Relational Database Service

Getting Started

Issue	27
Date	2023-07-17

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI 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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

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

Contents

1 Getting Started with RDS for MySQL

1.1 Step 1: Set Up for RDS

Registering a HUAWEI ID

If you already have a HUAWEI ID, skip this part. If you do not have a HUAWEI ID yet, perform the following steps to create one:

Step 1 Open the **Huawei Cloud website**.

Step 2 Click **Register** and complete the registration as instructed.

After the registration is successful, the system redirects you to your personal information page.

----End

Topping Up Your Account

- For details about RDS for MySQL prices, see **Price Calculator**.
- Before purchasing an RDS for MySQL instance, ensure that your account balance is sufficient. For details about how to top up an account, see **Topping Up an Account**.

Creating an IAM User and Granting Permissions

You can create an IAM user or user group on the Identity and Access Management (IAM) console and grant it specific operation permissions for fine-grained permissions management.

1. **Create a user group and assign permissions** to it.

   Create a user group on the IAM console, and attach the **RDS ReadOnlyAccess** policy to the group.

NOTE

To use some interconnected services, you also need to configure permissions of such services.

For example, to connect to your DB instance through the console, configure the **DAS FullAccess** permission of Data Admin Service (DAS) besides **RDS ReadOnlyAccess**.

2. **Create an IAM user and add it to the user group**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the RDS console by using the created user, and verify that the user only has read permissions for RDS.

   – Choose **Service List** > **Relational Database Service** and click **Buy DB Instance**. If a message appears indicating that you have insufficient permissions to perform the operation, the **RDS ReadOnlyAccess** policy has already been applied.

   – Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **RDS ReadOnlyAccess** policy has already taken effect.

1.2 Step 2: Buy a DB Instance

Scenarios

This section describes how to buy a DB instance on the management console.

RDS for MySQL supports the yearly/monthly and pay-per-use billing modes. RDS allows you to tailor your compute resources and storage space to your business needs.

You can create multiple read replicas when you are buying single or primary/standby DB instances.

Prerequisites

- Your account balance is greater than or equal to $0 USD.
- RDS for MySQL supports data transmission encryption during primary/standby replication. To use this function, contact customer service to apply for required permissions. After a DB instance is created, you can **manually enable SSL** for it.

Procedure

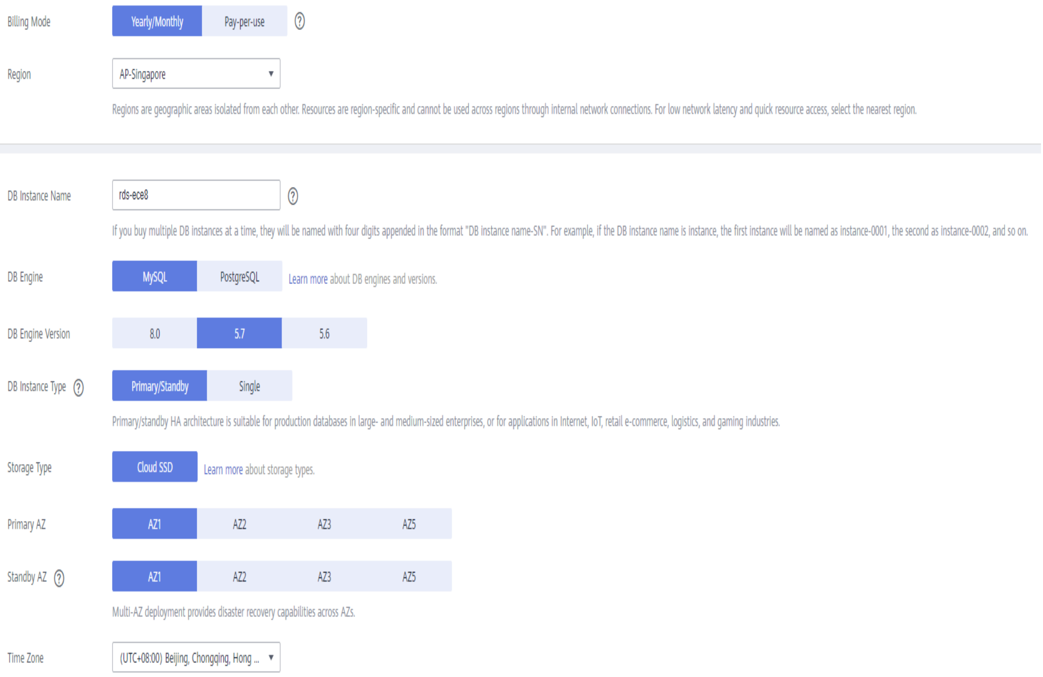
Step 1 Go to the **Buy DB Instance** page.

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

- Billing mode
  – **Yearly/Monthly**: If you select this mode, skip **Step 3** and go to **Step 4**.
  – **Pay-per-use**: If you select this mode, go to **Step 3**.

- Basic information

Figure 1-1 Billing mode and basic information



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

Region: AP-Singapore

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

DB Instance Name: rds-ece8

If you buy multiple DB instances at a time, they will be named with four digits appended in the format "DB instance name-SN". For example, if the DB instance name is instance, the first instance will be named as instance-0001, the second as instance-0002, and so on.

DB Engine: MySQL | PostgreSQL

Learn more about DB engines and versions.

DB Engine Version: 8.0 | 5.7 | 5.6

DB Instance Type: Primary/Standby | Single

Primary/standby HA architecture is suitable for production databases in large- and medium-sized enterprises, or for applications in Internet, IoT, retail e-commerce, logistics, and gaming industries.

Storage Type: Cloud SSD

Learn more about storage types.

Primary AZ: AZ1 | AZ2 | AZ3 | AZ5

Standby AZ: AZ1 | AZ2 | AZ3 | AZ5

Multi-AZ deployment provides disaster recovery capabilities across AZs.

Time Zone: (UTC+08:00) Beijing, Chongqing, Hong ...

Table 1-1 Basic information

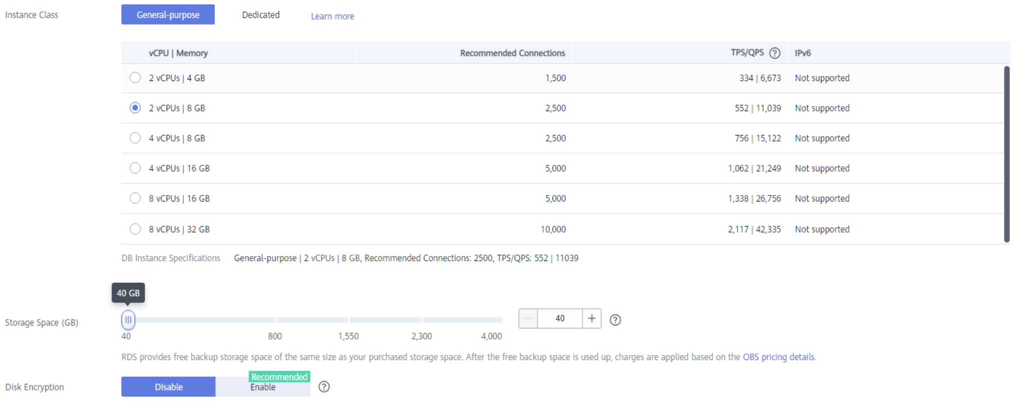
Parameter	Description
Region	Region where your resources are located. **NOTE** Products in different regions cannot communicate with each other through a private network. After a DB instance is created, the region cannot be changed. Therefore, exercise caution when selecting a region.
DB Instance Name	Must start with a letter and consist of 4 to 64 characters. Only letters (case-sensitive), digits, hyphens (-), and underscores (_) are allowed. – If you intend to buy multiple DB instances and read replicas at a time, the allowed length for each instance name will change. – If you buy multiple DB instances at a time, they will be named *instance-0001*, *instance-0002*, and so on. (*instance* indicates the DB instance name you specify.)
DB Engine	Set to **MySQL**.

Parameter	Description
DB Engine Version	For details, see **DB Engines and Versions**. Different DB engine versions are supported in different regions. When creating an RDS for MySQL instance, select a proper DB engine version tailored to your workloads. You are advised to select the latest available version because it is more stable, reliable, and secure.
DB Instance Type and AZ	– **Primary/Standby**: uses an HA architecture with a primary DB instance and a synchronous standby DB instance. It is suitable for production databases of large- and medium-sized enterprises in Internet, Internet of Things (IoT), retail e-commerce sales, logistics, gaming, and other sectors. The standby DB instance improves instance reliability and is invisible to you after being created. An AZ is a physical region where resources use independent power supply and networks. AZs are physically isolated but interconnected through an internal network. Some regions support both single AZs and multiple AZs and some only support single AZs. To achieve high reliability, RDS will automatically deploy your primary and standby instances in different physical servers even if you deploy them in the same AZ. If you attempt to create primary/standby DB instances in the same AZ in a Dedicated Computing Cluster (DCC) and there is only one physical server available, the creation will fail. You can deploy primary and standby DB instances in a single AZ or across AZs to achieve failover and high availability. – **Single**: uses a single-node architecture, which is more cost-effective than primary/standby DB instances. It is suitable for development and testing of microsites, and small and medium enterprises, or for learning about RDS.

Parameter	Description
Storage Type	Determines the DB instance read/write speed. The higher the maximum throughput is, the higher the DB instance read/write speed can be. – **Cloud SSD**: cloud drives used to decouple storage from compute. The maximum throughput is 350 MB/s. – **Extreme SSD**: uses 25GE network and RDMA technologies to provide you with up to 1,000 MB/s throughput per disk and sub-millisecond latency. – **Ultra-high I/O**: uses the SSD disk type that supports a maximum throughput of 350 MB/s. **NOTE** – If you have purchased the Dedicated Distributed Storage Service (DSS), only the storage type that you have selected when you buy the DSS service is displayed. – The cloud SSD and extreme SSD storage types are supported with general-purpose, dedicated, and Kunpeng general-enhanced DB instances. – After a DB instance is created, you can change its storage type. For details, see **Changing a DB Instance Class**. – The IOPS supported by cloud SSDs depends on the I/O performance of Elastic Volume Service (EVS) disks. For details, see the description about ultra-high I/O in **Disk Types and Performance** of *Elastic Volume Service Service Overview*. – The IOPS supported by extreme SSDs depends on the I/O performance of Elastic Volume Service (EVS) disks. For details, see the description about extreme SSDs in **Disk Types and Performance** of *Elastic Volume Service Service Overview*.
Time Zone	You need to select a time zone for your instance based on the region hosting your instance. You can select a time zone during instance creation and change it later as needed.

- Specifications and storage

Figure 1-2 Specifications and storage



	vCPU | Memory	Recommended Connections	TPS/QPS	IPv6
○	2 vCPUs | 4 GB	1,500	334 | 6,673	Not supported
●	2 vCPUs | 8 GB	2,500	552 | 11,039	Not supported
○	4 vCPUs | 8 GB	2,500	756 | 15,122	Not supported
○	4 vCPUs | 16 GB	5,000	1,062 | 21,249	Not supported
○	8 vCPUs | 16 GB	5,000	1,338 | 26,756	Not supported
○	8 vCPUs | 32 GB	10,000	2,117 | 42,335	Not supported

DB Instance Specifications General-purpose | 2 vCPUs | 8 GB, Recommended Connections: 2500, TPS/QPS: 552 | 11039

Storage Space (GB) 40

RDS provides free backup storage space of the same size as your purchased storage space. After the free backup space is used up, charges are applied based on the OBS pricing details.

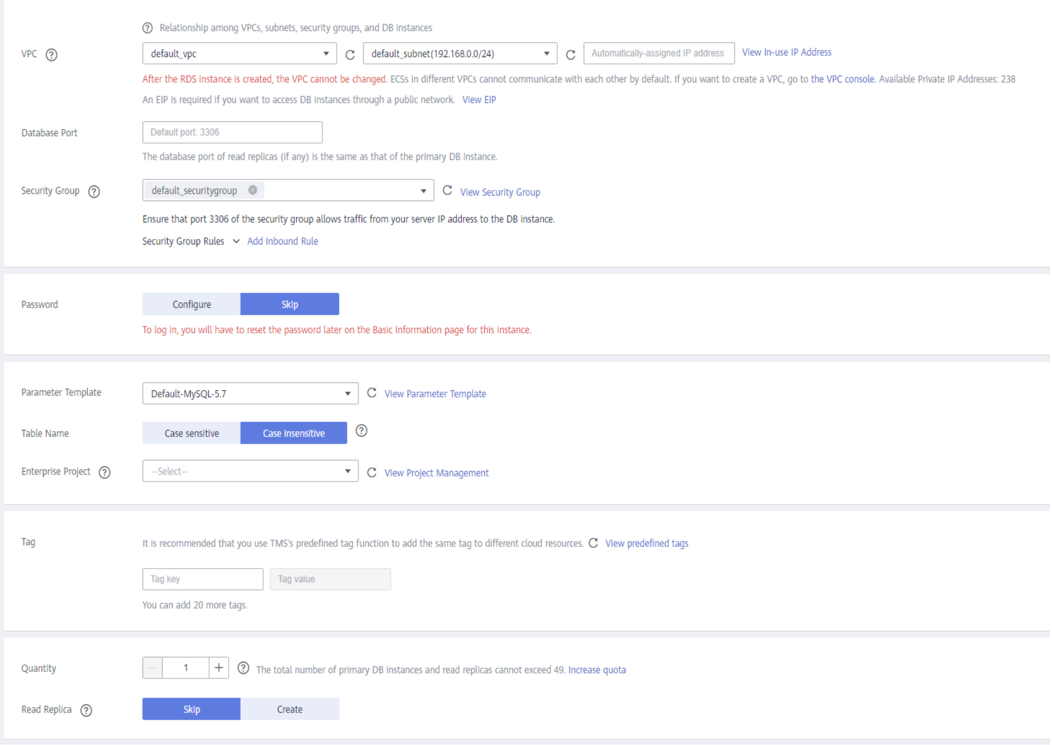
Table 1-2 Specifications and storage

Parameter	Description
Instance Class	Refers to the vCPU and memory of a DB instance. Different instance classes support different numbers of database connections and maximum IOPS. For details about instance classes, see **RDS for MySQL Instance Classes**. After a DB instance is created, you can change its vCPU and memory. For details, see **Changing a DB Instance Class**. **NOTE** Only general-enhanced DB instances are allowed for a DCC.
Resource Type	– **EVS** – **DSS** **NOTE** This option is displayed only when you have purchased **Dedicated Distributed Storage Service (DSS)**.
Storage Pool	Displayed only when you select **DSS** for **Resource Type**. The storage pool is secure because it is physically isolated from other pools.
Storage Space (GB)	Contains the file system overhead required for inode, reserved block, and database operation. If the storage type is cloud SSD or extreme SSD, you can enable storage autoscaling. If the available storage drops to a specified threshold, autoscaling is triggered. – **Enable autoscaling**: If you select this option, autoscaling is enabled. – **Trigger If Available Storage Drops To**: If the available storage drops to a specified threshold or 10 GB, autoscaling is triggered. – **Autoscaling Limit**: The default value range is from 40 GB to 4,000 GB. The limit must be no less than the storage of the DB instance. After a DB instance is created, you can scale up its storage space. For details, see **Scaling up Storage Space**. **NOTE** – Storage space can range in size from 40 GB to 4,000 GB and can be scaled up only by a multiple of 10 GB. – If you specify a read replica when creating a primary DB instance and enable storage autoscaling for the primary DB instance, storage autoscaling is also enabled for the read replica by default.

Parameter	Description
Disk Encryption	– **Disable**: Data stored in the disk is not encrypted. – **Enable**: Enabling disk encryption improves data security, but slightly affects the read and write performance of the database. ■ **Key Name**: Select the tenant key from the drop-down list. ■ Click **Create Key** and configure parameters in the displayed dialog box. For more information, see **Creating a Key** in the *Data Encryption Workshop User Guide*. **NOTE** – If you enable disk encryption during instance creation, the disk encryption status and the key cannot be changed later. Disk encryption will not encrypt backup data stored in OBS. To enable backup data encryption, contact customer service. – If disk encryption or backup data encryption is enabled, keep the key properly. Once the key is disabled, deleted, or frozen, the database will be unavailable and data may not be restored. If disk encryption is enabled but backup data encryption is not enabled, you can **restore data to a new instance from backups**. If both disk encryption and backup data encryption are enabled, data cannot be restored.

- Network and database configuration

Figure 1-3 Network and database configuration



Relationship among VPCs, subnets, security groups, and DB instances

VPC: default_vpc | default_subnet(192.168.0.0/24) | Automatically-assigned IP address | View In-use IP Address

After the RDS instance is created, the VPC cannot be changed. ECSs in different VPCs cannot communicate with each other by default. If you want to create a VPC, go to the VPC console. Available Private IP Addresses: 238

An EIP is required if you want to access DB instances through a public network. View EIP

Database Port: Default port: 3306

The database port of read replicas (if any) is the same as that of the primary DB instance.

Security Group: default_securitygroup | View Security Group

Ensure that port 3306 of the security group allows traffic from your server IP address to the DB instance.

Security Group Rules | Add Inbound Rule

Password: Configure [✓ Skip]

To log in, you will have to reset the password later on the Basic Information page for this instance.

Parameter Template: Default-MySQL-5.7 | View Parameter Template

Table Name: Case sensitive [✓ Case insensitive]

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

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

Tag key | Tag value

You can add 20 more tags.

Quantity: 1 | The total number of primary DB instances and read replicas cannot exceed 49. Increase quota

Read Replica: [✓ Skip] Create

Table 1-3 Network

Parameter	Description
VPC	A virtual network in which your RDS DB instances are located. A VPC can isolate networks for different workloads. You can select an existing VPC or create a VPC. For details on how to create a VPC, see "Creating a VPC" in *Virtual Private Cloud User Guide*. If no VPC is available, RDS allocates a VPC to you by default. **NOTICE** After a DB instance is created, the VPC cannot be changed.

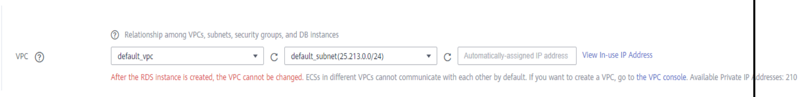
Parameter	Description
Subnet	Improves network security by providing dedicated network resources that are logically isolated from other networks. Subnets take effect only within an AZ. The Dynamic Host Configuration Protocol (DHCP) function is enabled by default for subnets in which you plan to create RDS DB instances and cannot be disabled. A floating IP address is automatically assigned when you create a DB instance. You can also enter an unused IPv4 or IPv6 floating IP address in the subnet CIDR block. After the DB instance is created, you can change the floating IP address. If no IPv6 subnets are available, contact customer service. **NOTICE** When creating a single-node DB instance, ensure that there are at least two available private IP addresses. – If you also need to create single-node read replicas, there should be at least four available private IP addresses. – If you need to create HA read replicas, there should be at least five available private IP addresses. When creating a primary/standby DB instance, ensure that there are at least three available private IP addresses. If HA read replicas are about to be created, there should be at least six available private IP addresses. **Figure 1-4** Viewing available private IP addresses  Relationship among VPCs, subnets, security groups, and DB instances VPC: default_vpc; default_subnet(25.213.0.0/24); Automatically-assigned IP address After the RDS instance is created, the VPC cannot be changed. ECSs in different VPCs cannot communicate with each other by default. If you want to create a VPC, go to the VPC console. Available Private IP Addresses: 210
Security Group	Enhances security by controlling access to RDS from other services. In addition, a network **access control list (ACL)** can help control inbound and outbound traffic of subnets in your VPC. Ensure that the security group you select allows the client to access the DB instance. When creating a DB instance, you can select multiple security groups. For better network performance, you are advised to select no more than five security groups. In such a case, the access rules of all the selected security groups apply on the instance. If no security group is available or has been created, RDS allocates a security group to you by default.
Database Port	The default database port is **3306**. You can change it after a DB instance is created. RDS for MySQL instances can use database ports 1024 to 65535, excluding 12017, 33071, and 33062, which are reserved for RDS system use.

Table 1-4 Database configuration

Parameter	Description
Password	– **Configure** (default setting): Configure a password for your DB instance during the creation process. – **Skip**: Configure a password later after the DB instance is created. NOTICE If you select **Skip** for **Password**, you need to reset the password before you can log in to the instance. After a DB instance is created, you can reset the password. For details, see **Resetting the Administrator Password**.
Administrator	The default login name for the database is **root**.
Administrator Password	Must consist of 8 to 32 characters and contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters (~ ! @ # $ % ^ * - _ = + ? , ( ) & . |). Enter a strong password and periodically change it for security reasons. If the password you provide is regarded as a weak password by the system, you will be prompted to enter a stronger password. Keep this password secure. The system cannot retrieve it. After a DB instance is created, you can reset this password. For details, see **Resetting the Administrator Password**.
Confirm Password	Must be the same as **Administrator Password**.
Parameter Template	Contains engine configuration values that can be applied to one or more DB instances. If you intend to create a primary/standby DB pair, they use the same parameter template. NOTICE If you use a custom parameter template when creating a DB instance, the following specification-related parameters in the custom template are not delivered. Instead, the default values are used. – **back_log** – **innodb_io_capacity_max** – **max_connections** – **innodb_io_capacity** – **innodb_buffer_pool_size** – **innodb_buffer_pool_instances** You can modify the instance parameters as required after the DB instance is created. For details, see **Modifying Parameters in a Parameter Template**.

Parameter	Description
Table Name	Specifies whether table names are case sensitive. The case sensitivity of table names for created RDS for MySQL 8.0 instances cannot be changed.
Certificate	(Optional) Specifies the certificate created by Cloud Certificate Manager (CCM). The default certificate is the system certificate that is automatically generated. You can also select another certificate from the drop-down list. **NOTICE** If you want to specify a certificate when creating a DB instance, contact customer service to apply for the permission.
Enterprise Project	If your account has been associated with an enterprise project, select the target project from the **Enterprise Project** drop-down list. For more information about enterprise projects, see ***Enterprise Management User Guide***.

- Tags

Table 1-5 Tags

Parameter	Description
Tag	Tags an RDS DB instance. This parameter is optional. Adding tags to RDS DB instances helps you better identify and manage the DB instances. A maximum of 20 tags can be added for each DB instance. If your organization has configured tag policies for RDS, add tags to DB instances based on the policies. If a tag does not comply with the policies, DB instance creation may fail. Contact your organization administrator to learn more about tag policies. After a DB instance is created, you can view its tag details on the **Tags** page. For details, see **Managing Tags**.

- Purchase period

Table 1-6 Purchase period

Parameter	Description
Required Duration	This option is available only for yearly/monthly DB instances. The system will automatically calculate the configuration fee based on the selected required duration. The longer the required duration is, the larger discount you will enjoy. If you want to set this parameter to 5 years, the restrictions are as follows: – You have obtained the required permissions from customer service. – This setting is supported only in CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, and CN Southwest-Guiyang1. – This setting is supported only with general-purpose instances.
Auto-renew	– This option is available only for yearly/monthly DB instances and is not selected by default. – If you select this option, the auto-renew cycle is determined by the selected required duration.
Quantity	RDS supports batch creation of DB instances. If you intend to create primary/standby DB instances and set **Quantity** to **1**, a primary DB instance and a synchronous standby DB instance will be created.
Read Replica	You can determine whether to create read replicas when creating a DB instance. – **Skip** is selected by default. – If you select **Create**, configure parameters based on **Table 1-7**. – To create yearly/monthly read replicas, contact customer service to apply for the required permissions.

- Read replicas

Table 1-7 Read replicas

Parameter	Description
Read Replica	By default, read replicas are named with "read" and two digits appended to the primary DB instance name. For example, if the primary instance name is instance-0001, the first read replica will be named instance-0001-read-01. The network and storage configurations are the same as those of the primary DB instance.

Parameter	Description
Read Replica AZ	By default, the primary DB instance and read replicas are deployed in different AZs. You can choose AZs as required. **NOTICE** Products in different regions cannot communicate with each other through a private network. After a DB instance is purchased, the region cannot be changed. Therefore, exercise caution when selecting a region.
Instance Class	Refers to the CPU and memory of a read replica.
Read Replica Quantity	You can create a maximum of five read replicas for each DB instance. After a DB instance is created, the system automatically triggers the creation of read replicas. If you intend to create primary/standby DB instances and set **Read Replica Quantity** to **1**, a pair of primary/standby DB instances and a read replica will be created.

If you have any questions about the price, click **Pricing details** at the bottom of the page.

NOTE

The performance of your DB instance depends on its configurations. Hardware configuration items include the instance specifications, storage type, and storage space.

Step 3 Confirm the specifications for pay-per-use DB instances.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Submit**.

Skip **Step 4** and **Step 5** and go to **Step 6**.

Step 4 Confirm the order for yearly/monthly DB instances.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Pay Now**.

Step 5 Select a payment method and complete the payment.

NOTE

This operation applies only to the yearly/monthly billing mode.

Step 6 To view and manage your DB instance, go to the **Instances** page.

- When your DB instance is being created, the status is **Creating**. The status changes to **Available** after the instance is created. To view the detailed progress and result of the creation, go to the **Task Center** page.
- The automated backup policy is enabled by default. You can change it after the DB instance is created. An automated full backup is immediately triggered once your DB instance is created.
- After a DB instance is created, you can enter a description for it.
- The default database port is **3306**. You can change it after a DB instance is created.

NOTE

You are advised to change the database port in a timely manner.

For details, see **Changing a Database Port**.

----End

Related Operations

Creating a DB Instance Using an API

Modifying RDS for MySQL Instance Parameters

1.3 Step 3: Connect to a DB Instance

1.3.1 Overview

An RDS DB instance can be connected through a private network, Data Admin Service (DAS), or a public network.

Table 1-8 RDS connection methods

Connect Through	IP Address	Scenarios	Description
DAS	No IP address is required. You can connect to your DB instance through DAS on the management console.	DAS enables you to manage databases on a web-based console and provides you with database development, O&M, and intelligent diagnosis to make it easy to use and maintain your databases. The permissions required for connecting to DB instances through DAS are enabled by default.	● Easy to use, secure, advanced, and intelligent ● Recommended

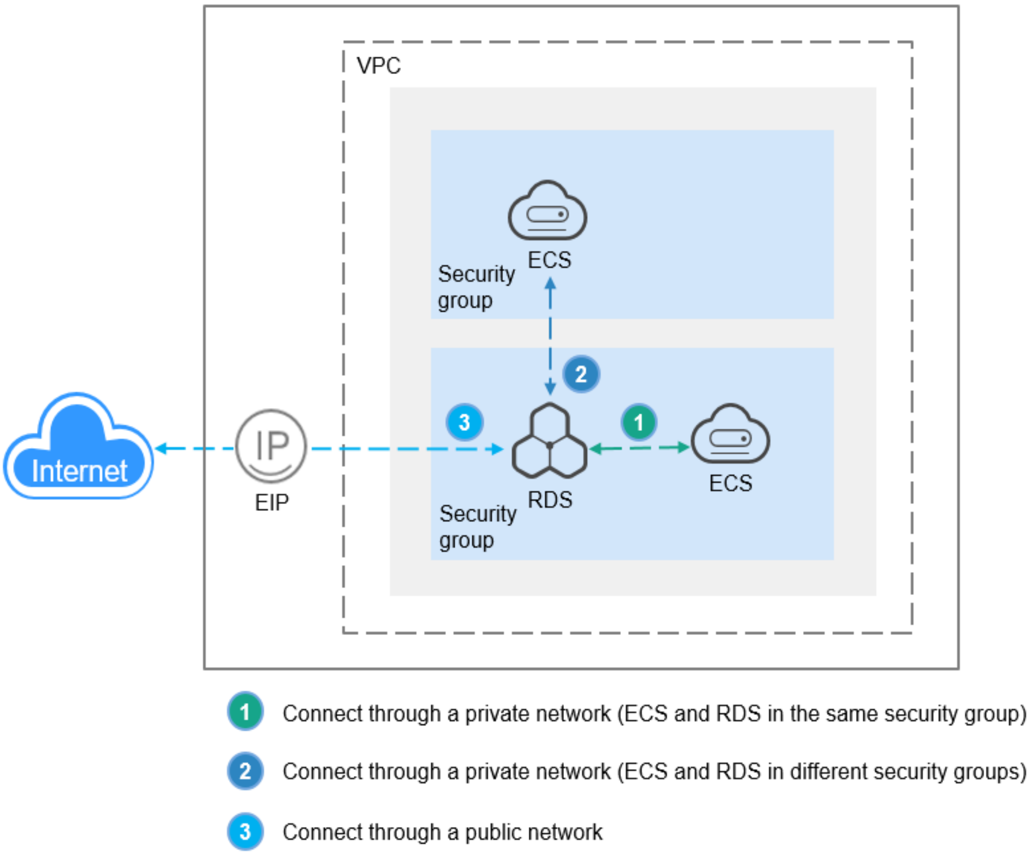
Connect Through	IP Address	Scenarios	Description
Private network	Floating IP	RDS provides a floating IP address by default. When your applications are deployed on an ECS that is in the same region and VPC as RDS, you are advised to use a floating IP address to connect to the RDS DB instance through the ECS.	- Secure and excellent performance - Recommended
Public network	EIP	If you cannot access an RDS DB instance through a floating IP address, bind an EIP to the DB instance and connect the DB instance through the EIP.	- A relatively lower level of security compared to other connection methods - To achieve a higher transmission rate and security level, you are advised to migrate your applications to an ECS that is in the same VPC as your RDS DB instance and use a floating IP address to access the DB instance. - You need to purchase an EIP. For details, see **EIP billing details**.

NOTE

- VPC: Virtual Private Cloud
- ECS: Elastic Cloud Server
- EIP: Elastic IP
- You can log in to DB instances using the Data Admin Service (DAS) service or other database clients.
- If the ECS is in the same VPC as your RDS DB instance, you do not need to apply for an EIP.

Figure 1-5 illustrates the connection over a private network or a public network.

Figure 1-5 DB instance connection


VPC
ECS
Security group
2
3
1
Internet
IP
EIP
RDS
ECS
Security group
1 Connect through a private network (ECS and RDS in the same security group)
2 Connect through a private network (ECS and RDS in different security groups)
3 Connect through a public network

Connecting to DB Instances Running Other DB Engines

- **Connecting to an RDS for MariaDB DB Instance**
- **Connecting to an RDS for PostgreSQL DB Instance**
- **Connecting to an RDS for SQL Server DB Instance**

1.3.2 Connecting to an RDS for MySQL DB Instance Through DAS (Recommended)

Scenarios

Data Admin Service (DAS) enables you to connect to and manage DB instances with ease on a web-based console. The permission required for connecting to DB instances through DAS has been enabled for you by default. Using DAS to connect to your DB instance is recommended, which is more secure and convenient.

Procedure

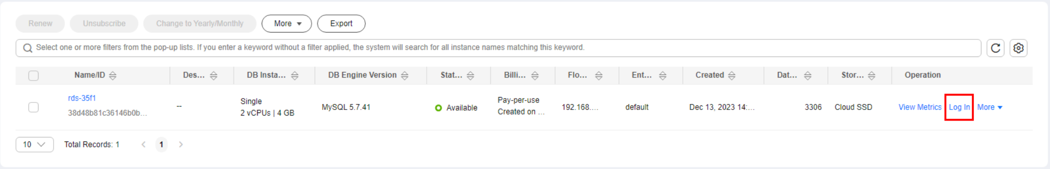
Step 1 Log in to the management console.

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

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

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

Figure 1-6 Logging in to an instance



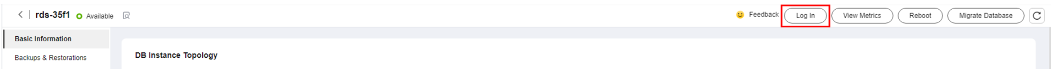
Select one or more filters from the pop-up lists. If you enter a keyword without a filter applied, the system will search for all instance names matching this keyword.

□	Name/ID	Des...	DB Insta...	DB Engine Version	Stat...	Billi...	Flo...	Ent...	Created	Dat...	Stor...	Operation
□	rds-35f1 38d48b81c36146b0b...	--	Single 2 vCPUs | 4 GB	MySQL 5.7.41	○ Available	Pay-per-use Created on ...	192.168....	default	Dec 13, 2023 14:...	3306	Cloud SSD	View Metrics Log In More

10 Total Records: 1 < 1 >

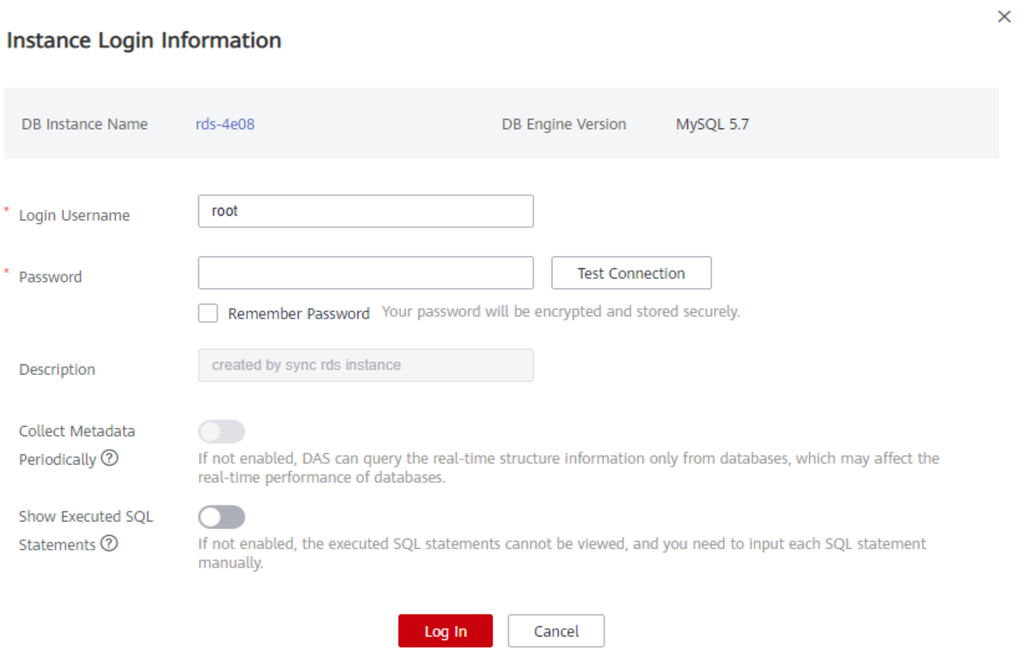
Alternatively, click the DB instance name on the **Instances** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner of the page.

Figure 1-7 Logging in to an instance



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

Figure 1-8 Login page



Instance Login Information

DB Instance Name	rds-4e08
DB Engine Version	MySQL 5.7

* Login Username: root

* Password:

□ Remember Password Your password will be encrypted and stored securely.

Description: created by sync rds instance

Collect Metadata Periodically ⓘ

If not enabled, DAS can query the real-time structure information only from databases, which may affect the real-time performance of databases.

Show Executed SQL Statements ⓘ

If not enabled, the executed SQL statements cannot be viewed, and you need to input each SQL statement manually.

----End

FAQ

- What Should I Do If I Can't Connect to My DB Instance Due to Insufficient Permissions?
- What Should I Do If I Can't Connect to My RDS for MySQL Instance?

Follow-up Operations

After logging in to the DB instance, you can create or migrate databases.

- Creating a MySQL Database Using the Console
- Creating a MySQL Database Using an API
- Migrating Data to RDS for MySQL

1.3.3 Connecting to an RDS for MySQL DB Instance Through a Private Network

1.3.3.1 Overview

Process

Figure 1-9 illustrates the process of connecting to an RDS for MySQL DB instance through a private network.

Figure 1-9 Connecting to a DB instance through a private network

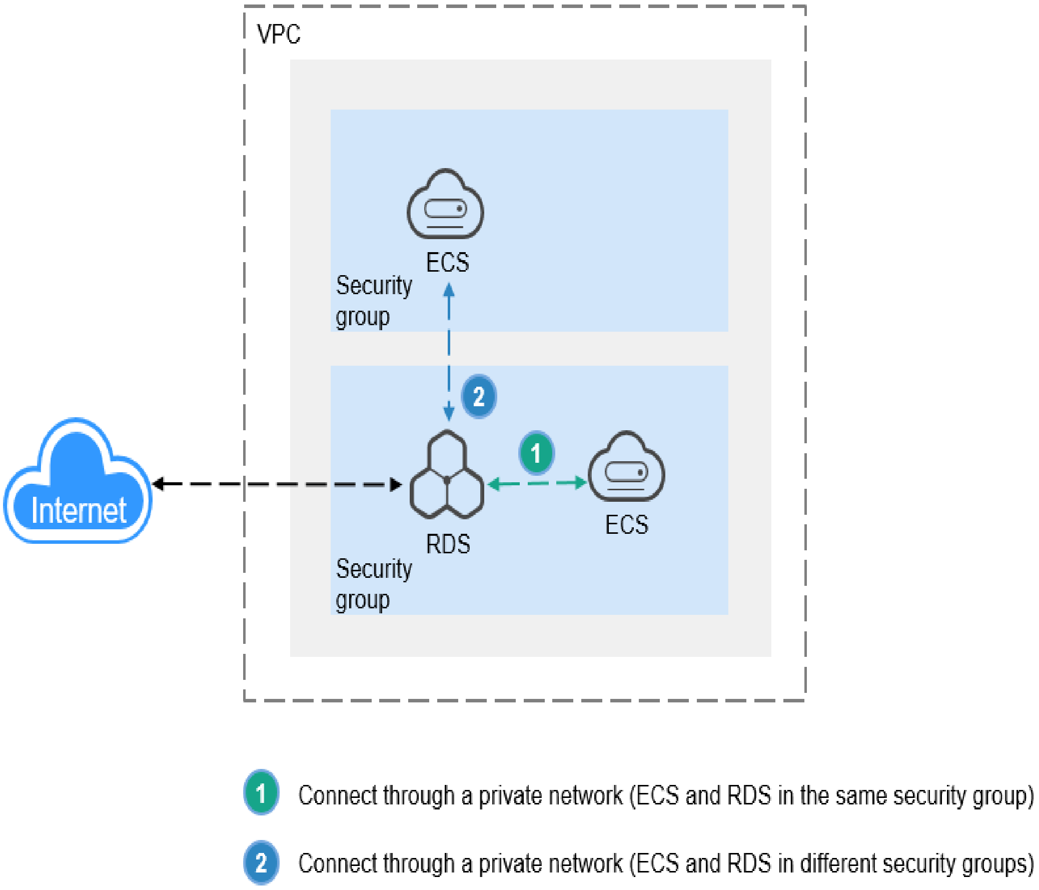

VPC
ECS
Security group
2
1
Internet
RDS
ECS
Security group
1 Connect through a private network (ECS and RDS in the same security group)
2 Connect through a private network (ECS and RDS in different security groups)

Table 1-9 Connection methods

Server	Connection Tool	IP Address	Default Port	Security Group Rules
Linux ECS	MySQL CLI	Floating IP address	3306	- If the ECS and RDS DB instance are in the same security group, they can communicate with each other by default. No security group rules need to be configured. - If they are in different security groups, configure security group rules for them, separately. – RDS DB instance: Configure an **inbound rule** for the security group with which the RDS DB instance is associated. For details, see **Configuring Security Group Rules**. – ECS: The default security group rule allows all outgoing data packets. In this case, you do not need to configure a security group rule for the ECS. If not all outbound traffic is allowed in the security group, you need to configure an **outbound rule** for the ECS.
Windows ECS	Database client such as MySQL-Front	Floating IP address	3306	

To connect to a DB instance from a Linux ECS, perform the following steps:

- **Step 1: Buy an ECS**: Purchase and log in to a Linux ECS. Ensure that the ECS and RDS for MySQL DB instance are in the same region and VPC.
- **Step 2: Test Connectivity and Install a MySQL Client**: Test the network connectivity between the ECS and the floating IP address and port of the RDS for MySQL DB instance, and install a MySQL client.
- **Step 3: Connect to the DB Instance Using Commands (Non-SSL Connection)**: Use the MySQL CLI to connect to the DB instance using the floating IP address and port.

To connect to a DB instance from a Windows ECS, perform the following steps:

- **Step 1: Buy an ECS**: Purchase and log in to a Windows ECS. Ensure that the ECS and RDS for MySQL DB instance are in the same region and VPC.
- **Step 2: Test Connectivity and Install MySQL-Front**: Test the network connectivity between the ECS and the floating IP address and port of the RDS for MySQL DB instance, and install MySQL-Front (MySQL-Front is used as an example).
- **Step 3: Connect to the DB Instance Using MySQL-Front**: Use MySQL-Front to connect to the DB instance using the floating IP address and port.

1.3.3.2 Connecting to a DB Instance from a Linux ECS

You can connect to your DB instance using a Linux ECS installed with a MySQL client over a private network.

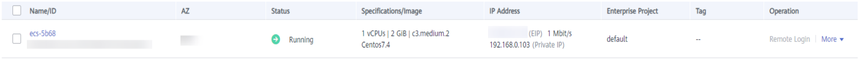
This section describes how to connect to a DB instance with SSL disabled. To connect to a DB instance with SSL enabled, see **Using MySQL CLI to Connect to an Instance Through a Private Network**.

- **Step 1: Buy an ECS**
- **Step 2: Test Connectivity and Install a MySQL Client**
- **Step 3: Connect to the DB Instance Using Commands (Non-SSL Connection)**

Step 1: Buy an ECS

1. **Log in to the management console** and check whether there is an ECS available.
   - If there is a Linux ECS, go to **3**.
   - If there is a Windows ECS, see **Connecting to a DB Instance from a Windows ECS**.
   - If no ECS is available, go to **2**.

   Figure 1-10 ECS

□	Name/ID	AZ	Status	Specifications/Image	IP Address	Enterprise Project	Tag	Operation
□	ecs-5b68 [redacted]	[redacted]	Running	1 vCPUs | 2 GiB | c3.medium.2 Centos7.4	[redacted] (EIP) 1 Mbit/s 192.168.0.103 (Private IP)	default	--	Remote Login | More ▾

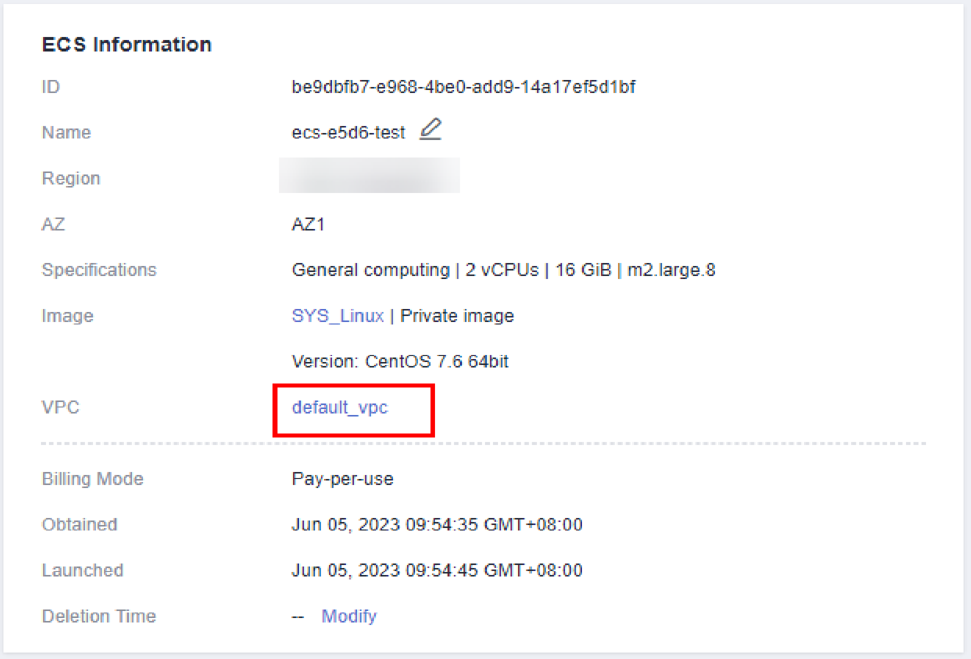
2. Buy an ECS and select Linux (for example, CentOS) as its OS.

   To download a MySQL client to the ECS, bind an EIP to the ECS. The ECS must be in the same region, VPC, and security group as the RDS for MySQL DB instance for mutual communications.

   For details about how to purchase a Linux ECS, see "**Purchasing an ECS**" in *Elastic Cloud Server Getting Started*.

3. On the **ECS Information** page, view the region and VPC of the ECS.

Figure 1-11 ECS information

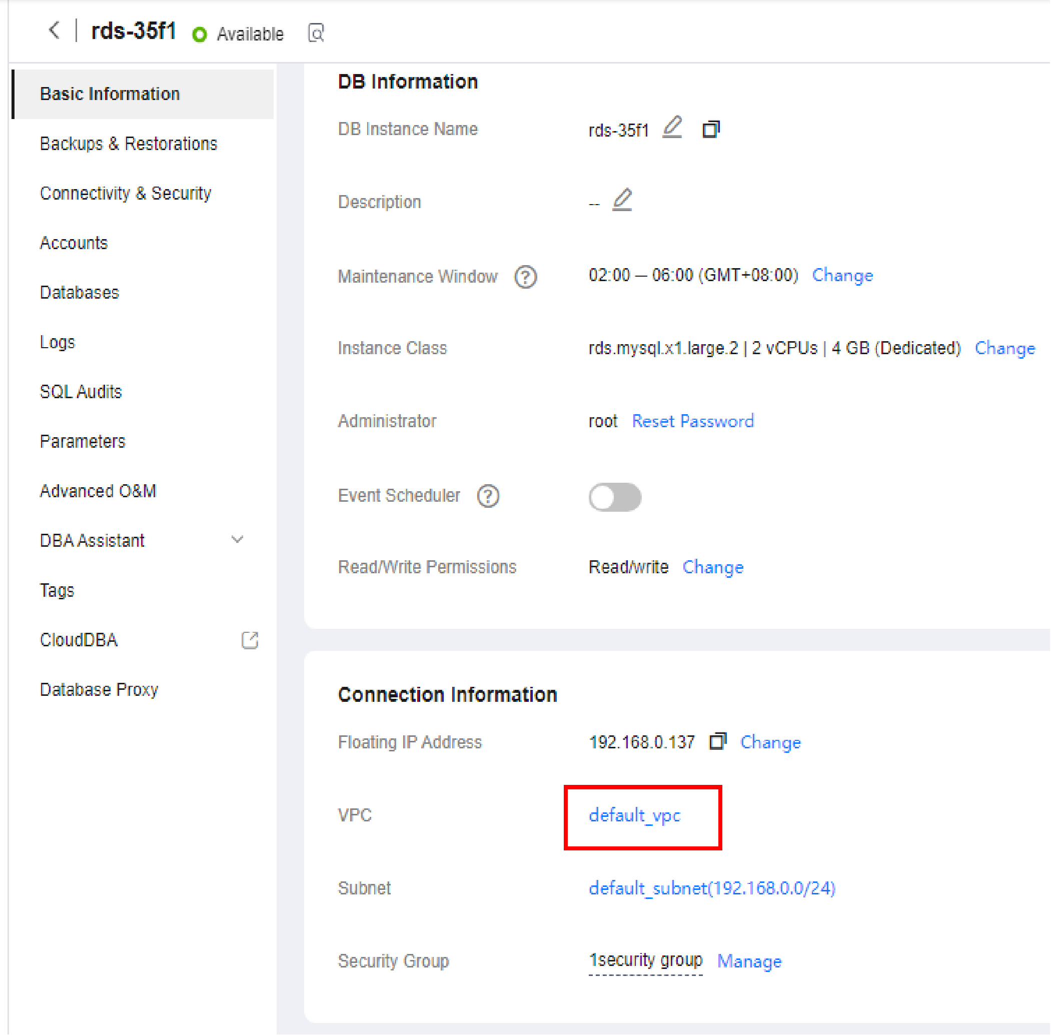


ECS Information

ID	be9dbfb7-e968-4be0-add9-14a17ef5d1bf
Name	ecs-e5d6-test
Region	[redacted]
AZ	AZ1
Specifications	General computing | 2 vCPUs | 16 GiB | m2.large.8
Image	SYS_Linux | Private image Version: CentOS 7.6 64bit
VPC	default_vpc
Billing Mode	Pay-per-use
Obtained	Jun 05, 2023 09:54:35 GMT+08:00
Launched	Jun 05, 2023 09:54:45 GMT+08:00
Deletion Time	-- Modify

4. On the **Basic Information** page of the RDS for MySQL instance, view the region and VPC of the DB instance.

Figure 1-12 DB instance information



rds-35f1 Available

DB Information

DB Instance Name: rds-35f1

Description: --

Maintenance Window: 02:00 — 06:00 (GMT+08:00)

Instance Class: rds.mysql.x1.large.2 | 2 vCPUs | 4 GB (Dedicated)

Administrator: root

Event Scheduler

Read/Write Permissions: Read/write

Connection Information

Floating IP Address: 192.168.0.137

VPC: default_vpc

Subnet: default_subnet(192.168.0.0/24)

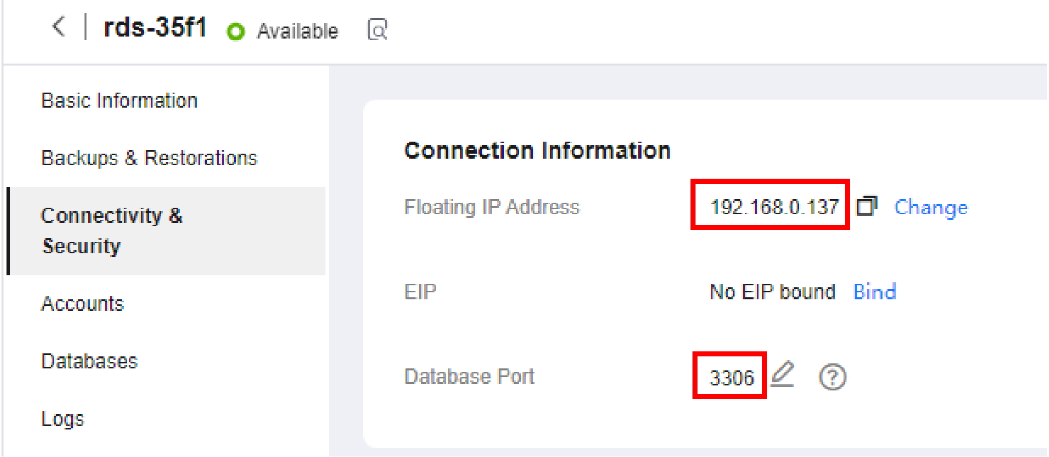
Security Group: 1security group

5. Check whether the ECS and RDS for MySQL instance are in the same region and VPC.
   - If yes, go to **Step 2: Test Connectivity and Install a MySQL Client**.
   - If they are not in the same region, purchase another ECS or DB instance. The ECS and DB instance in different regions cannot communicate with each other. To reduce network latency, deploy your DB instance in the region nearest to your workloads.
   - If the ECS and DB instance are in different VPCs, change the VPC of the ECS to that of the DB instance. For details, see **Changing a VPC**.

Step 2: Test Connectivity and Install a MySQL Client

1. Log in to the ECS. For details, see **Login Using VNC** in the *Elastic Cloud Server User Guide*.
2. On the **Instances** page, click the DB instance name.
3. Choose **Connectivity & Security** from the navigation pane. In the **Connection Information** area, obtain the floating IP address and database port of the DB instance.

Figure 1-13 Connection information



Connection Information

Floating IP Address 192.168.0.137

EIP No EIP bound

Database Port 3306

4. On the ECS, check whether the floating IP address and database port of the DB instance can be connected.

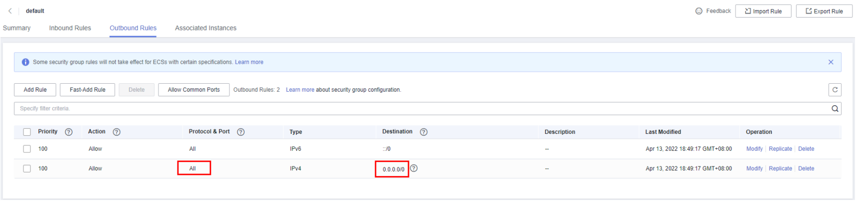
   telnet *192.168.6.144 3306*

   – If yes, network connectivity is available.

   – If no, check the security group rules.

     ■ If in the security group of the ECS, there is no outbound rule with **Destination** set to **0.0.0.0/0** and **Protocol & Port** set to **All**, add an outbound rule for the floating IP address and port of the DB instance.

     Figure 1-14 ECS security group

     Some security group rules will not take effect for ECSs with certain specifications. Learn more

     Outbound Rules: 2 Learn more about security group configuration.

Priority	Action	Protocol & Port	Type	Destination	Description	Last Modified	Operation
100	Allow	All	IPv6	::/0	--	Apr 13, 2022 18:49:17 GMT+08:00	Modify | Replicate | Delete
100	Allow	All	IPv4	0.0.0.0/0	--	Apr 13, 2022 18:49:17 GMT+08:00	Modify | Replicate | Delete

     ■ If in the security group of the DB instance, there is no inbound rule allowing the access from the private IP address and port of the ECS, add an inbound rule for the private IP address and port of the ECS. For details, see **Configuring Security Group Rules**.

5. Download the MySQL client installation package for Linux to the ECS. The package **mysql-community-client-5.7.38-1.el6.x86_64.rpm** is used as an example.

   A MySQL client running a version later than that of the DB instance is recommended.

   wget https://dev.mysql.com/get/mysql-community-client-5.7.38-1.el6.x86_64.rpm

6. Install the MySQL client.

   rpm -ivh --nodeps mysql-community-client-5.7.38-1.el6.x86_64.rpm

NOTE

- If any conflicts occur during the installation, add the **replacefiles** parameter to the command and install the client again.

  rpm -ivh --replacefiles mysql-community-client-5.7.38-1.el6.x86_64.rpm

- If a message is displayed prompting you to install a dependency package during the installation, add the **nodeps** parameter to the command and install the client again.

  rpm -ivh --nodeps mysql-community-client-5.7.38-1.el6.x86_64.rpm

Step 3: Connect to the DB Instance Using Commands (Non-SSL Connection)

1. Run the following command on the ECS to connect to the DB instance:

   mysql -h <*host*> **-P** <*port*> **-u** <*userName*> **-p**

   Example:

   mysql -h 192.168.6.144 -P 3306 -u root -p

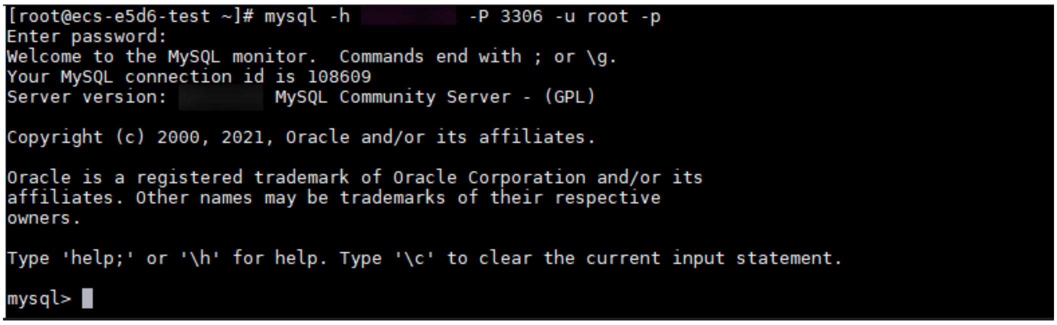
   Table 1-10 Parameter description

Parameter	Description
<*host*>	Floating IP address obtained in 3.
<*port*>	Database port obtained in 3. The default value is 3306.
<*userName*>	Administrator account **root**.

2. Enter the password of the database account if the following information is displayed:

```
Enter password:
```

Figure 1-15 Connection successful



```
[root@ecs-e5d6-test ~]# mysql -h [redacted] -P 3306 -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 108609
Server version: [redacted] MySQL Community Server - (GPL)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```

FAQ

What Should I Do If I Can't Connect to My RDS DB Instance?

Follow-up Operations

After logging in to the DB instance, you can create or migrate databases.

- **Creating a MySQL Database Using the Console**

- **Creating a MySQL Database Using an API**
- **Managing MySQL Databases Using DAS**
- **Migrating Data to RDS for MySQL**

1.3.3.3 Connecting to a DB Instance from a Windows ECS

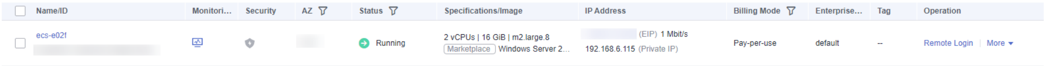
You can connect to your DB instance using a Windows ECS installed with a database client (for example, MySQL-Front) over a private network.

- **Step 1: Buy an ECS**
- **Step 2: Test Connectivity and Install MySQL-Front**
- **Step 3: Connect to the DB Instance Using MySQL-Front**

Step 1: Buy an ECS

1. **Log in to the management console** and check whether there is an ECS available.
   - If there is a Linux ECS, see **Connecting to a DB Instance from a Linux ECS**.
   - If there is a Windows ECS, go to **3**.
   - If no ECS is available, go to **2**.

   Figure 1-16 ECS

□	Name/ID	Monitori...	Security	AZ	Status	Specifications/Image	IP Address	Billing Mode	Enterprise...	Tag	Operation
□	ecs-e02f [redacted]			[redacted]	Running	2 vCPUs | 16 GiB | m2.large.8 Marketplace Windows Server 2...	[redacted] (EIP) 1 Mbit/s 192.168.6.115 (Private IP)	Pay-per-use	default	--	Remote Login | More ▾

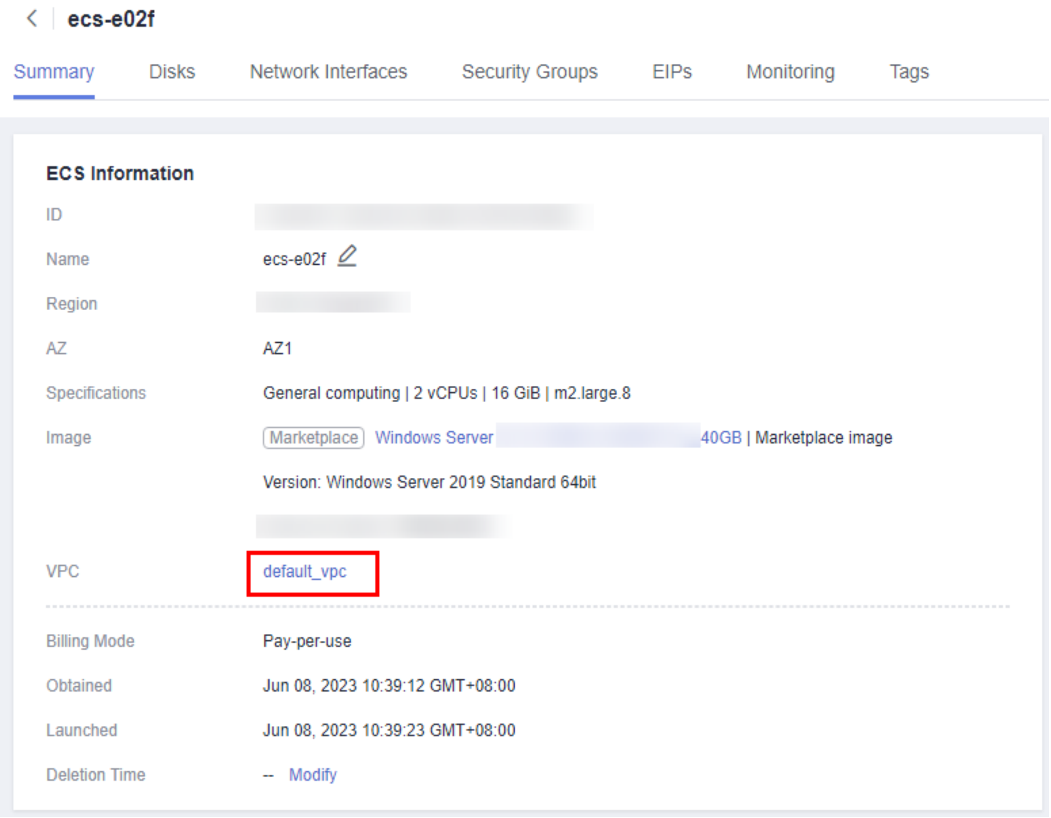
2. Buy an ECS and select Windows as its OS.

   To download a MySQL client to the ECS, bind an EIP to the ECS. The ECS must be in the same region, VPC, and security group as the RDS for MySQL DB instance for mutual communications.

   For details about how to purchase a Windows ECS, see "**Purchasing an ECS**" in *Elastic Cloud Server Getting Started*.

3. On the **ECS Information** page, view the region and VPC of the ECS.

Figure 1-17 ECS information



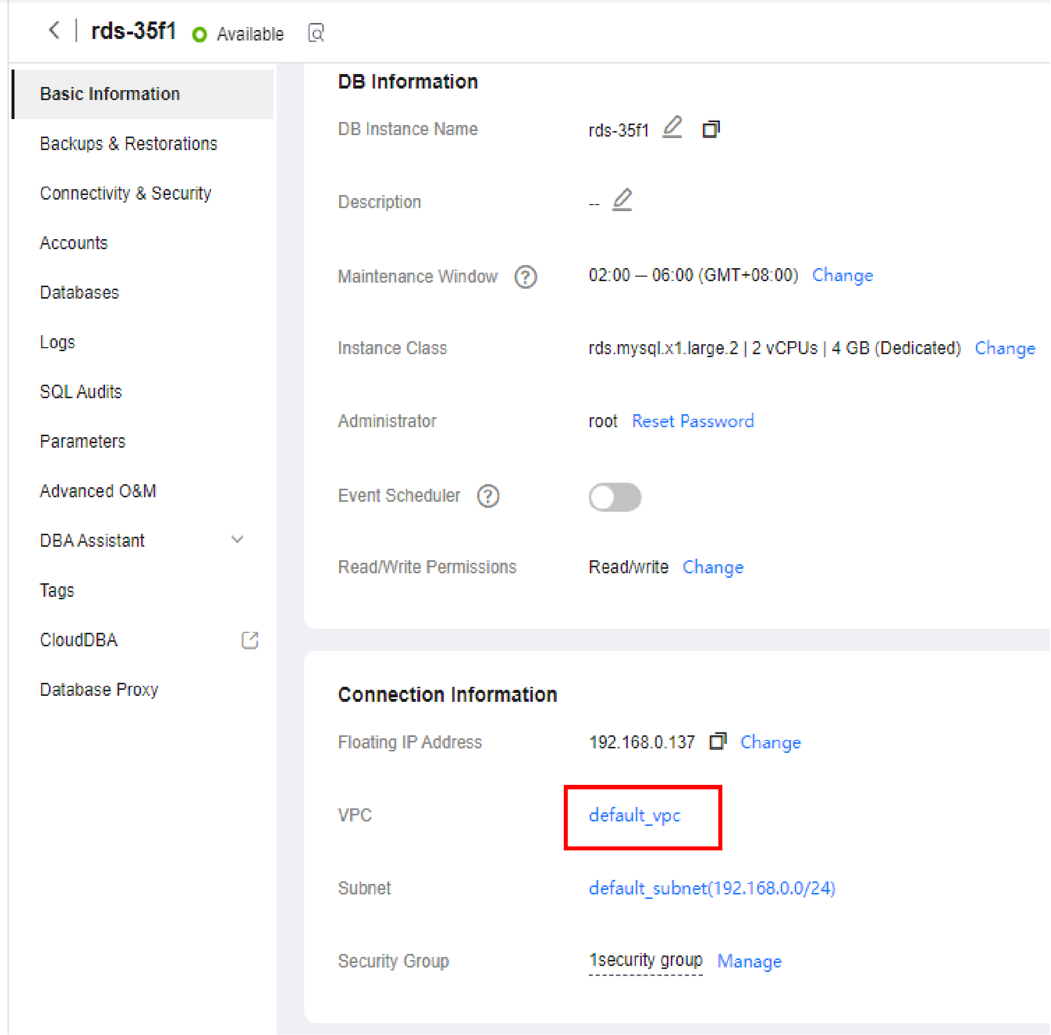
ecs-e02f

ECS Information

ID	[redacted]
Name	ecs-e02f
Region	[redacted]
AZ	AZ1
Specifications	General computing | 2 vCPUs | 16 GiB | m2.large.8
Image	Marketplace Windows Server [redacted] 40GB | Marketplace image Version: Windows Server 2019 Standard 64bit [redacted]
VPC	default_vpc
Billing Mode	Pay-per-use
Obtained	Jun 08, 2023 10:39:12 GMT+08:00
Launched	Jun 08, 2023 10:39:23 GMT+08:00
Deletion Time	-- Modify

4. On the **Basic Information** page of the RDS for MySQL instance, view the region and VPC of the DB instance.

Figure 1-18 DB instance information



DB Information

DB Instance Name	rds-35f1
Description	--
Maintenance Window	02:00 — 06:00 (GMT+08:00) Change
Instance Class	rds.mysql.x1.large.2 | 2 vCPUs | 4 GB (Dedicated) Change
Administrator	root Reset Password
Event Scheduler	
Read/Write Permissions	Read/write Change

Connection Information

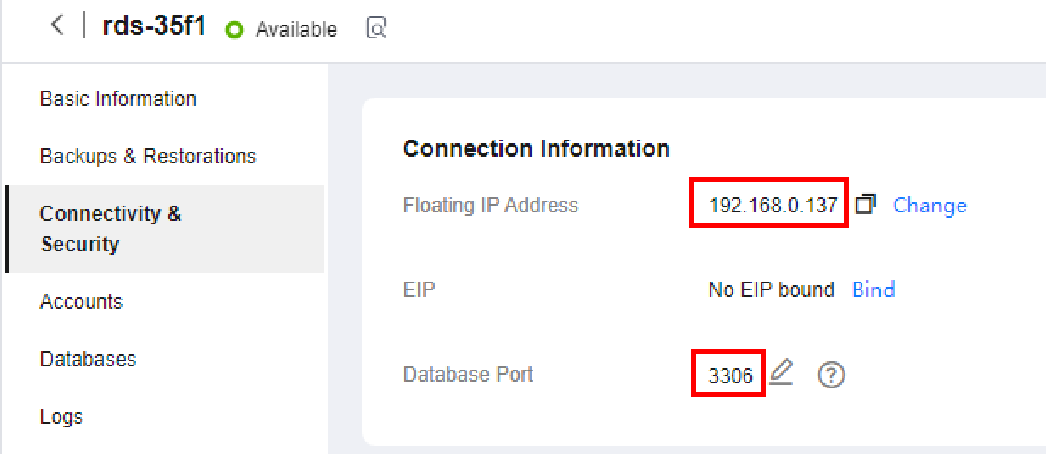
Floating IP Address	192.168.0.137 Change
VPC	default_vpc
Subnet	default_subnet(192.168.0.0/24)
Security Group	1security group Manage

5. Check whether the ECS and RDS for MySQL instance are in the same region and VPC.
   - If yes, go to **Step 2: Test Connectivity and Install MySQL-Front**.
   - If they are not in the same region, purchase another ECS or DB instance. The ECS and DB instance in different regions cannot communicate with each other. To reduce network latency, deploy your DB instance in the region nearest to your workloads.
   - If the ECS and DB instance are in different VPCs, change the VPC of the ECS to that of the DB instance. For details, see **Changing a VPC**.

Step 2: Test Connectivity and Install MySQL-Front

1. Log in to the ECS. For details, see **Login Using VNC** in the *Elastic Cloud Server User Guide*.
2. On the **Instances** page, click the DB instance name.
3. Choose **Connectivity & Security** from the navigation pane. In the **Connection Information** area, obtain the floating IP address and database port of the DB instance.

Figure 1-19 Connection information



Connection Information

Floating IP Address	192.168.0.137
EIP	No EIP bound
Database Port	3306

4. Open the cmd window on the ECS and check whether the floating IP address and database port of the DB instance can be connected.

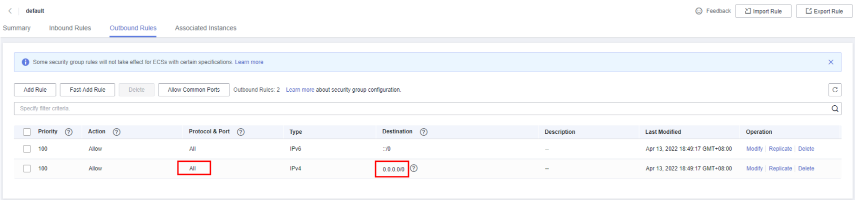
   telnet *192.168.6.144 3306*

   – If yes, network connectivity is available.

   – If no, check the security group rules.

     ■ If in the security group of the ECS, there is no outbound rule with **Destination** set to **0.0.0.0/0** and **Protocol & Port** set to **All**, add an outbound rule for the floating IP address and port of the DB instance.

     Figure 1-20 ECS security group

     Some security group rules will not take effect for ECSs with certain specifications. Learn more

     Outbound Rules: 2 Learn more about security group configuration.

     Specify filter criteria.

Priority	Action	Protocol & Port	Type	Destination	Description	Last Modified	Operation
100	Allow	All	IPv6	::/0	--	Apr 13, 2022 18:49:17 GMT+08:00	Modify | Replicate | Delete
100	Allow	All	IPv4	0.0.0.0/0	--	Apr 13, 2022 18:49:17 GMT+08:00	Modify | Replicate | Delete

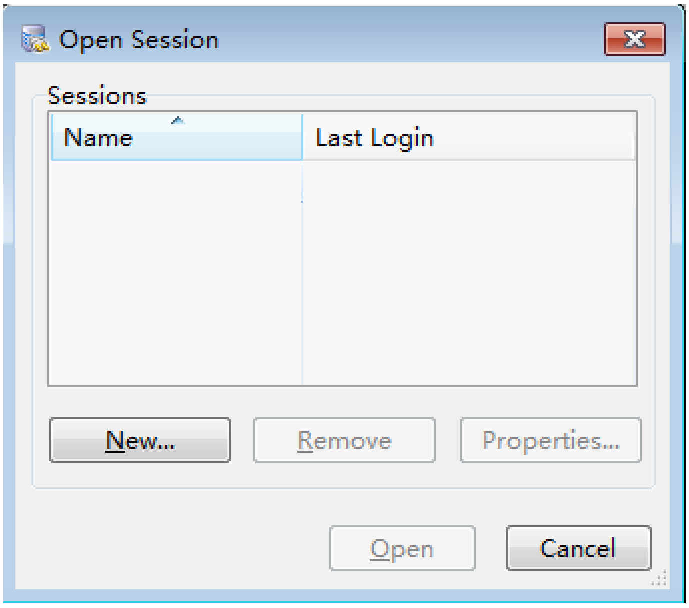
     ■ If in the security group of the DB instance, there is no inbound rule allowing the access from the private IP address and port of the ECS, add an inbound rule for the private IP address and port of the ECS. For details, see **Configuring Security Group Rules**.

5. Open a browser, and download and install the MySQL-Front tool on the ECS (version 5.4 is used as an example).

Step 3: Connect to the DB Instance Using MySQL-Front

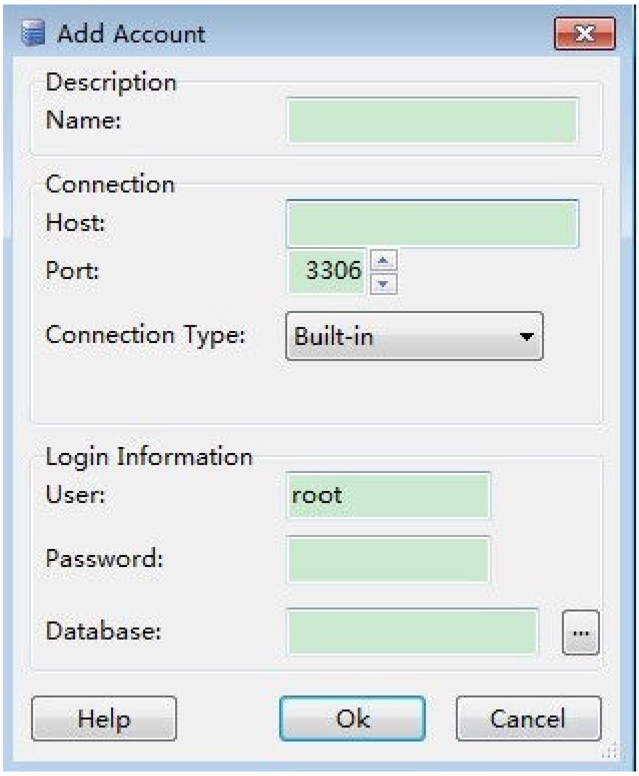
1. Start MySQL-Front.
2. In the displayed dialog box, click **New**.

Figure 1-21 Connection management



3. Enter the information of the DB instance to be connected and click **Ok**.

Figure 1-22 Adding an account



Port: 3306

Connection Type: Built-in

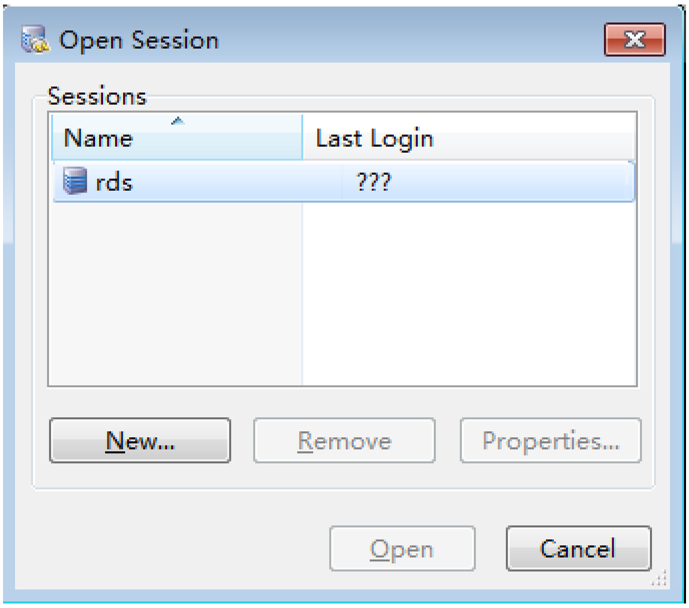
User: root

Table 1-11 Parameter description

Parameter	Description
Name	Name of the database connection task. If you do not specify this parameter, it will be the same as that configured for **Host** by default.
Host	Floating IP address obtained in 3.
Port	Database port obtained in 3. The default value is 3306.
User	Name of the user who will access the DB instance. The default user is **root**.
Password	Password of the account for accessing the DB instance.

4. In the displayed window, select the connection that you have created in 3 and click **Open**. If the connection information is correct, the DB instance will be connected.

Figure 1-23 Opening a session



FAQs

What Should I Do If I Can't Connect to My RDS DB Instance?

Follow-up Operations

After logging in to the DB instance, you can create or migrate your databases.

- **Creating a Database Using the Console**
- **Creating a Database Using an API**
- **Managing Databases Using DAS**

- **Migrating Data to RDS for MySQL**

1.3.3.4 Configuring Security Group Rules

Scenarios

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

Before you can connect to your DB instance, you need to create security group rules to enable specific IP addresses and ports to access your RDS instance.

First check whether the ECS and RDS DB instance are in the same security group.

- If they are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to **Connecting to a DB Instance from a Linux ECS**.
- If they are in different security groups, configure security group rules for them, separately.
  - RDS DB instance: Configure an **inbound rule** for the security group with which the RDS DB instance is associated.
  - ECS: The default security group rule allows all outgoing data packets. In this case, you do not need to configure a security group rule for the ECS. If not all outbound traffic is allowed in the security group, you need to configure an **outbound rule** for the ECS.

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

For details about the requirements of security group rules, see the **Adding a Security Group Rule** section in the *Virtual Private Cloud User Guide*.

Precautions

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.

- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS instance can be associated with multiple security groups, and one security group can be associated with multiple RDS instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for a security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

NOTE

To ensure the security of your data and DB instances, you are advised to use the principle of least privilege for database access. Change the default database port **3306**, and set the IP address to the remote server's address or the remote server's smallest subnet address to control the access from the remote server.

The default value of **Source** is **0.0.0.0/0**, indicating that RDS DB instances in the security group can be accessed from any IP address.

For details about the requirements of security group rules, see the **Adding a Security Group Rule** section in the *Virtual Private Cloud User Guide*.

Procedure

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

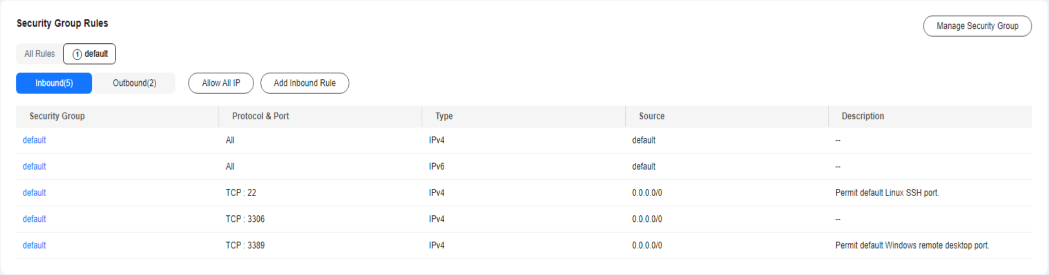
Step 2 Click in the upper left corner and select a region and a project.

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

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

Step 5 In the navigation pane, choose **Connectivity & Security**. In the **Security Group Rules** area, click the security group name to view the security group rules.

Figure 1-24 Security group rules



Security Group Rules

Security Group	Protocol & Port	Type	Source	Description
default	All	IPv4	default	--
default	All	IPv6	default	--
default	TCP : 22	IPv4	0.0.0.0/0	Permit default Linux SSH port.
default	TCP : 3306	IPv4	0.0.0.0/0	--
default	TCP : 3389	IPv4	0.0.0.0/0	Permit default Windows remote desktop port.

Step 6 Click **Add Inbound Rule** or **Allow All IP** to configure security group rules.

To add more inbound rules, click ⊕.

NOTE

Allow All IP allows all IP addresses to access RDS DB instances in the security group, which poses high security risks. Exercise caution when performing this operation.

Figure 1-25 Adding an inbound rule

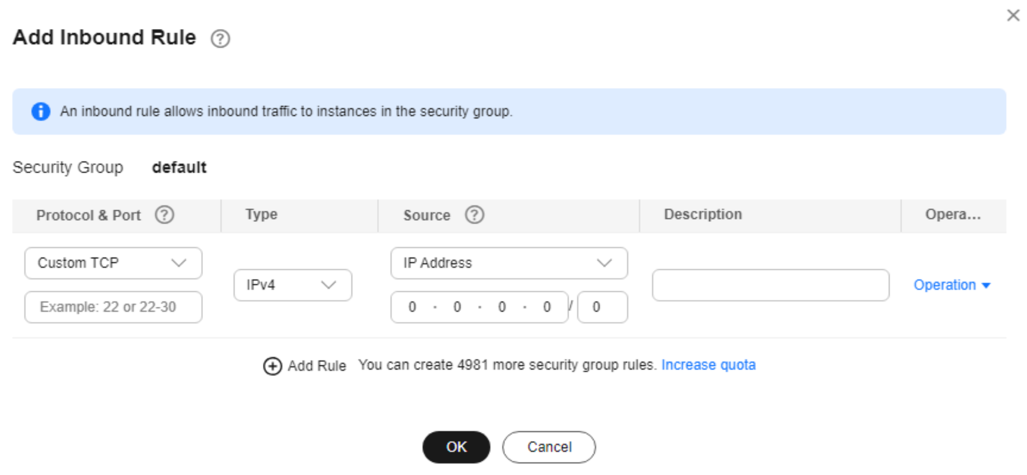


Table 1-12 Inbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	**Protocol**: network protocol. Available options: **All ports**, **Custom TCP**, **Custom UDP**, **ICMP**, or **GRE**.	Custom TCP
	Port: the port over which the traffic can reach your DB instance. RDS for MySQL instances can use database ports 1024 to 65535, excluding 12017 and 33071, which are reserved for RDS system use.	3306
Type	IP address type. ● IPv4 ● IPv6	IPv4

Parameter	Description	Example Value
Source	Source address. It can be a single IP address, an IP address group, or a security group to allow access from them to your DB instance. Examples: ● Single IP address: 192.168.10.10/32 (IPv4); 2002:50::44/128 (IPv6) ● All IP addresses: 0.0.0.0/0 (IPv4); ::/0 (IPv6) ● IP address range: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Security group: default_securitygroup	0.0.0.0/0
Description	Supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (<) or (>).	N/A

----End

1.3.4 Connecting to an RDS for MySQL DB Instance Through a Public Network

1.3.4.1 Overview

Process

Figure 1-26 illustrates the process of connecting to an RDS for MySQL DB instance through a public network.

Figure 1-26 Connecting to a DB instance through a public network

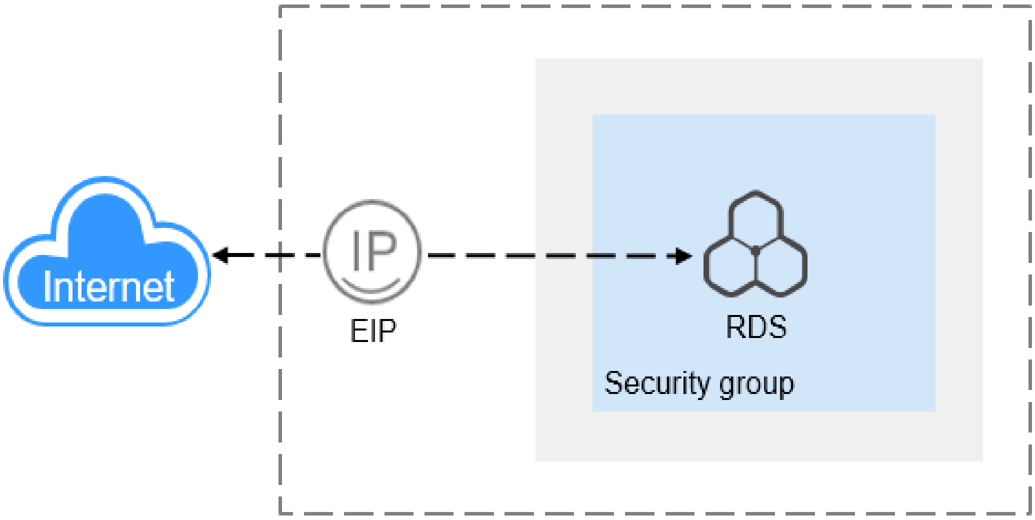


Table 1-13 Connection methods

Server	Connection Tool	IP Address	Default Port	Security Group Rules
Linux ECS	MySQL CLI	EIP	3306	To access your DB instance from a server that is not in the same security group as your DB instance, configure an inbound rule for the security group with which your DB instance is associated. For details, see **Configuring Security Group Rules**.
Local Windows Server	Database client such as MySQL-Front	EIP	3306	

To connect to a DB instance from a Linux ECS, perform the following steps:

- **Step 1: Buy an ECS**: Purchase and log in to a Linux ECS.
- **Step 2: Test Connectivity and Install a MySQL Client**: Test the network connectivity between the ECS and the EIP and port of the RDS for MySQL DB instance, and install a MySQL client.
- **Step 3: Connect to the DB Instance Using Commands (Non-SSL Connection)**: Use the MySQL CLI to connect to the DB instance via the EIP and port.

To connect to a DB instance from a local Windows server, perform the following steps:

- **Step 1: Test Connectivity and Install MySQL-Front**: Test the network connectivity between the local server and the EIP and port of the RDS for MySQL DB instance and install MySQL-Front (MySQL-Front is used as an example).
- **Step 2: Connect to the DB Instance Using MySQL-Front**: Use MySQL-Front to connect to the DB instance using the EIP and port.

1.3.4.2 Binding an EIP

Scenarios

You can bind an EIP to a DB instance for public accessibility and can unbind the EIP from the DB instance as required.

Precautions

- You need to configure security groups and enable specific IP addresses and ports to access the target DB instance. Before accessing the DB instance, add an individual IP address or an IP address range that will access the DB instance to the inbound rule. For details, see **Configuring Security Group Rules**.
- Traffic generated by the public network is charged. You can unbind the EIP from the DB instance when the EIP is no longer used.

Binding an EIP

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

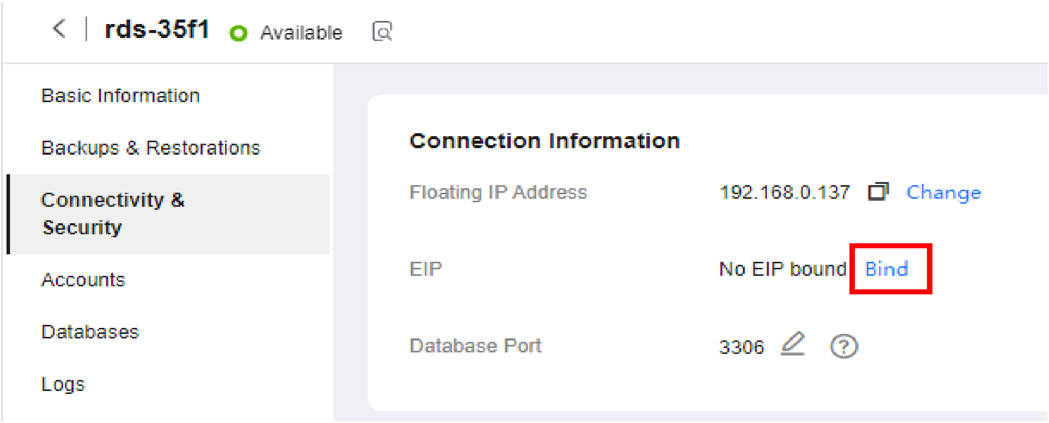
Step 2 Click 📍 in the upper left corner and select a region and a project.

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

Step 4 On the **Instances** page, click the target DB instance.

Step 5 In the navigation pane on the left, choose **Connectivity & Security**. In the **Connection Information** area, click **Bind** next to the **EIP** field.

Figure 1-27 Binding an EIP



Connection Information

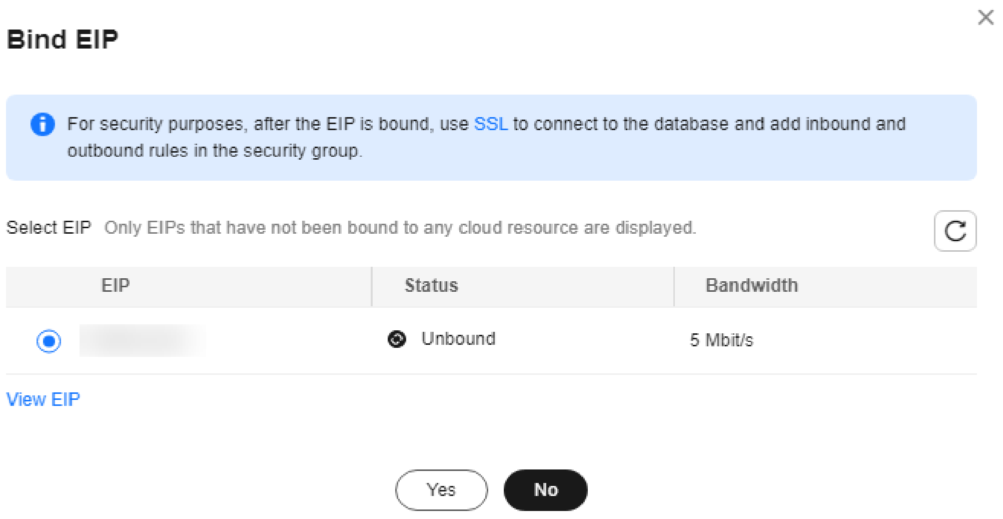
Floating IP Address 192.168.0.137 Change

EIP No EIP bound Bind

Database Port 3306

Step 6 In the displayed dialog box, select an EIP and click **Yes**.

Figure 1-28 Selecting an EIP



Bind EIP

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

Select EIP Only EIPs that have not been bound to any cloud resource are displayed.

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

View EIP

Yes No

Step 7 On the **Connectivity & Security** page, view the EIP that has been bound to the DB instance.

You can also view the progress and result of binding an EIP to a DB instance on the **Task Center** page.

----End

1.3.4.3 Connecting to a DB Instance from a Linux ECS

You can connect to your DB instance using a Linux ECS installed with a MySQL client over a public network.

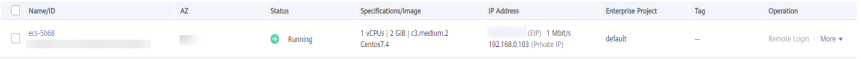
This section describes how to connect to a DB instance with SSL disabled. To connect to a DB instance with SSL enabled, see **Using MySQL CLI to Connect to an Instance Through a Public Network**.

- **Step 1: Buy an ECS**
- **Step 2: Test Connectivity and Install a MySQL Client**
- **Step 3: Connect to the DB Instance Using Commands (Non-SSL Connection)**

Step 1: Buy an ECS

1. **Log in to the management console** and check whether there is an ECS available.
   - If there is a Linux ECS, go to **3**.
   - If there is a Windows ECS, see **Connecting to a DB Instance from a Windows Server**.
   - If no ECS is available, go to **2**.

   Figure 1-29 ECS



□	Name/ID	AZ	Status	Specifications/Image	IP Address	Enterprise Project	Tag	Operation
□	ecs-5b68 [redacted]	[redacted]	Running	1 vCPUs | 2 GiB | c3.medium.2 Centos7.4	[redacted] (EIP) 1 Mbit/s 192.168.0.103 (Private IP)	default	--	Remote Login | More ▾

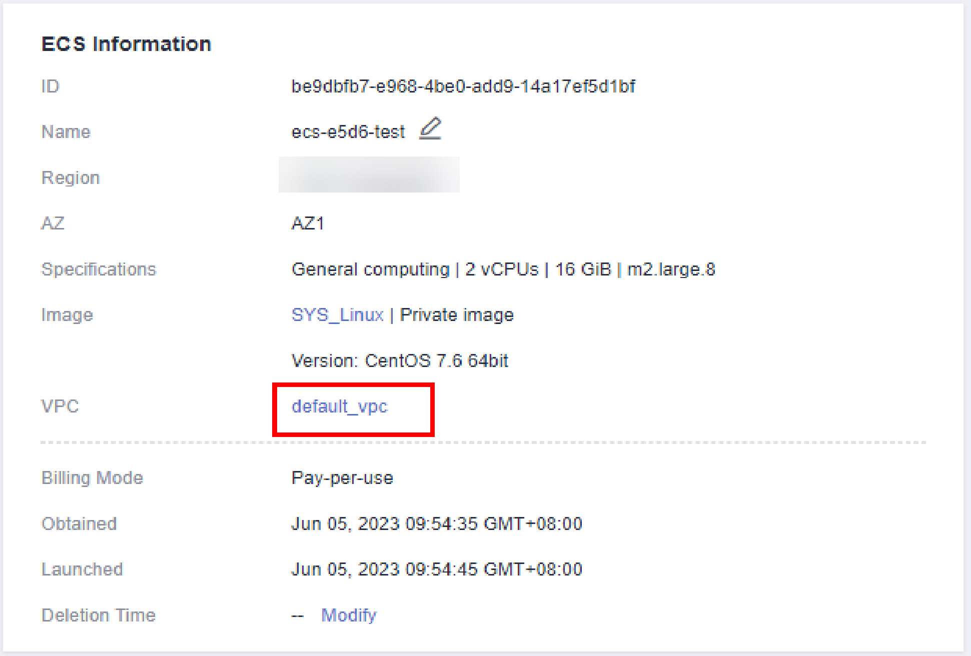
2. Buy an ECS and select Linux (for example, CentOS) as its OS.

   To download a MySQL client to the ECS, bind an EIP to the ECS.

   For details about how to purchase a Linux ECS, see "**Purchasing an ECS**" in *Elastic Cloud Server Getting Started*.

3. On the **ECS Information** page, view the region and VPC of the ECS.

Figure 1-30 ECS information

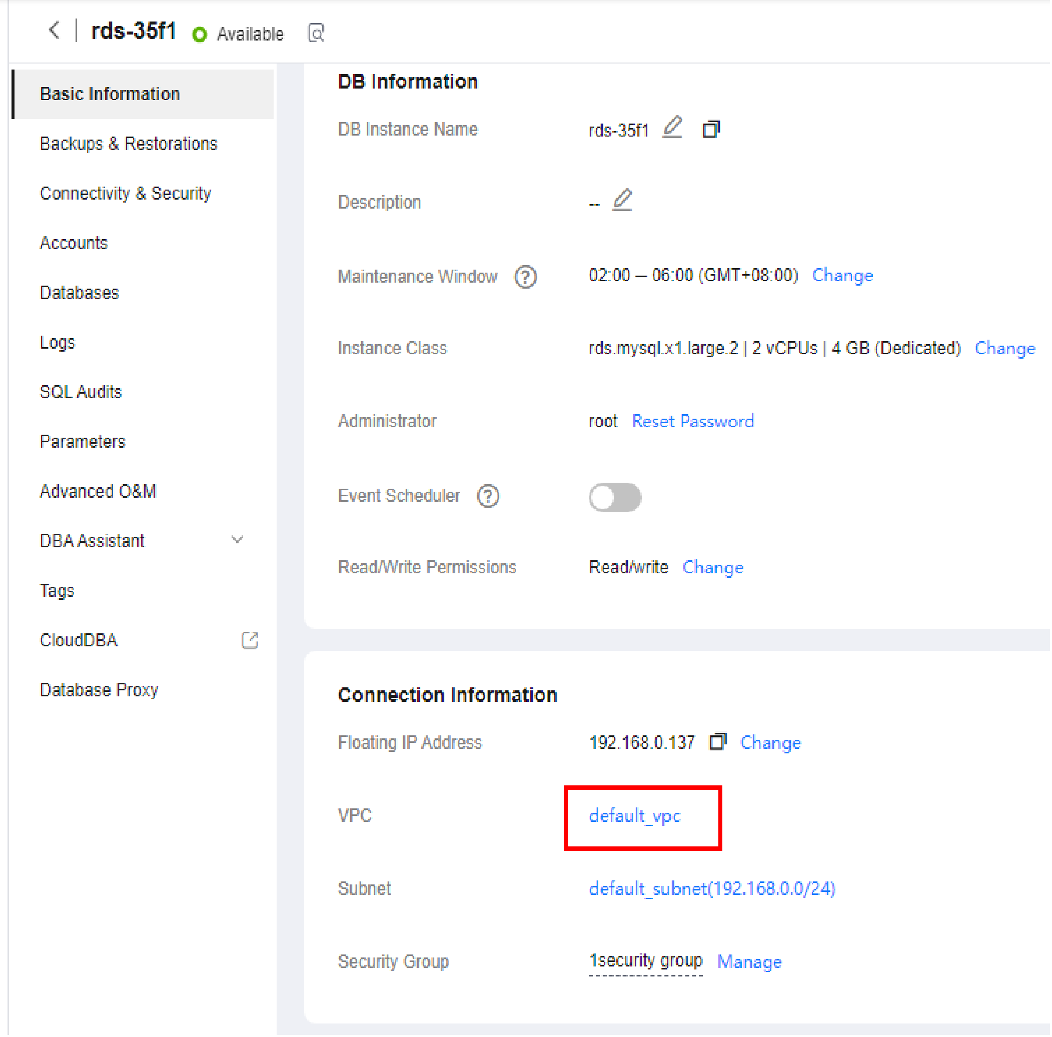


ECS Information

ID	be9dbfb7-e968-4be0-add9-14a17ef5d1bf
Name	ecs-e5d6-test
Region	[redacted]
AZ	AZ1
Specifications	General computing | 2 vCPUs | 16 GiB | m2.large.8
Image	SYS_Linux | Private image
	Version: CentOS 7.6 64bit
VPC	default_vpc
Billing Mode	Pay-per-use
Obtained	Jun 05, 2023 09:54:35 GMT+08:00
Launched	Jun 05, 2023 09:54:45 GMT+08:00
Deletion Time	-- Modify

4. On the **Basic Information** page of the RDS for MySQL instance, view the region and VPC of the DB instance.

Figure 1-31 DB instance information



DB Information

DB Instance Name	rds-35f1
Description	--
Maintenance Window	02:00 — 06:00 (GMT+08:00) Change
Instance Class	rds.mysql.x1.large.2 | 2 vCPUs | 4 GB (Dedicated) Change
Administrator	root Reset Password
Event Scheduler	
Read/Write Permissions	Read/write Change

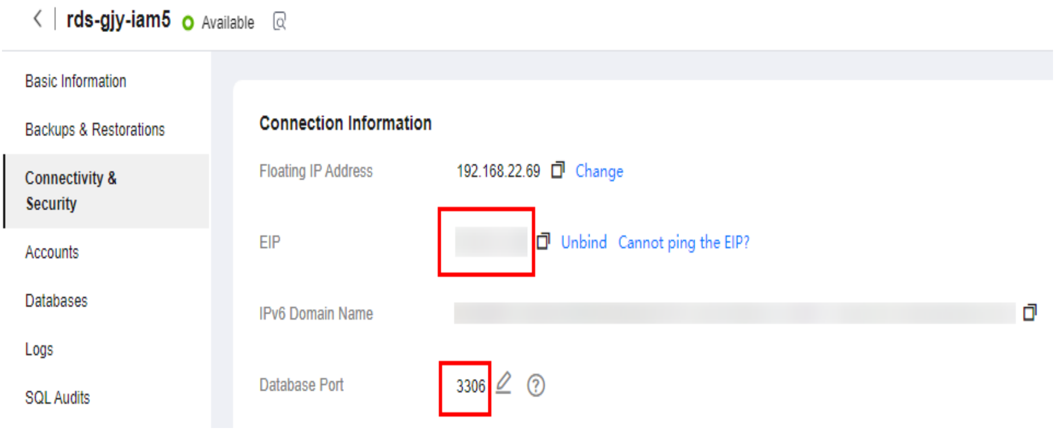
Connection Information

Floating IP Address	192.168.0.137 Change
VPC	default_vpc
Subnet	default_subnet(192.168.0.0/24)
Security Group	1security group Manage

Step 2: Test Connectivity and Install a MySQL Client

1. Log in to the ECS. For details, see **Login Using VNC** in the *Elastic Cloud Server User Guide*.
2. On the **Instances** page, click the DB instance name.
3. Choose **Connectivity & Security** from the navigation pane. In the **Connection Information** area, obtain the EIP and database port of the DB instance.

Figure 1-32 Connection information



Connection Information

Floating IP Address 192.168.22.69 Change

EIP [redacted] Unbind Cannot ping the EIP?

IPv6 Domain Name [redacted]

Database Port 3306

If no EIP has been bound to the DB instance, see **Binding an EIP**.

4. On the ECS, check whether the EIP and database port of the DB instance can be connected.

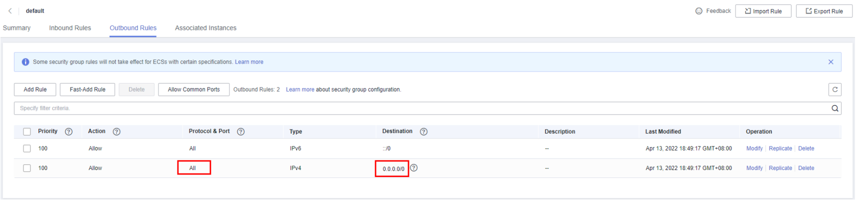
   telnet *EIP 3306*

   – If yes, network connectivity is available.

   – If no, check the security group rules.

     - If in the security group of the ECS, there is no outbound rule with **Destination** set to **0.0.0.0/0** and **Protocol & Port** set to **All**, add an outbound rule for the EIP and port of the DB instance.

       Figure 1-33 ECS security group

       Some security group rules will not take effect for ECSs with certain specifications. Learn more

       Outbound Rules: 2 Learn more about security group configuration.

Priority	Action	Protocol & Port	Type	Destination	Description	Last Modified	Operation
100	Allow	All	IPv6	::/0	--	Apr 13, 2022 18:49:17 GMT+08:00	Modify | Replicate | Delete
100	Allow	All	IPv4	0.0.0.0/0	--	Apr 13, 2022 18:49:17 GMT+08:00	Modify | Replicate | Delete

     - If in the security group of the DB instance, there is no inbound rule allowing the access from the private IP address and port of the ECS, add an inbound rule for the private IP address and port of the ECS. For details, see **Configuring Security Group Rules**.

5. Download the MySQL client installation package for Linux on the ECS. The mysql-community-client-5.7.38-1.el6.x86_64.rpm package is used as an example.

   A MySQL client running a version later than that of the DB instance is recommended.

   wget https://dev.mysql.com/get/mysql-community-client-5.7.38-1.el6.x86_64.rpm

6. Install the MySQL client.

   rpm -ivh --nodeps mysql-community-client-5.7.38-1.el6.x86_64.rpm

NOTE

- If any conflicts occur during the installation, add the **replacefiles** parameter to the command and install the client again.

  rpm -ivh --replacefiles mysql-community-client-5.7.38-1.el6.x86_64.rpm

- If a message is displayed prompting you to install a dependency package during the installation, add the **nodeps** parameter to the command and install the client again.

  rpm -ivh --nodeps mysql-community-client-5.7.38-1.el6.x86_64.rpm

Step 3: Connect to the DB Instance Using Commands (Non-SSL Connection)

1. Run the following command on the ECS to connect to the DB instance:

   mysql -h <*host*> **-P** <*port*> **-u** <*userName*> **-p**

   Example:

   mysql -h 192.168.0.1 -P 3306 -u root -p

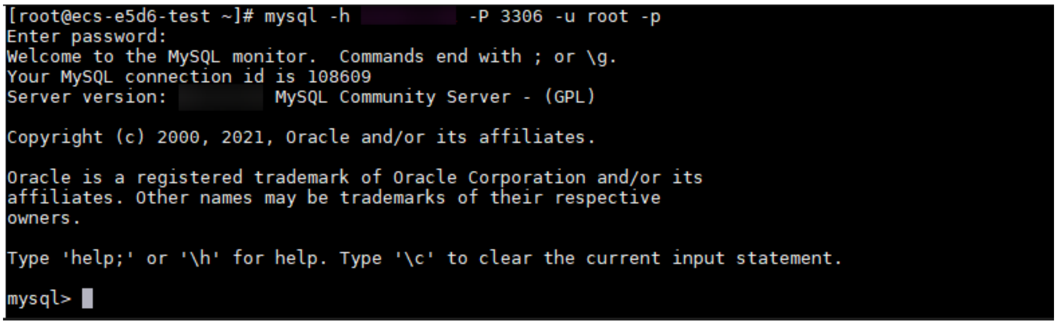
   Table 1-14 Parameter description

Parameter	Description
<*host*>	EIP obtained in 3.
<*port*>	Database port obtained in 3. The default value is 3306.
<*userName*>	Administrator account **root**.

2. Enter the password of the database account if the following information is displayed:

```
Enter password:
```

Figure 1-34 Connection successful



```
[root@ecs-e5d6-test ~]# mysql -h [redacted] -P 3306 -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 108609
Server version: [redacted] MySQL Community Server - (GPL)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```

FAQ

What Should I Do If I Can't Connect to My RDS DB Instance?

Follow-up Operations

After logging in to the DB instance, you can create or migrate databases.

- **Creating a MySQL Database Using the Console**

- **Creating a MySQL Database Using an API**
- **Managing MySQL Databases Using DAS**
- **Migrating Data to RDS for MySQL**

1.3.4.4 Connecting to a DB Instance from a Windows Server

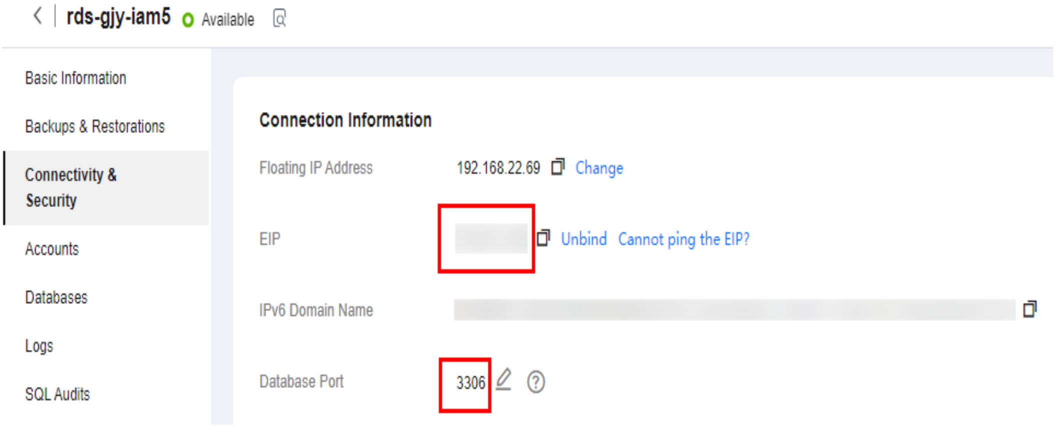
You can connect to your DB instance from a local Windows server installed with a database client (for example, MySQL-Front) over a public network.

- **Step 1: Test Connectivity and Install MySQL-Front**
- **Step 2: Connect to the DB Instance Using MySQL-Front**

Step 1: Test Connectivity and Install MySQL-Front

1. On the **Instances** page, click the DB instance name.
2. Choose **Connectivity & Security** from the navigation pane. In the **Connection Information** area, obtain the EIP and database port of the DB instance.

Figure 1-35 Connection information



Connection Information

Floating IP Address 192.168.22.69

EIP [redacted]

IPv6 Domain Name [redacted]

Database Port 3306

If no EIP has been bound to the DB instance, see **Binding an EIP**.

3. Open the cmd window on your local server and check whether the EIP and database port of the DB instance can be connected.

   telnet *EIP 3306*

   - If yes, network connectivity is available.
   - If no, check the security group rules.

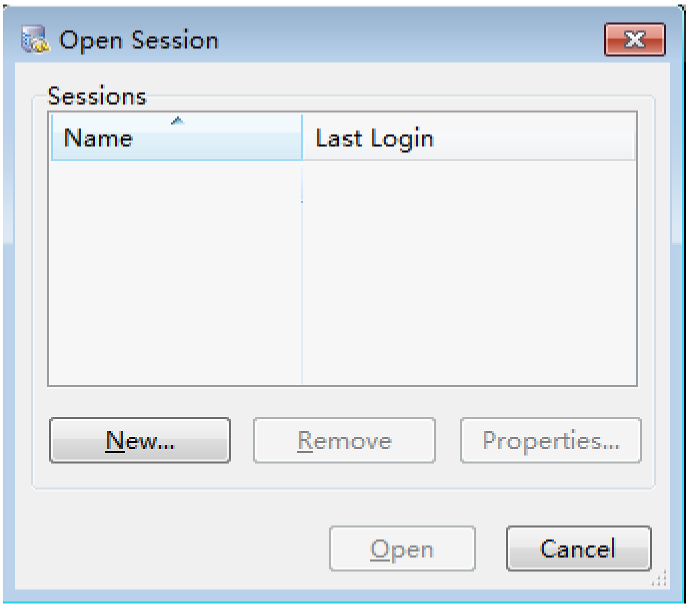
     Check inbound rules in the security group of the DB instance. Add an inbound rule to allow the EIP and port of the DB instance. For details, see **Configuring Security Group Rules**.

4. Open a browser, and download and install the MySQL-Front tool locally (version 5.4 is used as an example).

Step 2: Connect to the DB Instance Using MySQL-Front

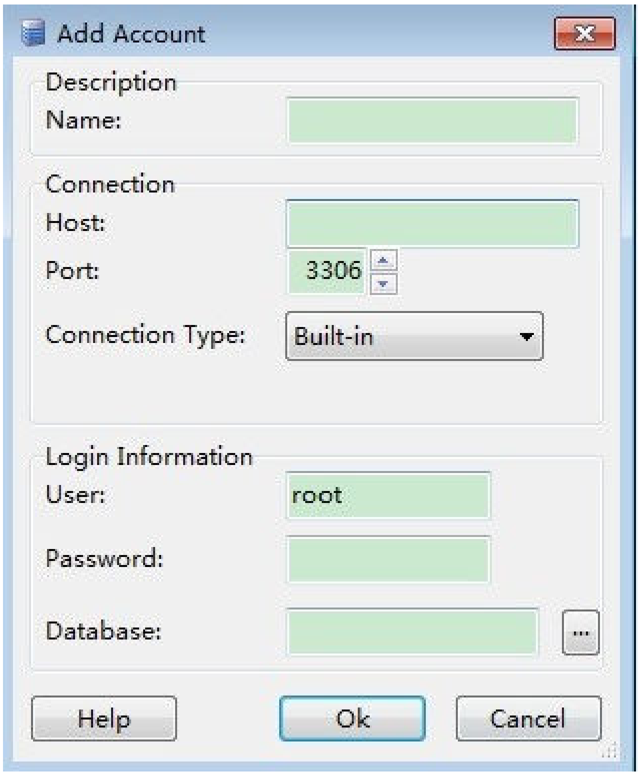
1. Start MySQL-Front.
2. In the displayed dialog box, click **New**.

Figure 1-36 Connection management



3. Enter the information of the DB instance to be connected and click **Ok**.

Figure 1-37 Adding an account



Name:

Host:

Port: 3306

Connection Type: Built-in

User: root

Password:

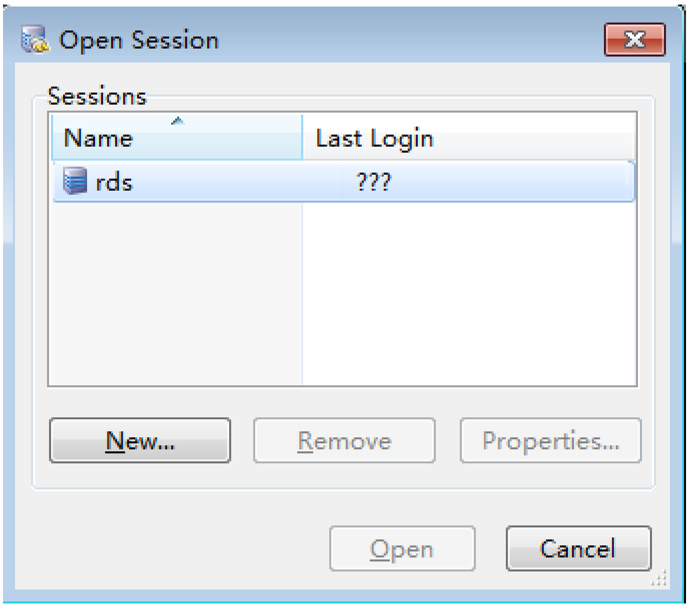
Database:

Table 1-15 Parameter description

Parameter	Description
Name	Name of the database connection task. If you do not specify this parameter, it will be the same as that configured for **Host** by default.
Host	EIP obtained in 2.
Port	Database port obtained in 2. The default value is 3306.
User	Name of the user who will access the DB instance. The default user is **root**.
Password	Password of the account for accessing the DB instance.

4. In the displayed window, select the connection that you have created in 3 and click **Open**. If the connection information is correct, the DB instance will be connected.

Figure 1-38 Opening a session



Open Session

Sessions

Name	Last Login
rds	???

FAQs

What Should I Do If I Can't Connect to My RDS DB Instance?

Follow-up Operations

After logging in to the DB instance, you can create or migrate your databases.

- **Creating a Database Using the Console**
- **Creating a Database Using an API**
- **Managing Databases Using DAS**

- Migrating Data to RDS for MySQL

1.3.4.5 Configuring Security Group Rules

Scenarios

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

Before you can connect to your DB instance, you need to create security group rules to enable specific IP addresses and ports to access your RDS instance.

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

Precautions

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.

- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS instance can be associated with multiple security groups, and one security group can be associated with multiple RDS instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for a security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

NOTE

To ensure the security of your data and DB instances, you are advised to use the principle of least privilege for database access. Change the default database port **3306**, and set the IP address to the remote server's address or the remote server's smallest subnet address to control the access from the remote server.

The default value of **Source** is **0.0.0.0/0**, indicating that RDS DB instances in the security group can be accessed from any IP address.

For details about the requirements of security group rules, see the **Adding a Security Group Rule** section in the *Virtual Private Cloud User Guide*.

Procedure

Step 1 Log in to the management console.

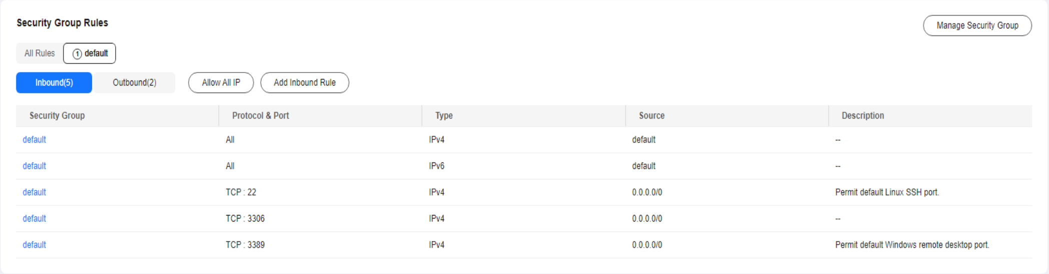
Step 2 Click 📍 in the upper left corner and select a region and a project.

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

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

Step 5 In the navigation pane, choose **Connectivity & Security**. In the **Security Group Rules** area, click the security group name to view the security group rules.

Figure 1-39 Security group rules



Security Group Rules

Security Group	Protocol & Port	Type	Source	Description
default	All	IPv4	default	--
default	All	IPv6	default	--
default	TCP : 22	IPv4	0.0.0.0/0	Permit default Linux SSH port.
default	TCP : 3306	IPv4	0.0.0.0/0	--
default	TCP : 3389	IPv4	0.0.0.0/0	Permit default Windows remote desktop port.

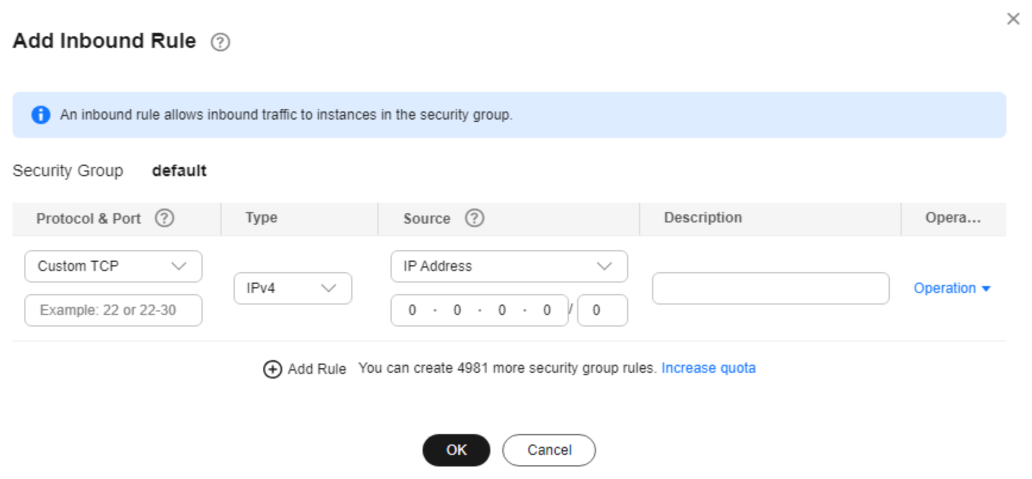
Step 6 Click **Add Inbound Rule** or **Allow All IP** to configure security group rules.

To add more inbound rules, click ⊕.

NOTE

Allow All IP allows all IP addresses to access RDS DB instances in the security group, which poses high security risks. Exercise caution when performing this operation.

Figure 1-40 Adding an inbound rule



Add Inbound Rule ⓘ

An inbound rule allows inbound traffic to instances in the security group.

Security Group default

Protocol & Port	Type	Source	Description	Opera...
Custom TCP Example: 22 or 22-30	IPv4	IP Address 0 · 0 · 0 · 0 / 0		Operation

⊕ Add Rule You can create 4981 more security group rules. Increase quota

Table 1-16 Inbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	**Protocol**: network protocol. Available options: **All ports**, **Custom TCP**, **Custom UDP**, **ICMP**, or **GRE**.	Custom TCP

Parameter	Description	Example Value
	Port: the port over which the traffic can reach your DB instance. RDS for MySQL instances can use database ports 1024 to 65535, excluding 12017 and 33071, which are reserved for RDS system use.	3306
Type	IP address type. ● IPv4 ● IPv6	IPv4
Source	Source address. It can be a single IP address, an IP address group, or a security group to allow access from them to your DB instance. Examples: ● Single IP address: 192.168.10.10/32 (IPv4); 2002:50::44/128 (IPv6) ● All IP addresses: 0.0.0.0/0 (IPv4); ::/0 (IPv6) ● IP address range: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Security group: default_securitygroup	0.0.0.0/0
Description	Supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (<) or (>).	N/A

----End

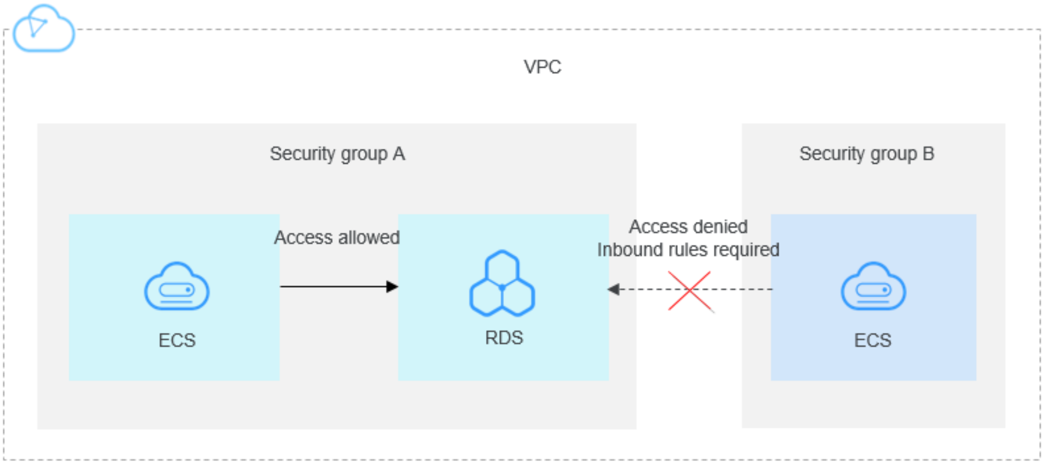
1.4 Example: Buy and Connect to an RDS for MySQL DB Instance

This example illustrates how to purchase an RDS for MySQL instance and connect to it from a Linux ECS over a private network.

- **Step 1: Create an RDS for MySQL DB Instance**

- Step 2: Create an ECS
- Step 3: Connect to the RDS for MySQL DB Instance

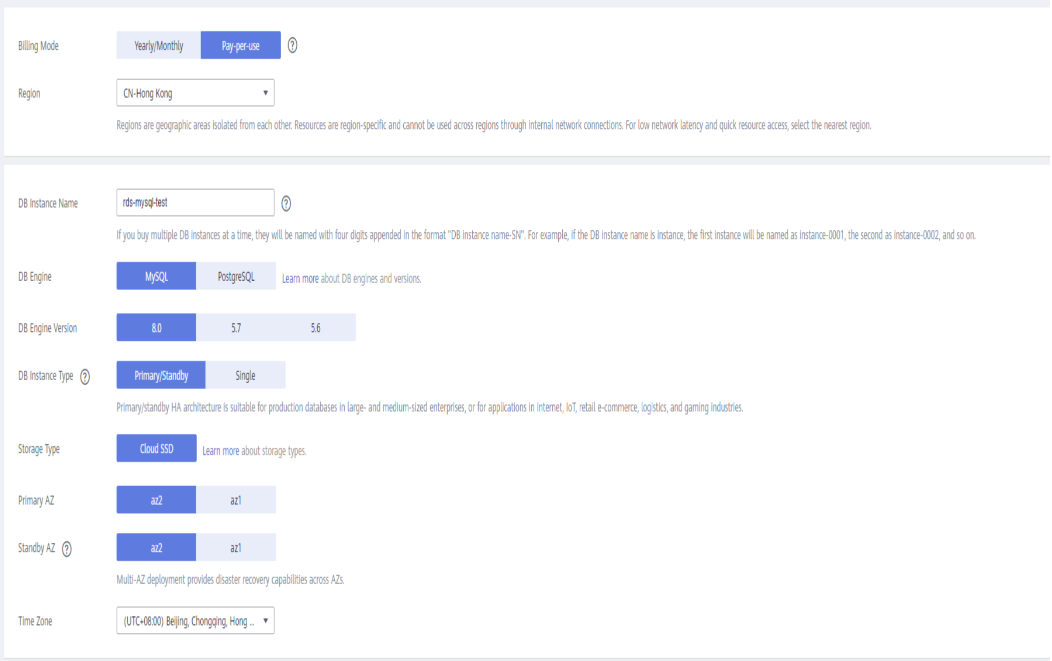
Figure 1-41 Example diagram



Step 1: Create an RDS for MySQL DB Instance

1. Go to the **Buy DB Instance** page.
2. Configure the instance information and click **Next**. Keep the region, AZ, VPC, and security group of the DB instance the same as those of the ECS.

Figure 1-42 Selecting an engine version



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

Region: CN-Hong Kong

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

DB Instance Name: rds-mysql-test

If you buy multiple DB instances at a time, they will be named with four digits appended in the format "DB instance name-SN". For example, if the DB instance name is instance, the first instance will be named as instance-0001, the second as instance-0002, and so on.

DB Engine: [✓ MySQL] PostgreSQL Learn more about DB engines and versions.

DB Engine Version: [✓ 8.0] 5.7 5.6

DB Instance Type: [✓ Primary/Standby] Single

Primary/standby HA architecture is suitable for production databases in large- and medium-sized enterprises, or for applications in Internet, IoT, retail e-commerce, logistics, and gaming industries.

Storage Type: [✓ Cloud SSD] Learn more about storage types.

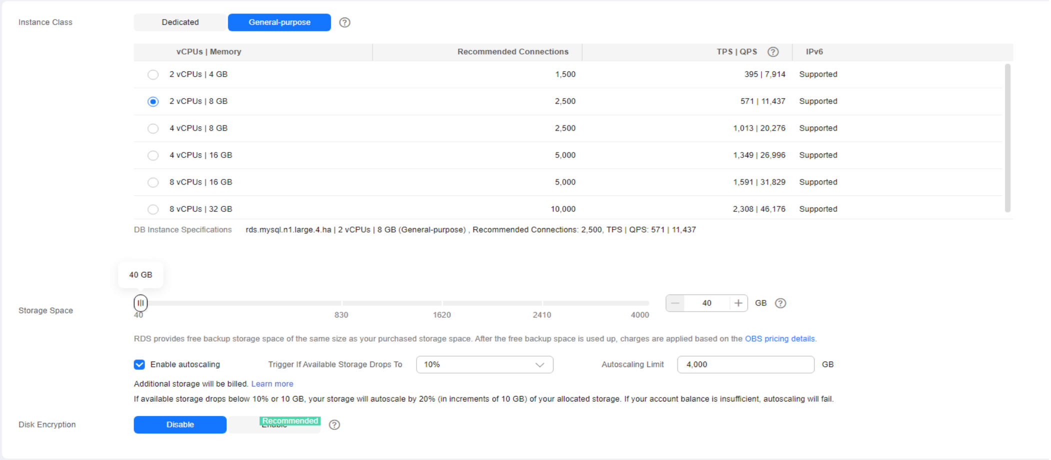
Primary AZ: [✓ az2] az1

Standby AZ: [✓ az2] az1

Multi-AZ deployment provides disaster recovery capabilities across AZs.

Time Zone: (UTC+08:00) Beijing, Chongqing, Hong ...

Figure 1-43 Selecting an instance class



Instance Class: Dedicated / General-purpose

	vCPUs | Memory	Recommended Connections	TPS | QPS	IPv6
○	2 vCPUs | 4 GB	1,500	395 | 7,914	Supported
●	2 vCPUs | 8 GB	2,500	571 | 11,437	Supported
○	4 vCPUs | 8 GB	2,500	1,013 | 20,276	Supported
○	4 vCPUs | 16 GB	5,000	1,349 | 26,996	Supported
○	8 vCPUs | 16 GB	5,000	1,591 | 31,829	Supported
○	8 vCPUs | 32 GB	10,000	2,308 | 46,176	Supported

DB Instance Specifications: rds.mysql.n1.large.4.ha | 2 vCPUs | 8 GB (General-purpose) , Recommended Connections: 2,500, TPS | QPS: 571 | 11,437

Storage Space: 40 GB

40 GB

RDS provides free backup storage space of the same size as your purchased storage space. After the free backup space is used up, charges are applied based on the OBS pricing details.

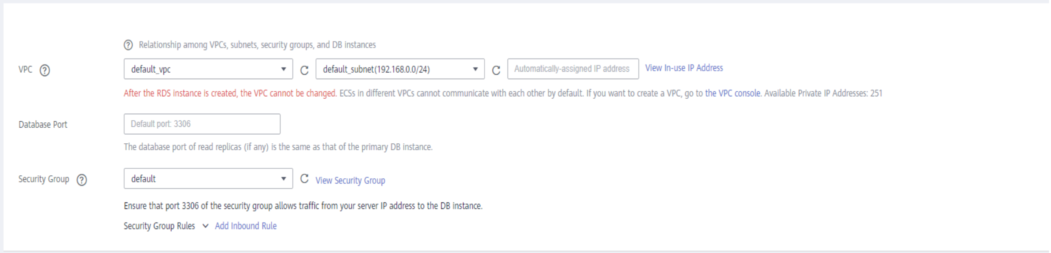
☑ Enable autoscaling Trigger If Available Storage Drops To: 10% Autoscaling Limit: 4,000 GB

Additional storage will be billed. Learn more

If available storage drops below 10% or 10 GB, your storage will autoscale by 20% (in increments of 10 GB) of your allocated storage. If your account balance is insufficient, autoscaling will fail.

Disk Encryption: Disable / Enable Recommended

Figure 1-44 Configuring network information



Relationship among VPCs, subnets, security groups, and DB instances

VPC: default_vpc default_subnet(192.168.0.0/24) Automatically-assigned IP address View In-use IP Address

After the RDS instance is created, the VPC cannot be changed. ECSs in different VPCs cannot communicate with each other by default. If you want to create a VPC, go to the VPC console. Available Private IP Addresses: 251

Database Port: Default port: 3306

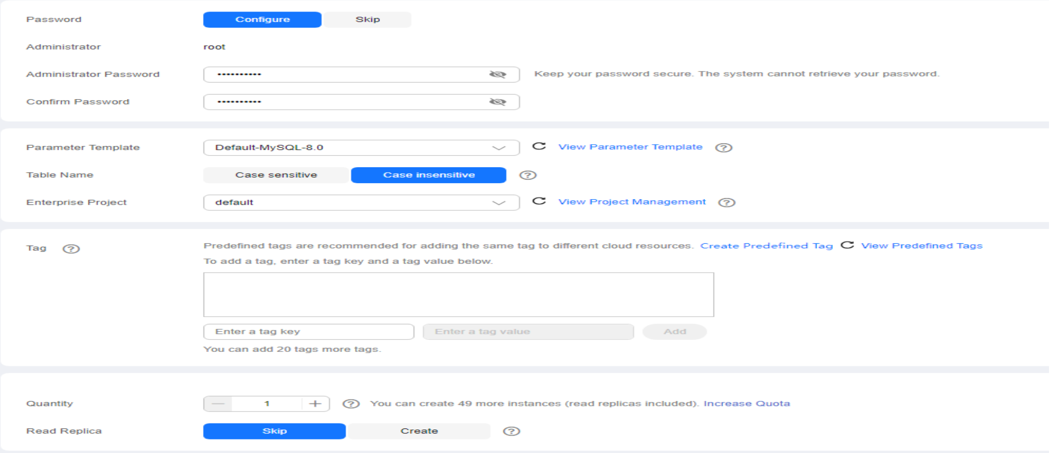
The database port of read replicas (if any) is the same as that of the primary DB instance.

Security Group: default View Security Group

Ensure that port 3306 of the security group allows traffic from your server IP address to the DB instance.

Security Group Rules Add Inbound Rule

Figure 1-45 Setting a password



Password: Configure / Skip

Administrator: root

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

Confirm Password: ••••••••••

Parameter Template: Default-MySQL-8.0 View Parameter Template

Table Name: Case sensitive / Case insensitive

Enterprise Project: default View Project Management

Tag: Predefined tags are recommended for adding the same tag to different cloud resources. Create Predefined Tag View Predefined Tags

To add a tag, enter a tag key and a tag value below.

Enter a tag key Enter a tag value Add

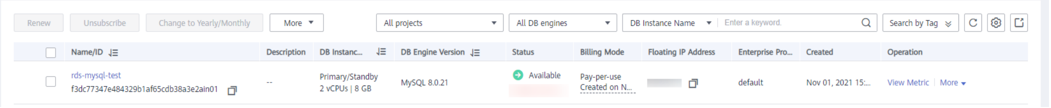
You can add 20 tags more tags.

Quantity: 1 You can create 49 more instances (read replicas included). Increase Quota

Read Replica: Skip / Create

3. View the purchased RDS instance.

Figure 1-46 Instance successfully purchased

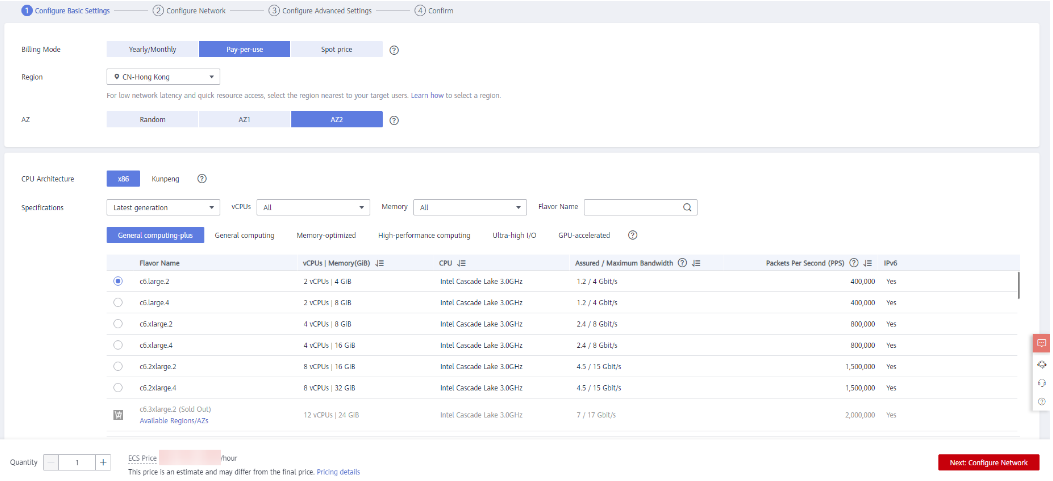


	Name/ID	Description	DB Instanc...	DB Engine Version	Status	Billing Mode	Floating IP Address	Enterprise Pro...	Created	Operation
□	rds-mysql-test f3dc77347e484329b1af65cdb38a3e2ain01	--	Primary/Standby 2 vCPUs | 8 GB	MySQL 8.0.21	Available	Pay-per-use Created on N...	[redacted]	default	Nov 01, 2021 15:...	View Metric More

Step 2: Create an ECS

1. Go to the **Buy ECS** page.
2. Configure basic settings and click **Next: Configure Network**. Keep the region and AZ of the ECS the same as those of the RDS for MySQL instance to be connected.

Figure 1-47 Basic configurations



Billing Mode: Pay-per-use

Region: CN-Hong Kong

For low network latency and quick resource access, select the region nearest to your target users. Learn how to select a region.

AZ: AZ2

CPU Architecture: x86

Specifications: Latest generation | vCPUs: All | Memory: All | Flavor Name:

General computing-plus

	Flavor Name	vCPUs | Memory(GiB)	CPU	Assured / Maximum Bandwidth	Packets Per Second (PPS)	IPv6
●	c6.large.2	2 vCPUs | 4 GiB	Intel Cascade Lake 3.0GHz	1.2 / 4 Gbit/s	400,000	Yes
○	c6.large.4	2 vCPUs | 8 GiB	Intel Cascade Lake 3.0GHz	1.2 / 4 Gbit/s	400,000	Yes
○	c6.xlarge.2	4 vCPUs | 8 GiB	Intel Cascade Lake 3.0GHz	2.4 / 8 Gbit/s	800,000	Yes
○	c6.xlarge.4	4 vCPUs | 16 GiB	Intel Cascade Lake 3.0GHz	2.4 / 8 Gbit/s	800,000	Yes
○	c6.2xlarge.2	8 vCPUs | 16 GiB	Intel Cascade Lake 3.0GHz	4.5 / 15 Gbit/s	1,500,000	Yes
○	c6.2xlarge.4	8 vCPUs | 32 GiB	Intel Cascade Lake 3.0GHz	4.5 / 15 Gbit/s	1,500,000	Yes
	c6.3xlarge.2 (Sold Out) Available Regions/AZs	12 vCPUs | 24 GiB	Intel Cascade Lake 3.0GHz	7 / 17 Gbit/s	2,000,000	Yes

Quantity: 1

ECS Price [redacted]/hour

This price is an estimate and may differ from the final price. Pricing details

Figure 1-48 Selecting an image

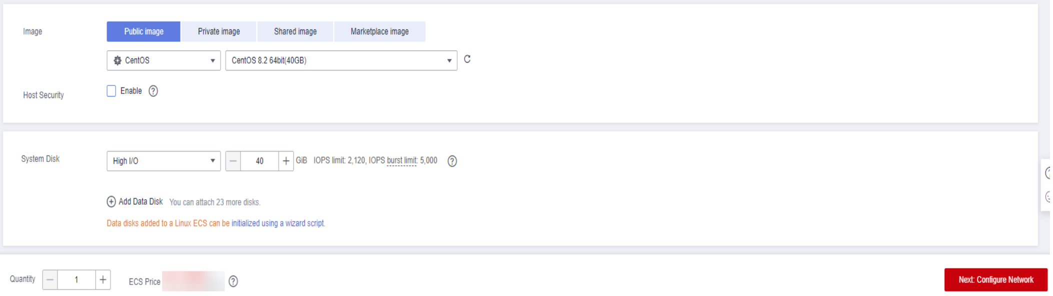


Image: Public image | CentOS | CentOS 8.2 64bit(40GB)

Host Security: □ Enable

System Disk: High I/O | 40 GiB IOPS limit: 2,120, IOPS burst limit: 5,000

You can attach 23 more disks.

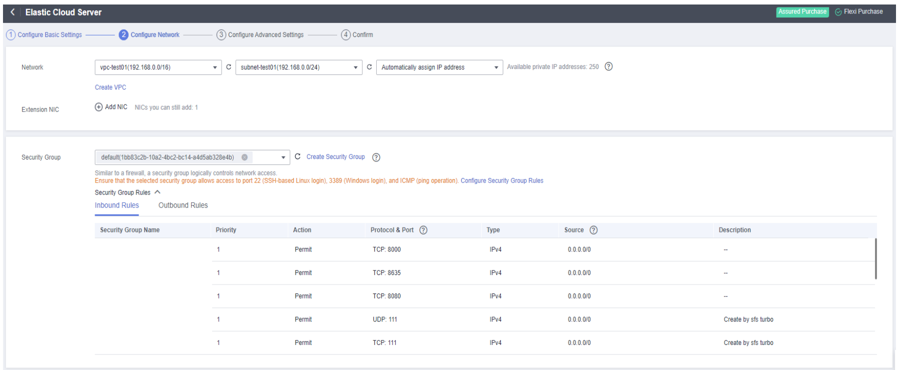
Data disks added to a Linux ECS can be initialized using a wizard script.

Quantity: 1

ECS Price [redacted]

3. Configure the ECS network information and click **Next: Configure Advanced Settings**. Keep the VPC and security group of the ECS the same as those of the RDS for MySQL instance to be connected.

Figure 1-49 Network settings



Network: vpc-test01(192.168.0.0/16) | subnet-test01(192.168.0.0/24) | Automatically assign IP address | Available private IP addresses: 250

Extension NIC: NICs you can still add: 1

Security Group: default(1bb83c2b-10a2-4bc2-bc14-a4d5ab328e4b)

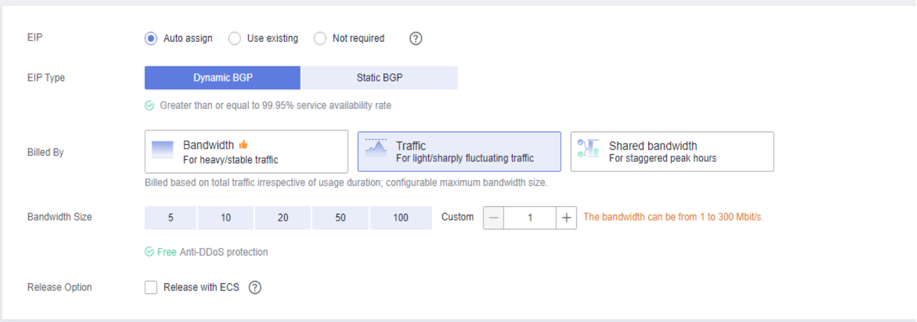
Similar to a firewall, a security group logically controls network access.
Ensure that the selected security group allows access to port 22 (SSH-based Linux login), 3389 (Windows login), and ICMP (ping operation). Configure Security Group Rules

Security Group Rules

Inbound Rules

Security Group Name	Priority	Action	Protocol & Port	Type	Source	Description
	1	Permit	TCP: 8000	IPv4	0.0.0.0/0	--
	1	Permit	TCP: 8635	IPv4	0.0.0.0/0	--
	1	Permit	TCP: 8080	IPv4	0.0.0.0/0	--
	1	Permit	UDP: 111	IPv4	0.0.0.0/0	Create by sfs turbo
	1	Permit	TCP: 111	IPv4	0.0.0.0/0	Create by sfs turbo

Figure 1-50 Selecting an EIP



EIP ● Auto assign ○ Use existing ○ Not required

EIP Type: Dynamic BGP | Static BGP

Greater than or equal to 99.95% service availability rate

Billed By: Bandwidth For heavy/stable traffic | Traffic For light/sharply fluctuating traffic | Shared bandwidth For staggered peak hours

Billed based on total traffic irrespective of usage duration; configurable maximum bandwidth size.

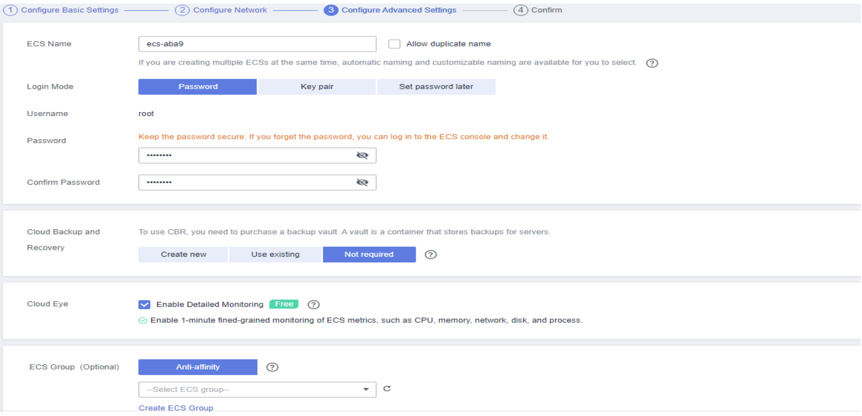
Bandwidth Size: 5 | 10 | 20 | 50 | 100 | Custom – 1 + The bandwidth can be from 1 to 300 Mbit/s.

Free Anti-DDoS protection

Release Option: □ Release with ECS

4. Configure the ECS password and click **Next: Confirm**.

Figure 1-51 Advanced settings



1 Configure Basic Settings — 2 Configure Network — 3 Configure Advanced Settings — 4 Confirm

ECS Name: ecs-aba9 □ Allow duplicate name

If you are creating multiple ECSs at the same time, automatic naming and customizable naming are available for you to select.

Login Mode: Password | Key pair | Set password later

Username: root

Password: Keep the password secure. If you forget the password, you can log in to the ECS console and change it.

•••••••••

Confirm Password: •••••••••

Cloud Backup and Recovery: To use CBR, you need to purchase a backup vault. A vault is a container that stores backups for servers.

Create new | Use existing | Not required

Cloud Eye: ☑ Enable Detailed Monitoring Free

Enable 1-minute fined-grained monitoring of ECS metrics, such as CPU, memory, network, disk, and process.

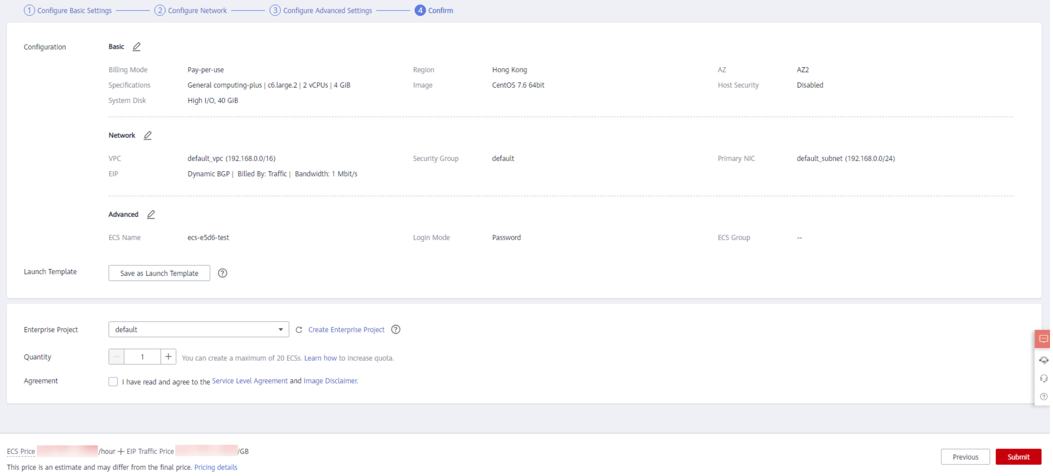
ECS Group (Optional): Anti-affinity

--Select ECS group--

Create ECS Group

5. Confirm the configurations and click **Submit**.

Figure 1-52 Confirming the configurations



1 Configure Basic Settings — 2 Configure Network — 3 Configure Advanced Settings — 4 Confirm

Configuration

Basic

Billing Mode: Pay-per-use | Region: Hong Kong | AZ: AZ2

Specifications: General computing-plus \| c6.large.2 \| 2 vCPUs \| 4 GiB | Image: CentOS 7.6 64bit | Host Security: Disabled

System Disk: High I/O, 40 GiB

Network

VPC: default_vpc (192.168.0.0/16) | Security Group: default | Primary NIC: default_subnet (192.168.0.0/24)

EIP: Dynamic BGP | Billed By: Traffic | Bandwidth: 1 Mbit/s

Advanced

ECS Name: ecs-e5d6-test | Login Mode: Password | ECS Group: --

Launch Template: Save as Launch Template

Enterprise Project: default Create Enterprise Project

Quantity: – 1 + You can create a maximum of 20 ECSs. Learn how to increase quota.

Agreement: □ I have read and agree to the Service Level Agreement and Image Disclaimer.

ECS Price [redacted]/hour + EIP Traffic Price [redacted]/GB

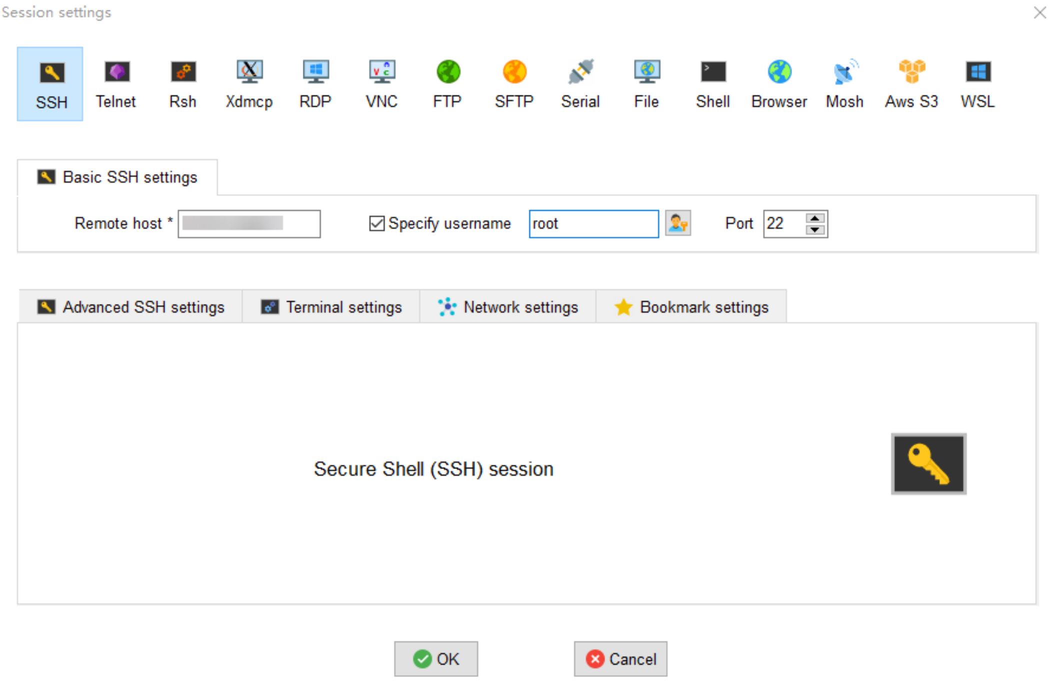
This price is an estimate and may differ from the final price. Pricing details

6. View the purchased ECS.

Step 3: Connect to the RDS for MySQL DB Instance

1. Use a Linux remote connection tool (for example, MobaXterm) to log in to the ECS. Enter the EIP bound to the ECS for **Remote host**.

Figure 1-53 Creating a session



Remote host * [redacted]

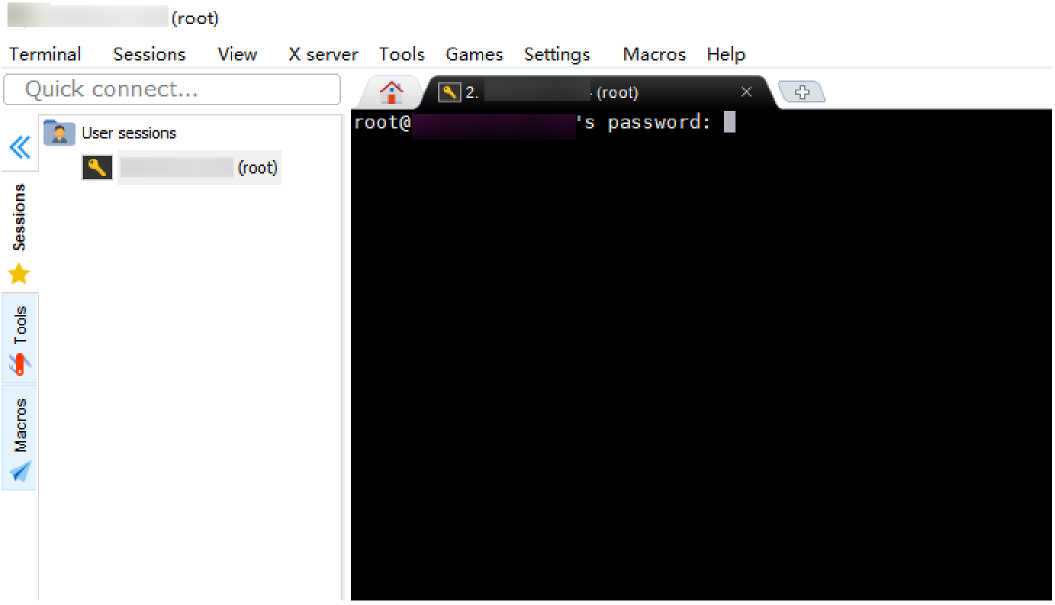
☑ Specify username root

Port 22

Secure Shell (SSH) session

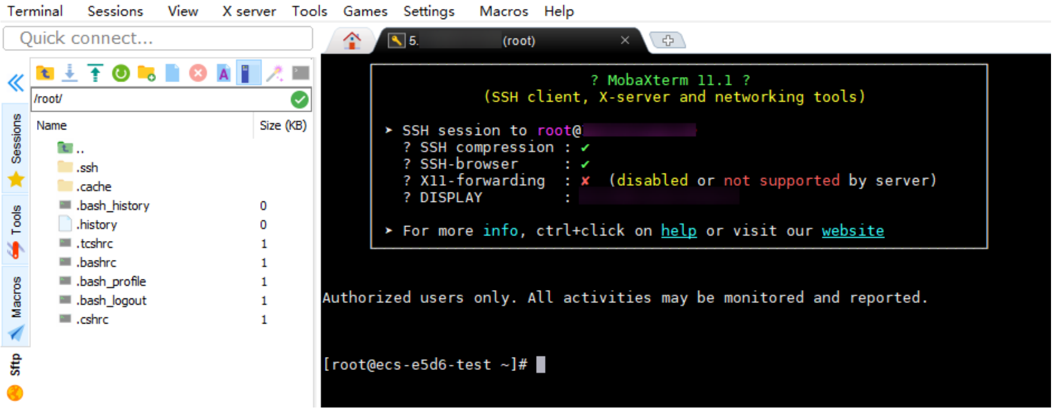
2. Enter the password of the ECS.

Figure 1-54 Entering the password



```
root@[redacted]'s password: 
```

Figure 1-55 Successful login

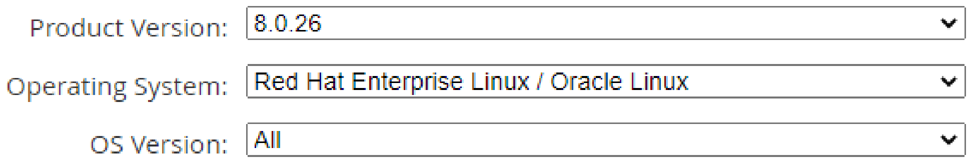


Name	Size (KB)
..	
.ssh	
.cache	
.bash_history	0
.history	0
.tcshrc	1
.bashrc	1
.bash_profile	1
.bash_logout	1
.cshrc	1

```
                         ? MobaXterm 11.1 ?
            (SSH client, X-server and networking tools)

 ➤ SSH session to root@[redacted]
   ? SSH compression : ✔
   ? SSH-browser     : ✔
   ? X11-forwarding  : ✘  (disabled or not supported by server)
   ? DISPLAY         : [redacted]

 ➤ For more info, ctrl+click on help or visit our website

Authorized users only. All activities may be monitored and reported.

[root@ecs-e5d6-test ~]#
```

3. Download the **mysql-community-client-8.0.26-1.el6.x86_64.rpm** client installation package by selecting the required product version and operating system.

Figure 1-56 Selecting a version

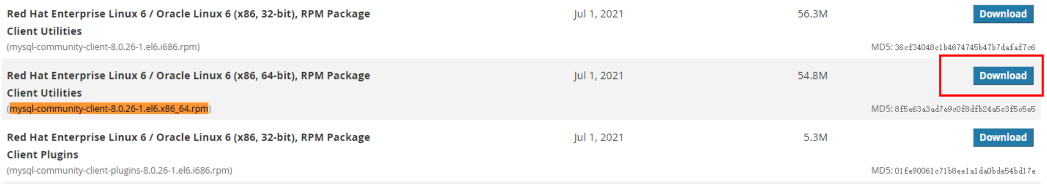


Product Version: 8.0.26

Operating System: Red Hat Enterprise Linux / Oracle Linux

OS Version: All

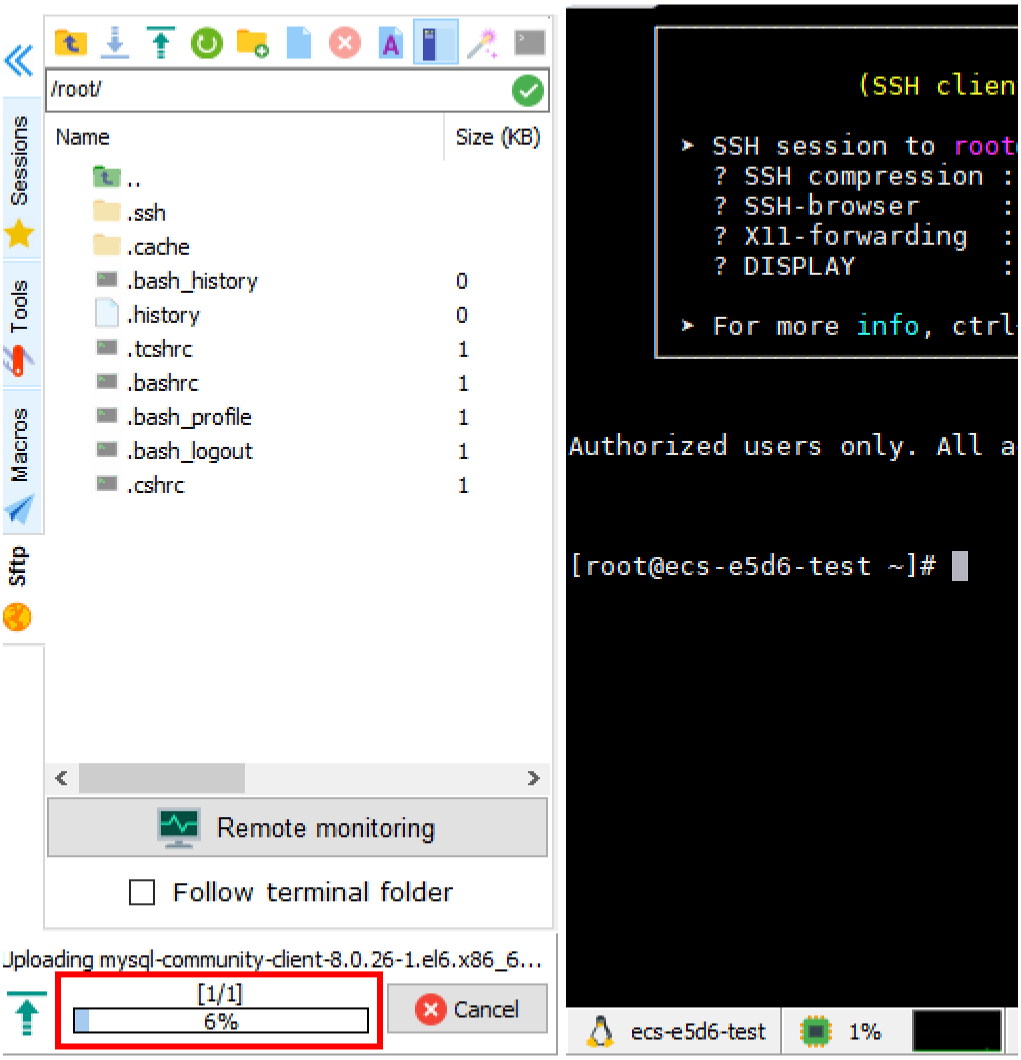
Figure 1-57 Downloading the client package



Red Hat Enterprise Linux 6 / Oracle Linux 6 (x86, 32-bit), RPM Package **Client Utilities** (mysql-community-client-8.0.26-1.el6.i686.rpm)	Jul 1, 2021	56.3M	Download MD5: 36cf34048c1b4674745b47b7dafaf7c6
Red Hat Enterprise Linux 6 / Oracle Linux 6 (x86, 64-bit), RPM Package **Client Utilities** (mysql-community-client-8.0.26-1.el6.x86_64.rpm)	Jul 1, 2021	54.8M	Download MD5: 8f5e63a3ad7e9c0f8dfb24a5c3f5c5e5
Red Hat Enterprise Linux 6 / Oracle Linux 6 (x86, 32-bit), RPM Package **Client Plugins** (mysql-community-client-plugins-8.0.26-1.el6.i686.rpm)	Jul 1, 2021	5.3M	Download MD5: 01fe90061c71b8ee1a1da0bde54bd17e

4. Upload the client installation package to the ECS.

Figure 1-58 Uploading the client package



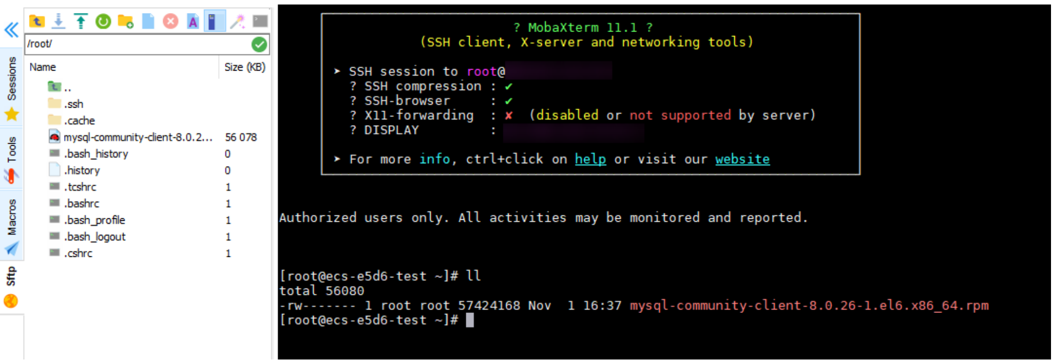
/root/

Name	Size (KB)
..	
.ssh	
.cache	
.bash_history	0
.history	0
.tcshrc	1
.bashrc	1
.bash_profile	1
.bash_logout	1
.cshrc	1

Uploading mysql-community-client-8.0.26-1.el6.x86_6...
[1/1]
6%

```
(SSH clien
➤ SSH session to root
  ? SSH compression :
  ? SSH-browser     :
  ? X11-forwarding  :
  ? DISPLAY         :

➤ For more info, ctrl

Authorized users only. All a

[root@ecs-e5d6-test ~]# 
```

Figure 1-59 Package uploaded



/root/

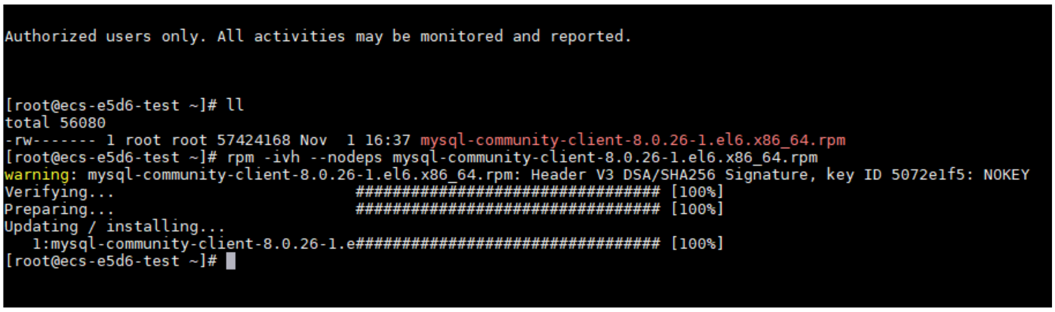
Name	Size (KB)
..	
.ssh	
.cache	
mysql-community-client-8.0.2...	56 078
.bash_history	0
.history	0
.tcshrc	1
.bashrc	1
.bash_profile	1
.bash_logout	1
.cshrc	1

```
                    ? MobaXterm 11.1 ?
            (SSH client, X-server and networking tools)

 ➤ SSH session to root@[redacted]
   ? SSH compression : ✓
   ? SSH-browser     : ✓
   ? X11-forwarding  : ✗  (disabled or not supported by server)
   ? DISPLAY         : [redacted]

 ➤ For more info, ctrl+click on help or visit our website


Authorized users only. All activities may be monitored and reported.


[root@ecs-e5d6-test ~]# ll
total 56080
-rw------- 1 root root 57424168 Nov  1 16:37 mysql-community-client-8.0.26-1.el6.x86_64.rpm
[root@ecs-e5d6-test ~]# 
```

5. Install the client.

```
rpm -ivh --nodeps mysql-community-client-8.0.26-1.el6.x86_64.rpm
```

Figure 1-60 Installing the client

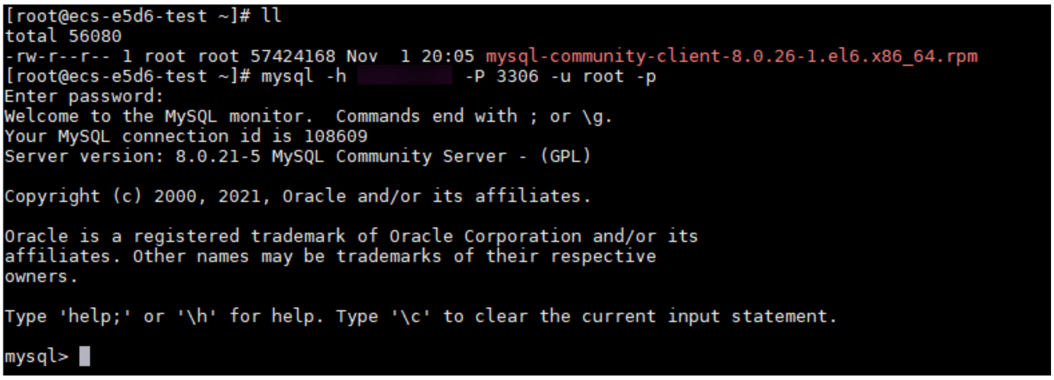


```
Authorized users only. All activities may be monitored and reported.


[root@ecs-e5d6-test ~]# ll
total 56080
-rw------- 1 root root 57424168 Nov  1 16:37 mysql-community-client-8.0.26-1.el6.x86_64.rpm
[root@ecs-e5d6-test ~]# rpm -ivh --nodeps mysql-community-client-8.0.26-1.el6.x86_64.rpm
warning: mysql-community-client-8.0.26-1.el6.x86_64.rpm: Header V3 DSA/SHA256 Signature, key ID 5072e1f5: NOKEY
Verifying...                          ################################# [100%]
Preparing...                          ################################# [100%]
Updating / installing...
   1:mysql-community-client-8.0.26-1.e################################# [100%]
[root@ecs-e5d6-test ~]# 
```

6. Connect to the RDS for MySQL instance.

```
mysql -h 192.168.6.198 -P 3306 -u root -p
```

Figure 1-61 Connection successful

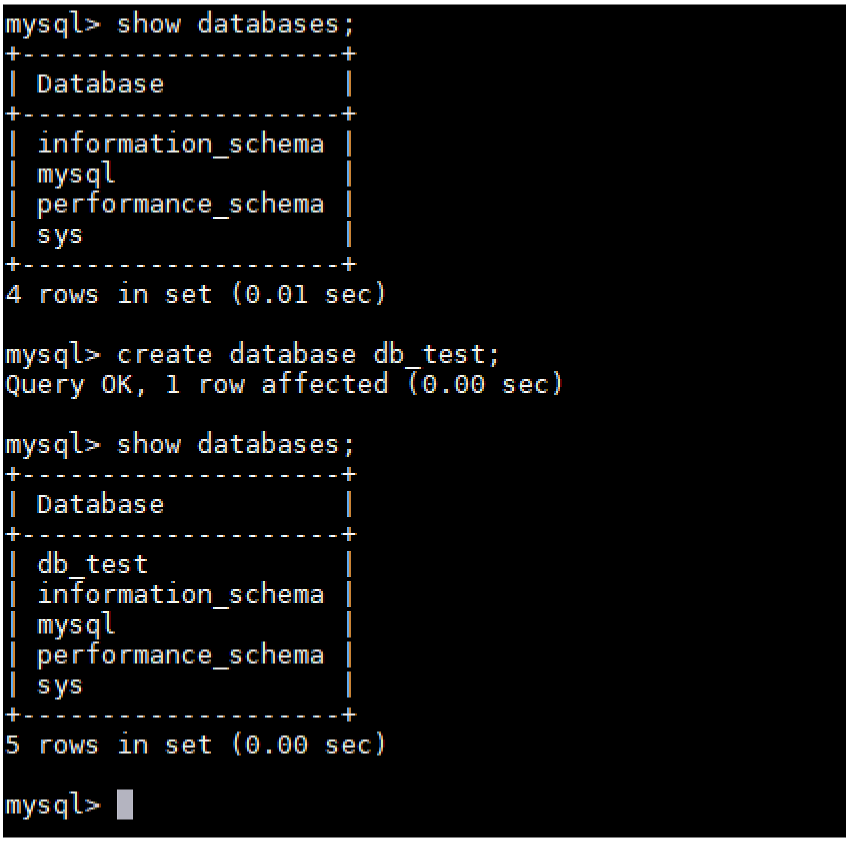


```
[root@ecs-e5d6-test ~]# ll
total 56080
-rw-r--r-- 1 root root 57424168 Nov  1 20:05 mysql-community-client-8.0.26-1.el6.x86_64.rpm
[root@ecs-e5d6-test ~]# mysql -h [redacted] -P 3306 -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 108609
Server version: 8.0.21-5 MySQL Community Server - (GPL)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```

7. Create a database, for example, **db_test**.

```
create database db_test;
```

Figure 1-62 Creating a database

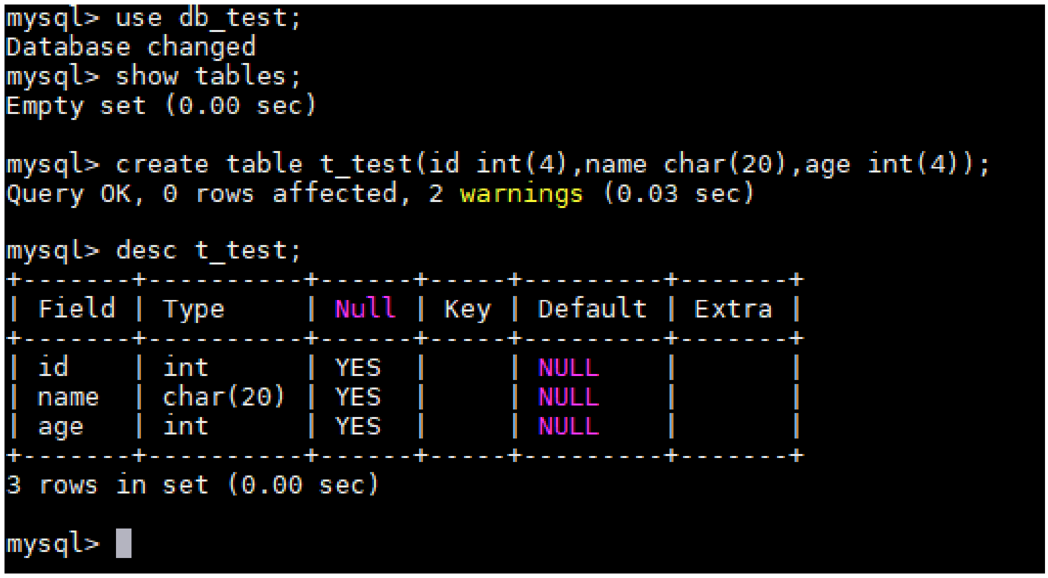


```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
4 rows in set (0.01 sec)

mysql> create database db_test;
Query OK, 1 row affected (0.00 sec)

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| db_test            |
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.00 sec)

mysql>
```

8. Create a table, for example, **t_test**.

```
create table t_test(id int(4), name char(20), age int(4));
```

Figure 1-63 Creating a table

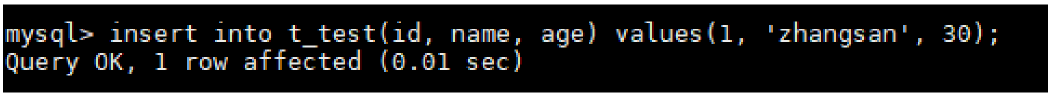


```
mysql> use db_test;
Database changed
mysql> show tables;
Empty set (0.00 sec)

mysql> create table t_test(id int(4),name char(20),age int(4));
Query OK, 0 rows affected, 2 warnings (0.03 sec)

mysql> desc t_test;
+-------+----------+------+-----+---------+-------+
| Field | Type     | Null | Key | Default | Extra |
+-------+----------+------+-----+---------+-------+
| id    | int      | YES  |     | NULL    |       |
| name  | char(20) | YES  |     | NULL    |       |
| age   | int      | YES  |     | NULL    |       |
+-------+----------+------+-----+---------+-------+
3 rows in set (0.00 sec)

mysql>
```

9. Insert one data record to the table.

```
insert into t_test(id, name, age) values(1, 'zhangsan', 30);
```

Figure 1-64 Inserting data

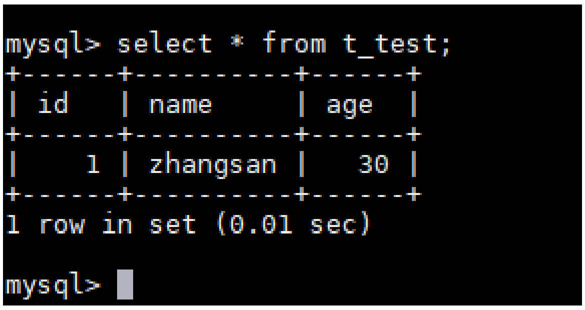


```
mysql> insert into t_test(id, name, age) values(1, 'zhangsan', 30);
Query OK, 1 row affected (0.01 sec)
```

10. Query table data.

```
select * from t_test;
```

Figure 1-65 Querying data

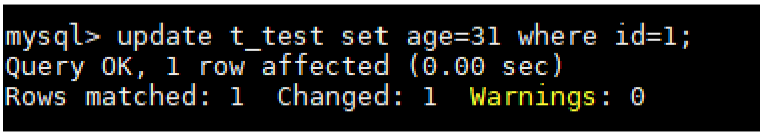


```
mysql> select * from t_test;
+------+----------+------+
| id   | name     | age  |
+------+----------+------+
|    1 | zhangsan |   30 |
+------+----------+------+
1 row in set (0.01 sec)

mysql>
```

11. Update the value of **age** for the data record whose **id** is **1** in the table.

```
update t_test set age=31 where id=1;
```

Figure 1-66 Updating data

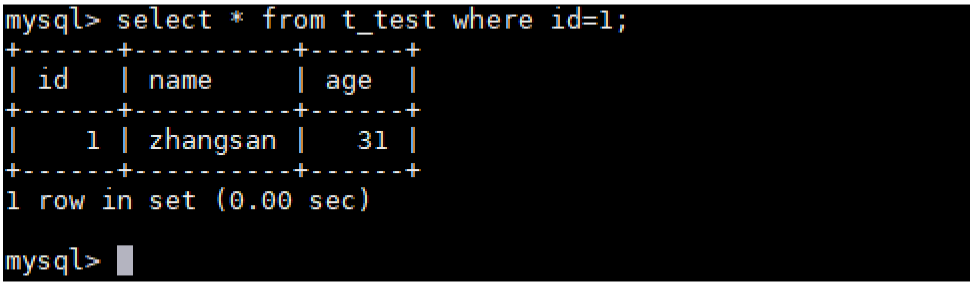


```
mysql> update t_test set age=31 where id=1;
Query OK, 1 row affected (0.00 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

12. Query the updated table data.

```
select * from t_test where id=1;
```

Figure 1-67 Querying updated data

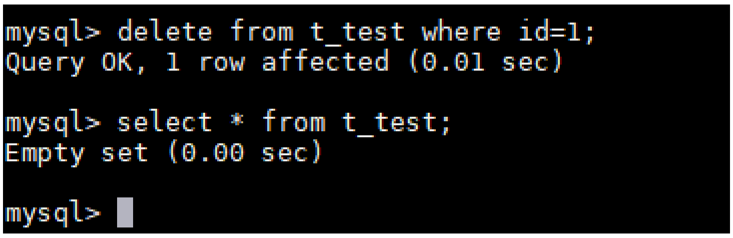


```
mysql> select * from t_test where id=1;
+------+----------+------+
| id   | name     | age  |
+------+----------+------+
|    1 | zhangsan |   31 |
+------+----------+------+
1 row in set (0.00 sec)

mysql>
```

13. Delete the data record whose **id** is **1** from the table.

```
delete from t_test where id=1;
```

Figure 1-68 Deleting table data

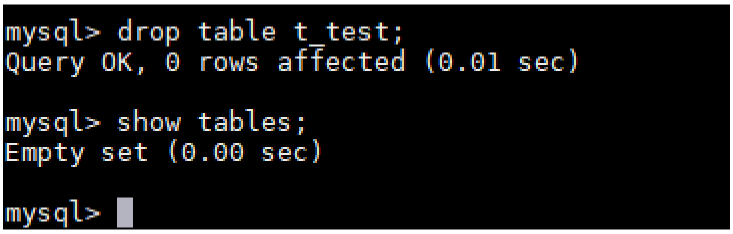


```
mysql> delete from t_test where id=1;
Query OK, 1 row affected (0.01 sec)

mysql> select * from t_test;
Empty set (0.00 sec)

mysql>
```

14. Delete the table structure.

```
drop table t_test;
```

Figure 1-69 Deleting table structure

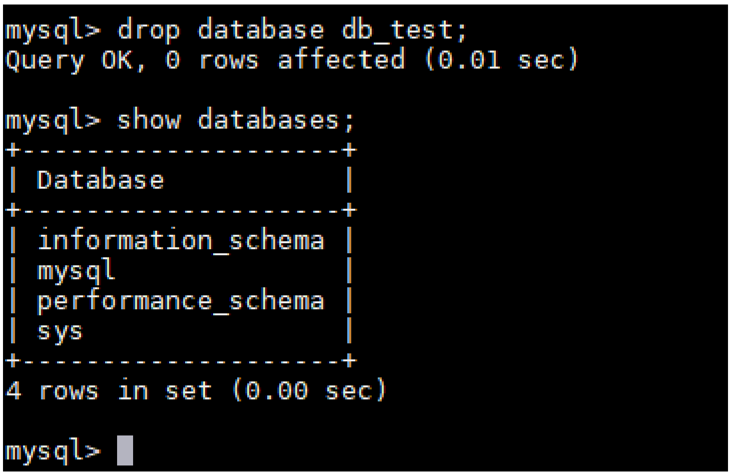


```
mysql> drop table t_test;
Query OK, 0 rows affected (0.01 sec)

mysql> show tables;
Empty set (0.00 sec)

mysql> 
```

15. Delete the database.

```
drop database db_test;
```

Figure 1-70 Deleting a database



```
mysql> drop database db_test;
Query OK, 0 rows affected (0.01 sec)

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
4 rows in set (0.00 sec)

mysql> 
```

2 Getting Started with RDS for MariaDB

2.1 Step 1: Set Up for RDS

You can buy and connect to DB instances on the RDS console.

Registering a HUAWEI ID

If you already have a HUAWEI ID, skip this part. If you do not have a HUAWEI ID yet, perform the following steps to create one:

Step 1 Open the **Huawei Cloud website**.

Step 2 Click **Register** and complete the registration as instructed.

After the registration is successful, the system redirects you to your personal information page.

----End

Topping Up Your Account

- For details about RDS for MariaDB prices, see **Price Calculator**.
- Before purchasing an RDS for MariaDB instance, ensure that your account balance is sufficient. For details about how to top up an account, see **Topping Up an Account**.

Creating an IAM User and Granting Permissions

You can create an IAM user or user group on the Identity and Access Management (IAM) console and grant it specific operation permissions for fine-grained permissions management.

1. **Create a user group and assign permissions** to it.

   Create a user group on the IAM console, and attach the **RDS ReadOnlyAccess** policy to the group.

NOTE

To use some interconnected services, you also need to configure permissions of such services.

For example, to connect to your DB instance through the console, configure the **DAS FullAccess** permission of Data Admin Service (DAS) besides **RDS ReadOnlyAccess**.

2. **Create an IAM user and add it to the user group**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the RDS console by using the created user, and verify that the user only has read permissions for RDS.

   – Choose **Service List** > **Relational Database Service** and click **Buy DB Instance**. If a message appears indicating that you have insufficient permissions to perform the operation, the **RDS ReadOnlyAccess** policy has already been applied.

   – Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **RDS ReadOnlyAccess** policy has already taken effect.

2.2 Step 2: Buy a DB Instance

Scenarios

This section describes how to buy a DB instance on the RDS console.

RDS for MariaDB only supports the pay-per-use billing mode. RDS allows you to tailor your compute resources and storage space to your business needs.

Prerequisites

Your account balance is greater than or equal to $0 USD.

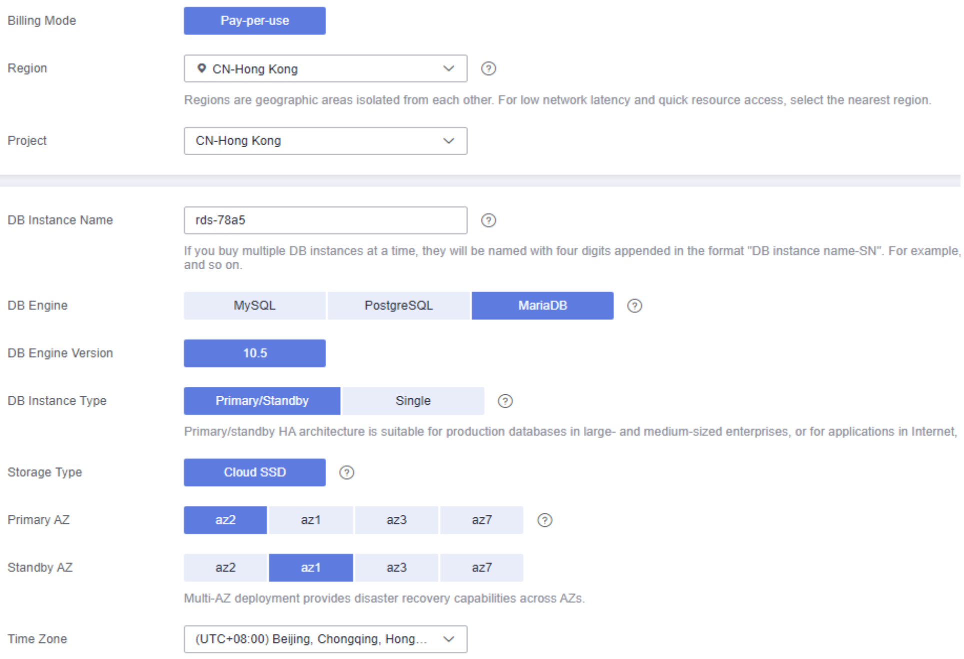
Procedure

Step 1 Go to the **Buy DB Instance** page.

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

- Basic information

Figure 2-1 Basic information



Billing Mode: Pay-per-use

Region: CN-Hong Kong

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

Project: CN-Hong Kong

DB Instance Name: rds-78a5

If you buy multiple DB instances at a time, they will be named with four digits appended in the format "DB instance name-SN". For example, and so on.

DB Engine: MySQL | PostgreSQL | [✓ MariaDB]

DB Engine Version: 10.5

DB Instance Type: [✓ Primary/Standby] | Single

Primary/standby HA architecture is suitable for production databases in large- and medium-sized enterprises, or for applications in Internet,

Storage Type: Cloud SSD

Primary AZ: [✓ az2] | az1 | az3 | az7

Standby AZ: az2 | [✓ az1] | az3 | az7

Multi-AZ deployment provides disaster recovery capabilities across AZs.

Time Zone: (UTC+08:00) Beijing, Chongqing, Hong...

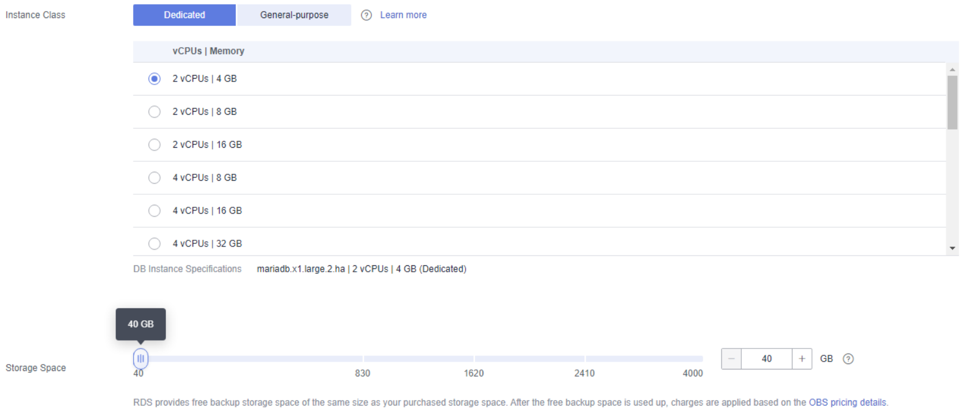
Table 2-1 Basic information

Parameter	Description
Billing Mode	Select **Pay-per-use**.
Region	Region where your resources are located. **NOTE** Products in different regions cannot communicate with each other through a private network. After a DB instance is created, the region cannot be changed. Therefore, exercise caution when selecting a region.
Project	The project corresponds to the region. Different regions correspond to different projects.
DB Instance Name	Must start with a letter and consist of 4 to 64 characters. Only letters (case-sensitive), digits, hyphens (-), and underscores (_) are allowed. – If you intend to buy multiple DB instances at a time, the allowed length for each instance name will change. – If you buy multiple DB instances at a time, they will be named *instance-0001*, *instance-0002*, and so on. (*instance* indicates the DB instance name you specify.)
DB Engine	MariaDB
DB Engine Version	For details, see **DB Engines and Versions**. The DB engine version differs in different regions.

Parameter	Description
DB Instance Type	– **Primary/Standby**: uses an HA architecture with a primary DB instance and a synchronous standby DB instance. It is suitable for production databases of large- and medium-sized enterprises in Internet, Internet of Things (IoT), retail e-commerce sales, logistics, gaming, and other sectors. The standby DB instance improves instance reliability and is invisible to you after being created. – **Single**: uses a single-node architecture, which is more cost-effective than primary/standby DB instances. It is only recommended for development and testing of microsites, and small and medium enterprises, or for learning about RDS.
AZ	An AZ is a physical region where resources use independent power supply and networks. AZs are physically isolated but interconnected through an internal network. Some regions support both single-AZ and multi-AZ deployment and some only support single-AZ deployment. To achieve high reliability, RDS will automatically deploy your primary and standby instances in different physical servers even if you deploy them in the same AZ. You can deploy primary and standby instances in a single AZ or across AZs to achieve failover and high availability.
Storage Type	Determines the DB instance read/write speed. The higher the maximum throughput is, the higher the DB instance read/write speed can be. – **Cloud SSD**: cloud drives used to decouple storage from compute. The maximum throughput is 350 MB/s. – **Extreme SSD**: uses 25GE network and RDMA technologies to provide you with up to 1,000 MB/s throughput per disk and sub-millisecond latency.
Time Zone	You need to select a time zone for your instance based on the region hosting your instance. You can select a time zone during instance creation and change it later as needed.

- Specifications and storage

Figure 2-2 Specifications and storage



Instance Class: Dedicated

vCPUs | Memory

● 2 vCPUs | 4 GB
○ 2 vCPUs | 8 GB
○ 2 vCPUs | 16 GB
○ 4 vCPUs | 8 GB
○ 4 vCPUs | 16 GB
○ 4 vCPUs | 32 GB

DB Instance Specifications mariadb.x1.large.2.ha | 2 vCPUs | 4 GB (Dedicated)

Storage Space 40 GB

40 830 1620 2410 4000

40 GB

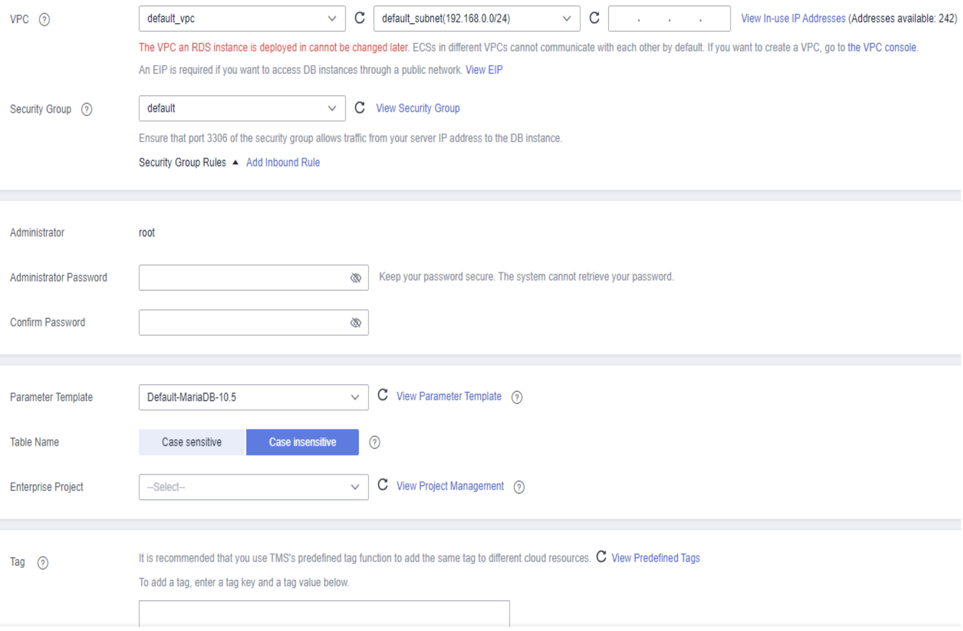
RDS provides free backup storage space of the same size as your purchased storage space. After the free backup space is used up, charges are applied based on the OBS pricing details.

Table 2-2 Specifications and storage

Parameter	Description
Instance Class	Refers to the vCPU and memory of a DB instance. Different instance classes have different numbers of database connections and different maximum IOPS. After a DB instance is created, you can change its vCPU and memory. For details, see **Changing a DB Instance Class**.
Storage Space (GB)	Contains the system overhead required for inodes, reserved blocks, and database operation. Storage space can range in size from 40 GB to 4,000 GB and can be scaled up only by a multiple of 10 GB. After a DB instance is created, you can scale up its storage space. For details, see **Scaling up Storage Space**.

- Network and database configuration

Figure 2-3 Network and database configuration



VPC: default_vpc; default_subnet(192.168.0.0/24)

The VPC an RDS instance is deployed in cannot be changed later. ECSs in different VPCs cannot communicate with each other by default. If you want to create a VPC, go to the VPC console.

An EIP is required if you want to access DB instances through a public network.

Security Group: default

Ensure that port 3306 of the security group allows traffic from your server IP address to the DB instance.

Administrator: root

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

Confirm Password

Parameter Template: Default-MariaDB-10.5

Table Name: Case sensitive | Case insensitive

Enterprise Project: --Select--

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

To add a tag, enter a tag key and a tag value below.

Table 2-3 Network

Parameter	Description
VPC	A virtual network in which your RDS DB instances are located. A VPC can isolate networks for different workloads. You can select an existing VPC or create a VPC. For details about how to create a VPC, see "Creating a VPC" in *Virtual Private Cloud User Guide*. If no VPC is available, RDS allocates a VPC to you by default. **NOTICE** After a DB instance is created, the VPC cannot be changed.
Subnet	Improves network security by providing dedicated network resources that are logically isolated from other networks. Subnets take effect only within an AZ. The Dynamic Host Configuration Protocol (DHCP) function is enabled by default for subnets in which you plan to create RDS DB instances and cannot be disabled. A floating IP address is automatically assigned when you create a DB instance. You can also enter an unused IPv4 floating IP address in the subnet CIDR block.
Security Group	Enhances security by controlling access to RDS from other services. A network **access control list (ACL)** can help control inbound and outbound traffic of subnets in your VPC. Ensure that the security group you select allows the client to access the DB instance. If no security group is available or has been created, RDS allocates a security group to you by default.

Table 2-4 Database configuration

Parameter	Description
Administrator	The default login name for the database is **root**.
Administrator Password	Must consist of 8 to 32 characters and contain the following character types: uppercase letters, lowercase letters, digits, and special characters (~!@#$%^*-_=+?,()&). Enter a strong password and periodically change it for security reasons. If the password you provide is regarded as a weak password by the system, you will be prompted to enter a stronger password. Keep this password secure. The system cannot retrieve it. After a DB instance is created, you can reset this password. For details, see **Resetting the Administrator Password**.
Confirm Password	Must be the same as **Administrator Password**.
Parameter Template	Contains engine configuration values that can be applied to one or more DB instances. If you intend to create a primary/standby DB pair, they use the same parameter template. You can modify the instance parameters as required after the DB instance is created. For details, see **Modifying Parameters in a Parameter Template**.
Table Name	Specifies whether table names are case sensitive. **NOTE** The case sensitivity of table names for created instances cannot be changed.
Enterprise Project	If your account has been associated with an enterprise project, select the target project from the **Enterprise Project** drop-down list. For more information about enterprise projects, see ***Enterprise Management User Guide***.

- Tags

Table 2-5 Tags

Parameter	Description
Tag	Tags an RDS DB instance. This parameter is optional. Adding tags to RDS DB instances helps you better identify and manage the DB instances. A maximum of 20 tags can be added for each DB instance. If your organization has configured tag policies for RDS, add tags to DB instances based on the policies. If a tag does not comply with the policies, DB instance creation may fail. Contact your organization administrator to learn more about tag policies. After a DB instance is created, you can view its tag details on the **Tags** page. For details, see **Managing Tags**.

- Purchase period

Table 2-6 Purchase period

Parameter	Description
Quantity	RDS supports DB instance creation in batches. If you choose to create primary/standby DB instances and set **Quantity** to **1**, a primary DB instance and a standby DB instance will be created synchronously.

NOTE

- If you have any questions about the price, move the cursor to ? in the **Price** area at the bottom of the page and click **Pricing details**.
- The performance of your DB instance depends on its configurations. Hardware configuration items include the instance specifications, storage type, and storage space.

Step 3 Confirm the specifications.

- If you do not need to modify your settings, click **Submit**.
- If you need to modify your settings, click **Previous**.

Step 4 To view and manage your DB instance, go to the **Instances** page.

- When your DB instance is being created, the status is **Creating**. The status changes to **Available** after the instance is created. To view the detailed progress and result of the creation, go to the **Task Center** page.
- The automated backup policy is enabled by default. You can change it after the DB instance is created. An automated full backup is immediately triggered once your DB instance is created.
- After a DB instance is created, you can enter a description for it.
- The default database port is **3306**. You can change it after a DB instance is created.

NOTE

You are advised to change the default database port in a timely manner. For details, see **Changing a Database Port**.

----End

2.3 Step 3: Connect to a DB Instance

2.3.1 Overview

An RDS DB instance can be connected through a private network, Data Admin Service (DAS), or a public network.

Table 2-7 RDS connection methods

Connect Through	IP Address	Scenarios	Description
DAS	No IP address required	DAS enables you to manage databases on a web-based console and provides you with database development, O&M, and intelligent diagnosis to make it easy to use and maintain your databases. The permissions required for connecting to DB instances through DAS are enabled by default.	● Easy to use, secure, advanced, and intelligent ● Recommended
Private network	Floating IP	RDS provides a floating IP address by default. If your applications are deployed on an ECS that is in the same region and VPC as your DB instance, you are advised to use a floating IP address to connect to the DB instance through the ECS.	● Secure and excellent performance ● Recommended

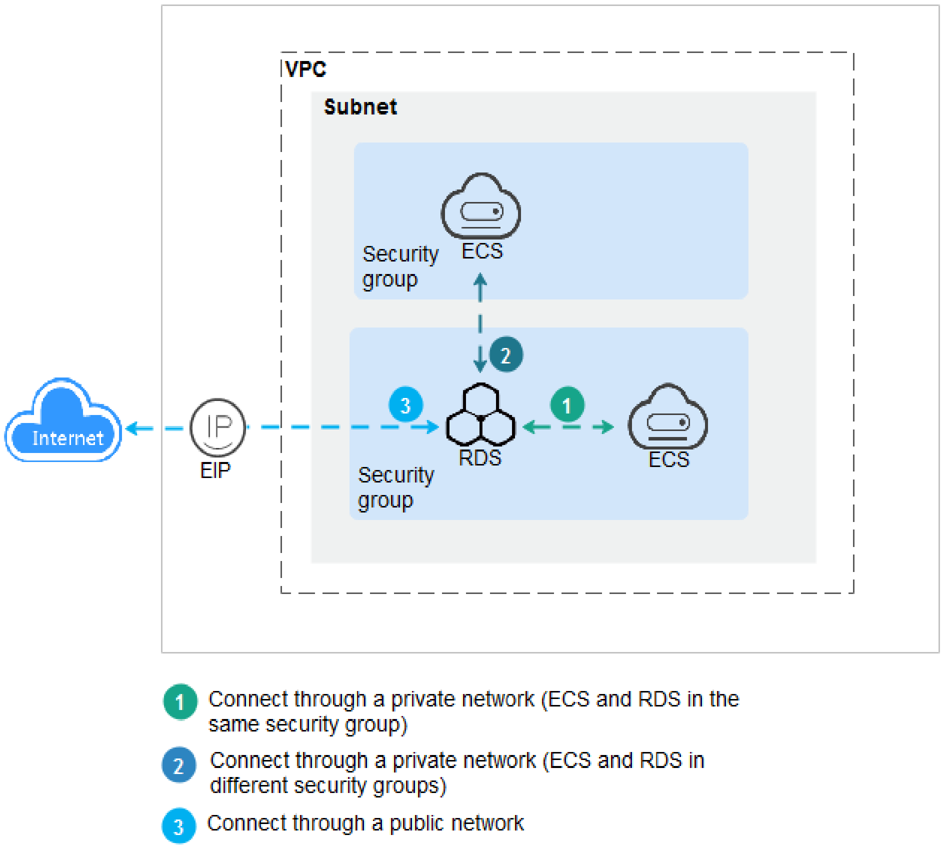
Connect Through	IP Address	Scenarios	Description
Public network	EIP	If you cannot access a DB instance through a floating IP address, bind an EIP to the DB instance and connect the DB instance through the EIP.	● A relatively lower level of security compared to other connection methods ● To achieve a higher transmission rate and security level, you are advised to migrate your applications to an ECS that is in the same VPC as your RDS DB instance and use a floating IP address to access the DB instance. ● You need to purchase an EIP. For details, see **EIP billing details**.

NOTE

- VPC: Virtual Private Cloud
- ECS: Elastic Cloud Server
- If the ECS is in the same VPC as your RDS DB instance, you do not need to apply for an EIP.

Figure 2-4 illustrates the connection over a private network or a public network.

Figure 2-4 DB instance connection


VPC
Subnet
Security group
ECS
2
Internet
IP
EIP
3
RDS
1
ECS
Security group
1 Connect through a private network (ECS and RDS in the same security group)
2 Connect through a private network (ECS and RDS in different security groups)
3 Connect through a public network

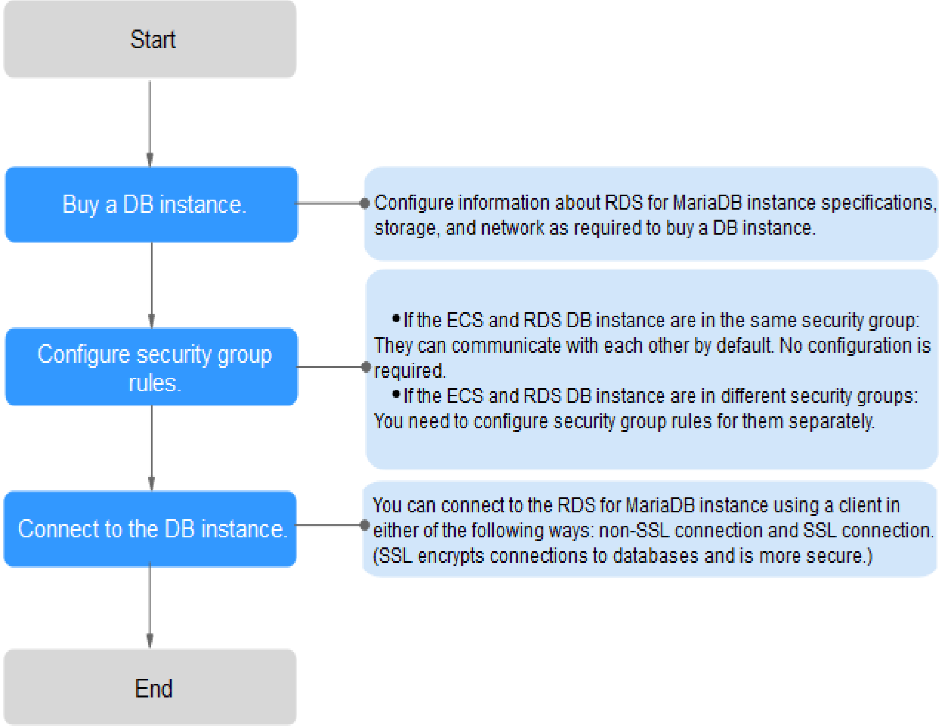
2.3.2 Connecting to a DB Instance Through a Private Network

2.3.2.1 Overview

Process

Figure 2-5 illustrates the process of connecting to an RDS for MariaDB instance through a private network.

Figure 2-5 Connecting to a DB instance through a private network


Start
Buy a DB instance.
Configure information about RDS for MariaDB instance specifications, storage, and network as required to buy a DB instance.
Configure security group rules.
• If the ECS and RDS DB instance are in the same security group: They can communicate with each other by default. No configuration is required.
• If the ECS and RDS DB instance are in different security groups: You need to configure security group rules for them separately.
Connect to the DB instance.
You can connect to the RDS for MariaDB instance using a client in either of the following ways: non-SSL connection and SSL connection. (SSL encrypts connections to databases and is more secure.)
End

2.3.2.2 Configuring Security Group Rules

Before you can connect to your DB instance, you need to create security group rules to enable specific IP addresses and ports to access your RDS DB instance. This section describes how to configure an inbound rule for a DB instance.

Context

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

Scenarios

First check whether the ECS and RDS DB instance are in the same security group.

- If they are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to **Connecting to a DB Instance Using a MariaDB Client**.
- If they are in different security groups, configure security group rules for them, separately.
  - RDS DB instance: Configure an **inbound rule** for the security group with which the RDS DB instance is associated.
  - ECS: The default security group rule allows all outgoing data packets. In this case, you do not need to configure a security group rule for the ECS. If not all outbound traffic is allowed in the security group, you need to configure an **outbound rule** for the ECS.

For details about the requirements of security group rules, see **Adding a Security Group Rule** in *Virtual Private Cloud User Guide*.

Constraints

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.

- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS instance can be associated only with one security group, but one security group can be associated with multiple RDS instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for a security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

NOTE

To ensure the security of your data and DB instances, you are advised to use the principle of least privilege for database access. Change the database port (default value: **3306**), and set the IP address to the remote server's address or any IP address in the remote server's smallest subnet to control the access from the remote server.

The default value of **Source** is **0.0.0.0/0**, indicating that RDS DB instances in the security group can be accessed from any IP address.

Procedure

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

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

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

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

Step 5 In the navigation pane on the left, choose **Connectivity & Security**. In the **Security Group Rules** area, view security group rules.

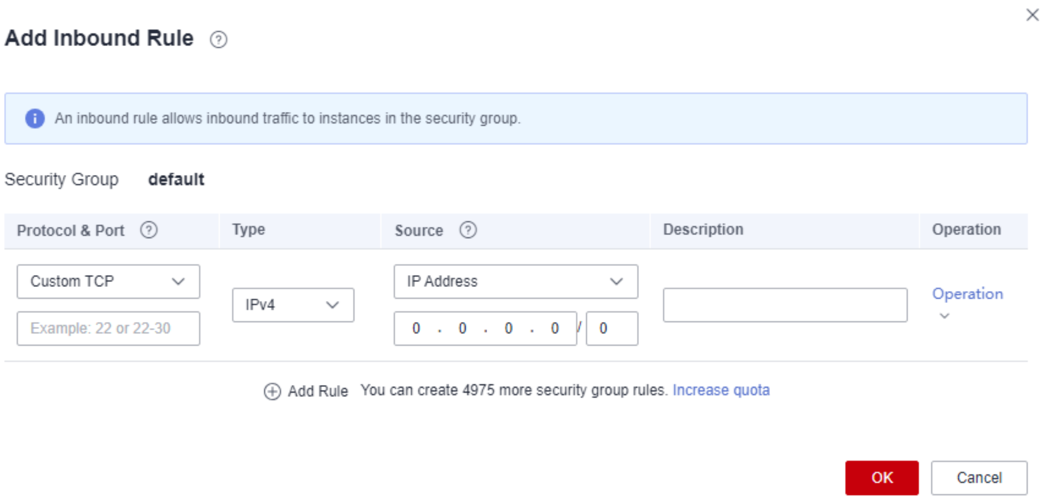
Step 6 Click **Add Inbound Rule** or **Allow All IP** to configure security group rules.

To add more inbound rules, click ⊕.

NOTE

Allow All IP allows all IP addresses to access RDS DB instances in the security group, which poses high security risks. Exercise caution when performing this operation.

Figure 2-6 Adding an inbound rule



Add Inbound Rule

An inbound rule allows inbound traffic to instances in the security group.

Security Group **default**

Protocol & Port	Type	Source	Description	Operation
Custom TCP Example: 22 or 22-30	IPv4	IP Address 0 . 0 . 0 . 0 / 0		Operation

Add Rule
You can create 4975 more security group rules. Increase quota
OK
Cancel

Table 2-8 Inbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	**Protocol**: network protocol. Available options: **All ports**, **Custom TCP**, **Custom UDP**, **ICMP**, or **GRE**.	Custom TCP
	Port: the port over which the traffic can reach your DB instance. RDS for MariaDB instances can use database ports 1024 to 65535, excluding 12017 and 33071, which are reserved for RDS system use.	3306
Type	Supported source IP address type. Its value can be: ● IPv4 ● IPv6	IPv4

Parameter	Description	Example Value
Source	The source in an inbound rule is used to match the IP address or address range of an external request. The source can be: ● Single IP address: 192.168.10.10/32 (IPv4 address) ● IP address segment: 192.168.1.0/24 (IPv4 address segment) ● All IP addresses: 0.0.0.0/0 (any IPv4 address) ● Security group: sg-abc ● IP address group: ipGroup-test	0.0.0.0/0
Description	Supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (<) or (>).	N/A

Step 7 Click **OK**.

----End

2.3.2.3 Connecting to a DB Instance Using a MariaDB Client

You can connect to a DB instance through a Secure Sockets Layer (SSL) connection or a non-SSL connection. SSL encrypts connections to your DB instance, making in-transit data more secure.

Prerequisites

1. You have logged in to an ECS.
   - For details on how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.
   - To connect to a DB instance through an ECS, you must ensure that:
     - The ECS and DB instance are in the same VPC.
     - The ECS is allowed by the security group to access the DB instance.
       - If the security group associated with the DB instance is the default security group, you do not need to configure security group rules.
       - If the security group associated with the DB instance is not the default security group, check whether the security group rules

allow the ECS to connect to the DB instance. For details, see **Configuring Security Group Rules**.

If the rules allow the access from the ECS, you can connect to the DB instance through the ECS.

If the rules do not allow the access from the ECS, you need to add a security group rule allowing the ECS to access the DB instance.

2. You have installed a database client to connect to DB instances.

   You can use a database client to connect to the target DB instance in Linux or Windows.

   – In Linux, install a **MariaDB client** on a device that can access RDS. It is recommended that you download a MariaDB client running a version later than that of the DB instance.

   – In Windows, you can use any common database client to connect to the target DB instance in a similar way.

Connecting to a DB Instance Using Commands (SSL Connection)

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

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

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

Step 4 On the **Instances** page, click the instance name to go to the **Basic Information** page.

Step 5 In the **DB Information** area, check whether SSL is enabled.

- If yes, go to **Step 6**.
- If no, click ◯. In the displayed dialog box, click **OK**. Then, go to **6**.

Step 6 Click ⤓ next to the **SSL** field to download **Certificate Download.zip**, and extract the root certificate **ca.pem** and bundle **ca-bundle.pem** from the package.

Step 7 Import the root certificate **ca.pem** to the Linux or Windows. For details, see **How Can I Import the Root Certificate to a Windows or Linux OS?**

Step 8 Connect to the RDS for MariaDB instance. In Linux, for example, run the following command:

- Method 1

  mysql -h <*host*> **-P** <*port*> **-u** <*userName*> **-p --ssl-ca=**<*caName*>

  Example:

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

- Method 2

  mysql -h <*host*> **-P** <*port*> **-u** <*userName*> **-p --ssl-capath=**<*caPath*>

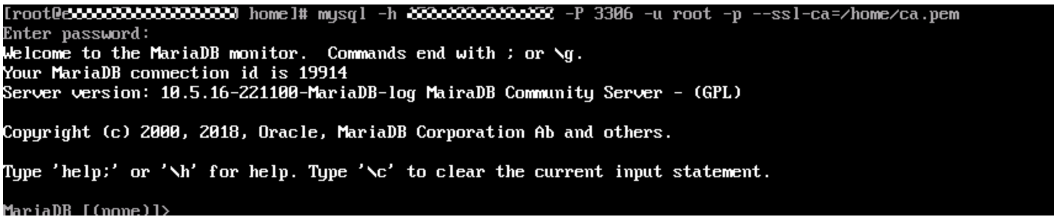
Table 2-9 Parameter description

Parameter	Description
<*host*>	Floating IP address. To obtain this parameter, go to the **Basic Information** page of the DB instance and view the floating IP address in the **Connection Information** area.
<*port*>	Database port. By default, the value is **3306**. To obtain this parameter, go to the **Basic Information** page of the DB instance and view the database port in the **Connection Information** area.
<*userName*>	Database account used for logging in to the DB instance. The default value is **root**.
<*caName*>	Name of the CA certificate. The certificate should be stored in the directory where the command is executed.
<*caPath*>	Path of the CA certificate.

Step 9 Enter the password of the database account if the following information is displayed:

```
Enter password:
```

Figure 2-7 Connection example



```
[root@[redacted] home]# mysql -h [redacted] -P 3306 -u root -p --ssl-ca=/home/ca.pem
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 19914
Server version: 10.5.16-221100-MariaDB-log MairaDB Community Server - (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

----End

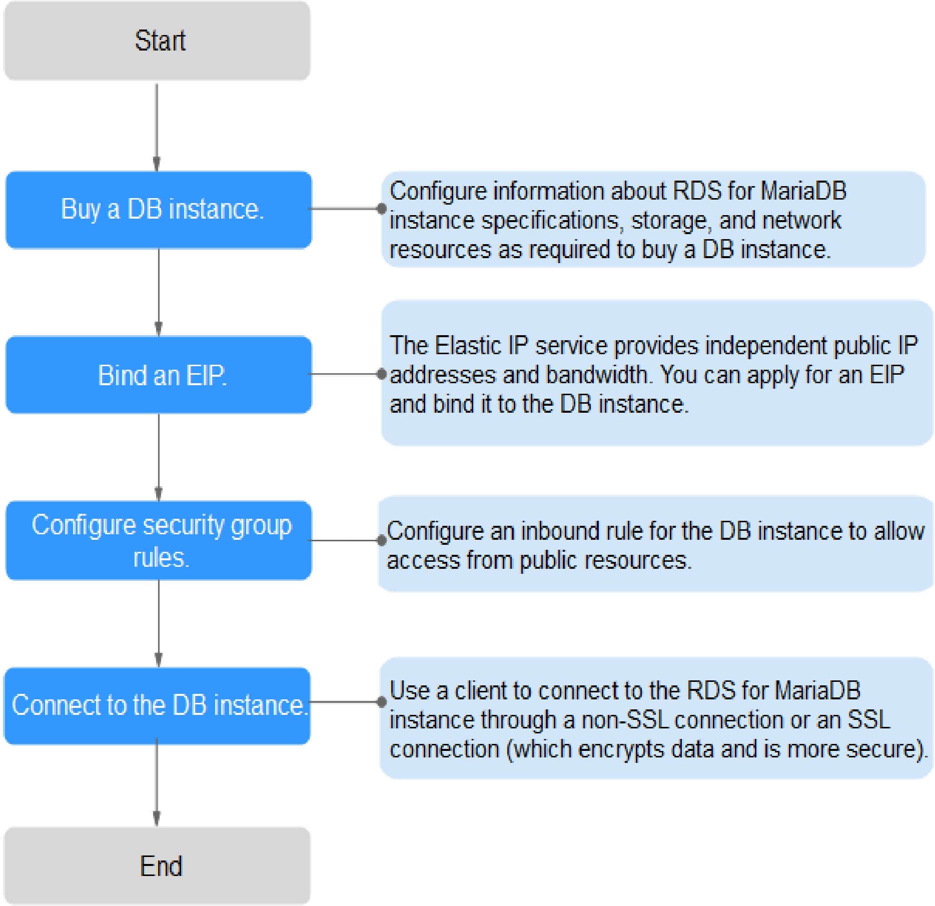
2.3.3 Connecting to a DB Instance Through a Public Network

2.3.3.1 Overview

Process

Figure 2-8 illustrates the process of connecting to an RDS for MariaDB instance through a public network.

Figure 2-8 Connecting to a DB instance through a public network


Start
Buy a DB instance.
Configure information about RDS for MariaDB instance specifications, storage, and network resources as required to buy a DB instance.
Bind an EIP.
The Elastic IP service provides independent public IP addresses and bandwidth. You can apply for an EIP and bind it to the DB instance.
Configure security group rules.
Configure an inbound rule for the DB instance to allow access from public resources.
Connect to the DB instance.
Use a client to connect to the RDS for MariaDB instance through a non-SSL connection or an SSL connection (which encrypts data and is more secure).
End

2.3.3.2 Binding an EIP

Scenarios

You can bind an EIP to a DB instance for public accessibility and can unbind the EIP from the DB instance as required.

Precautions

- To enable this function, contact customer service.
- You need to configure security groups and enable specific IP addresses and ports to access the target DB instance. Before accessing the DB instance, add an individual IP address or an IP address range that will access the DB instance to the inbound rule. For details, see **Configuring Security Group Rules**.
- Traffic generated by the public network is charged. You can unbind the EIP from the DB instance when the EIP is no longer used.

Binding an EIP

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

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

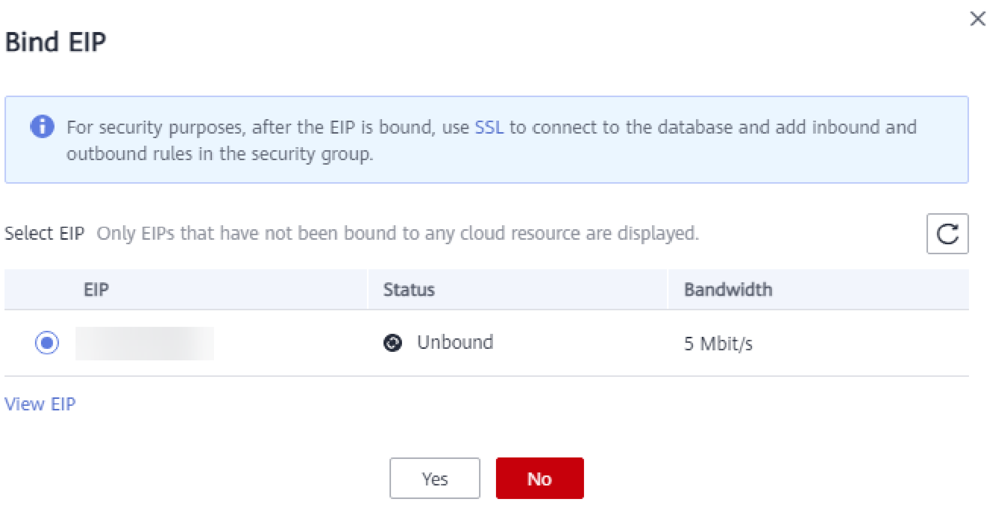
Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

Step 4 On the **Instances** page, click the target DB instance.

Step 5 In the navigation pane on the left, choose **Connectivity & Security**. In the **Connection Information** area, click **Bind** next to the **EIP** field.

Step 6 In the displayed dialog box, select an EIP and click **Yes**.

Figure 2-9 Selecting an EIP



Bind EIP

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

Select EIP Only EIPs that have not been bound to any cloud resource are displayed.

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

View EIP

Step 7 On the **Connectivity & Security** page, view the EIP that has been bound to the DB instance.

You can also view the progress and result of binding an EIP to a DB instance on the **Task Center** page.

----End

2.3.3.3 Configuring Security Group Rules

For security, you need to create security group rules to allow specific IP addresses and ports to access your RDS DB instance. When you attempt to connect to an RDS DB instance through an EIP, configure an **inbound rule** for the security group associated with the DB instance.

Context

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

Constraints

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.

- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS instance can be associated only with one security group, but one security group can be associated with multiple RDS instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for a security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

NOTE

To ensure the security of your data and DB instances, you are advised to use the principle of least privilege for database access. Change the database port (default value: **3306**), and set the IP address to the remote server's address or any IP address in the remote server's smallest subnet to control the access from the remote server.

The default value of **Source** is **0.0.0.0/0**, indicating that RDS DB instances in the security group can be accessed from any IP address.

Procedure

Step 1 Log in to the management console.

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

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

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

Step 5 In the navigation pane on the left, choose **Connectivity & Security**. In the **Security Group Rules** area, view security group rules.

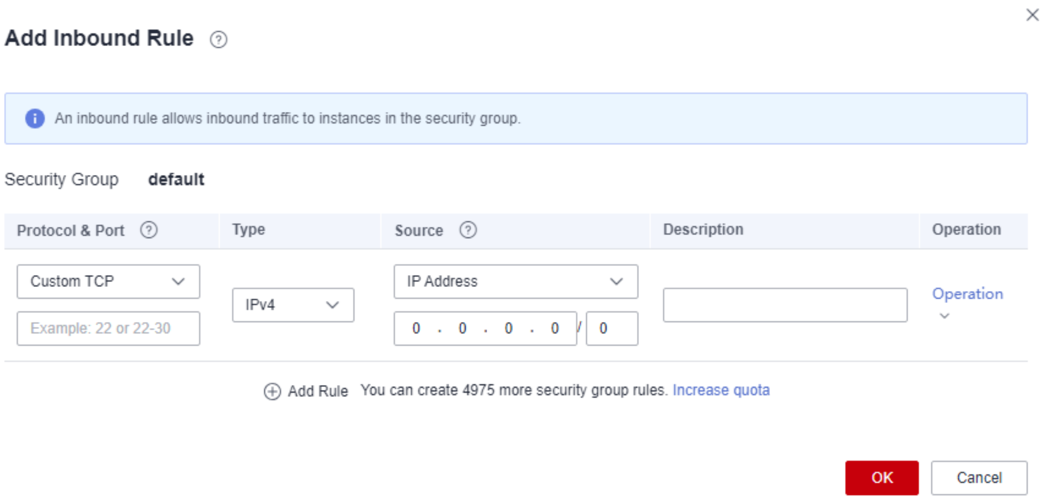
Step 6 Click **Add Inbound Rule** or **Allow All IP** to configure security group rules.

To add more inbound rules, click ⊕.

NOTE

Allow All IP allows all IP addresses to access RDS DB instances in the security group, which poses high security risks. Exercise caution when performing this operation.

Figure 2-10 Adding an inbound rule



Add Inbound Rule

An inbound rule allows inbound traffic to instances in the security group.

Security Group default

Protocol & Port	Type	Source	Description	Operation
Custom TCP Example: 22 or 22-30	IPv4	IP Address 0 . 0 . 0 . 0 / 0		Operation

Add Rule
You can create 4975 more security group rules. Increase quota
OK
Cancel

Table 2-10 Inbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	**Protocol**: network protocol. Available options: **All ports**, **Custom TCP**, **Custom UDP**, **ICMP**, or **GRE**.	Custom TCP
	Port: the port over which the traffic can reach your DB instance. RDS for MariaDB instances can use database ports 1024 to 65535, excluding 12017 and 33071, which are reserved for RDS system use.	3306
Type	Supported source IP address type. Its value can be: ● IPv4 ● IPv6	IPv4

Parameter	Description	Example Value
Source	The source in an inbound rule is used to match the IP address or address range of an external request. The source can be: ● Single IP address: 192.168.10.10/32 (IPv4 address) ● IP address segment: 192.168.1.0/24 (IPv4 address segment) ● All IP addresses: 0.0.0.0/0 (any IPv4 address) ● Security group: sg-abc ● IP address group: ipGroup-test	0.0.0.0/0
Description	Supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (<) or (>).	N/A

Step 7 Click **OK**.

----End

2.3.3.4 Connecting to a DB Instance Using a MariaDB Client

You can connect to an instance through a non-SSL connection or an SSL connection using a MariaDB client. SSL encrypts connections to your DB instance and is more secure.

Prerequisites

1. An EIP has been bound to the target DB instance and security group rules have been configured. The operations are as follows:

   a. Bind an EIP to your DB instance.

      For details about how to bind an EIP, see **Binding an EIP**.

   b. Obtain the IP address of the ECS you use to connect to the DB instance.

   c. Configure security group rules.

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

      For details about how to configure a security group rule, see **Configuring Security Group Rules**.

d. Run the **ping** command to check the connectivity between the ECS and the EIP that has been bound to the DB instance in **1.a**.

2. You have installed a database client to connect to DB instances.

   You can use a database client to connect to the target DB instance in Linux or Windows.

   – In Linux, you need to install a **MariaDB client** on your device. It is recommended that you download a MariaDB client running a version later than that of the DB instance.

   – In Windows, you can use any common database client to connect to the target DB instance in a similar way.

Connecting to a DB Instance Using Commands (SSL Connection)

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

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

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

Step 4 On the **Instances** page, click the instance name to go to the **Basic Information** page.

Step 5 In the **DB Information** area, check whether SSL is enabled.

- If yes, go to **6**.
- If no, click ○. In the displayed dialog box, click **OK**. Then, go to **6**.

Step 6 Click ⤓ next to the **SSL** field to download **Certificate Download.zip**, and extract the root certificate **ca.pem** and bundle **ca-bundle.pem** from the package.

Step 7 Import the root certificate **ca.pem** to the Linux or Windows. For details, see **How Can I Import the Root Certificate to a Windows or Linux OS?**

Step 8 Connect to the RDS for MariaDB instance. In Linux, for example, run the following command:

- Method 1

  mysql -h <*host*> **-P** <*port*> **-u** <*userName*> **-p --ssl-ca=**<*caName*>

  Example:

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

- Method 2

  mysql -h <*host*> **-P** <*port*> **-u** <*userName*> **-p --ssl-capath=**<*caPath*>

Table 2-11 Parameter description

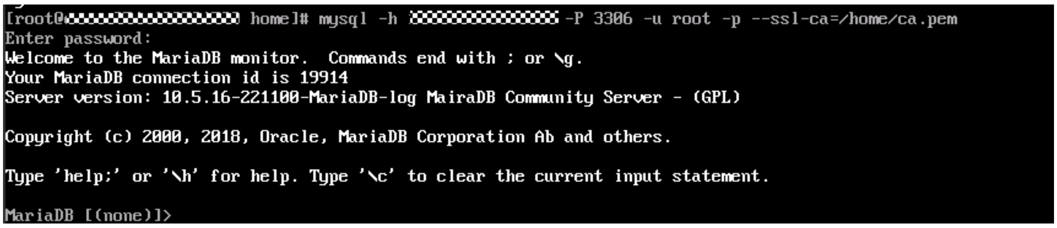
Parameter	Description
<*host*>	EIP of the DB instance to be connected.
<*port*>	Port of the DB instance to be connected.

Parameter	Description
<*userName*>	Database account used for logging in to the DB instance. The default value is **root**.
<*caName*>	Name of the CA certificate. The certificate should be stored in the directory where the command is executed.
<*caPath*>	Path of the CA certificate.

Step 9 Enter the password of the database account if the following information is displayed:

```
Enter password:
```

Figure 2-11 Connection example



```
[root@[redacted] home]# mysql -h [redacted] -P 3306 -u root -p --ssl-ca=/home/ca.pem
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 19914
Server version: 10.5.16-221100-MariaDB-log MairaDB Community Server - (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

NOTE

If the connection fails, ensure that preparations have been correctly made in **Prerequisites** and try again.

----End

2.3.4 Connecting to a DB Instance Through DAS

Scenarios

Data Admin Service (DAS) enables you to connect to and manage DB instances with ease on a web-based console. The permission required for connecting to DB instances through DAS has been enabled for you by default. Using DAS to connect to your DB instance is recommended, which is more secure and convenient.

Procedure

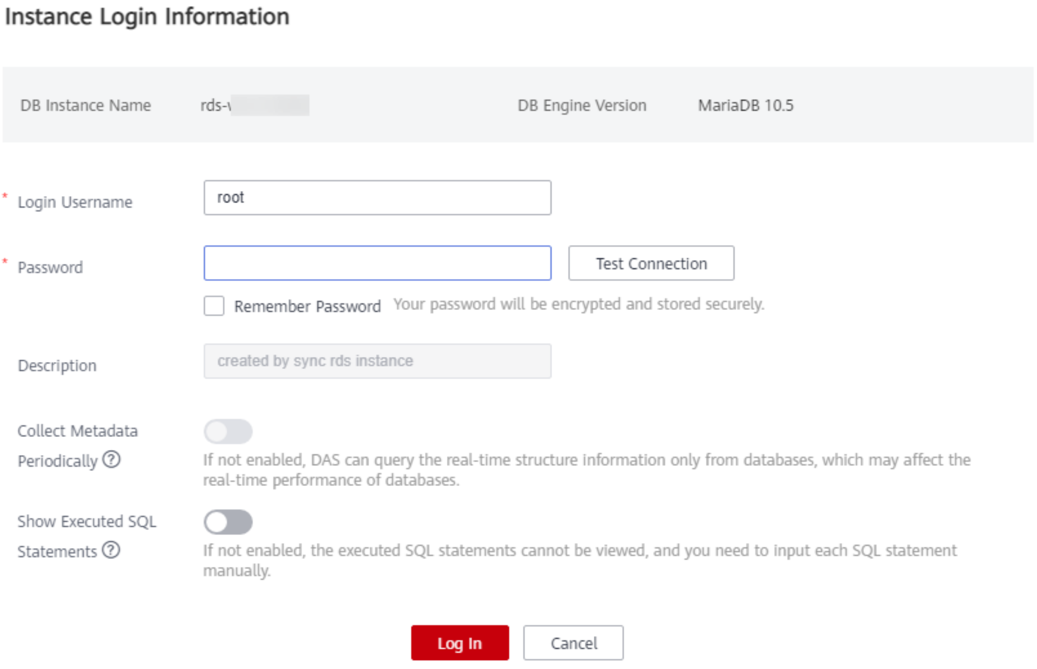
Step 1 **Log in to the management console**.

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

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

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

Figure 2-12 Login page



Instance Login Information

DB Instance Name rds-[redacted]

DB Engine Version MariaDB 10.5

* Login Username: root

* Password:

□ Remember Password Your password will be encrypted and stored securely.

Description: created by sync rds instance

Collect Metadata Periodically: If not enabled, DAS can query the real-time structure information only from databases, which may affect the real-time performance of databases.

Show Executed SQL Statements: If not enabled, the executed SQL statements cannot be viewed, and you need to input each SQL statement manually.

Step 5 Enter the database username and password and click **Test Connection**.

Step 6 After the connection test is successful, click **Log In**.

For details about how to manage databases using DAS, see **RDS for MariaDB Database Management** in the *Data Admin Service User Guide*.

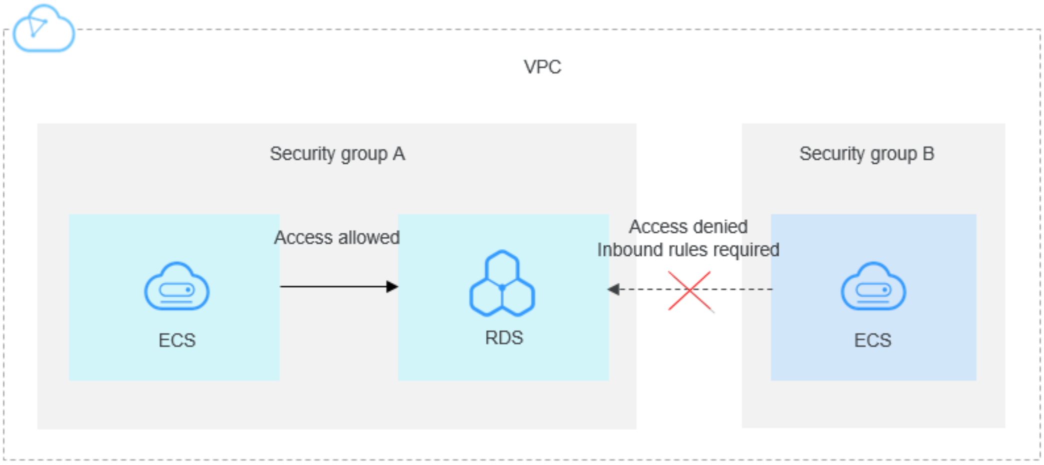
----End

2.4 Example: Buy and Connect to an RDS for MariaDB Instance

This example illustrates how to purchase an RDS for MariaDB instance and connect to it from a Linux ECS over a private network.

- **Step 1: Buy an RDS for MariaDB Instance**
- **Step 2: Buy an ECS**
- **Step 3: Connect to the RDS for MariaDB Instance**

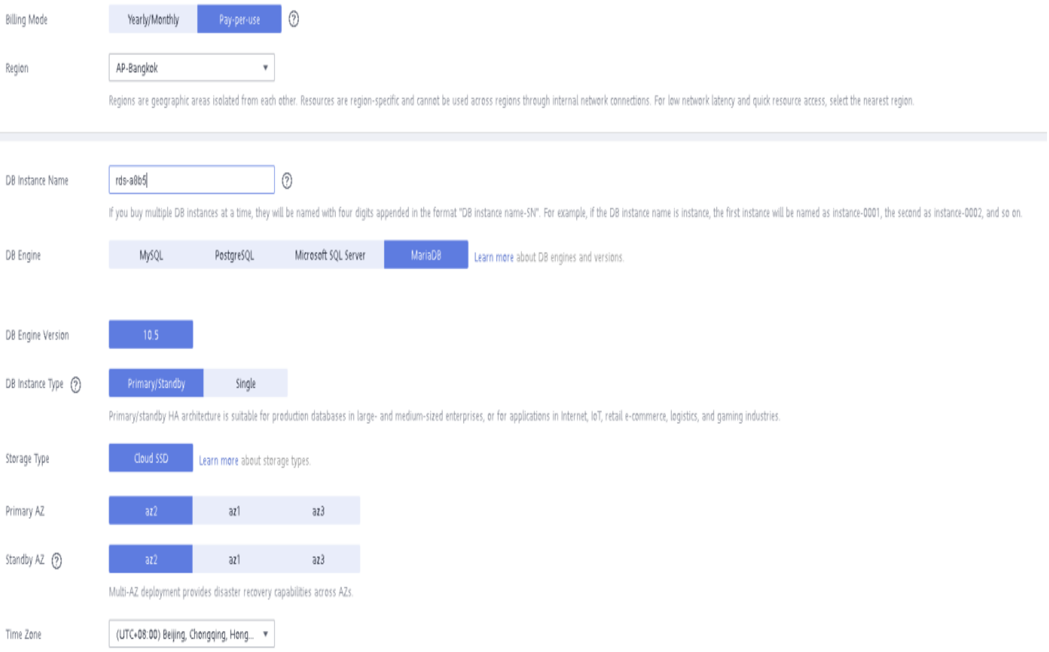
Figure 2-13 Example diagram



Step 1: Buy an RDS for MariaDB Instance

1. Go to the **Buy DB Instance** page.
2. Configure the instance information and click **Next**. Keep the region, AZ, VPC, and security group of the DB instance the same as those of the ECS.

Figure 2-14 Selecting an engine version



Billing Mode: Yearly/Monthly | Pay-per-use (selected)

Region: AP-Bangkok

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

DB Instance Name: rds-a8b5

If you buy multiple DB instances at a time, they will be named with four digits appended in the format "DB instance name-SN". For example, if the DB instance name is instance, the first instance will be named as instance-0001, the second as instance-0002, and so on.

DB Engine: MySQL | PostgreSQL | Microsoft SQL Server | MariaDB (selected) Learn more about DB engines and versions.

DB Engine Version: 10.5

DB Instance Type: Primary/Standby (selected) | Single

Primary/standby HA architecture is suitable for production databases in large- and medium-sized enterprises, or for applications in Internet, IoT, retail e-commerce, logistics, and gaming industries.

Storage Type: Cloud SSD Learn more about storage types.

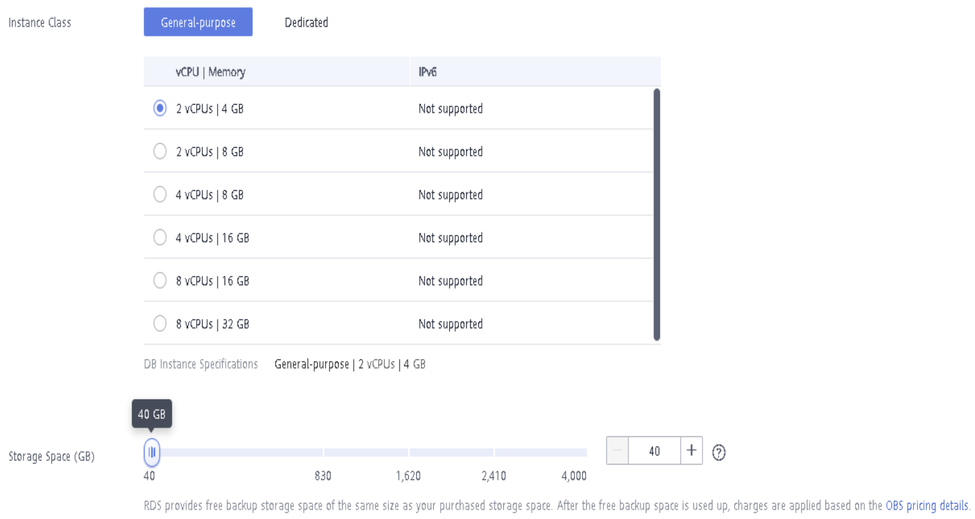
Primary AZ: az2 (selected) | az1 | az3

Standby AZ: az2 (selected) | az1 | az3

Multi-AZ deployment provides disaster recovery capabilities across AZs.

Time Zone: (UTC+08:00) Beijing, Chongqing, Hong...

Figure 2-15 Selecting an instance class



Instance Class: General-purpose | Dedicated

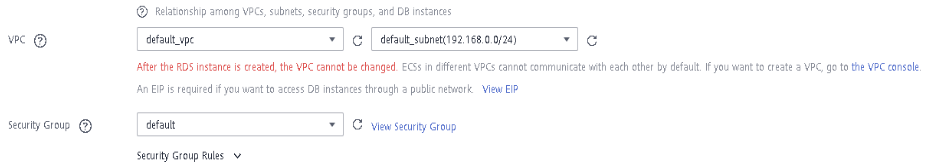
	vCPU | Memory	IPv6
●	2 vCPUs | 4 GB	Not supported
○	2 vCPUs | 8 GB	Not supported
○	4 vCPUs | 8 GB	Not supported
○	4 vCPUs | 16 GB	Not supported
○	8 vCPUs | 16 GB	Not supported
○	8 vCPUs | 32 GB	Not supported

DB Instance Specifications: General-purpose | 2 vCPUs | 4 GB

Storage Space (GB): 40 GB (40, 830, 1,620, 2,410, 4,000) 40

RDS provides free backup storage space of the same size as your purchased storage space. After the free backup space is used up, charges are applied based on the OBS pricing details.

Figure 2-16 Configuring network information



Relationship among VPCs, subnets, security groups, and DB instances

VPC: default_vpc | default_subnet(192.168.0.0/24)

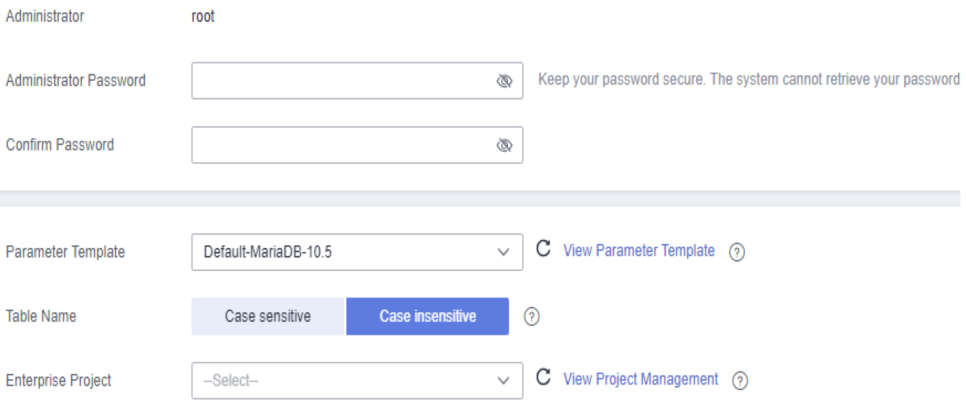
After the RDS instance is created, the VPC cannot be changed. ECSs in different VPCs cannot communicate with each other by default. If you want to create a VPC, go to the VPC console.

An EIP is required if you want to access DB instances through a public network. View EIP

Security Group: default | View Security Group

Security Group Rules

Figure 2-17 Setting a password



Administrator: root

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

Confirm Password:

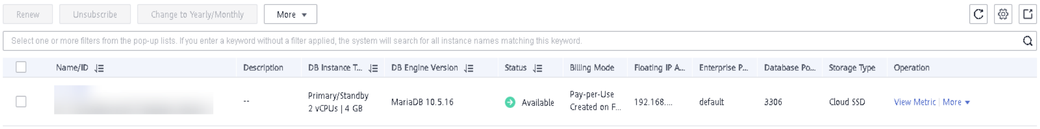
Parameter Template: Default-MariaDB-10.5 | View Parameter Template

Table Name: Case sensitive | Case insensitive

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

3. View the purchased RDS instance.

Figure 2-18 Instance successfully purchased



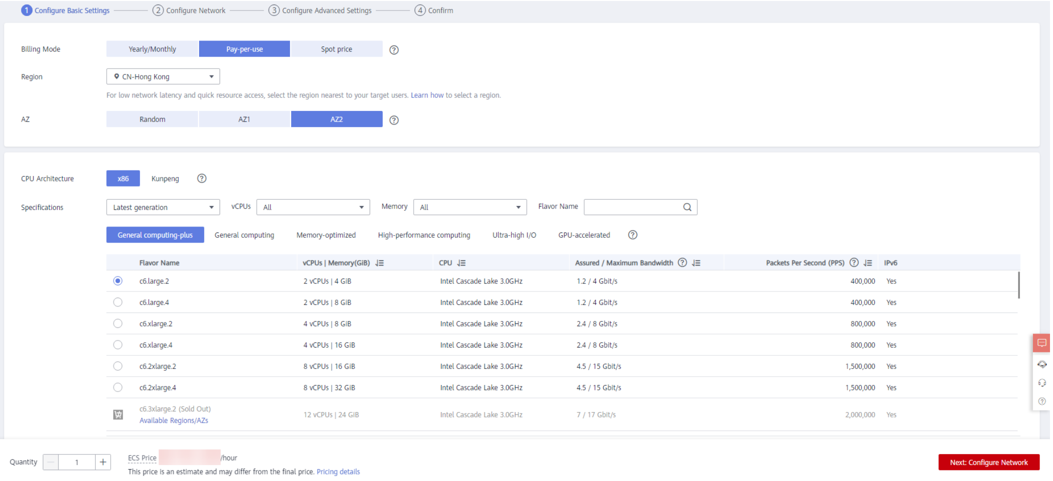
Select one or more filters from the pop-up lists. If you enter a keyword without a filter applied, the system will search for all instance names matching this keyword.

□	Name/ID	Description	DB Instance T...	DB Engine Version	Status	Billing Mode	Floating IP A...	Enterprise P...	Database Po...	Storage Type	Operation
□	[redacted]	--	Primary/Standby 2 vCPUs | 4 GB	MariaDB 10.5.16	Available	Pay-per-Use Created on F...	192.168....	default	3306	Cloud SSD	View Metric | More

Step 2: Buy an ECS

1. Go to the **Buy ECS** page.
2. Configure basic settings and click **Next: Configure Network**. Keep the region and AZ of the ECS the same as those of the RDS for MariaDB instance to be connected.

Figure 2-19 Basic configurations



1 Configure Basic Settings — 2 Configure Network — 3 Configure Advanced Settings — 4 Confirm

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

Region: CN-Hong Kong

For low network latency and quick resource access, select the region nearest to your target users. Learn how to select a region.

AZ: Random | AZ1 | **AZ2**

CPU Architecture: **x86** | Kunpeng

Specifications: Latest generation; vCPUs: All; Memory: All; Flavor Name:

General computing-plus | General computing | Memory-optimized | High-performance computing | Ultra-high I/O | GPU-accelerated

	Flavor Name	vCPUs | Memory(GiB)	CPU	Assured / Maximum Bandwidth	Packets Per Second (PPS)	IPv6
●	c6.large.2	2 vCPUs | 4 GiB	Intel Cascade Lake 3.0GHz	1.2 / 4 Gbit/s	400,000	Yes
○	c6.large.4	2 vCPUs | 8 GiB	Intel Cascade Lake 3.0GHz	1.2 / 4 Gbit/s	400,000	Yes
○	c6.xlarge.2	4 vCPUs | 8 GiB	Intel Cascade Lake 3.0GHz	2.4 / 8 Gbit/s	800,000	Yes
○	c6.xlarge.4	4 vCPUs | 16 GiB	Intel Cascade Lake 3.0GHz	2.4 / 8 Gbit/s	800,000	Yes
○	c6.2xlarge.2	8 vCPUs | 16 GiB	Intel Cascade Lake 3.0GHz	4.5 / 15 Gbit/s	1,500,000	Yes
○	c6.2xlarge.4	8 vCPUs | 32 GiB	Intel Cascade Lake 3.0GHz	4.5 / 15 Gbit/s	1,500,000	Yes
	c6.3xlarge.2 (Sold Out) Available Regions/AZs	12 vCPUs | 24 GiB	Intel Cascade Lake 3.0GHz	7 / 17 Gbit/s	2,000,000	Yes

Quantity: 1

ECS Price [redacted]/hour

This price is an estimate and may differ from the final price. Pricing details

Figure 2-20 Selecting an image

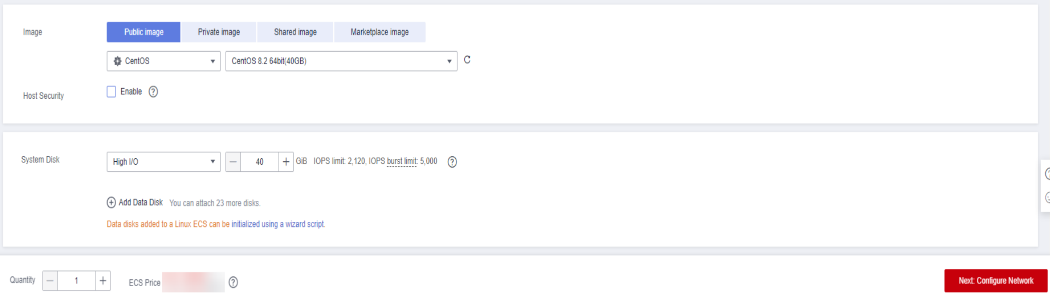


Image: **Public image** | Private image | Shared image | Marketplace image

CentOS; CentOS 8.2 64bit(40GB)

Host Security: □ Enable

System Disk: High I/O; 40 GiB IOPS limit: 2,120, IOPS burst limit: 5,000

Add Data Disk You can attach 23 more disks.

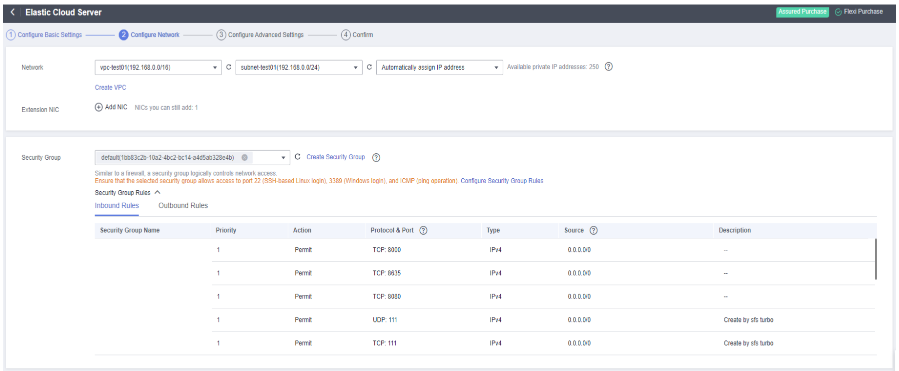
Data disks added to a Linux ECS can be initialized using a wizard script.

Quantity: 1

ECS Price [redacted]

3. Configure the ECS network information and click **Next: Configure Advanced Settings**. Keep the VPC and security group of the ECS the same as those of the RDS for MariaDB instance to be connected.

Figure 2-21 Network settings



1 Configure Basic Settings — 2 Configure Network — 3 Configure Advanced Settings — 4 Confirm

Network: vpc-test01(192.168.0.0/16); subnet-test01(192.168.0.0/24); Automatically assign IP address; Available private IP addresses: 250

Create VPC

Extension NIC: Add NIC NICs you can still add: 1

Security Group: default(1bb83c2b-10a2-4bc2-bc14-a4d5ab328e4b); Create Security Group

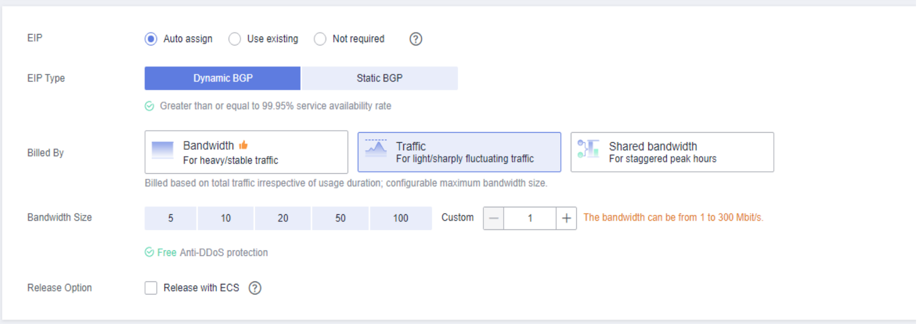
Similar to a firewall, a security group logically controls network access.
Ensure that the selected security group allows access to port 22 (SSH-based Linux login), 3389 (Windows login), and ICMP (ping operation). Configure Security Group Rules

Security Group Rules

Inbound Rules | Outbound Rules

Security Group Name	Priority	Action	Protocol & Port	Type	Source	Description
	1	Permit	TCP: 8000	IPv4	0.0.0.0/0	--
	1	Permit	TCP: 8635	IPv4	0.0.0.0/0	--
	1	Permit	TCP: 8080	IPv4	0.0.0.0/0	--
	1	Permit	UDP: 111	IPv4	0.0.0.0/0	Create by sfs turbo
	1	Permit	TCP: 111	IPv4	0.0.0.0/0	Create by sfs turbo

Figure 2-22 Selecting an EIP



EIP: ● Auto assign ○ Use existing ○ Not required

EIP Type: [✓ Dynamic BGP] Static BGP

Greater than or equal to 99.95% service availability rate

Billed By: Bandwidth (For heavy/stable traffic) | [✓ Traffic (For light/sharply fluctuating traffic)] | Shared bandwidth (For staggered peak hours)

Billed based on total traffic irrespective of usage duration; configurable maximum bandwidth size.

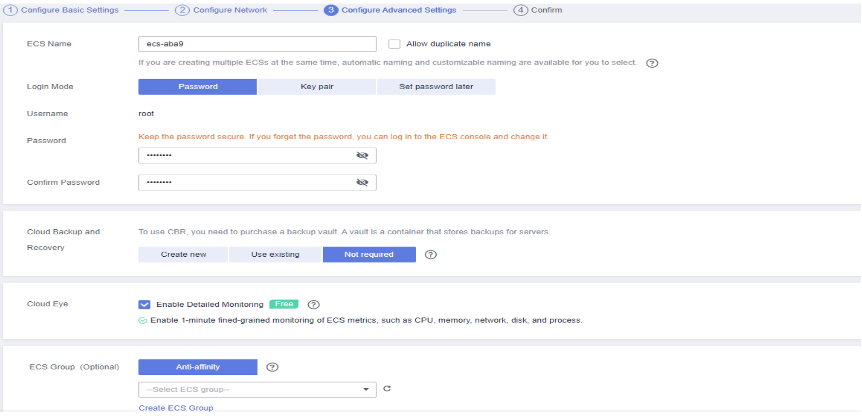
Bandwidth Size: 5 | 10 | 20 | 50 | 100 | Custom − 1 + The bandwidth can be from 1 to 300 Mbit/s.

Free Anti-DDoS protection

Release Option: □ Release with ECS

4. Configure the ECS password and click **Next: Confirm**.

Figure 2-23 Advanced settings



① Configure Basic Settings — ② Configure Network — ③ Configure Advanced Settings — ④ Confirm

ECS Name: ecs-aba9 □ Allow duplicate name

If you are creating multiple ECSs at the same time, automatic naming and customizable naming are available for you to select.

Login Mode: [✓ Password] Key pair Set password later

Username: root

Password: Keep the password secure. If you forget the password, you can log in to the ECS console and change it.
•••••••••

Confirm Password: •••••••••

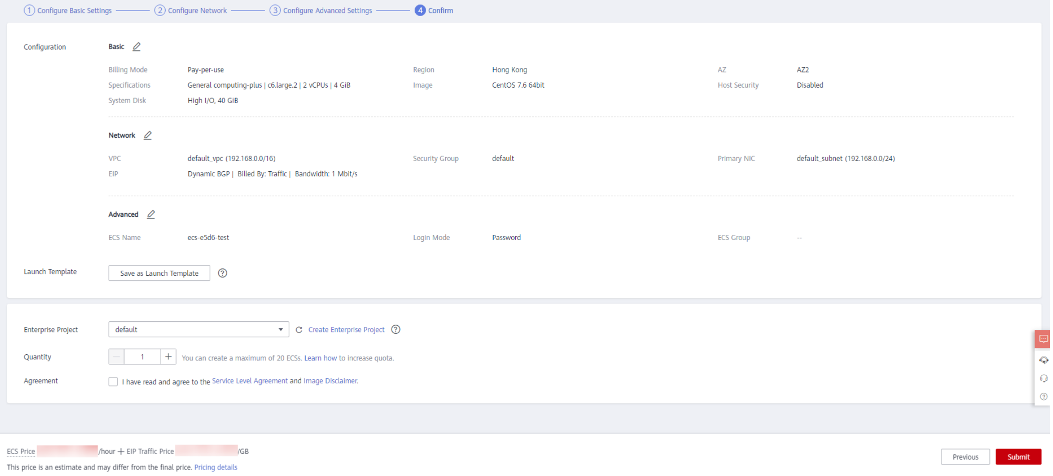
Cloud Backup and Recovery: To use CBR, you need to purchase a backup vault. A vault is a container that stores backups for servers.
Create new Use existing [✓ Not required]

Cloud Eye: ☑ Enable Detailed Monitoring Free
Enable 1-minute fined-grained monitoring of ECS metrics, such as CPU, memory, network, disk, and process.

ECS Group (Optional): [✓ Anti-affinity]
--Select ECS group--
Create ECS Group

5. Confirm the configurations and click **Submit**.

Figure 2-24 Confirming the configurations



① Configure Basic Settings — ② Configure Network — ③ Configure Advanced Settings — ④ Confirm

Configuration

Basic

Billing Mode	Pay-per-use	Region	Hong Kong	AZ	AZ2
Specifications	General computing-plus | c6.large.2 | 2 vCPUs | 4 GiB	Image	CentOS 7.6 64bit	Host Security	Disabled
System Disk	High I/O, 40 GiB				

Network

VPC	default_vpc (192.168.0.0/16)	Security Group	default	Primary NIC	default_subnet (192.168.0.0/24)
EIP	Dynamic BGP | Billed By: Traffic | Bandwidth: 1 Mbit/s				

Advanced

ECS Name	ecs-e5d6-test	Login Mode	Password	ECS Group	--

Launch Template: Save as Launch Template

Enterprise Project: default Create Enterprise Project

Quantity: − 1 + You can create a maximum of 20 ECSs. Learn how to increase quota.

Agreement: □ I have read and agree to the Service Level Agreement and Image Disclaimer.

ECS Price [redacted] /hour + EIP Traffic Price [redacted] /GB

This price is an estimate and may differ from the final price. Pricing details

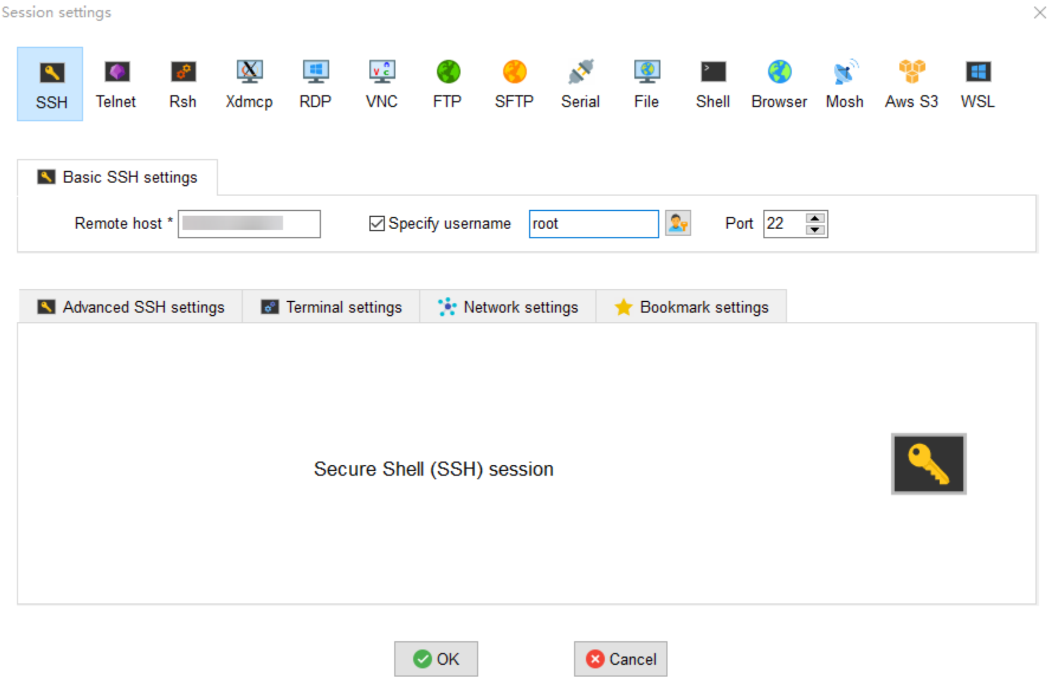
Previous Submit

6. View the purchased ECS.

Step 3: Connect to the RDS for MariaDB Instance

1. Use a Linux remote connection tool (for example, MobaXterm) to log in to the ECS. Enter the EIP bound to the ECS for **Remote host**.

Figure 2-25 Creating a session



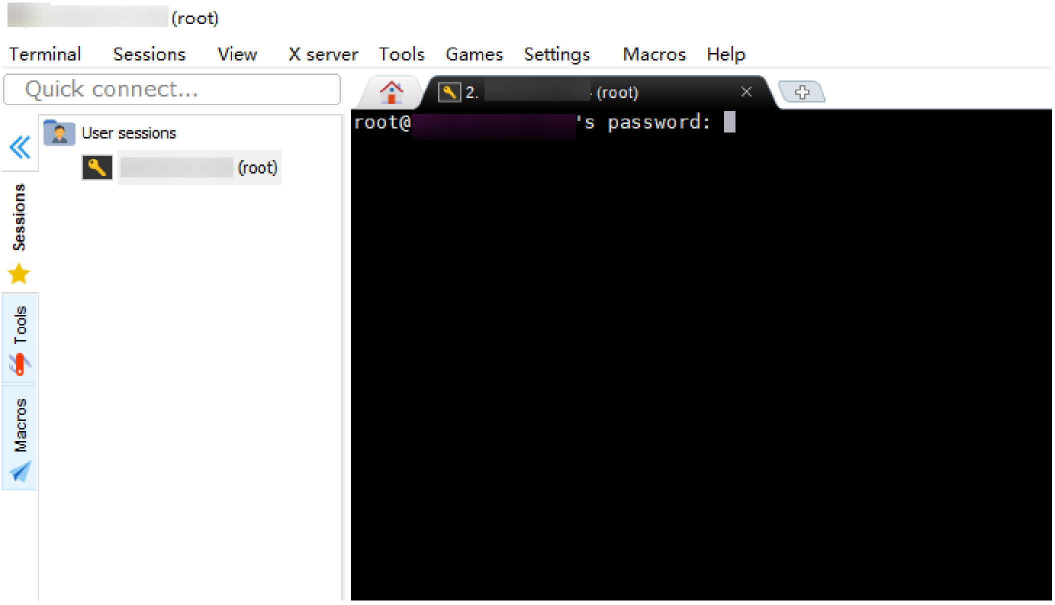
Remote host * [redacted]

☑ Specify username root

Port 22

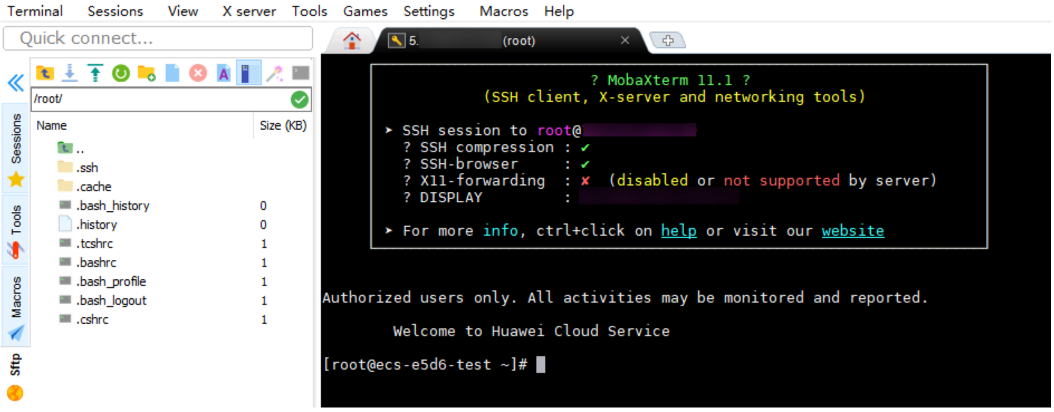
2. Enter the password of the ECS.

Figure 2-26 Entering the password



```
root@[redacted]'s password:
```

Figure 2-27 Successful login



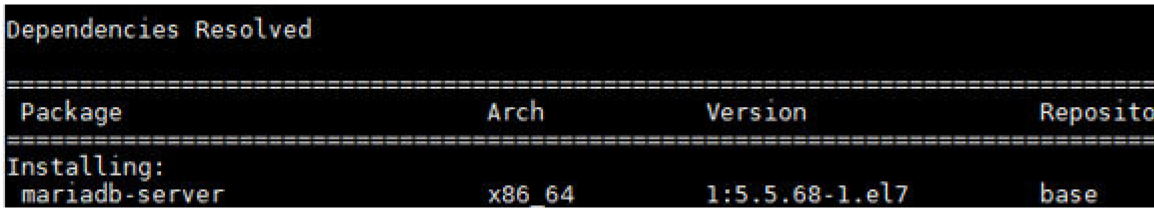
```
                    ? MobaXterm 11.1 ?
       (SSH client, X-server and networking tools)

 ➤ SSH session to root@[redacted]
   ? SSH compression : ✔
   ? SSH-browser     : ✔
   ? X11-forwarding  : ✘  (disabled or not supported by server)
   ? DISPLAY         : [redacted]

 ➤ For more info, ctrl+click on help or visit our website


Authorized users only. All activities may be monitored and reported.

        Welcome to Huawei Cloud Service

[root@ecs-e5d6-test ~]#
```

3. Install a **MariaDB client** by following the instructions provided in the official documentation.

   In CentOS, for example, run the following statement:

   ```
   yum install MariaDB-client
   ```

Figure 2-28 Installing a client

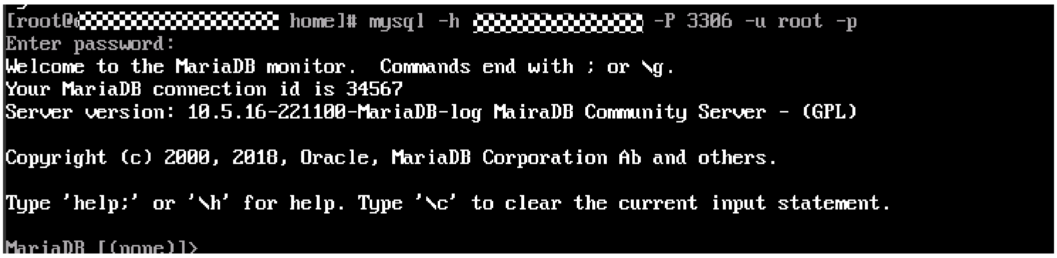


```
Dependencies Resolved

================================================================================
 Package                         Arch           Version               Reposito
================================================================================
Installing:
 mariadb-server                  x86_64         1:5.5.68-1.el7        base
```

4. Connect to the RDS for MariaDB instance.

   ```
   mysql -h ip -P 3306 -u root -p
   ```

Figure 2-29 Connection succeeded

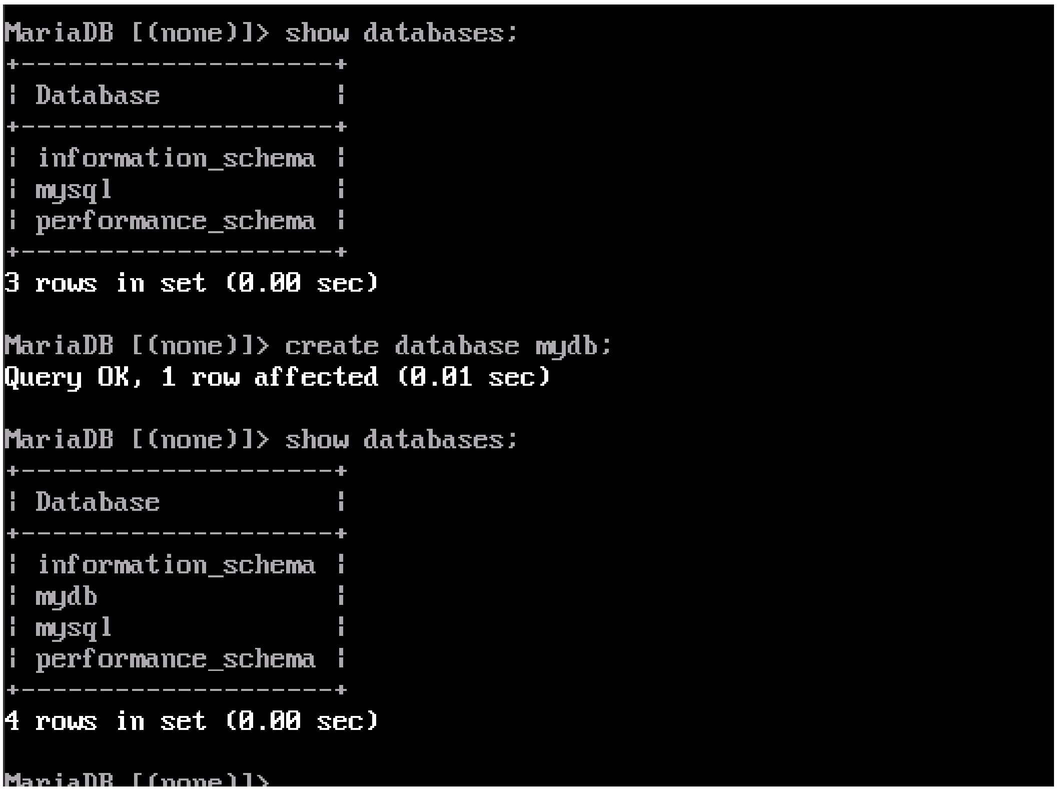


```
[root@[redacted] home]# mysql -h [redacted] -P 3306 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 34567
Server version: 10.5.16-221100-MariaDB-log MairaDB Community Server - (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

5. Create a database, for example, **mydb**.

   ```
   create database mydb;
   ```

Figure 2-30 Creating a database

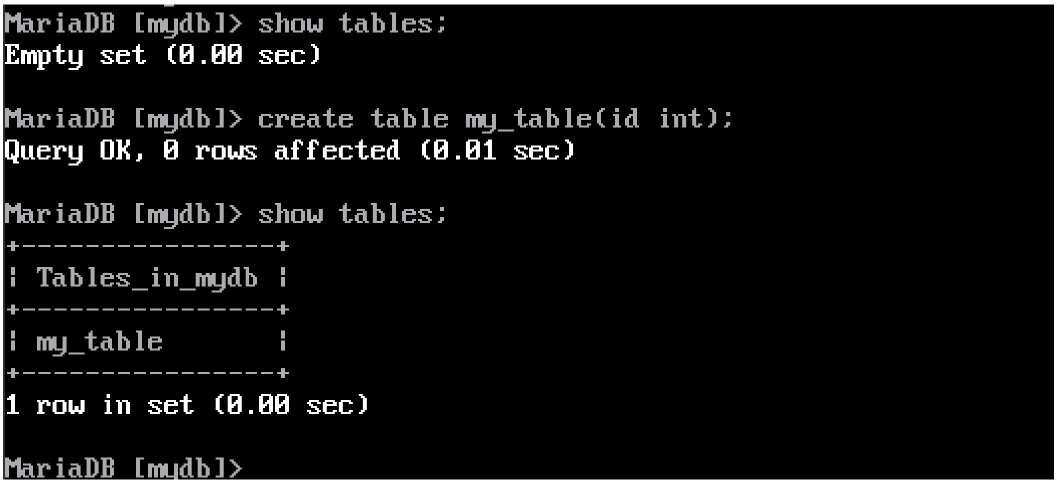


```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
3 rows in set (0.00 sec)

MariaDB [(none)]> create database mydb;
Query OK, 1 row affected (0.01 sec)

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mydb               |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.00 sec)

MariaDB [(none)]>
```

6. Create a table, for example, **my_table**.

```
create table my_table(id int);
```

Figure 2-31 Creating a table



```
MariaDB [mydb]> show tables;
Empty set (0.00 sec)

MariaDB [mydb]> create table my_table(id int);
Query OK, 0 rows affected (0.01 sec)

MariaDB [mydb]> show tables;
+----------------+
| Tables_in_mydb |
+----------------+
| my_table       |
+----------------+
1 row in set (0.00 sec)

MariaDB [mydb]>
```

3 Getting Started with RDS for PostgreSQL

3.1 Step 1: Set Up for RDS

Registering a HUAWEI ID

If you already have a HUAWEI ID, skip this part. If you do not have a HUAWEI ID yet, perform the following steps to create one:

Step 1 Open the **Huawei Cloud website**.

Step 2 Click **Register** and complete the registration as instructed.

After the registration is successful, the system redirects you to your personal information page.

----End

Topping Up Your Account

- For details about RDS for PostgreSQL prices, see **Price Calculator**.
- Before purchasing an RDS for PostgreSQL instance, ensure that your account balance is sufficient. For details about how to top up an account, see **Topping Up an Account**.

Creating an IAM User and Granting Permissions

You can create an IAM user or user group on the Identity and Access Management (IAM) console and grant it specific operation permissions for fine-grained permissions management.

1. **Create a user group and assign permissions** to it.

   Create a user group on the IAM console, and attach the **RDS ReadOnlyAccess** policy to the group.

> 🕮 NOTE
>
> To use some interconnected services, you also need to configure permissions of such services.
>
> For example, to connect to your DB instance through the console, configure the **DAS FullAccess** permission of Data Admin Service (DAS) besides **RDS ReadOnlyAccess**.

2. **Create an IAM user and add it to the user group**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the RDS console by using the created user, and verify that the user only has read permissions for RDS.

   – Choose **Service List** > **Relational Database Service** and click **Buy DB Instance**. If a message appears indicating that you have insufficient permissions to perform the operation, the **RDS ReadOnlyAccess** policy has already been applied.

   – Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **RDS ReadOnlyAccess** policy has already taken effect.

3.2 Step 2: Buy a DB Instance

Scenarios

This section describes how to buy a DB instance on the RDS console.

RDS for PostgreSQL supports the yearly/monthly and pay-per-use billing modes. RDS allows you to tailor your compute resources and storage space to your business needs.

Prerequisites

- You have **registered a Huawei ID and enabled Huawei Cloud services**.

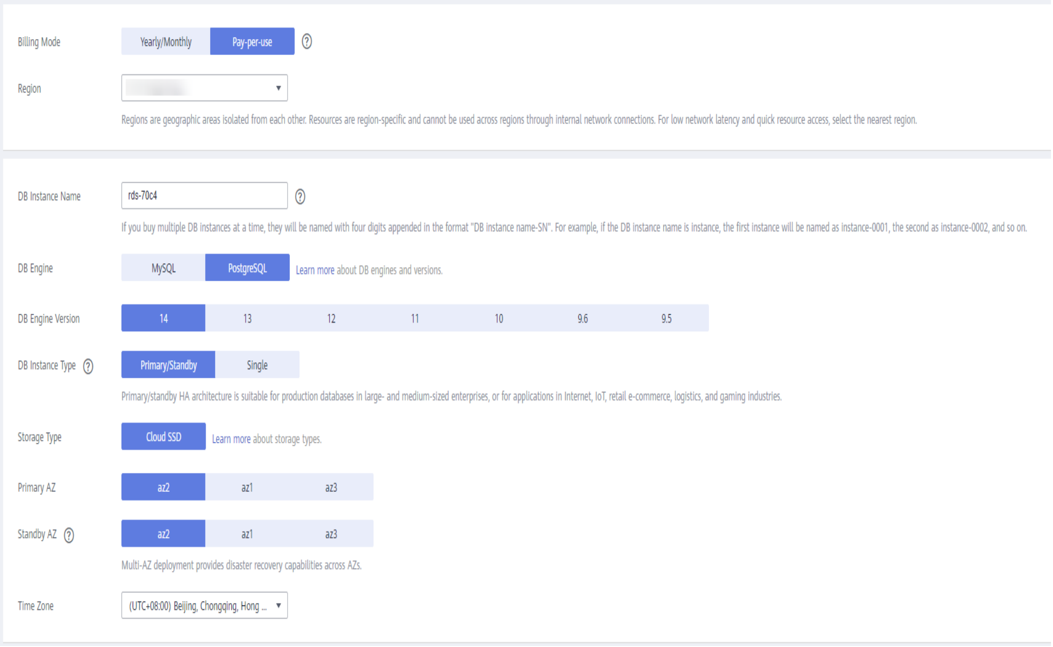
Procedure

Step 1 Go to the **Buy DB Instance** page.

Step 2 On the displayed page, configure information about your DB instance. Then, click **Next**.

- RDS provides the following billing modes:
  – **Yearly/Monthly**: If you select this mode, skip **Step 3** and go to **Step 4**.
  – **Pay-per-use**: If you select this mode, go to **Step 3**.
- Basic information

Figure 3-1 Billing mode and basic information



Billing Mode Yearly/Monthly Pay-per-use

Region

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

DB Instance Name rds-70c4

If you buy multiple DB instances at a time, they will be named with four digits appended in the format "DB instance name-SN". For example, if the DB instance name is instance, the first instance will be named as instance-0001, the second as instance-0002, and so on.

DB Engine MySQL PostgreSQL Learn more about DB engines and versions.

DB Engine Version 14 13 12 11 10 9.6 9.5

DB Instance Type Primary/Standby Single

Primary/standby HA architecture is suitable for production databases in large- and medium-sized enterprises, or for applications in Internet, IoT, retail e-commerce, logistics, and gaming industries.

Storage Type Cloud SSD Learn more about storage types.

Primary AZ az2 az1 az3

Standby AZ az2 az1 az3

Multi-AZ deployment provides disaster recovery capabilities across AZs.

Time Zone (UTC+08:00) Beijing, Chongqing, Hong ...

Table 3-1 Basic information

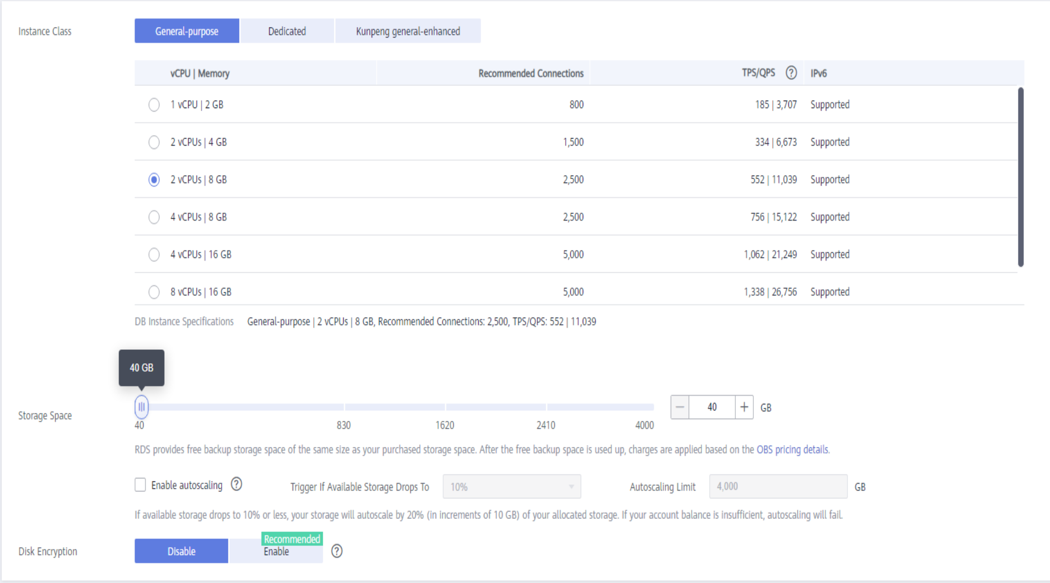
Parameter	Description
Region	Region where your resources are located. **NOTE** Products in different regions cannot communicate with each other through a private network. After a DB instance is created, the region cannot be changed. Therefore, exercise caution when selecting a region.
DB Instance Name	The instance name must start with a letter and consist of 4 to 64 characters. Only letters (case-sensitive), digits, hyphens (-), and underscores (_) are allowed. – If you intend to buy multiple DB instances at a time, the allowed length for each instance name will change. – If you buy multiple DB instances at a time, they will be named *instance-0001*, *instance-0002*, and so on. (*instance* indicates the DB instance name you specify.)
DB Engine	Set to **PostgreSQL**.
DB Engine Version	For details, see **DB Engines and Versions**. Different DB engine versions are supported in different regions. You are advised to select the latest available version because it is more stable, reliable, and secure.

Parameter	Description
DB Instance Type	– **Primary/Standby**: uses an HA architecture with a primary DB instance and a synchronous standby DB instance. It is suitable for production databases of large and medium enterprises in Internet, Internet of Things (IoT), retail e-commerce sales, logistics, gaming, and other sectors. The standby DB instance improves instance reliability and is invisible to you after being created. An AZ is a physical region where resources use independent power supply and networks. AZs are physically isolated but interconnected through an internal network. Some regions support both single AZs and multiple AZs and some only support single AZs. To achieve high reliability, RDS will automatically deploy your primary and standby instances in different physical servers even if you deploy them in the same AZ. If you attempt to create primary/standby DB instances in the same AZ in a Dedicated Computing Cluster (DCC) and there is only one physical server available, the creation will fail. You can deploy primary and standby DB instances in a single AZ or across AZs to achieve failover and high availability. – **Single**: uses a single-node architecture, which is more cost-effective than primary/standby DB instances. It is suitable for development and testing of microsites, and small- and medium-sized enterprises, or for learning about RDS.

Parameter	Description
Storage Type	Determines the DB instance read/write speed. The higher the maximum throughput is, the higher the DB instance read/write speed can be. – **Ultra-high I/O**: supports a maximum throughput of 350 MB/s. – **Cloud SSD**: cloud drives used to decouple storage from compute. – **Extreme SSD**: uses 25GE network and RDMA technologies to provide you with up to 1,000 MB/s throughput per disk and sub-millisecond latency. **NOTE** – The cloud SSD and extreme SSD storage types are supported with general-purpose, dedicated, and Kunpeng general-enhanced DB instances. – If you have purchased the Dedicated Distributed Storage Service (DSS), only the storage type that you have selected when you buy the DSS service is displayed. – The IOPS supported by cloud SSDs depends on the I/O performance of Elastic Volume Service (EVS) disks. For details, see the description about ultra-high I/O in **Disk Types and Performance** of *Elastic Volume Service Service Overview*. – The IOPS supported by extreme SSDs depends on the I/O performance of Elastic Volume Service (EVS) disks. For details, see the description about extreme SSDs in **Disk Types and Performance** of *Elastic Volume Service Service Overview*.
Time Zone	You need to select a time zone for your instance based on the region hosting your instance. You can select a time zone during instance creation and change it later as needed.

- DB instance specifications

Figure 3-2 DB instance specifications



Instance Class: General-purpose | Dedicated | Kunpeng general-enhanced

	vCPU | Memory	Recommended Connections	TPS/QPS	IPv6
○	1 vCPU | 2 GB	800	185 | 3,707	Supported
○	2 vCPUs | 4 GB	1,500	334 | 6,673	Supported
●	2 vCPUs | 8 GB	2,500	552 | 11,039	Supported
○	4 vCPUs | 8 GB	2,500	756 | 15,122	Supported
○	4 vCPUs | 16 GB	5,000	1,062 | 21,249	Supported
○	8 vCPUs | 16 GB	5,000	1,338 | 26,756	Supported

DB Instance Specifications: General-purpose | 2 vCPUs | 8 GB, Recommended Connections: 2,500, TPS/QPS: 552 | 11,039

Storage Space: 40 GB (40 – 4000) GB

RDS provides free backup storage space of the same size as your purchased storage space. After the free backup space is used up, charges are applied based on the OBS pricing details.

□ Enable autoscaling   Trigger If Available Storage Drops To: 10%   Autoscaling Limit: 4,000 GB

If available storage drops to 10% or less, your storage will autoscale by 20% (in increments of 10 GB) of your allocated storage. If your account balance is insufficient, autoscaling will fail.

Disk Encryption: Disable | Enable (Recommended)

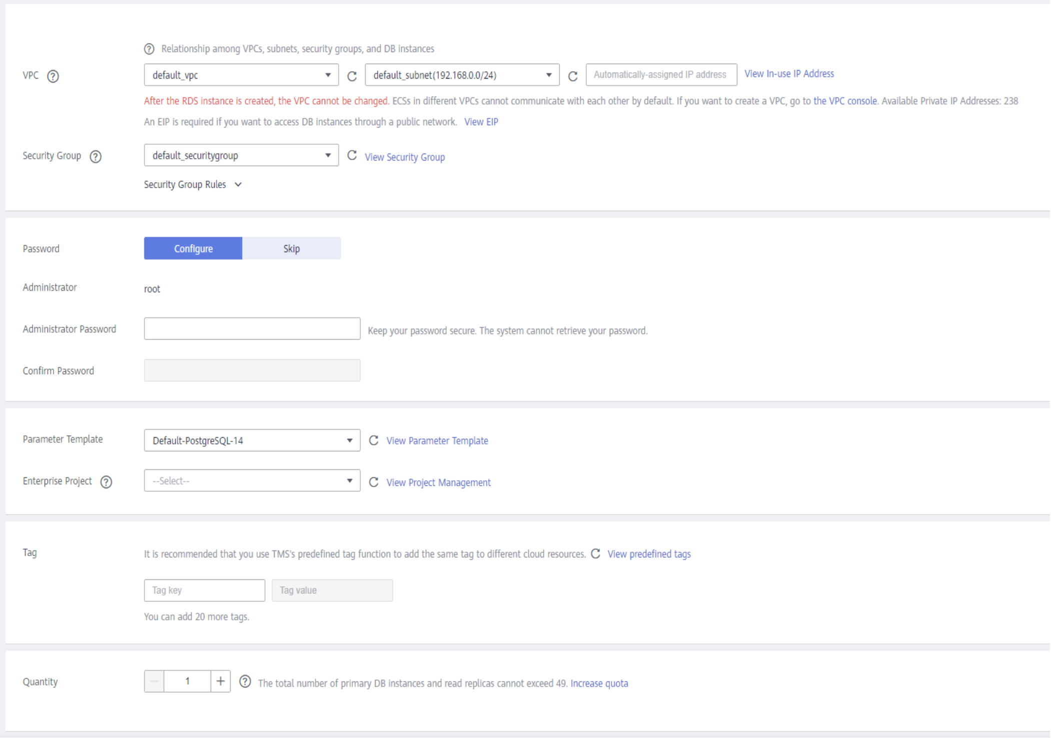
Table 3-2 Instance specifications

Parameter	Description
Instance Class	Refers to the vCPU and memory of a DB instance. Different instance classes support different numbers of database connections and maximum IOPS. After a DB instance is created, you can change its vCPU and memory. For details, see **Changing a DB Instance Class**. **NOTE** Only general-enhanced DB instances are allowed for a DCC.
Resource Type	– **EVS** – **DSS** **NOTE** This option is displayed only when you have purchased the Dedicated Distributed Storage Service (DSS) service.
Storage Pool	Displayed only when you select **DSS** for **Resource Type**. The storage pool is secure because it is physically isolated from other pools.

Parameter	Description
Storage Space (GB)	Contains the file system overhead required for inode, reserved block, and database operation. Storage space can range in size from 40 GB to 4,000 GB and can be scaled up only by a multiple of 10 GB. If the storage type is cloud SSD or extreme SSD, you can enable storage autoscaling. If the available storage drops to a specified threshold, autoscaling is triggered. If you specify a read replica when creating a primary DB instance and enable storage autoscaling for the primary DB instance, storage autoscaling is also enabled for the read replica by default. – **Enable autoscaling**: If you select this option, autoscaling is enabled. – **Trigger If Available Storage Drops To**: If the available storage drops to a specified threshold or 10 GB, autoscaling is triggered. – **Autoscaling Limit**: The default value range is from 40 GB to 4,000 GB. The limit must be no less than the storage of the DB instance. After a DB instance is created, you can scale up its storage space. For details, see **Scaling up Storage Space**.
Disk Encryption	– **Disable**: indicates the encryption function is disabled. – **Enable**: indicates the encryption function is enabled, improving data security but affecting system performance. ■ **Key Name**: indicates the tenant key. Select one from the drop-down list. ■ Click **Create Key** and configure parameters in the displayed dialog box. For more information, see **Creating a Key** in the *Data Encryption Workshop User Guide*. **NOTE** ■ If you enable disk encryption during instance creation, the disk encryption status and the key cannot be changed later. Disk encryption will not encrypt backup data stored in OBS. To enable backup data encryption, contact customer service. ■ If disk encryption or backup data encryption is enabled, keep the key properly. Once the key is disabled, deleted, or frozen, the database will be unavailable and data may not be restored. If disk encryption is enabled but backup data encryption is not enabled, you can **restore data to a new instance from backups**. If both disk encryption and backup data encryption are enabled, data cannot be restored.

- Network and database configuration

Figure 3-3 Network and database configuration



Relationship among VPCs, subnets, security groups, and DB instances

VPC: default_vpc; default_subnet(192.168.0.0/24); Automatically-assigned IP address

After the RDS instance is created, the VPC cannot be changed. ECSs in different VPCs cannot communicate with each other by default. If you want to create a VPC, go to the VPC console. Available Private IP Addresses: 238

An EIP is required if you want to access DB instances through a public network.

Security Group: default_securitygroup

Password: Configure

Administrator: root

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

Confirm Password

Parameter Template: Default-PostgreSQL-14

Enterprise Project: --Select--

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

Tag key, Tag value

You can add 20 more tags.

Quantity: 1

The total number of primary DB instances and read replicas cannot exceed 49.

Table 3-3 Network

Parameter	Description
VPC	A virtual network in which your RDS DB instances are located. A VPC can isolate networks for different workloads. You can select an existing VPC or create a VPC. For details on how to create a VPC, see the "Creating a VPC" section in the *Virtual Private Cloud User Guide*. If no VPC is available, RDS allocates a VPC to you by default. **NOTICE** After a DB instance is created, the VPC cannot be changed.

Parameter	Description
Subnet	Improves network security by providing dedicated network resources that are logically isolated from other networks. Subnets take effect only within an AZ. The Dynamic Host Configuration Protocol (DHCP) function is enabled by default for subnets in which you plan to create RDS DB instances and cannot be disabled. A floating IP address is automatically assigned when you create a DB instance. You can also enter an unused floating IP address in the subnet CIDR block. After the DB instance is created, you can change the floating IP address.
Security Group	Controls the access that traffic has in and out of a DB instance. By default, the security group associated with the DB instance is authorized. In addition, a network **access control list (ACL)** can help control inbound and outbound traffic of subnets in your VPC. Enhances security by controlling access to RDS from other services. You need to add inbound rules to a security group so that you can connect to your DB instance. When creating a DB instance, you can select multiple security groups. For better network performance, you are advised to select no more than five security groups. In such a case, the access rules of all the selected security groups apply on the instance. To use multiple security groups, choose **Service Tickets > Create Service Ticket** in the upper right corner of the management console to apply for the required permissions. If no security group is available, RDS allocates a security group to you by default.

Table 3-4 Database configuration

Parameter	Description
Password	– **Configure** (default setting): Configure a password for your DB instance during the creation process. – **Skip**: Configure a password later after the DB instance is created. **NOTICE** If you select **Skip** for **Password**, you need to reset the password before you can log in to the instance. After a DB instance is created, you can reset the password. For details, see **Resetting the Administrator Password**.
Administrator	The default login name for the database is **root**.

Parameter	Description
Administrator Password	Must consist of 8 to 32 characters and contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters (~ ! @ # $ % ^ * - _ = + ? ,). Enter a strong password and periodically change it for security reasons. If the password you provide is regarded as a weak password by the system, you will be prompted to enter a stronger password. Keep this password secure. The system cannot retrieve it. After a DB instance is created, you can reset this password. For details, see **Resetting the Administrator Password**.
Confirm Password	Must be the same as **Administrator Password**.
Parameter Template	Contains engine configuration values that can be applied to one or more DB instances. If you intend to create primary/ standby DB instances, they use the same parameter template. **NOTICE** If you use a custom parameter template when creating a DB instance, the following specification-related parameters in the custom template are not delivered. Instead, the default values are used. – **maintenance_work_mem** – **shared_buffers** – **max_connections** – **effective_cache_size** You can modify the instance parameters as required after the DB instance is created. For details, see section **Modifying Parameters in a Parameter Template**.
Enterprise Project	If your account has been associated with an enterprise project, select the target project from the **Enterprise Project** drop-down list. For more information about enterprise projects, see ***Enterprise Management User Guide***.

- Tags

Table 3-5 Tags

Parameter	Description
Tag	Tags an RDS DB instance. This parameter is optional. Adding tags to RDS DB instances helps you better identify and manage the DB instances. A maximum of 20 tags can be added for each DB instance. If your organization has configured tag policies for RDS, add tags to DB instances based on the policies. If a tag does not comply with the policies, DB instance creation may fail. Contact your organization administrator to learn more about tag policies. After a DB instance is created, you can view its tag details on the **Tags** page. For details, see **Managing Tags**.

- Purchase period

Table 3-6 Purchase period

Parameter	Description
Required Duration	This option is available only for yearly/monthly DB instances. The system will automatically calculate the configuration fee based on the selected required duration. The longer the required duration is, the larger discount you will enjoy.
Auto-renew	– This option is available only for yearly/monthly DB instances and is not selected by default. – If you select this option, the auto-renew cycle is determined by the selected required duration.
Quantity	RDS supports batch creation of DB instances. If you intend to create primary/standby DB instances and set **Quantity** to **1**, a primary DB instance and a synchronous standby DB instance will be created.

If you have any questions about the price, click **Pricing details** at the bottom of the page.

NOTE

The performance of your DB instance depends on its configurations. Hardware configuration items include the instance specifications, storage type, and storage space.

Step 3 Confirm the specifications for pay-per-use DB instances.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Submit**.

Skip **Step 4** and **Step 5** and go to **Step 6**.

Step 4 Confirm the order for yearly/monthly DB instances.

- If you need to modify your settings, click **Previous**.
- If you do not need to modify your settings, click **Pay Now**.

Step 5 Select a payment method and complete the payment.

NOTE

This operation applies only to the yearly/monthly billing mode.

Step 6 To view and manage your DB instance, go to the **Instances** page.

- When your DB instance is being created, the status is **Creating**. The status changes to **Available** after the instance is created.
- The automated backup policy is enabled by default. You can change it after the DB instance is created. An automated full backup is immediately triggered once your DB instance is created.
- After a DB instance is created, you can enter a description for it.
- The default database port is **5432**. You can change it after a DB instance is created.

  NOTE

  You are advised to change the database port in a timely manner.

  For details, see **Changing a Database Port**.

----End

Related Operations

Creating a DB Instance Using an API

3.3 Step 3: Connect to a DB Instance

3.3.1 Overview

An RDS DB instance can be connected through a private network, Data Admin Service (DAS), or a public network.

Table 3-7 RDS connection methods

Connect Through	IP Address	Scenarios	Description
DAS	No IP address is required. You can connect to your DB instance through DAS on the management console.	DAS enables you to manage databases on a web-based console and provides you with database development, O&M, and intelligent diagnosis to make it easy to use and maintain your databases. The permissions required for connecting to DB instances through DAS are enabled by default.	● Easy to use, secure, advanced, and intelligent ● Recommended
Private network	Floating IP	RDS provides a floating IP address by default. When your applications are deployed on an ECS that is in the same region and VPC as RDS, you are advised to use a floating IP address to connect to the RDS DB instance through the ECS.	● Secure and excellent performance ● Recommended

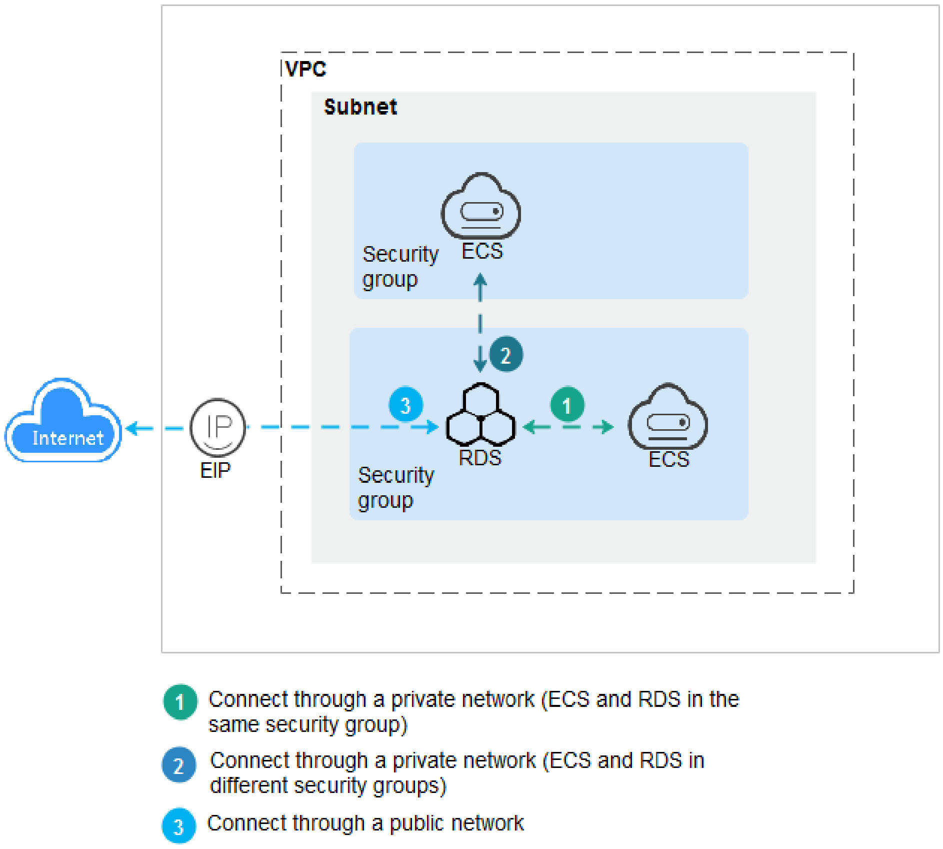
Connect Through	IP Address	Scenarios	Description
Public network	EIP	If you cannot access an RDS DB instance through a floating IP address, bind an EIP to the DB instance and connect the DB instance through the EIP.	● A relatively lower level of security compared to other connection methods ● To achieve a higher transmission rate and security level, you are advised to migrate your applications to an ECS that is in the same VPC as your RDS DB instance and use a floating IP address to access the DB instance. ● You need to purchase an EIP. For details, see **EIP billing details**.

NOTE

- VPC: indicates the Virtual Private Cloud.
- ECS: indicates the Elastic Cloud Server.
- You can log in to DB instances using the DAS service or other database clients.
- If the ECS is in the same VPC as your RDS DB instance, you do not need to apply for an EIP.

Figure 3-4 illustrates the connection over a private network or a public network.

Figure 3-4 DB instance connection



1 Connect through a private network (ECS and RDS in the same security group)

2 Connect through a private network (ECS and RDS in different security groups)

3 Connect through a public network

Connecting to DB Instances Running Other DB Engines

- Connecting to an RDS for MySQL DB Instance
- Connecting to an RDS for SQL Server DB Instance

3.3.2 Connecting to a DB Instance Through DAS (Recommended)

Scenarios

Data Admin Service (DAS) enables you to connect to and manage databases with ease on a web-based console. The permissions required for connecting to DB instances through DAS are enabled by default. Using DAS to connect to your DB instance is recommended, which is more secure and convenient.

Procedure

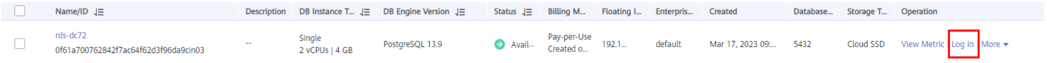
Step 1 Log in to the management console.

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

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

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

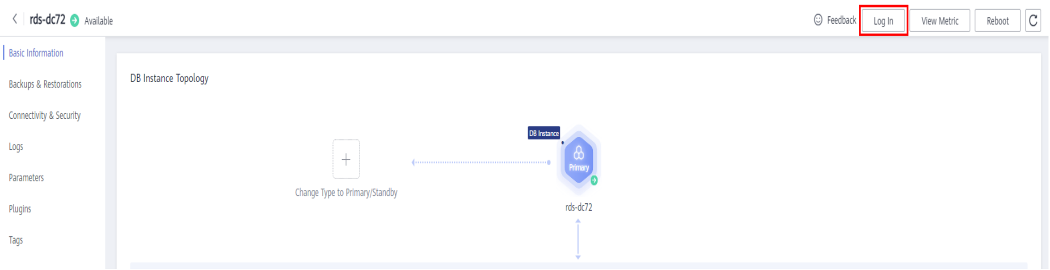
Figure 3-5 Logging in to an instance



□	Name/ID	Description	DB Instance T...	DB Engine Version	Status	Billing M...	Floating I...	Enterpris...	Created	Database...	Storage T...	Operation
□	rds-dc72 0f61a700762842f7ac64f62d3f96da9cin03	--	Single 2 vCPUs | 4 GB	PostgreSQL 13.9	Avail...	Pay-per-Use Created o...	192.1...	default	Mar 17, 2023 09:...	5432	Cloud SSD	View Metric Log In More ▾

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

Figure 3-6 Logging in to an instance



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

----End

FAQ

- **What Should I Do If I Can't Connect to My DB Instance Due to Insufficient Permissions?**
- **What Should I Do If I Can't Connect to My RDS for PostgreSQL Instance?**

Follow-up Operations

After logging in to the DB instance, you can create or migrate databases.

- **Creating a PostgreSQL Database Using an API**
- **Managing PostgreSQL Databases Using DAS**
- **Migration Solution Overview**

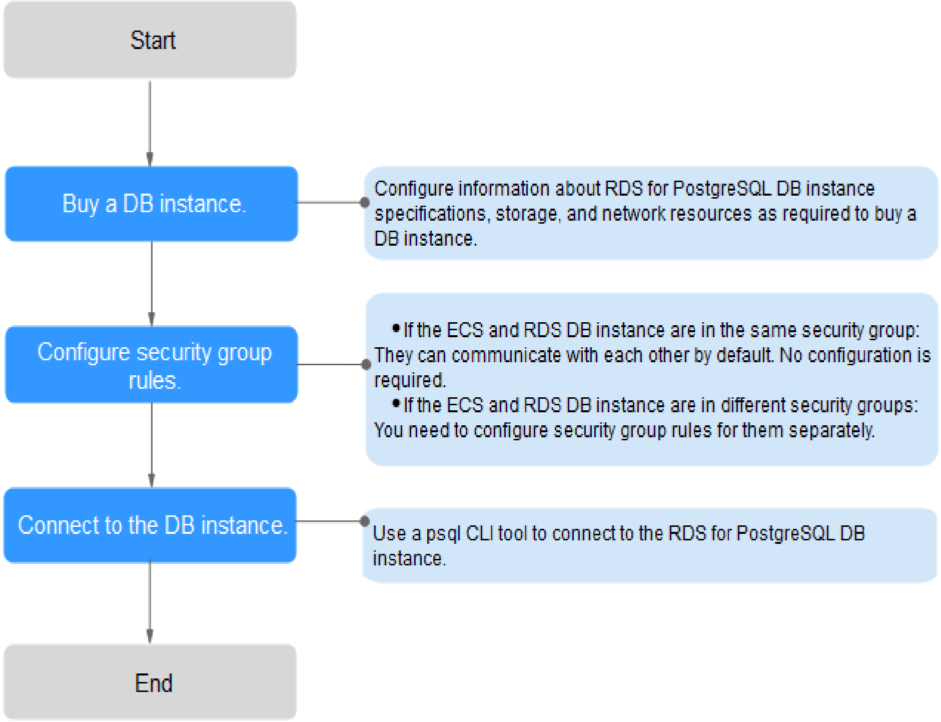
3.3.3 Connecting to a DB Instance Through a Private Network

3.3.3.1 Overview

Process

Figure 3-7 illustrates the process of connecting to an RDS for PostgreSQL DB instance through a private network.

Figure 3-7 Connecting to a DB instance through a private network



Configure information about RDS for PostgreSQL DB instance specifications, storage, and network resources as required to buy a DB instance.

- If the ECS and RDS DB instance are in the same security group: They can communicate with each other by default. No configuration is required.
- If the ECS and RDS DB instance are in different security groups: You need to configure security group rules for them separately.

Use a psql CLI tool to connect to the RDS for PostgreSQL DB instance.

3.3.3.2 Connecting to a DB Instance from a Linux ECS

You can connect to your DB instance using a Linux ECS installed with a PostgreSQL client over a private network.

You can use the PostgreSQL client psql to connect to your DB instance over a Secure Sockets Layer (SSL) connection. SSL encrypts connections to your DB instance, making in-transit data more secure.

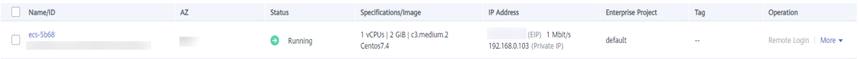
SSL is enabled by default when you create an RDS for PostgreSQL DB instance and cannot be disabled after the instance is created.

Enabling SSL reduces the read-only and read/write performance of your instance by about 20%.

Step 1: Buy an ECS

1. **Log in to the management console** and check whether there is an ECS available.
   - If there is a Linux ECS, go to **3**.
   - If no Linux ECS is available, go to **2**.

   Figure 3-8 ECS

□ Name/ID	AZ	Status	Specifications/Image	IP Address	Enterprise Project	Tag	Operation
□ ecs-5b68 [redacted]	[redacted]	Running	1 vCPUs | 2 GiB | c3.medium.2 Centos7.4	[redacted] (EIP) 1 Mbit/s 192.168.0.103 (Private IP)	default	--	Remote Login | More ▾

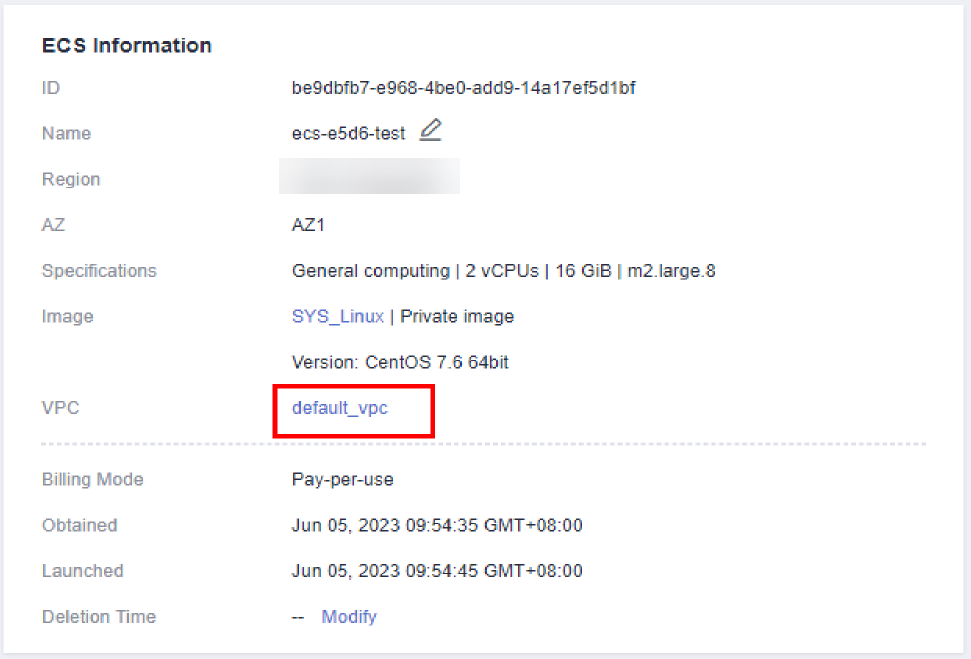
2. Buy an ECS and select Linux (for example, CentOS) as its OS.

   To download a PostgreSQL client to the ECS, bind an EIP to the ECS. The ECS must be in the same region, VPC, and security group as the RDS for PostgreSQL DB instance for mutual communications.

For details about how to purchase a Linux ECS, see "**Purchasing an ECS**" in *Elastic Cloud Server Getting Started*.

3. On the **ECS Information** page, view the region and VPC of the ECS.

Figure 3-9 ECS information

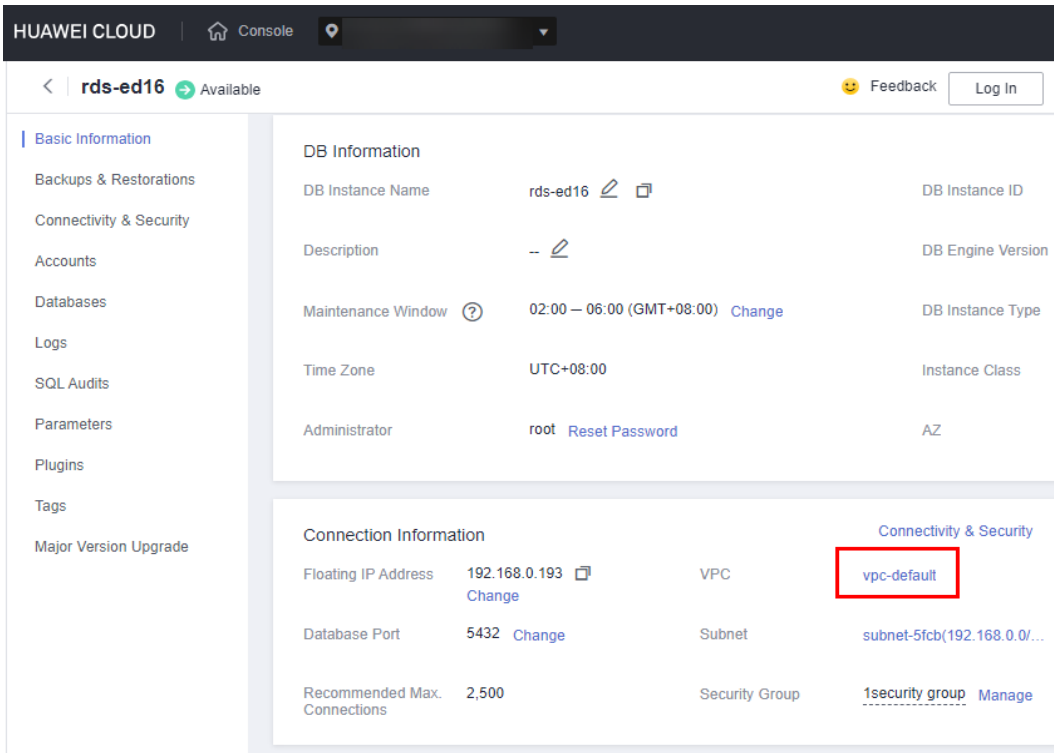


ECS Information

ID	be9dbfb7-e968-4be0-add9-14a17ef5d1bf
Name	ecs-e5d6-test
Region	
AZ	AZ1
Specifications	General computing | 2 vCPUs | 16 GiB | m2.large.8
Image	SYS_Linux | Private image Version: CentOS 7.6 64bit
VPC	default_vpc
Billing Mode	Pay-per-use
Obtained	Jun 05, 2023 09:54:35 GMT+08:00
Launched	Jun 05, 2023 09:54:45 GMT+08:00
Deletion Time	-- Modify

4. On the **Basic Information** page of the RDS for PostgreSQL instance, view the region and VPC of the DB instance.

Figure 3-10 DB instance information



DB Information

DB Instance Name rds-ed16

Description --

Maintenance Window 02:00 — 06:00 (GMT+08:00)

Time Zone UTC+08:00

Administrator root

DB Instance ID

DB Engine Version

DB Instance Type

Instance Class

AZ

Connection Information

Floating IP Address 192.168.0.193

VPC vpc-default

Database Port 5432

Subnet subnet-5fcb(192.168.0.0/...

Recommended Max. Connections 2,500

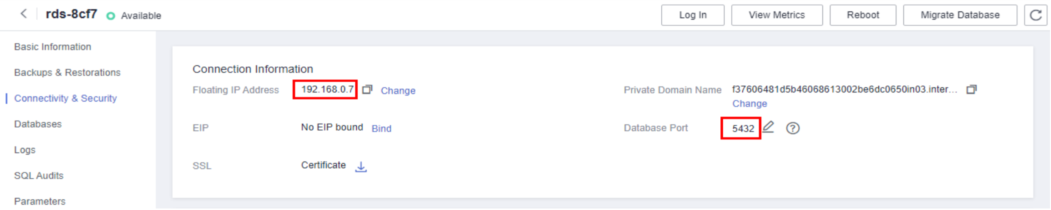
Security Group 1security group

5. Check whether the ECS and RDS for PostgreSQL instance are in the same region and VPC.
   - If yes, go to **Step 2: Test Connectivity and Install a PostgreSQL Client**.
   - If they are not in the same region, purchase another ECS or DB instance. The ECS and DB instance in different regions cannot communicate with each other. To reduce network latency, deploy your DB instance in the region nearest to your workloads.
   - If the ECS and DB instance are in different VPCs, change the VPC of the ECS to that of the DB instance. For details, see **Changing a VPC**.

Step 2: Test Connectivity and Install a PostgreSQL Client

1. Log in to the ECS. For details, see **Login Using VNC** in the *Elastic Cloud Server User Guide*.
2. On the **Instances** page, click the DB instance name.
3. Choose **Connectivity & Security** from the navigation pane. In the **Connection Information** area, obtain the floating IP address and database port of the DB instance.

Figure 3-11 Connection information



Connection Information

Floating IP Address 192.168.0.7

EIP No EIP bound

SSL Certificate

Private Domain Name f37606481d5b46068613002be6dc0650in03.inter...

Database Port 5432

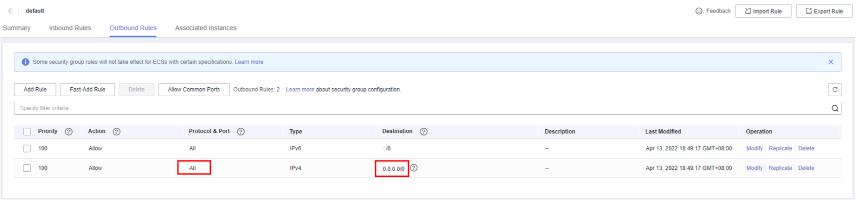
4. On the ECS, check whether the floating IP address and database port of the DB instance can be connected.

   telnet *192.168.0.7 5432*

   – If yes, network connectivity is normal.
   – If no, check the security group rules.

     ■ If in the security group of the ECS, there is no outbound rule with **Destination** set to **0.0.0.0/0** and **Protocol & Port** set to **All**, add an outbound rule for the floating IP address and port of the DB instance.

     Figure 3-12 ECS security group



Some security group rules will not take effect for ECSs with certain specifications. Learn more

Outbound Rules: 2 Learn more about security group configuration.

Specify filter criteria.

Priority	Action	Protocol & Port	Type	Destination	Description	Last Modified	Operation
100	Allow	All	IPv6	::/0	--	Apr 13, 2022 18:49:17 GMT+08:00	Modify | Replicate | Delete
100	Allow	All	IPv4	0.0.0.0/0	--	Apr 13, 2022 18:49:17 GMT+08:00	Modify | Replicate | Delete

     ■ If in the security group of the DB instance, there is no inbound rule allowing the access from the private IP address and port of the ECS, add an inbound rule for the private IP address and port of the ECS. For details, see **Configuring Security Group Rules**.

5. Open the **client installation** page.

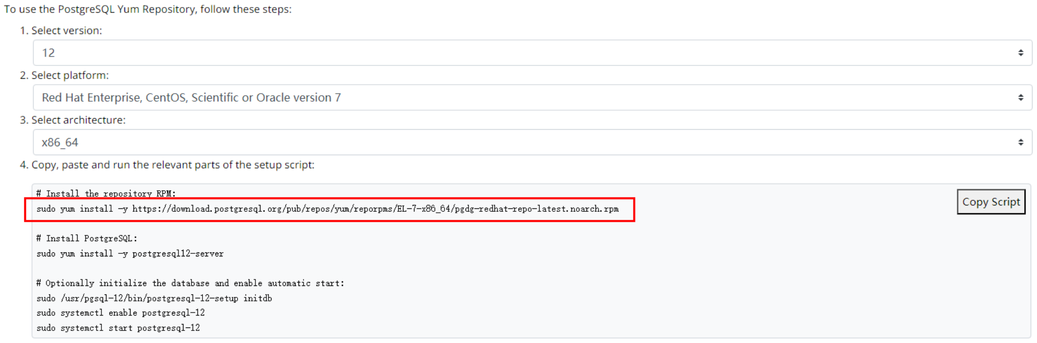
   PostgreSQL provides **client installation methods** for different OSs on its official website.

   The following describes how to install a PostgreSQL 12 client in CentOS.

6. Select a DB engine version, OS, and OS architecture, and run the following commands on the ECS to install a PostgreSQL client:

```
sudo yum install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm
```

Figure 3-13 Installing a client



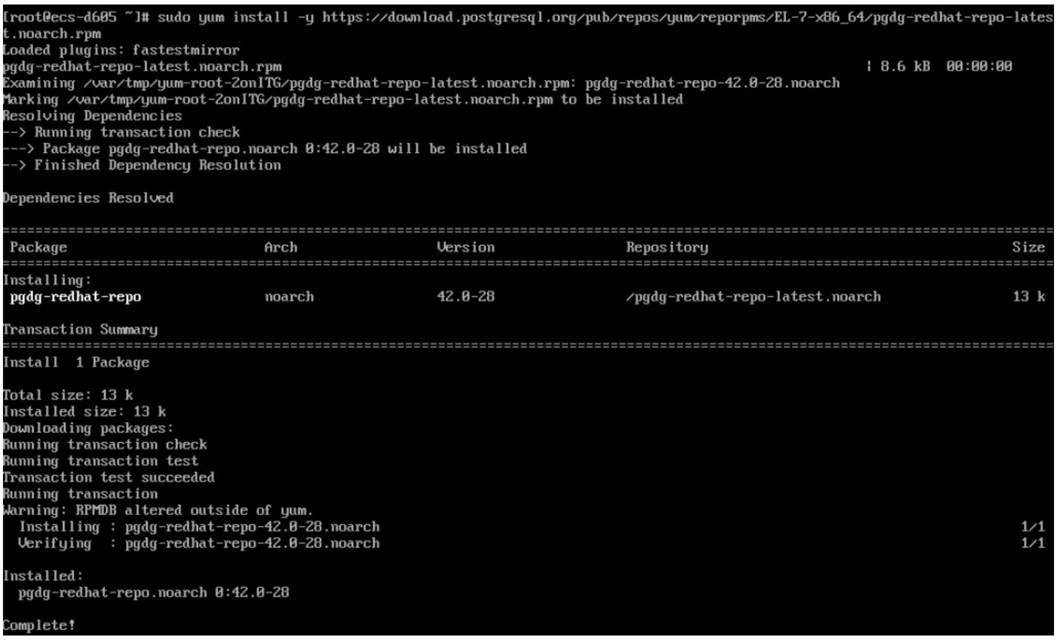
To use the PostgreSQL Yum Repository, follow these steps:

1. Select version:
   12
2. Select platform:
   Red Hat Enterprise, CentOS, Scientific or Oracle version 7
3. Select architecture:
   x86_64
4. Copy, paste and run the relevant parts of the setup script:

```
# Install the repository RPM:
sudo yum install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm

# Install PostgreSQL:
sudo yum install -y postgresql12-server

# Optionally initialize the database and enable automatic start:
sudo /usr/pgsql-12/bin/postgresql-12-setup initdb
sudo systemctl enable postgresql-12
sudo systemctl start postgresql-12
```

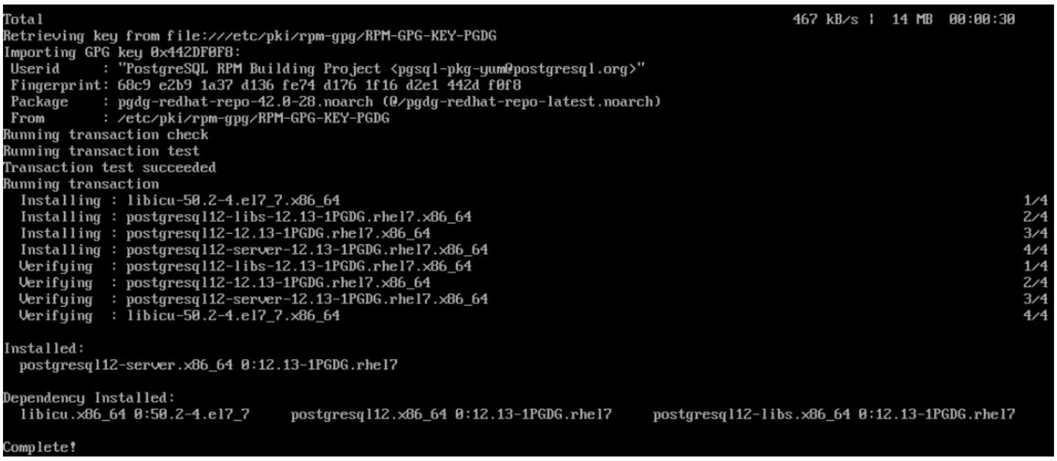
   – Select a DB engine version that is consistent with that of your RDS for PostgreSQL instance.
   – Select an OS that is consistent with that of the ECS.
   – Select an OS architecture that is consistent with that of the ECS.

Figure 3-14 Installing the RPM package



```
[root@ecs-d605 ~]# sudo yum install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/pgdg-redhat-repo-lates
t.noarch.rpm
Loaded plugins: fastestmirror
pgdg-redhat-repo-latest.noarch.rpm                                                                  | 8.6 kB  00:00:00
Examining /var/tmp/yum-root-2onITG/pgdg-redhat-repo-latest.noarch.rpm: pgdg-redhat-repo-42.0-28.noarch
Marking /var/tmp/yum-root-2onITG/pgdg-redhat-repo-latest.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package pgdg-redhat-repo.noarch 0:42.0-28 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================================
 Package                       Arch                 Version                 Repository                                   Size
================================================================================================================================
Installing:
 pgdg-redhat-repo              noarch               42.0-28                 /pgdg-redhat-repo-latest.noarch              13 k

Transaction Summary
================================================================================================================================
Install  1 Package

Total size: 13 k
Installed size: 13 k
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Warning: RPMDB altered outside of yum.
  Installing : pgdg-redhat-repo-42.0-28.noarch                                                                            1/1
  Verifying  : pgdg-redhat-repo-42.0-28.noarch                                                                            1/1

Installed:
  pgdg-redhat-repo.noarch 0:42.0-28

Complete!
```

Figure 3-15 Client installed

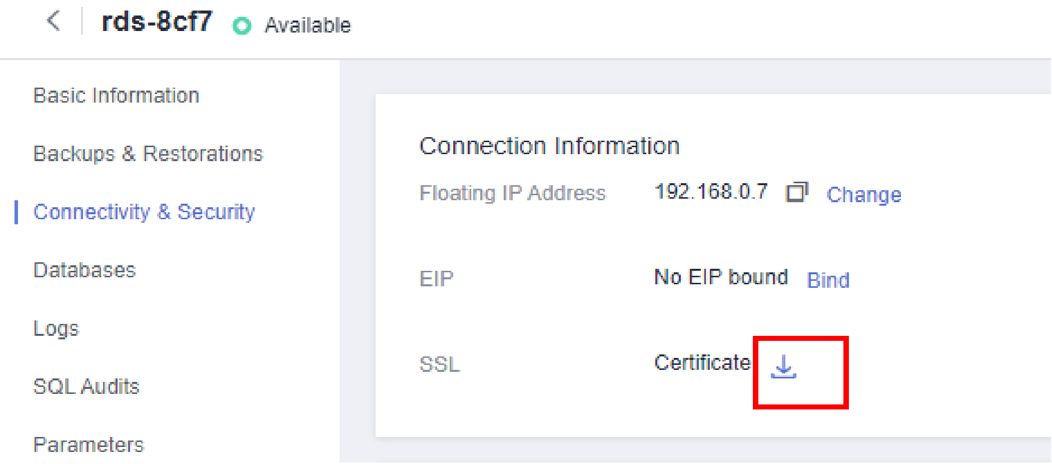


```
Total                                                                                        467 kB/s |  14 MB  00:00:30
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
Importing GPG key 0x442DF0F8:
 Userid     : "PostgreSQL RPM Building Project <pgsql-pkg-yum@postgresql.org>"
 Fingerprint: 68c9 e2b9 1a37 d136 fe74 d176 1f16 d2e1 442d f0f8
 Package    : pgdg-redhat-repo-42.0-28.noarch (@/pgdg-redhat-repo-latest.noarch)
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : libicu-50.2-4.el7_7.x86_64                                                                                 1/4
  Installing : postgresql12-libs-12.13-1PGDG.rhel7.x86_64                                                                 2/4
  Installing : postgresql12-12.13-1PGDG.rhel7.x86_64                                                                      3/4
  Installing : postgresql12-server-12.13-1PGDG.rhel7.x86_64                                                               4/4
  Verifying  : postgresql12-libs-12.13-1PGDG.rhel7.x86_64                                                                 1/4
  Verifying  : postgresql12-12.13-1PGDG.rhel7.x86_64                                                                      2/4
  Verifying  : postgresql12-server-12.13-1PGDG.rhel7.x86_64                                                               3/4
  Verifying  : libicu-50.2-4.el7_7.x86_64                                                                                 4/4

Installed:
  postgresql12-server.x86_64 0:12.13-1PGDG.rhel7

Dependency Installed:
  libicu.x86_64 0:50.2-4.el7_7     postgresql12.x86_64 0:12.13-1PGDG.rhel7     postgresql12-libs.x86_64 0:12.13-1PGDG.rhel7

Complete!
```

Step 3: Connect to the DB Instance Using Commands (SSL Connection)

1. On the **Instances** page, click the DB instance name.
2. In the navigation pane, choose **Connectivity & Security**.
3. In the **Connection Information** area, click ⤓ next to the **SSL** field to download **Certificate Download.zip**, and extract the root certificate **ca.pem** and bundle **ca-bundle.pem** from the package.

Figure 3-16 Downloading a certificate



4. Upload **ca.pem** to the ECS.

NOTE

- TLS v1.2 or later is recommended. Versions earlier than TLS v1.2 have security risks.
- The recommended protocol algorithm is EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:EDH+aRSA+AESGCM:EDH+aDSS+AESGCM:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!SRP:!RC4. Using other options have security risks.
- **ca-bundle.pem** contains both the new certificate provided as of April 2017 and the old certificate.
- Both **ca.pem** and **ca-bundle.pem** can be used for SSL connections because **ca-bundle.pem** contains **ca.pem**.

5. Run the following command on the ECS to connect to the DB instance:

psql --no-readline -h *<host>* **-p** *<port>* **"dbname=***<database>* **user=***<user>* **sslmode=verify-ca sslrootcert=***<ca-file-directory>***"**

Example:

psql --no-readline -h 192.168.0.7 -p 5432 "dbname=postgres user=root sslmode=verify-ca sslrootcert=/root/ca.pem"

Table 3-8 Parameter description

Parameter	Description
<host>	Floating IP address obtained in 3.
<port>	Database port obtained in 3. The default value is **5432**.
<database>	Name of the database to be connected. The default database name is **postgres**.
<user>	Administrator account **root**.
<ca-file-directory>	Directory of the CA certificate used for the SSL connection. This certificate should be stored in the directory where the command is executed.
sslmode	SSL connection mode. Set it to **verify-ca** to use a CA to check whether the service is trusted.

6. Enter the password of the database account as prompted.

```
Password:
```

If the following information is displayed, the connection is successful.

```
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression:
off)
```

Follow-up Operations

After logging in to the DB instance, you can create or migrate databases.

- **Creating a PostgreSQL Database Using an API**
- **Managing PostgreSQL Databases Using DAS**
- **Migration Solution Overview**

3.3.3.3 Configuring Security Group Rules

Scenarios

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

Before you can connect to your DB instance, you need to create security group rules to enable specific IP addresses and ports to access your RDS instance.

First check whether the ECS and RDS DB instance are in the same security group.

- If they are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to **Connecting to a DB Instance from a Linux ECS**.
- If they are in different security groups, configure security group rules for them, separately.
  - RDS DB instance: Configure an **inbound rule** for the security group with which the RDS DB instance is associated.
  - ECS: The default security group rule allows all outgoing data packets. In this case, you do not need to configure a security group rule for the ECS. If not all outbound traffic is allowed in the security group, you need to configure an **outbound rule** for the ECS.

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

For details about the requirements of security group rules, see the **Adding a Security Group Rule** section in the *Virtual Private Cloud User Guide*.

Precautions

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.

- By default, you can create a maximum of 100 security groups in your cloud account.

- By default, you can add up to 50 security group rules to a security group.
- One RDS DB instance can be associated with multiple security groups, and one security group can be associated with multiple RDS DB instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for a security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

> **NOTE**
>
> To ensure the security of your data and DB instances, you are advised to use the principle of least privilege for database access. Change the database port (default value: **5432**), and set the IP address to the remote server's address or any IP address in the remote server's smallest subnet to control the access from the remote server.
>
> The default value of **Source** is **0.0.0.0/0**, indicating that RDS DB instances in the security group can be accessed from any IP address.

For details about the requirements of security group rules, see the **Adding a Security Group Rule** section in the *Virtual Private Cloud User Guide*.

Procedure

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

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

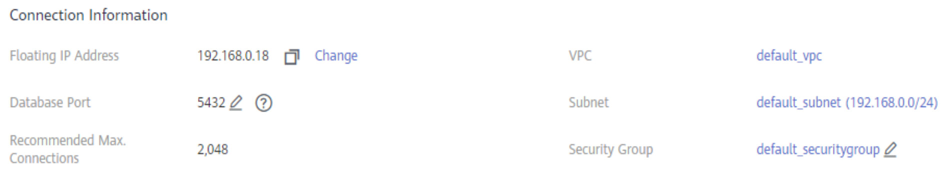
Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

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

Step 5 Configure security group rules.

In the **Connection Information** area, click the security group.

Figure 3-17 Connection information



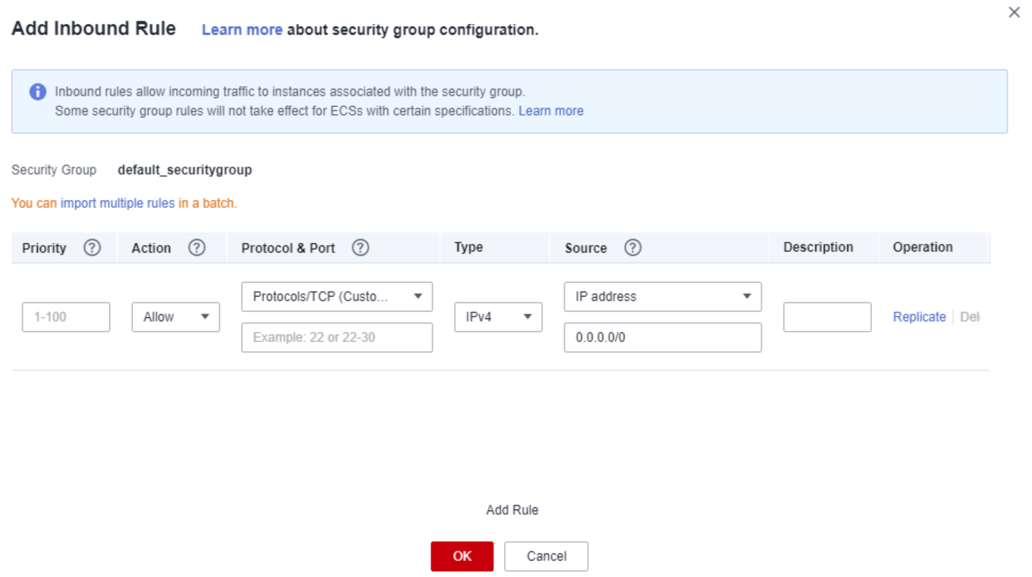
Connection Information

Floating IP Address	192.168.0.18 Change	VPC	default_vpc
Database Port	5432	Subnet	default_subnet (192.168.0.0/24)
Recommended Max. Connections	2,048	Security Group	default_securitygroup

Step 6 On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

You can click **+** to add more inbound rules.

Figure 3-18 Adding an inbound rule



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.
Some security group rules will not take effect for ECSs with certain specifications. Learn more

Security Group default_securitygroup

You can import multiple rules in a batch.

Priority	Action	Protocol & Port	Type	Source	Description	Operation
1-100	Allow	Protocols/TCP (Custo... Example: 22 or 22-30	IPv4	IP address 0.0.0.0/0		Replicate | Del

Table 3-9 Inbound rule parameter description

Parameter	Description	Example Value
Priority	Security group rule priority. Value range: 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	Security group rule actions. A rule with a deny action overrides another with an allow action if the two rules have the same priority.	Allow
Protocol & Port	**Protocol**: network protocol. Available options: **All**, **TCP**, **UDP**, **ICMP**, or **GRE**.	TCP
	Port: the port over which the traffic can reach your DB instance. RDS for PostgreSQL instances can use database ports 2100 to 9500.	5432
Type	IP address type. Currently, only IPv4 is supported.	IPv4

Parameter	Description	Example Value
Source	Source address. It can be a single IP address, an IP address group, or a security group to allow access from them to your DB instance. Examples: ● Single IP address: 192.168.10.10/32 (IPv4 address) ● IP address segment: 192.168.1.0/24 (IPv4 address segment) ● All IP addresses: 0.0.0.0/0 (any IPv4 address) ● Security group: sg-abc ● IP address group: ipGroup-test	0.0.0.0/0
Description	Supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (<) or (>).	-

----End

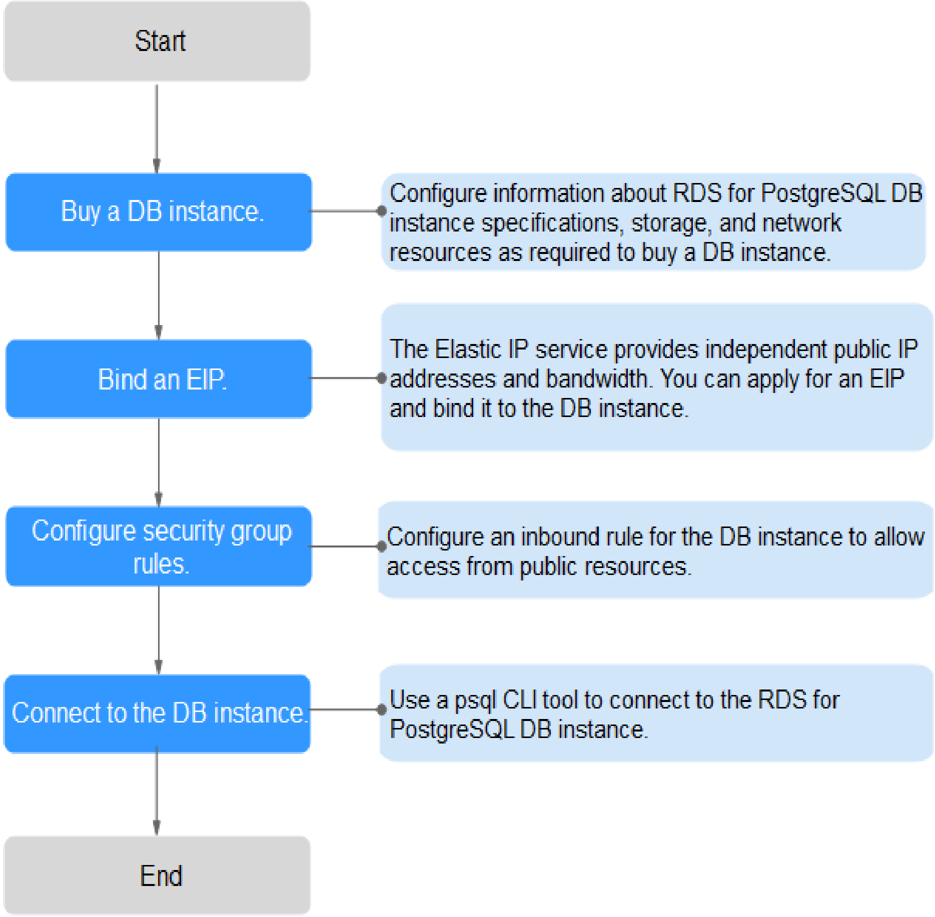
3.3.4 Connecting to a DB Instance Through a Public Network

3.3.4.1 Overview

Process

Figure 3-19 illustrates the process of connecting to an RDS for PostgreSQL DB instance through a public network.

Figure 3-19 Connecting to a DB instance through a public network


Start
Buy a DB instance.
Configure information about RDS for PostgreSQL DB instance specifications, storage, and network resources as required to buy a DB instance.
Bind an EIP.
The Elastic IP service provides independent public IP addresses and bandwidth. You can apply for an EIP and bind it to the DB instance.
Configure security group rules.
Configure an inbound rule for the DB instance to allow access from public resources.
Connect to the DB instance.
Use a psql CLI tool to connect to the RDS for PostgreSQL DB instance.
End

3.3.4.2 Binding an EIP

Scenarios

You can bind an EIP to a DB instance for public accessibility and can unbind the EIP from the DB instance as required.

Precautions

- You need to configure security groups and enable specific IP addresses and ports to access the target DB instance. Before accessing the DB instance, add an individual IP address or an IP address range that will access the DB instance to the inbound rule. For details, see section **Configuring Security Group Rules**.
- Traffic generated by the public network is charged. You can unbind the EIP from your DB instance when the EIP is no longer used.

Binding an EIP

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

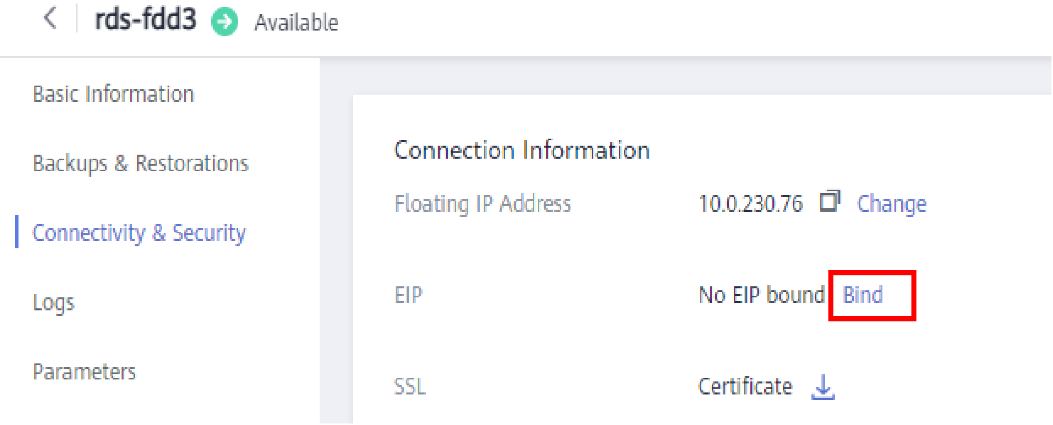
Step 2 Click 📍 in the upper left corner and select a region and a project.

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

Step 4 On the **Instances** page, click the target DB instance.

Step 5 In the navigation pane on the left, choose **Connectivity & Security**. In the **Connection Information** area, click **Bind** next to the **EIP** field.

Figure 3-20 Connectivity & Security



Connection Information

Floating IP Address 10.0.230.76 Change

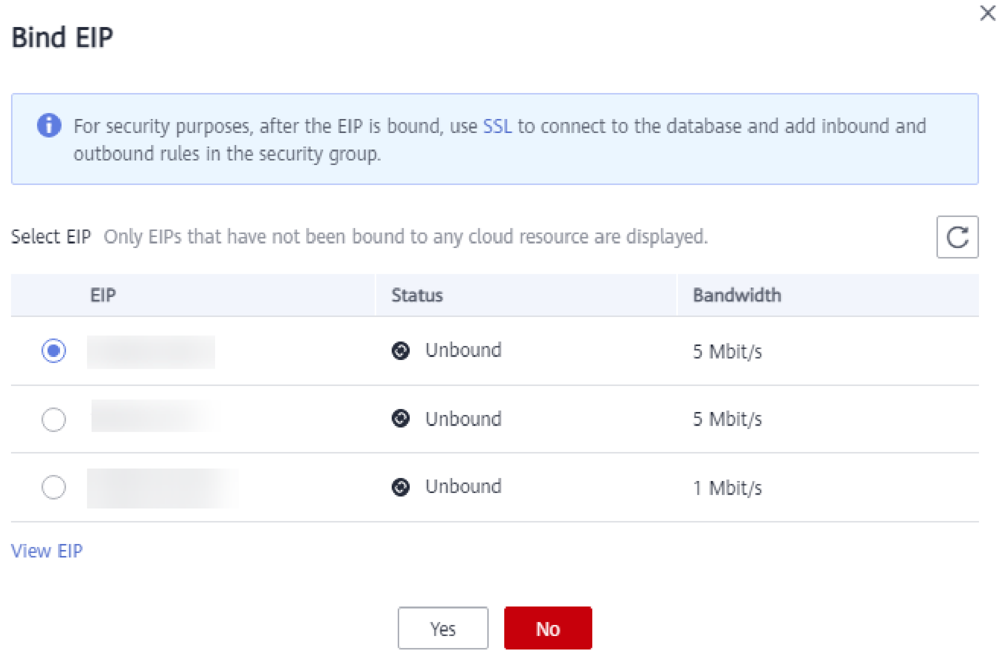
EIP No EIP bound Bind

SSL Certificate

Step 6 In the displayed dialog box, select an EIP and click **Yes**.

If no available EIPs are displayed, click **View EIP** to obtain an EIP.

Figure 3-21 Selecting an EIP



Bind EIP

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

Select EIP Only EIPs that have not been bound to any cloud resource are displayed.

	EIP	Status	Bandwidth
●	[redacted]	Unbound	5 Mbit/s
○	[redacted]	Unbound	5 Mbit/s
○	[redacted]	Unbound	1 Mbit/s

Step 7 On the **EIPs** page, view the EIP that has been bound to the DB instance.

You can also view the progress and result of binding an EIP to a DB instance on the **Task Center** page.

----End

3.3.4.3 Connecting to a DB Instance from a Linux ECS

You can connect to your DB instance using a Linux ECS installed with a PostgreSQL client over a public network.

You can use the PostgreSQL client psql to connect to your DB instance over a Secure Sockets Layer (SSL) connection. SSL encrypts connections to your DB instance, making in-transit data more secure.

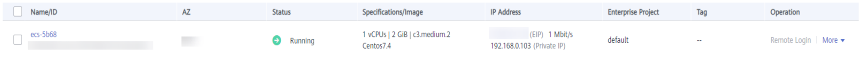
SSL is enabled by default when you create an RDS for PostgreSQL DB instance and cannot be disabled after the instance is created.

Enabling SSL reduces the read-only and read/write performance of your instance by about 20%.

Step 1: Buy an ECS

1. **Log in to the management console** and check whether there is an ECS available.
   - If there is a Linux ECS, go to **3**.
   - If no Linux ECS is available, go to **2**.

   Figure 3-22 ECS

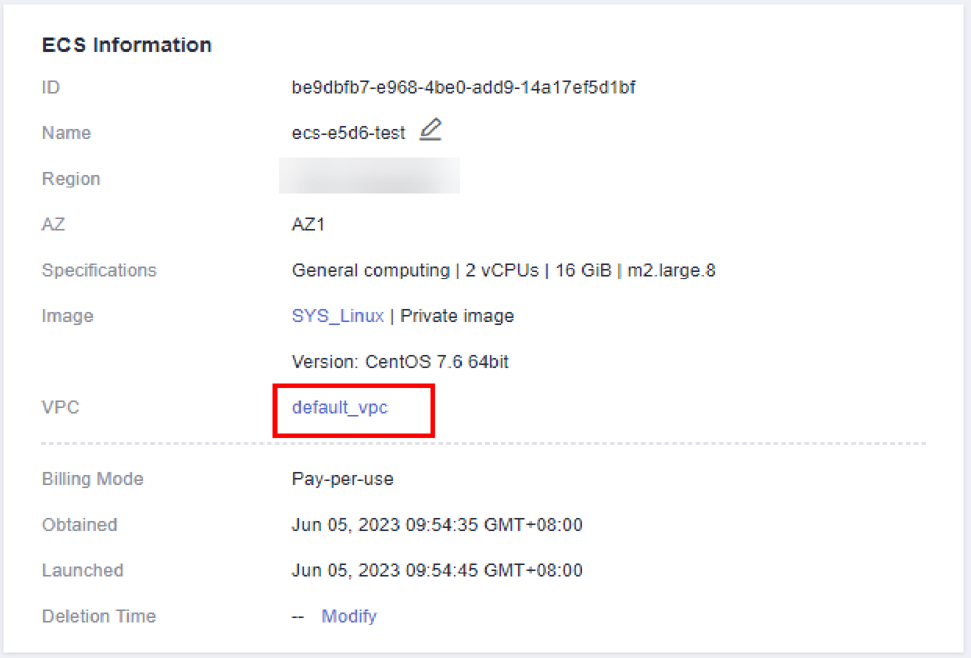
□	Name/ID	AZ	Status	Specifications/Image	IP Address	Enterprise Project	Tag	Operation
□	ecs-5b68 [redacted]	[redacted]	Running	1 vCPUs | 2 GiB | c3.medium.2 Centos7.4	[redacted] (EIP) 1 Mbit/s 192.168.0.103 (Private IP)	default	--	Remote Login | More ▾

2. Buy an ECS and select Linux (for example, CentOS) as its OS.

   To download a PostgreSQL client to the ECS, bind an EIP to the ECS.

   For details about how to purchase a Linux ECS, see "**Purchasing an ECS**" in *Elastic Cloud Server Getting Started*.
3. On the **ECS Information** page, view the region and VPC of the ECS.

Figure 3-23 ECS information

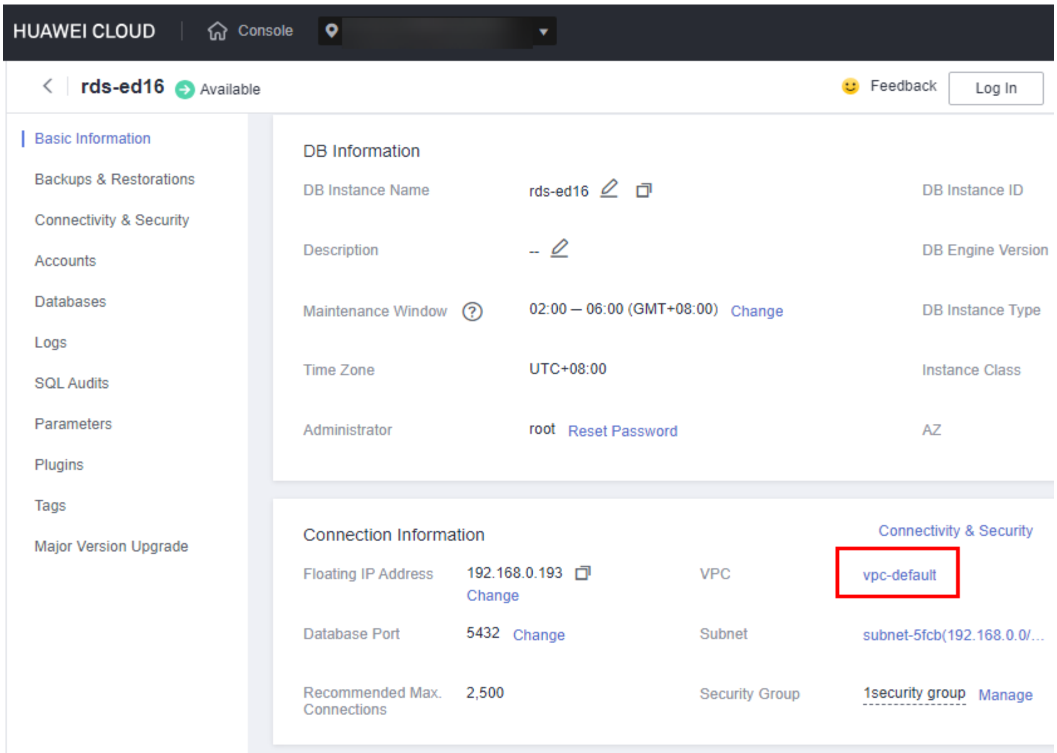


ECS Information

ID	be9dbfb7-e968-4be0-add9-14a17ef5d1bf
Name	ecs-e5d6-test
Region	[redacted]
AZ	AZ1
Specifications	General computing | 2 vCPUs | 16 GiB | m2.large.8
Image	SYS_Linux | Private image Version: CentOS 7.6 64bit
VPC	default_vpc
Billing Mode	Pay-per-use
Obtained	Jun 05, 2023 09:54:35 GMT+08:00
Launched	Jun 05, 2023 09:54:45 GMT+08:00
Deletion Time	-- Modify

4. On the **Basic Information** page of the RDS for PostgreSQL instance, view the region and VPC of the DB instance.

Figure 3-24 DB instance information



DB Information

DB Instance Name	rds-ed16	DB Instance ID
Description	--	DB Engine Version
Maintenance Window	02:00 — 06:00 (GMT+08:00) Change	DB Instance Type
Time Zone	UTC+08:00	Instance Class
Administrator	root Reset Password	AZ

Connection Information — Connectivity & Security

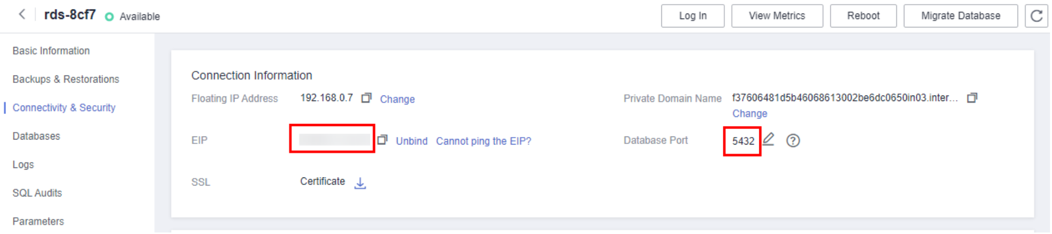
Floating IP Address	192.168.0.193 Change	VPC	vpc-default
Database Port	5432 Change	Subnet	subnet-5fcb(192.168.0.0/...
Recommended Max. Connections	2,500	Security Group	1security group Manage

Step 2: Test Connectivity and Install a PostgreSQL Client

1. Log in to the ECS. For details, see **Login Using VNC** in the *Elastic Cloud Server User Guide*.

2. On the **Instances** page, click the DB instance name.
3. Choose **Connectivity & Security** from the navigation pane. In the **Connection Information** area, obtain the EIP and database port of the DB instance.

Figure 3-25 Connection information



Connection Information

Floating IP Address 192.168.0.7

Private Domain Name f37606481d5b46068613002be6dc0650in03.inter...

EIP [redacted]

Database Port 5432

SSL Certificate

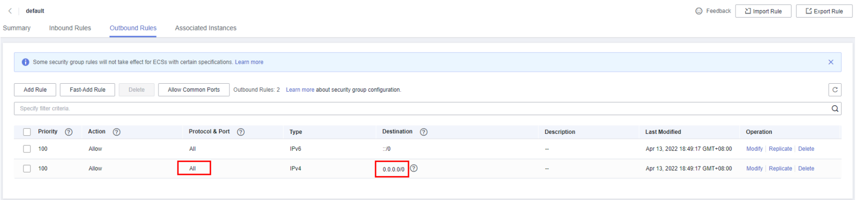
If no EIP has been bound to the DB instance, see **Binding an EIP**.

4. On the ECS, check whether the EIP and database port of the DB instance can be connected.

   telnet *EIP 3306*

   – If yes, network connectivity is normal.
   – If no, check the security group rules.
     ■ If in the security group of the ECS, there is no outbound rule with **Destination** set to **0.0.0.0/0** and **Protocol & Port** set to **All**, add an outbound rule for the EIP and port of the DB instance.

Figure 3-26 ECS security group



Some security group rules will not take effect for ECSs with certain specifications. Learn more

Outbound Rules: 2 Learn more about security group configuration.

Specify filter criteria.

Priority	Action	Protocol & Port	Type	Destination	Description	Last Modified	Operation
100	Allow	All	IPv6	::/0	--	Apr 13, 2022 18:49:17 GMT+08:00	Modify | Replicate | Delete
100	Allow	All	IPv4	0.0.0.0/0	--	Apr 13, 2022 18:49:17 GMT+08:00	Modify | Replicate | Delete

     ■ If in the security group of the DB instance, there is no inbound rule allowing the access from the private IP address and port of the ECS, add an inbound rule for the private IP address and port of the ECS. For details, see **Configuring Security Group Rules**.

5. Open the **client installation** page.

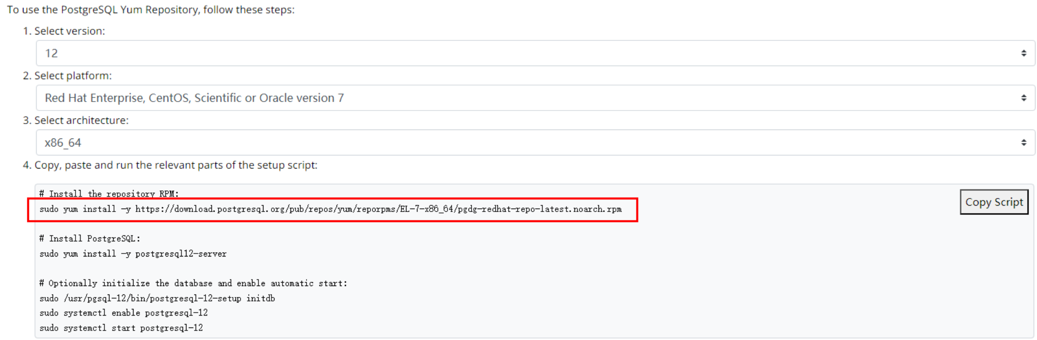
   PostgreSQL provides **client installation methods** for different OSs on its official website.

   The following describes how to install a PostgreSQL 12 client in CentOS.

6. Select a DB engine version, OS, and OS architecture, and run the following commands on the ECS to install a PostgreSQL client:

```
sudo yum install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm
```

Figure 3-27 Installing a client



To use the PostgreSQL Yum Repository, follow these steps:

1. Select version:

   12

2. Select platform:

   Red Hat Enterprise, CentOS, Scientific or Oracle version 7

3. Select architecture:

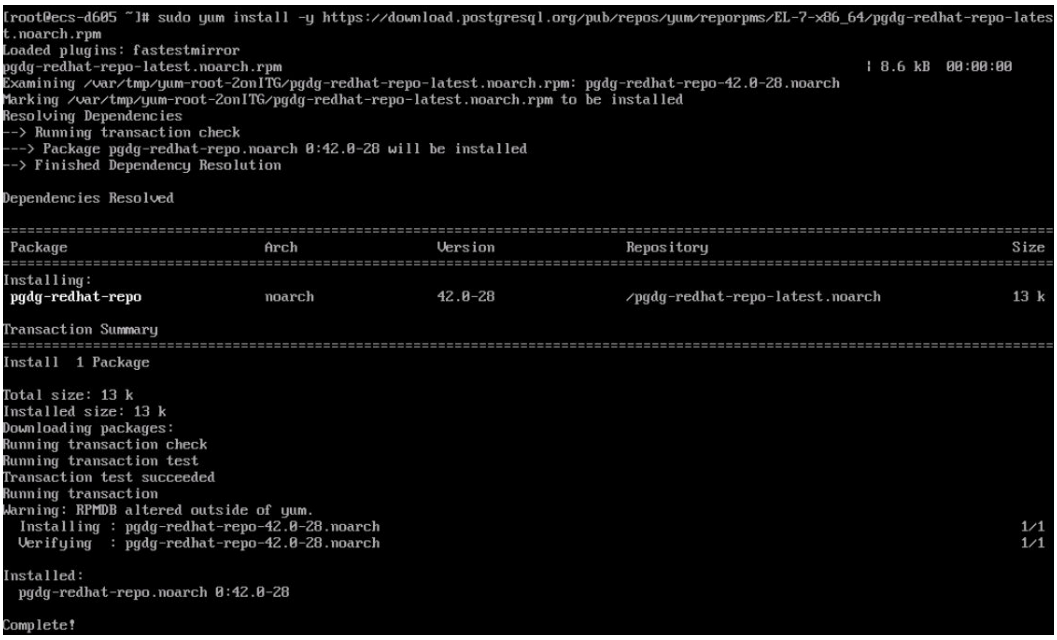
   x86_64

4. Copy, paste and run the relevant parts of the setup script:

```
# Install the repository RPM:
sudo yum install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/pgdg-redhat-repo-latest.noarch.rpm

# Install PostgreSQL:
sudo yum install -y postgresql12-server

# Optionally initialize the database and enable automatic start:
sudo /usr/pgsql-12/bin/postgresql-12-setup initdb
sudo systemctl enable postgresql-12
sudo systemctl start postgresql-12
```

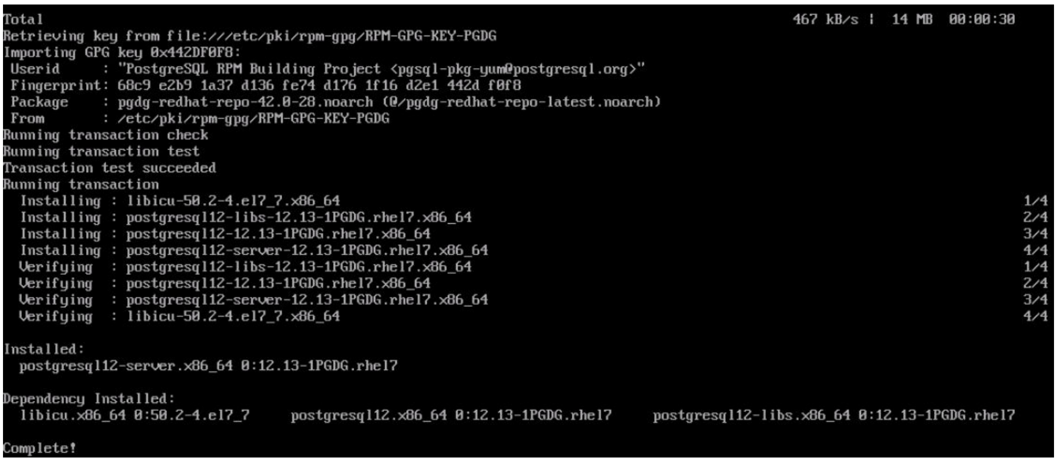
- Select a DB engine version that is consistent with that of your RDS for PostgreSQL instance.
- Select an OS that is consistent with that of the ECS.
- Select an OS architecture that is consistent with that of the ECS.

Figure 3-28 Installing the RPM package



```
[root@ecs-d605 ~]# sudo yum install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/pgdg-redhat-repo-lates
t.noarch.rpm
Loaded plugins: fastestmirror
pgdg-redhat-repo-latest.noarch.rpm                                                             | 8.6 kB  00:00:00
Examining /var/tmp/yum-root-2onITG/pgdg-redhat-repo-latest.noarch.rpm: pgdg-redhat-repo-42.0-28.noarch
Marking /var/tmp/yum-root-2onITG/pgdg-redhat-repo-latest.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package pgdg-redhat-repo.noarch 0:42.0-28 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================================
 Package                         Arch                  Version                 Repository                               Size
================================================================================================================================
Installing:
 pgdg-redhat-repo                noarch                42.0-28                 /pgdg-redhat-repo-latest.noarch          13 k

Transaction Summary
================================================================================================================================
Install  1 Package

Total size: 13 k
Installed size: 13 k
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Warning: RPMDB altered outside of yum.
  Installing : pgdg-redhat-repo-42.0-28.noarch                                                                              1/1
  Verifying  : pgdg-redhat-repo-42.0-28.noarch                                                                              1/1

Installed:
  pgdg-redhat-repo.noarch 0:42.0-28

Complete!
```

Figure 3-29 Client installed

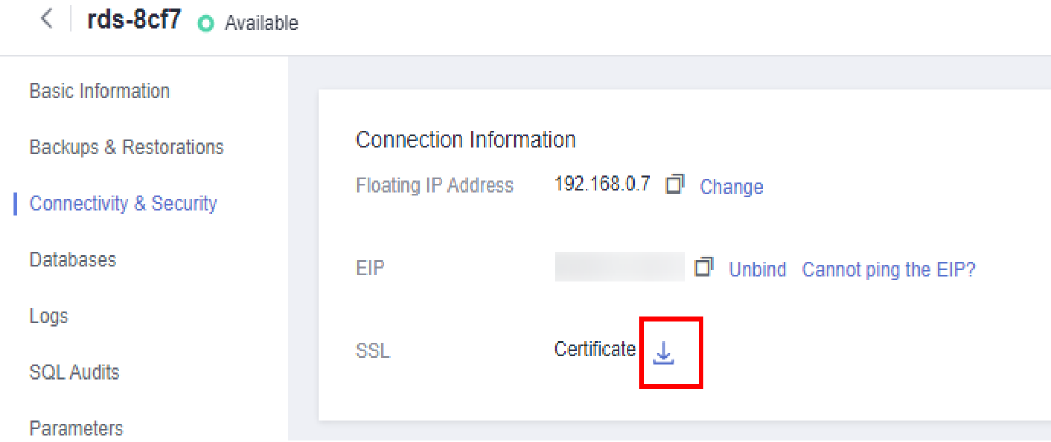


```
Total                                                              467 kB/s |  14 MB  00:00:30
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
Importing GPG key 0x442DF0F8:
 Userid     : "PostgreSQL RPM Building Project <pgsql-pkg-yum@postgresql.org>"
 Fingerprint: 68c9 e2b9 1a37 d136 fe74 d176 1f16 d2e1 442d f0f8
 Package    : pgdg-redhat-repo-42.0-28.noarch (@/pgdg-redhat-repo-latest.noarch)
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-PGDG
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : libicu-50.2-4.el7_7.x86_64                                                        1/4
  Installing : postgresql12-libs-12.13-1PGDG.rhel7.x86_64                                        2/4
  Installing : postgresql12-12.13-1PGDG.rhel7.x86_64                                             3/4
  Installing : postgresql12-server-12.13-1PGDG.rhel7.x86_64                                      4/4
  Verifying  : postgresql12-libs-12.13-1PGDG.rhel7.x86_64                                        1/4
  Verifying  : postgresql12-12.13-1PGDG.rhel7.x86_64                                             2/4
  Verifying  : postgresql12-server-12.13-1PGDG.rhel7.x86_64                                      3/4
  Verifying  : libicu-50.2-4.el7_7.x86_64                                                        4/4

Installed:
  postgresql12-server.x86_64 0:12.13-1PGDG.rhel7

Dependency Installed:
  libicu.x86_64 0:50.2-4.el7_7     postgresql12.x86_64 0:12.13-1PGDG.rhel7     postgresql12-libs.x86_64 0:12.13-1PGDG.rhel7

Complete!
```

Step 3: Connect to the DB Instance Using Commands (SSL Connection)

1. On the **Instances** page, click the DB instance name.
2. In the navigation pane, choose **Connectivity & Security**.
3. In the **Connection Information** area, click ⤓ next to the **SSL** field to download **Certificate Download.zip**, and extract the root certificate **ca.pem** and bundle **ca-bundle.pem** from the package.

Figure 3-30 Downloading a certificate



Connection Information

Floating IP Address 192.168.0.7

EIP [redacted]

SSL Certificate ⤓

4. Upload **ca.pem** to the ECS.

NOTE

- TLS v1.2 or later is recommended. Versions earlier than TLS v1.2 have security risks.
- The recommended protocol algorithm is EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:EDH+aRSA+AESGCM:EDH+aDSS+AESGCM:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!SRP:!RC4. Using other options have security risks.
- **ca-bundle.pem** contains both the new certificate provided as of April 2017 and the old certificate.
- Both **ca.pem** and **ca-bundle.pem** can be used for SSL connections because **ca-bundle.pem** contains **ca.pem**.

5. Run the following command on the ECS to connect to the DB instance:

psql --no-readline -h *<host>* **-p** *<port>* **"dbname=***<database>* **user=***<user>* **sslmode=verify-ca sslrootcert=***<ca-file-directory>***"**

Example:

psql --no-readline -h 192.168.0.44 -p 5432 "dbname=postgres user=root sslmode=verify-ca sslrootcert=/root/ca.pem"

Table 3-10 Parameter description

Parameter	Description
<host>	EIP obtained in 3.
<port>	Database port obtained in 3. The default value is **5432**.
<database>	Name of the database to be connected. The default database name is **postgres**.
<user>	Administrator account **root**.
<ca-file-directory>	Directory of the CA certificate used for the SSL connection. This certificate should be stored in the directory where the command is executed.
sslmode	SSL connection mode. Set it to **verify-ca** to use a CA to check whether the service is trusted.

6. Enter the password of the database account as prompted.

```
Password:
```

If the following information is displayed, the connection is successful.

```
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
```

Follow-up Operations

After logging in to the DB instance, you can create or migrate databases.

- **Creating a PostgreSQL Database Using an API**
- **Managing PostgreSQL Databases Using DAS**
- **Migration Solution Overview**

3.3.4.4 Configuring Security Group Rules

Scenarios

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

This section describes how to create a security group to enable specific IP addresses and ports to access RDS.

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

Precautions

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are deployed in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.

- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS DB instance can be associated with multiple security groups, and one security group can be associated with multiple RDS DB instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for each security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

NOTE

> To ensure the security of your data and DB instances, you are advised to use the principle of least privilege for database access. Change the database port (default value: **5432**), and set the IP address to the remote server's address or any IP address in the remote server's smallest subnet to control the access from the remote server.
>
> The default value of **Source** is **0.0.0.0/0**, indicating that RDS DB instances in the security group can be accessed from any IP address.

For details about the requirements of security group rules, see the **Adding a Security Group Rule** section in the *Virtual Private Cloud User Guide*.

Procedure

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

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

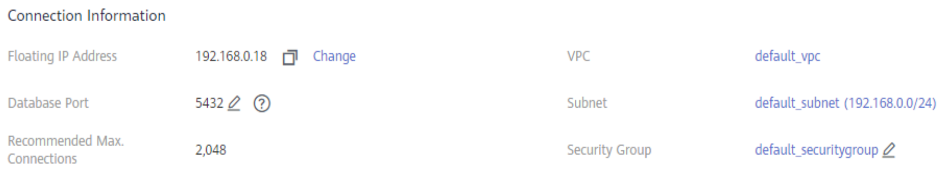
Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

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

Step 5 Configure security group rules.

In the **Connection Information** area, click the security group.

Figure 3-31 Connection information



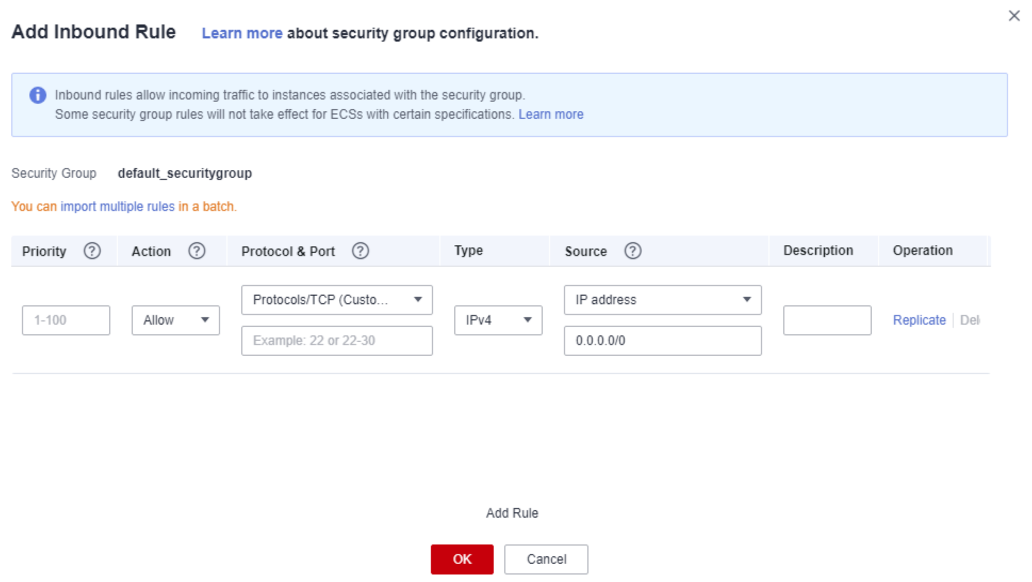
Connection Information

Floating IP Address	192.168.0.18 Change	VPC	default_vpc
Database Port	5432	Subnet	default_subnet (192.168.0.0/24)
Recommended Max. Connections	2,048	Security Group	default_securitygroup

Step 6 On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

You can click **+** to add more inbound rules.

Figure 3-32 Adding an inbound rule



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.
Some security group rules will not take effect for ECSs with certain specifications. Learn more

Security Group default_securitygroup

You can import multiple rules in a batch.

Priority	Action	Protocol & Port	Type	Source	Description	Operation
1-100	Allow	Protocols/TCP (Custo... Example: 22 or 22-30	IPv4	IP address 0.0.0.0/0		Replicate | Del

Table 3-11 Inbound rule parameter description

Parameter	Description	Example Value
Priority	Security group rule priority. Value range: 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	Security group rule actions. A rule with a deny action overrides another with an allow action if the two rules have the same priority.	Allow
Protocol & Port	**Protocol**: network protocol. Available options: **All**, **TCP**, **UDP**, **ICMP**, or **GRE**.	TCP
	Port: the port over which the traffic can reach your DB instance. RDS for PostgreSQL instances can use database ports 2100 to 9500.	5432
Type	IP address type. Currently, only IPv4 is supported.	IPv4

Parameter	Description	Example Value
Source	Source address. It can be a single IP address, an IP address group, or a security group to allow access from them to your DB instance. Examples: ● Single IP address: 192.168.10.10/32 (IPv4 address) ● IP address segment: 192.168.1.0/24 (IPv4 address segment) ● All IP addresses: 0.0.0.0/0 (any IPv4 address) ● Security group: sg-abc ● IP address group: ipGroup-test	0.0.0.0/0
Description	Supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (<) or (>).	-

----End

3.4 Example: Buy and Connect to an RDS for PostgreSQL DB Instance

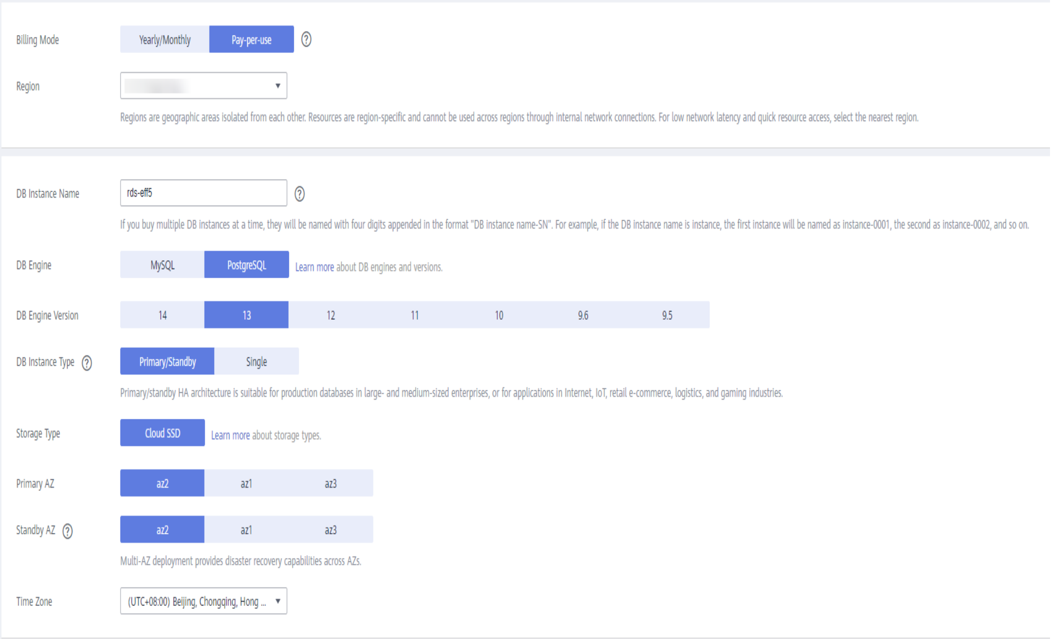
This example illustrates how to purchase an RDS for PostgreSQL instance and how to connect to it using DAS.

- **Step 1: Create an RDS for PostgreSQL Instance**
- **Step 2: Connect to the RDS for PostgreSQL Instance**

Step 1: Create an RDS for PostgreSQL Instance

1. Go to the **Buy DB Instance** page.
2. Configure the instance information and click **Next**.

Figure 3-33 Selecting a billing mode, DB engine, storage type, and instance type



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

Region:

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

DB Instance Name: rds-eff5

If you buy multiple DB instances at a time, they will be named with four digits appended in the format "DB instance name-SN". For example, if the DB instance name is instance, the first instance will be named as instance-0001, the second as instance-0002, and so on.

DB Engine: MySQL [✓ PostgreSQL] Learn more about DB engines and versions.

DB Engine Version: 14 [✓ 13] 12 11 10 9.6 9.5

DB Instance Type: [✓ Primary/Standby] Single

Primary/standby HA architecture is suitable for production databases in large- and medium-sized enterprises, or for applications in Internet, IoT, retail e-commerce, logistics, and gaming industries.

Storage Type: [✓ Cloud SSD] Learn more about storage types.

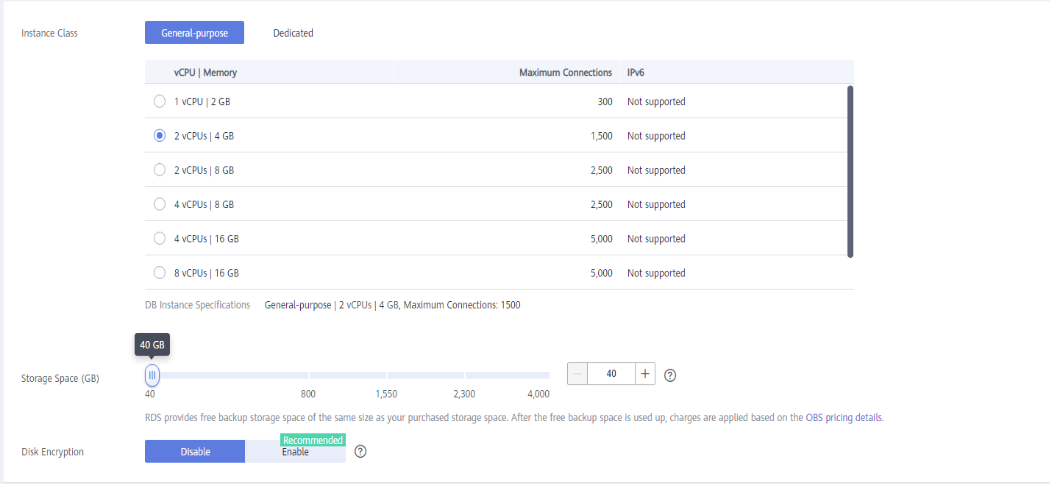
Primary AZ: [✓ az2] az1 az3

Standby AZ: [✓ az2] az1 az3

Multi-AZ deployment provides disaster recovery capabilities across AZs.

Time Zone: (UTC+08:00) Beijing, Chongqing, Hong ...

Figure 3-34 Selecting an instance class



Instance Class: [✓ General-purpose] Dedicated

	vCPU | Memory	Maximum Connections	IPv6
○	1 vCPU | 2 GB	300	Not supported
●	2 vCPUs | 4 GB	1,500	Not supported
○	2 vCPUs | 8 GB	2,500	Not supported
○	4 vCPUs | 8 GB	2,500	Not supported
○	4 vCPUs | 16 GB	5,000	Not supported
○	8 vCPUs | 16 GB	5,000	Not supported

DB Instance Specifications: General-purpose | 2 vCPUs | 4 GB, Maximum Connections: 1500

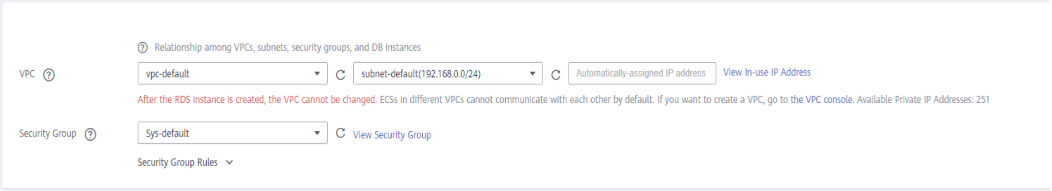
Storage Space (GB): 40 GB

40

RDS provides free backup storage space of the same size as your purchased storage space. After the free backup space is used up, charges are applied based on the OBS pricing details.

Disk Encryption: [✓ Disable] Enable Recommended

Figure 3-35 Configuring network information



Relationship among VPCs, subnets, security groups, and DB instances

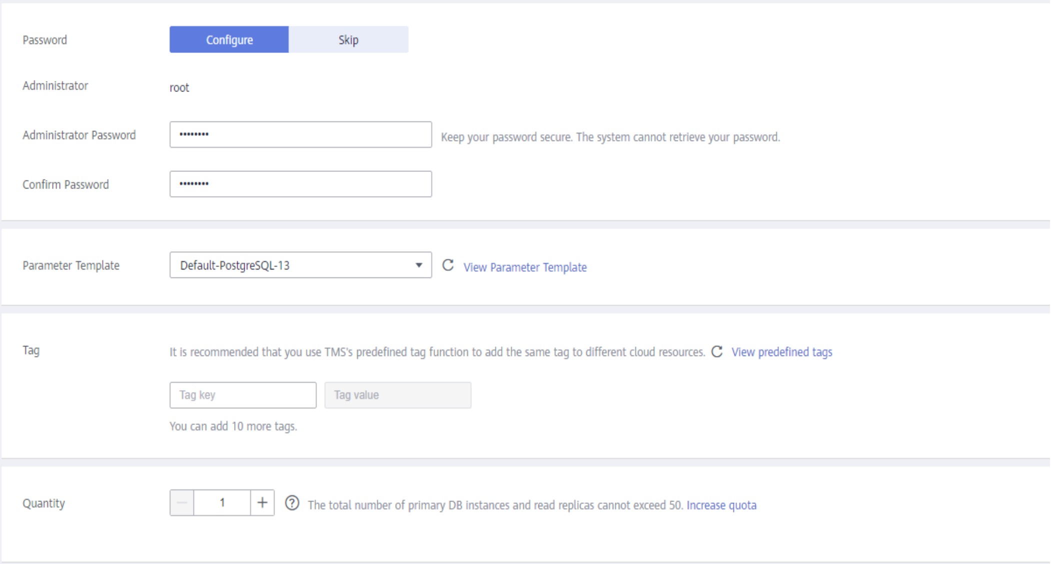
VPC: vpc-default, subnet-default(192.168.0.0/24), Automatically-assigned IP address, View In-use IP Address

After the RDS instance is created, the VPC cannot be changed. ECSs in different VPCs cannot communicate with each other by default. If you want to create a VPC, go to the VPC console. Available Private IP Addresses: 251

Security Group: Sys-default, View Security Group

Security Group Rules

Figure 3-36 Setting a password



Password: Configure

Administrator: root

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

Confirm Password: ········

Parameter Template: Default-PostgreSQL-13 View Parameter Template

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

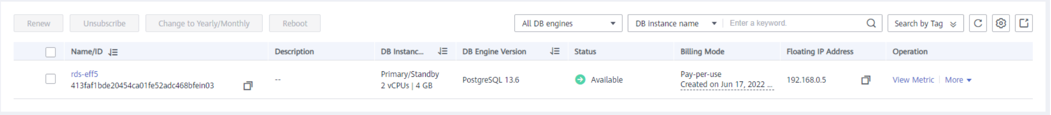
Tag key | Tag value

You can add 10 more tags.

Quantity: 1 The total number of primary DB instances and read replicas cannot exceed 50. Increase quota

3. View the purchased RDS instance.

Figure 3-37 Instance successfully purchased

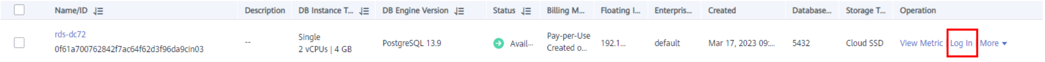


	Name/ID	Description	DB Instanc...	DB Engine Version	Status	Billing Mode	Floating IP Address	Operation
□	rds-eff5 413faf1bde20454ca01fe52adc468bfein03	--	Primary/Standby 2 vCPUs | 4 GB	PostgreSQL 13.6	Available	Pay-per-use Created on Jun 17, 2022 ...	192.168.0.5	View Metric | More

Step 2: Connect to the RDS for PostgreSQL Instance

1. Click **Log In** in the **Operation** column.

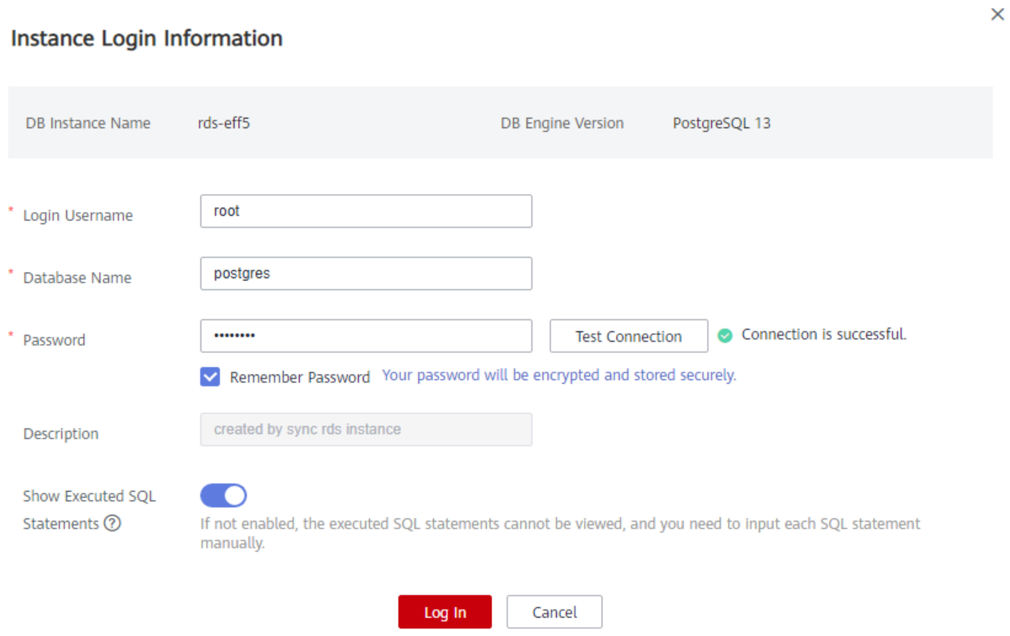
Figure 3-38 Instances



	Name/ID	Description	DB Instance T...	DB Engine Version	Status	Billing M...	Floating I...	Enterpris...	Created	Database...	Storage T...	Operation
□	rds-dc72 0f61a700762842f7ac64f62d3f96da9cin03	--	Single 2 vCPUs | 4 GB	PostgreSQL 13.9	Avail...	Pay-per-Use Created o...	192.1...	default	Mar 17, 2023 09:...	5432	Cloud SSD	View Metric Log In More

2. Enter the **root** password you configured during instance creation and click **Log In**.

Figure 3-39 Instance login



Instance Login Information

DB Instance Name	rds-eff5	DB Engine Version	PostgreSQL 13

* Login Username: root

* Database Name: postgres

* Password: •••••••• Test Connection Connection is successful.

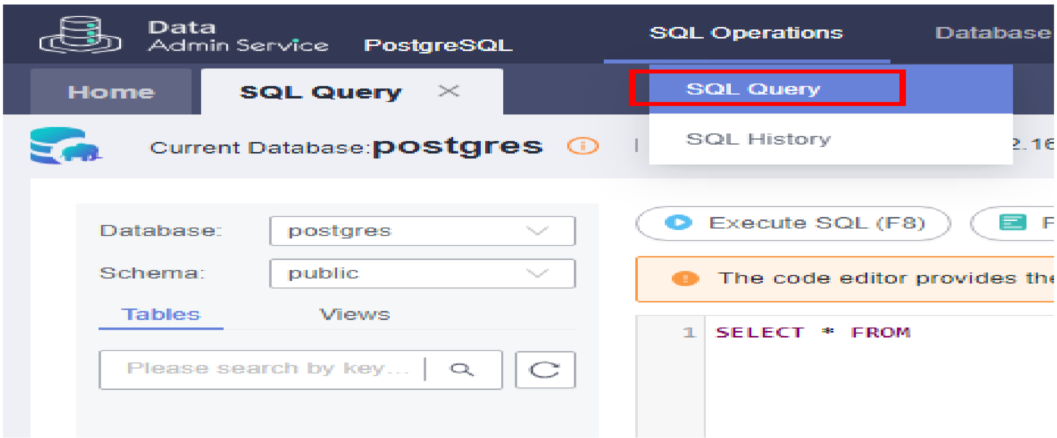
☑ Remember Password Your password will be encrypted and stored securely.

Description: created by sync rds instance

Show Executed SQL Statements: If not enabled, the executed SQL statements cannot be viewed, and you need to input each SQL statement manually.

3. Choose **SQL Operations** > **SQL Query**.

Figure 3-40 SQL Query

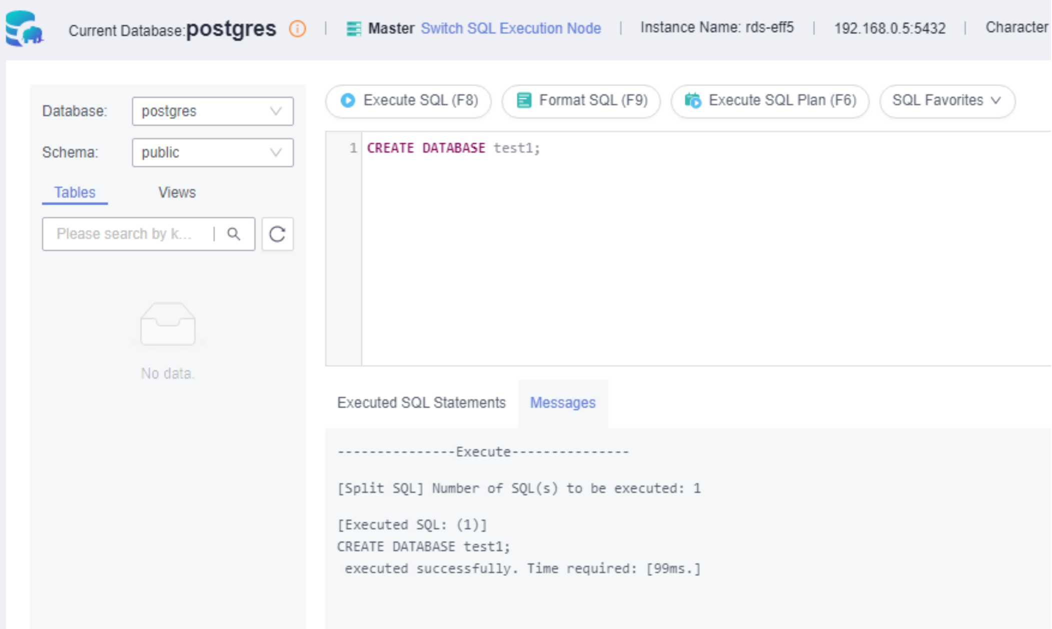


```
SELECT * FROM
```

4. Create a database named **test1**.

CREATE DATABASE test1;

Figure 3-41 Creating a database



Database: postgres

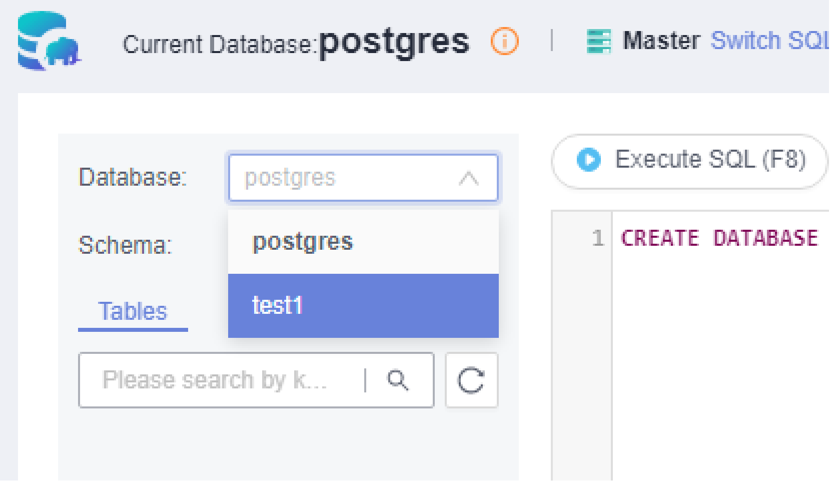
Schema: public

```
CREATE DATABASE test1;
```

```
--------------Execute--------------
[Split SQL] Number of SQL(s) to be executed: 1
[Executed SQL: (1)]
CREATE DATABASE test1;
 executed successfully. Time required: [99ms.]
```

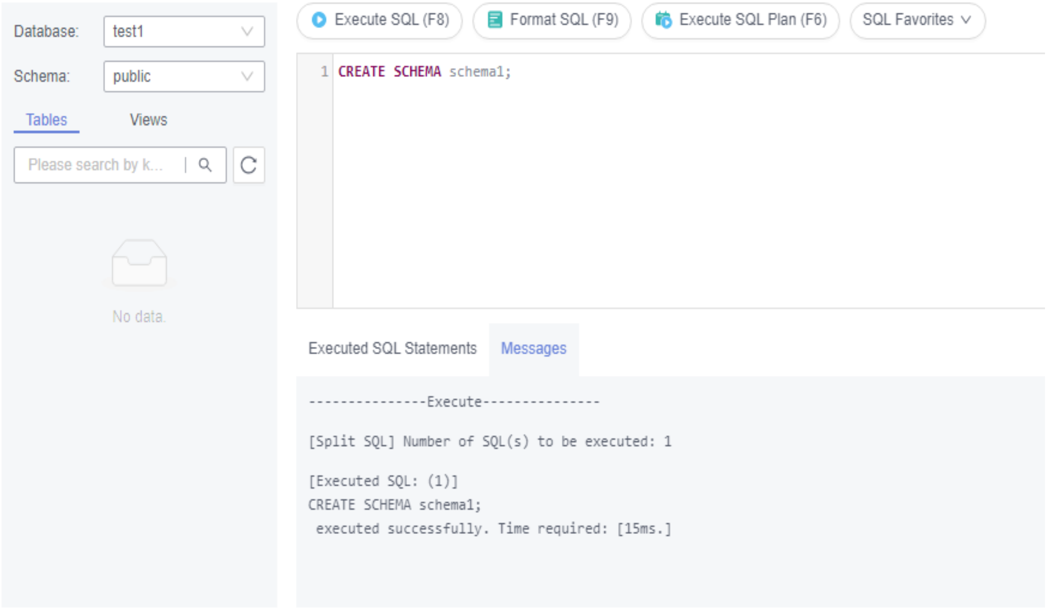
5. Switch to **test1** and create a schema named **schema1** in the database.

Figure 3-42 Switching to the database



CREATE SCHEMA schema1;

Figure 3-43 Creating a schema



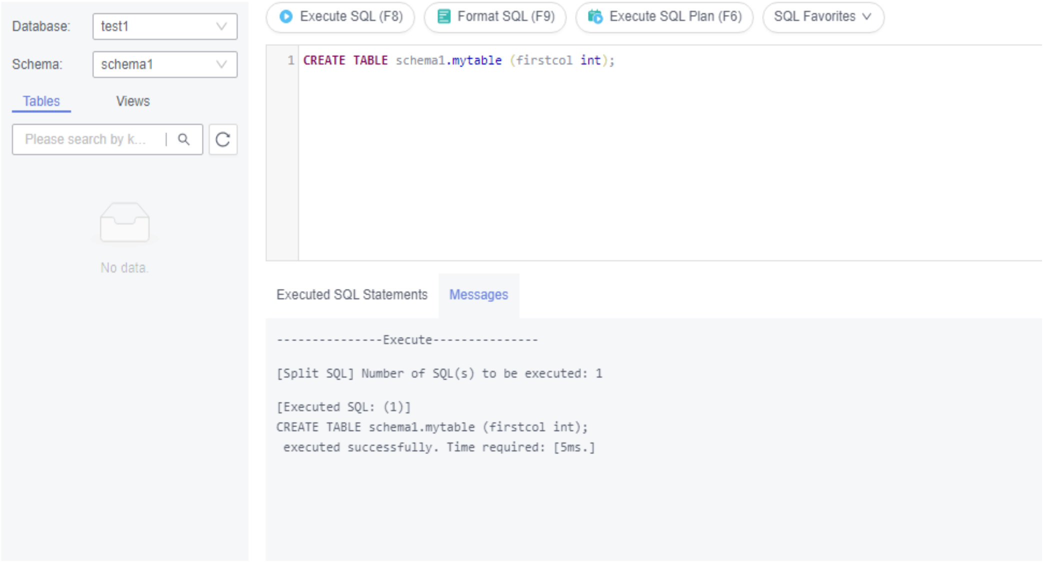
```
CREATE SCHEMA schema1;
```

```
--------------Execute--------------
[Split SQL] Number of SQL(s) to be executed: 1
[Executed SQL: (1)]
CREATE SCHEMA schema1;
 executed successfully. Time required: [15ms.]
```

6. Switch to **schema1** and create a table named **mytable** with only one column. Specify the column name as **firstcol** and the column type as **integer**.

   CREATE TABLE schema1.mytable (firstcol int);

Figure 3-44 Creating a table



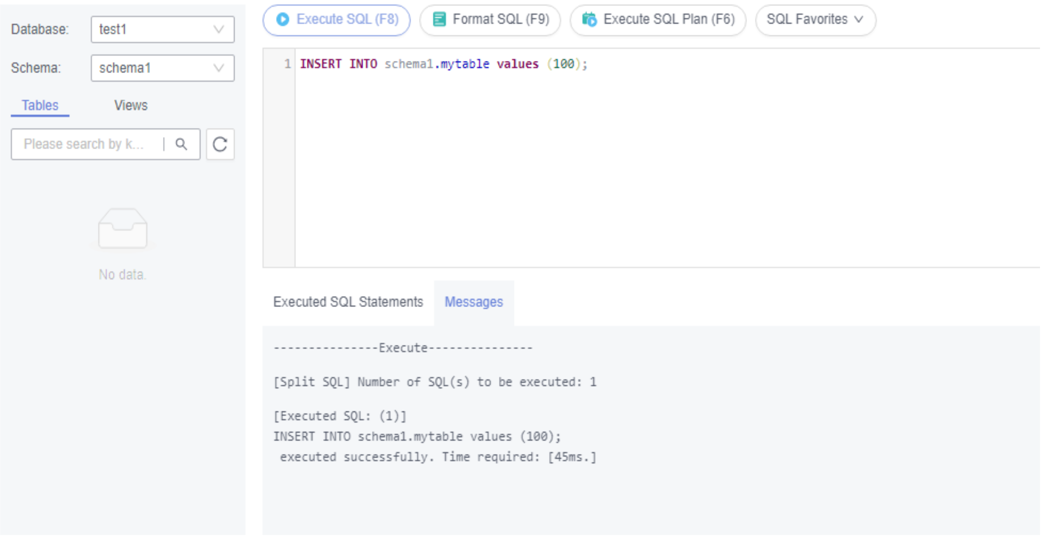
```
CREATE TABLE schema1.mytable (firstcol int);
```

```
--------------Execute--------------
[Split SQL] Number of SQL(s) to be executed: 1
[Executed SQL: (1)]
CREATE TABLE schema1.mytable (firstcol int);
 executed successfully. Time required: [5ms.]
```

7. Insert data to the table.

   INSERT INTO schema1.mytable values (100);

Figure 3-45 Inserting data



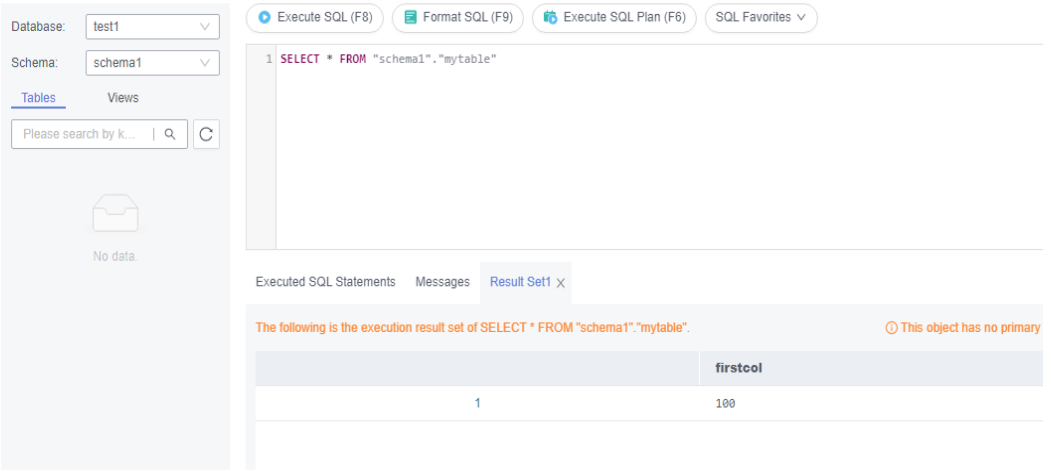
```
INSERT INTO schema1.mytable values (100);
```

```
--------------Execute--------------

[Split SQL] Number of SQL(s) to be executed: 1

[Executed SQL: (1)]
INSERT INTO schema1.mytable values (100);
 executed successfully. Time required: [45ms.]
```

Query data in the table.

SELECT * FROM "schema1"."mytable"

Figure 3-46 Querying data



```
SELECT * FROM "schema1"."mytable"
```

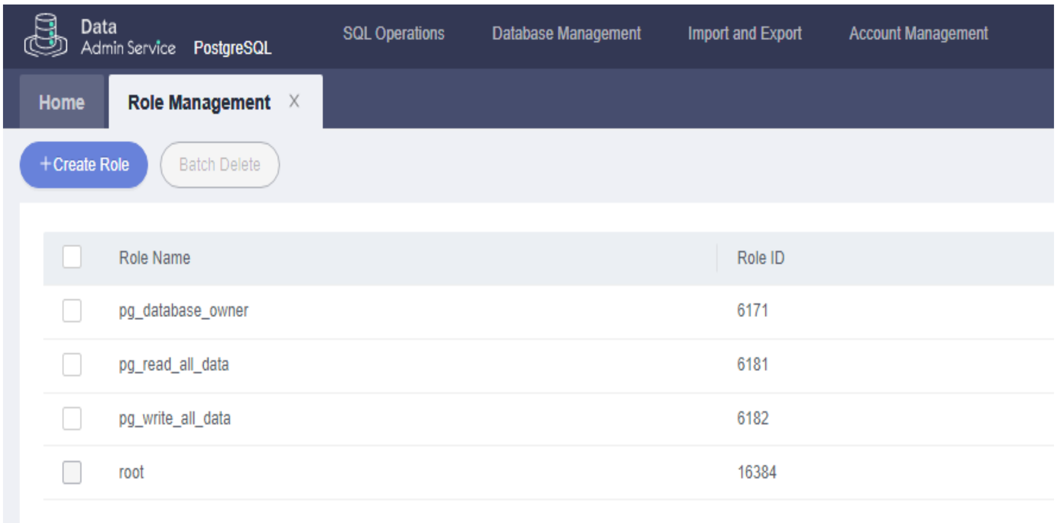
The following is the execution result set of SELECT * FROM "schema1"."mytable".

ⓘ This object has no primary

	firstcol
1	100

8. In the upper part of the page, choose **Account Management** > **Role Management**.

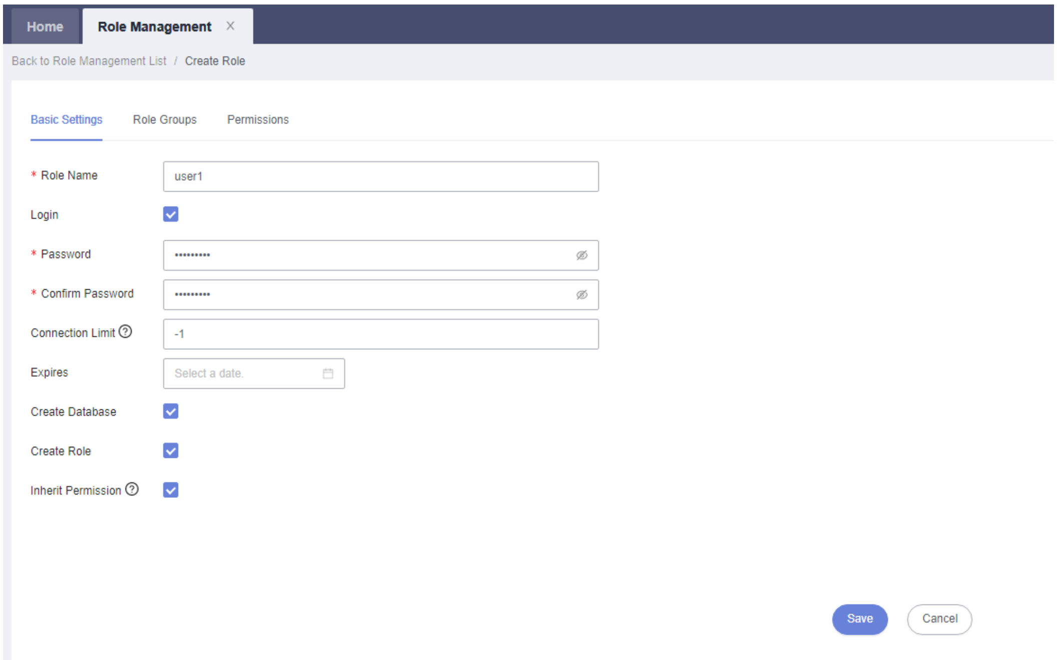
Figure 3-47 Role management



□	Role Name	Role ID
□	pg_database_owner	6171
□	pg_read_all_data	6181
□	pg_write_all_data	6182
□	root	16384

9. Click **Create Role** and complete basic settings. **user1** is used as an example.

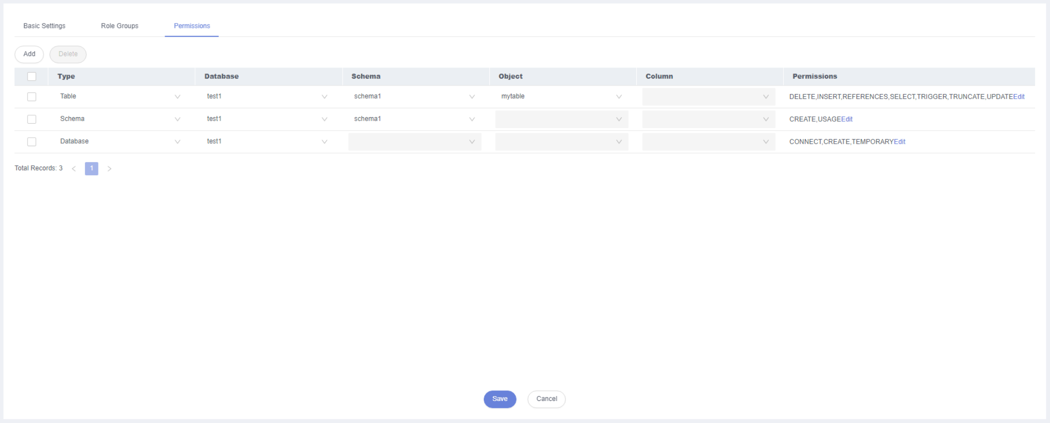
Figure 3-48 Creating a role



* Role Name	user1
Login	☑
* Password	•••••••••
* Confirm Password	•••••••••
Connection Limit	-1
Expires	Select a date.
Create Database	☑
Create Role	☑
Inherit Permission	☑

10. Click the **Permissions** tab and grant **user1** the permissions to perform operations on databases, schemas, and tables.

Figure 3-49 Granting permissions

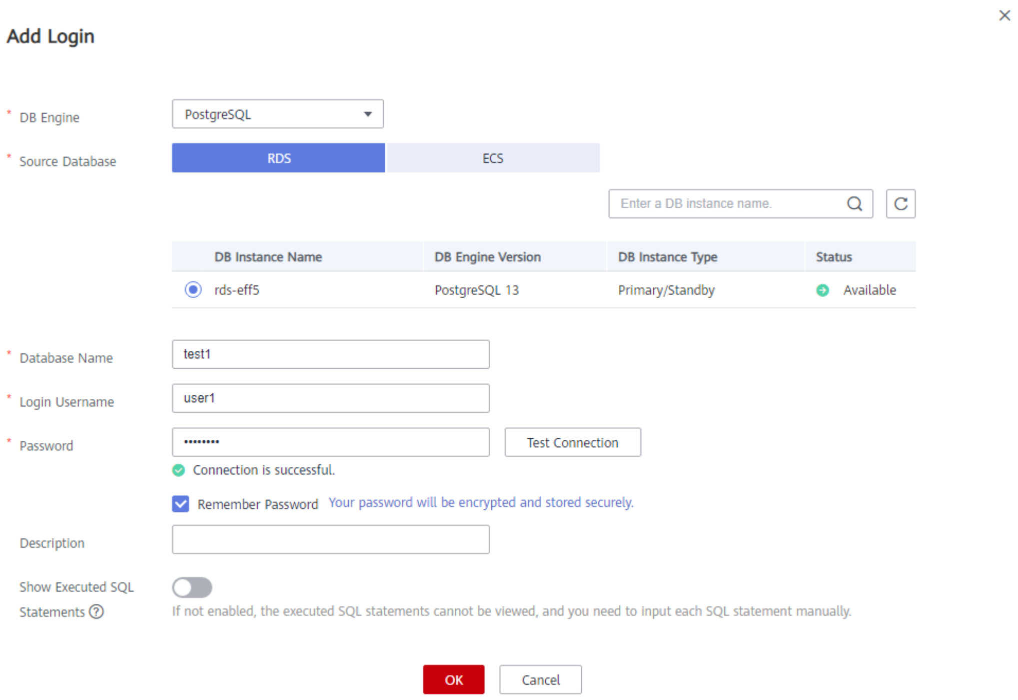


□	Type	Database	Schema	Object	Column	Permissions
□	Table	test1	schema1	mytable		DELETE,INSERT,REFERENCES,SELECT,TRIGGER,TRUNCATE,UPDATEEdit
□	Schema	test1	schema1			CREATE,USAGEEdit
□	Database	test1				CONNECT,CREATE,TEMPORARYEdit

Total Records: 3 < 1 >

11. On the **Development Tool** page, click **Add Login** and log in to the database as **user1**.

Figure 3-50 Adding login


Add Login

* DB Engine: PostgreSQL

* Source Database: RDS | ECS

Enter a DB instance name.

	DB Instance Name	DB Engine Version	DB Instance Type	Status
●	rds-eff5	PostgreSQL 13	Primary/Standby	Available

* Database Name: test1

* Login Username: user1

* Password: •••••••• Test Connection

Connection is successful.

☑ Remember Password Your password will be encrypted and stored securely.

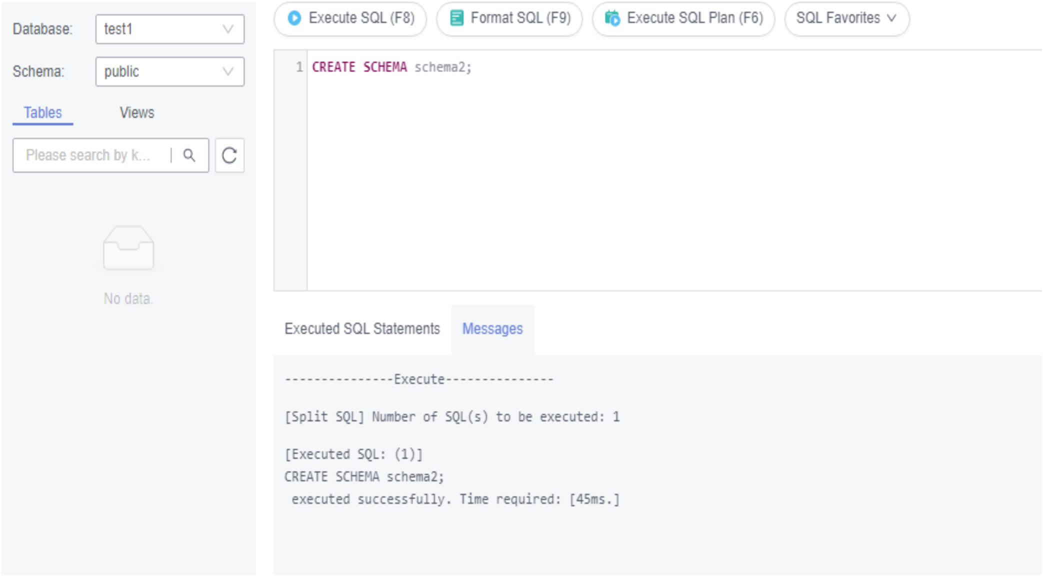
Description:

Show Executed SQL Statements: If not enabled, the executed SQL statements cannot be viewed, and you need to input each SQL statement manually.

12. Create **schema2** in **test1** to verify that **user1** has the **CREATE** permission.

CREATE SCHEMA schema2;

Figure 3-51 Verifying permissions



```
CREATE SCHEMA schema2;
```

```
--------------Execute--------------

[Split SQL] Number of SQL(s) to be executed: 1

[Executed SQL: (1)]
CREATE SCHEMA schema2;
 executed successfully. Time required: [45ms.]
```

4 Getting Started with RDS for SQL Server

4.1 Overview

An RDS DB instance can be connected through a private network, Data Admin Service (DAS), or a public network.

Table 4-1 RDS connection methods

Connect Through	IP Address	Scenarios	Description
DAS	No IP address is required. You can log in to the DAS console and use RDS directly.	DAS enables you to manage databases on a web-based console and provides you with database development, O&M, and intelligent diagnosis to make it easy to use and maintain your databases. The permissions required for connecting to DB instances through DAS are enabled by default.	● Easy to use, secure, advanced, and intelligent ● Recommended
Private network	Floating IP	RDS provides a floating IP address by default. When your applications are deployed on an ECS that is in the same region and VPC as RDS, you are advised to use a floating IP address to connect to the RDS DB instance through the ECS.	● Secure and excellent performance ● Recommended

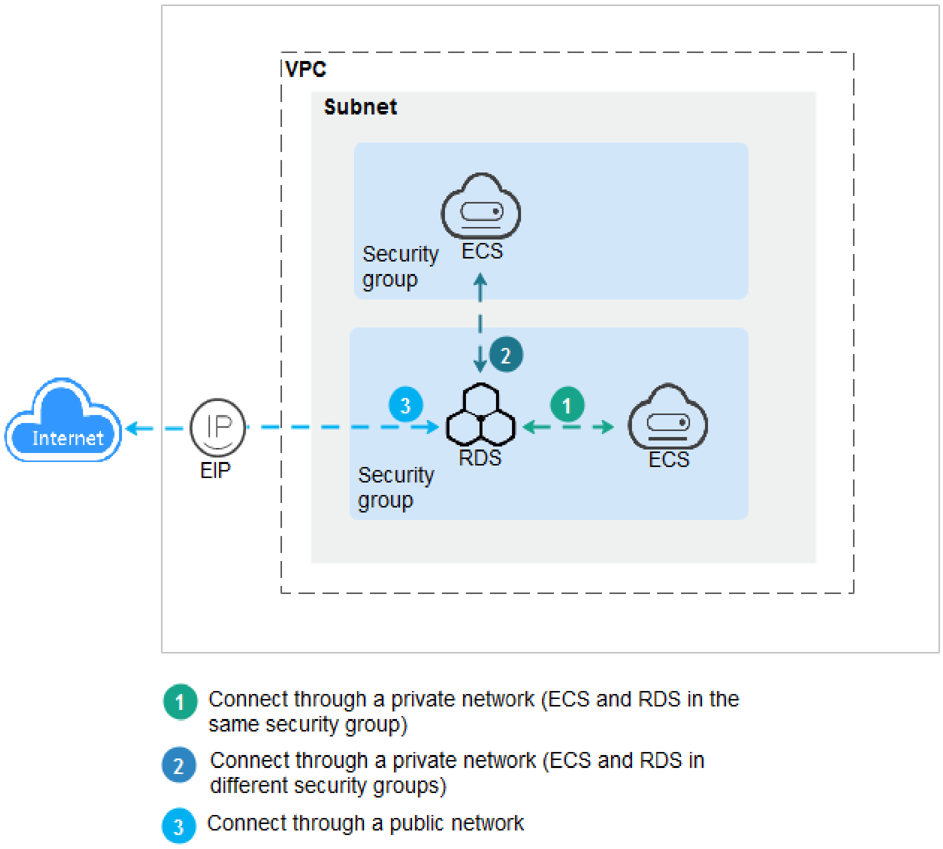
Connect Through	IP Address	Scenarios	Description
Public network	EIP	If you cannot access an RDS DB instance through a floating IP address, bind an EIP to the DB instance and connect the DB instance to the ECS through the EIP.	● A relatively lower level of security compared to other connection methods ● To achieve a higher transmission rate and security level, you are advised to migrate your applications to an ECS that is in the same VPC as your RDS DB instance and use a floating IP address to access the DB instance. ● You need to purchase an EIP. For details, see **EIP billing details**.

NOTE

- VPC: indicates the Virtual Private Cloud.
- ECS: indicates the Elastic Cloud Server.
- You can log in to DB instances using the Data Admin Service (DAS) service or other database clients.
- If the ECS is in the same VPC as the RDS DB instance, you do not need to apply for an EIP.

Figure 4-1 illustrates the connection over a private network or a public network.

Figure 4-1 DB instance connection


VPC
Subnet
Security group
ECS
2
Internet
IP
EIP
3
RDS
1
ECS
Security group
1 Connect through a private network (ECS and RDS in the same security group)
2 Connect through a private network (ECS and RDS in different security groups)
3 Connect through a public network

Connecting to DB Instances Running Other DB Engines

- **Connecting to an RDS for MySQL DB Instance**
- **Connecting to an RDS for PostgreSQL DB Instance**

4.2 Connecting to a DB Instance Through DAS (Recommended)

Scenarios

Data Admin Service (DAS) enables you to connect to and manage databases with ease on a web-based console. The permissions required for connecting to DB instances through DAS are enabled by default. You are advised to use this connection method.

Procedure

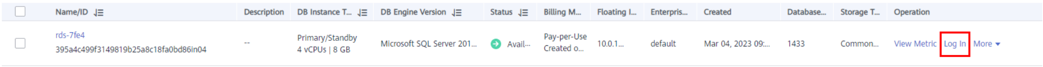
Step 1 **Log in to the management console**.

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

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

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

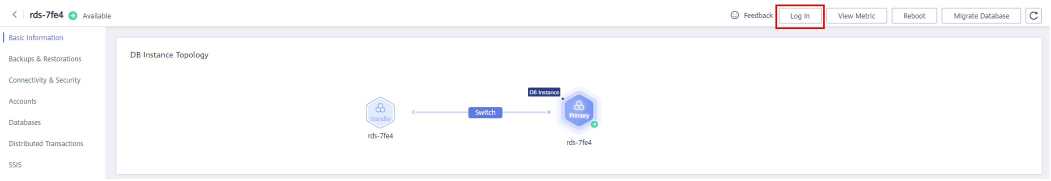
Figure 4-2 Logging in to an instance



□	Name/ID	Description	DB Instance T...	DB Engine Version	Status	Billing M...	Floating I...	Enterpris...	Created	Database...	Storage T...	Operation
□	rds-7fe4 395a4c499f3149819b25a8c18fa0bd86in04	--	Primary/Standby 4 vCPUs | 8 GB	Microsoft SQL Server 201...	Avail...	Pay-per-Use Created o...	10.0.1...	default	Mar 04, 2023 09:...	1433	Common...	View Metric Log In More ▾

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

Figure 4-3 Logging in to an instance



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

----End

FAQ

- What Should I Do If I Can't Connect to My DB Instance Due to Insufficient Permissions?
- What Should I Do If I Can't Connect to My RDS for SQL Server Instance?

Follow-up Operations

After logging in to the DB instance, you can create or migrate databases.

- Managing RDS for SQL Server Databases Using DAS
- Migration Solution Overview

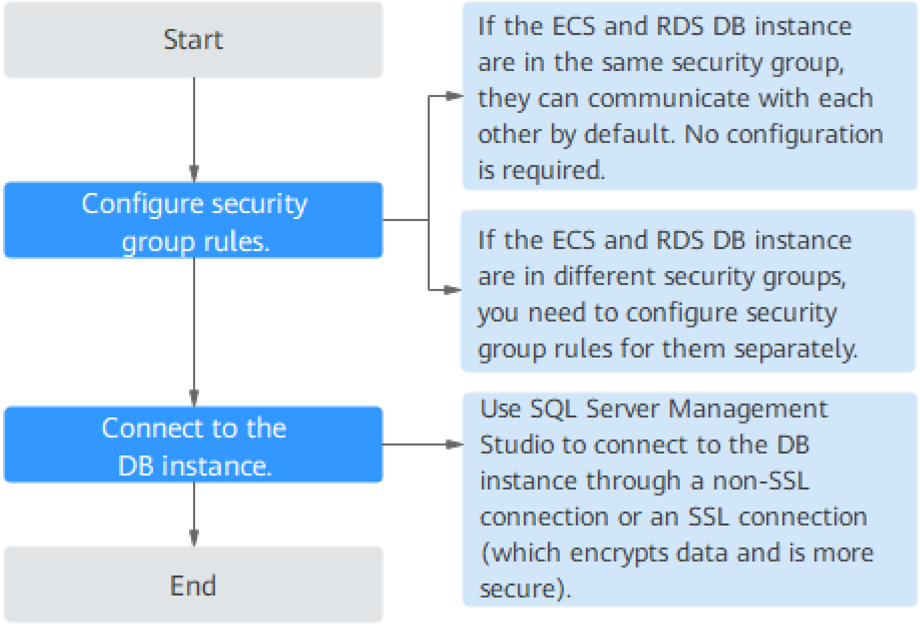
4.3 Connecting to a DB Instance Through a Private Network

4.3.1 Connecting to a DB Instance Through a Private Network

Process

Figure 4-4 illustrates the process of connecting to an RDS for SQL Server DB instance through a private network.

Figure 4-4 Connecting to a DB instance through a private network


Start
Configure security group rules.
If the ECS and RDS DB instance are in the same security group, they can communicate with each other by default. No configuration is required.
If the ECS and RDS DB instance are in different security groups, you need to configure security group rules for them separately.
Connect to the DB instance.
Use SQL Server Management Studio to connect to the DB instance through a non-SSL connection or an SSL connection (which encrypts data and is more secure).
End

4.3.2 Connecting to a DB Instance from a Windows ECS

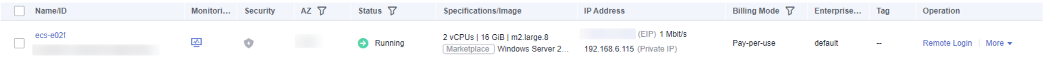
You can connect to your DB instance using a Windows ECS installed with SQL Server Management Studio over a private network.

This section describes how to connect to a DB instance with SSL disabled. To connect to a DB instance with SSL enabled, see **Connecting to an Instance Through a Private Network**.

Step 1: Buy an ECS

1. **Log in to the management console** and check whether there is an ECS available.
   - If there is a Windows ECS, go to **3**.
   - If no Windows ECS is available, go to **2**.

   Figure 4-5 ECS

□	Name/ID	Monitori...	Security	AZ	Status	Specifications/Image	IP Address	Billing Mode	Enterprise...	Tag	Operation
□	ecs-e02f [redacted]			[redacted]	Running	2 vCPUs | 16 GiB | m2.large.8 Marketplace Windows Server 2...	[redacted] (EIP) 1 Mbit/s 192.168.6.115 (Private IP)	Pay-per-use	default	--	Remote Login | More

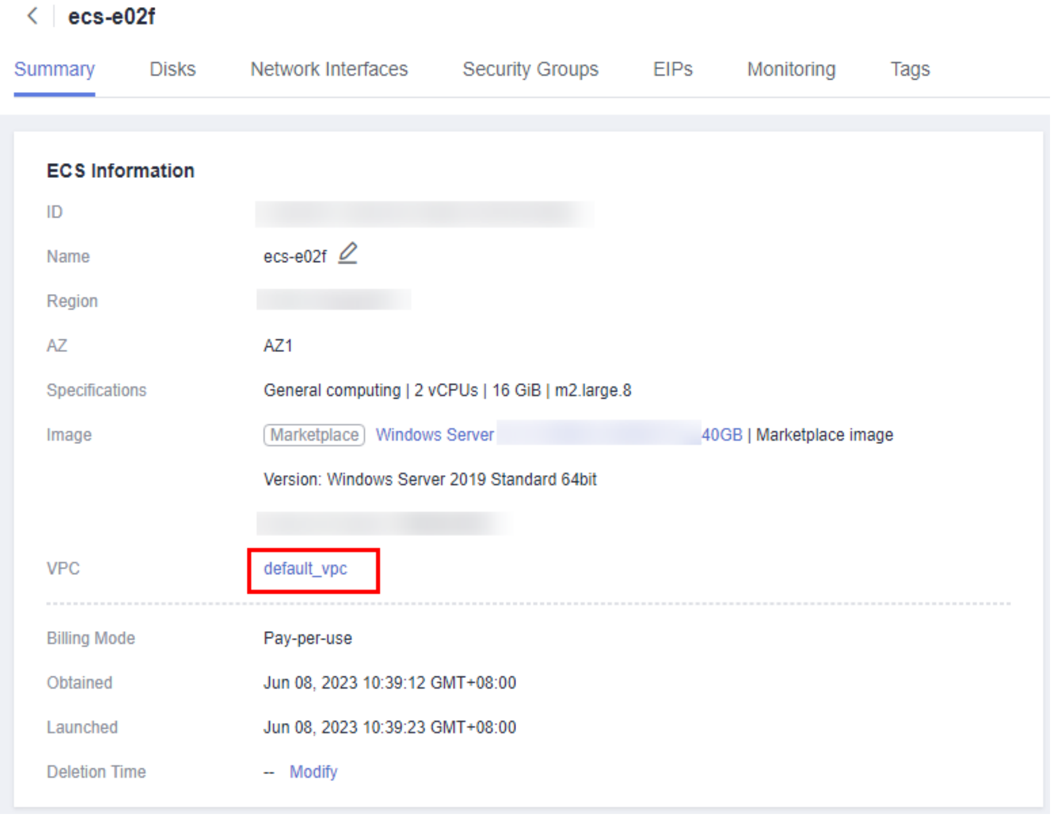
2. Buy an ECS and select Windows as its OS.

   To download SQL Server Management Studio to the ECS, bind an EIP to the ECS. The ECS must be in the same region, VPC, and security group as the RDS for SQL Server DB instance for mutual communications.

   For details about how to purchase a Windows ECS, see "**Purchasing an ECS**" in *Elastic Cloud Server Getting Started*.

3. On the **ECS Information** page, view the region and VPC of the ECS.

Figure 4-6 ECS information

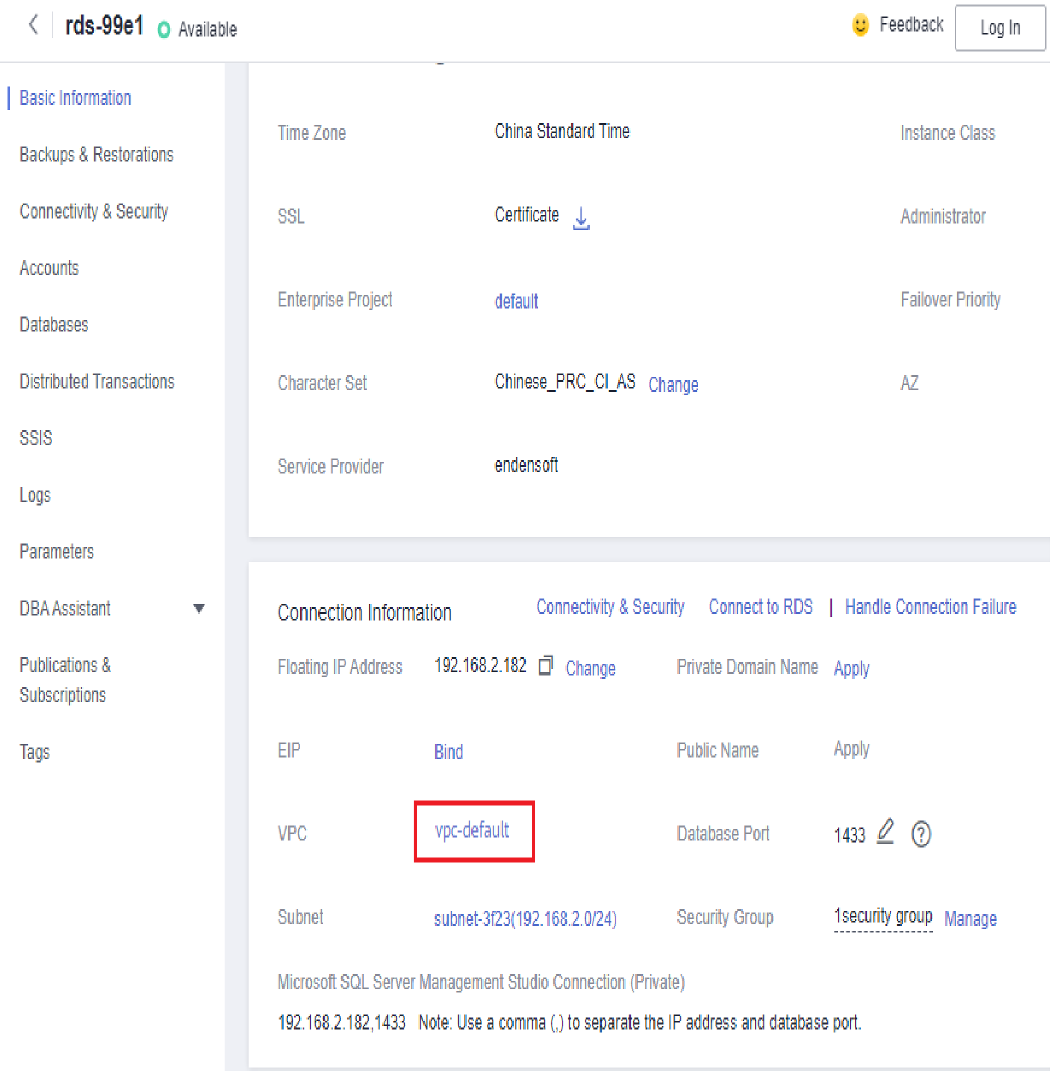


ECS Information

ID	
Name	ecs-e02f
Region	
AZ	AZ1
Specifications	General computing | 2 vCPUs | 16 GiB | m2.large.8
Image	Marketplace Windows Server 40GB | Marketplace image Version: Windows Server 2019 Standard 64bit
VPC	default_vpc
Billing Mode	Pay-per-use
Obtained	Jun 08, 2023 10:39:12 GMT+08:00
Launched	Jun 08, 2023 10:39:23 GMT+08:00
Deletion Time	-- Modify

4. On the **Basic Information** page of the RDS for SQL Server instance, view the region and VPC of the DB instance.

Figure 4-7 DB instance information



Time Zone China Standard Time

SSL Certificate

Enterprise Project default

Character Set Chinese_PRC_CI_AS Change

Service Provider endensoft

Instance Class

Administrator

Failover Priority

AZ

Connection Information

Floating IP Address 192.168.2.182 Change

Private Domain Name Apply

EIP Bind

Public Name Apply

VPC vpc-default

Database Port 1433

Subnet subnet-3f23(192.168.2.0/24)

Security Group 1security group Manage

Microsoft SQL Server Management Studio Connection (Private)

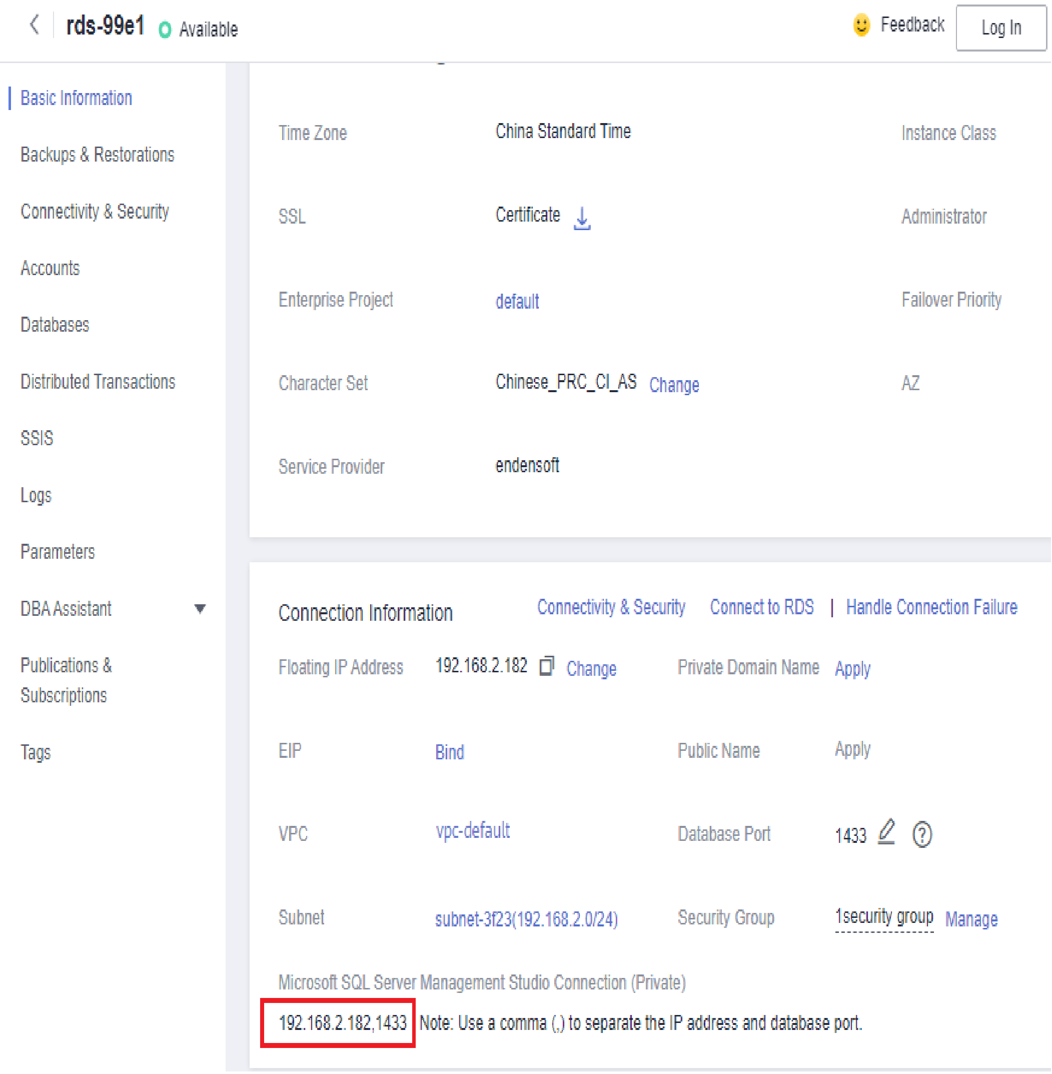
192.168.2.182,1433 Note: Use a comma (,) to separate the IP address and database port.

5. Check whether the ECS and RDS for SQL Server instance are in the same region and VPC.
   - If yes, go to **Step 2: Test Connectivity and Install SQL Server Management Studio**.
   - If they are not in the same region, purchase another ECS or DB instance. The ECS and DB instance in different regions cannot communicate with each other. To reduce network latency, deploy your DB instance in the region nearest to your workloads.
   - If the ECS and DB instance are in different VPCs, change the VPC of the ECS to that of the DB instance. For details, see **Changing a VPC**.

Step 2: Test Connectivity and Install SQL Server Management Studio

1. Log in to the ECS. For details, see **Login Using VNC** in the *Elastic Cloud Server User Guide*.
2. On the **Instances** page, click the DB instance name.
3. In the **Connection Information** area, obtain the floating IP address and database port of the DB instance.

Figure 4-8 Connection information



Time Zone China Standard Time
Instance Class
SSL Certificate
Administrator
Enterprise Project default
Failover Priority
Character Set Chinese_PRC_CI_AS
AZ
Service Provider endensoft

Connection Information

Floating IP Address 192.168.2.182
Private Domain Name
EIP
Public Name
VPC vpc-default
Database Port 1433
Subnet subnet-3f23(192.168.2.0/24)
Security Group 1security group

Microsoft SQL Server Management Studio Connection (Private)

192.168.2.182,1433 Note: Use a comma (,) to separate the IP address and database port.

4. Open the cmd window on the ECS and check whether the floating IP address and database port of the DB instance can be connected.

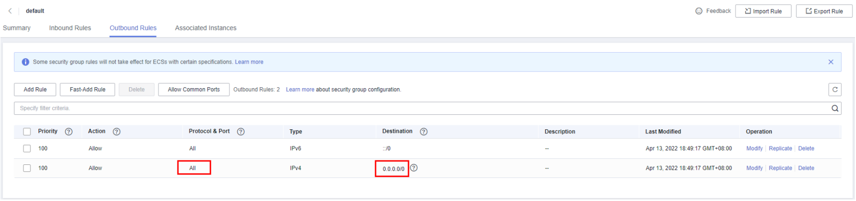
   telnet *192.168.2.182 1433*

   – If yes, network connectivity is normal.

   – If no, check the security group rules.

     ▪ If in the security group of the ECS, there is no outbound rule with **Destination** set to **0.0.0.0/0** and **Protocol & Port** set to **All**, add an outbound rule for the floating IP address and port of the DB instance.

Figure 4-9 ECS security group



Some security group rules will not take effect for ECSs with certain specifications. Learn more

Outbound Rules: 2 Learn more about security group configuration.

Priority	Action	Protocol & Port	Type	Destination	Description	Last Modified	Operation
100	Allow	All	IPv6	::/0	--	Apr 13, 2022 18:49:17 GMT+08:00	Modify | Replicate | Delete
100	Allow	All	IPv4	0.0.0.0/0	--	Apr 13, 2022 18:49:17 GMT+08:00	Modify | Replicate | Delete

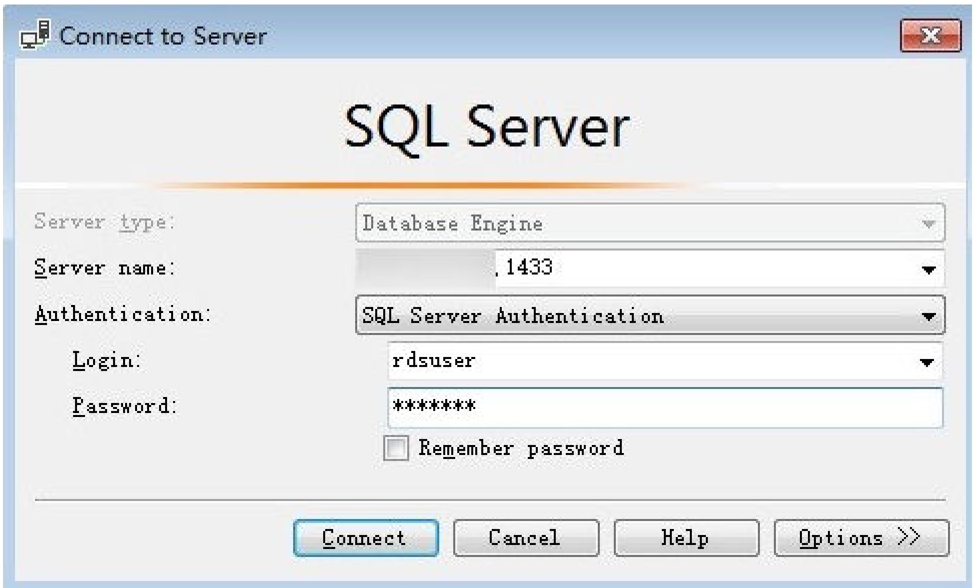
- If in the security group of the DB instance, there is no inbound rule allowing the access from the private IP address and port of the ECS, add an inbound rule for the private IP address and port of the ECS. For details, see **Configuring Security Group Rules**.

5. Open a browser on the ECS, visit the **Microsoft website**, and download the installation package, for example, SQL Server Management Studio 18.0.
6. Double-click the installation package and complete the installation as instructed.

Step 3: Connect to the DB Instance Using SQL Server Management Studio

1. Start SQL Server Management Studio.
2. Choose **Connect** > **Database Engine**. In the displayed dialog box, enter login information.

Figure 4-10 Connecting to the server



Connect to Server

SQL Server

Server type: Database Engine

Server name: [redacted],1433

Authentication: SQL Server Authentication

Login: rdsuser

Password: *******

□ Remember password

Table 4-2 Parameter description

Parameter	Description
Server name	Floating IP address and database port obtained in **3**.
Authentication	Authentication mode. Select **SQL Server Authentication**.
Login	Name of the account used to access the DB instance. The default value is **rdsuser**.
Password	Password of the account.

3. Click **Connect** to connect to the DB instance.

Follow-up Operations

After logging in to the DB instance, you can create or migrate databases.

- **Managing RDS for SQL Server Databases Using DAS**
- **Migration Solution Overview**

4.3.3 Configuring Security Group Rules

Scenarios

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

This section describes how to create a security group to enable specific IP addresses and ports to access RDS.

First check whether the ECS and RDS DB instance are in the same security group.

- If the ECS and RDS DB instance are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to **Connecting to a DB Instance from a Windows ECS**.
- If the ECS and RDS DB instance are in different security groups, you need to configure security group rules for them, separately.
  - RDS DB instance: Configure an **inbound rule** for the security group with which the RDS DB instance is associated.
  - ECS: The default security group rule allows all outgoing data packets. In this case, you do not need to configure a security group rule for the ECS. If not all outbound traffic is allowed in the security group, you need to configure an **outbound rule** for the ECS.

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

For details about the requirements of security group rules, see the **Adding a Security Group Rule** section in the *Virtual Private Cloud User Guide*.

Precautions

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are deployed in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.

- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS DB instance can be associated with multiple security groups, and one security group can be associated with multiple RDS DB instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for each security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

NOTE

To ensure the security of your data and DB instances, you are advised to use the principle of least privilege for database access. Change the database port (default value: **1433**), and set the IP address to the remote server's address or any IP address in the remote server's smallest subnet to control the access from the remote server.

The default value of **Source** is **0.0.0.0/0**, indicating that RDS DB instances in the security group can be accessed from any IP address.

For details about the requirements of security group rules, see the **Adding a Security Group Rule** section in the *Virtual Private Cloud User Guide*.

Procedure

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

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

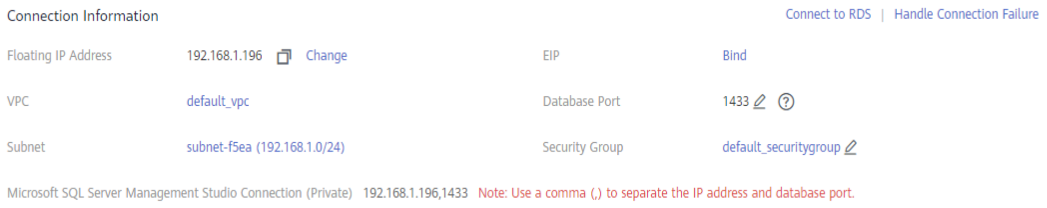
Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

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

Step 5 Configure security group rules.

In the **Connection Information** area on the **Basic Information** page, click the security group.

Figure 4-11 Connection information



Connection Information

Connect to RDS | Handle Connection Failure

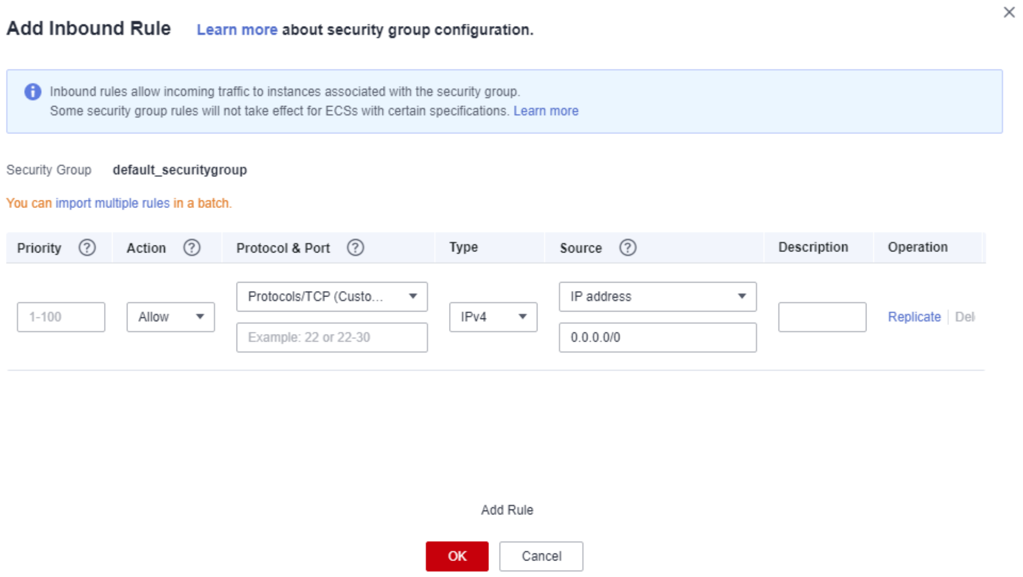
Floating IP Address	192.168.1.196 Change	EIP	Bind
VPC	default_vpc	Database Port	1433
Subnet	subnet-f5ea (192.168.1.0/24)	Security Group	default_securitygroup

Microsoft SQL Server Management Studio Connection (Private) 192.168.1.196,1433 Note: Use a comma (,) to separate the IP address and database port.

Step 6 On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

You can click **+** to add more inbound rules.

Figure 4-12 Adding an inbound rule



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.
Some security group rules will not take effect for ECSs with certain specifications. Learn more

Security Group default_securitygroup

You can import multiple rules in a batch.

Priority	Action	Protocol & Port	Type	Source	Description	Operation
1-100	Allow	Protocols/TCP (Custo... Example: 22 or 22-30	IPv4	IP address 0.0.0.0/0		Replicate | Del

Table 4-3 Inbound rule parameter description

Parameter	Description	Example Value
Priority	Security group rule priority. Value range: 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	Security group rule actions. A rule with a deny action overrides another with an allow action if the two rules have the same priority.	Allow
Protocol & Port	**Protocol**: network protocol. Available options: **All**, **TCP**, **UDP**, **ICMP**, or **GRE**.	TCP

Parameter	Description	Example Value
	Port: the port over which the traffic can reach your DB instance. An RDS for SQL Server instance can use the default database port 1433 or any port from the range 2100-9500 (excluding 5355 and 5985). If your instance uses 2019 Enterprise Edition, 2019 Standard Edition, 2019 Web Edition, 2017 Enterprise Edition, 2017 Standard Edition, or 2017 Web Edition, ports 5050, 5353, and 5986 cannot be specified for it.	1433
Type	IP address type. Currently, only IPv4 is supported.	IPv4
Source	Source address. It can be a single IP address, an IP address group, or a security group to allow access from them to your DB instance. Examples: ● Single IP address: 192.168.10.10/32 (IPv4 address) ● IP address segment: 192.168.1.0/24 (IPv4 address segment) ● All IP addresses: 0.0.0.0/0 (any IPv4 address) ● Security group: sg-abc ● IP address group: ipGroup-test	0.0.0.0/0
Description	Supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (<) or (>).	-

----End

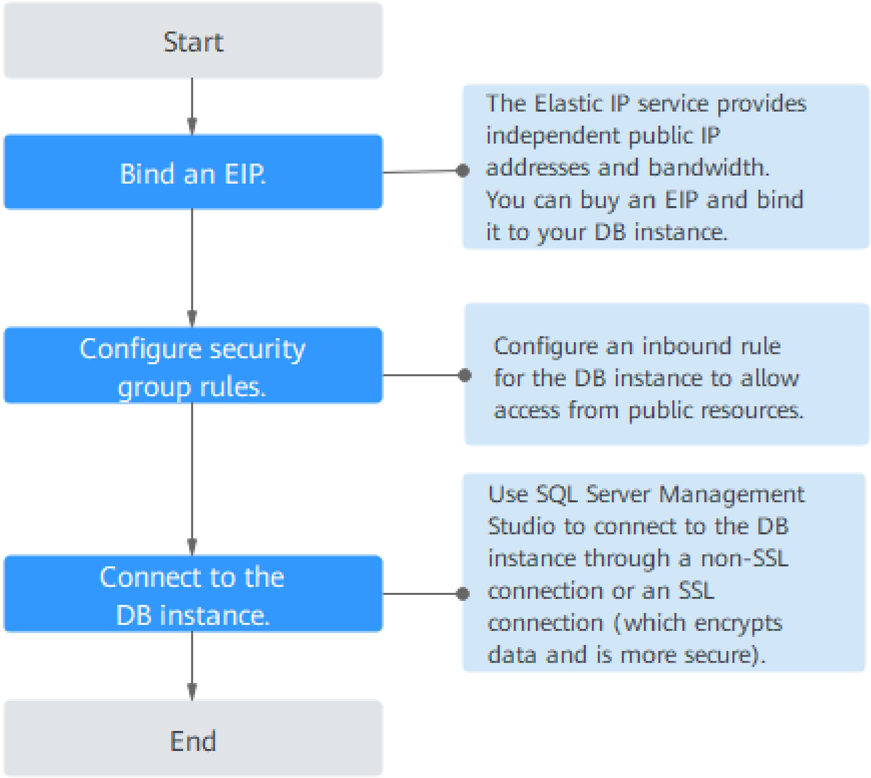
4.4 Connecting to a DB Instance Through a Public Network

4.4.1 Connecting to a DB Instance Through a Public Network

Process

Figure 4-13 illustrates the process of connecting to an RDS for SQL Server DB instance through a public network.

Figure 4-13 Connecting to a DB instance through a public network


Start
Bind an EIP.
The Elastic IP service provides independent public IP addresses and bandwidth. You can buy an EIP and bind it to your DB instance.
Configure security group rules.
Configure an inbound rule for the DB instance to allow access from public resources.
Connect to the DB instance.
Use SQL Server Management Studio to connect to the DB instance through a non-SSL connection or an SSL connection (which encrypts data and is more secure).
End

4.4.2 Binding an EIP

Scenarios

You can bind an EIP to a DB instance for public accessibility and can unbind the EIP from the DB instance as required.

Precautions

- You need to configure security groups and enable specific IP addresses and ports to access the target DB instance. Before accessing the DB instance, you need to add an individual IP address or an IP address range that will access the DB instance to the inbound rule. For details, see section **Configuring Security Group Rules**.

- Traffic generated by the public network is charged. You can unbind the EIP from your DB instance when the EIP is no longer used.

Binding an EIP

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

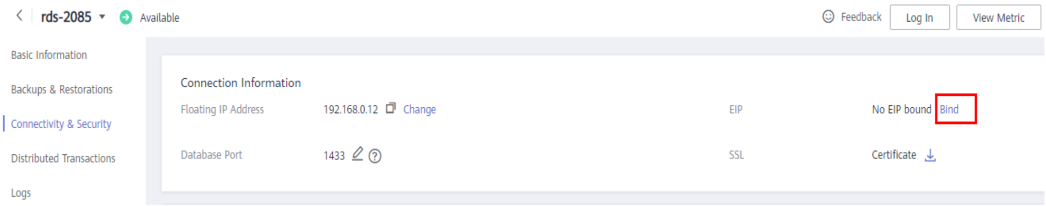
Step 2 Click 📍 in the upper left corner and select a region and a project.

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

Step 4 On the **Instances** page, click the target DB instance.

Step 5 In the navigation pane on the left, choose **Connectivity & Security**. In the **Connection Information** area, click **Bind** next to the **EIP** field.

Figure 4-14 Binding an EIP



Connection Information

Floating IP Address 192.168.0.12 Change

EIP No EIP bound Bind

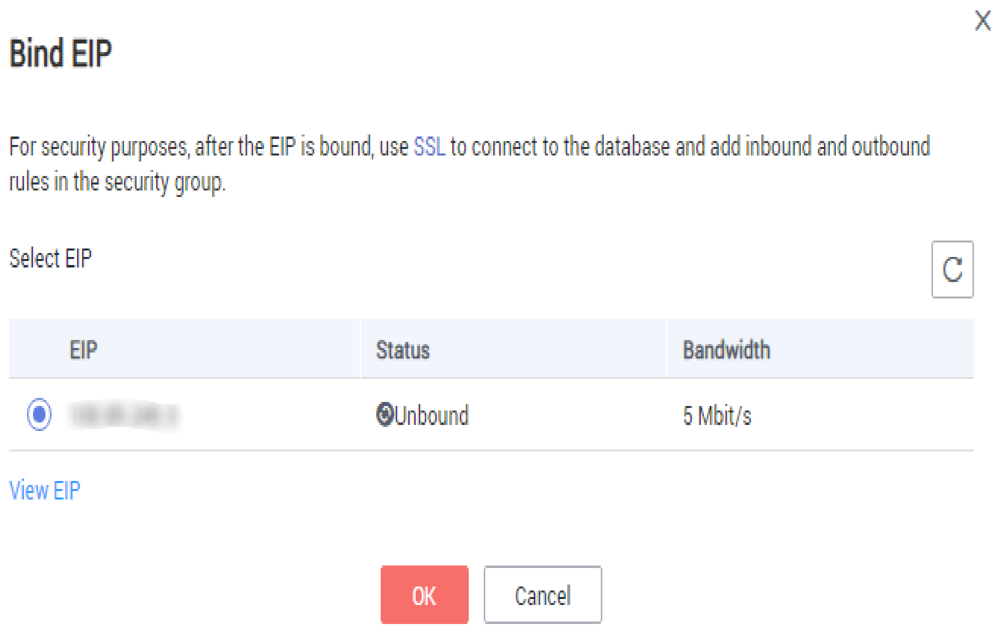
Database Port 1433

SSL Certificate

Step 6 In the displayed dialog box, select an EIP and click **OK**.

If no available EIPs are displayed, click **View EIP** and obtain an EIP.

Figure 4-15 Selecting an EIP



Bind EIP

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

Select EIP

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

Step 7 On the **Connectivity & Security** page, view the EIP that has been bound to the DB instance.

You can also view the progress and result of binding an EIP to a DB instance on the **Task Center** page.

----End

4.4.3 Connecting to a DB Instance from a Windows Server

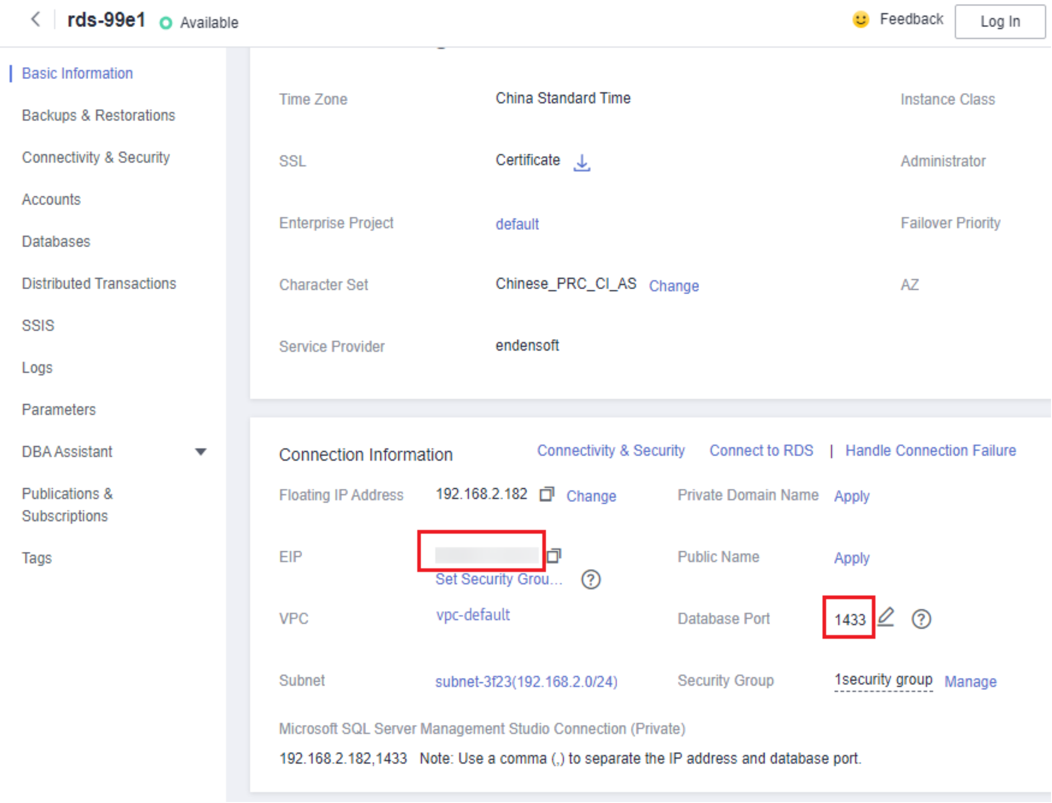
You can connect to your DB instance from a local Windows server installed with SQL Server Management Studio over a public network.

This section describes how to connect to a DB instance with SSL disabled. To connect to a DB instance with SSL enabled, see **Connecting to an Instance Through a Public Network**.

Step 1: Test Connectivity and Install SQL Server Management Studio

1. On the **Instances** page, click the DB instance name.
2. In the **Connection Information** area, obtain the EIP and database port of the DB instance.

Figure 4-16 Connection information



Time Zone	China Standard Time	Instance Class
SSL	Certificate	Administrator
Enterprise Project	default	Failover Priority
Character Set	Chinese_PRC_CI_AS Change	AZ
Service Provider	endensoft	

Connection Information — Connectivity & Security | Connect to RDS | Handle Connection Failure

Floating IP Address	192.168.2.182 Change	Private Domain Name	Apply
EIP	[redacted] Set Security Grou...	Public Name	Apply
VPC	vpc-default	Database Port	1433
Subnet	subnet-3f23(192.168.2.0/24)	Security Group	1security group Manage

Microsoft SQL Server Management Studio Connection (Private)

192.168.2.182,1433 Note: Use a comma (,) to separate the IP address and database port.

If no EIP has been bound to the DB instance, see **Binding an EIP**.

3. Open the cmd window on your local server and check whether the EIP and database port of the DB instance can be connected.

telnet *EIP 1433*

- If yes, network connectivity is normal.
- If no, check the security group rules.

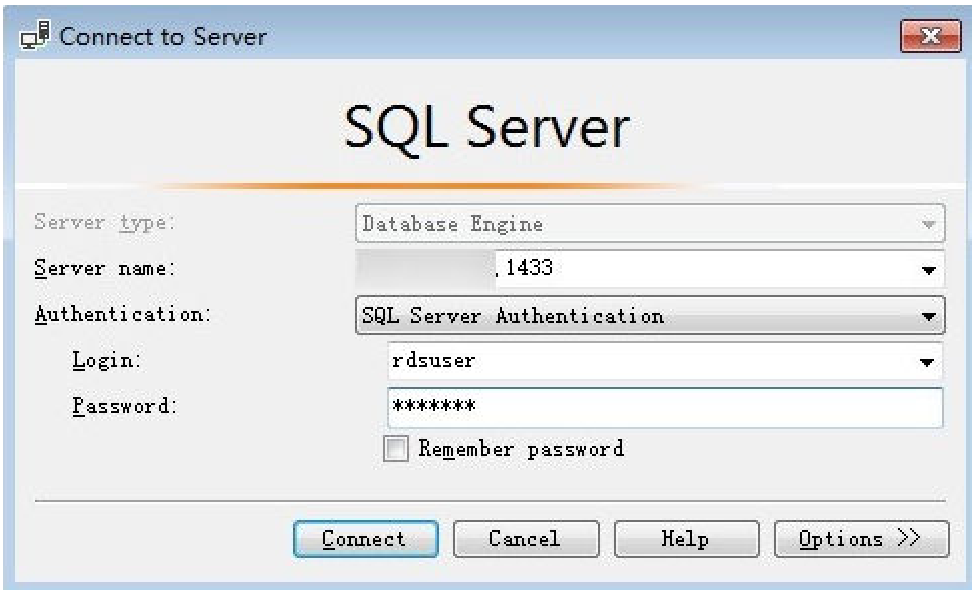
  Check inbound rules in the security group of the DB instance. Add an inbound rule for the EIP and port of the DB instance. For details, see **Configuring Security Group Rules**.

4. Open a browser on the local server, visit the **Microsoft website**, and download the installation package, for example, SQL Server Management Studio 18.0.
5. Double-click the installation package and complete the installation as instructed.

Step 2: Connect to the DB Instance Using SQL Server Management Studio

1. Start SQL Server Management Studio.
2. Choose **Connect** > **Database Engine**. In the displayed dialog box, enter login information.

Figure 4-17 Connecting to the server



Connect to Server

SQL Server

Server type: Database Engine
Server name: ,1433
Authentication: SQL Server Authentication
Login: rdsuser
Password: *******
□ Remember password

Table 4-4 Parameter description

Parameter	Description
Server name	EIP and database port obtained in 2.
Authentication	Authentication mode. Select **SQL Server Authentication**.
Login	Name of the account used to access the DB instance. The default value is **rdsuser**.
Password	Password of the account.

3. Click **Connect** to connect to the DB instance.

Follow-up Operations

After logging in to the DB instance, you can create or migrate databases.

- **Managing RDS for SQL Server Databases Using DAS**
- **Migration Solution Overview**

4.4.4 Configuring Security Group Rules

Scenarios

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

This section describes how to create a security group to enable specific IP addresses and ports to access RDS.

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

Precautions

The default security group rule allows all outgoing data packets. ECSs and RDS DB instances can access each other if they are deployed in the same security group. After a security group is created, you can configure security group rules to control access from and to the DB instances in the security group.

- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- One RDS DB instance can be associated with multiple security groups, and one security group can be associated with multiple RDS DB instances.
- Too many security group rules will increase the first packet latency. You are advised to create no more than 50 rules for a security group.
- To enable access to an RDS DB instance from resources outside the security group, you need to configure an **inbound rule** for the security group associated with the RDS DB instance.

NOTE

To ensure the security of your data and DB instances, you are advised to use the principle of least privilege for database access. Change the database port (default value: **1433**), and set the IP address to the remote server's address or any IP address in the remote server's smallest subnet to control the access from the remote server.

The default value of **Source** is **0.0.0.0/0**, indicating that RDS DB instances in the security group can be accessed from any IP address.

For details about the requirements of security group rules, see the **Adding a Security Group Rule** section in the *Virtual Private Cloud User Guide*.

Procedure

Step 1 Log in to the management console.

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

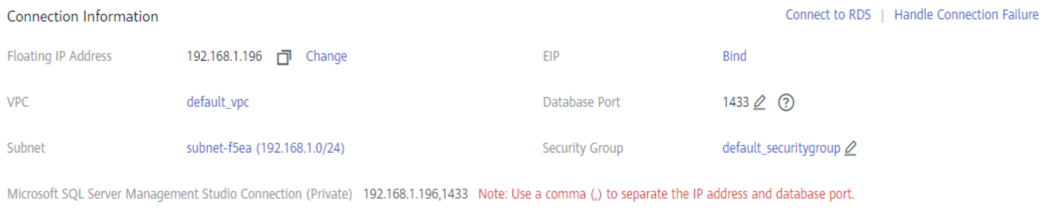
Step 3 Click ☰ in the upper left corner of the page and choose **Databases** > **Relational Database Service**.

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

Step 5 Configure security group rules.

In the **Connection Information** area on the **Basic Information** page, click the security group.

Figure 4-18 Connection information



Connection Information | Connect to RDS | Handle Connection Failure

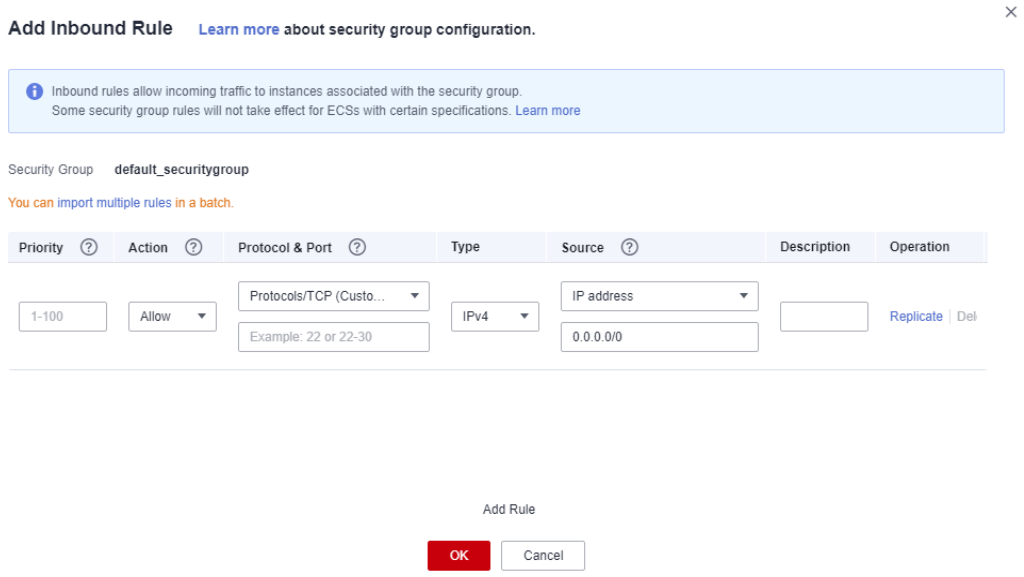
Floating IP Address	192.168.1.196 Change	EIP	Bind
VPC	default_vpc	Database Port	1433
Subnet	subnet-f5ea (192.168.1.0/24)	Security Group	default_securitygroup

Microsoft SQL Server Management Studio Connection (Private) 192.168.1.196,1433 Note: Use a comma (,) to separate the IP address and database port.

Step 6 On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

You can click **+** to add more inbound rules.

Figure 4-19 Adding an inbound rule



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.
Some security group rules will not take effect for ECSs with certain specifications. Learn more

Security Group default_securitygroup

You can import multiple rules in a batch.

Priority	Action	Protocol & Port	Type	Source	Description	Operation
1-100	Allow	Protocols/TCP (Custo... Example: 22 or 22-30	IPv4	IP address 0.0.0.0/0		Replicate | Del

Table 4-5 Inbound rule parameter description

Parameter	Description	Example Value
Priority	Security group rule priority. Value range: 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	Security group rule actions. A rule with a deny action overrides another with an allow action if the two rules have the same priority.	Allow
Protocol & Port	**Protocol**: network protocol. Available options: **All**, **TCP**, **UDP**, **ICMP**, or **GRE**.	TCP
	Port: the port over which the traffic can reach your DB instance. An RDS for SQL Server instance can use the default database port 1433 or any port from the range 2100-9500 (excluding 5355 and 5985). If your instance uses 2019 Enterprise Edition, 2019 Standard Edition, 2019 Web Edition, 2017 Enterprise Edition, 2017 Standard Edition, or 2017 Web Edition, ports 5050, 5353, and 5986 cannot be specified for it.	1433
Type	IP address type. Currently, only IPv4 is supported.	IPv4

Parameter	Description	Example Value
Source	Source address. It can be a single IP address, an IP address group, or a security group to allow access from them to your DB instance. Examples: ● Single IP address: 192.168.10.10/32 (IPv4 address) ● IP address segment: 192.168.1.0/24 (IPv4 address segment) ● All IP addresses: 0.0.0.0/0 (any IPv4 address) ● Security group: sg-abc ● IP address group: ipGroup-test	0.0.0.0/0
Description	Supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (<) or (>).	-

----End

5 Getting Started with RDS for MySQL Common Practices

After purchasing and connecting to a DB instance, you can view common practices to better use RDS for MySQL.

Table 5-1 Common practices

Practice		Description
Suggestions on using RDS for MySQL	**Instance Usage Suggestions**	This practice provides suggestions on using RDS for MySQL in terms of DB instances, database connection, reliability and availability, backup and restoration, SQL audit, routine O&M, and security.
	Database Usage Suggestions	This practice provides suggestions on database naming, database design, field design, index design, and SQL statement development.
Website setup	**Using RDS for MySQL to Set Up WordPress**	This practice describes how to set up WordPress in a LAMP environment using Huawei Cloud Virtual Private Cloud (VPC), Elastic Cloud Server (ECS), and RDS for MySQL.
	Using RDS for MySQL to Set Up Discuz!	This practice describes how to set up Discuz! in a LAMP environment using Huawei Cloud VPC, ECS, and RDS for MySQL.
Data migration	**Migrating Data to RDS for MySQL Using mysqldump**	This practice describes how to use mysqldump to copy data from the source to an RDS for MySQL DB instance.

Practice		Description
	From RDS for MySQL to RDS for MySQL	This practice describes how to use Data Replication Service (DRS) to migrate table, database, or instance data of the source to an RDS for MySQL DB instance.
	Migrating Data to RDS for MySQL Using the Export and Import Functions of DAS	This practice describes how to use Data Admin Service (DAS) to export data from the source and then import the data to an RDS for MySQL DB instance.
	From RDS for MySQL to RDS for MySQL	This practice describes how to use DRS to synchronize data from the source to an RDS for MySQL DB instance.
	• **Configuring Remote Single-Active DR for an RDS for MySQL Instance Using DRS** • **From RDS for MySQL to RDS for MySQL (Dual-Active DR)**	This practice describes how to use DRS to synchronize data from the source to a DR RDS for MySQL instance.
	From DDM to RDS for MySQL	This practice describes how to use DRS to synchronize data from a DDM instance to an RDS for MySQL DB instance.
	From GaussDB Distributed to RDS for MySQL	This practice describes how to use DRS to synchronize data from a GaussDB distributed instance to an RDS for MySQL DB instance.
	From GaussDB Primary/Standby to RDS for MySQL	This practice describes how to use DRS to synchronize data from a GaussDB primary/standby instance to an RDS for MySQL DB instance.
	From GaussDB(for MySQL) to RDS for MySQL	This practice describes how to use DRS to synchronize data from a GaussDB(for MySQL) DB instance to an RDS for MySQL DB instance.
	Migrating Data from Self-Managed MySQL Databases to RDS for MySQL	This practice describes how to use DRS to migrate data from a self-managed MySQL database to an RDS for MySQL DB instance.

Practice		Description
	From Self-Managed MySQL to RDS for MySQL	This practice describes how to use DRS to synchronize data from a self-managed MySQL database to an RDS for MySQL DB instance.
	• From Self-Managed MySQL to RDS for MySQL (Single-Active DR) • From Self-Managed MySQL to RDS for MySQL (Dual-Active DR)	This practice describes how to use DRS to synchronize data from a self-managed MySQL database to a DR RDS for MySQL instance.
	From Oracle to RDS for MySQL	This practice describes how to use DRS to synchronize data from a self-managed Oracle database to an RDS for MySQL DB instance.
	Migrating MySQL Databases from Other Clouds to RDS for MySQL	This practice describes how to use DRS to migrate MySQL databases from other clouds to RDS for MySQL.
	From MySQL on Other Clouds to RDS for MySQL	This practice describes how to use DRS to synchronize MySQL databases from other clouds to RDS for MySQL.
	• From MySQL on Other Clouds to RDS for MySQL (Single-Active DR) • From MySQL on Other Clouds to RDS for MySQL (Dual-Active DR)	This practice describes how to use DRS to synchronize MySQL databases from other clouds to DR RDS for MySQL instances.
Data backup	Intra-region automated backup	This practice describes how RDS for MySQL automatically creates backups for a DB instance during a backup window and saves the backups based on the configured retention period.
	Intra-region manual backup	This practice describes how to create manual backups for a DB instance. These backups can be used to restore data for improved reliability.

Practice		Description
	Cross-region automated backup	This practice describes how to store backups of a DB instance in another region for disaster recovery. If the DB instance fails, the backups in another region can be used to restore the data to a new DB instance.
Data restoration	**Restoring from Full Backups to RDS for MySQL Instances**	This practice describes how to use an automated or manual backup to restore a DB instance to how it was when the backup was created. The restoration is at the instance level.
	Restoring a DB Instance to a Point in Time	This practice describes how to use an automated backup to restore instance data to a specified point in time.
	Restoring Databases or Tables to a Point in Time	This practice describes how to use an automated backup to restore databases or tables to a specified point in time.

6 Getting Started with RDS for PostgreSQL Common Practices

After purchasing and connecting to a DB instance, you can view common practices to better use RDS for PostgreSQL.

Table 6-1 Common practices

Practice		Description
Suggestions on using RDS for PostgreSQL	**Instance Usage Suggestions**	This practice provides suggestions on using RDS for PostgreSQL in terms of database connection, read replicas, reliability and availability, logical replication, database age, stability, routine O&M, and security.
	Database Usage Suggestions	This practice provides suggestions on database naming, table design, index design, SQL design, and security.
Data migration	**Migrating Data to RDS for PostgreSQL Using psql**	This practice describes how to use pg_dump to copy data from the source to an RDS for PostgreSQL DB instance.
	Migrating Data to RDS for PostgreSQL Using the Export and Import Functions of DAS	This practice describes how to use Data Admin Service (DAS) to export data from the source and then import the data to an RDS for PostgreSQL DB instance.
	From RDS for PostgreSQL to RDS for PostgreSQL	This practice describes how to use DRS to synchronize data from the source to an RDS for PostgreSQL DB instance.

Practice		Description
	From Self-Managed PostgreSQL to RDS for PostgreSQL	This practice describes how to use DRS to synchronize data from a self-managed PostgreSQL database to an RDS for PostgreSQL DB instance.
	For PostgreSQL on Other Clouds to RDS for PostgreSQL	This practice describes how to use DRS to synchronize data from PostgreSQL databases on other clouds to RDS for PostgreSQL.
	From Oracle to RDS for PostgreSQL	This practice describes how to use DRS to synchronize data from a self-managed Oracle database to an RDS for PostgreSQL DB instance.
	From RDS for MySQL to RDS for PostgreSQL	This practice describes how to use DRS to synchronize data from an RDS for MySQL DB instance to an RDS for PostgreSQL DB instance.
	From Self-Managed MySQL to RDS for PostgreSQL	This practice describes how to use DRS to synchronize data from a self-managed MySQL database to an RDS for PostgreSQL DB instance.
	For MySQL on Other Clouds to RDS for PostgreSQL	This practice describes how to use DRS to synchronize data from MySQL databases on other clouds to RDS for PostgreSQL.
Data backup	**Intra-region automated backup**	This practice describes how RDS for PostgreSQL automatically creates backups for a DB instance during a backup window and saves the backups based on the configured retention period.
	Intra-region manual backup	This practice describes how to create manual backups for a DB instance. These backups can be used to restore data for improved reliability.
Data restoration	**Restoring from Full Backups to RDS for PostgreSQL Instances**	This practice describes how to use an automated or manual backup to restore a DB instance to how it was when the backup was created. The restoration is at the instance level.
	Restoring a DB Instance to a Point in Time	This practice describes how to use an automated backup to restore instance data to a specified point in time.

7 Getting Started with RDS for SQL Server Common Practices

After purchasing and connecting to a DB instance, you can view common practices to better use RDS for SQL Server.

Table 7-1 Common practices

Practice		Description
Suggestions on using RDS for SQL Server	**Instance Usage Suggestions**	This practice provides suggestions on DB instance class, database connection, database migration, and instance usage.
SSRS deployment	**Deploying SQL Server Reporting Services (SSRS) on RDS for SQL Server**	This practice describes how to deploy SSRS on RDS for SQL Server.
Data migration	**Migrating Data to RDS for SQL Server Using the Export and Import Functions of DAS**	This practice describes how to use Data Admin Service (DAS) to export data from the source and then import the data to an RDS for SQL Server DB instance.
	Migrating Data from an ECS-Hosted SQL Server Database to RDS for SQL Server Using the Export and Import Functions of SSMS	This practice describes how to use SQL Server Management Studio (SSMS) to migrate data from an ECS-hosted SQL Server database to an RDS for SQL Server DB instance.
	Migrating Data from an On-Premises SQL Server Database to RDS for SQL Server Using the Export and Import Functions of SSMS	This practice describes how to use SSMS to migrate data from an on-premises SQL Server database to an RDS for SQL Server DB instance.

Practice		Description
	Deploying SQL Server Reporting Services (SSRS) on RDS for SQL Server	This practice describes how to deploy SSRS on RDS for SQL Server.
	Migrating Backup Data of an RDS for SQL Server DB Instance to Another RDS for SQL Server DB Instance	This practice describes how to use DRS to migrate backup data from the source to an RDS for SQL Server DB instance.
	From RDS for SQL Server to RDS for SQL Server	This practice describes how to use DRS to synchronize data from an RDS for SQL Server DB instance to another RDS for SQL Server DB instance.
	Migrating Backup Data of an On-Premises SQL Server Database to an RDS for SQL Server DB Instance	This practice describes how to use DRS to migrate backup data of an on-premises SQL Server database to an RDS for SQL Server DB instance.
	From On-Premises SQL Server to RDS for SQL Server	This practice describes how to use DRS to synchronize data from an on-premises SQL Server database to an RDS for SQL Server DB instance.
	Migrating Backup Data of SQL Server Databases on Other Clouds to RDS for SQL Server	This practice describes how to use DRS to migrate backup data of SQL Server databases on other clouds to RDS for SQL Server.
	From SQL Server on Other Clouds to RDS for SQL Server	This practice describes how to use DRS to synchronize data from SQL Server databases on other clouds to RDS for SQL Server.
Data backup	Intra-region automated backup	This practice describes how RDS for SQL Server automatically creates backups for a DB instance during a backup window and saves the backups based on the configured retention period.
	Intra-region manual backup	This practice describes how to create manual backups for a DB instance. These backups can be used to restore data for improved reliability.

Practice		Description
Data restoration	**Restoring from Full Backups to RDS for SQL Server Instances**	This practice describes how to use an automated or manual backup to restore a DB instance to how it was when the backup was created. The restoration is at the instance level.
	Restoring a DB Instance to a Point in Time	This practice describes how to use an automated backup to restore instance data to a specified point in time.

A Change History

Released On	Description
2023-07-17	This issue is the twenty-seventh official release, which incorporates the following changes: - Added **Getting Started with RDS for MySQL Common Practices**. - Added **Getting Started with RDS for PostgreSQL Common Practices**. - Added **Getting Started with RDS for SQL Server Common Practices**.
2023-06-01	This issue is the twenty-sixth official release, which incorporates the following change: Supported multiple security groups for an RDS for PostgreSQL instance.
2023-05-10	This issue is the twenty-fifth official release, which incorporates the following change: Supported RDS for MariaDB.
2022-07-30	This issue is the twenty-fourth official release, which incorporates the following changes: - Supported multiple security groups for an RDS for MySQL instance.
2021-10-25	This issue is the twenty-third official release, which incorporates the following changes: Optimized the constraints on MySQL instance names.

Released On	Description
2021-09-27	This issue is the twenty-second official release, which incorporates the following changes: Supported AD domain for Microsoft SQL Server 2017 Standard Edition and 2017 Web Edition.
2021-07-22	This issue is the twenty-first official release, which incorporates the following changes: ● Supported 5-year yearly/monthly RDS for MySQL DB instances for subscription. ● Added the storage type **Extreme SSD** for buying an RDS for PostgreSQL DB instance.
2021-06-17	This issue is the twentieth official release, which incorporates the following change: ● Supported () and & for MySQL database account passwords.
2021-05-18	This issue is the nineteenth official release, which incorporates the following changes: Added the storage type **Extreme SSD** for buying an RDS for MySQL DB instance.
2021-04-21	This issue is the eighteenth official release, which incorporates the following change: Supported storage autoscaling for an RDS for MySQL DB instance.
2021-04-19	This issue is the seventeenth official release, which incorporates the following changes: Optimized the description of available instance classes and storage types for buying a MySQL DB instance.
2021-02-25	This issue is the sixteenth official release, which incorporates the following change: Adjusted the "Getting Started" outline.
2020-11-11	This issue is the fifteenth official release, which incorporates the following change: Supported the selection of your local time zone for RDS for SQL Server DB instances.

Released On	Description
2020-02-05	This issue is the fourteenth official release, which incorporates the following change: Added prompts for DB instance types during the DB instance purchase.
2019-12-30	This issue is the thirteenth official release, which incorporates the following change: ● Supported password setting after a DB instance is created.
2019-10-12	This issue is the twelfth official release, which incorporates the following changes: ● Optimized the constraints on the AD domain name. ● Adjusted the getting started structure. ● Optimized the description of binding and unbind EIPs.
2019-08-12	This issue is the eleventh official release, which incorporates the following changes: ● Optimized the password policy of purchasing DB instances. ● Supported database proxy for RDS for MySQL DB instances.
2019-07-12	This issue is the tenth official release, which incorporates the following changes: ● Supported batch creation of read replicas for RDS for MySQL DB instances. ● Supported a maximum of 10 read replicas for each RDS for MySQL primary DB instance. ● Added the root user permissions for RDS for MySQL DB instances.
2019-06-12	This issue is the ninth official release, which incorporates the following changes: ● Supported batch creation of read replicas during the DB instance creation. ● Supported access to RDS for MySQL DB instances through private domain names.

Released On	Description
2019-02-15	This issue is the eighth official release, which incorporates the following changes: ● Supported adding EIPs to the whitelist for RDS for SQL Server. ● Supported downloading incremental backups for RDS for PostgreSQL DB instances. ● Optimized the descriptions of connecting to RDS for MySQL, RDS for PostgreSQL, and RDS for SQL Server DB instances.
2018-11-20	This issue is the seventh official release, which incorporates the following changes: ● Supported RDS for PostgreSQL Enhanced Edition. ● Supported creating read replicas for RDS for SQL Server DB instances. ● Supported specifying a VIP when you create an RDS for SQL Server DB instance. ● Supported enterprise project management.
2018-09-04	This issue is the sixth official release, which incorporates the following changes: ● Optimized EIP mechanism for RDS for MySQL, RDS for PostgreSQL, and RDS for SQL Server.
2018-07-13	This issue is the fifth official release, which incorporates the following changes: ● Changed the default port number to **5432** when an RDS for PostgreSQL DB instance is created.

Released On	Description
2018-06-30	This issue is the fourth official release, which incorporates the following changes: ● Supported the configuration and change of the floating IP address for an RDS for MySQL DB instance. ● Supported enabling and disabling public accessibility for RDS for MySQL read replicas. ● Supported storage space scaling of RDS for MySQL and RDS for PostgreSQL DB instances numerous times. Each scaling must be a multiple of 10 GB. ● Supported storage space scaling of RDS for SQL Server DB instances by a multiple of 10 GB. ● Supported downloading backup data of a specific database for RDS for SQL Server.
2018-06-15	This issue is the third official release, which incorporates the following changes: ● Supported auto renewal during the creation of yearly/monthly DB instances. ● Increased the backup retention period to 732 days. ● Displayed the maximum number of connections for RDS for MySQL and RDS for PostgreSQL DB instances. ● Supported time zone selections when creating an RDS for MySQL DB instance. ● Supported 1 vCPU | 2 GB and 1 vCPU | 4 GB instance classes for RDS for PostgreSQL DB instances.

Released On	Description
2018-06-01	This issue is the second official release, which incorporates the following changes: ● Supported working with the DSS service. ● Supported a maximum of 4,000 GB of storage space when you create or scale up a DB instance. ● Supported parameter group selections during DB instance creation. ● Supported creating yearly/monthly DB instances in batches. ● Supported enabling and disabling public accessibility for MySQL DB instances. ● Changed the default port number to **3306** when an RDS for MySQL DB instance is created. ● Supported display of progress and logs of creating or scaling RDS for MySQL DB instances in the task center. ● Supported PostgreSQL 10. ● Supported Microsoft SQL Server 2008 R2 SP3 Enterprise Edition.
2018-05-04	This issue is the first official release.