Alibaba Cloud ApsaraDB for MySQL

Quick Start for MySQL

Issue: 20190716

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 Limits

To guarantee the stability and security of ApsaraDB for MySQL, certain limits are proposed.

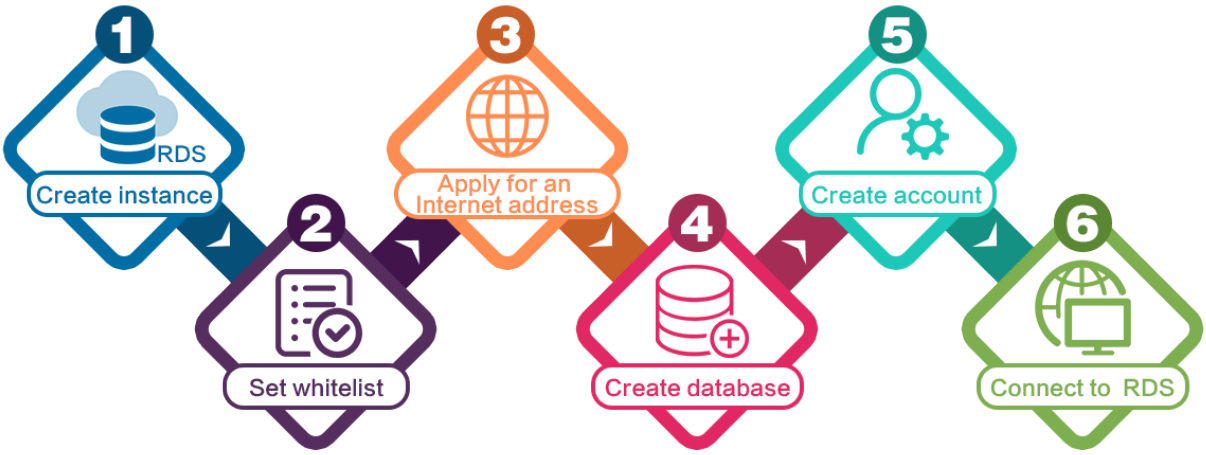
Items	Restrictions
Parameter modification	The RDS console or APIs must be used to modify database parameters. But some parameters cannot be modified. For more information, see Set parameters through the RDS console.
Root permission	The root or sa permission is not provided.
Backup	· Command lines or graphical interfaces can be used for logical backup. · For physical backup, the RDS console or APIs must be used.
Restoration	· Command lines or graphical interfaces can be used for logical restoration. · For physical restoration, the RDS console or APIs must be used.
Migration	· Command lines or graphical interfaces can be used for logical import. · You can use the MySQL command line tool or Data Transmission Service (DTS) to migrate data.
MySQL storage engine	· Currently only InnoDB and TokuDB are supported. The MyISAM engine has defects and may cause data loss. If you create MyISAM engine tables, they are automatically converted to InnoDB engine tables. For more information, see Why does RDS for MySQL not support the MyISAM engine? · The InnoDB storage engine is recommended for performance and security requirements. · The Memory engine is not supported. If you create Memory engine tables, they are automatically converted to InnoDB engine tables.
Replication	MySQL provides a dual-node cluster based on the master/slave replication architecture, so you manual deployment is not required . The slave instance in the architecture is invisible to you, and your application cannot access to the slave instance directly.
Restarting RDS instances	Instances must be restarted through the RDS console or APIs.

Items	Restrictions
User, password, and database management	By default, RDS console is used to manage users, passwords, and databases, including operations such as instance creation, instance deletion, permission modification, and password modification. MySQL also allows you to create a master account for finer-grained management.
Common account	· Does not support customized authorization. · The account management and database management interfaces are provided on the RDS console. · Instances that support common accounts also support master accounts.
Master account	· Support customized authorization. · SQL statements can be used for management.
Network settings	If a MySQL 5.5/5.6 instance is in a classic network and its access mode is safe connection mode, do not enable net.ipv4.tcp_timestamps in SNAT mode.

2 General process

This Quick Start describes the procedure from purchasing an RDS instance to using it.

Quick Start flowchart



1. Create an RDS for MySQL instance
2. Configure a whitelist
3. Apply for an Internet address
4. Create accounts and databases
5. Connect to an instance

3 Create an RDS for MySQL instance

You can use the RDS console or APIs to create an RDS instance. For more information about instance pricing, see Billing methods and billing items. This document describes how to use the RDS console to create an instance. For more information about how to use APIs to create an instance, see CreateDBInstance.

Prerequisites

You have registered an Alibaba Cloud account.

Precautions

- Subscription instances cannot be converted to Pay-As-You-Go instances.
- Pay-As-You-Go instances can be converted to Subscription instances. For operation instructions, see Change the billing method.
- An Alibaba Cloud account can create up to 30 Pay-As-You-Go RDS instances. You can open a ticket to apply for increasing the limit.

Procedure

1. Log on to the RDS console.
2. On the Instances page, click Create Instance.
3. Select a billing method:
   - Pay-As-You-Go: indicates post payment (billed by hour). For short-term requirements, create Pay-As-You-Go instances, because they can be released at any time to save costs.
   - Subscription: indicates prepayment. You need to pay when creating an instance. For long-term requirements, create Subscription instances because they are more cost-effective. Furthermore, the longer the subscription, the higher the discount.

4. Set the following parameters.

Parameter	Description
Region	Indicates the location of the RDS instance you want to purchase. The region cannot be changed after the purchase. · Select the region closest to your users for high access speed. · Make sure to select the region where your ECS instance is deployed so that the ECS instance can access the RDS instance through the intranet; otherwise, they intercommunicate through the Internet and the access speed is affected.
Database Engine	The supported database engines are MySQL, Microsoft SQL Server, PostgreSQL, PPAS (compatible with Oracle), and MariaDB TX. In this example, select MySQL. Note: The available database engines vary depending on the region you select.
Version	For RDS for MySQL, the supported versions are MySQL 5.5, 5.6, 5.7, and 8.0. Note: The available versions vary depending on the region you select.
Edition	RDS for MySQL instances support the Basic Edition and High-availability Edition. · Basic Edition: It provides a single node and separates computing from storage, and is extremely cost-effective. · High-availability Edition: It adopts the high-availability architecture with one master node and one slave node. It is applicable to over 80% of scenarios. Note: The available product series vary depending on the region you select. For more information on the product series, see Product series overview.

Parameter	Description
Zone	A zone is a physical area within a region. Different zones in the same region are basically the same. You can deploy the master slave nodes of an RDS instance in the same zone or in different zones.
Network type	· Classic Network: indicates the traditional network type. · VPC (recommended): short for Virtual Private Cloud. A VPC is an isolated network environment and therefore provides higher security and performance than the classic network. Note: Make sure the network type is the same as that of your ECS instance so that the ECS instance can access the RDS instance through the intranet.
Type	Indicates instance specifications. For specific resources (CPU cores, memory, maximum number of connections, and IOPS) provided by each instance type, see Instance type list. RDS supports the following instance type families: · General-purpose instance: owns dedicated memory and I/O resources, but shares CPU and storage resources with other general-purpose instances on the same server. · Dedicated instance: owns dedicated CPU, memory, storage, and I/O resources. · Dedicated host: owns all the CPU, memory, storage, and I/O resources on the server on which it is located. For example, 8 Cores 32 GB (Basic) indicates a general-purpose instance, and 8 Cores 32 GB (Dedicated) indicates a dedicated instance.
Capacity	The capacity is used for storing data, system files, binlog files, and transaction files.

5. Set the duration (only for Subscription instances) and quantity, and click Buy Now.

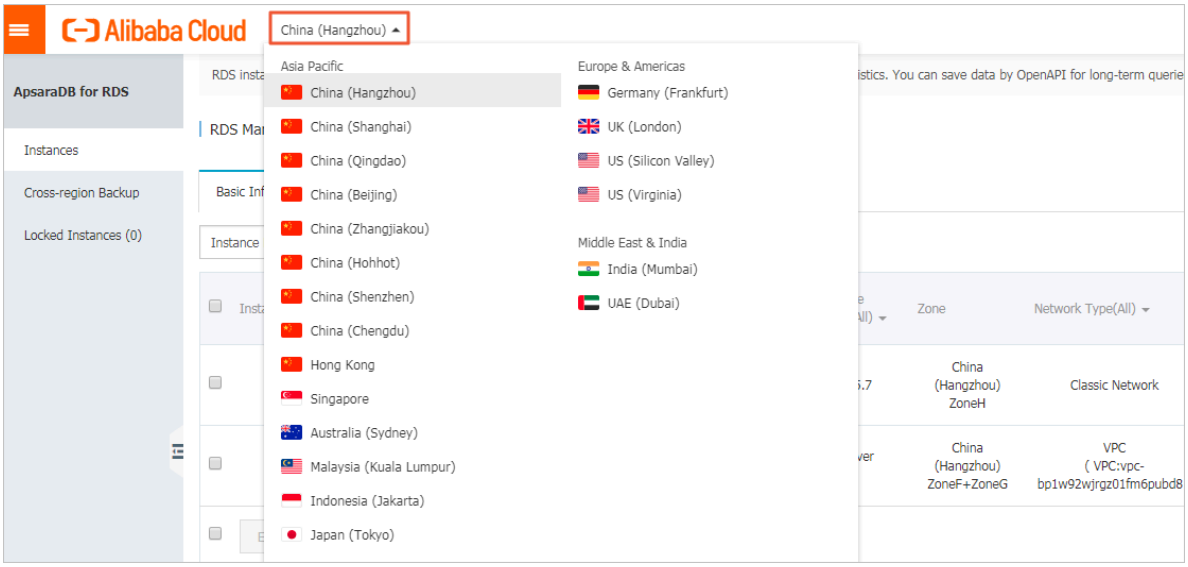
Note:
For a Subscription instance, you can:

- Select Auto Renew in the Duration section. Then the system can automatically deduct fees to extend the validity period of your instance. For example, if you purchase a three-month Subscription instance with Auto Renew selected, the system automatically deducts frees of three months when the instance is about to expire.
- Click Add to Cart and then click the cart to place the order.

6. On the Order Confirmation page, review the order information, select Terms of Service, Service Level Agreement, and Terms of Use, click Pay Now, and complete the payment.

What to do next

1. In the upper left corner of the RDS console, select the region where the instance is located, and view the instance details.



2. Configure a whitelist.
3. Create a databse account.
4. Apply for an Internet address (if you want to access RDS through the Internet).
5. Connect to the RDS instance.

FAQ

How do I authorize a RAM user to manage RDS instances?

See Manage RDS permissions by using RAM.

APIs

API	Description
CreateDBInstance	Used to create an RDS instance.

4 Initial configuration

4.1 Set the whitelist

To ensure database security and stability, before you start using an RDS instance, you must whitelist the IP addresses or IP address segments that need to access the database. We recommend that you periodically check and adjust your whitelist according to your requirements to maintain RDS security. This document provides information about and the procedure of setting a whitelist.

Background information

You can access the RDS instance through the intranet, the Internet, or both the intranet and Internet. For more information about the applicable scenarios of each connection type (intranet and Internet), see Background information of Set intranet and Internet addresses.

Before setting the connection type, you must add the IP addresses or IP address segments of your application service or the ECS instance to the whitelist of your RDS instance. When the whitelist is set, the system automatically generates the intranet IP address for the RDS instance. If you need an Internet IP address, refer to Apply for an Internet address.

Note:

If you cannot connect to the RDS instance after adding the application service IP address to the whitelist, refer to How to locate the local IP address using ApsaraDB for MySQL to obtain the actual IP address of the application service.

Attention

- The system automatically creates a default whitelist group for each newly created RDS instance. This default whitelist group can only be modified or cleared, but cannot be deleted.
- For each newly created RDS instance, the local loopback IP address 127.0.0.1 is added to the default whitelist group by default. This means that all the IP addresses or IP address segments are prohibited to access this RDS instance. Therefore, you

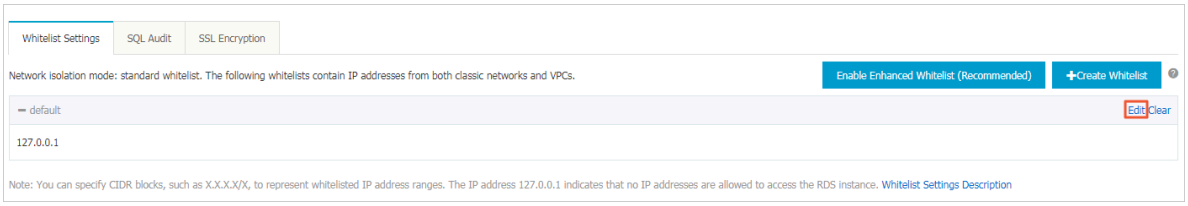
must delete 127.0.0.1 from the default whitelist group before you add other IP addresses or IP address segments to the whitelist.

- % or 0.0.0.0/0 indicates any IP address is allowed to access the RDS instance. This configuration greatly reduces the security of the database and is not recommended .

Procedure

1. Log on to the RDS console.
2. Select the region where the target instance is located.
3. Click the name of the target instance to go to the Basic Information page.
4. Select Security Controls in the left-side navigation pane to visit the Security Controls page.
5. On the Whitelist Settings tab page, click Modify of the default whitelist group, as shown in the following figure.

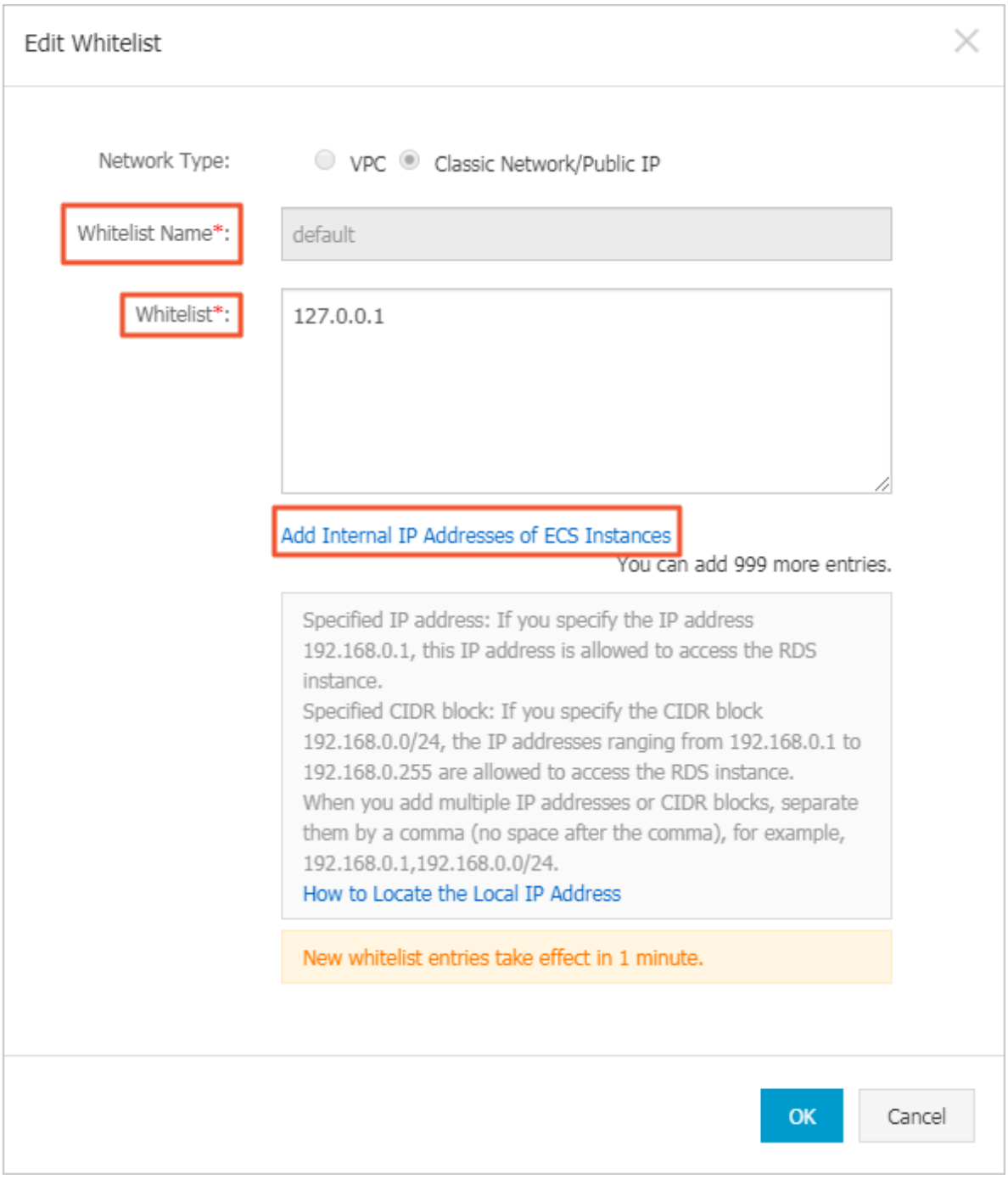
   Note:
   If you want to add a customized whitelist group to the RDS instance, you can click Clear of the default whitelist group to delete the IP address 127.0.0.1 first, and then click Add a Whitelist Group. The setting steps for a customized whitelist are similar to the following steps.



6. On the Modify Group page, add the IP addresses or IP address segments allowed to access the RDS instance to the Whitelist field. If you want to add the ECS intranet IP addresses, click Upload ECS Intranet IP Address and select the IP addresses according to the prompt window, as shown in the following figure.

   Note:

After you add a new IP address or IP address segment to the default group, the loopback address 127.0.0.1 is automatically deleted.



Parameters description:

- `Group Name` **: It can contain 2 to 32 characters including lowercase letters, digits, or underscores (_). The group name must start with a lowercase letter**

and end with a letter or digit. This name cannot be modified once the whitelist group is successfully created.

- `Whitelist` : Enter the customized IP addresses or IP address segments that are allowed to access the RDS instance.
  - If you enter an IP address segment, such as 10.10.10.0/24, it indicates that any IP address in the format of 10.10.10.X can access the RDS instance.
  - If you want to enter multiple IP addresses or IP address segments, separate them by commas (,) (do not add blank spaces), such as 192.168.0.1,172.16.213.9.
  - For each whitelist group, up to 1,000 IP addresses or IP address segments can be set for MySQL, PostgreSQL, and PPAS instances and up to 800 can be set for SQL Server instances.
- Upload ECS intranet IP Address: By clicking this button, you can select the intranet IP address of the ECS instance under the same account as the RDS instance. This is a quick method to add ECS intranet IP address.

7. Click OK.

Modify or delete the whitelist group

You can modify or delete the whitelist group according your business requirements. The detailed procedure is as follows:

1. Log on to the RDS console.
2. Select the region where the target instance is located.
3. Click the name of the target instance to go to the Basic Information page.
4. Select Security in the left-side navigation pane.
5. On the Whitelist Settings tab page, click the Modify or Delete button of the target whitelist group.
6. Click OK after you modify the IP addresses or IP address segments. Alternatively, click Confirm if you are sure that the whitelist group is to be deleted.

4.2 Apply for an Internet address

RDS provides two types of addresses: intranet addresses and Internet addresses.

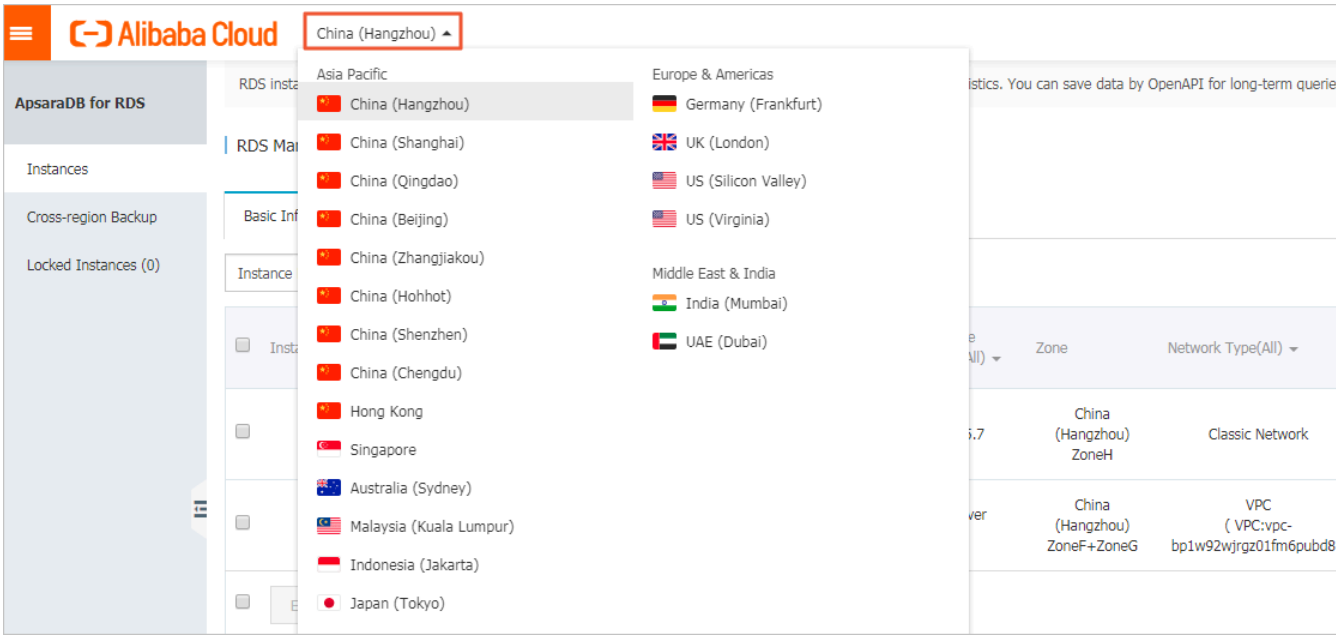
Intranet and Internet addresses

Address	Description
Intranet address	The intranet address is generated by default. Use the intranet address if all of the following conditions are met: · Your application is deployed on an ECS instance. · The ECS instance is located in the same region as your RDS instance. · The ECS instance has the same network type as your RDS instance. The intranet address is recommended because accessing RDS through the intranet is most secure and delivers optimal performance.
Internet address	You need to manually apply for the Internet address. You can also release it anytime. Use the Internet address if you cannot access RDS through the intranet. Specific scenarios are as follows: · An ECS instance accesses your RDS instance but the ECS instance is located in a different region or has a network type different from your RDS instance. · A server or computer outside Alibaba Cloud accesses your RDS instance. Note: · The Internet address and traffic are currently free of charge. · Using the Internet address reduces security. Please exercise caution . · To ensure high security and performance, we recommend that you migrate your application to an ECS instance that is in the same region and has the same network type as your RDS instance and then use the intranet address.

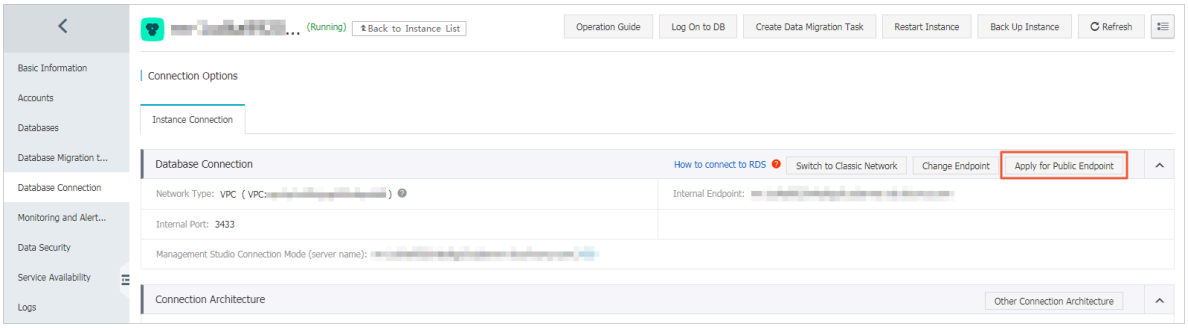
Apply for an Internet address

1. Log on to the RDS console.

2. In the upper-left corner, select the region where the RDS instance is located.



3. Find the RDS instance and click its ID.
4. In the left-side navigation pane, click Database Connection.
5. Click Apply for Public Endpoint.



6. In the displayed dialog box, click OK.

   The Internet address is generated.

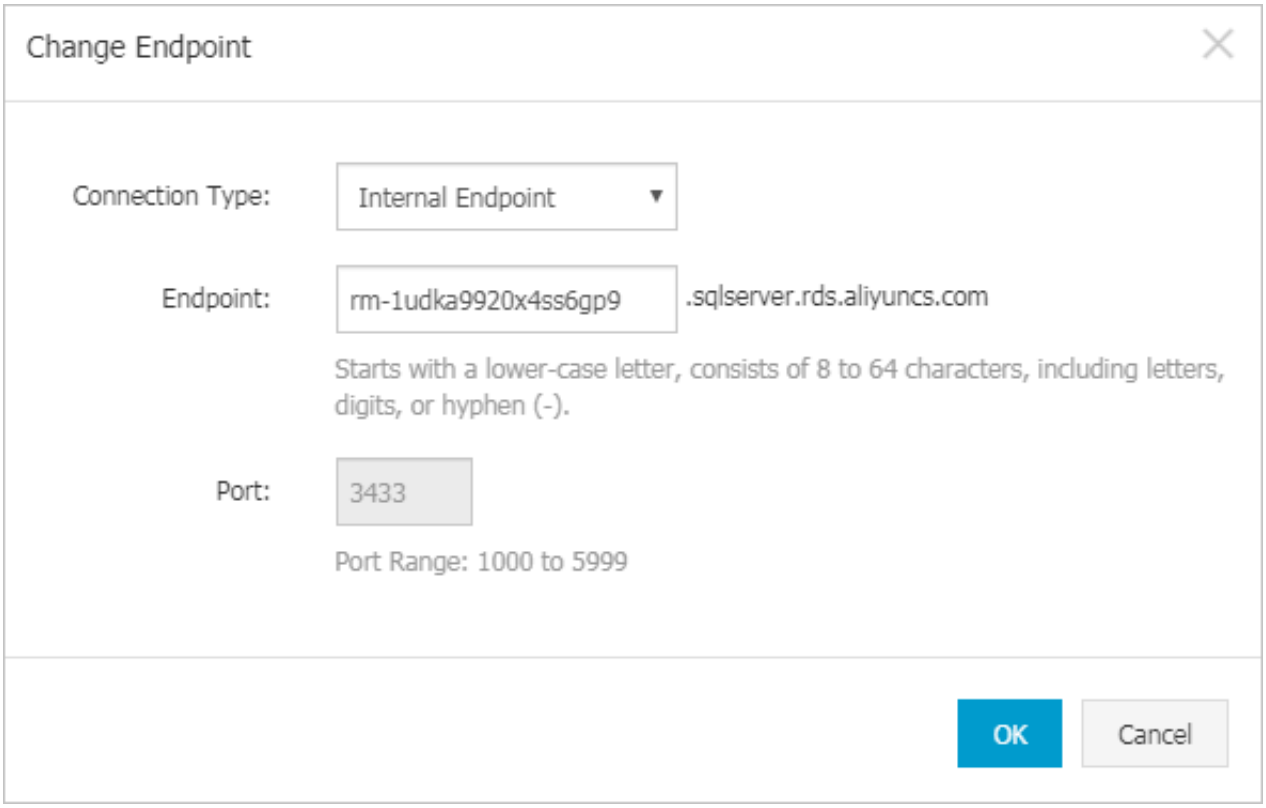
7. Optional. To modify the Internet address or port number, click Change Endpoint. In the displayed dialog box, select a connection type, set the Internet address and port number, and click OK.

   - Connection Type: Select Public endpoint.

   Note:

The Public endpoint option is available only after you have applied for the Internet address.

- Endpoint: The address contains 8 to 64 characters, including letters, digits, and hyphens (-). The address prefix must start with a lower-case letter.
- Port: The port number can be modified only when the RDS network type is classic network.



APIs

API	Description
AllocateInstancePublicConnection	Used to apply for an Internet address.

4.3 Create accounts and databases

This article describes how to create accounts and databases for an RDS for MySQL instance.

Account types

RDS for MySQL supports two types of database accounts: superuser accounts and standard accounts. You can manage all your accounts and databases on the console. For specific privileges, see Account privileges.

Account Type	Description
Superuser account	· Can only be created and managed through the console or API. · Each instance can have only one superuser account, which can be used to manage all databases and standard accounts. · Has more privileges than standard accounts and can manage privileges at a more fine-grained level. For example, it can assign table-level query privileges to other accounts. · Can disconnect the connections established by any other accounts.
Standard account	· Can be created and managed through the console, API, or SQL statements. · Each instance can have up to 200 standard accounts. · Need to be manually granted with database privileges. · Cannot create or manage other accounts, or terminate the connections established by other accounts.

Account Type	Number of databases	Number of tables	Number of users
Superuser account	Unlimited	< 200,000	Varies depending on the instance kernel parameters.
Standard account	500	<200,000	Varies depending on the instance kernel parameters.

Differences between the superuser account privileges and SUPER privileges

Superuser account privileges

- Can manage all databases and standard accounts. Account privileges lists the privileges of the superuser account.
- Can terminate the connections established by other accounts.
- Running the `show processlis t` command shows only the processes of the current account, excluding processes on the control level.

SUPER privileges

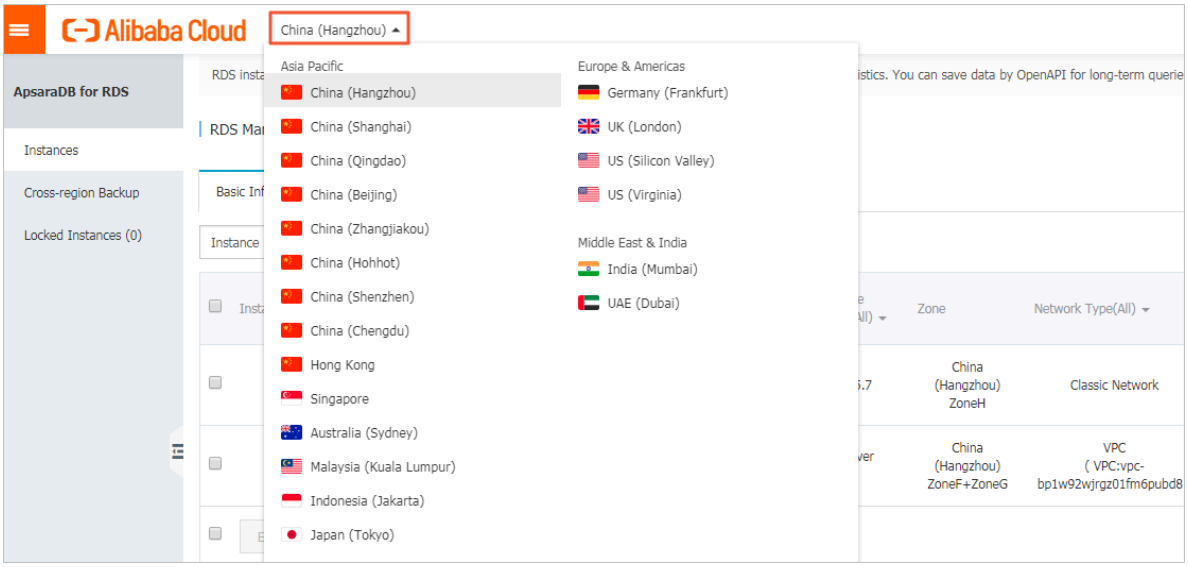
To prevent potential incorrect operations, RDS for MySQL does not provide the SUPER privileges.

- Can terminate any connections.

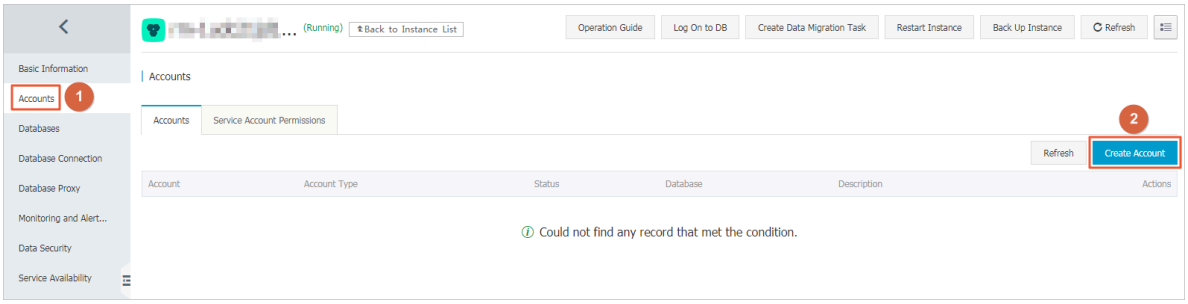
- Running the `show processlis t` command shows all processes, including processes on the control level.
- Can use the `SET` statement to modify any global variables.
- Can use the `CHANGE MASTER` and `PURGE MASTER LOGS` commands.
- Can perform operations on files stored on the host.

Create the superuser account

1. Log on to the RDS console.
2. In the upper-left corner of the page, select the region where the instance is located.



3. Find the target instance and click its ID.
4. In the left-side navigation pane, click Accounts.
5. Click Create Account.



6. Set the following parameters.

Parameter	Description
Database Account	Enter the account name. Requirements are as follows: · Consists of 2 to 16 characters. · Starts with a letter and ends with a letter or digit. · Consists of lower-case letters, digits, or underscores (_).
Account Type	Select Superuser Account.
Password	Enter the account password. Requirements are as follows: · Consists of 8 to 32 characters. · Contains at least three of the following types: upper-case letters, lower-case letters, digits, and special characters. These special characters are as follows: ! @ # $ % ^ & * ( ) _ + -
Re-enter Password	Enter the password again.
Note	Enter relevant information, with up to 256 characters.

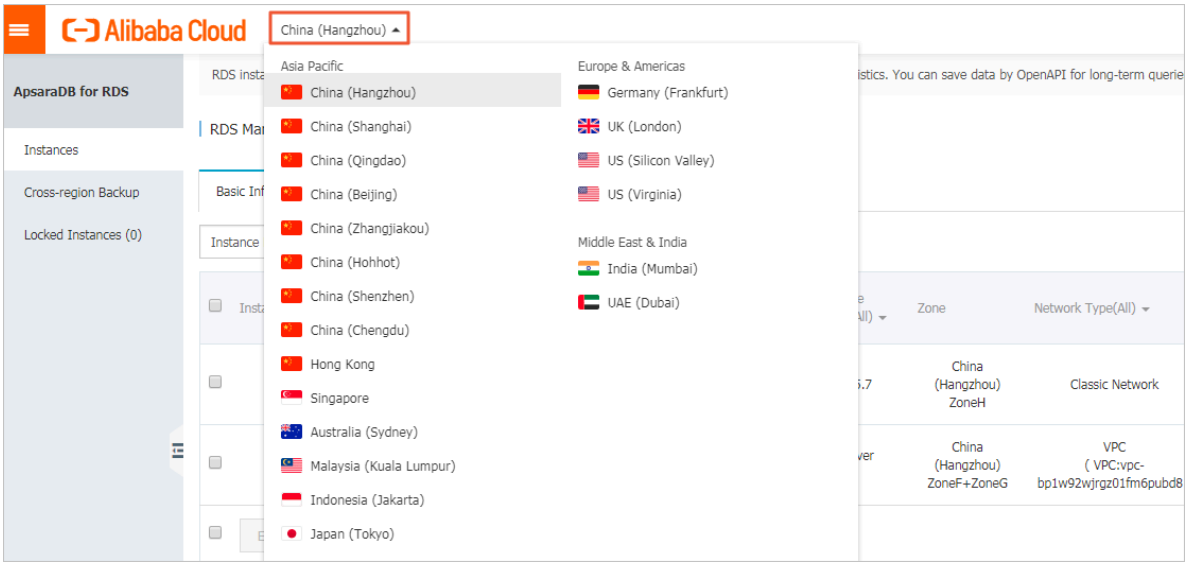
7. Click OK.

Reset the privileges of the superuser account

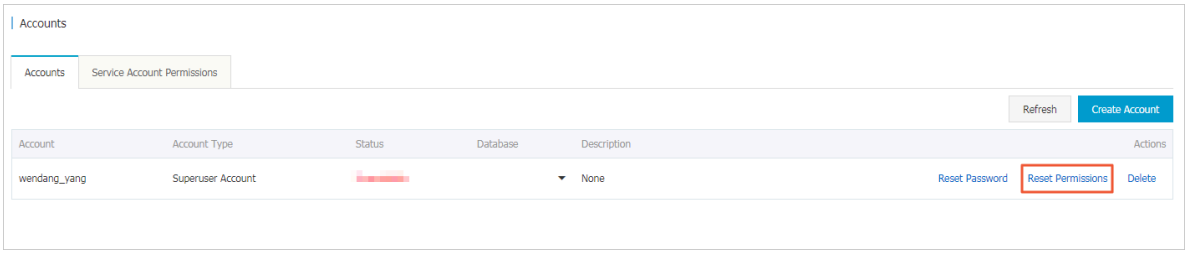
If the superuser account is abnormal (for example, privileges are unexpectedly revoked), you can reset the privileges.

1. Log on to the RDS console.

2. In the upper-left corner of the page, select the region where the instance is located.



3. Find the target instance and click its ID.
4. In the left-side navigation pane, click Accounts.
5. Click Reset Account Permissions for the superuser account.

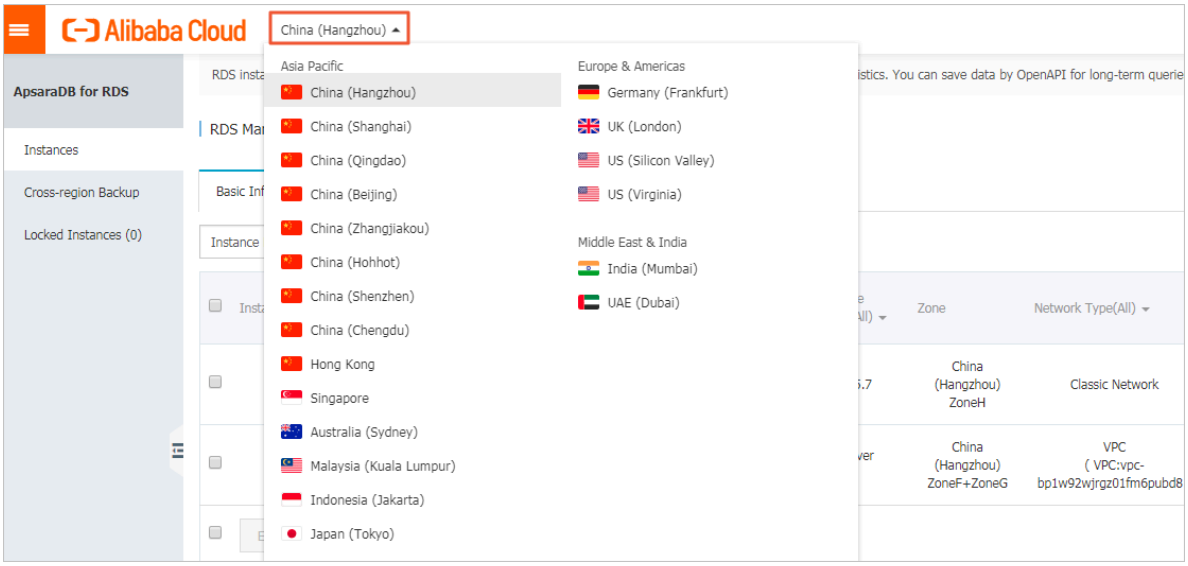


6. Enter the superuser account password to reset the account privileges, and then click OK.

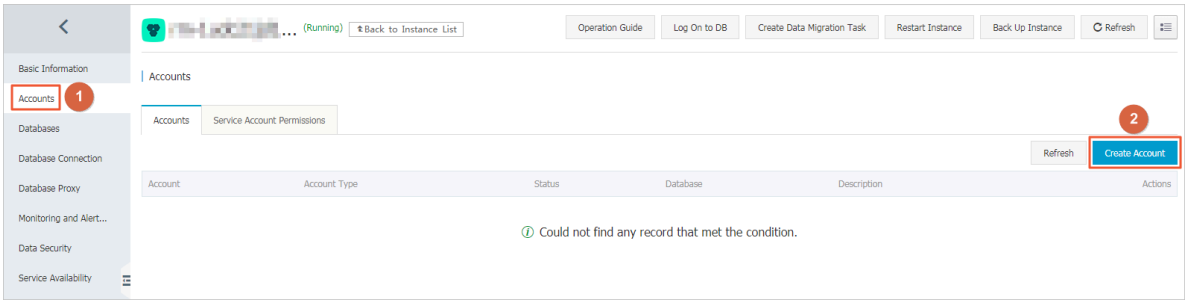
Create a standard account

1. Log on to the RDS console.

2. In the upper-left corner of the page, select the region where the instance is located.



3. Find the target instance and click its ID.
4. In the left-side navigation bar, click Accounts.
5. Click Create Account.



6. Set the following parameters.

Parameter	Description
Database Account	Enter the account name. Requirements are as follows: · Consists of 2 to 16 characters. · Starts with a letter and ends with a letter or digit. · Consists of lower-case letters, digits, or underscores (_).
Account Type	Select Standard Account.

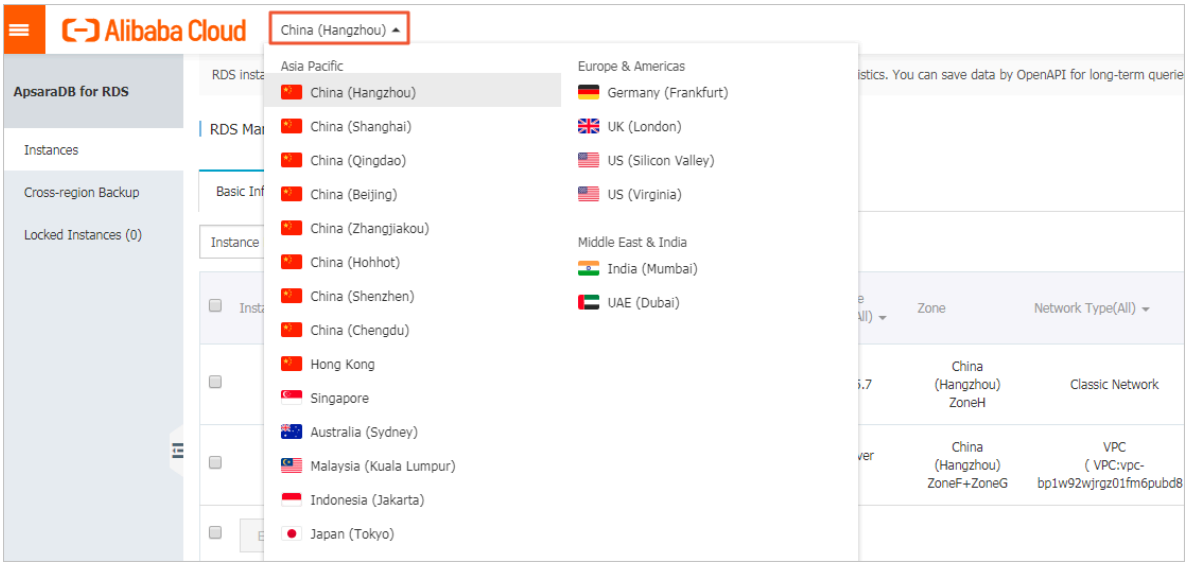
Parameter	Description
Authorized Database	Grant database privileges to this account. You can also leave this field blank and grant privileges to the account after the account is created. a. Select one or more databases from the left, and click Add to add the selected database to the right-hand box. b. In the right-hand box, select Read/Write, Read-only, DDL Only, or DML Only. If you want to set the privileges of multiple databases at the same time, click the button (for example, Grant All Read/Write) in the upper-right corner of the right-hand box. Note: The button in the upper-right corner changes as you click.
Password	Enter the account password. Requirements are as follows: · Consists of 8 to 32 characters. · Contains at least three of the following types: upper-case letters , lower-case letters, digits, and special characters. These special characters are as follows: ! @ # $ % ^ & * ( ) _ + - =
Re-enter Password	Enter the password again.
Note	Enter relevant information, with up to 256 characters.

7. Click OK.

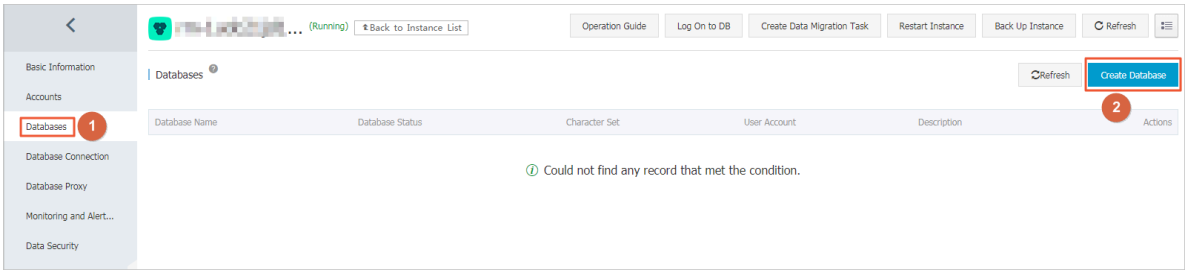
Create a database

1. Log on to the RDS console.

2. In the upper-left corner of the page, select the region where the instance is located.



3. Find the target instance and click its ID.
4. In the left-side navigation pane, click Databases.
5. Click Create Database.



6. Set the following parameters.

Parameters	Description
Database Name	· Consists of 2 to 64 characters. · Starts with a letter and ends with a letter or a digit. · Consists of lower-case letters, digits, underscores (_), or hyphens (-). · Must be unique in the instance.
Supported Character Set	Select utf8, gbk, latin1, or utf8mb4. If you need another character set, select all and then select the character set from the list.

Parameters	Description
Authorized Account	Select the account that needs to access this database. You can also leave this field blank and set the authorized account after the database is created. Note: Only standard accounts are displayed, because the superuser account already has privileges for all databases.
Account Type	Select Read/Write, Read-only, DDL only, or DML only.
Remarks	Optional. Enter relevant information, with up to 256 characters.

7. Click OK.

Account privileges

Acc type	授权类型	权限				
高权限账号	-	SELECT	INSERT	UPDATE	DELETE	CREATE
		DROP	RELOAD	PROCESS	REFERENCES	INDEX
		ALTER	CREATE TEMPORARY TABLES	LOCK TABLES	EXECUTE	REPLICATION SLAVE
		REPLICATION CLIENT	CREATE VIEW	SHOW VIEW	CREATE ROUTINE	ALTER ROUTINE
		CREATE USER	EVENT	TRIGGER		
普通账号	只读	SELECT	LOCK TABLES	SHOW VIEW	PROCESS	REPLICATION SLAVE
		REPLICATION CLIENT				
	读写	SELECT	INSERT	UPDATE	DELETE	CREATE
		DROP	REFERENCES	INDEX	ALTER	CREATE TEMPORARY TABLES
		LOCK TABLES	EXECUTE	CREATE VIEW	SHOW VIEW	CREATE ROUTINE

Acc type	授权类型	权限				
		ALTER ROUTINE	EVENT	TRIGGER	PROCESS	REPLICATION SLAVE
		REPLICATION CLIENT				
	仅DDL	CREATE	DROP	INDEX	ALTER	CREATE TEMPORARY TABLES
		LOCK TABLES	CREATE VIEW	SHOW VIEW	CREATE ROUTINE	ALTER ROUTINE
		PROCESS	REPLICATION SLAVE	REPLICATION CLIENT		
	只DML	SELECT	INSERT	UPDATE	DELETE	CREATE TEMPORARY TABLES
		LOCK TABLES	EXECUTE	SHOW VIEW	EVENT	TRIGGER
		PROCESS	REPLICATION SLAVE	REPLICATION CLIENT		

Account type	Privilege type	Privileges				
Superuser account	-	SELECT	INSERT	UPDATE	DELETE	CREATE
		DROP	RELOAD	PROCESS	REFERENCES	INDEX
		ALTER	CREATE TEMPORARY TABLES	LOCK TABLES	EXECUTE	REPLICATION SLAVE
		REPLICATION CLIENT	CREATE VIEW	SHOW VIEW	CREATE ROUTINE	ALTER ROUTINE
		CREATE USER	EVENT	TRIGGER		
Standard account	Read-only	SELECT	LOCK TABLES	SHOW VIEW	PROCESS	REPLICATION SLAVE

Account type	Privilege type	Privileges				
		REPLICATION CLIENT				
	Read/write	SELECT	INSERT	UPDATE	DELETE	CREATE
		DROP	REFERENCES	INDEX	ALTER	CREATE TEMPORARY TABLES
		LOCK TABLES	EXECUTE	CREATE VIEW	SHOW VIEW	CREATE ROUTINE
		ALTER ROUTINE	EVENT	TRIGGER	PROCESS	REPLICATION SLAVE
		REPLICATION CLIENT				
	DDL only	CREATE	DROP	INDEX	ALTER	CREATE TEMPORARY TABLES
		LOCK TABLES	CREATE VIEW	SHOW VIEW	CREATE ROUTINE	ALTER ROUTINE
		PROCESS	REPLICATION SLAVE	REPLICATION CLIENT		
	DML only	SELECT	INSERT	UPDATE	DELETE	CREATE TEMPORARY TABLES
		LOCK TABLES	EXECUTE	SHOW VIEW	EVENT	TRIGGER
		PROCESS	REPLICATION SLAVE	REPLICATION CLIENT		

5 Connect to an instance

Background

After creating an instance, setting the whitelist, and creating a database account, you can connect to te RDS for MySQL instance through any MySQL client or your application by configuring the connection address, port number, and account information. The MySQL client and your application can be deployed on ECS or a local computer.

If you are connecting from ECS to RDS through the intranet address, make sure that:

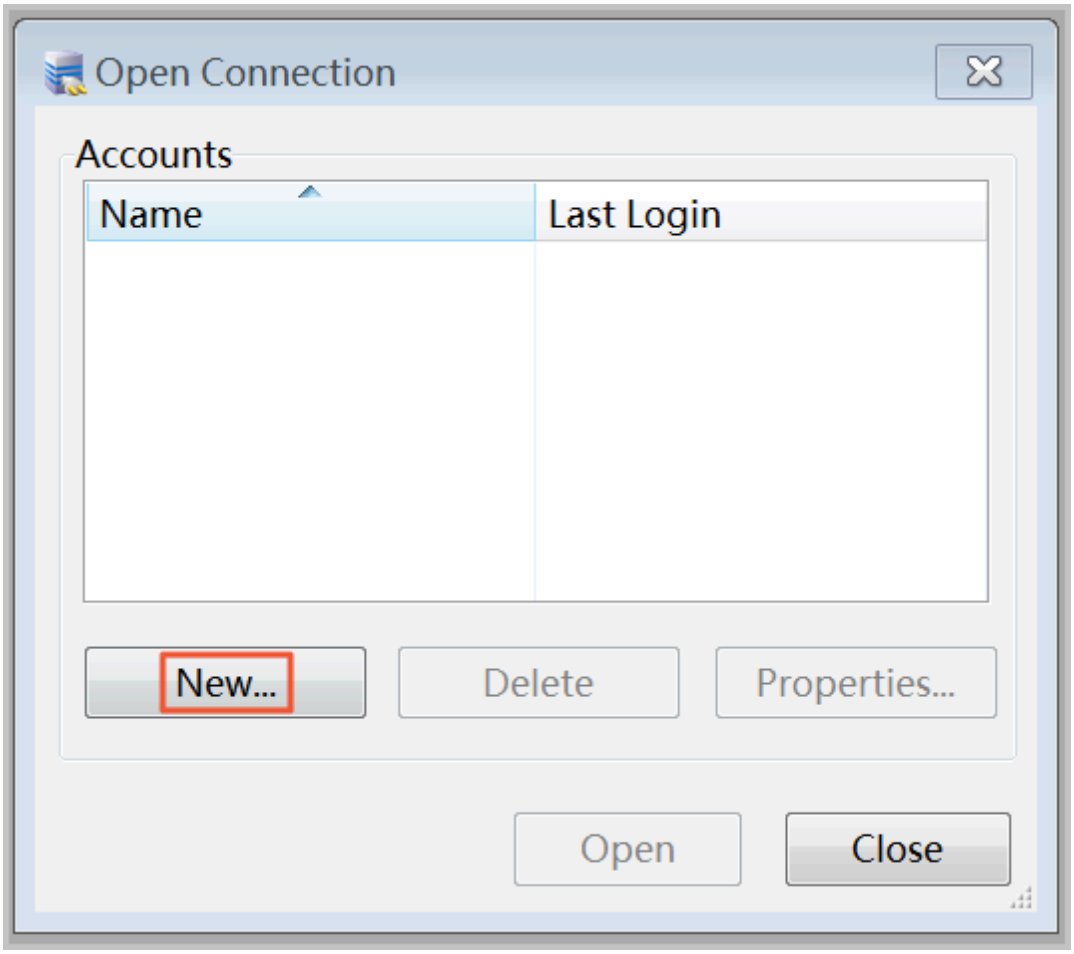
- The ECS and RDS instances are both in the classic network or in the same VPC.
- You have added the ECS intranet address to the RDS whitelist.

Use a client to connect to RDS for MySQL

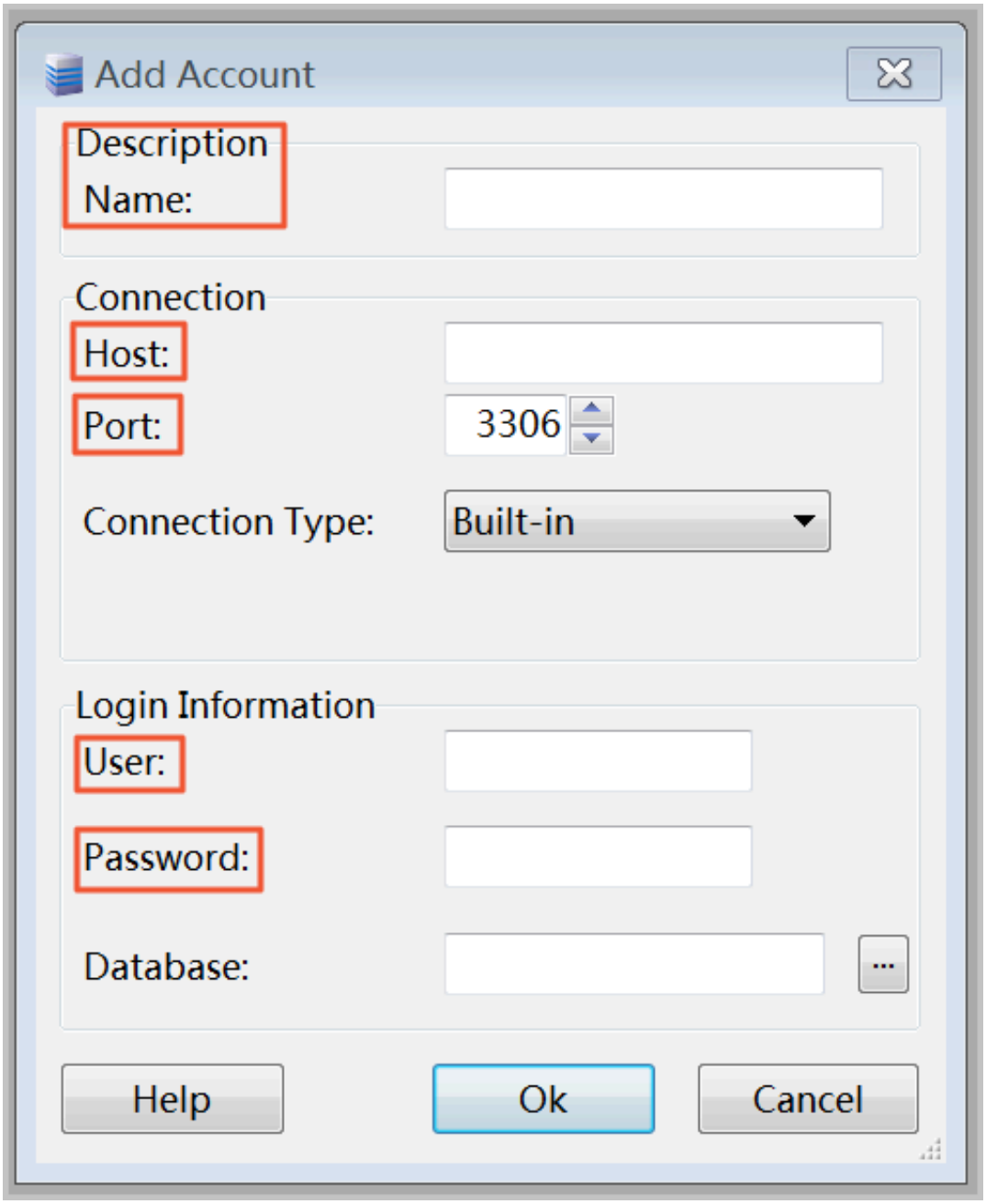
The following uses MySQL-Front as an example.

1. Start the MySQL-Front client.

2. In the Open Connection window, click New.



3. Enter the RDS connection information.



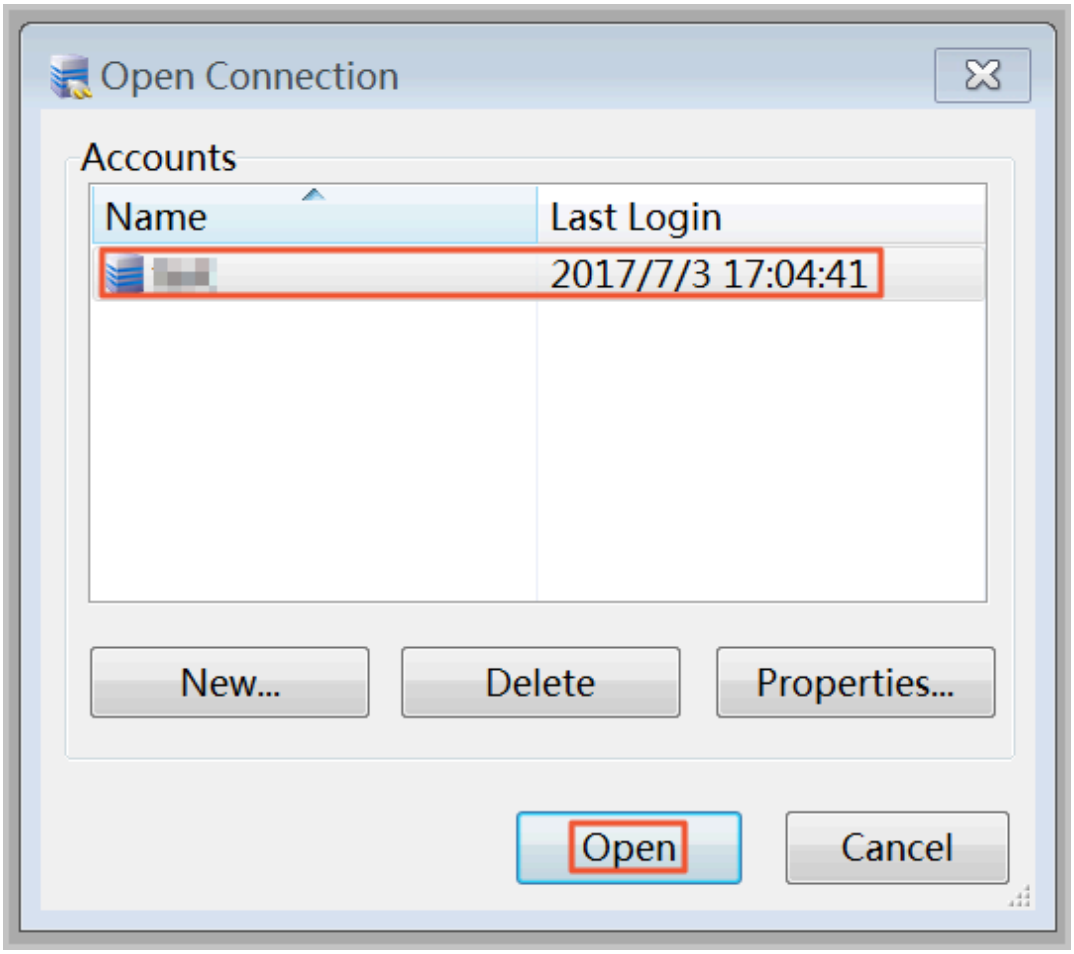
Parameter	Description
Description Name	Enter the connection task name. It is the same as the Host field by default.

Parameter	Description
Host	Enter the intranet or Internet address of the RDS instance. · If your client is deployed on an ECS instance that is in the same region and has the same network type as your RDS instance, use the intranet address. · In other cases, use the Internet address. You can view the address and port information as follows: a. Log on to the RDS console. b. Select the region where the target instance is located. c. Click the ID of the instance to visit the Basic Information page. d. In the Basic Information area, you can find the Internet and intranet addresses and port numbers. 
Port	· Enter the intranet port number if you use an intranet address. · Enter the Internet port number if you use an Internet address.
User	Enter an account name of the RDS instance.
Password	Enter the password of the preceding account.

4. Click OK.

5. In the Open Connection window, select the connection that you created and click Open.

   If the connection information is correct, the RDS instance gets connected successfully.



6 Scale instances

6.1 Read-only instance

6.1.1 Introduction to MySQL read-only instances

Scenario

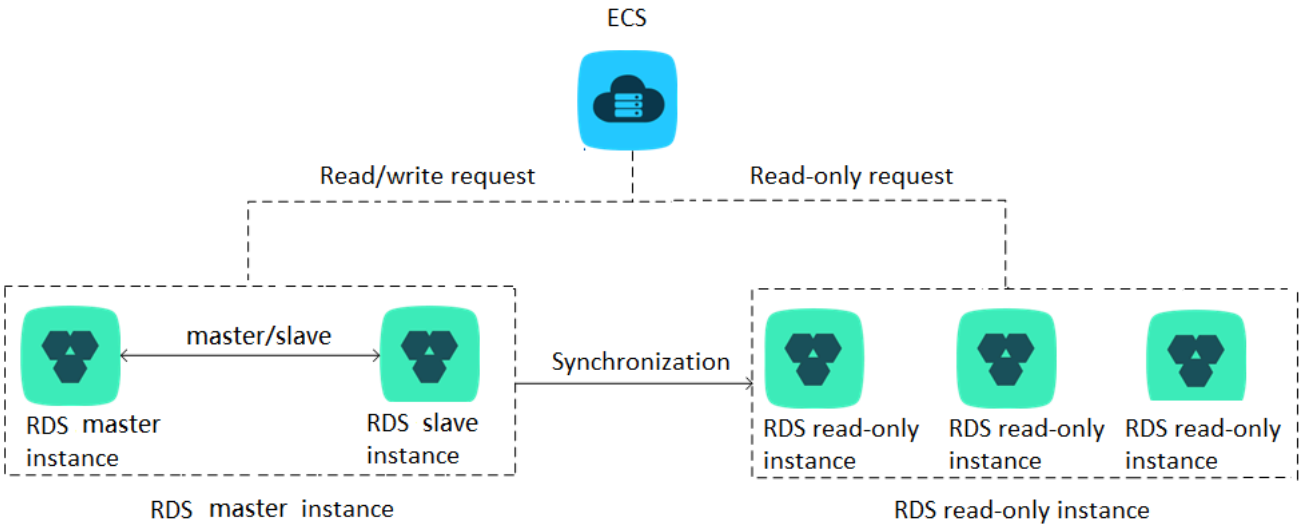
For services that involve a small number of write requests but a great number of read requests, a single instance may not be able to resist the read pressure. As a result, services may be affected. To achieve the elastic expansion of the read ability and share the pressure of the database, you can create one or more read-only instances in a region. The read-only instances can handle massive read requests and increase the application throughput.

Overview

A read-only instance is a read-only copy of the master instance. Changes to the master instance are also automatically synchronized to all relevant read-only instances. The synchronization works even if the master and read-only instances have different network types. Read-only instances and the master instance must be in the same region, but they can be in different zones. The following topology shows the positioning of the read-only instance.

Note:

- Currently the following instances support read-only instances:
  - MySQL 5.7 High-Availability Edition (based on local SSDs)
  - MySQL 5.6
  - SQL Server 2017
- Each read-only instance adopts a single-node architecture (without slave nodes).



Pricing

The billing method of read-only instances is Pay-As-You-Go. For more information, see Pricing.

> Note:
> For information about data retention policies for read-only instances, see Impact of expiration and overdue payment.

Features

Read-only instances offer the following features:

- The specifications of a read-only instance differ from those of the master instance, and can be changed at any time, to facilitate easy elastic upgrade and downgrade.
- Read-only instances support billing measured per hour, which is user-friendly and cost-efficient.
- No account or database maintenance is required for a read-only instance. Both the account and database are synchronized through the master instance.
- Read-only instances support independent whitelist configuration.
- Read-only instances support system performance monitoring.

  Up to 20 system performance monitoring views can be used, which includes disk capacity, IOPS, connections, CPU utilization, and network traffic. Users can view the load of instances at ease.

- Read-only instances provide optimization suggestions.

  Optimization tools support storage engine check, primary key check, large table check, and excessive indexing and missing indexing checks.

Restrictions

- Quantity of read-only instances

Database type	Memory	Max number of read-only instances
MySQL	⩾ 64 GB	10
	< 64 GB	5

- Read-only instances do not support backup settings or temporary backup.
- Instance recovery:
  - Read-only instances do not support the creation of temporary instances through backup files or backups at any point in time. Read-only instances do not support the overwriting of instances using backup sets.
  - After creating a read-only instance, the master instance does not support data recovery through the direct overwriting of instances using backup sets.
- You cannot migrate data to read-only instances.
- You cannot create or delete databases for read-only instances.
- You cannot create or delete accounts for read-only instances.
- You cannot authorize accounts or modify account passwords for read-only instances.

FAQs

Can the accounts on the master instance be used on the read-only instances?

Answer: Accounts on the master instance are synchronized to the read-only instances . You can use the accounts to read data from the read-only instances but cannot write data into the read-only instances.

6.1.2 Create a read-only instance

You can create read-only instances to process massive read requests sent to the database and increase the application throughput. A read-only instance is a read-only copy of the master instance. Changes to the master instance are also automatica

lly synchronized to all relevant read-only instances through the native replication capability of MySQL.

Attention

- Currently the following instances support read-only instances:
  - MySQL 5.7 High-Availability Edition (based on local SSDs)
  - MySQL 5.6
  - SQL Server 2017
- Quantity of read-only instances

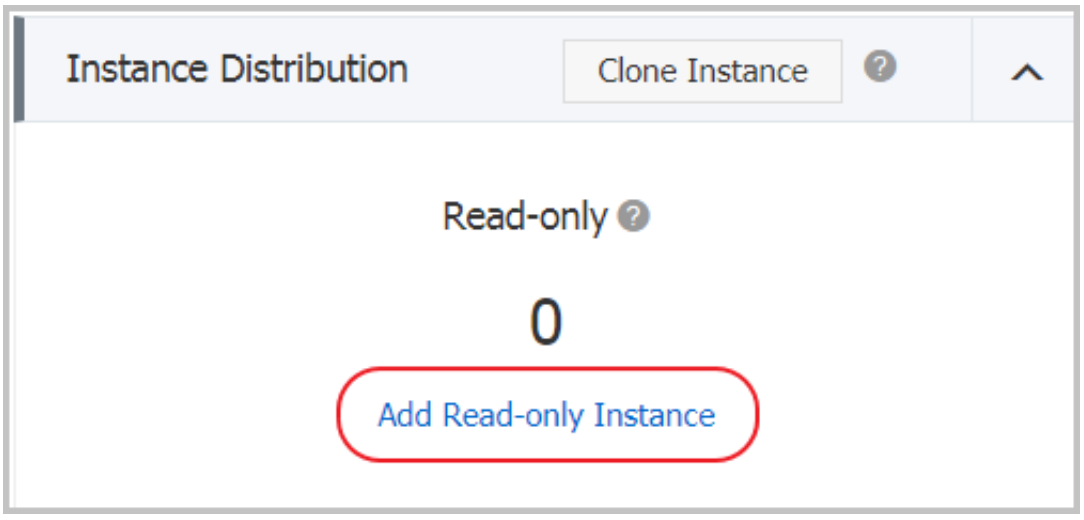
Database type	Memory	Max number of read-only instances
MySQL	⩾ 64 GB	10
	< 64 GB	5
SQL Server	Any	7

- Read-only instance is subject to an additional charge and its billing method is Pay-As-You-Go. For more information, see Pricing for read-only instances.
- The read-only instance automatically copies the whitelist its master instance, but the whitelist of the read-only instance and that of the master instance are independent. To modify the whitelist of the read-only instance, see Configure a whitelist.

Procedure

1. Log on to the RDS console.
2. Select the region where the target instance is located.
3. Click the ID of the target instance to visit the Basic Information page.

4. In the Instance Distribution area, click Add Read-only Instance, as shown in the following figure.



5. On the purchasing page, choose the configuration of the read-only instance, and then click Buy Now.

> Note:
>
> - We recommend that the read-only instance and the master instance be in the same VPC.
> - To guarantee sufficient I/O for data synchronization, we recommend that the configuration of the read-only instance (the memory) is not less than that of the master instance.
> - We recommend that you purchase multiple read-only instances to improve availability.

6. Select Product Terms of Service and Service Level Notice and Terms of Use, and then click Pay Now.

7. After creating the read-only instance, you can view it on the Instances page, as shown in the following figure.