect to the DB instance in the directory where the MongoDB client is located.

- Method 1: Using Linux commands

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

  Enter the database account password when prompted:

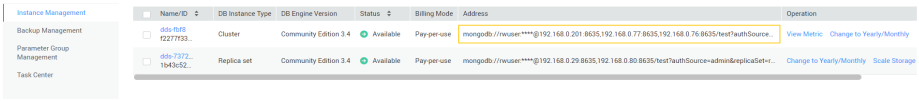
  ```
  Enter password:
  ```

- Method 2: Using the private connection address. Enter the IP addresses and ports based on the number of DB instance nodes.

  ./mongo mongodb://
  rwuser:**@***<DB_HOST>***:***<DB_PORT>***,***<DB_HOST>***:***<DB_PORT>***/test?authSource=admin --ssl --sslCAFile** *<FILE_PATH>* **--sslAllowInvalidHostnames**

  The connection information can be obtained in the **Address** column on the **Instance Management** page.

  Figure 2-11 Connections

  A connection address indicates that one of the mongos nodes will be randomly connected. If you use this method to connect to a DB instance, use the MongoDB client of version later than 4.0.

NOTE

- **DB_HOST** indicates the IP address of the remotely connected DB instance. Obtain the value from the **Private IP Address** column in the node list on the **Connections** page.
- **DB_PORT** indicates the port number. Obtain the value from **Database Port** in the **Basic Information** area on the **Connections** page.
- **DB_USER** indicates the database account name. The default value is **rwuser**.
- ********** indicates the password of the database account. If you use the connection address to connect to a DB instance:
  - If the password contains the at sign (@), change @ to %40.
  - If the password contains the exclamation mark (!), add an escape character (\) before the exclamation mark (!).
- **FILE_PATH** indicates the path where the root certificate is stored.

- Connect to the instance using Linux commands. The following is an example command:

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

- Connect to the DB instance using the private connection address. The following is an example command:

  ./mongo mongodb://rwuser:**@192.168.1.6:8635/test?authSource=admin --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames**

Step 6 Check the connection result. If the following information is displayed, the connection is successful.

```
mongos>
```

----End

Connecting to a DB Instance Using the MongoDB Client (Non-SSL)

NOTICE

If you connect to a DB instance using this method, you need to disable the SSL connection. For details, see **Enabling or Disabling SSL**.

Step 1 Connect to the ECS.

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

- Method 1: Using Linux commands

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

  Enter the database account password when prompted:

  ```
  Enter password:
  ```

- Method 2: Using the private connection address. Enter the IP addresses and ports based on the number of DB instance nodes.

  ./mongo mongodb://rwuser:**@**<*DB_HOST1*>**:**<*DB_PORT1*>**,**<*DB_HOST2*>**:**<*DB_PORT2*>**/test?authSource=admin**

  The connection information can be obtained in the **Address** column on the **Instance Management** page.

  A connection address indicates that one of the mongos nodes will be randomly connected. If you use this method to connect to a DB instance, use the MongoDB client of version later than 4.0.

NOTE

- **DB_HOST** indicates the IP address of the remotely connected DB instance. Obtain the value from the **Private IP Address** column in the node list on the **Connections** page.
- **DB_PORT** indicates the port number. Obtain the value from **Database Port** in the **Basic Information** area on the **Connections** page.
- **DB_USER** indicates the database account name. The default value is **rwuser**.
- ********** indicates the password of the database account. If you use the connection address to connect to a DB instance:
  - If the password contains the at sign (@), change @ to %40.
  - If the password contains the exclamation mark (!), add an escape character (\) before the exclamation mark (!).

- Connect to the instance using Linux commands. The following is an example command:

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

- Connect to the DB instance using the private connection address. The following is an example command:

  ./mongo mongodb://rwuser:**@192.168.1.6:8635/test?authSource=admin**

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

```
mongos>
```

----End

2.4 Connecting to a Cluster Instance Over Public Networks

2.4.1 Overview

Scenarios

This section describes how to buy a cluster instance on the management console, set a security group, bind an EIP, and connect to a cluster instance over public networks.

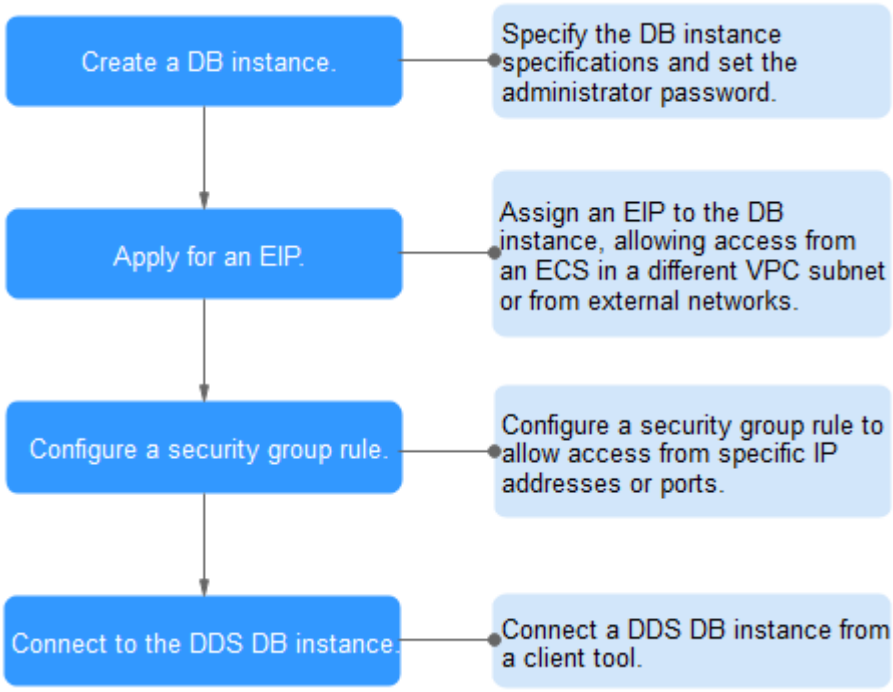
Process

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

- **Step 1: Buy a Cluster Instance**
- **Step 2: Bind an EIP**
- **Step 3: Set a Security Group**
- **Step 4: Connect to a Cluster Instance Over Public Networks**

The following describes the steps from creating a DB instance to using it.

Figure 2-12 Accessing DB instances from a public network



2.4.2 Step 1: Buy a Cluster Instance

Scenarios

This section describes how to create a Community Edition cluster instance on the DDS management console. Currently, DDS cluster instance of Community Edition supports the yearly/monthly and pay-per-use billing modes. DDS allows you to tailor your compute resources and storage space to your business needs.

You can use your account to create up to 10 cluster instances.

Prerequisites

- You have registered a HUAWEI CLOUD account.
- Your account balance is greater than or equal to ¥0.

Procedure

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

Step 2 On the **Instance Management** page, click Buy DB Instance.

Step 3 On the displayed page, select a billing mode, select your DB instance specifications and click **Next**.

Figure 2-13 Billing mode and basic information

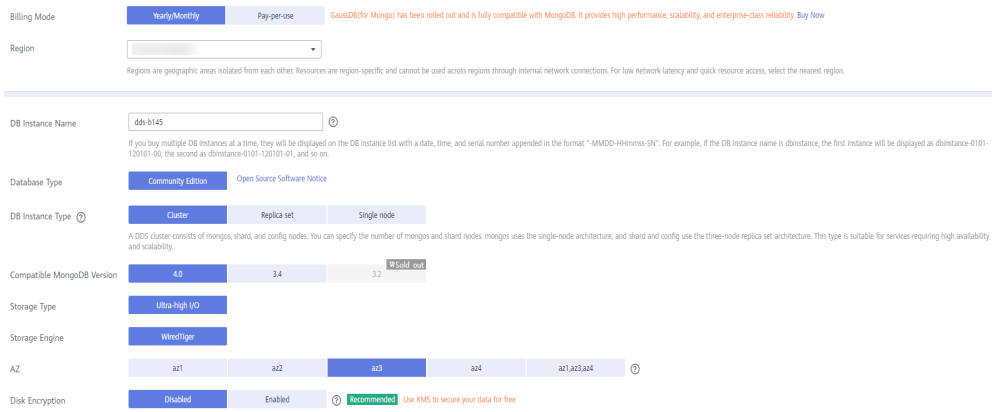


Table 2-17 Billing mode

Parameter	Description
Billing Mode	Select a billing mode, **Yearly/Monthly** or **Pay-per-use**. • Yearly/Monthly – You need to set **Validity Period** as required. Then, the system deducts the fees incurred at one time from your account based on the service price. – When you renew a yearly/monthly DB instance, you can change its billing mode from yearly/monthly to pay-per-use based on your service requirements. For details, see **Changing Yearly/Monthly Instances to a Pay-per-Use**. **NOTE** DB instances paid in yearly/monthly mode cannot be deleted. They support only resource unsubscription. For details, see section **Unsubscribing from a Yearly/Monthly DB Instance**. • Pay-per-use – You do not need to set **Validity Period** because the system deducts the fees incurred from your account based on the service duration. – If you want to use a DB instance at a low cost for a long period of time, you can change its billing mode from pay-per-use to yearly/monthly. For details, see **Changing the Billing Mode in Batches**.

Table 2-18 Basic information

Parameter	Description
Region	A region where the tenant is located. It can be changed in the upper left corner. **NOTE** DB instances deployed in different regions cannot communicate with each other through a private network, and you cannot change the region of a DB instance once it is purchased. Exercise caution when selecting a region.
DB Instance Name	The DB instance name can be 4 to 64 characters long. It must start with a letter and can contain only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_). If you buy multiple DB instances, you can only enter 4 to 49 characters to set the DB instance name, and then the system automatically appends a date, time, and serial number to the end of the instance names (format: *instance_name-MMDD-HHmmss-SN*). After the DB instance is created, you can change its name. For details, see **Modifying the DB Instance Name**.
Database Type	Community Edition
DB Instance Type	Select **Cluster**. A cluster instance includes three types of nodes: mongos, shard, and config. Each shard and config is a three-node replica set to ensure high availability.
Compatible MongoDB Version	• 4.0 • 3.4 • 3.2
CPU Type	Currently, DDS supports two CPU architectures: x86 and Kunpeng. The two architectures have similar capabilities and performance, both of which can meet your service requirements. For details about the instance types, versions, and specifications supported by the two CPU architectures, see **DB Instance Specifications**.

Parameter	Description
Resource Type	If you use DeC, this parameter is displayed. EVS and DSS disks are provided based on whether storage resources are exclusively used. DSS disks provide dedicated storage resources. ● If you have applied for a storage pool on the DSS page, click the **DSS** tab and create disks in the obtained storage pool. ● If you have not applied for an exclusive storage pool, click the **EVS** disk tab. Then, the created disks use public storage resources.
Storage Type	If you do not use DeC, the storage type is ultra-high I/O by default. For DeC users, the supported storage types vary depending on the selected resource type. ● If you select **EVS** for **Resource Type**, **Storage Type** is set to **Ultra-high I/O**. ● If you select **DSS** for **Resource Type**, **Storage Type** can be set to **Common I/O**, **High I/O**, or **Ultra-high I/O**.
Storage Pool	This option is displayed only when you select **DSS** for **Resource Type**. The storage pool is physically isolated from other pools and is secure.
Storage Engine	WiredTiger
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 an internal network. Currently, instances can be deployed in a single AZ or three AZs. ● If you want to deploy an instance in a single AZ, select one AZ. ● If you want to deploy an instance across AZs for disaster recovery, select three AZs. In this deployment mode, the nodes are evenly distributed in the three AZs.

Parameter	Description
Disk Encryption	• **Disabled**: Disable the encryption function. • **Enabled**: Enable the encryption function. 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 a DB instance is created, the disk encryption status and the key cannot be changed. The backup data stored in OBS is not encrypted. – The key cannot be disabled, deleted, or frozen when being used. Otherwise, the database becomes unavailable. – For details about how to create a key, see the "Creating a CMK" section in the *Data Encryption Workshop User Guide*.

Figure 2-14 Instance specifications

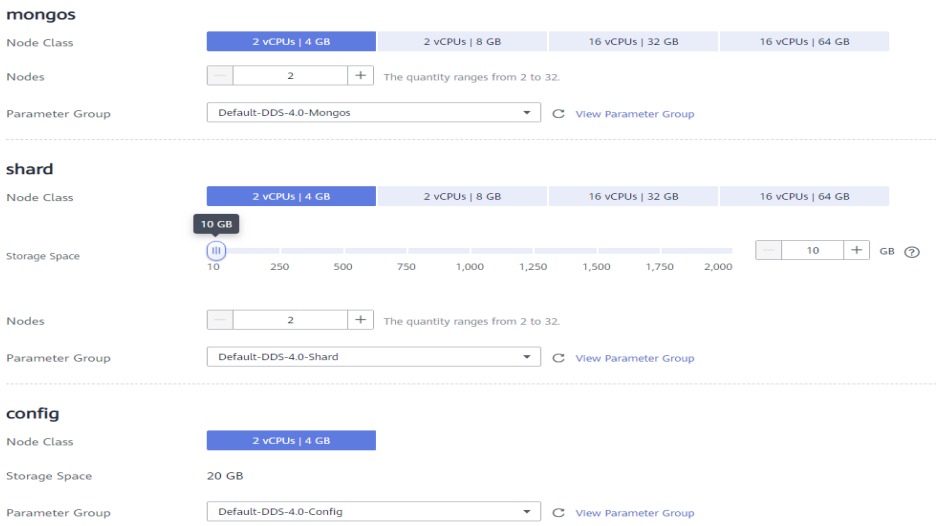


Table 2-19 Specifications

Parameter	Description
Specifications	In the x86 CPU architecture, the following specifications can be selected to suit different application scenarios: General-purpose (s6), Enhanced (c3), and Enhanced II (c6). For details about the supported DB instance specifications, see **DB Instance Specifications**.
Dedicated Cloud	If you use DeC, this parameter is displayed. For details about DB instance specifications in your DeC, see **Database Instance Specifications**.

Parameter	Description
mongos class	For details about the mongos CPU and memory, see **DB Instance Specifications**. After a DB instance is created, you can change its CPU and memory. For details, see **Changing the CPU or Memory of a Cluster DB Instance**.
mongos quantity	The number of mongos nodes. The value ranges from 2 to 32. After a DB instance is created, you can add mongos nodes if necessary. For details, see section **Adding Cluster Instance Nodes**.
mongos parameter group	The parameters that apply to the mongos nodes. After a DB instance is created, you can change the parameter group of a node to bring out the best performance. For details, see **Editing a Parameter Group**.
shard class	For details about the shard CPU and memory, see **DB Instance Specifications**. After a DB instance is created, you can change its CPU and memory. For details, see **Changing the CPU or Memory of a Cluster DB Instance**.
shard storage space	The value ranges from 10 GB to 2000 GB and must be a multiple of 10. After a DB instance is created, you can scale up its storage space. For details, see **Scaling Up Storage Space**.
shard quantity	The number of shard nodes. The shard node stores user data but cannot be accessed directly. The value ranges from 2 to 32. After a DB instance is created, you can add shard nodes if necessary. For details, see **Adding Cluster Instance Nodes**.
shard parameter group	The parameters that apply to the shard nodes. After a DB instance is created, you can change the parameter group of a node to bring out the best performance. For details, see **Editing a Parameter Group**.
config class	The CPU and memory of a config node. The config node stores the DB instance configurations but cannot be accessed directly. For details, see **DB Instance Specifications**.
config storage space	The storage space is 20 GB and cannot be scaled up.
config parameter group	The parameters that apply to the config nodes. After a DB instance is created, you can change the parameter group of a node to bring out the best performance. For details, see **Editing a Parameter Group**.

Figure 2-15 Network and database configuration

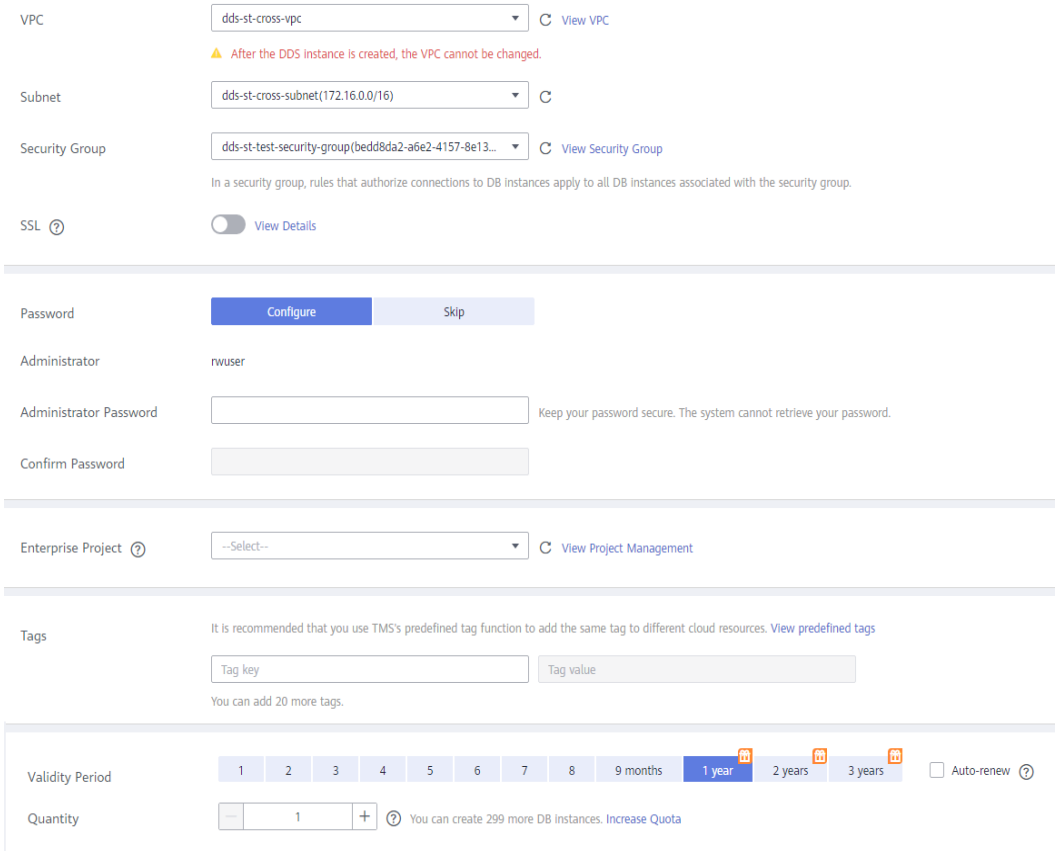


Table 2-20 Network

Parameter	Description
VPC	The VPC where your DB instances are located. A VPC isolates networks for different services, so you can easily manage and configure internal networks and change network configuration. For details about how to create a VPC, see section "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 allocates resources to 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 network security. After the instance is created, you can change the private IP address assigned by the subnet. For details, see **Changing a Private IP Address**.

Parameter	Description
Security Group	A security group controls access between DDS and other services for security. If there are no security groups available, DDS allocates resources to you by default. **NOTE** Ensure that the security group rule you set allows clients to access DB instances. For example, select the TCP protocol with inbound direction, input the default port number **8635**, and enter a subnet IP address or select a security group that the DB instance belongs to.
SSL	Secure Sockets Layer (SSL) certificates set up encrypted connections between clients and servers, preventing data from being tampered with or stolen during transmission. You can enable SSL to improve data security. After a DB instance is created, you can connect to it using SSL.
IPv6	Before enabling IPv6, ensure that IPv6 has been enabled for the VPC and subnet where the DB instance is located. For details about the application scenarios and procedures for enabling IPv6 for the VPC and subnet, see **IPv4 and IPv6 Dual-Stack Network**. After IPv6 is enabled, the DB instance can run in dual-stack mode. It means that the DB instance can use both the IPv4 address and IPv6 address. The DB instance can access the Internet using either IPv4 or IPv6 addresses, and the communications are independent of each other.

Table 2-21 Database configuration

Parameter	Description
Password	• Configure Enter and confirm the administrator password for connecting to the DB instance. • Skip Set the administrator password later. When you need to connect to the DB instance, locate the DB instance and click **Reset Password** in the **Operation** column to set a password for connecting to the DB instance.
Administrator	The default account is **rwuser**.
Administrator Password	Set a password for the administrator. The password is a string of 8 to 32 characters. It must be a combination of uppercase letters, lowercase letters, digits, and special characters. You can also use the following special characters: ~!@#%^*-_=+? Keep this password secure. If lost, the system cannot retrieve it for you.

Parameter	Description
Confirm Password	Enter the administrator password again.
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**. 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 the *Enterprise Management User Guide*.

Table 2-22 Tag

Parameter	Description
Tags	This setting is optional. Adding tags helps you better identify and manage your DB instances. Up to 20 tags can be added for a DB instance. A tag is composed of a key-value pair. • Key: Mandatory if the DB instance is going to be tagged – Each tag key must be unique for each DB instance. – A tag key consists of up to 36 characters. – The key can only consist of digits, letters, underscores (_), and hyphens (-). • Value: Optional if the DB instance is going to be tagged – The value consists of up to 43 characters. – The value can only consist of digits, letters, underscores (_), dots (.), and hyphens (-). After a DB instance is created, you can view its tag details on the **Tags** tab. In addition, you can add, modify, and delete tags for existing DB instances. For details, see **Tag**.

Table 2-23 Required duration and quantity

Parameter	Description
Validity Period	Sets the service duration if you select the **Yearly/Monthly** billing mode. The service duration ranges from one month to three years.

Parameter	Description
Auto-renew	• By default, this option is not selected. • If you select this option, the auto-renew cycle is determined by the selected required duration.
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 increasing the quota as prompted. The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

NOTE

DB instance performance is determined by how you configure it during the creation. The hardware configuration items that can be selected include the node class and storage space.

Step 4 On the displayed page, confirm the DB instance information.

- Yearly/Monthly
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify your settings, click **Pay Now** to go to the payment page and complete the payment.
- Pay-per-use
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, click **Submit** to start the instance creation.

Step 5 After a DDS DB instance is created, you can view and manage it on the **Instance Management** 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**.
- DDS enables the automated backup policy by default. After a DB instance is created, you can modify or disable the automated backup policy. An automated full backup is immediately triggered after the creation of a DB instance.
- The default DDS port is 8635, but this port can be modified if necessary. If you change the port, you need to add the security group rule to enable access.
- The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

----End

2.4.3 Step 2: Bind an EIP

Scenarios

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

Precautions

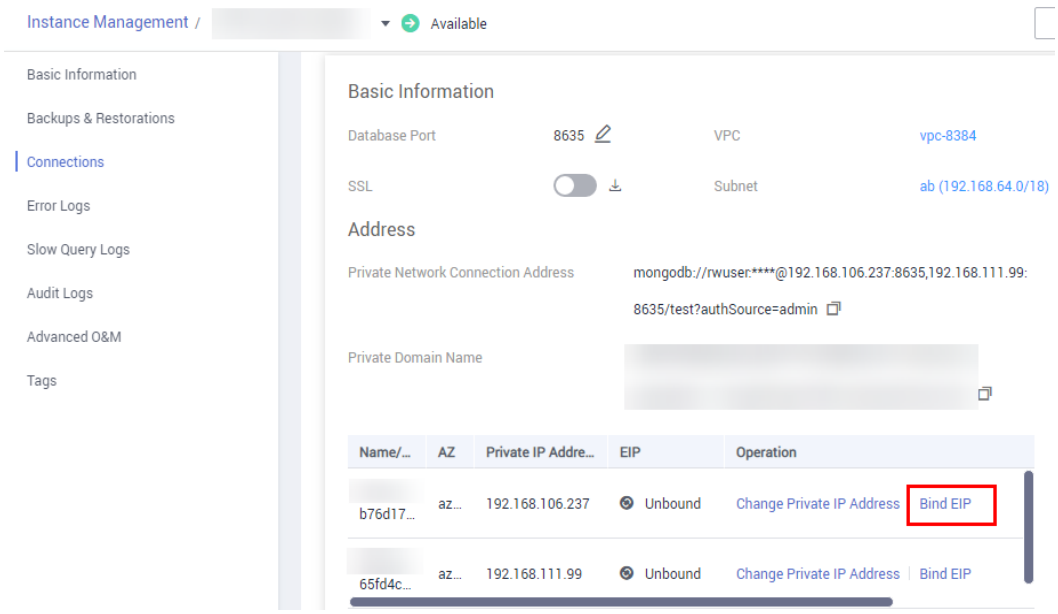
- Before accessing a database, you need to apply for an EIP on the VPC console. Then, add an inbound rule to allow the IP addresses or IP address ranges of ECSs. For details, see section **Step 3: Set a Security Group**.
- In the cluster instance, only mongos can be bound to an EIP. To change the EIP that has been bound to a node, you need to unbind it from the node first.

Binding an EIP

Step 1 On the **Instance Management** page, click the target cluster instance.

Step 2 In the navigation pane on the left, choose **Connections**. In the **Basic Information** area, locate the target mongos node and click **Bind EIP** in the **Operation** column.

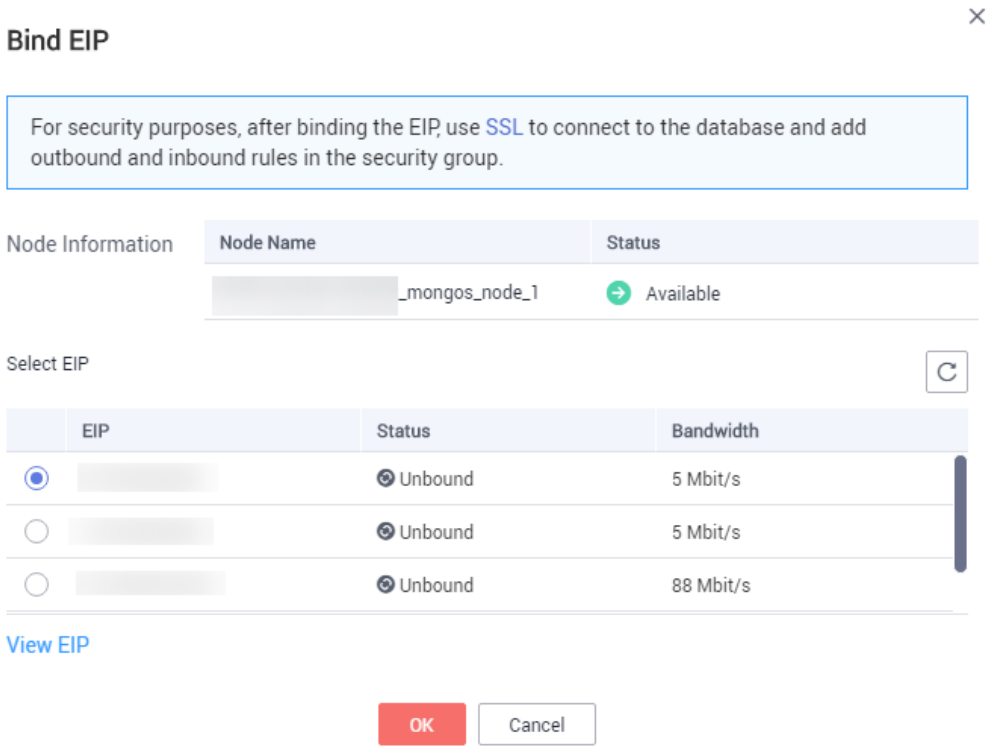
Figure 2-16 Binding an EIP



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

Step 3 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 2-17 Selecting an EIP



Step 4 In the **EIP** column on the **mongos** tab, view the EIP that is successfully bound.

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

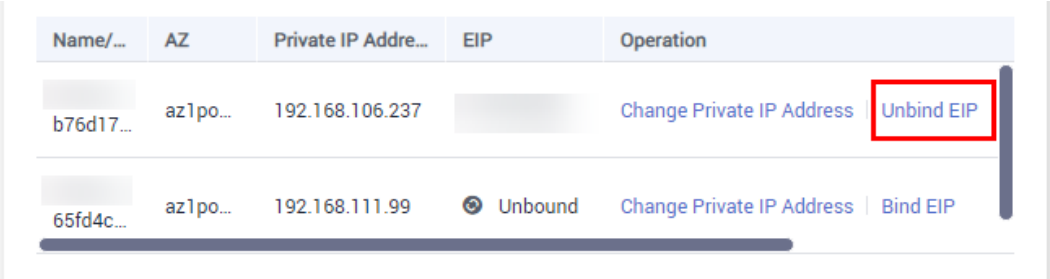
----End

Unbinding an EIP

Step 1 On the **Instance Management** page, click the target cluster instance.

Step 2 In the navigation pane on the left, choose **Connections**. In the **Basic Information** area, locate the target mongos node and click **Unbind EIP** in the **Operation** column.

Figure 2-18 Unbinding an EIP



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

Step 3 In the displayed dialog box, click **Yes**.

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

----End

2.4.4 Step 3: Set a Security Group

Scenarios

This section explains how to add a security group rule to control access to and from the DDS DB instances associated with a security group.

Precautions

The default security group rule allows all outgoing data packets. ECSs and DDS DB instances in the same security group can access each other. After a security group is created, you can create different rules for that security group, which allows you to control access to the DB instances that are in it.

To access a DB instance in a security group from a source outside of that group, you need to create an inbound rule.

For details about the constraints on using security groups, see **Security Group Overview**.

Procedure

Step 1 On the **Instance Management** page, click the target cluster instance.

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

Step 3 In the **Security Group** area, on the **Inbound Rules** tab, click **Add Rule**. In the displayed **Add Inbound Rule** dialog box, set required parameters to add inbound rules. On the **Outbound Rules** tab, click **Add Rule**. In the displayed **Add Outbound Rule** dialog box, set required parameters to add outbound rules.

You can click  to add more rules.

Figure 2-19 Add Inbound Rule

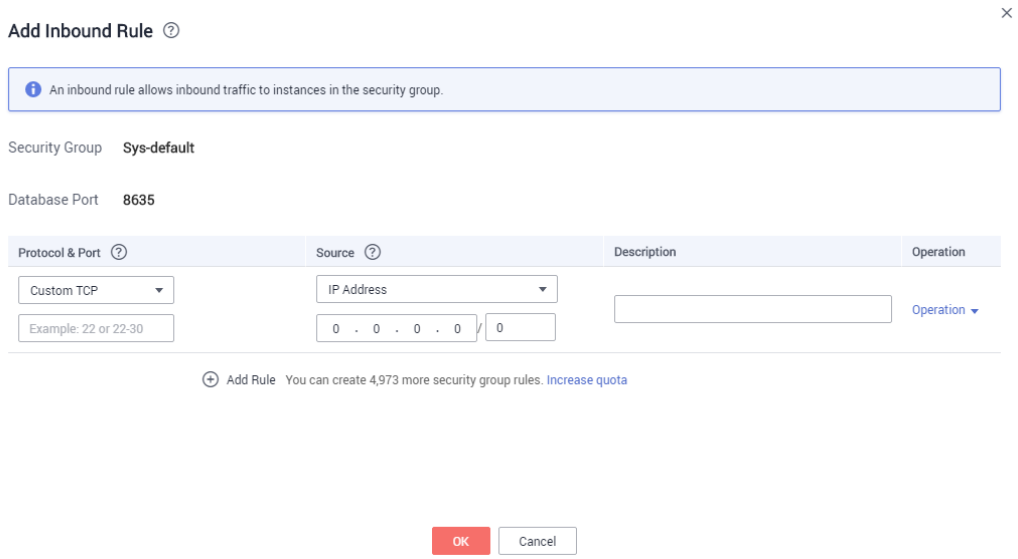
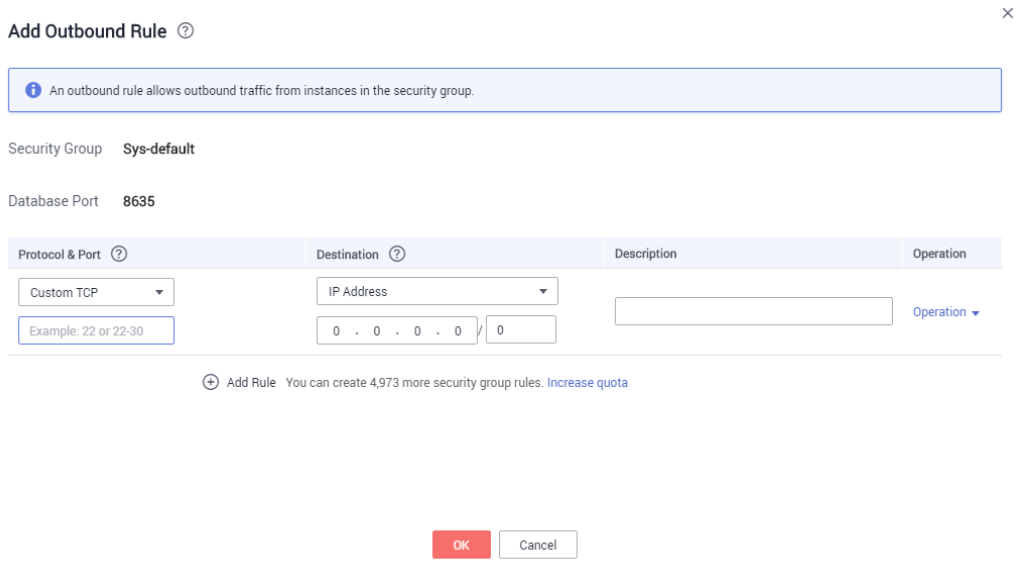


Figure 2-20 Add Outbound Rule



Step 4 Add a security group rule as prompted.

Table 2-24 Parameter description

Parameter	Description	Value Example
Protocol	The network protocol required for access. You can allow all protocols or specify a specific protocol, TCP, UDP, ICMP, and SSH.	TCP

Parameter	Description	Value Example
Port	Specifies the port that allows the access to ECSs or external devices. Common ports are listed in **Common Ports Used by ECSs**.	8635
Source/ Destination	Specifies the supported IP address and security group that the rule applies to. • **IP address**: The IP address or subnet that the rule applies to. Single IP addresses must be expressed using slash notation. – Single IP address: xxx.xxx.xxx.xxx/32 (IPv4) – Subnet: xxx.xxx.xxx.0/24 – All IP addresses: 0.0.0.0/0 • **Security group**: A security group that access will be allowed from. ECSs in this security group will be granted access to DDS instance in the current security group.	• 192.168.10.0/24 • default

Step 5 Click **OK**.

----End

2.4.5 Step 4: Connect to a Cluster Instance Over Public Networks

Scenarios

This section describes how to connect to a cluster instance using the MongoDB client and Robo 3T over public networks.

The MongoDB client and Robo 3T can connect to a DB instance with a common connection or an encrypted connection (SSL). To improve data transmission security, you are advised to connect to DB instances using the SSL connection.

Different OS scenarios: The following uses Linux ECS and Window client as an example.

For best practices about connections to a DB instance over public networks, see **Connecting to a DB Instance Through an EIP**.

Prerequisites

1. **Bind an EIP** to the cluster instance and **set security group rules** to ensure that the EIP can be accessed through the ECS or Robo 3T.
2. Install the MongoDB client or Robo 3T.

   MongoDB client

   a. For details on how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.

b. Install the MongoDB client on the ECS.

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

NOTE

If you use a **connection address** to connect to a cluster instance, download the MongoDB client of version later than 4.0.

Robo 3T

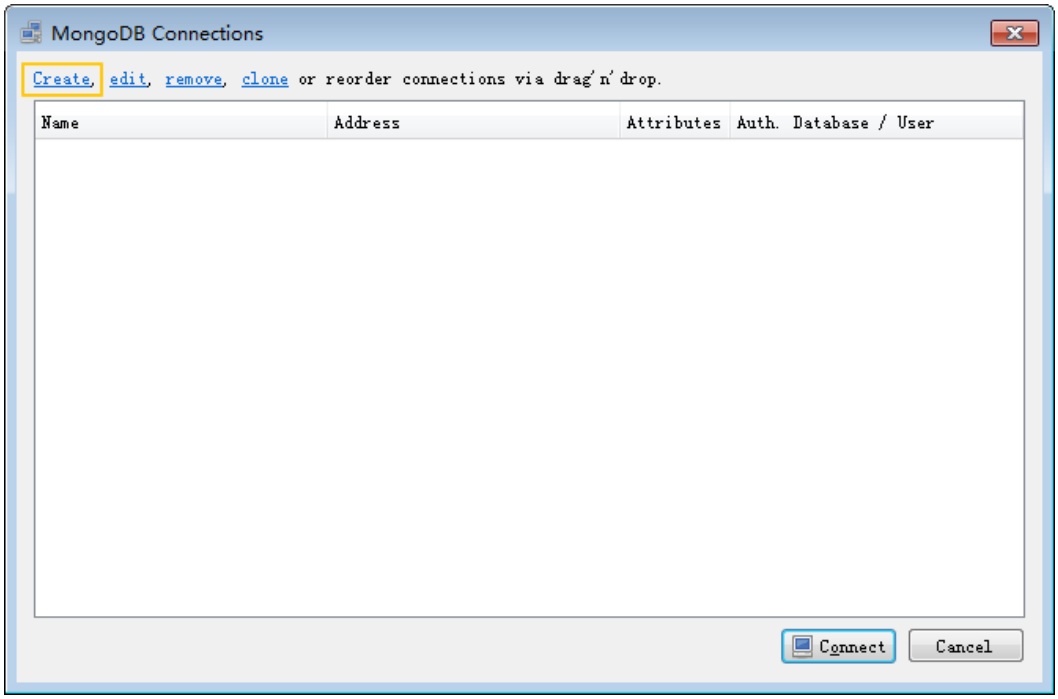
Install Robo 3T. For details, see **How Can I Install Robo 3T?**

3. If you select the SSL mode, download the SSL certificate on the DDS console.
   a. On the **Instance Management** page, click the target DB instance.
   b. In the navigation pane on the left, choose **Connections**.
   c. In the **Basic Information** area, click next to the **SSL** field.

Connecting to a DB Instance Using Robo 3T (SSL)

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

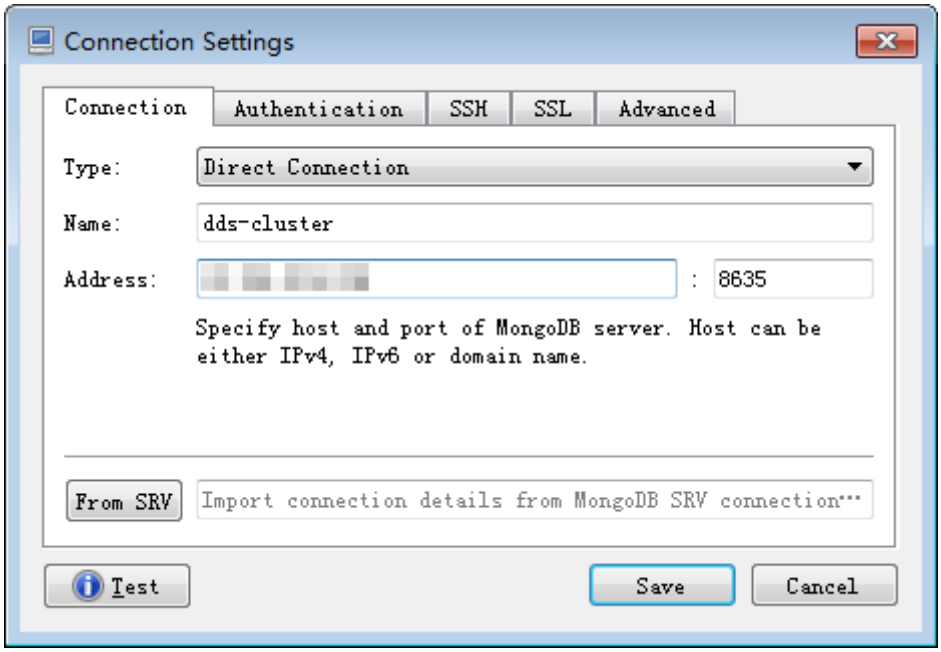
Figure 2-21 Connections



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

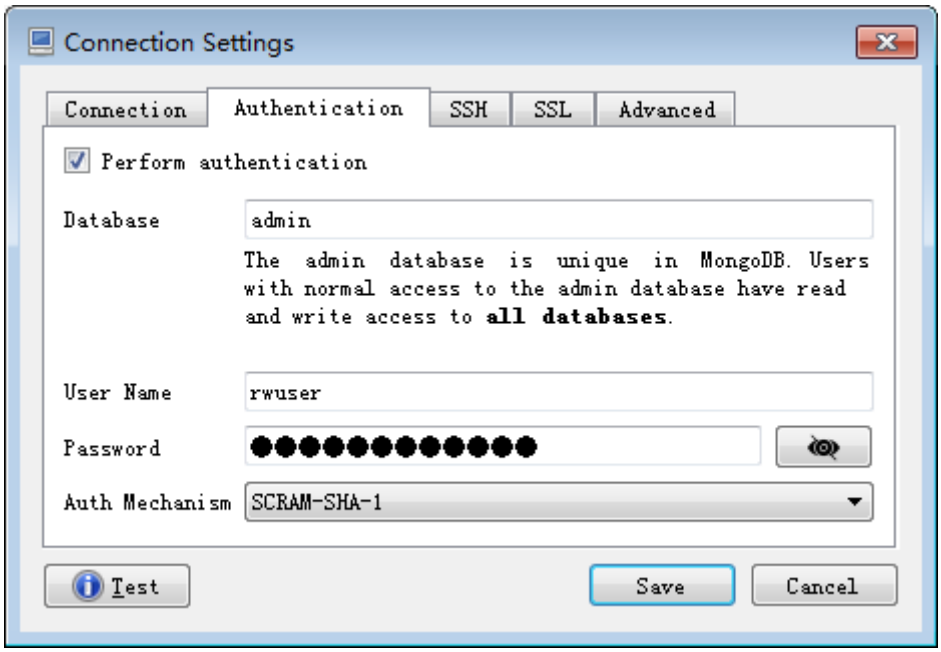
1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the DDS DB instance in the **Address** text box.

Figure 2-22 Connection



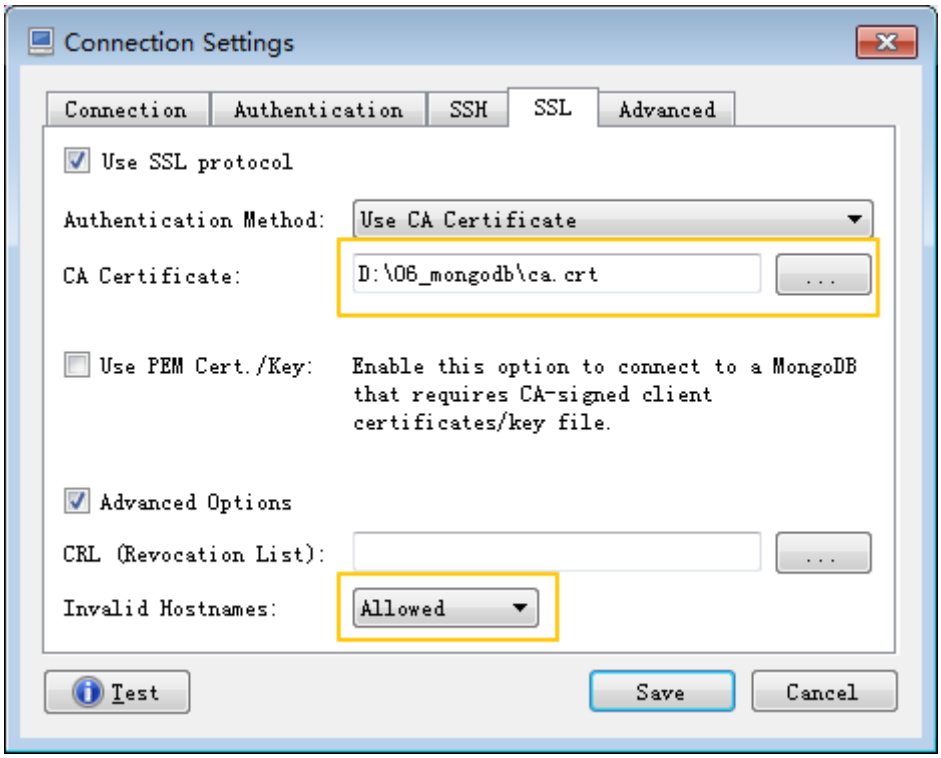
2. On the **Authentication** tab, set **Database** to **admin**, **User Name** to **rwuser**, and **Password** to the administrator password you set during the creation of the cluster instance.

Figure 2-23 Authentication



3. On the **SSL** tab, upload the SSL certificate and select **Allowed** for **Invalid Hostnames**.

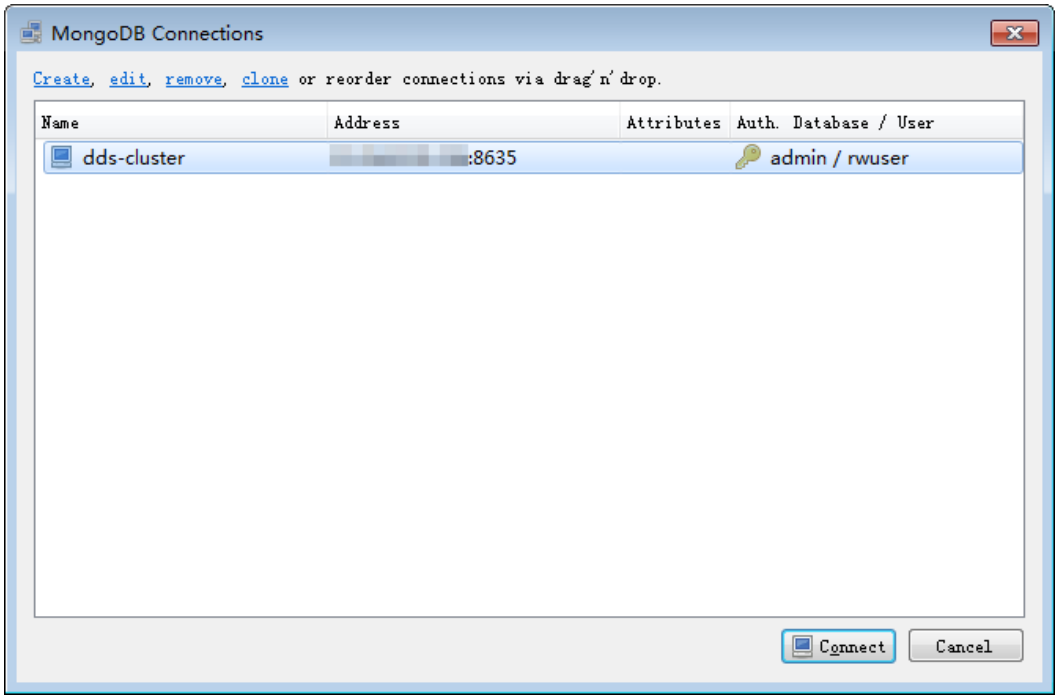
Figure 2-24 SSL



4. Click **Save**.

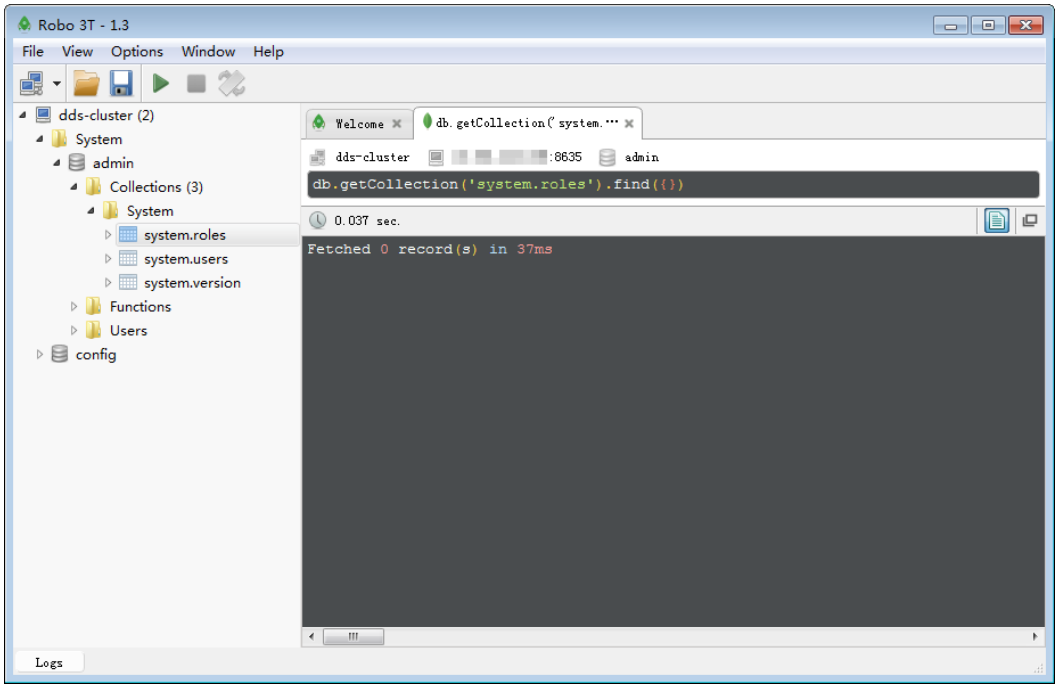
Step 3 On the **MongoDB Connections** page, click **Connect** to connect to the cluster instance.

Figure 2-25 Connections



Step 4 If the cluster instance is successfully connected, the page shown in **Figure 2-26** is displayed.

Figure 2-26 Connection succeeded



----End

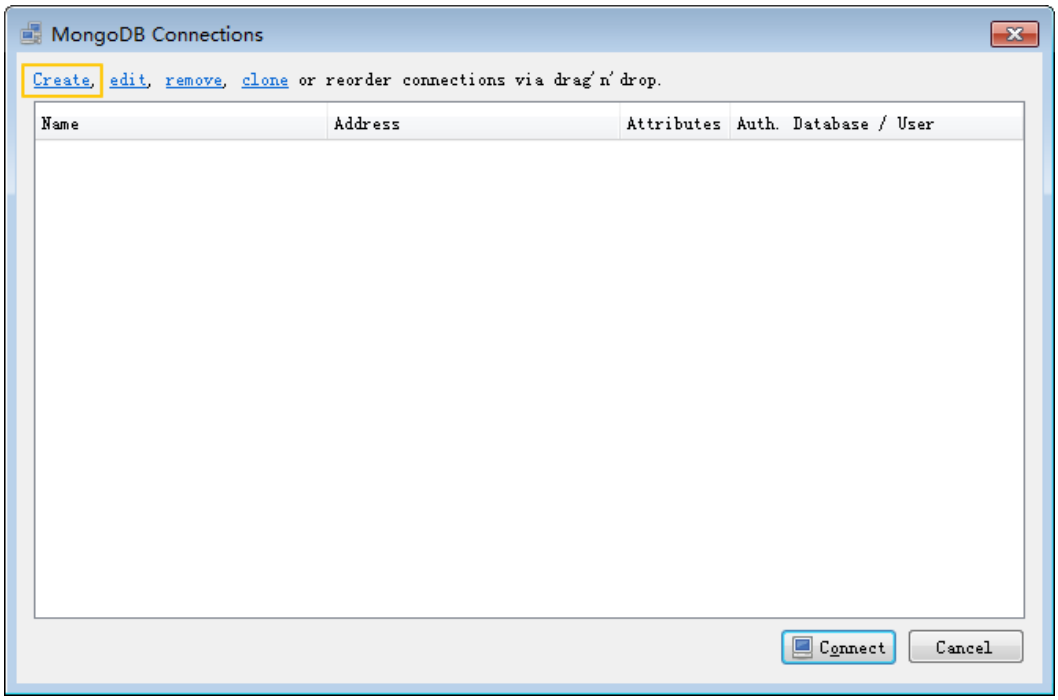
Connecting to a DB Instance Using Robo 3T (Non-SSL)

NOTICE

If you connect to a DB instance using this method, you need to disable the SSL connection. For details, see **Enabling or Disabling SSL**.

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

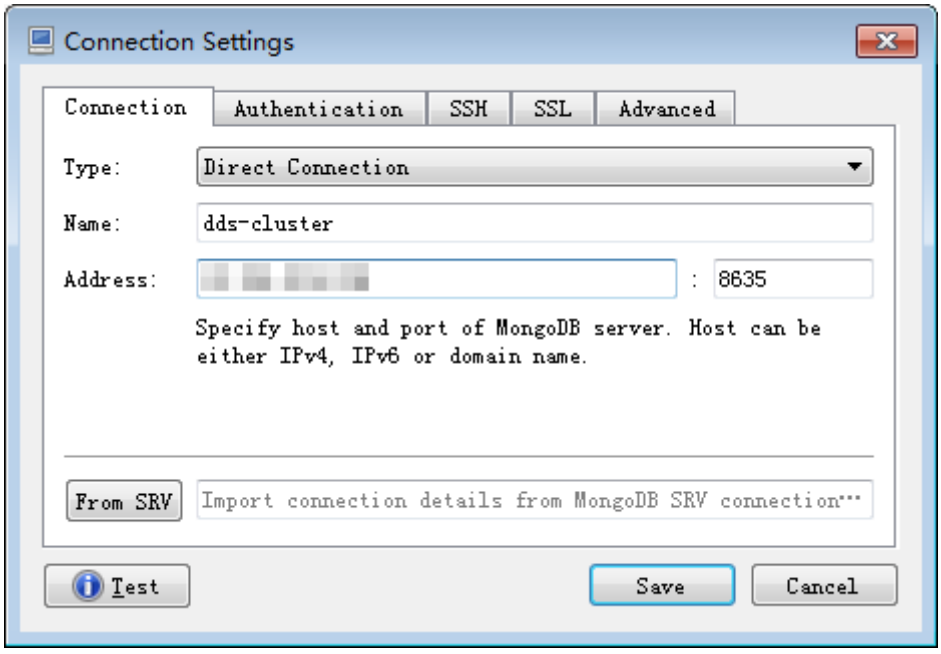
Figure 2-27 Connections



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

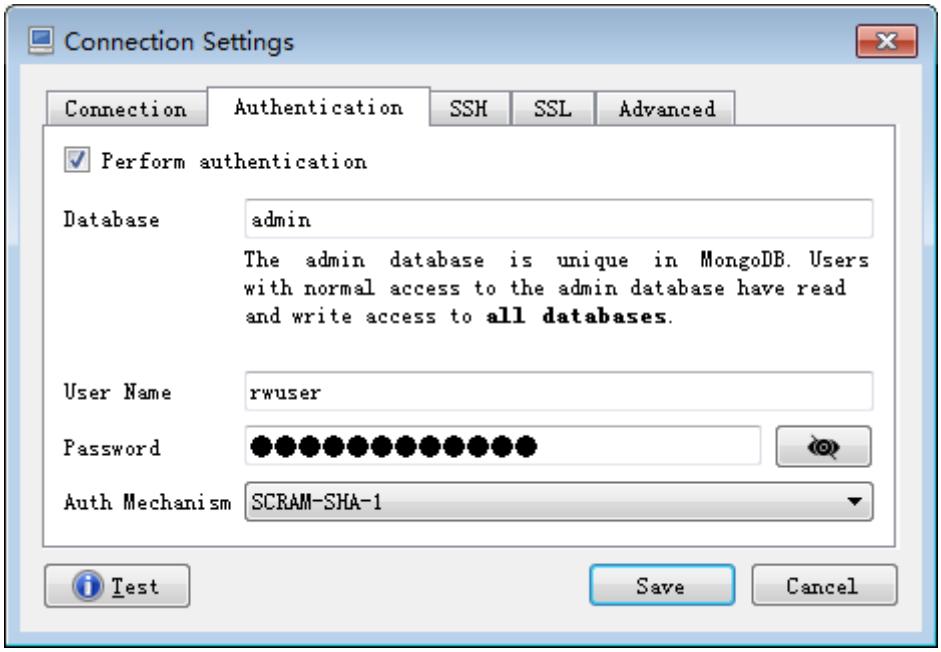
1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the DDS DB instance in the **Address** text box.

   Figure 2-28 Connection



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.

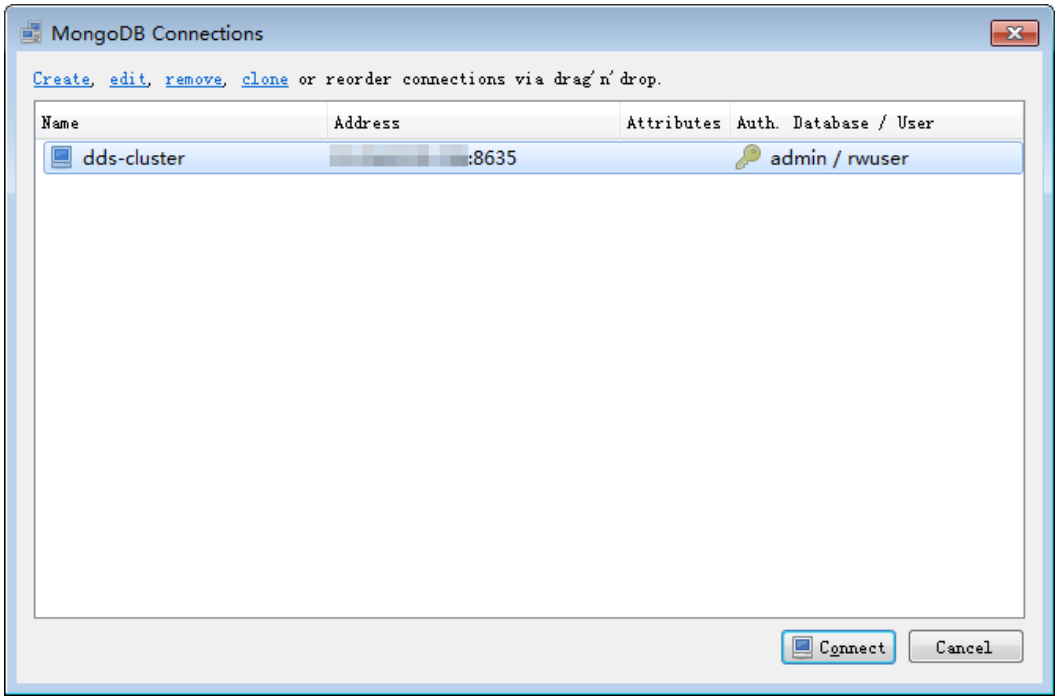
Figure 2-29 Authentication



3. Click **Save**.

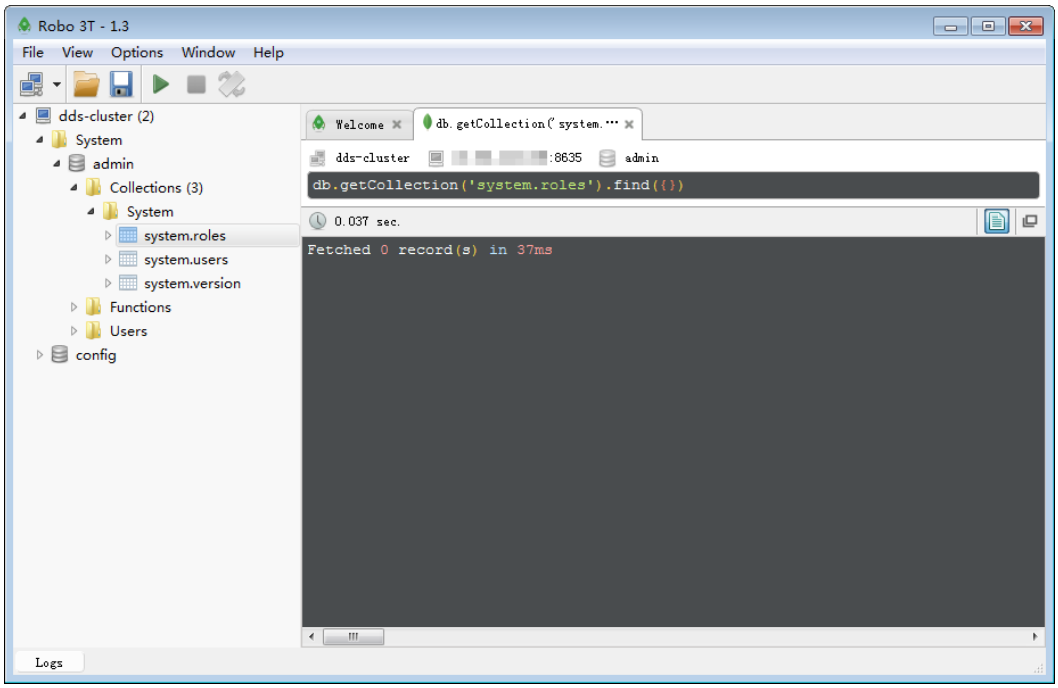
Step 3 On the **MongoDB Connections** page, click **Connect** to connect to the cluster instance.

Figure 2-30 Connections



Step 4 If the cluster instance is successfully connected, the page shown in **Figure 2-31** is displayed.

Figure 2-31 Connection succeeded



----End

Connecting to a DB Instance Using the MongoDB Client (SSL)

Step 1 On the **Instance Management** page, click the target DB instance.

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

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

Step 5 Connect to the DB instance in the directory where the MongoDB client is located.

- Method 1: Using Linux commands

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

Enter the database account password when prompted:

```
Enter password:
```

- Method 2: Using the public connection address

  ./mongo mongodb://rwuser:**@**<*DB_HOST*>**:**<*DB_PORT*>**/test?authSource=admin --ssl --sslCAFile** <*FILE_PATH*> **--sslAllowInvalidHostnames**

  To obtain the public connection address, click the instance name and choose **Connections**. The address is displayed in **Public Network Connection Address** field on the **Public Connection** tab.

NOTE

- A cluster instance uses the management IP address to generate SSL certificate. **--sslAllowInvalidHostnames** is needed for the SSL connection in a public network.
- **DB_HOST** indicates the IP address of the remotely connected DB instance. Obtain the value from the **EIP** column in the node list on the **Connections** page.
- **DB_PORT** indicates the port number. Obtain the value from **Database Port** in the **Basic Information** area on the **Connections** page.
- **DB_USER** indicates the database account name. The default value is **rwuser**.
- ********** indicates the password of the database account. If you use the connection address to connect to a DB instance:
  - If the password contains the at sign (@), change @ to %40.
  - If the password contains the exclamation mark (!), add an escape character (\) before the exclamation mark (!).
- **FILE_PATH** indicates the path where the root certificate is stored.

- Connect to the instance using Linux commands. The following is an example command:

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

- Connect to the DB instance using the public connection address. The following is an example command:

  ./mongo mongodb://rwuser:**@192.168.1.80:8635/test?authSource=admin --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames**

Step 6 Check the connection result. If the following information is displayed, the connection is successful.

```
mongos>
```

----End

Connecting to a DB Instance Using the MongoDB Client (Non-SSL)

NOTICE

If you connect to a DB instance using this method, you need to disable the SSL connection. For details, see **Enabling or Disabling SSL**.

Step 1 Connect to the ECS.

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

- Method 1: Using Linux commands

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

  Enter the database account password when prompted:

  ```
  Enter password:
  ```

- Method 2: Using the public connection address

  ./mongo mongodb://rwuser:******@<*DB_HOST*>:<*DB_PORT*>/test?authSource=admin**

  To obtain the public connection address, click the instance name and choose **Connections**. The address is displayed in **Public Network Connection Address** field on the **Public Connection** tab.

  NOTE

  - **DB_HOST** indicates the IP address of the remotely connected DB instance. Obtain the value from the **EIP** column in the node list on the **Connections** page.
  - **DB_PORT** indicates the port number. Obtain the value from **Database Port** in the **Basic Information** area on the **Connections** page.
  - **DB_USER** indicates the database account name. The default value is **rwuser**.
  - ********** indicates the password of the database account. If you use the connection address to connect to a DB instance:
    - If the password contains the at sign (@), change @ to %40.
    - If the password contains the exclamation mark (!), add an escape character (\) before the exclamation mark (!).

- Connect to the instance using Linux commands. The following is an example command:

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

- Connect to the DB instance using the public connection address. The following is an example command:

  ./mongo mongodb://rwuser:**@192.168.1.80:8635/test?authSource=admin**

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

```
mongos>
```

----End

3 Getting Started with Replica Sets

3.1 Connection Methods

HUAWEI CLOUD DDS can be accessed using Data Admin Service (DAS), private networks, and public networks.

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. For details, see **Step 2: Connect to a Replica Set Instance Through DAS**.

Table 3-1 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

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 that is in the same region, AZ, and VPC subnet as your DDS DB instance, you are advised to use a private IP address to connect the ECS to your DDS DB instances. • By default, DDS is not accessible from ECSs that are not in the same security group. If the ECS is not in the same group, you need to add an inbound rule to enable access. • The default DDS port is 8635, but this port can be modified if necessary.	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, you are advised to 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 Connecting to Replica Set Instances Through DAS

3.2.1 Overview

Scenarios

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:

- **Step 1: Buy a Replica Set Instance**
- **Step 2: Connect to a Replica Set Instance Through DAS**

3.2.2 Step 1: Buy a Replica Set Instance

Scenarios

This section describes how to create a replica set instance on the DDS management console. Currently, DDS replica set instance supports the yearly/monthly and pay-per-use billing modes. DDS allows you to tailor your compute resources and storage space to your business needs.

You can use your account to create up to 50 replica set instances.

Prerequisites

- You have registered a HUAWEI CLOUD account.
- Your account balance is greater than or equal to ¥0.
- If you want to use compute and network resources exclusively, you need to **Enabling a DeC** and **Applying for DCC Resources**. Then, you can create DDS DB instances. Click  in the upper left corner and select a region and a project.

NOTE

You will be charged for purchasing DDS DB instances through DeC.
Currently, only pay-per-use replica set instances can be purchased through DeC.

Procedure

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

Step 2 On the **Instance Management** page, click **Buy DB Instance**.

Step 3 On the displayed page, select a billing mode, select your DB instance specifications and click **Next**.

Figure 3-1 Billing mode and basic information

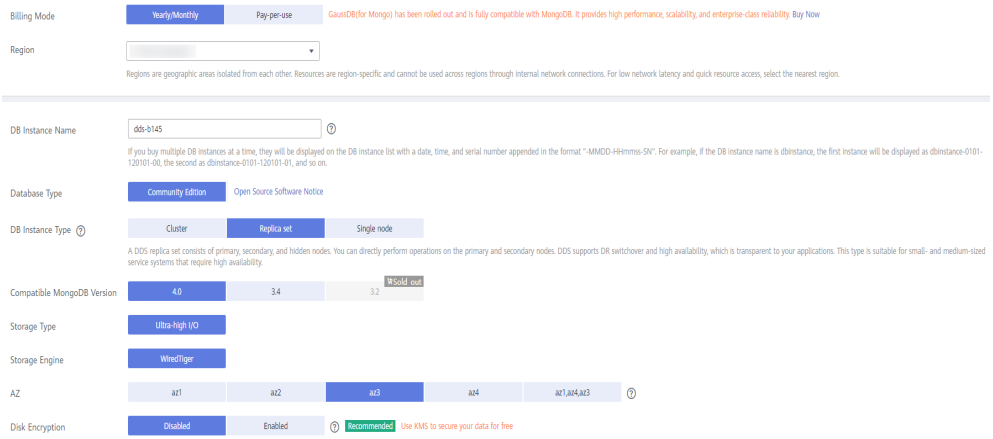


Table 3-2 Billing mode

Parameter	Description
Billing Mode	Select a billing mode, **Yearly/Monthly** or **Pay-per-use**. • Yearly/Monthly – You need to set **Validity Period** as required. Then, the system deducts the fees incurred at one time from your account based on the service price. – When you renew a yearly/monthly DB instance, you can change its billing mode from yearly/monthly to pay-per-use based on your service requirements. For details, see **Changing Yearly/Monthly Instances to a Pay-per-Use**. **NOTE** DB instances paid in yearly/monthly mode cannot be deleted. They support only resource unsubscription. For details, see section **Unsubscribing from a Yearly/Monthly DB Instance**. • Pay-per-use – You do not need to set **Validity Period** because the system deducts the fees incurred from your account based on the service duration. – If you want to use a DB instance at a low cost for a long period of time, you can change its billing mode from pay-per-use to yearly/monthly. For details, see **Changing the Billing Mode in Batches**.

Table 3-3 Basic information

Parameter	Description
Region	A region where the tenant is located. It can be changed in the upper left corner. **NOTE** DB instances deployed in different regions cannot communicate with each other through a private network, and you cannot change the region of a DB instance once it is purchased. Exercise caution when selecting a region.
DB Instance Name	The DB instance name can be 4 to 64 characters long. It must start with a letter and can contain only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_). If you buy multiple DB instances, you can only enter 4 to 49 characters to set the DB instance name, and then the system automatically appends a date, time, and serial number to the end of the instance names (format: *instance_name-MMDD-HHmmss-SN*). After the DB instance is created, you can change its name. For details, see **Modifying the DB Instance Name**.
Database Type	Community Edition
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	• 4.0 • 3.4 • 3.2
CPU Type	Currently, DDS supports two CPU architectures: x86 and Kunpeng. The two architectures have similar capabilities and performance, both of which can meet your service requirements. For details about the instance types, versions, and specifications supported by the two CPU architectures, see **DB Instance Specifications**.

Parameter	Description
Resource Type	If you use DeC, this parameter is displayed. EVS and DSS disks are provided based on whether storage resources are exclusively used. DSS disks provide dedicated storage resources. ● If you have applied for a storage pool on the DSS page, click the **DSS** tab and create disks in the obtained storage pool. ● If you have not applied for an exclusive storage pool, click the **EVS** disk tab. Then, the created disks use public storage resources.
Storage Type	If you do not use DeC, the storage type is ultra-high I/O by default. For DeC users, the supported storage types vary depending on the selected resource type. ● If you select **EVS** for **Resource Type**, **Storage Type** is set to **Ultra-high I/O**. ● If you select **DSS** for **Resource Type**, **Storage Type** can be set to **Common I/O**, **High I/O**, or **Ultra-high I/O**.
Storage Pool	This option is displayed only when you select **DSS** for **Resource Type**. The storage pool is physically isolated from other pools and is secure.
Storage Engine	WiredTiger
AZ	An AZ is a part of a region with its own independent power supplies and networks. AZs are physically isolated but can communicate through an internal network connection. Currently, instances can be deployed in a single AZ or three AZs. ● If you want to deploy an instance in a single AZ, select one AZ. ● If you want to deploy an instance across AZs for disaster recovery, select three AZs. In this deployment mode, the nodes are evenly distributed in the three AZs.

Parameter	Description
Disk Encryption	• **Disabled**: Disable the encryption function. • **Enabled**: Enable the encryption function. 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 a DB instance is created, the disk encryption status and the key cannot be changed. The backup data stored in OBS is not encrypted. – The key cannot be disabled, deleted, or frozen when being used. Otherwise, the database becomes unavailable. – For details about how to create a key, see the "Creating a CMK" section in the *Data Encryption Workshop User Guide*.

Figure 3-2 Instance class and storage space

Table 3-4 Specifications

Parameter	Description
Specifications	In the x86 CPU architecture, the following specifications can be selected to suit different application scenarios: General-purpose (s6), Enhanced (c3), and Enhanced II (c6).
Dedicated Cloud	If you use DeC, this parameter is displayed. For details about DB instance specifications in your DeC, see **Database Instance Specifications**.
Node Class	For details about the DB instance specifications, see **DB Instance Specifications**.
Storage Space	The value ranges from 10 GB to 3000 GB and must be a multiple of 10.

Figure 3-3 Network and database configuration

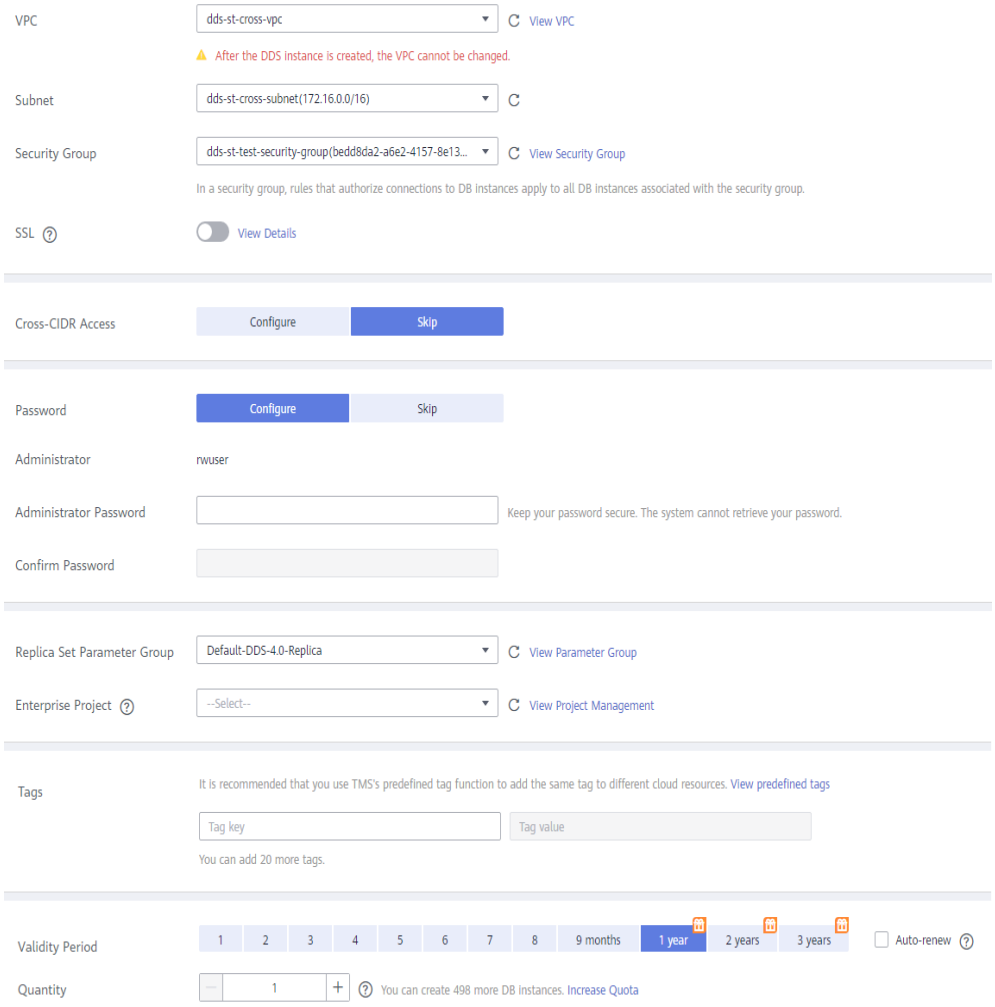


Table 3-5 Network

Parameter	Description
VPC	The VPC where your DB instances are located. A VPC isolates networks for different services, so you can easily manage and configure internal networks and change network configuration. You need to create or select the required VPC. For details about how to create a VPC, see section "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 allocates resources to you by default.

Parameter	Description
Subnet	A subnet provides dedicated network resources that are logically isolated from other networks for network security. After the instance is created, you can change the private IP address assigned by the subnet. For details, see **Changing a Private IP Address**.
Security Group	A security group controls access between DDS and other services for security. If there are no security groups available, DDS allocates resources to you by default. **NOTE** Ensure that the security group rule you set allows clients to access DB instances. For example, select the TCP protocol with inbound direction, input the default port number **8635**, and enter a subnet IP address or select a security group that the DB instance belongs to.
SSL	Secure Sockets Layer (SSL) certificates set up encrypted connections between clients and servers, preventing data from being tampered with or stolen during transmission. You can enable SSL to improve data security. After a DB instance is created, you can connect to it using SSL.
Cross-CIDR Access	• Configure Add the VPC CIDR block of your client. Ensure that the ECS where your client is installed can connect to the DB instance. **NOTE** – To ensure the ECS and the DB instance can communicate with each other, configure the connection by referring to **VPC Peering Connection Overview**. – VPC CIDR blocks can only be added, but not modified or deleted. – Up to 9 CIDR blocks can be configured, and each of them does not overlap. • 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**.
IPv6	Before enabling IPv6, ensure that IPv6 has been enabled for the VPC and subnet where the DB instance is located. For details about the application scenarios and procedures for enabling IPv6 for the VPC and subnet, see **IPv4 and IPv6 Dual-Stack Network**. After IPv6 is enabled, the DB instance can run in dual-stack mode. It means that the DB instance can use both the IPv4 address and IPv6 address. The DB instance can access the Internet using either IPv4 or IPv6 addresses, and the communications are independent of each other.

Parameter	Description
Anti-affinity Deployment	If you use DeC, this parameter is displayed. This option is enabled by default. Anti-affinity deployment requires the primary, secondary, and hidden nodes to be deployed on different physical machines to achieve high availability.

Table 3-6 Database configuration

Parameter	Description
Password	• Configure Enter and confirm the administrator password for connecting to the DB instance. • Skip Set the administrator password later. When you need to connect to the DB instance, locate the DB instance and click **Reset Password** in the **Operation** column to set a password for connecting to the DB instance.
Administrator	The default account is **rwuser**.
Administrator Password	Set a password for the administrator. The password is a string of 8 to 32 characters. It must be a combination of uppercase letters, lowercase letters, digits, and special characters. You can also use the following special characters: ~!@#%^*-_=+? Keep this password secure. If lost, the system cannot retrieve it for you.
Confirm Password	Enter the administrator password again.
Replica Set Parameter Group	The parameters that apply to the replica set instances. After a DB instance is created, you can change the parameter group you configured for the DB instance to bring out the best performance. For details, see **Editing a Parameter Group**.

Parameter	Description
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**. 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 the *Enterprise Management User Guide*.

Table 3-7 Tag

Parameter	Description
Tags	This setting is optional. Adding tags helps you better identify and manage your DB instances. Up to 20 tags can be added for a DB instance. A tag is composed of a key-value pair. • Key: Mandatory if the DB instance is going to be tagged – Each tag key must be unique for each DB instance. – A tag key consists of up to 36 characters. – The key can only consist of digits, letters, underscores (_), and hyphens (-). • Value: Optional if the DB instance is going to be tagged – The value consists of up to 43 characters. – The value can only consist of digits, letters, underscores (_), dots (.), and hyphens (-). After a DB instance is created, you can view its tag details on the **Tags** tab. In addition, you can add, modify, and delete tags for existing DB instances. For details, see **Tag**.

Table 3-8 Required duration and quantity

Parameter	Description
Validity Period	The system will automatically calculate the fee based on the validity period you have selected.
Auto-renew	• By default, this option is not selected. • If you select this option, the auto-renew cycle is determined by the selected required duration.

Parameter	Description
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. The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

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

NOTE

DB instance performance is determined by how you configure it during the creation. The hardware configuration items that can be selected include the class and storage space of the replica set.

Step 4 On the displayed page, confirm the DB instance information.

- Yearly/Monthly
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify your settings, click **Pay Now** to go to the payment page and complete the payment.
- Pay-per-use
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, click **Submit** to start the instance creation.

Step 5 After a DDS DB instance is created, you can view and manage it on the **Instance Management** 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**.
- DDS enables the automated backup policy by default. After a DB instance is created, you can modify or disable the automated backup policy. An automated full backup is immediately triggered after the creation of a DB instance.
- The default DDS port is 8635, but this port can be modified if necessary. If you change the port, you need to add the security group rule to enable access.
- The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

----End

3.2.3 Step 2: Connect to a Replica Set Instance Through DAS

Scenarios

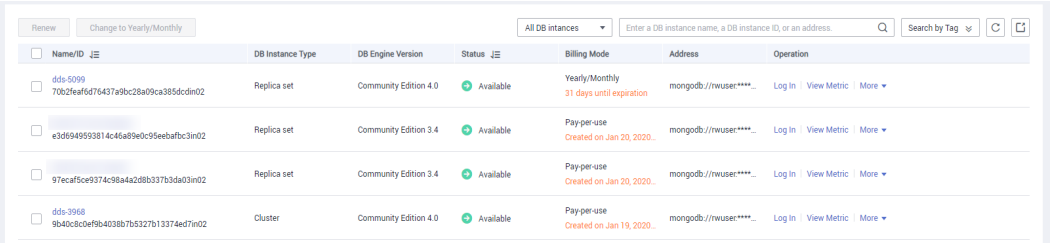
Data Admin Service (DAS) enables you to manage DB instances on a web-based console, simplifying database management and improving working efficiency. By default, you have the remote login permission. It is recommended that you use the DAS service to connect to DB instances, which is more secure and convenient.

Procedure

Step 1 On the **Instance Management** page, locate the target DB instance and click **Log In** in the **Operation** column.

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

Figure 3-4 Instance management



Step 2 On the displayed login page, enter the administrator username and password and click **Login**.

For details about how to manage databases through DAS, see **User Interface Overview**.

----End

3.3 Connecting to a Replica Set Instance Over Private Networks

3.3.1 Overview

Scenarios

This section describes how to buy a replica set instance on the management console, set a security group, and connect to a replica set instance over private networks.

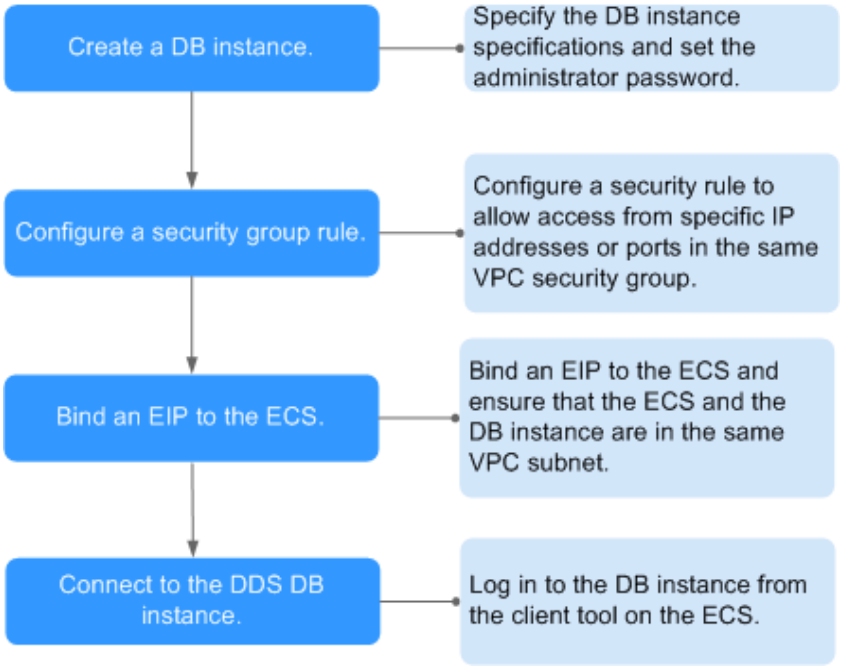
Process

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

- **Step 1: Buy a Replica Set Instance**
- **Step 2: Set a Security Group**
- **Step 3: Connect to a Replica Set Instance Over Private Networks**

The following describes the steps from creating a DB instance to using it.

Figure 3-5 Accessing DB instances from a private network



3.3.2 Step 1: Buy a Replica Set Instance

Scenarios

This section describes how to create a replica set instance on the DDS management console. Currently, DDS replica set instance supports the yearly/monthly and pay-per-use billing modes. DDS allows you to tailor your compute resources and storage space to your business needs.

You can use your account to create up to 50 replica set instances.

Prerequisites

- You have registered a HUAWEI CLOUD account.
- Your account balance is greater than or equal to ¥0.
- If you want to use compute and network resources exclusively, you need to **Enabling a DeC** and **Applying for DCC Resources**. Then, you can create DDS DB instances. Click in the upper left corner and select a region and a project.

NOTE

You will be charged for purchasing DDS DB instances through DeC.

Currently, only pay-per-use replica set instances can be purchased through DeC.

Procedure

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

Step 2 On the **Instance Management** page, click **Buy DB Instance**.

Step 3 On the displayed page, select a billing mode, select your DB instance specifications and click **Next**.

Figure 3-6 Billing mode and basic information

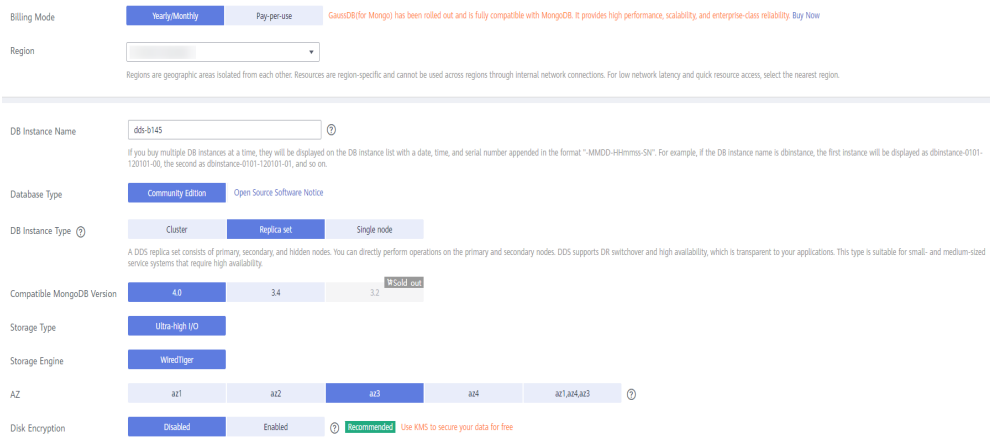


Table 3-9 Billing mode

Parameter	Description
Billing Mode	Select a billing mode, **Yearly/Monthly** or **Pay-per-use**. • Yearly/Monthly – You need to set **Validity Period** as required. Then, the system deducts the fees incurred at one time from your account based on the service price. – When you renew a yearly/monthly DB instance, you can change its billing mode from yearly/monthly to pay-per-use based on your service requirements. For details, see **Changing Yearly/Monthly Instances to a Pay-per-Use**. **NOTE** DB instances paid in yearly/monthly mode cannot be deleted. They support only resource unsubscription. For details, see section **Unsubscribing from a Yearly/Monthly DB Instance**. • Pay-per-use – You do not need to set **Validity Period** because the system deducts the fees incurred from your account based on the service duration. – If you want to use a DB instance at a low cost for a long period of time, you can change its billing mode from pay-per-use to yearly/monthly. For details, see **Changing the Billing Mode in Batches**.

Table 3-10 Basic information

Parameter	Description
Region	A region where the tenant is located. It can be changed in the upper left corner. **NOTE** DB instances deployed in different regions cannot communicate with each other through a private network, and you cannot change the region of a DB instance once it is purchased. Exercise caution when selecting a region.
DB Instance Name	The DB instance name can be 4 to 64 characters long. It must start with a letter and can contain only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_). If you buy multiple DB instances, you can only enter 4 to 49 characters to set the DB instance name, and then the system automatically appends a date, time, and serial number to the end of the instance names (format: *instance_name-MMDD-HHmmss-SN*). After the DB instance is created, you can change its name. For details, see **Modifying the DB Instance Name**.
Database Type	Community Edition
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	• 4.0 • 3.4 • 3.2
CPU Type	Currently, DDS supports two CPU architectures: x86 and Kunpeng. The two architectures have similar capabilities and performance, both of which can meet your service requirements. For details about the instance types, versions, and specifications supported by the two CPU architectures, see **DB Instance Specifications**.

Parameter	Description
Resource Type	If you use DeC, this parameter is displayed. EVS and DSS disks are provided based on whether storage resources are exclusively used. DSS disks provide dedicated storage resources. ● If you have applied for a storage pool on the DSS page, click the **DSS** tab and create disks in the obtained storage pool. ● If you have not applied for an exclusive storage pool, click the **EVS** disk tab. Then, the created disks use public storage resources.
Storage Type	If you do not use DeC, the storage type is ultra-high I/O by default. For DeC users, the supported storage types vary depending on the selected resource type. ● If you select **EVS** for **Resource Type**, **Storage Type** is set to **Ultra-high I/O**. ● If you select **DSS** for **Resource Type**, **Storage Type** can be set to **Common I/O**, **High I/O**, or **Ultra-high I/O**.
Storage Pool	This option is displayed only when you select **DSS** for **Resource Type**. The storage pool is physically isolated from other pools and is secure.
Storage Engine	WiredTiger
AZ	An AZ is a part of a region with its own independent power supplies and networks. AZs are physically isolated but can communicate through an internal network connection. Currently, instances can be deployed in a single AZ or three AZs. ● If you want to deploy an instance in a single AZ, select one AZ. ● If you want to deploy an instance across AZs for disaster recovery, select three AZs. In this deployment mode, the nodes are evenly distributed in the three AZs.

Parameter	Description
Disk Encryption	• **Disabled**: Disable the encryption function. • **Enabled**: Enable the encryption function. 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 a DB instance is created, the disk encryption status and the key cannot be changed. The backup data stored in OBS is not encrypted. – The key cannot be disabled, deleted, or frozen when being used. Otherwise, the database becomes unavailable. – For details about how to create a key, see the "Creating a CMK" section in the *Data Encryption Workshop User Guide*.

Figure 3-7 Instance class and storage space

Table 3-11 Specifications

Parameter	Description
Specifications	In the x86 CPU architecture, the following specifications can be selected to suit different application scenarios: General-purpose (s6), Enhanced (c3), and Enhanced II (c6).
Dedicated Cloud	If you use DeC, this parameter is displayed. For details about DB instance specifications in your DeC, see **Database Instance Specifications**.
Node Class	For details about the DB instance specifications, see **DB Instance Specifications**.
Storage Space	The value ranges from 10 GB to 3000 GB and must be a multiple of 10.

Figure 3-8 Network and database configuration

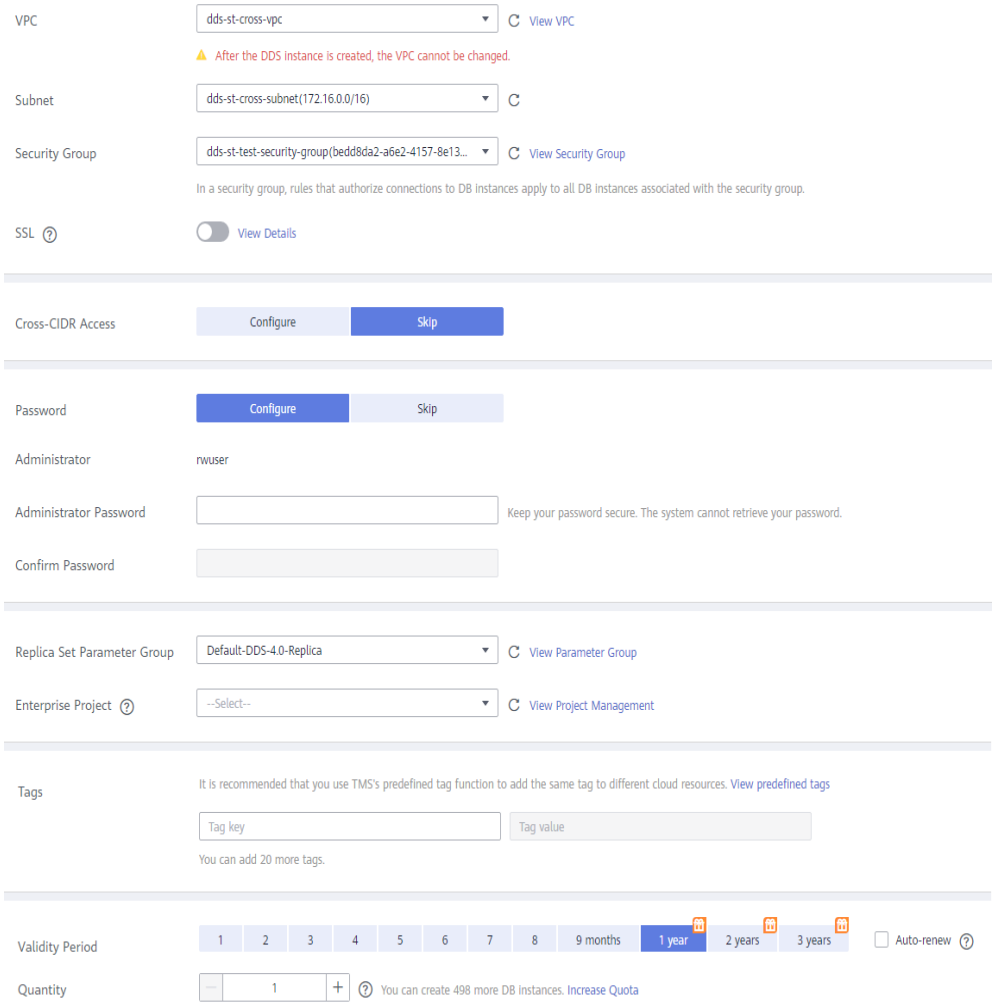


Table 3-12 Network

Parameter	Description
VPC	The VPC where your DB instances are located. A VPC isolates networks for different services, so you can easily manage and configure internal networks and change network configuration. You need to create or select the required VPC. For details about how to create a VPC, see section "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 allocates resources to you by default.

Parameter	Description
Subnet	A subnet provides dedicated network resources that are logically isolated from other networks for network security. After the instance is created, you can change the private IP address assigned by the subnet. For details, see **Changing a Private IP Address**.
Security Group	A security group controls access between DDS and other services for security. If there are no security groups available, DDS allocates resources to you by default. **NOTE** Ensure that the security group rule you set allows clients to access DB instances. For example, select the TCP protocol with inbound direction, input the default port number **8635**, and enter a subnet IP address or select a security group that the DB instance belongs to.
SSL	Secure Sockets Layer (SSL) certificates set up encrypted connections between clients and servers, preventing data from being tampered with or stolen during transmission. You can enable SSL to improve data security. After a DB instance is created, you can connect to it using SSL.
Cross-CIDR Access	• Configure Add the VPC CIDR block of your client. Ensure that the ECS where your client is installed can connect to the DB instance. **NOTE** – To ensure the ECS and the DB instance can communicate with each other, configure the connection by referring to **VPC Peering Connection Overview**. – VPC CIDR blocks can only be added, but not modified or deleted. – Up to 9 CIDR blocks can be configured, and each of them does not overlap. • 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**.
IPv6	Before enabling IPv6, ensure that IPv6 has been enabled for the VPC and subnet where the DB instance is located. For details about the application scenarios and procedures for enabling IPv6 for the VPC and subnet, see **IPv4 and IPv6 Dual-Stack Network**. After IPv6 is enabled, the DB instance can run in dual-stack mode. It means that the DB instance can use both the IPv4 address and IPv6 address. The DB instance can access the Internet using either IPv4 or IPv6 addresses, and the communications are independent of each other.

Parameter	Description
Anti-affinity Deployment	If you use DeC, this parameter is displayed. This option is enabled by default. Anti-affinity deployment requires the primary, secondary, and hidden nodes to be deployed on different physical machines to achieve high availability.

Table 3-13 Database configuration

Parameter	Description
Password	• Configure Enter and confirm the administrator password for connecting to the DB instance. • Skip Set the administrator password later. When you need to connect to the DB instance, locate the DB instance and click **Reset Password** in the **Operation** column to set a password for connecting to the DB instance.
Administrator	The default account is **rwuser**.
Administrator Password	Set a password for the administrator. The password is a string of 8 to 32 characters. It must be a combination of uppercase letters, lowercase letters, digits, and special characters. You can also use the following special characters: ~!@#%^*-_=+? Keep this password secure. If lost, the system cannot retrieve it for you.
Confirm Password	Enter the administrator password again.
Replica Set Parameter Group	The parameters that apply to the replica set instances. After a DB instance is created, you can change the parameter group you configured for the DB instance to bring out the best performance. For details, see **Editing a Parameter Group**.

Parameter	Description
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**. 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 the *Enterprise Management User Guide*.

Table 3-14 Tag

Parameter	Description
Tags	This setting is optional. Adding tags helps you better identify and manage your DB instances. Up to 20 tags can be added for a DB instance. A tag is composed of a key-value pair. • Key: Mandatory if the DB instance is going to be tagged – Each tag key must be unique for each DB instance. – A tag key consists of up to 36 characters. – The key can only consist of digits, letters, underscores (_), and hyphens (-). • Value: Optional if the DB instance is going to be tagged – The value consists of up to 43 characters. – The value can only consist of digits, letters, underscores (_), dots (.), and hyphens (-). After a DB instance is created, you can view its tag details on the **Tags** tab. In addition, you can add, modify, and delete tags for existing DB instances. For details, see **Tag**.

Table 3-15 Required duration and quantity

Parameter	Description
Validity Period	The system will automatically calculate the fee based on the validity period you have selected.
Auto-renew	• By default, this option is not selected. • If you select this option, the auto-renew cycle is determined by the selected required duration.

Parameter	Description
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. The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

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

NOTE

DB instance performance is determined by how you configure it during the creation. The hardware configuration items that can be selected include the class and storage space of the replica set.

Step 4 On the displayed page, confirm the DB instance information.

- Yearly/Monthly
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify your settings, click **Pay Now** to go to the payment page and complete the payment.
- Pay-per-use
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, click **Submit** to start the instance creation.

Step 5 After a DDS DB instance is created, you can view and manage it on the **Instance Management** 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**.
- DDS enables the automated backup policy by default. After a DB instance is created, you can modify or disable the automated backup policy. An automated full backup is immediately triggered after the creation of a DB instance.
- The default DDS port is 8635, but this port can be modified if necessary. If you change the port, you need to add the security group rule to enable access.
- The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

----End

3.3.3 Step 2: Set a Security Group

Scenarios

This section guides you on how to add a security group rule to control access from and to DDS DB instances associated with a security group. The following describes how to set security groups.

Precautions

The default security group rule allows all outgoing data packets. ECSs and DDS DB instances in the same security group can access each other. After a security group is created, you can create different rules for that security group, which allows you to control access to the DB instances that are in it.

To access a DB instance in a security group from a source outside of that group, you need to create an inbound rule.

For details about the constraints on using security groups, see **Security Group Overview**.

Procedure

Step 1 On the **Instance Management** page, click the target replica set instance.

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

Step 3 In the **Security Group** area, on the **Inbound Rules** tab, click **Add Rule**. In the displayed **Add Inbound Rule** dialog box, set required parameters to add inbound rules. On the **Outbound Rules** tab, click **Add Rule**. In the displayed **Add Outbound Rule** dialog box, set required parameters to add outbound rules.

You can click ⊕ to add more rules.

Figure 3-9 Add Inbound Rule

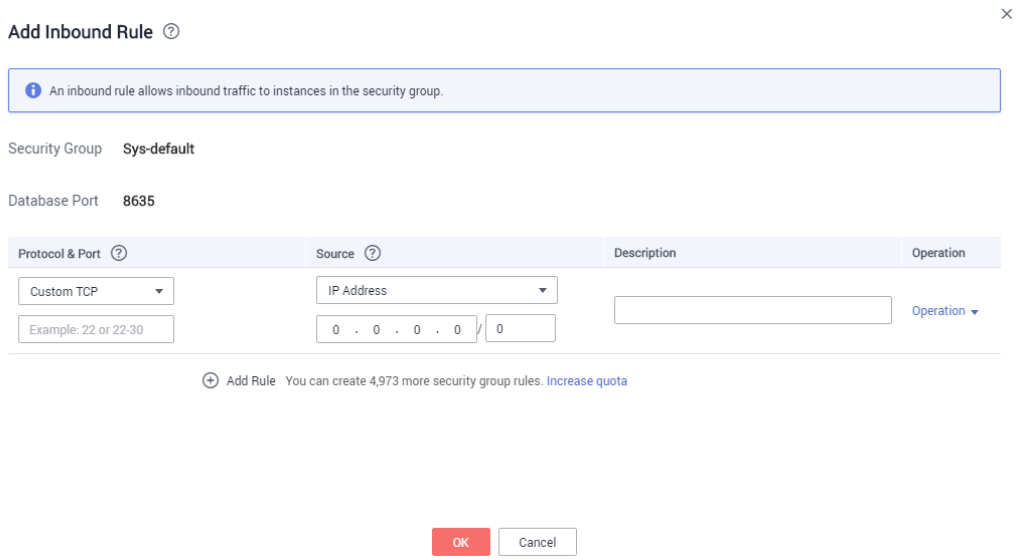
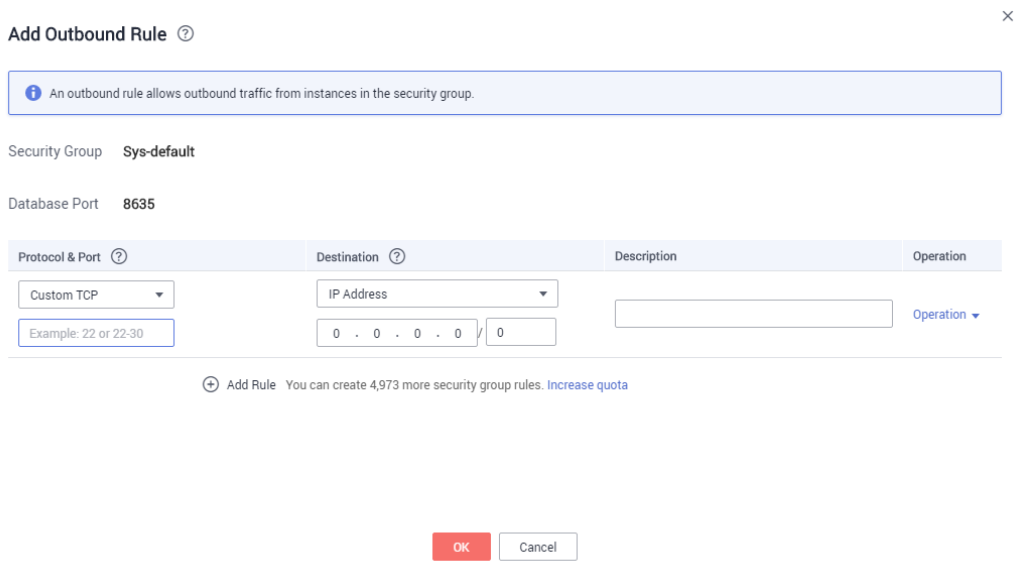


Figure 3-10 Add Outbound Rule



Step 4 Add a security group rule as prompted.

Table 3-16 Parameter description

Parameter	Description	Value Example
Protocol	The network protocol required for access. You can allow all protocols or specify a specific protocol, TCP, UDP, ICMP, and SSH.	TCP
Port	Specifies the port that allows the access to ECSs or external devices. Common ports are listed in **Common Ports Used by ECSs**.	8635
Source/ Destination	Specifies the supported IP address and security group that the rule applies to. • **IP address**: The IP address or subnet that the rule applies to. Single IP addresses must be expressed using slash notation. – Single IP address: xxx.xxx.xxx.xxx/32 (IPv4) – Subnet: xxx.xxx.xxx.0/24 – All IP addresses: 0.0.0.0/0 • **Security group**: A security group that access will be allowed from. ECSs in this security group will be granted access to DDS instance in the current security group.	• 192.168.10.0/24 • default

Step 5 Click **OK**.

----End

3.3.4 Step 3: Connect to a Replica Set Instance Over Private Networks

Scenarios

This section describes how to connect to a replica set instance using the MongoDB client over private networks.

You can directly perform operations on the primary and secondary nodes. Primary nodes are used for processing read and write requests. Secondary nodes replicate data from the primary and are used for processing read requests only.

The MongoDB client can connect to a DB instance with a common connection or an encrypted connection (SSL). To improve data transmission security, you are advised to connect to DB instances using the SSL connection.

Different OS scenarios: The following uses Linux ECS and Window client as an example.

For best practices about connections to DB instances over private networks, see **Connecting to a DB Instance Through an ECS**.

Constraints

For details about constraints on connecting to a replica set DB instance over private networks, see **Constraints**.

Prerequisites

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

Connecting to a DB Instance Using the MongoDB Client (SSL)

Step 1 On the **Instance Management** page, click the target DB instance.

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

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

Step 5 Connect to a DDS DB instance.

- Method 1: Using Linux commands

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

  Enter the database account password when prompted:

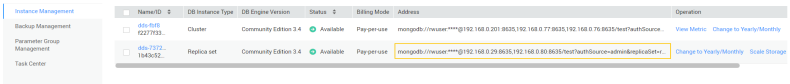
  ```
  Enter password:
  ```

- Method 2: Using the private connection address

  ./mongo "mongodb://rwuser:**@***<DB_HOST1>*:*<DB_PORT1>*,*<DB_HOST2>*:*<DB_PORT2>***/test?authSource=admin&replicaSet=replica" --ssl --sslCAFile** *<FILE_PATH>* **--sslAllowInvalidHostnames**

  If the DB instance is connected using the connection address, add double quotation marks before and after the connection information. The connection information can be obtained in the **Address** column on the **Instance Management** page.

  Figure 3-11 Connections

  In contrast to directly connecting to the primary node, this connection mode provides higher data read/write performance and avoids write errors after a primary/standby switchover. For details, see **Connecting to a Replica Set Instance for Read and Write Separation and High Availability** in the *Document Database Service Best Practices*.

NOTE

- A replica set instance uses the management IP address to generate SSL certificate. **--sslAllowInvalidHostnames** is needed for the SSL connection through a private network.
- **DB_HOST** indicates the IP address of the remotely connected DB instance. Obtain the value from the **Private IP Address** column in the node list on the **Connections** page.
- **DB_PORT** indicates the port number. Obtain the value from **Database Port** in the **Basic Information** area on the **Connections** page.
- **DB_USER** indicates the database account name. The default value is **rwuser**.
- ********** indicates the password of the database account. If you use the connection address to connect to a DB instance:
  - If the password contains the at sign (@), change @ to %40.
  - If the password contains the exclamation mark (!), add an escape character (\) before the exclamation mark (!).
- **FILE_PATH** indicates the path where the root certificate is stored.

- Connect to the instance using Linux commands. The following is an example command:

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

- Connect to the DB instance using the private connection address. The following is an example command:

  ./mongo "mongodb://rwuser:**@192.168.1.6:8635,192.168.1.80:8635/test?authSource=admin&replicaSet=replica" --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames**

Step 6 Check the connection result. If the following information is displayed, the connection is successful.

- Result from connecting the primary node in a replica set:
  ```
  replica:PRIMARY>
  ```
- Result from connecting the secondary node in a replica set:
  ```
  replica:SECONDARY>
  ```

----End

Connecting to a DB Instance Using the MongoDB Client (Non-SSL)

NOTICE

If you connect to a DB instance using this method, you need to disable the SSL connection. For details, see **Enabling or Disabling SSL**.

Step 1 Connect to the ECS.

Step 2 Connect to a DDS DB instance.

- Method 1: Using Linux commands

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

  Enter the database account password when prompted:

  ```
  Enter password:
  ```


- Method 2: Using the private connection address

  ./mongo "mongodb://
  rwuser:***@*<*DB_HOST1*>**:**<*DB_PORT1*>**,**<*DB_HOST2*>**:**<*DB_PORT2*>**/test?**
  authSource=admin&replicaSet=replica"

  If the DB instance is connected using the connection address, add double quotation marks before and after the connection information. The connection information can be obtained in the **Address** column on the **Instance Management** page.

  In contrast to directly connecting to the primary node, this connection mode provides higher data read/write performance and avoids write errors after a primary/standby switchover. For details, see **Connecting to a Replica Set Instance for Read and Write Separation and High Availability** in the *Document Database Service Best Practices*.

  NOTE

  - **DB_HOST** indicates the IP address of the remotely connected DB instance. Obtain the value from the **Private IP Address** column in the node list on the **Connections** page.
  - **DB_PORT** indicates the port number. Obtain the value from **Database Port** in the **Basic Information** area on the **Connections** page.
  - **DB_USER** indicates the database account name. The default value is **rwuser**.
  - ***** indicates the password of the database account. If you use the connection address to connect to a DB instance:
    - If the password contains the at sign (@), change @ to %40.
    - If the password contains the exclamation mark (!), add an escape character (\) before the exclamation mark (!).

- Connect to the instance using Linux commands. The following is an example command:

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

- Connect to the DB instance using the private connection address. The following is an example command:

  ./mongo "mongodb://rwuser:**@192.168.1.6:8635,192.168.1.80:8635/**
  test?authSource=admin&replicaSet=replica"

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

- Result from connecting the primary node in a replica set:
  ```
  replica:PRIMARY>
  ```
- Result from connecting the secondary node in a replica set:
  ```
  replica:SECONDARY>
  ```

----End

3.4 Connecting to a Replica Set Instance Over Public Networks

3.4.1 Overview

Scenarios

This section describes how to buy a replica set instance on the management console, set a security group, bind an EIP, and connect to a replica set instance over public networks.

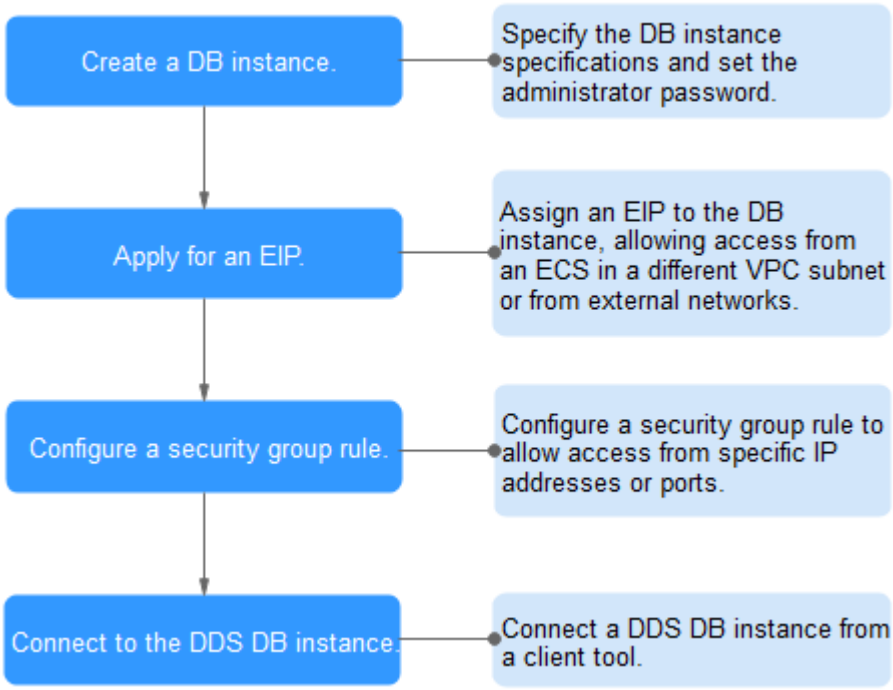
Process

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

- **Step 1: Buy a Replica Set Instance**
- **Step 2: Bind an EIP**
- **Step 3: Set a Security Group**
- **Step 4: Connect to a Replica Set Instance Over Public Networks**

The following describes the steps from creating a DB instance to using it.

Figure 3-12 Accessing DB instances from a public network



3.4.2 Step 1: Buy a Replica Set Instance

Scenarios

This section describes how to create a replica set instance on the DDS management console. Currently, DDS replica set instance supports the yearly/monthly and pay-per-use billing modes. DDS allows you to tailor your compute resources and storage space to your business needs.

You can use your account to create up to 50 replica set instances.

Prerequisites

- You have registered a HUAWEI CLOUD account.
- Your account balance is greater than or equal to ¥0.
- If you want to use compute and network resources exclusively, you need to **Enabling a DeC** and **Applying for DCC Resources**. Then, you can create DDS DB instances. Click in the upper left corner and select a region and a project.

NOTE

You will be charged for purchasing DDS DB instances through DeC.

Currently, only pay-per-use replica set instances can be purchased through DeC.

Procedure

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

Step 2 On the **Instance Management** page, click **Buy DB Instance**.

Step 3 On the displayed page, select a billing mode, select your DB instance specifications and click **Next**.

Figure 3-13 Billing mode and basic information

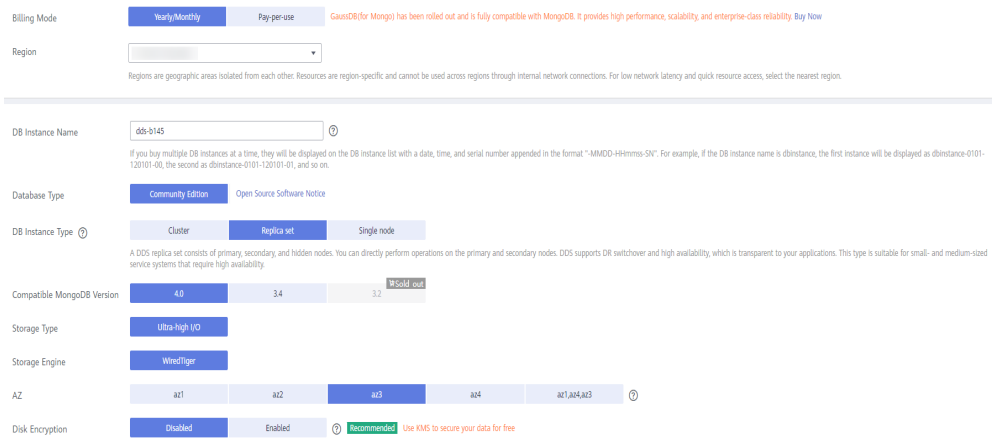


Table 3-17 Billing mode

Parameter	Description
Billing Mode	Select a billing mode, **Yearly/Monthly** or **Pay-per-use**. • Yearly/Monthly – You need to set **Validity Period** as required. Then, the system deducts the fees incurred at one time from your account based on the service price. – When you renew a yearly/monthly DB instance, you can change its billing mode from yearly/monthly to pay-per-use based on your service requirements. For details, see **Changing Yearly/Monthly Instances to a Pay-per-Use**. **NOTE** DB instances paid in yearly/monthly mode cannot be deleted. They support only resource unsubscription. For details, see section **Unsubscribing from a Yearly/Monthly DB Instance**. • Pay-per-use – You do not need to set **Validity Period** because the system deducts the fees incurred from your account based on the service duration. – If you want to use a DB instance at a low cost for a long period of time, you can change its billing mode from pay-per-use to yearly/monthly. For details, see **Changing the Billing Mode in Batches**.

Table 3-18 Basic information

Parameter	Description
Region	A region where the tenant is located. It can be changed in the upper left corner. **NOTE** DB instances deployed in different regions cannot communicate with each other through a private network, and you cannot change the region of a DB instance once it is purchased. Exercise caution when selecting a region.

Parameter	Description
DB Instance Name	The DB instance name can be 4 to 64 characters long. It must start with a letter and can contain only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_). If you buy multiple DB instances, you can only enter 4 to 49 characters to set the DB instance name, and then the system automatically appends a date, time, and serial number to the end of the instance names (format: *instance_name-MMDD-HHmmss-SN*). After the DB instance is created, you can change its name. For details, see **Modifying the DB Instance Name**.
Database Type	Community Edition
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	• 4.0 • 3.4 • 3.2
CPU Type	Currently, DDS supports two CPU architectures: x86 and Kunpeng. The two architectures have similar capabilities and performance, both of which can meet your service requirements. For details about the instance types, versions, and specifications supported by the two CPU architectures, see **DB Instance Specifications**.
Resource Type	If you use DeC, this parameter is displayed. EVS and DSS disks are provided based on whether storage resources are exclusively used. DSS disks provide dedicated storage resources. • If you have applied for a storage pool on the DSS page, click the **DSS** tab and create disks in the obtained storage pool. • If you have not applied for an exclusive storage pool, click the **EVS** disk tab. Then, the created disks use public storage resources.

Parameter	Description
Storage Type	If you do not use DeC, the storage type is ultra-high I/O by default. For DeC users, the supported storage types vary depending on the selected resource type. • If you select **EVS** for **Resource Type**, **Storage Type** is set to **Ultra-high I/O**. • If you select **DSS** for **Resource Type**, **Storage Type** can be set to **Common I/O**, **High I/O**, or **Ultra-high I/O**.
Storage Pool	This option is displayed only when you select **DSS** for **Resource Type**. The storage pool is physically isolated from other pools and is secure.
Storage Engine	WiredTiger
AZ	An AZ is a part of a region with its own independent power supplies and networks. AZs are physically isolated but can communicate through an internal network connection. Currently, instances can be deployed in a single AZ or three AZs. • If you want to deploy an instance in a single AZ, select one AZ. • If you want to deploy an instance across AZs for disaster recovery, select three AZs. In this deployment mode, the nodes are evenly distributed in the three AZs.
Disk Encryption	• **Disabled**: Disable the encryption function. • **Enabled**: Enable the encryption function. 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 a DB instance is created, the disk encryption status and the key cannot be changed. The backup data stored in OBS is not encrypted. – The key cannot be disabled, deleted, or frozen when being used. Otherwise, the database becomes unavailable. – For details about how to create a key, see the "Creating a CMK" section in the *Data Encryption Workshop User Guide*.

Figure 3-14 Instance class and storage space

Table 3-19 Specifications

Parameter	Description
Specifications	In the x86 CPU architecture, the following specifications can be selected to suit different application scenarios: General-purpose (s6), Enhanced (c3), and Enhanced II (c6).
Dedicated Cloud	If you use DeC, this parameter is displayed. For details about DB instance specifications in your DeC, see **Database Instance Specifications**.
Node Class	For details about the DB instance specifications, see **DB Instance Specifications**.
Storage Space	The value ranges from 10 GB to 3000 GB and must be a multiple of 10.

Figure 3-15 Network and database configuration

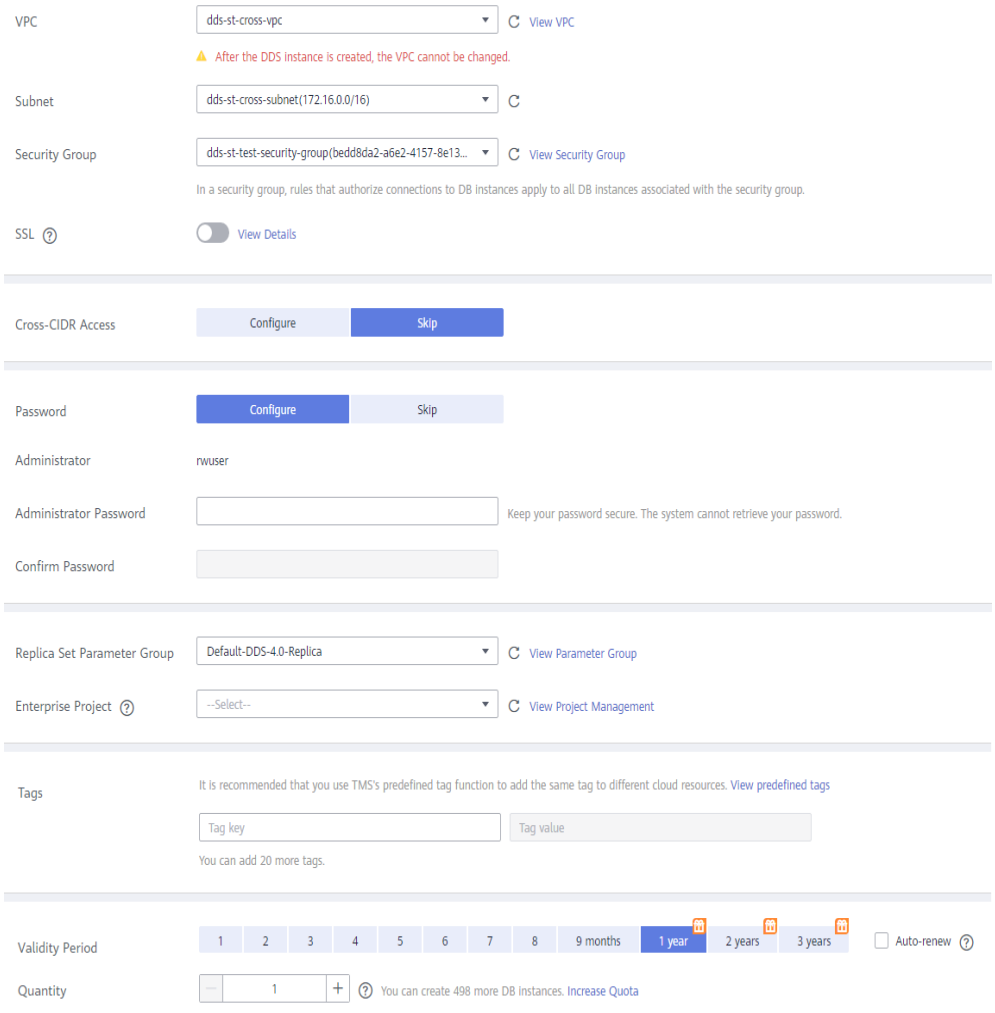


Table 3-20 Network

Parameter	Description
VPC	The VPC where your DB instances are located. A VPC isolates networks for different services, so you can easily manage and configure internal networks and change network configuration. You need to create or select the required VPC. For details about how to create a VPC, see section "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 allocates resources to you by default.
Subnet	A subnet provides dedicated network resources that are logically isolated from other networks for network security. After the instance is created, you can change the private IP address assigned by the subnet. For details, see **Changing a Private IP Address**.
Security Group	A security group controls access between DDS and other services for security. If there are no security groups available, DDS allocates resources to you by default. **NOTE** Ensure that the security group rule you set allows clients to access DB instances. For example, select the TCP protocol with inbound direction, input the default port number **8635**, and enter a subnet IP address or select a security group that the DB instance belongs to.
SSL	Secure Sockets Layer (SSL) certificates set up encrypted connections between clients and servers, preventing data from being tampered with or stolen during transmission. You can enable SSL to improve data security. After a DB instance is created, you can connect to it using SSL.
Cross-CIDR Access	• Configure Add the VPC CIDR block of your client. Ensure that the ECS where your client is installed can connect to the DB instance. **NOTE** – To ensure the ECS and the DB instance can communicate with each other, configure the connection by referring to **VPC Peering Connection Overview**. – VPC CIDR blocks can only be added, but not modified or deleted. – Up to 9 CIDR blocks can be configured, and each of them does not overlap. • 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**.

Parameter	Description
IPv6	Before enabling IPv6, ensure that IPv6 has been enabled for the VPC and subnet where the DB instance is located. For details about the application scenarios and procedures for enabling IPv6 for the VPC and subnet, see **IPv4 and IPv6 Dual-Stack Network**. After IPv6 is enabled, the DB instance can run in dual-stack mode. It means that the DB instance can use both the IPv4 address and IPv6 address. The DB instance can access the Internet using either IPv4 or IPv6 addresses, and the communications are independent of each other.
Anti-affinity Deployment	If you use DeC, this parameter is displayed. This option is enabled by default. Anti-affinity deployment requires the primary, secondary, and hidden nodes to be deployed on different physical machines to achieve high availability.

Table 3-21 Database configuration

Parameter	Description
Password	• Configure Enter and confirm the administrator password for connecting to the DB instance. • Skip Set the administrator password later. When you need to connect to the DB instance, locate the DB instance and click **Reset Password** in the **Operation** column to set a password for connecting to the DB instance.
Administrator	The default account is **rwuser**.
Administrator Password	Set a password for the administrator. The password is a string of 8 to 32 characters. It must be a combination of uppercase letters, lowercase letters, digits, and special characters. You can also use the following special characters: ~!@#%^*-_=+? Keep this password secure. If lost, the system cannot retrieve it for you.
Confirm Password	Enter the administrator password again.
Replica Set Parameter Group	The parameters that apply to the replica set instances. After a DB instance is created, you can change the parameter group you configured for the DB instance to bring out the best performance. For details, see **Editing a Parameter Group**.

Parameter	Description
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**. 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 the *Enterprise Management User Guide*.

Table 3-22 Tag

Parameter	Description
Tags	This setting is optional. Adding tags helps you better identify and manage your DB instances. Up to 20 tags can be added for a DB instance. A tag is composed of a key-value pair. • Key: Mandatory if the DB instance is going to be tagged – Each tag key must be unique for each DB instance. – A tag key consists of up to 36 characters. – The key can only consist of digits, letters, underscores (_), and hyphens (-). • Value: Optional if the DB instance is going to be tagged – The value consists of up to 43 characters. – The value can only consist of digits, letters, underscores (_), dots (.), and hyphens (-). After a DB instance is created, you can view its tag details on the **Tags** tab. In addition, you can add, modify, and delete tags for existing DB instances. For details, see **Tag**.

Table 3-23 Required duration and quantity

Parameter	Description
Validity Period	The system will automatically calculate the fee based on the validity period you have selected.
Auto-renew	• By default, this option is not selected. • If you select this option, the auto-renew cycle is determined by the selected required duration.

Parameter	Description
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. The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

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

NOTE

DB instance performance is determined by how you configure it during the creation. The hardware configuration items that can be selected include the class and storage space of the replica set.

Step 4 On the displayed page, confirm the DB instance information.

- Yearly/Monthly
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify your settings, click **Pay Now** to go to the payment page and complete the payment.
- Pay-per-use
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, click **Submit** to start the instance creation.

Step 5 After a DDS DB instance is created, you can view and manage it on the **Instance Management** 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**.
- DDS enables the automated backup policy by default. After a DB instance is created, you can modify or disable the automated backup policy. An automated full backup is immediately triggered after the creation of a DB instance.
- The default DDS port is 8635, but this port can be modified if necessary. If you change the port, you need to add the security group rule to enable access.
- The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

----End

3.4.3 Step 2: Bind an EIP

Scenarios

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

Precautions

- Before accessing a database, you need to 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 section **Step 3: Set a Security Group**.
- In the replica set instance, only primary and secondary nodes can be bound to an EIP. To change the EIP that has been bound to a node, you need to unbind it from the node first.

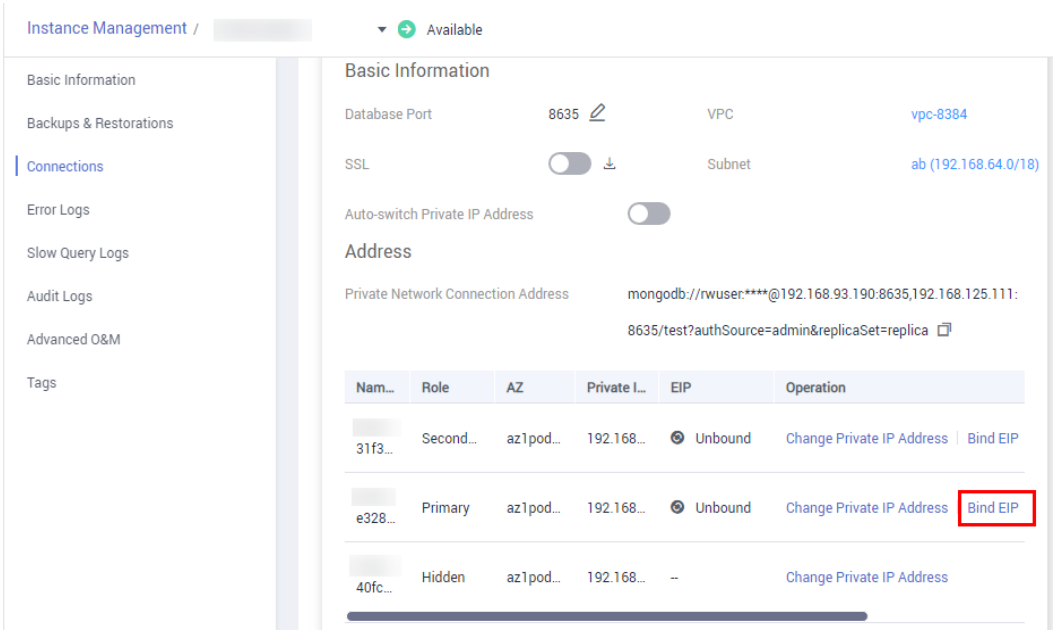
Binding an EIP

Step 1 On the **Instance Management** page, click the target replica set instance.

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

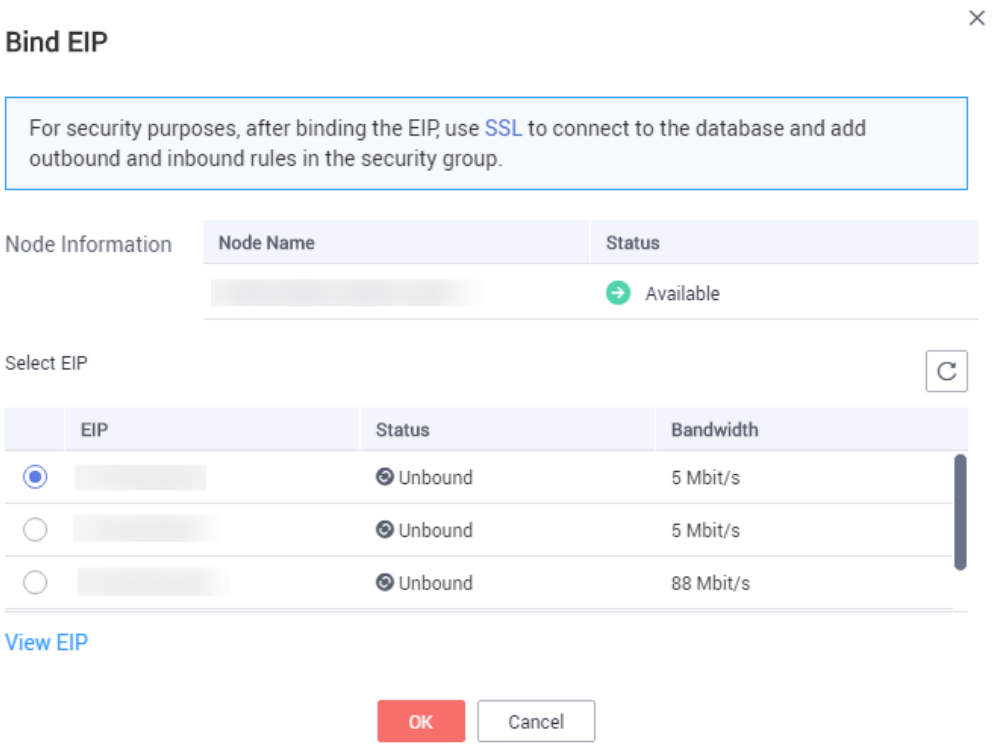
Step 3 In the **Basic Information** area, locate the target node and click **Bind EIP** in the **Operation** column.

Figure 3-16 Binding an EIP



Step 4 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 3-17 Selecting an EIP



Step 5 Locate the target node, in the **EIP** column, view the EIP that is successfully bound.

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

----End

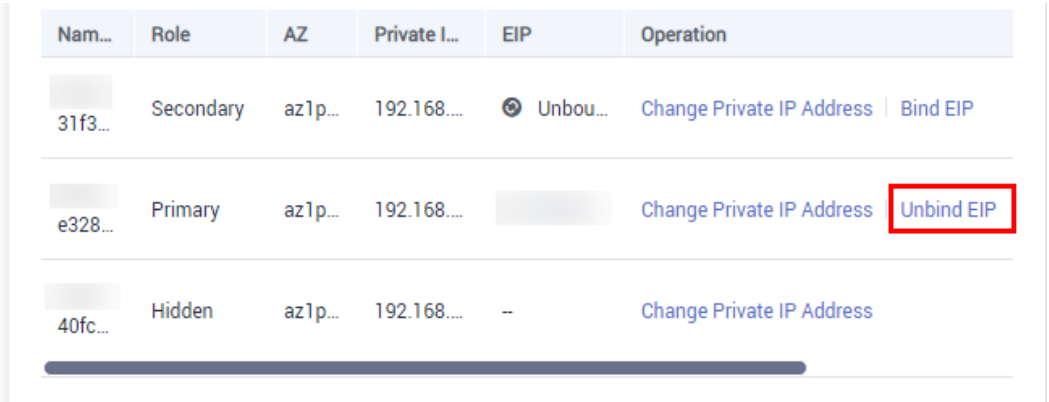
Unbinding an EIP

Step 1 On the **Instance Management** page, click the replica set instance that has been bound with an EIP.

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

Step 3 In the **Basic Information** area, locate the target node and click **Unbind EIP** in the **Operation** column.

Figure 3-18 Unbinding an EIP



Step 4 In the displayed dialog box, click **Yes**.

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

----End

3.4.4 Step 3: Set a Security Group

Scenarios

This section guides you on how to add a security group rule to control access from and to DDS DB instances associated with a security group. The following describes how to set security groups.

Precautions

The default security group rule allows all outgoing data packets. ECSs and DDS DB instances in the same security group can access each other. After a security group is created, you can create different rules for that security group, which allows you to control access to the DB instances that are in it.

To access a DB instance in a security group from a source outside of that group, you need to create an inbound rule.

For details about the constraints on using security groups, see **Security Group Overview**.

Procedure

Step 1 On the **Instance Management** page, click the target replica set instance.

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

Step 3 In the **Security Group** area, on the **Inbound Rules** tab, click **Add Rule**. In the displayed **Add Inbound Rule** dialog box, set required parameters to add inbound rules. On the **Outbound Rules** tab, click **Add Rule**. In the displayed **Add Outbound Rule** dialog box, set required parameters to add outbound rules.

You can click ⊕ to add more rules.

Figure 3-19 Add Inbound Rule

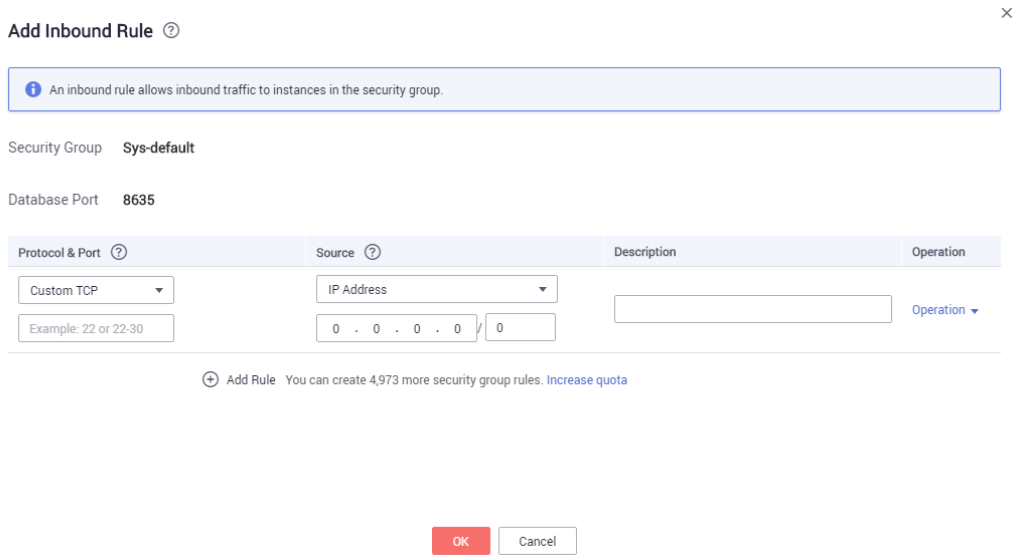
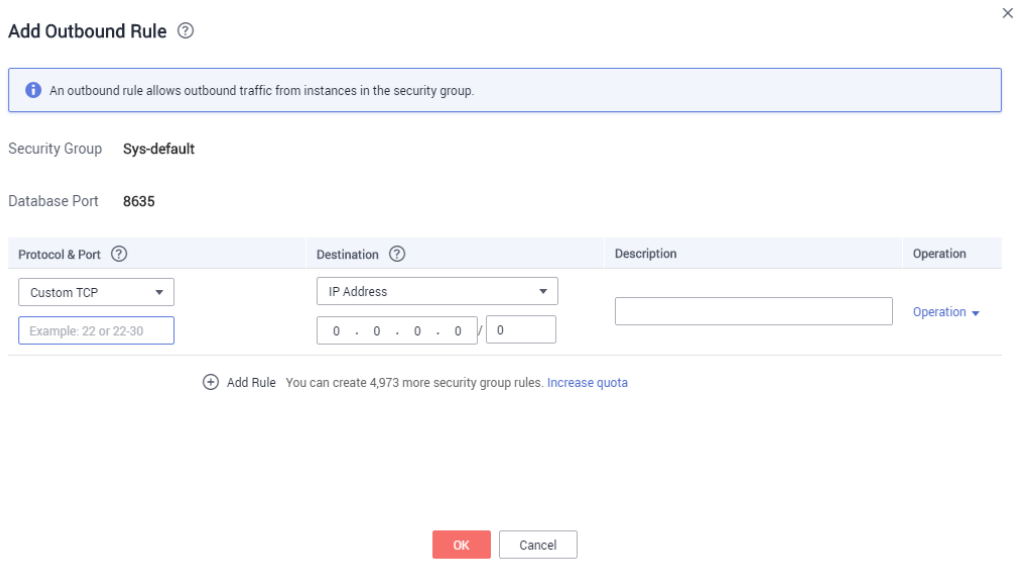


Figure 3-20 Add Outbound Rule



Step 4 Add a security group rule as prompted.

Table 3-24 Parameter description

Parameter	Description	Value Example
Protocol	The network protocol required for access. You can allow all protocols or specify a specific protocol, TCP, UDP, ICMP, and SSH.	TCP

Parameter	Description	Value Example
Port	Specifies the port that allows the access to ECSs or external devices. Common ports are listed in **Common Ports Used by ECSs**.	8635
Source/ Destination	Specifies the supported IP address and security group that the rule applies to. • **IP address**: The IP address or subnet that the rule applies to. Single IP addresses must be expressed using slash notation. – Single IP address: xxx.xxx.xxx.xxx/32 (IPv4) – Subnet: xxx.xxx.xxx.0/24 – All IP addresses: 0.0.0.0/0 • **Security group**: A security group that access will be allowed from. ECSs in this security group will be granted access to DDS instance in the current security group.	• 192.168.10.0/24 • default

Step 5 Click **OK**.

----End

3.4.5 Step 4: Connect to a Replica Set Instance Over Public Networks

Scenarios

This section describes how to connect to a replica set instance using the MongoDB client and Robo 3T over public networks.

You can directly perform operations on the primary and secondary nodes. Primary nodes are used for processing read and write requests. Secondary nodes replicate data from the primary and are used for processing read requests only.

The MongoDB client and Robo 3T can connect to a DB instance with a common connection or an encrypted connection (SSL). To improve data transmission security, you are advised to connect to DB instances using the SSL connection.

Different OS scenarios: The following uses Linux ECS and Window client as an example.

For best practices about connections to a DB instance over public networks, see **Connecting to a DB Instance Through an EIP**.

Prerequisites

1. **Bind an EIP** to the cluster instance and **set security group rules** to ensure that the EIP can be accessed through the ECS or Robo 3T.
2. Install the MongoDB client or Robo 3T.

MongoDB client

a. For details on how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.

b. Install the MongoDB client on the ECS.

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

Robo 3T

Install Robo 3T. For details, see **How Can I Install Robo 3T?**

3. If you select SSL mode, download the SSL certificate on the DDS console.

a. On the **Instance Management** page, click the target DB instance.

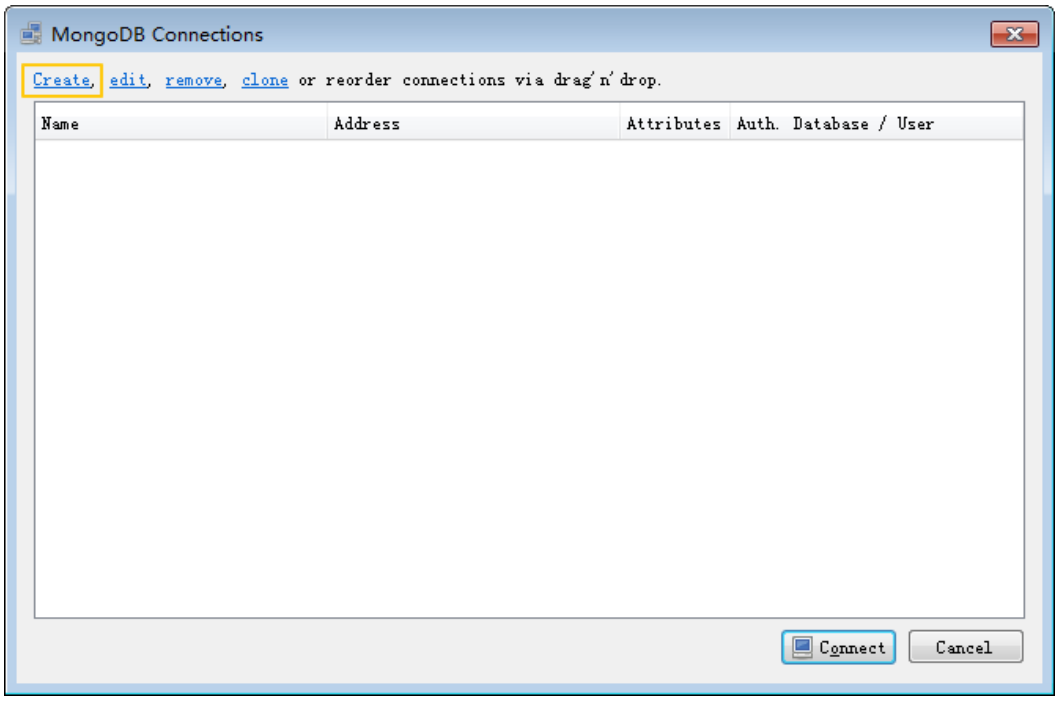
b. In the navigation pane on the left, choose **Connections**.

c. In the **Basic Information** area, click next to the **SSL** field.

Connecting to a DB Instance Using Robo 3T (SSL)

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

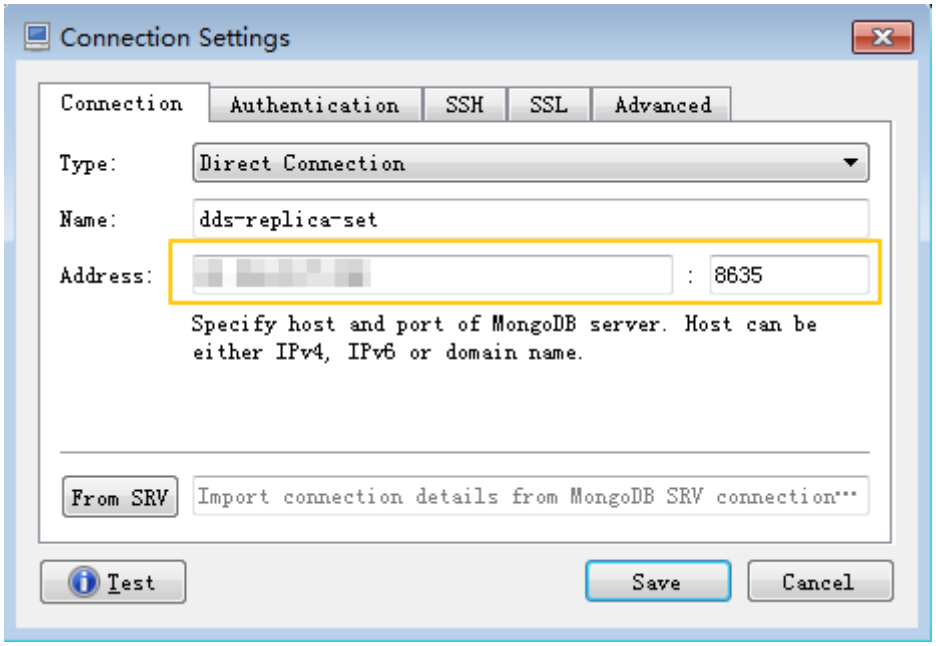
Figure 3-21 Connections



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

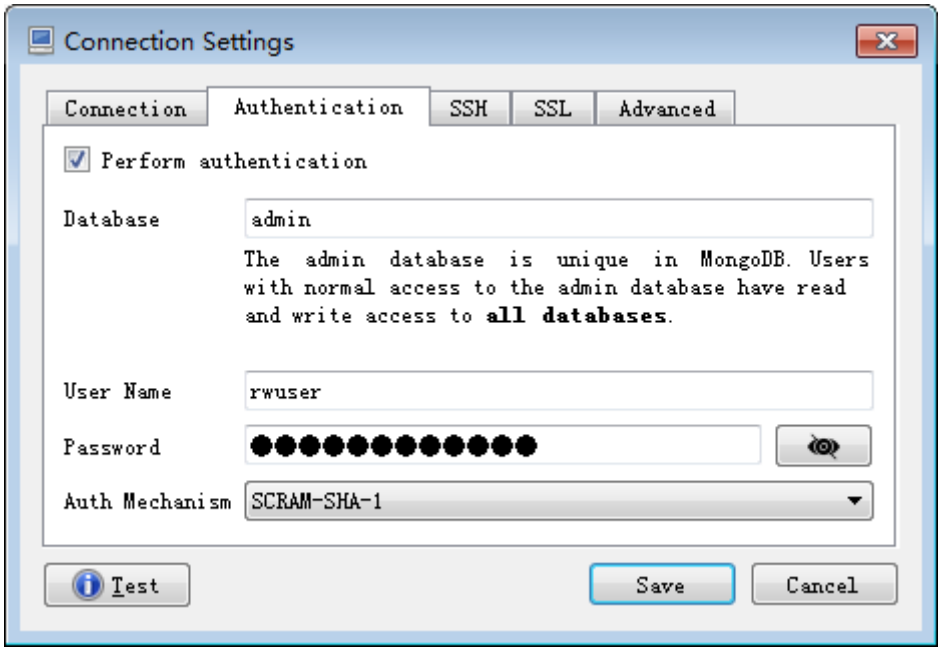
1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the replica set instance in the **Address** text box.

Figure 3-22 Connection



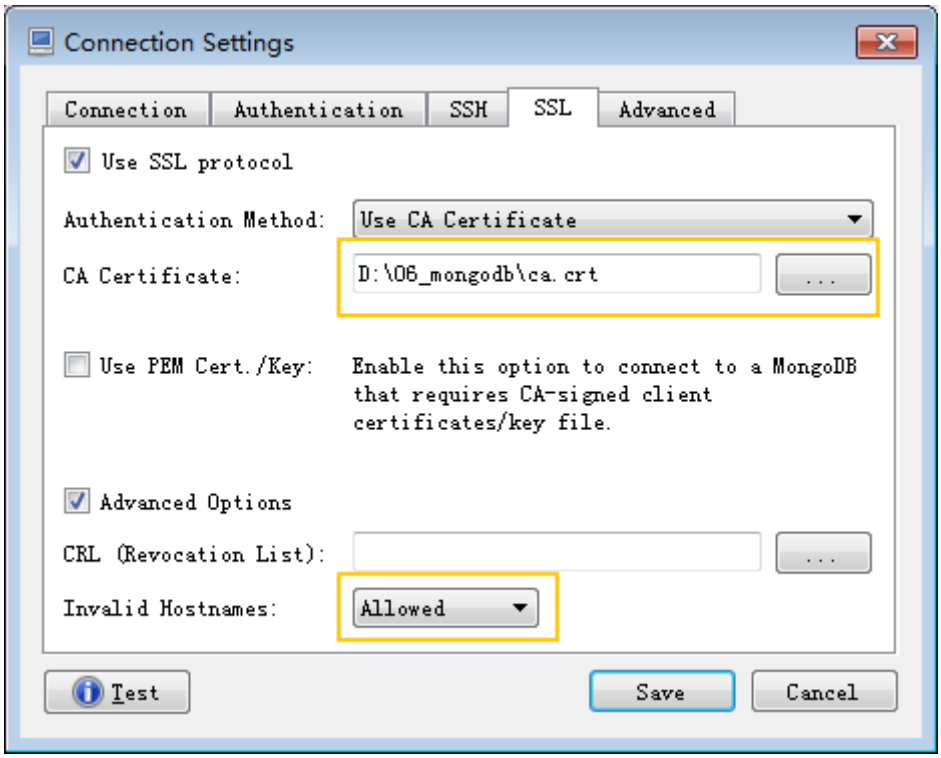
2. On the **Authentication** tab, set **Database** to **admin**, **User Name** to **rwuser**, and **Password** to the administrator password you set during the creation of the replica set instance.

Figure 3-23 Authentication



3. On the **SSL** tab, upload the SSL certificate and select **Allowed** for **Invalid Hostnames**.

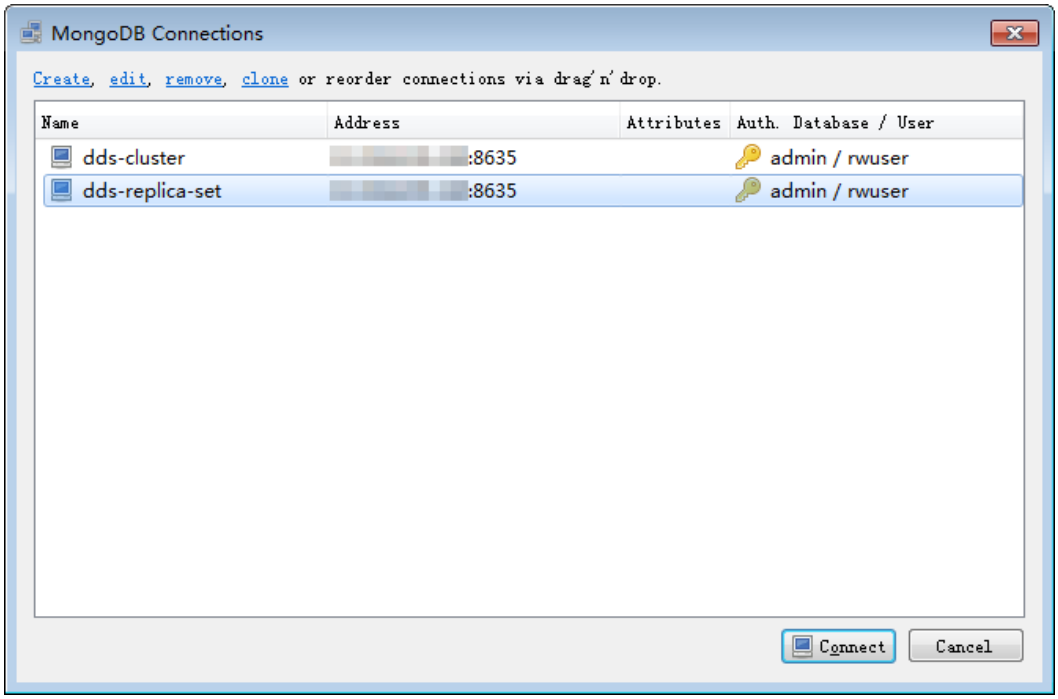
Figure 3-24 SSL



4. Click **Save**.

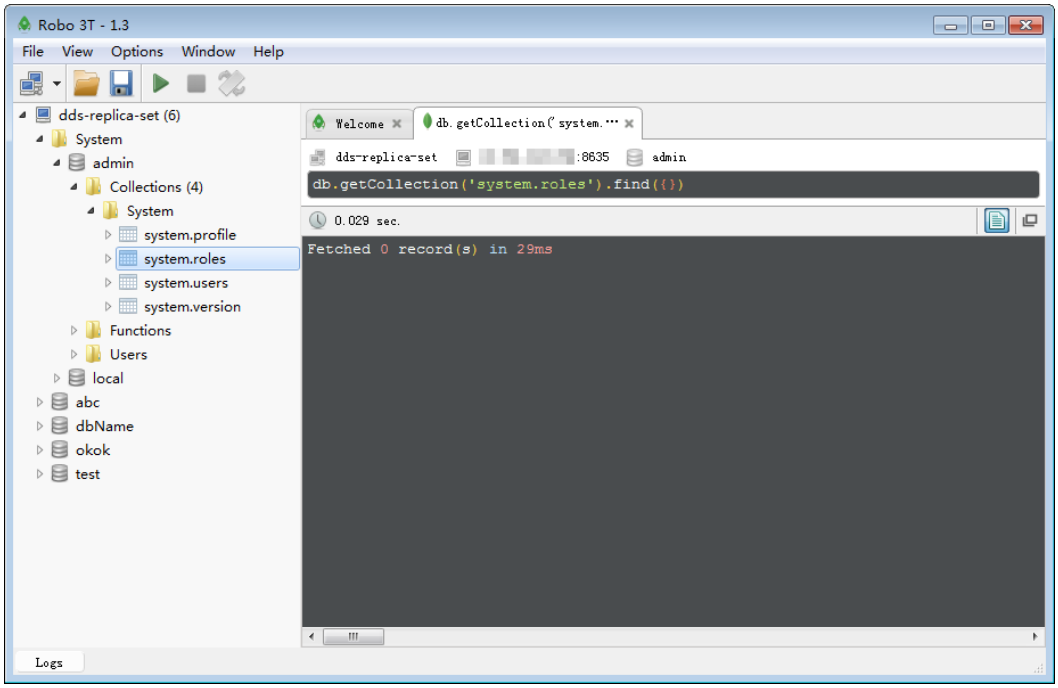
Step 3 On the **MongoDB Connections** page, click **Connect** to connect to the replica set instance.

Figure 3-25 Connections



Step 4 If the replica set instance is successfully connected, the page shown in **Figure 3-26** is displayed.

Figure 3-26 Connection succeeded



----End

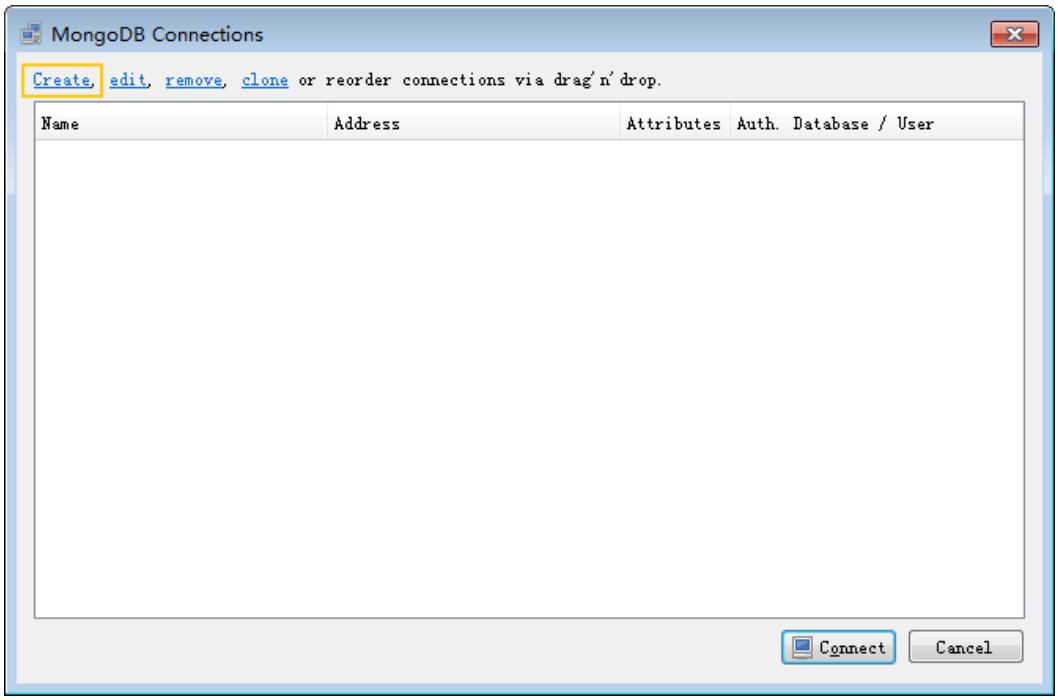
Connecting to a DB Instance Using Robo 3T (Non-SSL)

NOTICE

If you connect to a DB instance using this method, you need to disable the SSL connection. For details about how to disable the SSL connection, see section **Enabling or Disabling SSL**.

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

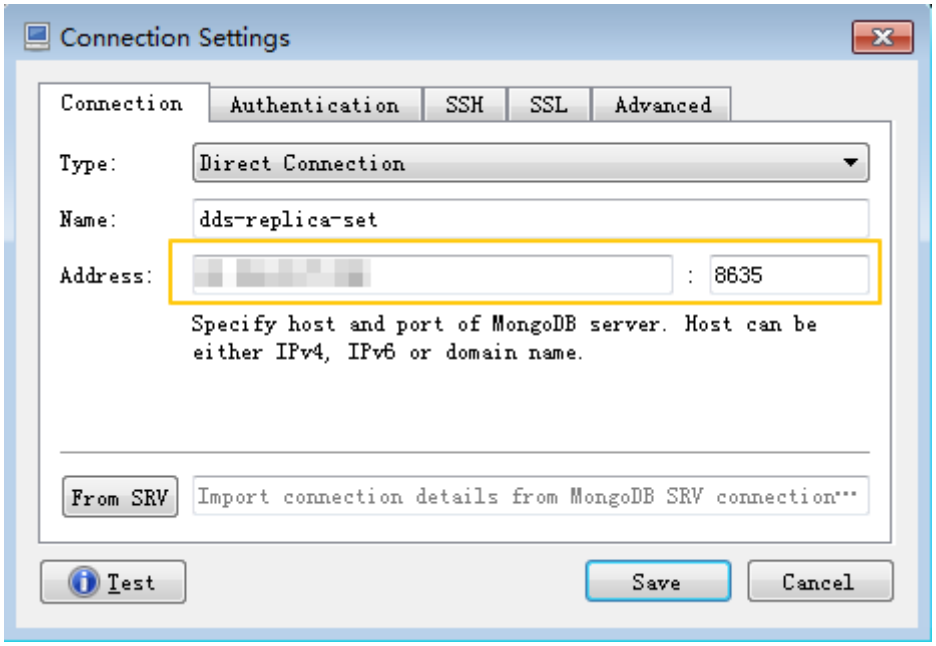
Figure 3-27 Connections



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

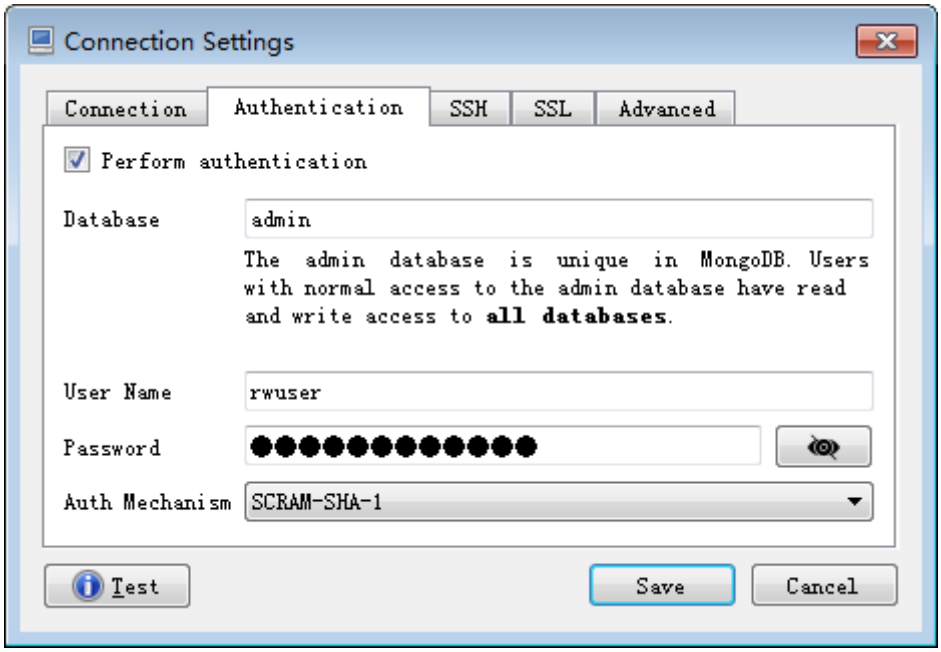
1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the replica set instance in the **Address** text box.

Figure 3-28 Connection



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 replica set instance.

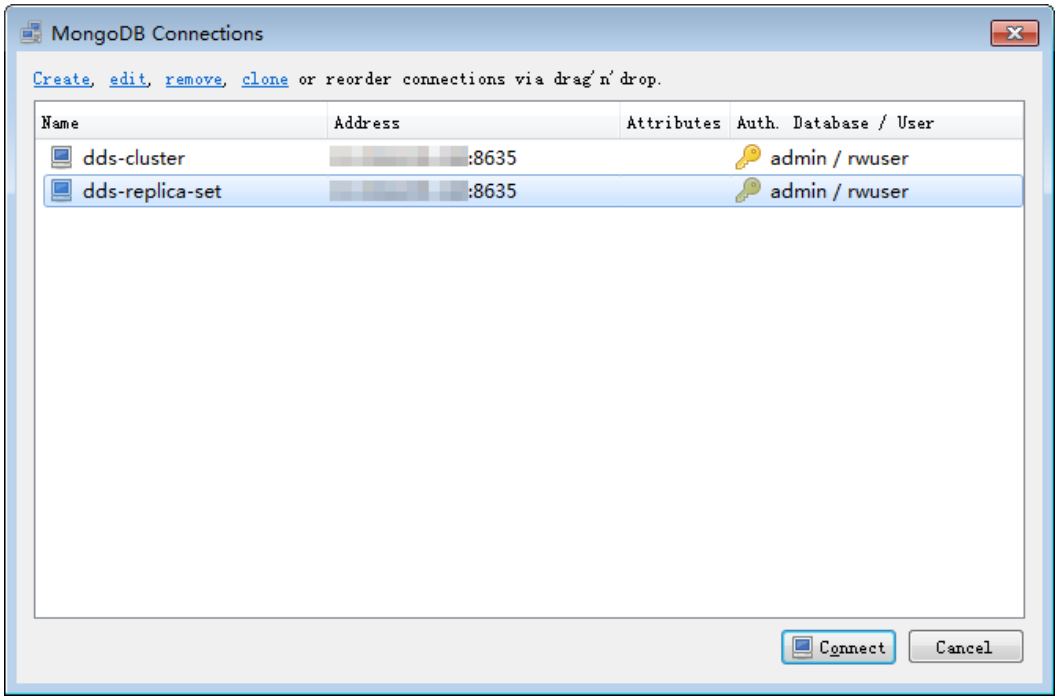
Figure 3-29 Authentication



3. Click **Save**.

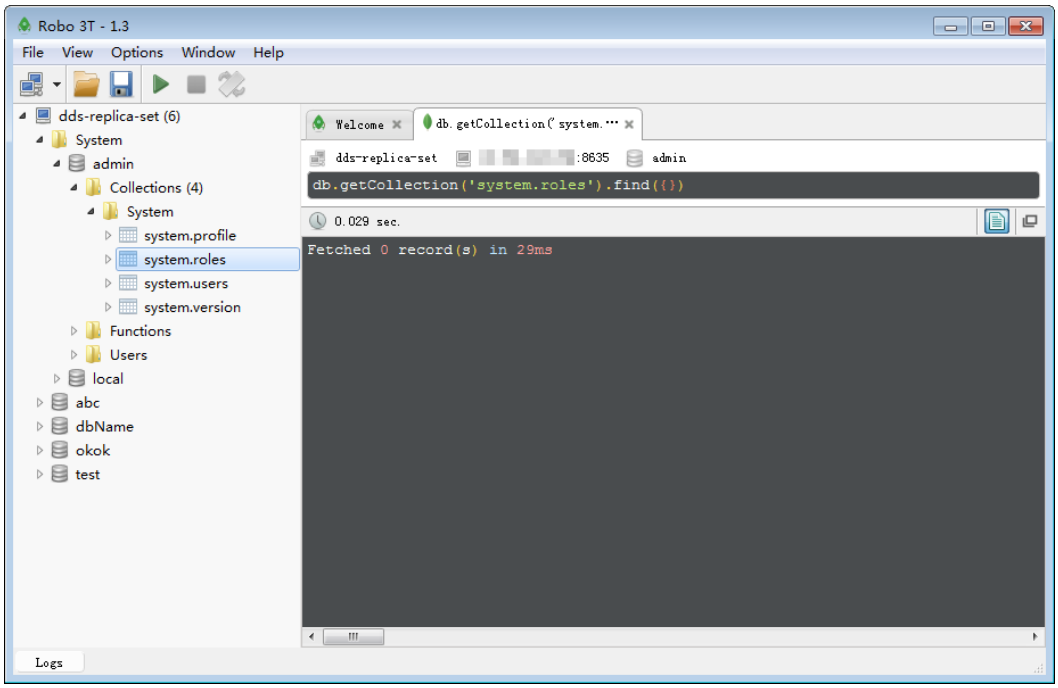
Step 3 On the **MongoDB Connections** page, click **Connect** to connect to the replica set instance.

Figure 3-30 Connections



Step 4 If the replica set instance is successfully connected, the page shown in **Figure 3-31** is displayed.

Figure 3-31 Connection succeeded



----End

Connecting to a DB Instance Using the MongoDB Client (SSL)

Step 1 On the **Instance Management** page, click the target DB instance.

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

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

Step 5 Connect to the DB instance in the directory where the MongoDB client is located.

- Method 1: Using Linux commands

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

Enter the database account password when prompted:

```
Enter password:
```

- Method 2: Using the public connection address

  ./mongo "mongodb://rwuser:******@<*DB_HOST*>:<*DB_PORT*>/test?authSource=admin&replicaSet=replica" --ssl --sslCAFile** <*FILE_PATH*> **--sslAllowInvalidHostnames**

  To obtain the public connection address, click the instance name and choose **Connections**. The address is displayed in **Public Network Connection Address** field on the **Public Connection** tab.

  In contrast to directly connecting to the primary node, this connection mode provides higher data read/write performance and avoids write errors after a primary/standby switchover. For details, see **Connecting to a Replica Set Instance for Read and Write Separation and High Availability** in the *Document Database Service Best Practices*.

NOTE

- A replica set instance uses the management IP address to generate SSL certificate. **--sslAllowInvalidHostnames** is needed for the SSL connection through a public network.
- **DB_HOST** indicates the IP address of the remotely connected DB instance. Obtain the value from the **EIP** column in the node list on the **Connections** page.
- **DB_PORT** indicates the port number. Obtain the value from **Database Port** in the **Basic Information** area on the **Connections** page.
- **DB_USER** indicates the database account name. The default value is **rwuser**.
- ********** indicates the password of the database account. If you use the connection address to connect to a DB instance:
  - If the password contains the at sign (@), change @ to %40.
  - If the password contains the exclamation mark (!), add an escape character (\) before the exclamation mark (!).
- **FILE_PATH** indicates the path where the root certificate is stored.

- Connect to the instance using Linux commands. The following is an example command:

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

- Connect to the DB instance using the public connection address. The following is an example command:

  ./mongo "mongodb://rwuser:**@192.168.1.80:8635/test?authSource=admin&replicaSet=replica" --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames**

Step 6 Check the connection result. If the following information is displayed, the connection is successful.

- Result from connecting the primary node in a replica set:

  ```
  replica:PRIMARY>
  ```

- Result from connecting the secondary node in a replica set:

  ```
  replica:SECONDARY>
  ```

----End

Connecting to a DB Instance Using the MongoDB Client (Non-SSL)

NOTICE

If you connect to a DB instance using this method, you need to disable the SSL connection. For details about how to disable the SSL connection, see section **Enabling or Disabling SSL**.

Step 1 Connect to the ECS.

Step 2 Connect to a DDS DB instance.

- Method 1: Using Linux commands

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

  Enter the database account password when prompted:

  ```
  Enter password:
  ```

- Method 2: Using the public connection address

  ./mongo "mongodb://rwuser:**@**<*DB_HOST*>**:**<*DB_PORT*>**/test?authSource=admin&replicaSet=replica"**

  To obtain the public connection address, click the instance name and choose **Connections**. The address is displayed in **Public Network Connection Address** field on the **Public Connection** tab.

  In contrast to directly connecting to the primary node, this connection mode provides higher data read/write performance and avoids write errors after a primary/standby switchover. For details, see **Connecting to a Replica Set Instance for Read and Write Separation and High Availability** in the *Document Database Service Best Practices*.

  NOTE

  - **DB_HOST** indicates the IP address of the remotely connected DB instance. Obtain the value from the **EIP** column in the node list on the **Connections** page.
  - **DB_PORT** indicates the port number. Obtain the value from **Database Port** in the **Basic Information** area on the **Connections** page.
  - **DB_USER** indicates the database account name. The default value is **rwuser**.
  - ******** indicates the password of the database account. If you use the connection address to connect to a DB instance:
    - If the password contains the at sign (@), change @ to %40.
    - If the password contains the exclamation mark (!), add an escape character (\) before the exclamation mark (!).

- Connect to the instance using Linux commands. The following is an example command:

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

- Connect to the DB instance using the public connection address. The following is an example command:

  ./mongo "mongodb://rwuser:**@192.168.1.80:8635/test?authSource=admin&replicaSet=replica"**

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

- Result from connecting the primary node in a replica set:
  ```
  replica:PRIMARY>
  ```
- Result from connecting the secondary node in a replica set:
  ```
  replica:SECONDARY>
  ```

----End

4 Getting Started with Single Nodes

4.1 Connection Methods

HUAWEI CLOUD DDS can be accessed using Data Admin Service (DAS), private networks, and public networks.

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. For details, see **Step 2: Connect to a Single Node Instance Through DAS**.

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

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 that is in the same region, AZ, and VPC subnet as your DDS DB instance, you are advised to use a private IP address to connect the ECS to your DDS DB instances. • By default, DDS is not accessible from ECSs that are not in the same security group. If the ECS is not in the same group, you need to add an inbound rule to enable access. • The default DDS port is 8635, but this port can be modified if necessary.	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, you are advised to 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.

4.2 Connecting to Single Node Instances Through DAS

4.2.1 Overview

Scenarios

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 single node instance on the management console and how to connect to the single node instance through DAS.

Process

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

- **Step 1: Buy a Single Node Instance**
- **Step 2: Connect to a Replica Set Instance Through DAS**

4.2.2 Step 1: Buy a Single Node Instance

Scenarios

This section describes how to create a single node instance on the DDS management console. Currently, DDS single node instance supports the yearly/monthly and pay-per-use billing modes. DDS allows you to tailor your computing resources and storage space to your business needs.

You can use your account to create a maximum of 20 single nodes in total.

Prerequisites

- You have registered a HUAWEI CLOUD account.
- Your account balance is greater than or equal to ¥0.

Procedure

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

Step 2 On the **Instance Management** page, click **Buy DB Instance**.

Step 3 On the displayed page, select a billing mode, select your DB instance specifications and click **Next**.

Figure 4-1 Billing mode and basic information

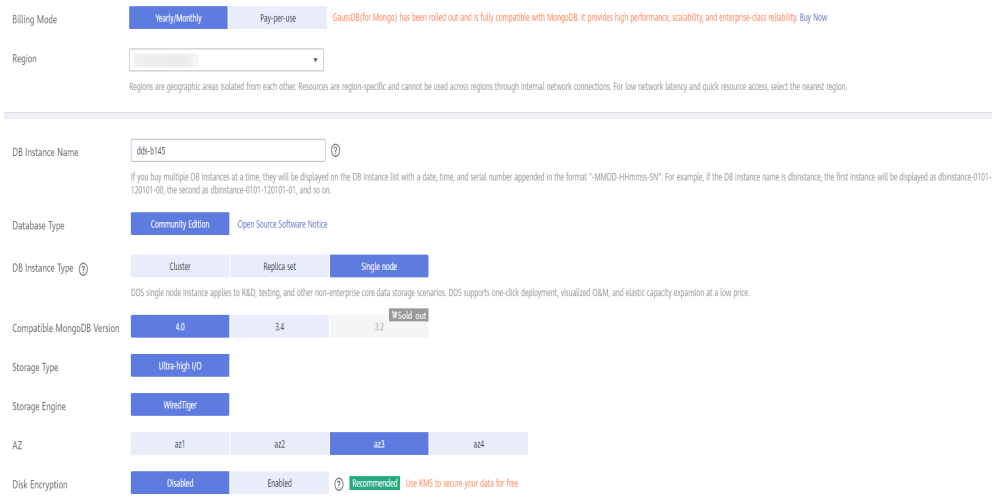


Table 4-2 Billing mode

Parameter	Description
Billing Mode	Select a billing mode, **Yearly/Monthly** or **Pay-per-use**. • Yearly/Monthly – You need to set **Validity Period** as required. Then, the system deducts the fees incurred at one time from your account based on the service price. – When you renew a yearly/monthly DB instance, you can change its billing mode from yearly/monthly to pay-per-use based on your service requirements. For details, see **Changing Yearly/Monthly Instances to a Pay-per-Use**. **NOTE** DB instances paid in yearly/monthly mode cannot be deleted. They support only resource unsubscription. For details, see section **Unsubscribing from a Yearly/Monthly DB Instance**. • Pay-per-use – You do not need to set **Validity Period** because the system deducts the fees incurred from your account based on the service duration. – If you want to use a DB instance at a low cost for a long period of time, you can change its billing mode from pay-per-use to yearly/monthly. For details, see **Changing the Billing Mode in Batches**.

Table 4-3 Basic information

Parameter	Description
DB Instance Name	The DB instance name can be 4 to 64 characters long. It must start with a letter and can contain only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_). If you buy multiple DB instances, you can only enter 4 to 49 characters to set the DB instance name, and then the system automatically appends a date, time, and serial number to the end of the instance names (format: *instance_name-MMDD-HHmmss-SN*). After the DB instance is created, you can change its name. For details, see **Modifying the DB Instance Name**.
Database Type	Community Edition
DB Instance Type	Select **Single Node**. The single node architecture is another option for you, helping you reduce costs while ensuring data reliability.

Parameter	Description
Compatible MongoDB Version	• 4.0 • 3.4 • 3.2
CPU Type	Currently, DDS supports two CPU architectures: x86 and Kunpeng. The two architectures have similar capabilities and performance, both of which can meet your service requirements. For details about the instance types, versions, and specifications supported by the two CPU architectures, see **DB Instance Specifications**.
Storage Type	The default storage type is ultra-high I/O.
Storage Engine	WiredTiger
AZ	An AZ is a part of a region with its own independent power supplies and networks. AZs are physically isolated but can communicate through an internal network connection.
Disk Encryption	• **Disabled**: Disable the encryption function. • **Enabled**: Enable the encryption function. 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 a DB instance is created, the disk encryption status and the key cannot be changed. The backup data stored in OBS is not encrypted. – The key cannot be disabled, deleted, or frozen when being used. Otherwise, the database becomes unavailable. – For details about how to create a key, see the "Creating a CMK" section in the *Data Encryption Workshop User Guide*.

Figure 4-2 Instance class and storage space

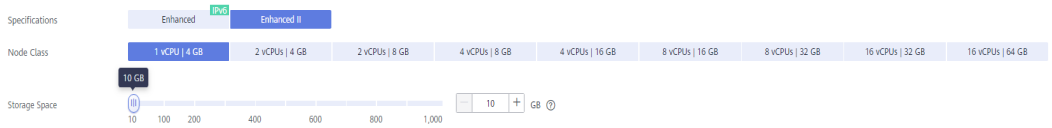


Table 4-4 Specifications

Parameter	Description
Specifications	In the x86 CPU architecture, the following specifications can be selected to suit different application scenarios: General-purpose (s6), Enhanced (c3), and Enhanced II (c6).
Node Class	For details about the DB instance specifications, see **DB Instance Specifications**.
Storage Space	The value ranges from 10 GB to 1,000 GB and must be a multiple of 10.

Figure 4-3 Network and database configuration

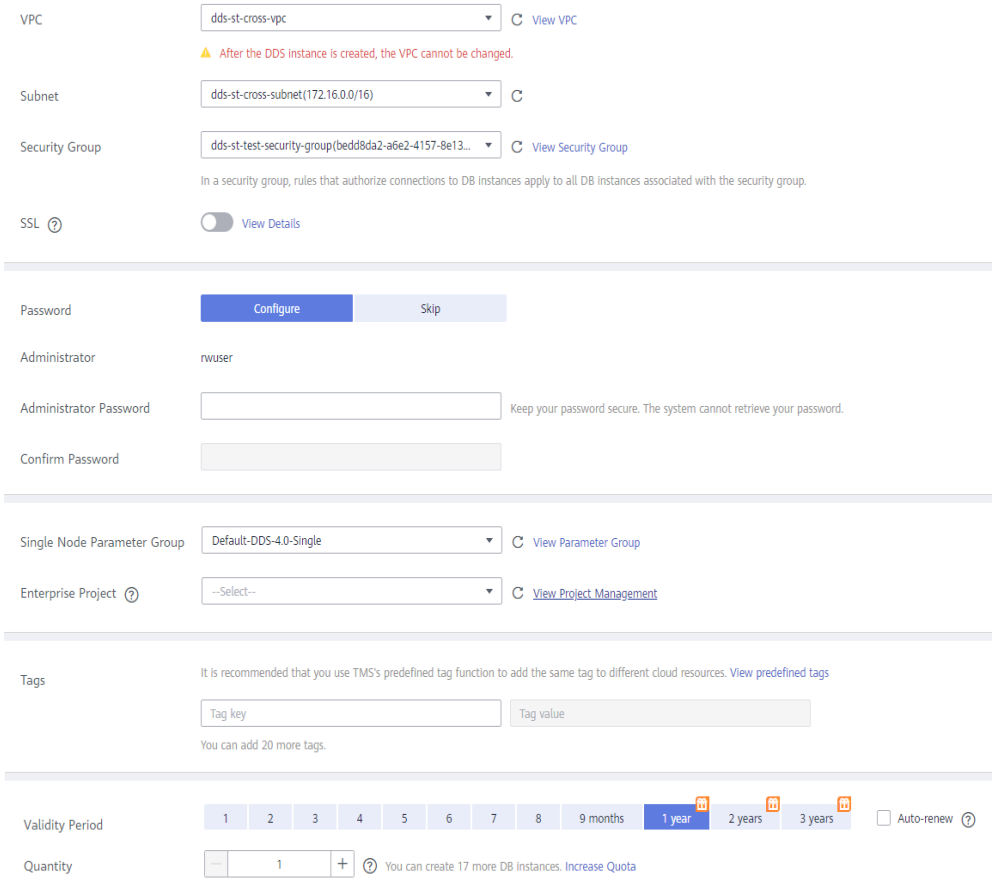


Table 4-5 Network

Parameter	Description
VPC	The VPC where your DB instances are located. A VPC isolates networks for different services, so you can easily manage and configure internal networks and change network configuration. You need to create or select the required VPC. For details about how to create a VPC, see section "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 allocates resources to you by default.
Subnet	A subnet provides dedicated network resources that are logically isolated from other networks for network security. After the instance is created, you can change the private IP address assigned by the subnet. For details, see **Changing a Private IP Address**.
Security Group	A security group controls access between DDS and other services for security. If there are no security groups available, DDS allocates resources to you by default. **NOTE** Ensure that the security group rule you set allows clients to access DB instances. For example, select the TCP protocol with inbound direction, input the default port number **8635**, and enter a subnet IP address or select a security group that the DB instance belongs to.
SSL	Secure Sockets Layer (SSL) certificates set up encrypted connections between clients and servers, preventing data from being tampered with or stolen during transmission. You can enable SSL to improve data security. After a DB instance is created, you can connect to it using SSL.
IPv6	Before enabling IPv6, ensure that IPv6 has been enabled for the VPC and subnet where the DB instance is located. For details about the application scenarios and procedures for enabling IPv6 for the VPC and subnet, see **IPv4 and IPv6 Dual-Stack Network**. After IPv6 is enabled, the DB instance can run in dual-stack mode. It means that the DB instance can use both the IPv4 address and IPv6 address. The DB instance can access the Internet using either IPv4 or IPv6 addresses, and the communications are independent of each other.

Table 4-6 Database configuration

Parameter	Description
Password	• Configure Enter and confirm the administrator password for connecting to the DB instance. • Skip Set the administrator password later. When you need to connect to the DB instance, locate the DB instance and click **Reset Password** in the **Operation** column to set a password for connecting to the DB instance.
Administrator	The default account is **rwuser**.
Administrator Password	Set a password for the administrator. The password is a string of 8 to 32 characters. It must be a combination of uppercase letters, lowercase letters, digits, and special characters. You can also use the following special characters: ~!@#%^*-_=+? Keep this password secure. If lost, the system cannot retrieve it for you.
Confirm Password	Enter the administrator password again.
Single Node Parameter Group	The parameters that apply to single node instances. After a DB instance is created, you can change the parameter group you configured for the DB instance to bring out the best performance. For details, see **Editing a Parameter Group**.
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**. 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 the *Enterprise Management User Guide*.

Table 4-7 Tag

Parameter	Description
Tags	This setting is optional. Adding tags helps you better identify and manage your DB instances. Up to 20 tags can be added for a DB instance. A tag is composed of a key-value pair. ● Key: Mandatory if the DB instance is going to be tagged – Each tag key must be unique for each DB instance. – A tag key consists of up to 36 characters. – The key can only consist of digits, letters, underscores (_), and hyphens (-). ● Value: Optional if the DB instance is going to be tagged – The value consists of up to 43 characters. – The value can only consist of digits, letters, underscores (_), dots (.), and hyphens (-). After a DB instance is created, you can view its tag details on the **Tags** tab. In addition, you can add, modify, and delete tags for existing DB instances. For details, see **Tag**.

Table 4-8 Required duration and quantity

Parameter	Description
Validity Period	The system will automatically calculate the fee based on the validity period you have selected.
Auto-renew	● By default, this option is not selected. ● If you select this option, the auto-renew cycle is determined by the selected required duration.
Quantity	The purchase quantity depends on the single node 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. The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

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

NOTE

DB instance performance is determined by how you configure it during the creation. The hardware configuration items that can be selected include the node class and storage space.

Step 4 On the displayed page, confirm the DB instance information.

- Yearly/Monthly
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify your settings, click **Pay Now** to go to the payment page and complete the payment.
- Pay-per-use
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, click **Submit** to start the instance creation.

Step 5 After a DDS DB instance is created, you can view and manage it on the **Instance Management** 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**.
- DDS enables the automated backup policy by default. After a DB instance is created, you can modify or disable the automated backup policy. An automated full backup is immediately triggered after the creation of a DB instance.
- The default DDS port is 8635, but this port can be modified if necessary. If you change the port, you need to add the security group rule to enable access.
- The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

----End

4.2.3 Step 2: Connect to a Single Node Instance Through DAS

Scenarios

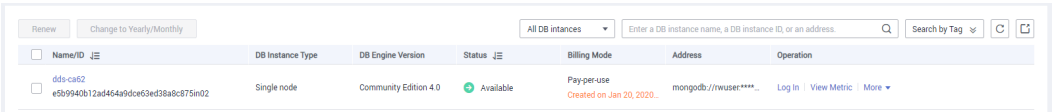
Data Admin Service (DAS) enables you to manage DB instances on a web-based console, simplifying database management and improving working efficiency. By default, you have the remote login permission. It is recommended that you use the DAS service to connect to DB instances, which is more secure and convenient.

Procedure

Step 1 On the **Instance Management** page, locate the target DB instance and click **Log In** in the **Operation** column.

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

Figure 4-4 Instance management



Step 2 On the displayed login page, enter the administrator username and password and click **Login**.

For details about how to manage databases through DAS, see **User Interface Overview**.

----End

4.3 Connecting to a Single-Node Instance Over Private Networks

4.3.1 Overview

Scenarios

This section describes how to buy a single node instance on the management console, set a security group, and connect to a single node instance over private networks.

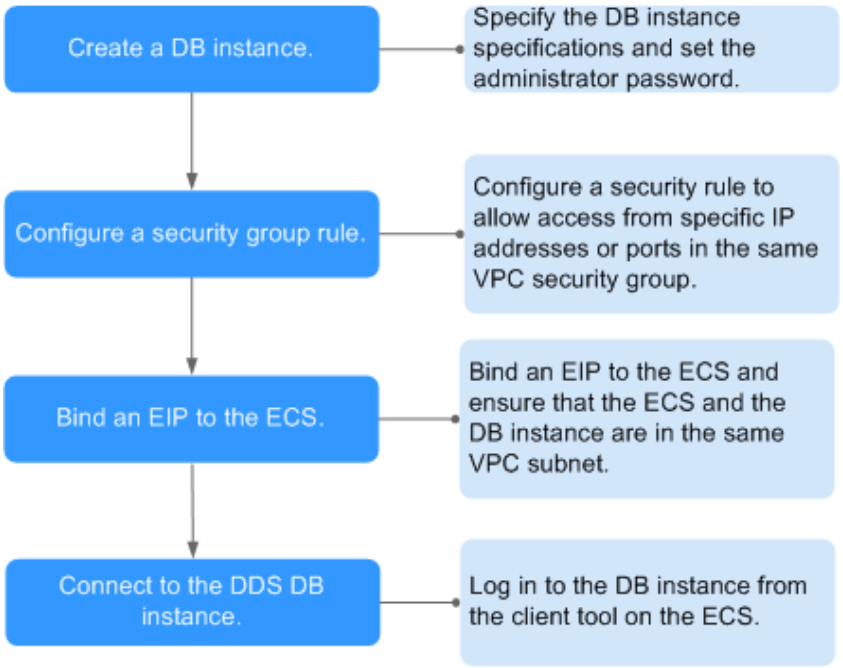
Process

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

- **Step 1: Buy a Single Node Instance**
- **Step 2: Set a Security Group**
- **Step 3: Connect to a Single Node Instance Over Private Networks**

The following describes the steps from creating a DB instance to using it.

Figure 4-5 Accessing DB instances from a private network



4.3.2 Step 1: Buy a Single Node Instance

Scenarios

This section describes how to create a single node instance on the DDS management console. Currently, DDS single node instance supports the yearly/monthly and pay-per-use billing modes. DDS allows you to tailor your computing resources and storage space to your business needs.

You can use your account to create a maximum of 20 single nodes in total.

Prerequisites

- You have registered a HUAWEI CLOUD account.
- Your account balance is greater than or equal to ¥0.

Procedure

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

Step 2 On the **Instance Management** page, click **Buy DB Instance**.

Step 3 On the displayed page, select a billing mode, select your DB instance specifications and click **Next**.

Figure 4-6 Billing mode and basic information

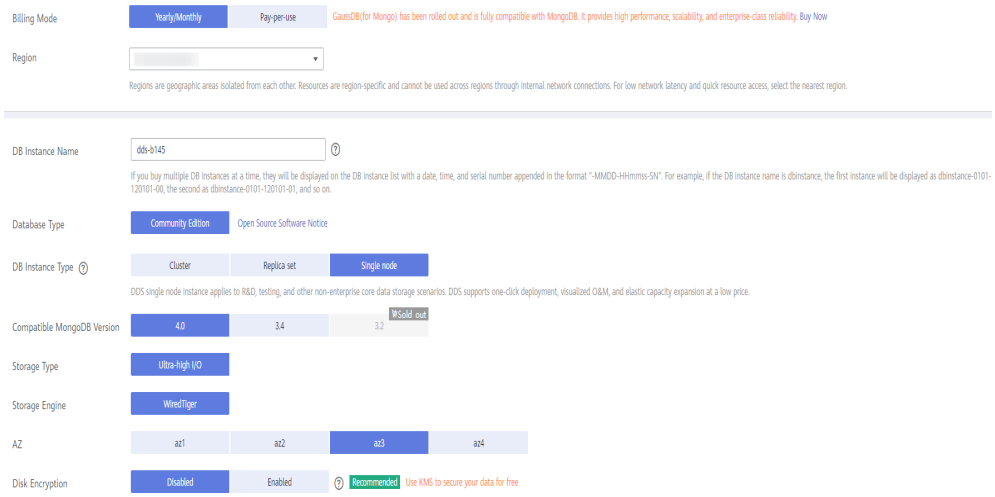


Table 4-9 Billing mode

Parameter	Description
Billing Mode	Select a billing mode, **Yearly/Monthly** or **Pay-per-use**. • Yearly/Monthly – You need to set **Validity Period** as required. Then, the system deducts the fees incurred at one time from your account based on the service price. – When you renew a yearly/monthly DB instance, you can change its billing mode from yearly/monthly to pay-per-use based on your service requirements. For details, see **Changing Yearly/Monthly Instances to a Pay-per-Use**. **NOTE** DB instances paid in yearly/monthly mode cannot be deleted. They support only resource unsubscription. For details, see section **Unsubscribing from a Yearly/Monthly DB Instance**. • Pay-per-use – You do not need to set **Validity Period** because the system deducts the fees incurred from your account based on the service duration. – If you want to use a DB instance at a low cost for a long period of time, you can change its billing mode from pay-per-use to yearly/monthly. For details, see **Changing the Billing Mode in Batches**.

Table 4-10 Basic information

Parameter	Description
DB Instance Name	The DB instance name can be 4 to 64 characters long. It must start with a letter and can contain only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_). If you buy multiple DB instances, you can only enter 4 to 49 characters to set the DB instance name, and then the system automatically appends a date, time, and serial number to the end of the instance names (format: *instance_name-MMDD-HHmmss-SN*). After the DB instance is created, you can change its name. For details, see **Modifying the DB Instance Name**.
Database Type	Community Edition
DB Instance Type	Select **Single Node**. The single node architecture is another option for you, helping you reduce costs while ensuring data reliability.

Parameter	Description
Compatible MongoDB Version	• 4.0 • 3.4 • 3.2
CPU Type	Currently, DDS supports two CPU architectures: x86 and Kunpeng. The two architectures have similar capabilities and performance, both of which can meet your service requirements. For details about the instance types, versions, and specifications supported by the two CPU architectures, see **DB Instance Specifications**.
Storage Type	The default storage type is ultra-high I/O.
Storage Engine	WiredTiger
AZ	An AZ is a part of a region with its own independent power supplies and networks. AZs are physically isolated but can communicate through an internal network connection.
Disk Encryption	• **Disabled**: Disable the encryption function. • **Enabled**: Enable the encryption function. 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 a DB instance is created, the disk encryption status and the key cannot be changed. The backup data stored in OBS is not encrypted. – The key cannot be disabled, deleted, or frozen when being used. Otherwise, the database becomes unavailable. – For details about how to create a key, see the "Creating a CMK" section in the *Data Encryption Workshop User Guide*.

Figure 4-7 Instance class and storage space

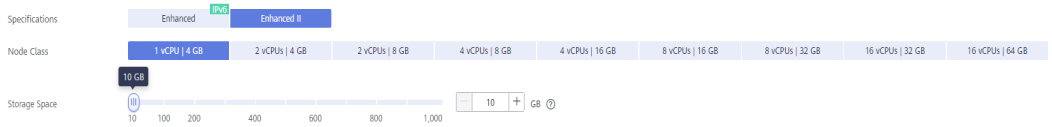


Table 4-11 Specifications

Parameter	Description
Specifications	In the x86 CPU architecture, the following specifications can be selected to suit different application scenarios: General-purpose (s6), Enhanced (c3), and Enhanced II (c6).
Node Class	For details about the DB instance specifications, see **DB Instance Specifications**.
Storage Space	The value ranges from 10 GB to 1,000 GB and must be a multiple of 10.

Figure 4-8 Network and database configuration

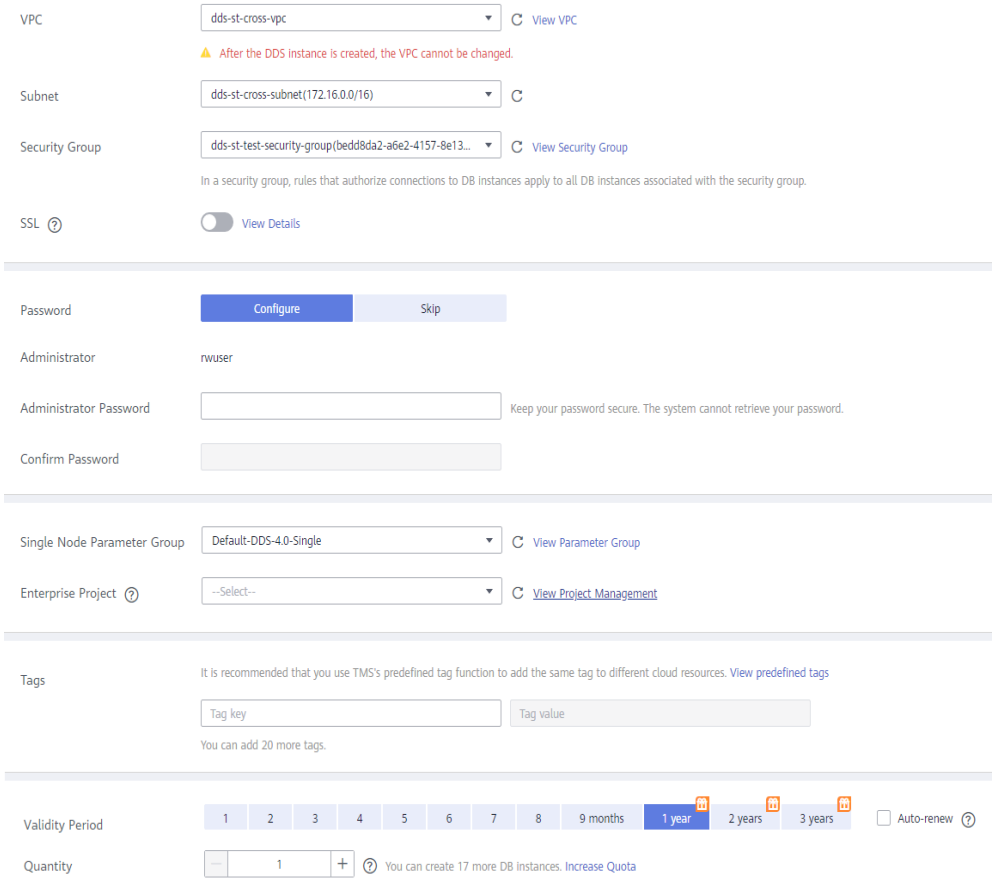


Table 4-12 Network

Parameter	Description
VPC	The VPC where your DB instances are located. A VPC isolates networks for different services, so you can easily manage and configure internal networks and change network configuration. You need to create or select the required VPC. For details about how to create a VPC, see section "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 allocates resources to you by default.
Subnet	A subnet provides dedicated network resources that are logically isolated from other networks for network security. After the instance is created, you can change the private IP address assigned by the subnet. For details, see **Changing a Private IP Address**.
Security Group	A security group controls access between DDS and other services for security. If there are no security groups available, DDS allocates resources to you by default. **NOTE** Ensure that the security group rule you set allows clients to access DB instances. For example, select the TCP protocol with inbound direction, input the default port number **8635**, and enter a subnet IP address or select a security group that the DB instance belongs to.
SSL	Secure Sockets Layer (SSL) certificates set up encrypted connections between clients and servers, preventing data from being tampered with or stolen during transmission. You can enable SSL to improve data security. After a DB instance is created, you can connect to it using SSL.
IPv6	Before enabling IPv6, ensure that IPv6 has been enabled for the VPC and subnet where the DB instance is located. For details about the application scenarios and procedures for enabling IPv6 for the VPC and subnet, see **IPv4 and IPv6 Dual-Stack Network**. After IPv6 is enabled, the DB instance can run in dual-stack mode. It means that the DB instance can use both the IPv4 address and IPv6 address. The DB instance can access the Internet using either IPv4 or IPv6 addresses, and the communications are independent of each other.

Table 4-13 Database configuration

Parameter	Description
Password	• Configure Enter and confirm the administrator password for connecting to the DB instance. • Skip Set the administrator password later. When you need to connect to the DB instance, locate the DB instance and click **Reset Password** in the **Operation** column to set a password for connecting to the DB instance.
Administrator	The default account is **rwuser**.
Administrator Password	Set a password for the administrator. The password is a string of 8 to 32 characters. It must be a combination of uppercase letters, lowercase letters, digits, and special characters. You can also use the following special characters: ~!@#%^*-_=+? Keep this password secure. If lost, the system cannot retrieve it for you.
Confirm Password	Enter the administrator password again.
Single Node Parameter Group	The parameters that apply to single node instances. After a DB instance is created, you can change the parameter group you configured for the DB instance to bring out the best performance. For details, see **Editing a Parameter Group**.
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**. 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 the *Enterprise Management User Guide*.

Table 4-14 Tag

Parameter	Description
Tags	This setting is optional. Adding tags helps you better identify and manage your DB instances. Up to 20 tags can be added for a DB instance. A tag is composed of a key-value pair. ● Key: Mandatory if the DB instance is going to be tagged – Each tag key must be unique for each DB instance. – A tag key consists of up to 36 characters. – The key can only consist of digits, letters, underscores (_), and hyphens (-). ● Value: Optional if the DB instance is going to be tagged – The value consists of up to 43 characters. – The value can only consist of digits, letters, underscores (_), dots (.), and hyphens (-). After a DB instance is created, you can view its tag details on the **Tags** tab. In addition, you can add, modify, and delete tags for existing DB instances. For details, see **Tag**.

Table 4-15 Required duration and quantity

Parameter	Description
Validity Period	The system will automatically calculate the fee based on the validity period you have selected.
Auto-renew	● By default, this option is not selected. ● If you select this option, the auto-renew cycle is determined by the selected required duration.
Quantity	The purchase quantity depends on the single node 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. The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

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

NOTE

DB instance performance is determined by how you configure it during the creation. The hardware configuration items that can be selected include the node class and storage space.

Step 4 On the displayed page, confirm the DB instance information.

- Yearly/Monthly
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify your settings, click **Pay Now** to go to the payment page and complete the payment.
- Pay-per-use
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, click **Submit** to start the instance creation.

Step 5 After a DDS DB instance is created, you can view and manage it on the **Instance Management** 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**.
- DDS enables the automated backup policy by default. After a DB instance is created, you can modify or disable the automated backup policy. An automated full backup is immediately triggered after the creation of a DB instance.
- The default DDS port is 8635, but this port can be modified if necessary. If you change the port, you need to add the security group rule to enable access.
- The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

----End

4.3.3 Step 2: Set a Security Group

Scenarios

This section guides you on how to add a security group rule to control access from and to DDS DB instances in a security group.

Precautions

The default security group rule allows all outgoing data packets. ECSs and DDS DB instances in the same security group can access each other. After a security group is created, you can create different rules for that security group, which allows you to control access to the DB instances that are in it.

To access a DB instance in a security group from a source outside of that group, you need to create an inbound rule.

For details about the constraints on using security groups, see **Security Group Overview**.

Procedure

Step 1 On the **Instance Management** page, click the target single node instance.

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

Step 3 In the **Security Group** area, on the **Inbound Rules** tab, click **Add Rule**. In the displayed **Add Inbound Rule** dialog box, set required parameters to add inbound rules. On the **Outbound Rules** tab, click **Add Rule**. In the displayed **Add Outbound Rule** dialog box, set required parameters to add outbound rules.

You can click ⊕ to add more rules.

Figure 4-9 Add Inbound Rule

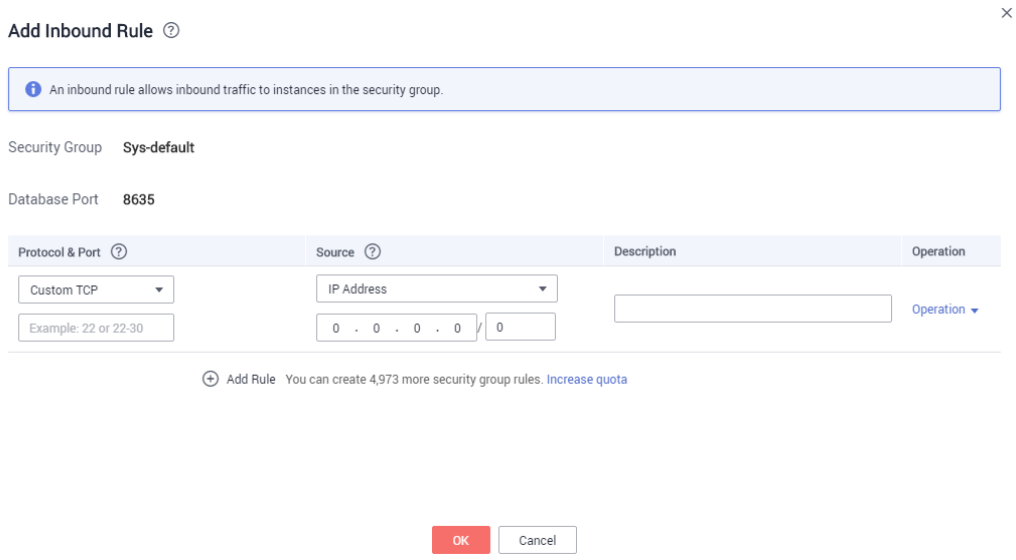
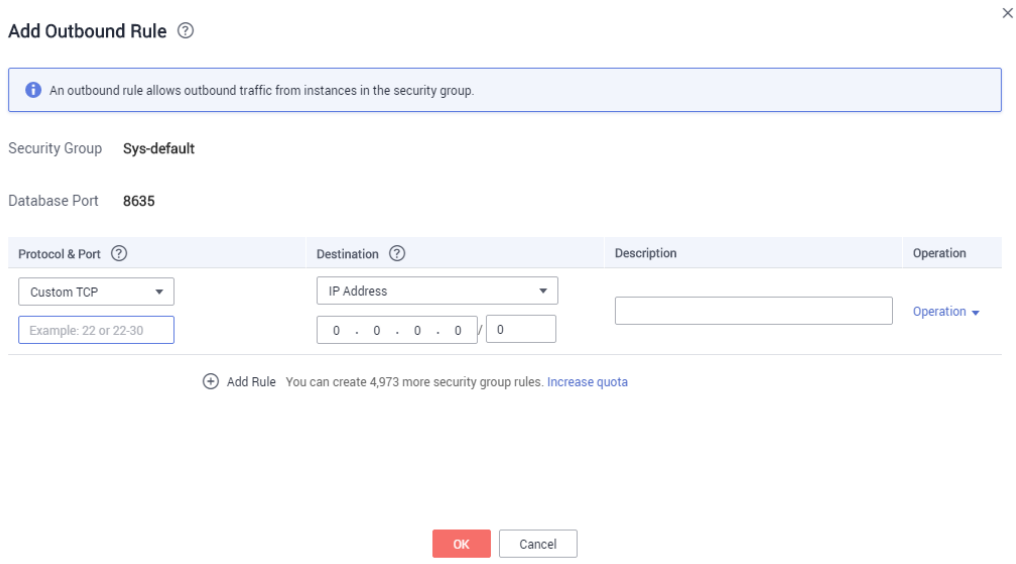


Figure 4-10 Add Outbound Rule



Step 4 Add a security group rule as prompted.

Table 4-16 Parameter description

Parameter	Description	Value Example
Protocol	The network protocol required for access. You can allow all protocols or specify a specific protocol, TCP, UDP, ICMP, and SSH.	TCP
Port	Specifies the port that allows the access to ECSs or external devices. Common ports are listed in **Common Ports Used by ECSs**.	8635
Source/ Destination	Specifies the supported IP address and security group that the rule applies to. • **IP address**: The IP address or subnet that the rule applies to. Single IP addresses must be expressed using slash notation. – Single IP address: xxx.xxx.xxx.xxx/32 (IPv4) – Subnet: xxx.xxx.xxx.0/24 – All IP addresses: 0.0.0.0/0 • **Security group**: A security group that access will be allowed from. ECSs in this security group will be granted access to DDS instance in the current security group.	• 192.168.10.0/24 • default

Step 5 Click **OK**.

----End

4.3.4 Step 3: Connect to a Single Node Instance Over Private Networks

Scenarios

This section describes how to connect to a single-node instance using the MongoDB client over private networks.

The MongoDB client can connect to a DB instance with a common connection or an encrypted connection (SSL). To improve data transmission security, you are advised to connect to DB instances using the SSL connection.

Different OS scenarios: The following uses Linux ECS and Window client as an example.

- For best practices about connections to DB instances over private networks, see **Connecting to a DB Instance Through an ECS**.

Constraints

For details about constraints on connecting to a single node instance over private networks, see **Constraints**.

Prerequisites

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

Connecting to a DB Instance Using the MongoDB Client (SSL)

Step 1 On the **Instance Management** page, click the target DB instance.

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

Step 5 Connect to a DDS DB instance.

- Method 1: Using Linux commands

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

  Enter the database account password when prompted:

  ```
  Enter password:
  ```
- Method 2: Using the private connection address

  ./mongo mongodb://rwuser:******@*<DB_HOST>*:*<DB_PORT>*/test?authSource=admin --ssl --sslCAFile** <*FILE_PATH*> **--sslAllowInvalidHostnames**

  The connection information can be obtained in the **Address** column on the **Instance Management** page.

  Figure 4-11 Connections

NOTE

- A single node instance uses the management IP address to generate SSL certificate. **--sslAllowInvalidHostnames** is needed for the SSL connection over private networks.
- **DB_HOST** indicates the IP address of the remotely connected DB instance. Obtain the value from the **Private IP Address** column in the node list on the **Connections** page.
- **DB_PORT** indicates the port number. Obtain the value from **Database Port** in the **Basic Information** area on the **Connections** page.
- **DB_USER** indicates the database account name. The default value is **rwuser**.
- ********** indicates the password of the database account. If you use the connection address to connect to a DB instance:
  - If the password contains the at sign (@), change @ to %40.
  - If the password contains the exclamation mark (!), add an escape character (\) before the exclamation mark (!).
- **FILE_PATH** indicates the path where the root certificate is stored.

- Connect to the DB instance using Linux commands. The following is an example command:

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

- Connect to the DB instance using the private connection address. The following is an example command:

  ./mongo mongodb://rwuser:**@192.168.1.6:8635/test?authSource=admin --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames**

Step 6 Check the connection result. If the following information is displayed, the connection is successful.

```
replica:PRIMARY>
```

----End

Connecting to a DB Instance Using the MongoDB Client (Non-SSL)

NOTICE

If you connect to a DB instance using this method, you need to disable the SSL connection. For details about how to disable the SSL connection, see section **Enabling or Disabling SSL**.

Step 1 Connect to the ECS.

Step 2 Connect to a DDS DB instance.

- Method 1: Using Linux commands

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

  Enter the database account password when prompted:

  ```
  Enter password:
  ```

- Method 2: Using the private connection address

./mongo mongodb://rwuser:***@*<DB_HOST>*:*<DB_PORT>*/test?authSource=admin**

The connection information can be obtained in the **Address** column on the **Instance Management** page.

NOTE

- **DB_HOST** indicates the IP address of the remotely connected DB instance. Obtain the value from the **Private IP Address** column in the node list on the **Connections** page.
- **DB_PORT** indicates the port number. Obtain the value from **Database Port** in the **Basic Information** area on the **Connections** page.
- **DB_USER** indicates the database account name. The default value is **rwuser**.
- ***** indicates the password of the database account. If you use the connection address to connect to a DB instance:
  - If the password contains the at sign (@), change @ to %40.
  - If the password contains the exclamation mark (!), add an escape character (\) before the exclamation mark (!).

- Connect to the DB instance using Linux commands. The following is an example command:

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

- Connect to the DB instance using the private connection address. The following is an example command:

  ./mongo mongodb://rwuser:**@192.168.1.6:8635/test?authSource=admin**

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

```
replica:PRIMARY>
```

----End

4.4 Connecting to a Single Node Instance Over Public Networks

4.4.1 Overview

Scenarios

This section describes how to buy a single node instance on the management console, set a security group, bind an EIP, and connect to a single node instance over public networks.

Process

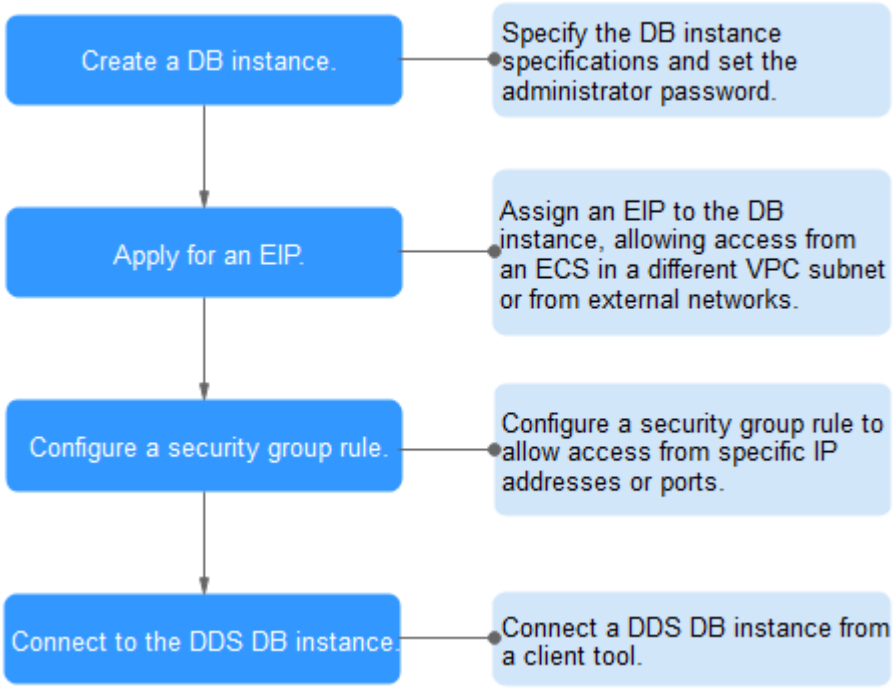
To purchase and connect to a single node instance, perform the following steps:

- **Step 1: Buy a Single Node Instance**
- **Step 2: Bind an EIP**

- **Step 3: Set a Security Group**
- **Step 4: Connect to a Single Node Instance Over Public Networks**

The following describes the steps from creating a DB instance to using it.

Figure 4-12 Accessing DB instances from a public network



4.4.2 Step 1: Buy a Single Node Instance

Scenarios

This section describes how to create a single node instance on the DDS management console. Currently, DDS single node instance supports the yearly/monthly and pay-per-use billing modes. DDS allows you to tailor your computing resources and storage space to your business needs.

You can use your account to create a maximum of 20 single nodes in total.

Prerequisites

- You have registered a HUAWEI CLOUD account.
- Your account balance is greater than or equal to ¥0.

Procedure

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

Step 2 On the **Instance Management** page, click **Buy DB Instance**.

Step 3 On the displayed page, select a billing mode, select your DB instance specifications and click **Next**.

Figure 4-13 Billing mode and basic information

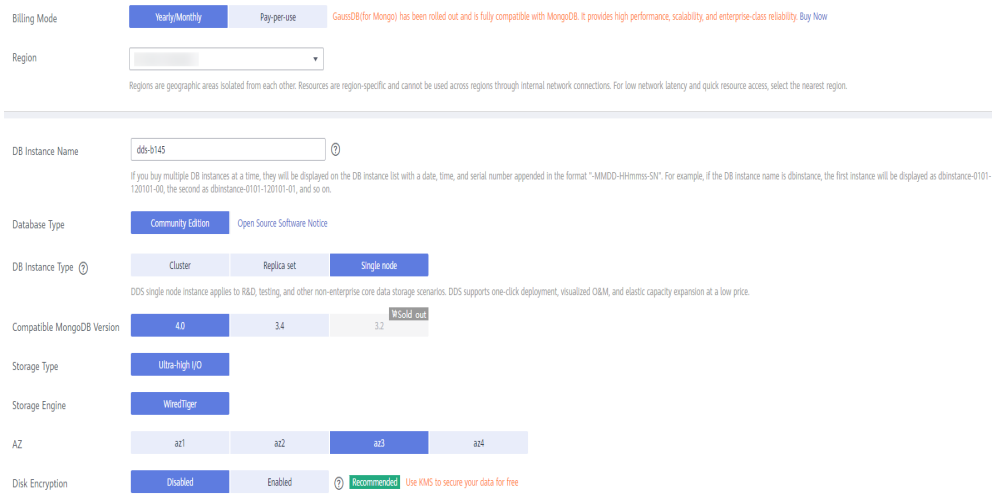


Table 4-17 Billing mode

Parameter	Description
Billing Mode	Select a billing mode, **Yearly/Monthly** or **Pay-per-use**. • Yearly/Monthly – You need to set **Validity Period** as required. Then, the system deducts the fees incurred at one time from your account based on the service price. – When you renew a yearly/monthly DB instance, you can change its billing mode from yearly/monthly to pay-per-use based on your service requirements. For details, see **Changing Yearly/Monthly Instances to a Pay-per-Use**. **NOTE** DB instances paid in yearly/monthly mode cannot be deleted. They support only resource unsubscription. For details, see section **Unsubscribing from a Yearly/Monthly DB Instance**. • Pay-per-use – You do not need to set **Validity Period** because the system deducts the fees incurred from your account based on the service duration. – If you want to use a DB instance at a low cost for a long period of time, you can change its billing mode from pay-per-use to yearly/monthly. For details, see **Changing the Billing Mode in Batches**.

Table 4-18 Basic information

Parameter	Description
DB Instance Name	The DB instance name can be 4 to 64 characters long. It must start with a letter and can contain only uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_). If you buy multiple DB instances, you can only enter 4 to 49 characters to set the DB instance name, and then the system automatically appends a date, time, and serial number to the end of the instance names (format: *instance_name-MMDD-HHmmss-SN*). After the DB instance is created, you can change its name. For details, see **Modifying the DB Instance Name**.
Database Type	Community Edition
DB Instance Type	Select **Single Node**. The single node architecture is another option for you, helping you reduce costs while ensuring data reliability.
Compatible MongoDB Version	• 4.0 • 3.4 • 3.2
CPU Type	Currently, DDS supports two CPU architectures: x86 and Kunpeng. The two architectures have similar capabilities and performance, both of which can meet your service requirements. For details about the instance types, versions, and specifications supported by the two CPU architectures, see **DB Instance Specifications**.
Storage Type	The default storage type is ultra-high I/O.
Storage Engine	WiredTiger
AZ	An AZ is a part of a region with its own independent power supplies and networks. AZs are physically isolated but can communicate through an internal network connection.

Parameter	Description
Disk Encryption	• **Disabled**: Disable the encryption function. • **Enabled**: Enable the encryption function. 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 a DB instance is created, the disk encryption status and the key cannot be changed. The backup data stored in OBS is not encrypted. – The key cannot be disabled, deleted, or frozen when being used. Otherwise, the database becomes unavailable. – For details about how to create a key, see the "Creating a CMK" section in the *Data Encryption Workshop User Guide*.

Figure 4-14 Instance class and storage space

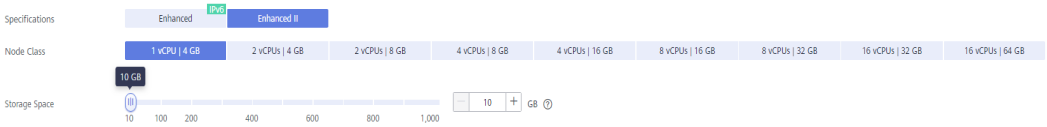


Table 4-19 Specifications

Parameter	Description
Specifications	In the x86 CPU architecture, the following specifications can be selected to suit different application scenarios: General-purpose (s6), Enhanced (c3), and Enhanced II (c6).
Node Class	For details about the DB instance specifications, see **DB Instance Specifications**.
Storage Space	The value ranges from 10 GB to 1,000 GB and must be a multiple of 10.

Figure 4-15 Network and database configuration

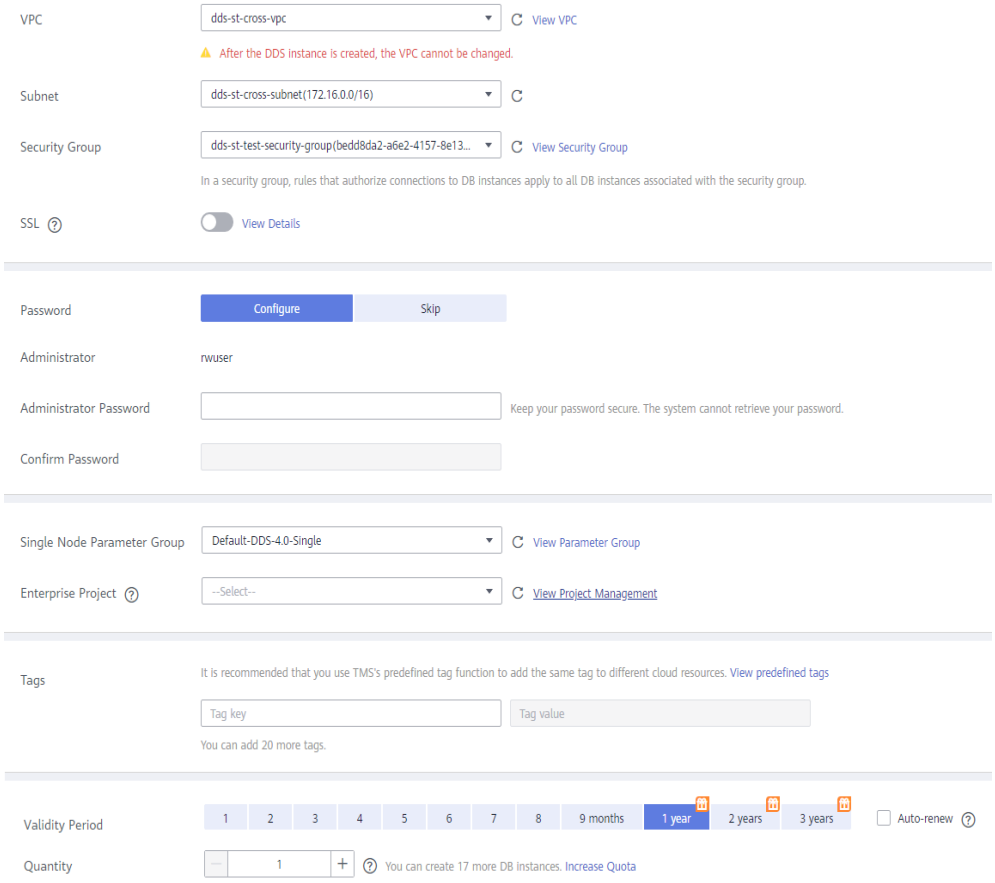


Table 4-20 Network

Parameter	Description
VPC	The VPC where your DB instances are located. A VPC isolates networks for different services, so you can easily manage and configure internal networks and change network configuration. You need to create or select the required VPC. For details about how to create a VPC, see section "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 allocates resources to you by default.
Subnet	A subnet provides dedicated network resources that are logically isolated from other networks for network security. After the instance is created, you can change the private IP address assigned by the subnet. For details, see **Changing a Private IP Address**.

Parameter	Description
Security Group	A security group controls access between DDS and other services for security. If there are no security groups available, DDS allocates resources to you by default. **NOTE** Ensure that the security group rule you set allows clients to access DB instances. For example, select the TCP protocol with inbound direction, input the default port number **8635**, and enter a subnet IP address or select a security group that the DB instance belongs to.
SSL	Secure Sockets Layer (SSL) certificates set up encrypted connections between clients and servers, preventing data from being tampered with or stolen during transmission. You can enable SSL to improve data security. After a DB instance is created, you can connect to it using SSL.
IPv6	Before enabling IPv6, ensure that IPv6 has been enabled for the VPC and subnet where the DB instance is located. For details about the application scenarios and procedures for enabling IPv6 for the VPC and subnet, see **IPv4 and IPv6 Dual-Stack Network**. After IPv6 is enabled, the DB instance can run in dual-stack mode. It means that the DB instance can use both the IPv4 address and IPv6 address. The DB instance can access the Internet using either IPv4 or IPv6 addresses, and the communications are independent of each other.

Table 4-21 Database configuration

Parameter	Description
Password	• Configure Enter and confirm the administrator password for connecting to the DB instance. • Skip Set the administrator password later. When you need to connect to the DB instance, locate the DB instance and click **Reset Password** in the **Operation** column to set a password for connecting to the DB instance.
Administrator	The default account is **rwuser**.
Administrator Password	Set a password for the administrator. The password is a string of 8 to 32 characters. It must be a combination of uppercase letters, lowercase letters, digits, and special characters. You can also use the following special characters: ~!@#%^*-_=+? Keep this password secure. If lost, the system cannot retrieve it for you.

Parameter	Description
Confirm Password	Enter the administrator password again.
Single Node Parameter Group	The parameters that apply to single node instances. After a DB instance is created, you can change the parameter group you configured for the DB instance to bring out the best performance. For details, see **Editing a Parameter Group**.
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**. 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 the *Enterprise Management User Guide*.

Table 4-22 Tag

Parameter	Description
Tags	This setting is optional. Adding tags helps you better identify and manage your DB instances. Up to 20 tags can be added for a DB instance. A tag is composed of a key-value pair. • Key: Mandatory if the DB instance is going to be tagged – Each tag key must be unique for each DB instance. – A tag key consists of up to 36 characters. – The key can only consist of digits, letters, underscores (_), and hyphens (-). • Value: Optional if the DB instance is going to be tagged – The value consists of up to 43 characters. – The value can only consist of digits, letters, underscores (_), dots (.), and hyphens (-). After a DB instance is created, you can view its tag details on the **Tags** tab. In addition, you can add, modify, and delete tags for existing DB instances. For details, see **Tag**.

Table 4-23 Required duration and quantity

Parameter	Description
Validity Period	The system will automatically calculate the fee based on the validity period you have selected.
Auto-renew	• By default, this option is not selected. • If you select this option, the auto-renew cycle is determined by the selected required duration.
Quantity	The purchase quantity depends on the single node 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. The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

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

NOTE

DB instance performance is determined by how you configure it during the creation. The hardware configuration items that can be selected include the node class and storage space.

Step 4 On the displayed page, confirm the DB instance information.

- Yearly/Monthly
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify your settings, click **Pay Now** to go to the payment page and complete the payment.
- Pay-per-use
  - If you need to modify the specifications, click **Previous** to return to the previous page.
  - If you do not need to modify the specifications, click **Submit** to start the instance creation.

Step 5 After a DDS DB instance is created, you can view and manage it on the **Instance Management** 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**.
- DDS enables the automated backup policy by default. After a DB instance is created, you can modify or disable the automated backup policy. An automated full backup is immediately triggered after the creation of a DB instance.
- The default DDS port is 8635, but this port can be modified if necessary. If you change the port, you need to add the security group rule to enable access.

- The yearly/monthly DB instances that are purchased in batches have the same specifications except for the DB instance name and ID.

----End

4.4.3 Step 2: Bind an EIP

Scenarios

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

Precautions

- Before accessing a database, you need to 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 section **Step 3: Set a Security Group**.
- To change the EIP that has been bound to a node, you need to unbind it from the node first.

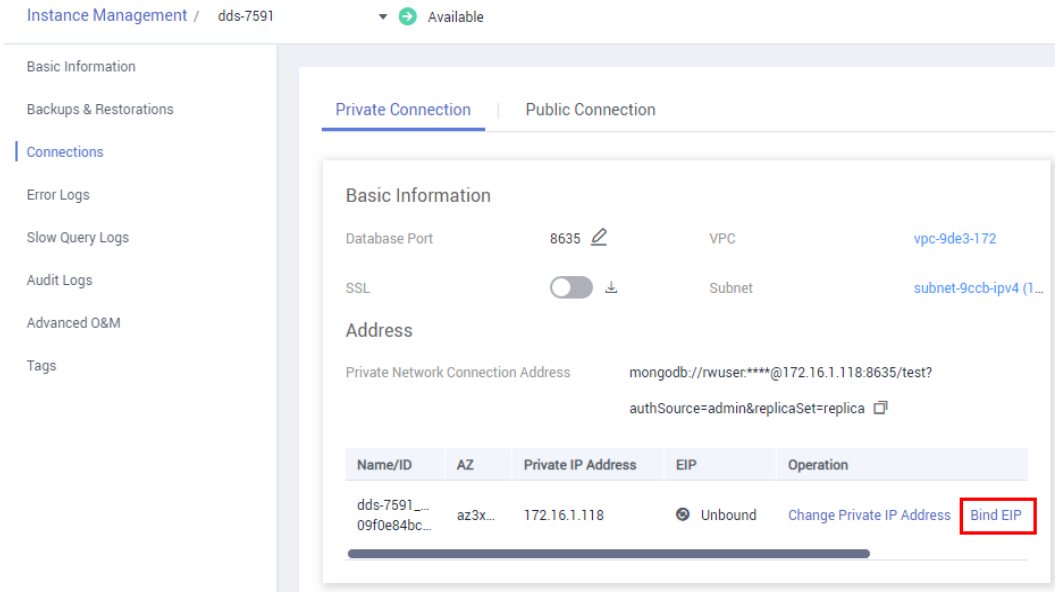
Binding an EIP

Step 1 On the **Instance Management** page, click the target single node instance.

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

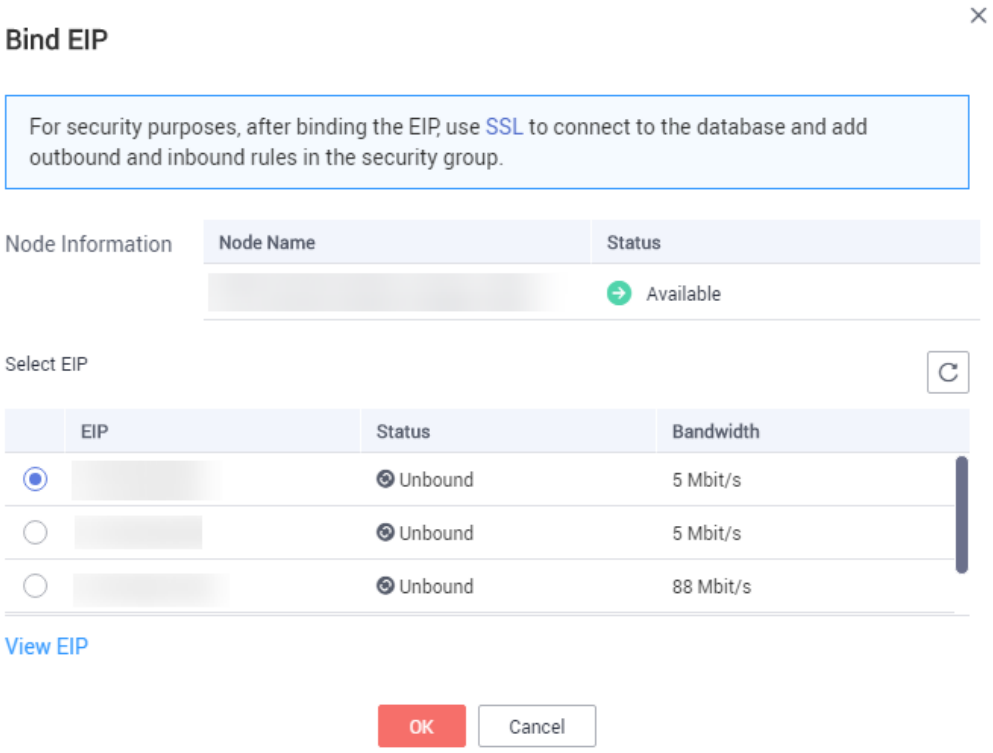
Step 3 In the **Basic Information** area, locate the target node and click **Bind EIP** in the **Operation** column.

Figure 4-16 Binding an EIP



Step 4 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 4-17 Selecting an EIP



Step 5 Locate the target node, in the **EIP** column, view the EIP that is successfully bound.

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

----End

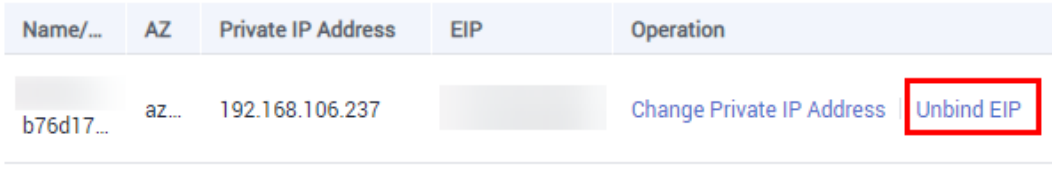
Unbinding an EIP

Step 1 On the **Instance Management** page, click the target single node instance.

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

Step 3 In the **Basic Information** area, locate the target node and click **Unbind EIP** in the **Operation** column.

Figure 4-18 Unbinding an EIP



Step 4 In the displayed dialog box, click **Yes**.

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

----End

4.4.4 Step 3: Set a Security Group

Scenarios

This section guides you on how to add a security group rule to control access from and to DDS DB instances in a security group.

Precautions

The default security group rule allows all outgoing data packets. ECSs and DDS DB instances in the same security group can access each other. After a security group is created, you can create different rules for that security group, which allows you to control access to the DB instances that are in it.

To access a DB instance in a security group from a source outside of that group, you need to create an inbound rule.

For details about the constraints on using security groups, see **Security Group Overview**.

Procedure

Step 1 On the **Instance Management** page, click the target single node instance.

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

Step 3 In the **Security Group** area, on the **Inbound Rules** tab, click **Add Rule**. In the displayed **Add Inbound Rule** dialog box, set required parameters to add inbound rules. On the **Outbound Rules** tab, click **Add Rule**. In the displayed **Add Outbound Rule** dialog box, set required parameters to add outbound rules.

You can click ⊕ to add more rules.

Figure 4-19 Add Inbound Rule

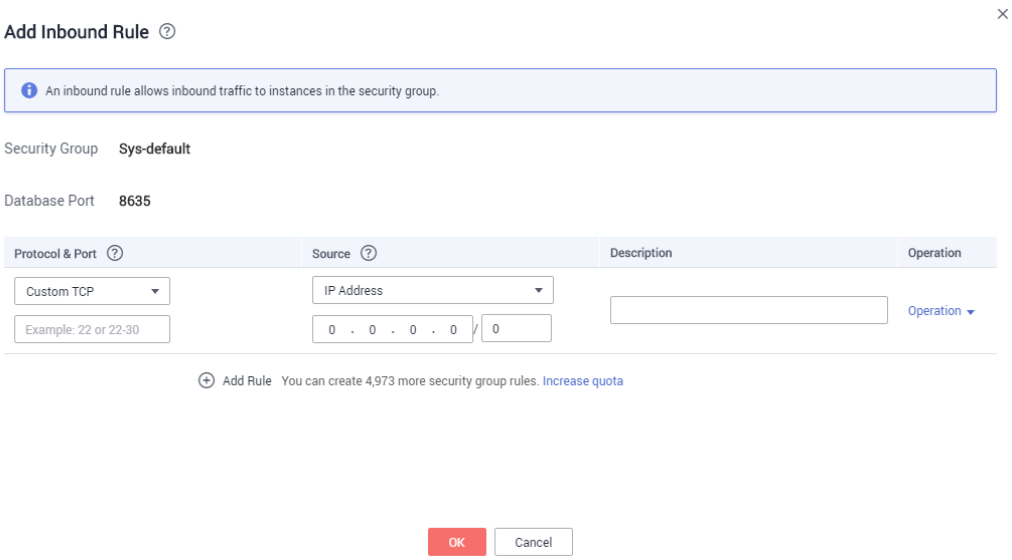
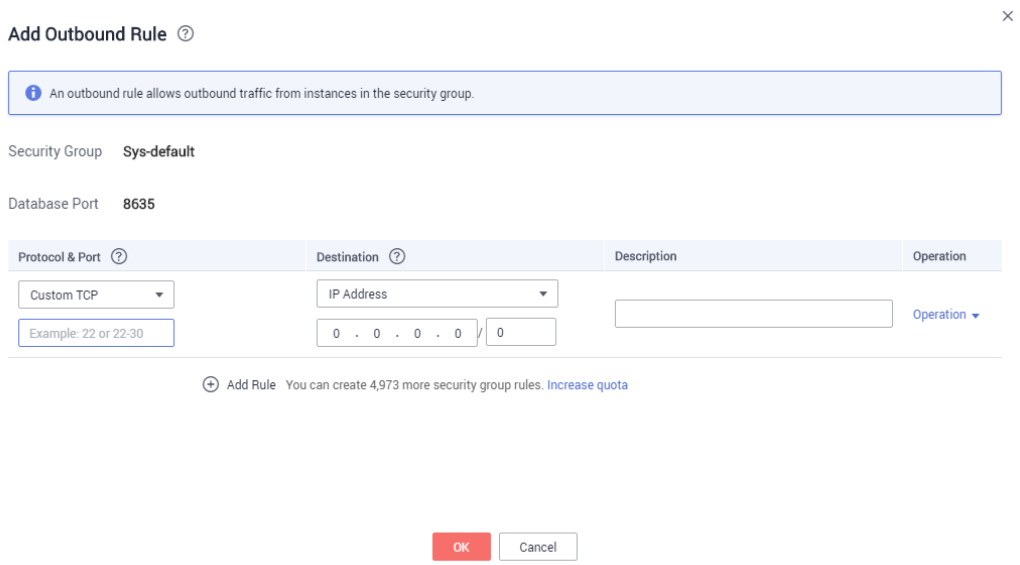


Figure 4-20 Add Outbound Rule



Step 4 Add a security group rule as prompted.

Table 4-24 Parameter description

Parameter	Description	Value Example
Protocol	The network protocol required for access. You can allow all protocols or specify a specific protocol, TCP, UDP, ICMP, and SSH.	TCP
Port	Specifies the port that allows the access to ECSs or external devices. Common ports are listed in **Common Ports Used by ECSs**.	8635
Source/ Destination	Specifies the supported IP address and security group that the rule applies to. • **IP address**: The IP address or subnet that the rule applies to. Single IP addresses must be expressed using slash notation. – Single IP address: xxx.xxx.xxx.xxx/32 (IPv4) – Subnet: xxx.xxx.xxx.0/24 – All IP addresses: 0.0.0.0/0 • **Security group**: A security group that access will be allowed from. ECSs in this security group will be granted access to DDS instance in the current security group.	• 192.168.10.0/24 • default

Step 5 Click **OK**.

----End

4.4.5 Step 4: Connect to a Single Node Instance Over Public Networks

Scenarios

This section describes how to connect to a single-node instance using the MongoDB client and Robo 3T over public networks.

The MongoDB client and Robo 3T can connect to a DB instance with a common connection or an encrypted connection (SSL). To improve data transmission security, you are advised to connect to DB instances using the SSL connection.

Different OS scenarios: The following uses Linux ECS and Window client as an example.

- For best practices about connections to a DB instance over public networks, see **Connecting to a DB Instance Through an EIP**.

Prerequisites

1. **Bind an EIP** to the cluster instance and **set security group rules** to ensure that the EIP can be accessed through the ECS or Robo 3T.
2. Install the MongoDB client or Robo 3T.

   MongoDB client

   a. For details on how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.

   b. Install the MongoDB client on the ECS.

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

   Robo 3T

   Install Robo 3T. For details, see **How Can I Install Robo 3T?**
3. If you select SSL mode, download the SSL certificate on the DDS console.

   a. On the **Instance Management** page, click the target DB instance.

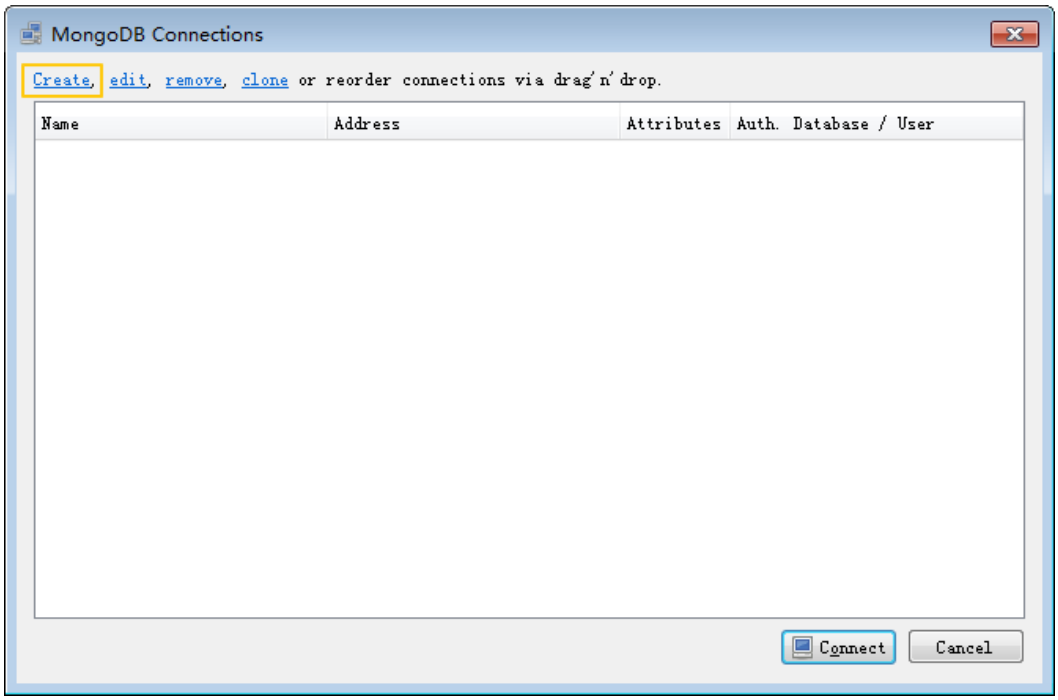
   b. In the navigation pane on the left, choose **Connections**.

   c. In the **Basic Information** area, click next to the **SSL** field.

Connecting to a DB Instance Using Robo 3T (SSL)

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

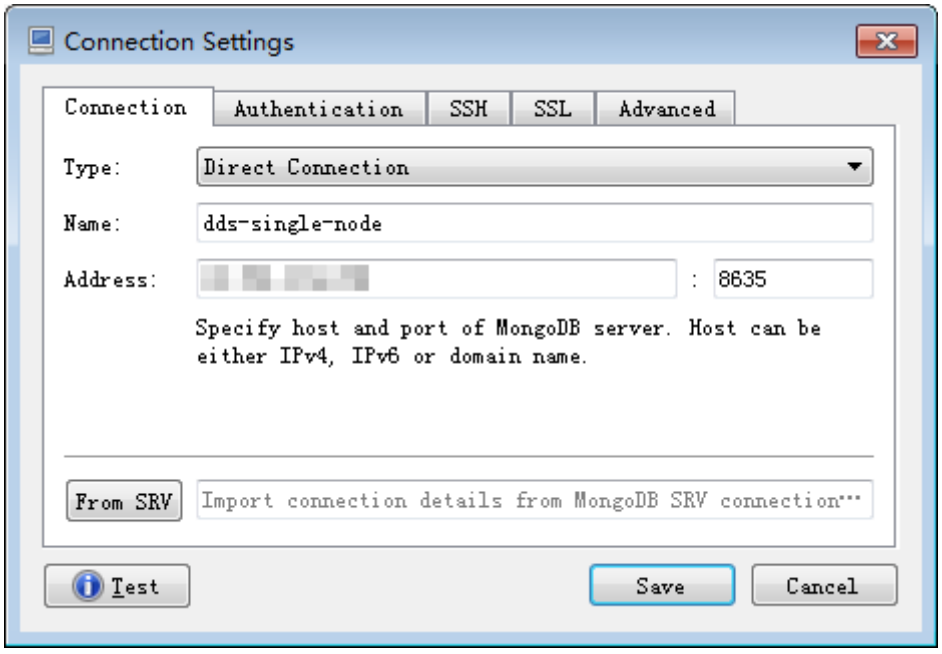
Figure 4-21 Connections



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

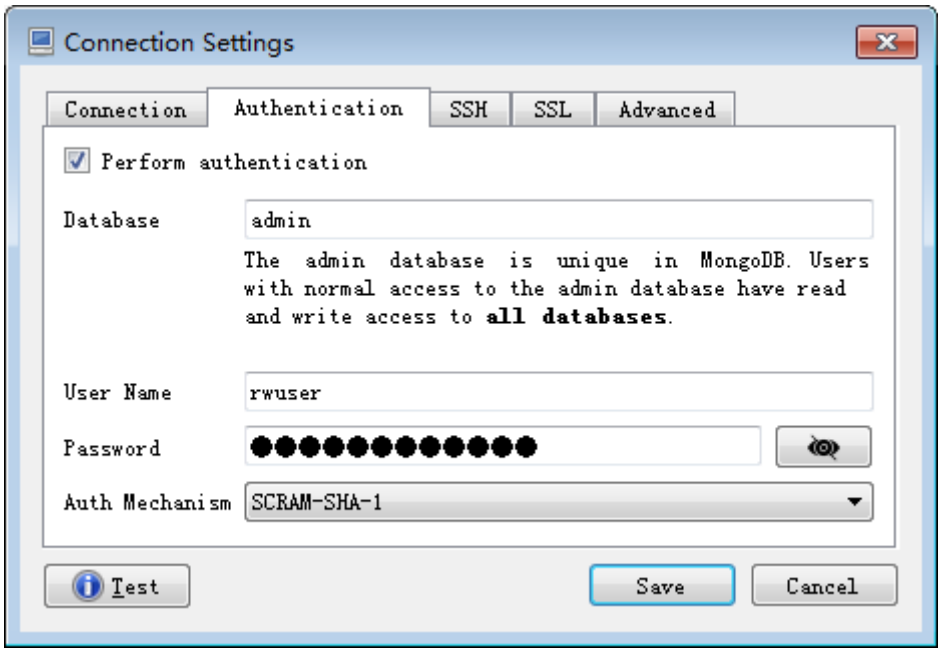
1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the single-node instance in the **Address** text box.

   Figure 4-22 Connection

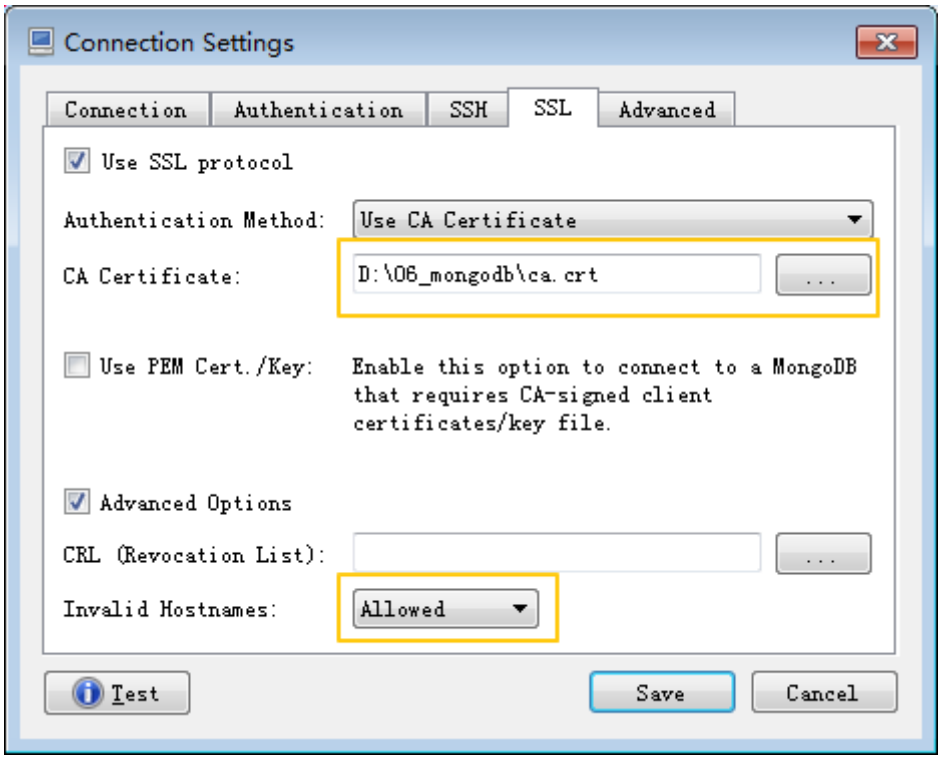
2. On the **Authentication** tab, set **Database** to **admin**, **User Name** to **rwuser**, and **Password** to the administrator password you set during the creation of the single-node instance.

Figure 4-23 Authentication



3. On the **SSL** tab, upload the SSL certificate and select **Allowed** for **Invalid Hostnames**.

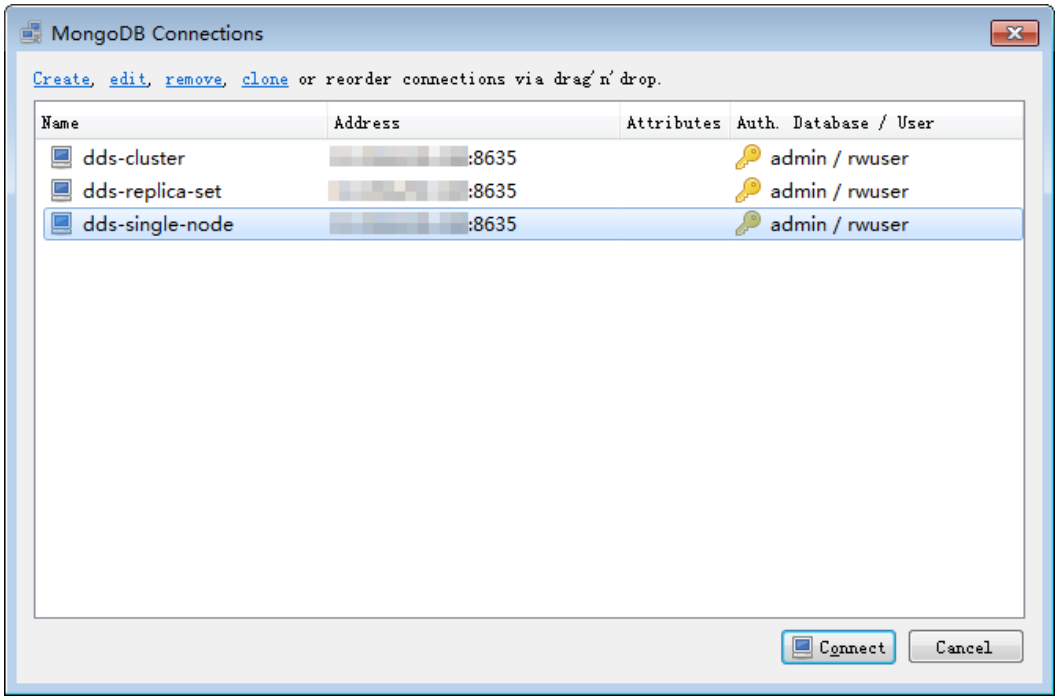
Figure 4-24 SSL



4. Click **Save**.

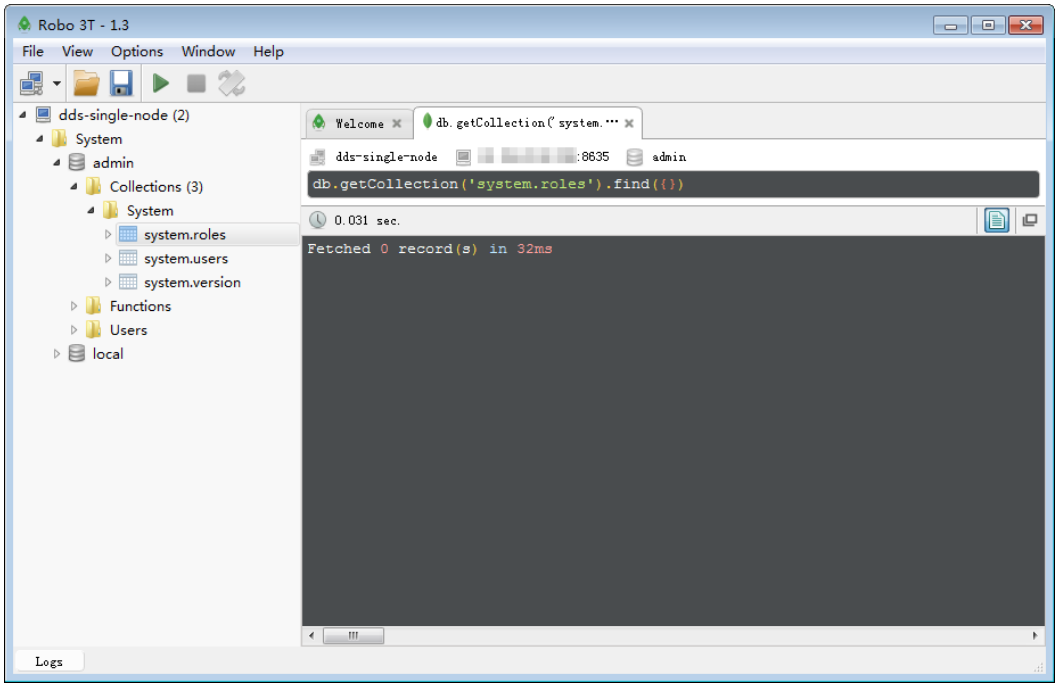
Step 3 On the **MongoDB Connections** page, click **Connect** to connect to the single-node instance.

Figure 4-25 Connections



Step 4 If the single-node instance is successfully connected, the page shown in **Figure 4-26** is displayed.

Figure 4-26 Connection succeeded



----End

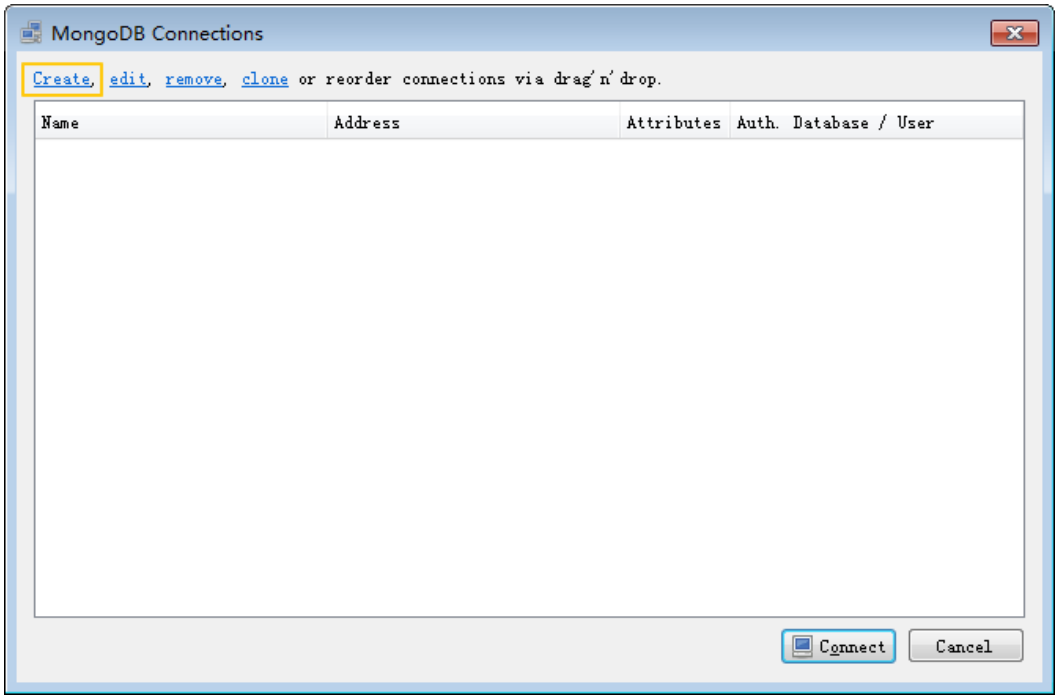
Connecting to a DB Instance Using Robo 3T (Non-SSL)

NOTICE

If you connect to a DB instance using this method, you need to disable the SSL connection. For details about how to disable the SSL connection, see section **Enabling or Disabling SSL**.

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

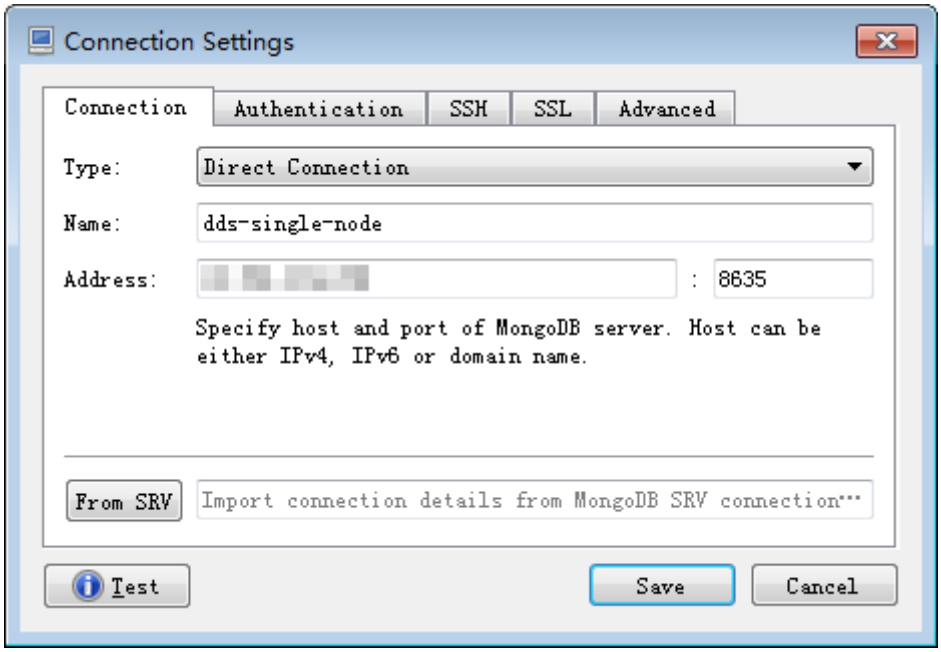
Figure 4-27 Connections



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

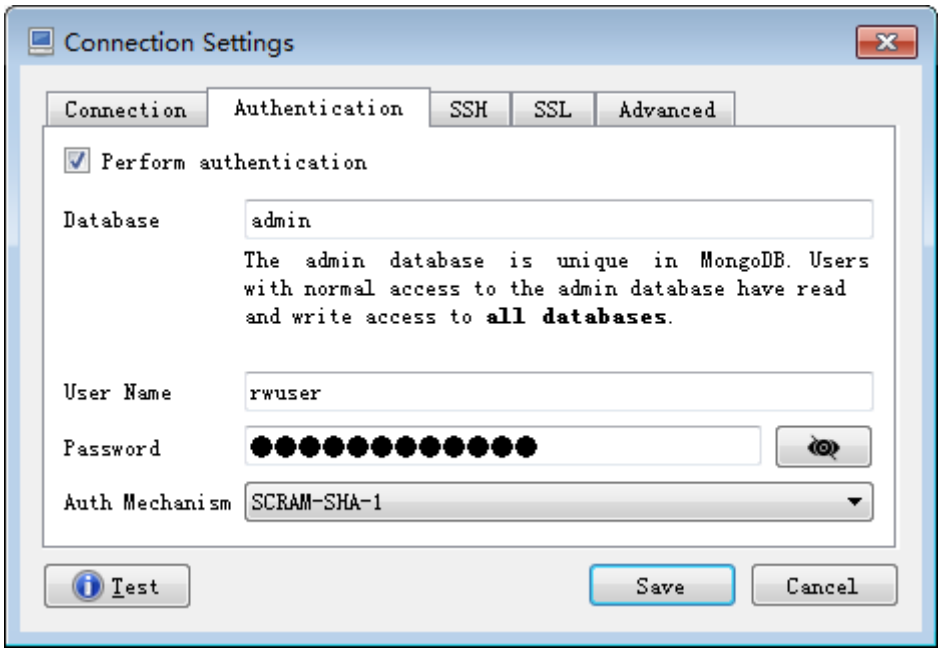
1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the single-node instance in the **Address** text box.

Figure 4-28 Connection



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 single-node instance.

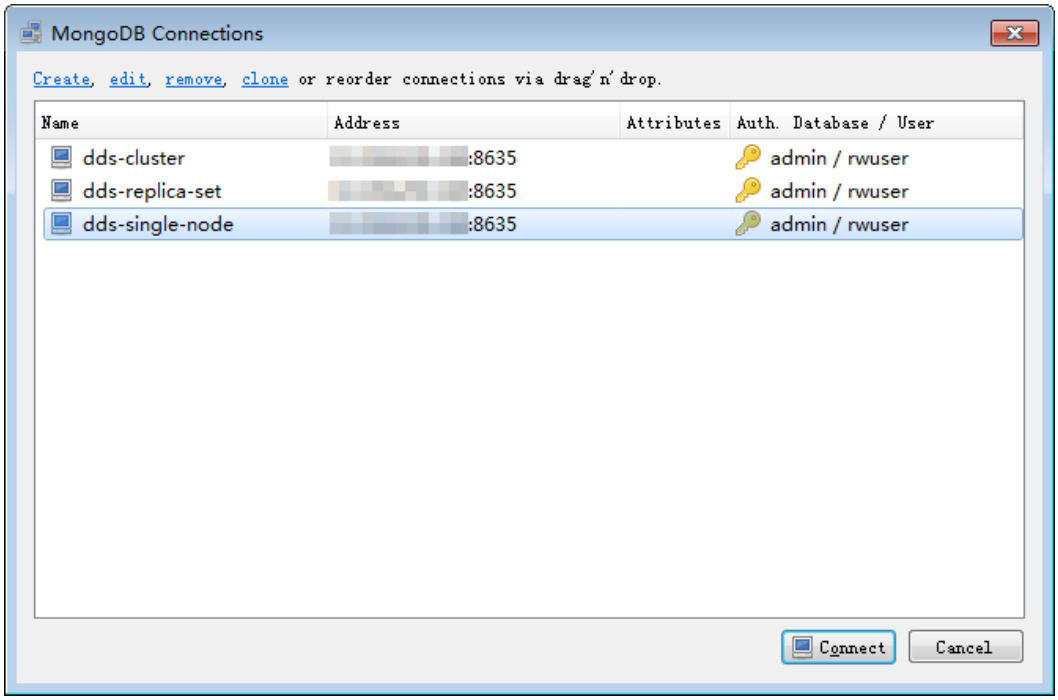
Figure 4-29 Authentication



3. Click **Save**.

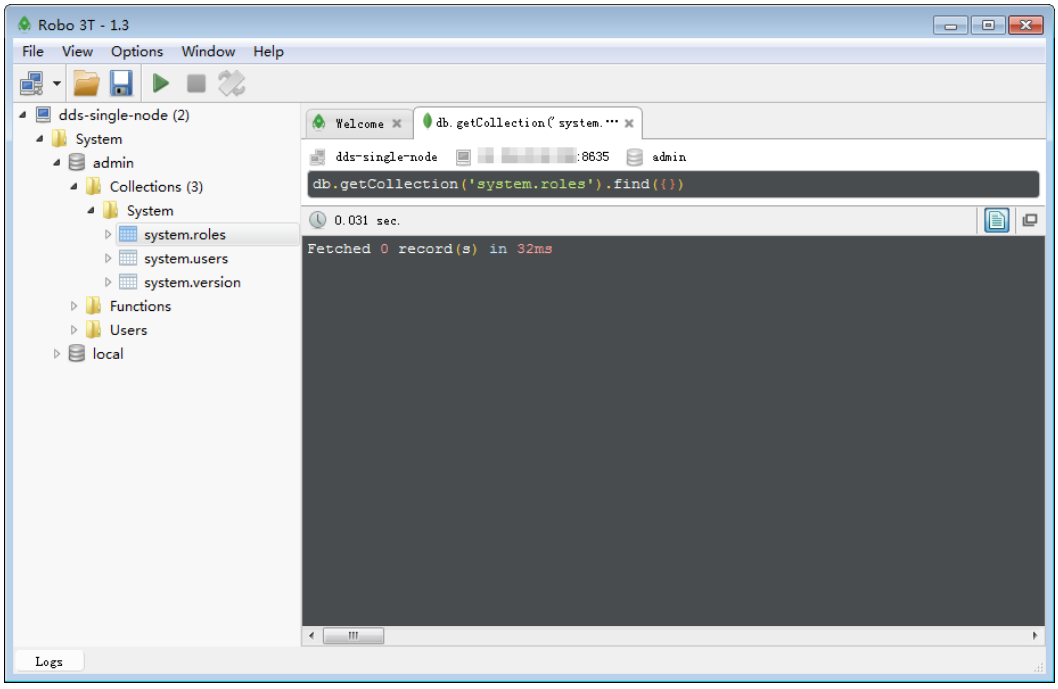
Step 3 On the **MongoDB Connections** page, click **Connect** to connect to the single-node instance.

Figure 4-30 Connections



Step 4 If the single-node instance is successfully connected, the page shown in **Figure 4-31** is displayed.

Figure 4-31 Connection succeeded



----End

Connecting to a DB Instance Using the MongoDB Client (SSL)

Step 1 On the **Instance Management** page, click the target DB instance.

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

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

Step 5 Connect to the DB instance in the directory where the MongoDB client is located.

- Method 1: Using Linux commands

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

  Enter the database account password when prompted:

  ```
  Enter password:
  ```

- Method 2: Using the public connection address

  ./mongo mongodb://rwuser:******@<*DB_HOST*>**:**<*DB_PORT*>**/test?authSource=admin --ssl --sslCAFile** <*FILE_PATH*> **--sslAllowInvalidHostnames**

  To obtain the public connection address, click the instance name and choose **Connections**. The address is displayed in **Public Network Connection Address** field on the **Public Connection** tab.

NOTE

- A single node instance uses the management IP address to generate SSL certificate. **--sslAllowInvalidHostnames** is needed for the SSL connection through a public network.
- **DB_HOST** indicates the IP address of the remotely connected DB instance. Obtain the value from the **EIP** column in the node list on the **Connections** page.
- **DB_PORT** indicates the port number. Obtain the value from **Database Port** in the **Basic Information** area on the **Connections** page.
- **DB_USER** indicates the database account name. The default value is **rwuser**.
- ******* indicates the password of the database account. If you use the connection address to connect to a DB instance:
  - If the password contains the at sign (@), change @ to %40.
  - If the password contains the exclamation mark (!), add an escape character (\) before the exclamation mark (!).
- **FILE_PATH** indicates the path where the root certificate is stored.

- Connect to the instance using Linux commands. The following is an example command:

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

- Connect to the DB instance using the public connection address. The following is an example command:

  ./mongo mongodb://rwuser:**@192.168.1.80:8635/test?authSource=admin --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames**

Step 6 Check the connection result. If the following information is displayed, the connection is successful.

```
replica:PRIMARY>
```

----End

Connecting to a DB Instance Using the MongoDB Client (Non-SSL)

NOTICE

If you connect to a DB instance using this method, you need to disable the SSL connection. For details about how to disable the SSL connection, see section **Enabling or Disabling SSL**.

Step 1 Connect to the ECS.

Step 2 Connect to a DDS DB instance.

- Method 1: Using Linux commands

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

  Enter the database account password when prompted:

  ```
  Enter password:
  ```

- Method 2: Using the public connection address

./mongo mongodb://rwuser:***@*<DB_HOST>*:*<DB_PORT>*/test?authSource=admin**

To obtain the public connection address, click the instance name and choose **Connections**. The address is displayed in **Public Network Connection Address** field on the **Public Connection** tab.

NOTE

- **DB_HOST** indicates the IP address of the remotely connected DB instance. Obtain the value from the **EIP** column in the node list on the **Connections** page.
- **DB_PORT** indicates the port number. Obtain the value from **Database Port** in the **Basic Information** area on the **Connections** page.
- **DB_USER** indicates the database account name. The default value is **rwuser**.
- ******* indicates the password of the database account. If you use the connection address to connect to a DB instance:
  - If the password contains the at sign (@), change @ to %40.
  - If the password contains the exclamation mark (!), add an escape character (\) before the exclamation mark (!).

- Connect to the instance using Linux commands. The following is an example command:

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

- Connect to the DB instance using the public connection address. The following is an example command:

  ./mongo mongodb://rwuser:**@192.168.1.80:8635/test?authSource=admin**

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

```
replica:PRIMARY>
```

----End

A Change History

Released On	Description
2020-10-30	This issue is the twenty-seventh official release, which incorporates the following change: Supported up to 20 tags per instance.
2020-09-30	This issue is the twenty-sixth official release, which incorporates the following changes: • Taken Enhanced Edition offline. • Supported Kunpeng-based instances of Community Edition 4.0.
2020-08-30	This issue is the twenty-fifth official release, which incorporates the following changes: • Supported up to 32 mongos nodes and 32 shard nodes in each Community Edition cluster instance. • Supported up to 3000 GB of the replica set storage space.
2020-07-30	This issue is the twenty-fourth official release, which incorporates the following changes: Supported cross-CIDR access to replica set instances.
2020-07-15	This issue is the twenty-third official release, which incorporates the following change: Supported DCC.
2020-05-30	This issue is the twenty-second official release, which incorporates the following change: Supported enterprise projects for the Enhanced cluster instance.

Released On	Description
2020-04-30	This issue is the twenty-first 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 twentieth 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 nineteenth 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.
2020-03-13	This issue is the eighteenth official release, which incorporates the following change: Modified the single node instance connection address.
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.
2019-11-11	This issue is the fifteenth official release, which incorporates the following change: Supported up to 2000 GB of storage of a Community Edition cluster instance.
2019-10-18	This issue is the fourteenth official release, which incorporates the following changes: ● Supported the selection of s6 specifications. ● Supported both the IPv4 and IPv6 IP addresses. ● 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 mongos nodes and 16 shards for a Community Edition cluster instance.

Released On	Description
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. ● Supported migrating single-node databases using DRS. ● Supported connection to DB instances of Enhanced Edition using program code.
2019-01-07	This issue is the seventh official release, which incorporates the following changes: ● Supported the yearly/monthly DB instance of Enhanced Edition. ● 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.
2018-09-06	This issue is the fifth official release, which incorporates the following change: ● Supported enterprise project management. ● Put the single node instance into commercial use. ● Supported creation of yearly/monthly single node instances.

Released On	Description
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: ● Added no restrictions on operations issued by users if their account balance is greater than or equal to ¥0. ● Supported DDS Enhanced Edition. ● 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 2000 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.

