

# Alibaba Cloud ApsaraDB for MySQL Quick Start for MariaDB TX

Issue: 20190816

# 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.	 <b>Danger:</b> 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.	 <b>Warning:</b> 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.	 <b>Notice:</b> 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.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
<b>Bold</b>	It is used for buttons, menus, page names, and other UI elements.	Click <b>OK</b> .
Courier font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid <i>Instance_ID</i></code>
[ ] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

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



# Contents

---

Legal disclaimer.....	I
Generic conventions.....	I
1 Create an RDS for MariaDB TX instance.....	1
2 Initial configuration.....	5
2.1 Configure a whitelist.....	5
2.2 Apply for an Internet address.....	12
2.3 Create accounts and databases.....	15
3 Connect to an RDS for MariaDB TX instance.....	22

# 1 Create an RDS for MariaDB TX instance

---

You can use the RDS console or APIs to create an RDS for MariaDB TX instance. For more information about instance pricing, see [#unique\\_4](#). This topic describes how to create an RDS for MariaDB TX instance in the RDS console. For information about how to create an RDS for MariaDB TX by using APIs, see [#unique\\_5](#).

## Prerequisites

You have registered an Alibaba Cloud account. For more information, see [Sign up with Alibaba Cloud](#).

## Precautions

- Subscription instances cannot be converted to Pay-As-You-Go instances.
- Pay-As-You-Go instances can be converted to Subscription instances. For more information, see [#unique\\_6](#).
- 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	<p>Indicates the location of the RDS instance you want to purchase. You cannot change the region once you confirm your order.</p> <ul style="list-style-type: none"> <li>• Select the region closest to your users to increase the access speed.</li> <li>• Select the region where your ECS instance is located so that the ECS instance can access the RDS instance through the intranet. If the ECS instance and RDS instance are located in different regions, they can communicate only through the Internet and hence performance is degraded.</li> </ul>
Zone	<p>A zone is a physical area within a region. Different zones in the same region are basically the same.</p> <p>You can deploy the master and slave nodes of your RDS instance in the same zone or in different zones.</p>
Database Engine	<p>The supported database engines are MySQL, Microsoft SQL Server, PostgreSQL, PPAS (compatible with Oracle), and MariaDB TX.</p> <p>In this example, select MariaDB TX.</p> <div style="background-color: #f0f0f0; padding: 5px;">  <b>Note:</b>  The available database engines vary depending on the region you select. </div>
Version	<p>For RDS for MariaDB TX, the supported version is MariaDB TX 10.3.</p>
Edition	<p>Select High-availability. This edition adopts the high-availability architecture with one master node and one slave node.</p> <div style="background-color: #f0f0f0; padding: 5px;">  <b>Note:</b>  The available product series vary depending on the region you select. For more information on the product series, see <a href="#">#unique_7</a>. </div>

Parameter	Description
Network Type	<p>You do not need to select a network type. MariaDB TX supports only the VPC network type.</p> <p>A Virtual Private Cloud (VPC) is an isolated network environment and therefore provides higher security and performance than a classic network. For more information, see <a href="#">Create a default VPC and VSwitch</a>.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;">  <b>Note:</b>                      Make sure the network type of the RDS instance is the same as that of your ECS instance so that the ECS instance can access the RDS instance through the intranet.                 </div>
Type	<p>Indicates the specifications of the RDS instance. Each instance type supports a specific number of CPU cores, memory size, maximum number of connections, and maximum IOPS. For more information, see <a href="#">#unique_8</a>.</p> <p>RDS for MariaDB TX supports the following instance type families:</p> <ul style="list-style-type: none"> <li>· <b>General-purpose instance:</b> owns dedicated memory and I/O resources, but shares CPU and storage resources with the other general-purpose instances on the same server.</li> <li>· <b>Dedicated instance:</b> owns dedicated CPU, memory, storage, and I/O resources.</li> <li>· <b>Dedicated host:</b> owns all the CPU, memory, storage, and I/O resources on the server where it is located.</li> </ul> <p>8 Cores 32 GB (Basic) indicates a general-purpose instance, and 8 Cores 32 GB (Dedicated) indicates a dedicated instance.</p>
Capacity	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

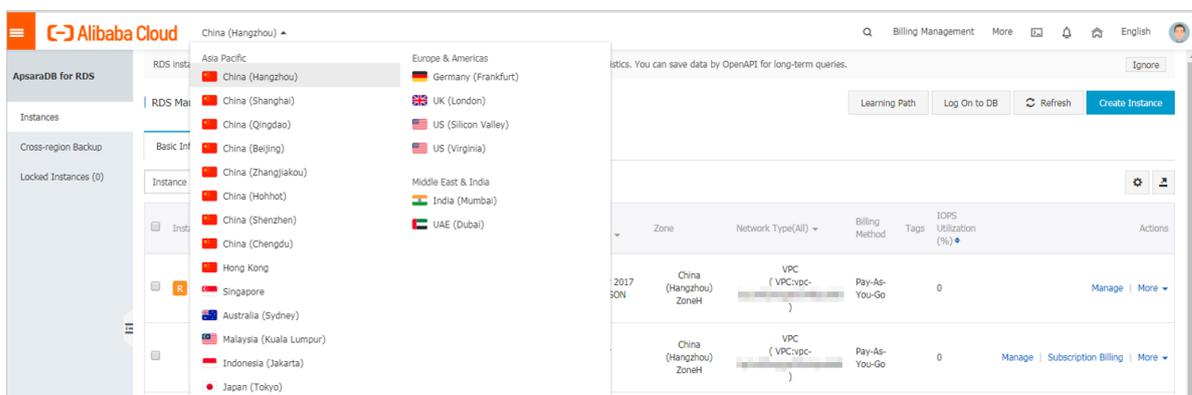
purchase a three-month Subscription instance with Auto Renew selected, the system automatically deducts fees of three months when the instance is about to expire.

- Click Add to Cart and then click the cart to place the order.

6. On Order Confirmation page, 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. [#unique\\_9](#).
3. [Create accounts](#).
4. [#unique\\_11](#) (if you want to access the RDS instance through the Internet).
5. [Connect to the RDS instance](#).

## 2 Initial configuration

### 2.1 Configure a whitelist

After you create an RDS instance, you must configure a whitelist to allow external devices to access the instance. The default whitelist contains only 127.0.0.1. Before you add new IP addresses to the whitelist, no devices are allowed to access the RDS instance.

To configure a whitelist, you can perform the following operations:

- **Configure a whitelist:** Add IP addresses to the whitelist to allow access to the RDS instance.
- **Configure an ECS security group:** Add an ECS security group for the RDS instance to allow ECS instances in the group to access the RDS instance.

A whitelist can be used to improve the security of your RDS instance. We recommend that you update the whitelist on a regular basis. Configuring a whitelist does not affect the normal operation of your RDS instance.

#### Configure an IP address whitelist

##### Precautions

- The default IP whitelist can only be edited or cleared, but cannot be deleted.
- You must confirm which network isolation mode your RDS instance is in before configuring the whitelist. Refer to the corresponding operations based on the network isolation mode.

Basic Information | Data Security

Accounts

Databases | Whitelist Settings | SQL Audit | SSL Encryption

Database Connection | Network isolation mode: enhanced whitelist. Each of the following whitelists serve a classic network or VPC. +Create Whitelist

Database Proxy | default Classic Network Edit Clear

Monitoring and Alert... | 127.0.0.1

Data Security | Note: You can specify CIDR blocks, such as X.X.X.X/X, to represent whitelisted IP address ranges. The IP address 127.0.0.1 indicates that no IP addresses are allowed to access the RDS instance. Whitelist Settings Description

Basic Information | Data Security

Accounts

Databases | Whitelist Settings

Database Connection | Network isolation mode: standard whitelist. The following whitelists contain IP addresses from both classic networks and VPCs. +Create Whitelist

Monitoring and Alert... | default Edit Clear

Data Security | 127.0.0.1

Service Availability | Note: You can specify CIDR blocks, such as X.X.X.X/X, to represent whitelisted IP address ranges. The IP address 127.0.0.1 indicates that no IP addresses are allowed to access the RDS instance. Whitelist Settings Description

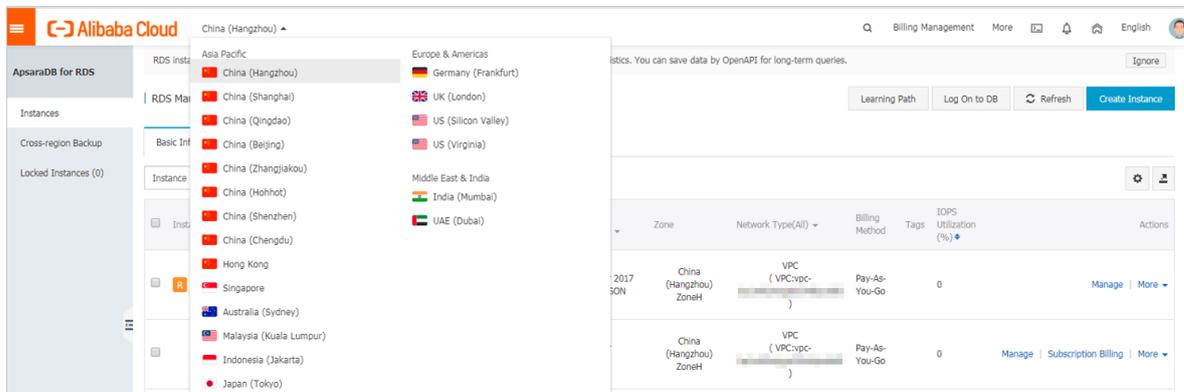


**Note:**

The intranet where an RDS for MariaDB instance is located must be a VPC.

## Configure an enhanced whitelist

1. Log on to the [RDS console](#).
2. In the upper-left corner, select the region where the target instance is located.



3. Find the target instance and click its ID.
4. In the left-side navigation pane, click Data Security.
5. On the Whitelist Settings tab page, follow these instructions based on your usage scenario:

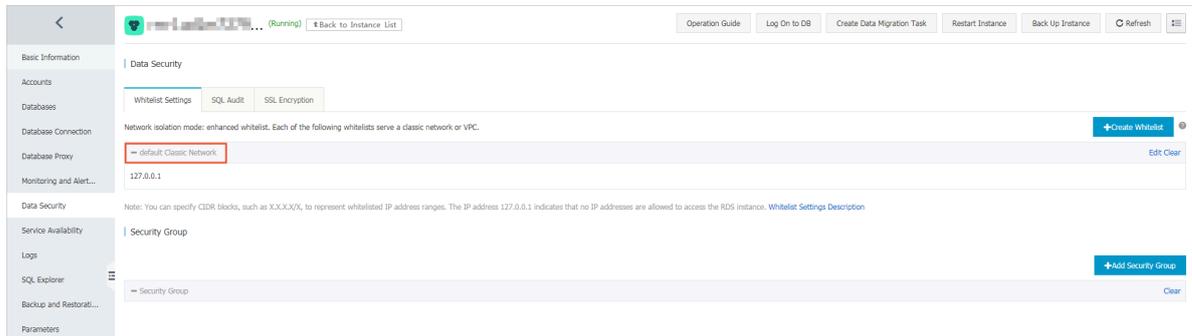
- Accessing an RDS instance from an ECS instance located within a VPC: Click Edit next to the default VPC whitelist.
- Accessing an RDS instance from an ECS instance located within a classic network: RDS for MariaDB TX instances do not support classic networks. Therefore, you can apply for an Internet IP address for your RDS for MariaDB TX instance and then use the Internet IP address to connect to your RDS for MariaDB TX instance.
- Accessing an RDS instance from an instance or host located in a public network: Click Edit next to the default Classic Network whitelist.



### Note:

- If the ECS instance accesses the RDS instance by using the VPC, you must make sure that the two instances are in the same region and have the same **network type**. Otherwise, the connection fails.

- You can also click **Create Whitelist**. In the displayed **Create Whitelist** dialog box, select a network type, VPC or Classic Network/Public IP.



6. In the displayed **Edit Whitelist** dialog box, specify IP addresses or CIDR blocks used to access the instance, and then click **OK**.

- If you specify the CIDR block 10.10.10.0/24, any IP addresses in the 10.10.10.X format are allowed to access the RDS instance.
- To add multiple IP addresses or CIDR blocks, separate each entry with a comma (without spaces), for example, 192.168.0.1,172.16.213.9.
- After you click **Add Internal IP Addresses of ECS Instances**, the IP addresses of all the ECS instances under your Alibaba Cloud account are displayed. You can quickly add internal IP addresses to the whitelist.



**Note:**

After you add an IP address or CIDR block to the default whitelist, the default address 127.0.0.1 is automatically deleted.

Edit Whitelist

Network Type:  VPC  Classic Network/Public IP

You currently cannot configure network isolation settings. You must [enable enhanced whitelists](#) first before configuring network isolation settings.

Whitelist Name\*: default

Whitelist\*: 127.0.0.1

[Add Internal IP Addresses of ECS Instances](#)

You can add 999 more entries.

Specified IP address: If you specify the IP address 192.168.0.1, this IP address is allowed to access the RDS instance.  
Specified CIDR block: If you specify the CIDR block 192.168.0.0/24, the IP addresses ranging from 192.168.0.1 to 192.168.0.255 are allowed to access the RDS instance.  
When you add multiple IP addresses or CIDR blocks, separate them by a comma (no space after the comma), for example, 192.168.0.1,192.168.0.0/24.  
[How to Locate the Local IP Address](#)

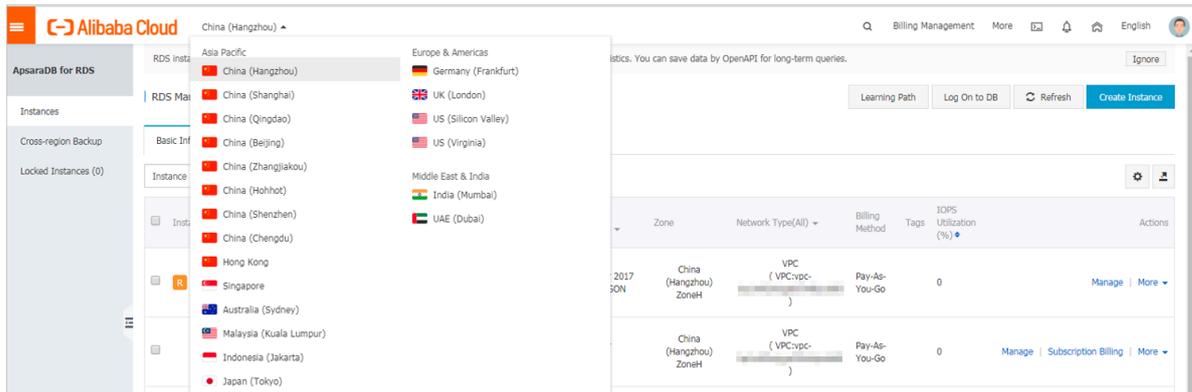
New whitelist entries take effect in 1 minute.

OK Cancel

### Configure a standard whitelist

1. Log on to the [RDS console](#).

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



3. Find the target instance and click its ID.

4. In the left-side navigation pane, click Data Security.

5. On the Whitelist Settings tab page, click Edit corresponding to the default whitelist.



**Note:**

You can also click Create Whitelist to create a whitelist.



6. In the displayed Edit Whitelist dialog box, specify the IP addresses or CIDR blocks used to access the instance, and then click OK.

- If you specify the CIDR block 10.10.10.0/24, any IP addresses in the 10.10.10.X format are allowed to access the RDS instance.
- To add multiple IP addresses or CIDR blocks, separate each entry with a comma (without spaces), for example, 192.168.0.1,172.16.213.9.
- After you click Add Internal IP Addresses of ECS Instances, the IP addresses of all the ECS instances under your Alibaba Cloud account are displayed. You can select the internal IP addresses to add to the whitelist.



**Note:**

After you add a new IP address or CIDR block to the default whitelist, the default address 127.0.0.1 is automatically deleted.

Edit Whitelist
✕

Network Type:  VPC  Classic Network/Public IP

You currently cannot configure network isolation settings. You must [enable enhanced whitelists](#) first before configuring network isolation settings.

**Whitelist Name\*:**

**Whitelist\*:**

[Add Internal IP Addresses of ECS Instances](#)

You can add 999 more entries.

Specified IP address: If you specify the IP address 192.168.0.1, this IP address is allowed to access the RDS instance.

Specified CIDR block: If you specify the CIDR block 192.168.0.0/24, the IP addresses ranging from 192.168.0.1 to 192.168.0.255 are allowed to access the RDS instance.

When you add multiple IP addresses or CIDR blocks, separate them by a comma (no space after the comma), for example, 192.168.0.1,192.168.0.0/24.

[How to Locate the Local IP Address](#)

New whitelist entries take effect in 1 minute.

### Common errors

- The default address 127.0.0.1 in Data Security > Whitelist Settings indicates that no device is allowed to access the RDS instance. Therefore, you need to add IP addresses of devices to the whitelist to allow access to the instance.
- The IP address in the whitelist is set to 0.0.0.0, but the correct format is 0.0.0.0/0.



Note:

0.0.0.0/0 indicates that all devices are allowed to access the RDS instance. Exercise caution when using this IP address.

- If you enable the [enhanced whitelist](#) mode, you must make sure that:
  - If the network type is VPC, the internal IP address of the ECS instance is added to the whitelist whose network isolation mode is default VPC.
  - If you are connecting to the RDS instance through [ClassicLink](#), the internal IP address of the ECS instance must be added to the default VPC whitelist.
  - If you are connecting to the RDS instance through a public network, the public IP address of the device must be added to the whitelist whose network isolation mode is default Classic Network .
- The Internet IP address that you add to the whitelist may not be the real egress IP address. The reasons are as follows:
  - The Internet IP address is not fixed and may dynamically change.
  - The tools or websites used to query the Internet IP addresses provide wrong IP addresses.

For more information, see [#unique\\_17](#)

### Configure an ECS security group

An ECS security group is a virtual firewall that is used to control the inbound and outbound traffic of ECS instances in a security group. After an ECS security group is added to the RDS whitelist, the ECS instances in the security group can access the RDS instance.

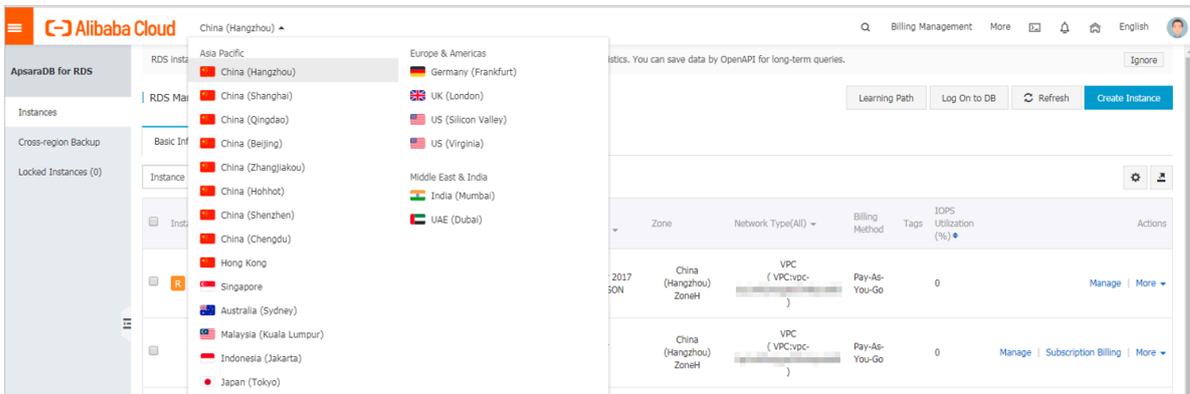
For more information, see [Create a security group](#).

### Precautions

- Regions that support ECS security groups are China (Hangzhou), China (Qingdao), and China(Hong Kong).
- You can configure both an IP address whitelist and an ECS security group. The IP addresses in the whitelist and the ECS instances in the security group can all access the RDS instance.
- You can only add one ECS security group to an RDS instance.
- Updates to the ECS security group are automatically synchronized to the IP address whitelist in real time.

### Procedure

1. Log on to the [RDS console](#).
2. In the upper-left corner, select the region where the target instance is located.



3. Find the target instance and click its ID.
4. In the left-side navigation pane, click Data Security.
5. On the Whitelist Settings tab page, click Add Security Group.
6. Select the security group to be added and click OK.

 **Note:**  
Security groups with a VPC tag are security groups that are within VPCs.

APIs

API	Description
<a href="#">#unique_18</a>	Used to view the IP address whitelist of an RDS instance.
<a href="#">#unique_19</a>	Used to modify the IP address whitelist of an RDS instance.

## 2.2 Apply for an Internet address

The RDS supports two kinds of addresses: intranet addresses and Internet addresses. Specific instructions are described in the following table.

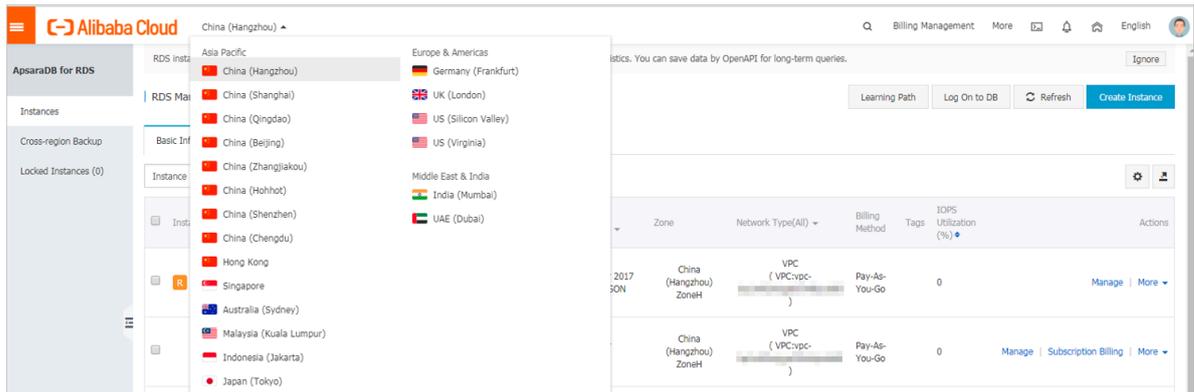
## Intranet and Internet addresses

Address Type	Description
Intranet address	<p>The intranet address is generated by default.</p> <p>Use the intranet address if all of the following conditions are met:</p> <ul style="list-style-type: none"> <li>· Your application is deployed on an ECS instance.</li> <li>· The ECS instance is located in the same region as your RDS instance.</li> <li>· The ECS instance has the same <b>network type</b> as your RDS instance.</li> </ul> <p>We recommend that you use the intranet address to access your RDS instance because this is more secure and delivers optimal performance.</p>
Internet address	<p>You need to manually apply for the Internet address. You can also release it anytime.</p> <p>Use the Internet address if you cannot access RDS through the intranet. Specific scenarios are as follows:</p> <ul style="list-style-type: none"> <li>· 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.</li> <li>· A server or computer outside Alibaba Cloud accesses your RDS instance.</li> </ul> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>· The Internet address and traffic are currently free of charge.</li> <li>· Using the Internet address reduces security. Please exercise caution</li> <li>·</li> <li>· 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.</li> </ul> </div>

## Apply for an Internet address

1. Log in to the [RDS console](#).

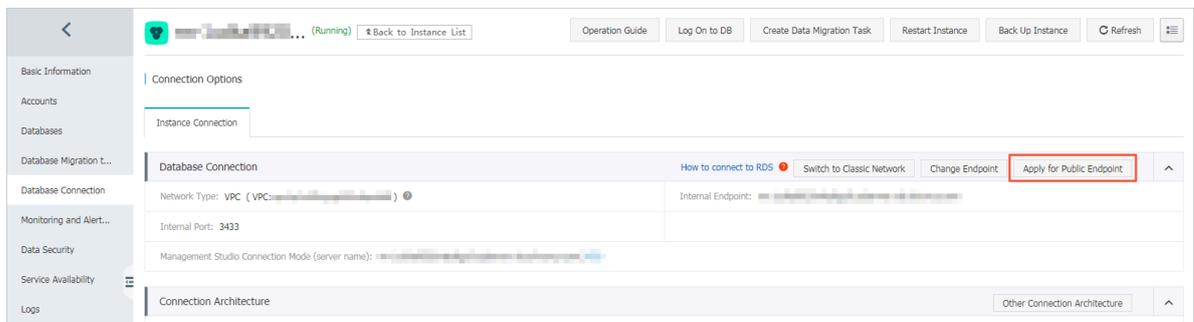
2. In the upper-left corner, select the region where the target instance is located.



3. Find the target 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 successfully.

7. Optional. If you want to change the Internet address or port number, click Change Endpoint. In the displayed dialog box, 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 an Internet address.

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

Change Endpoint
✕

Connection Type: Internal Endpoint ▾

Endpoint: rm-1udka9920x4ss6gp9 .sqlserver.rds.aliyuncs.com

Starts with a lower-case letter, consists of 8 to 64 characters, including letters, digits, or hyphen (-).

Port: 3433

Port Range: 1000 to 5999

OK
Cancel

APIs

API	Description
<a href="#">#unique_22</a>	Used to apply for an Internet address for an RDS instance.

## 2.3 Create accounts and databases

This topic describes how to create accounts and databases for RDS for MariaDB TX instances.

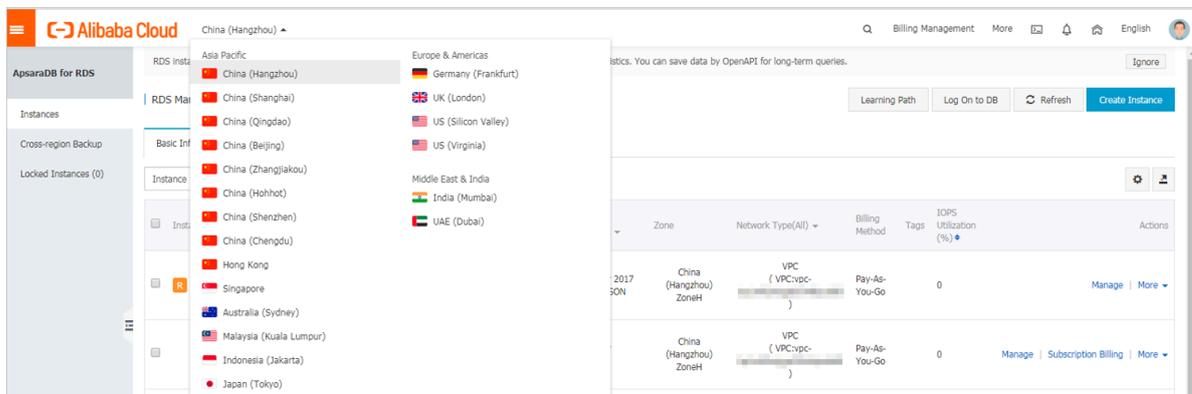
### Account types

RDS for MariaDB instances support two types of database accounts: superuser accounts and standard accounts. You can manage all your accounts and databases in the RDS console.

Account type	Description
Superuser account	<ul style="list-style-type: none"> <li>You can create and manage superuser accounts only in the RDS console or through APIs.</li> <li>You can create only one superuser account for an instance. The superuser account can manage all standard accounts and databases under this instance.</li> <li>Additional permissions are available for superuser accounts to meet the requirements for fine-grained, personalized management. For example, you can grant the permission of querying different tables to different users.</li> <li>A superuser account has permissions on all databases under the instance.</li> <li>A superuser account can disconnect any account from the instance.</li> </ul>
Standard account	<ul style="list-style-type: none"> <li>You can create and manage standard accounts in the RDS console, through APIs, or by using SQL statements.</li> <li>You can create multiple standard accounts for an instance, depending on the number of instance cores.</li> <li>You need to manually grant permissions on a specific database to a standard account.</li> <li>A standard account cannot create or manage other accounts or disconnect other accounts from the instance.</li> </ul>

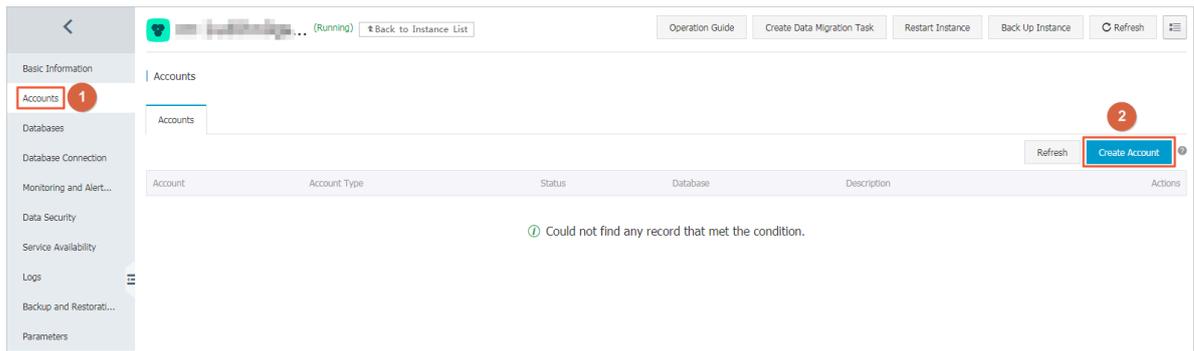
Create a superuser account

1. Log on to the [RDS Console](#).
2. In the upper-left corner, select the region where the target 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.

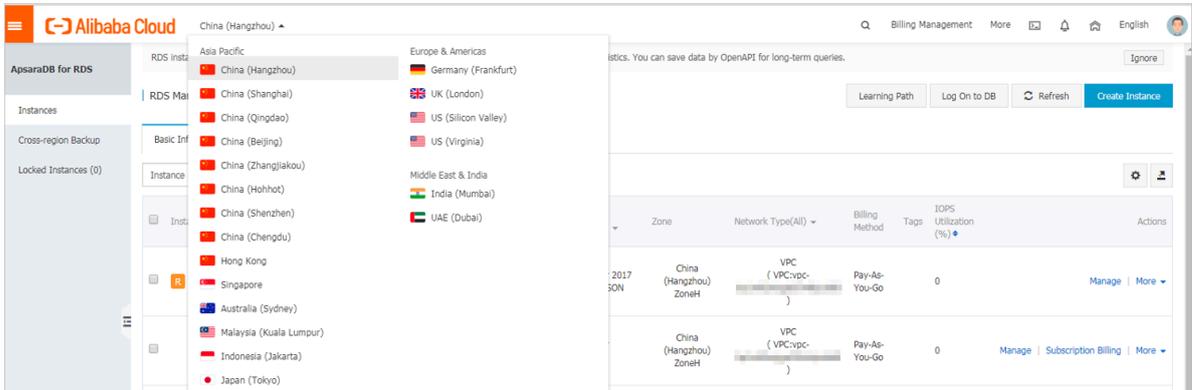
Parameter	Description
Database Account	<p>The account name contains 2 to 16 characters, including lowercase letters, numbers, and underscores (_). It must begin with a letter and ends with a letter or digit.</p> <p> <b>Note:</b> If the name of the superuser account to be created is the same as that of an existing standard account, the standard account will be replaced with the superuser account.</p>
Account Type	Select Superuser Account.
Password	<p>The password contains 8 to 32 characters, including at least three of the following types of characters: uppercase letters, lowercase letters, digits, and special characters. The allowed special characters are as follows:</p> <p>! @ # \$ % ^ &amp; * ( ) _ + - =</p>
Re-enter Password	Enter the password again.
Note	Optional. Enter the other account information that helps to better manage the account. You can enter up to 256 characters.

7. Click OK.

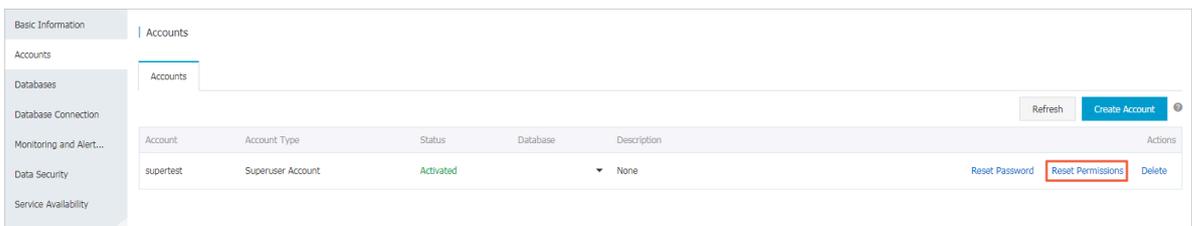
Reset the permissions of a superuser account

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

1. Log on to the [RDS Console](#).
2. In the upper-left corner, select the region where the target instance is located.



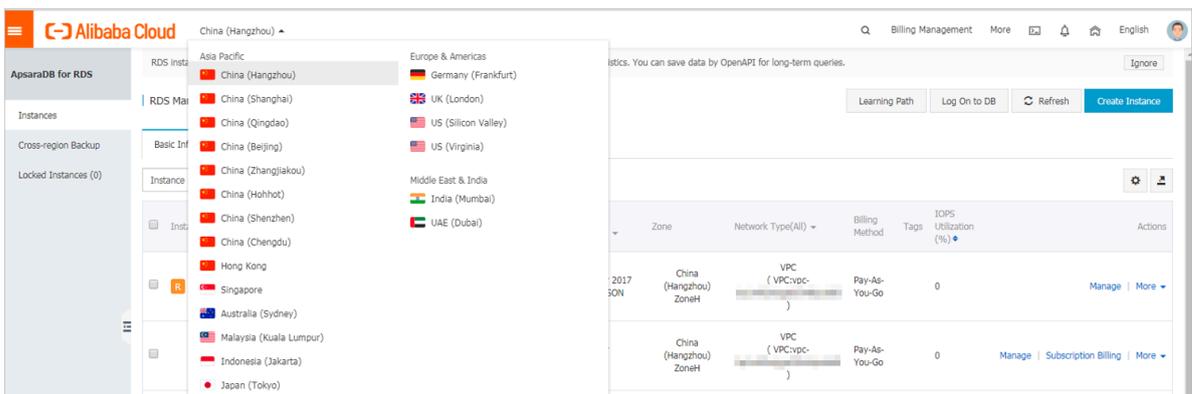
3. Find the target instance and click its ID.
4. In the left-side navigation pane, click Accounts.
5. Find the superuser account, and click Reset Permissions in the Actions column.



6. Enter the password of the superuser account and click OK.

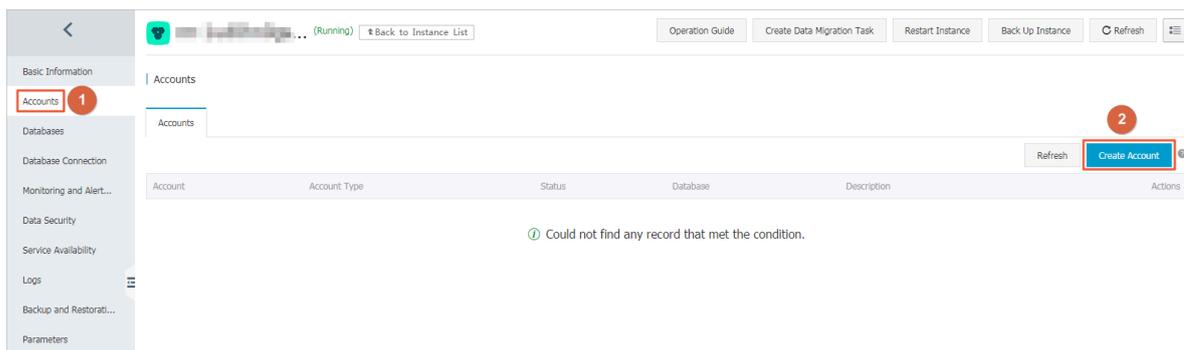
Create a standard account

1. Log on to the [RDS Console](#).
2. In the upper-left corner, select the region where the target 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.

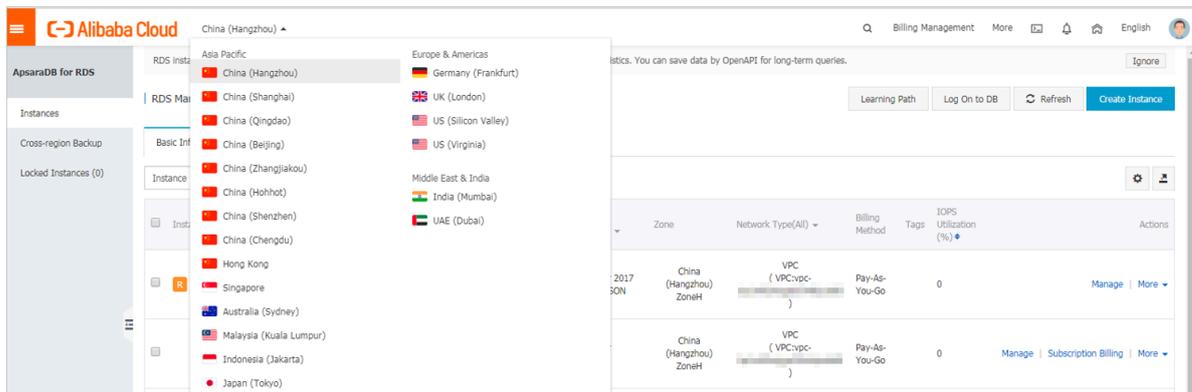
Parameter	Description
Database Account	The account name contains 2 to 16 characters, including lowercase letters, digits, and underscores (_). It must begin with a letter and end with a letter or digit.
Account Type	Select Standard Account.
Authorized Databases	<p>Grant the permissions for one or more databases to the account. This parameter is optional. You can choose to grant permissions to the account after you create it. For more information, see <a href="#">#unique_24</a>.</p> <p>a. Select one or more databases from the left area and click Add to add them to the right area.</p> <p>b. In the right area, click Read/Write, Read-only, DDL Only, or DML Only.</p> <p>If you want to grant the permissions for multiple databases in batches, select all the databases and in the upper-right corner click the button such as Full Control Read/Write.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> <b>Note:</b></p> <p>The button in the upper-right corner changes as you click. For example, after you click Full Control Read/Write, the permission changes to Full Control Read-only.</p> </div>

Parameter	Description
Password	The password contains 8 to 32 characters, including at least three of the following types of characters: uppercase letters, lowercase letters, digits, and special characters. The allowed special characters are as follows:  ! @ # \$ % ^ & * ( ) _ + - =
Re-enter Password	Enter the password again.
Note	Optional. Enter the other account information that helps to better manage the account. You can enter up to 256 characters.

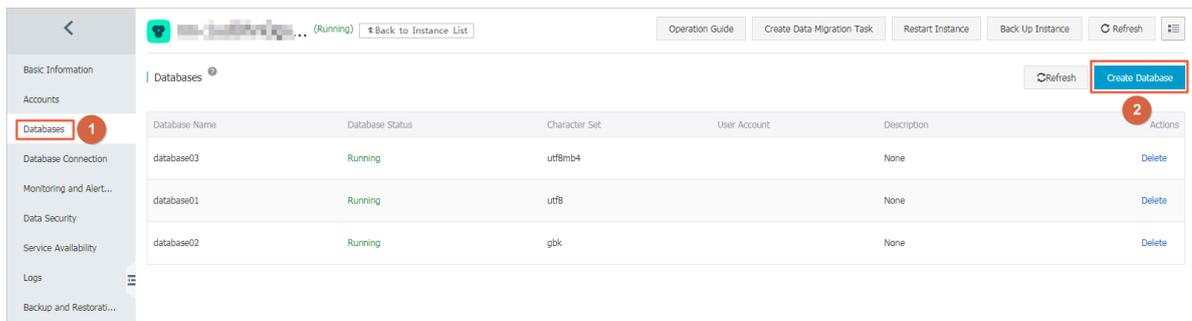
7. Click OK.

Create a database

1. Log on to the [RDS Console](#).
2. In the upper-left corner, select the region where the target 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.

Parameter	Description
Database Name	The database name contains 2 to 64 characters including lowercase letters, digits, underscores (_), and hyphens (-). It must begin with a letter and end with a letter or digit.
Supported Character Set	Select utf8, gbk, latin1, or utf8mb4.
Authorized Account	Select the account that needs to access this database. You can also leave this parameter blank and set the authorized account after the database is created. For more information, see <a href="#">#unique_25</a> .  <div style="background-color: #f0f0f0; padding: 5px;">  <b>Note:</b> Only standard accounts are displayed because the superuser account has all permissions for all databases. </div>
Account Type	Select Read/Write, Read-only, DDL only, or DML only.
Remarks	Optional. Enter the other account information that helps to better manage the account. You can enter up to 256 characters.

## 7. Click OK.

## APIs

API	Description
<a href="#">#unique_26</a>	Used to create an account.
<a href="#">#unique_27</a>	Used to create a database.

## 3 Connect to an RDS for MariaDB TX instance

---

You can connect to an RDS for MariaDB TX instance through any MySQL client. This topic uses [MySQL-Front](#) as an example.

### Prerequisites

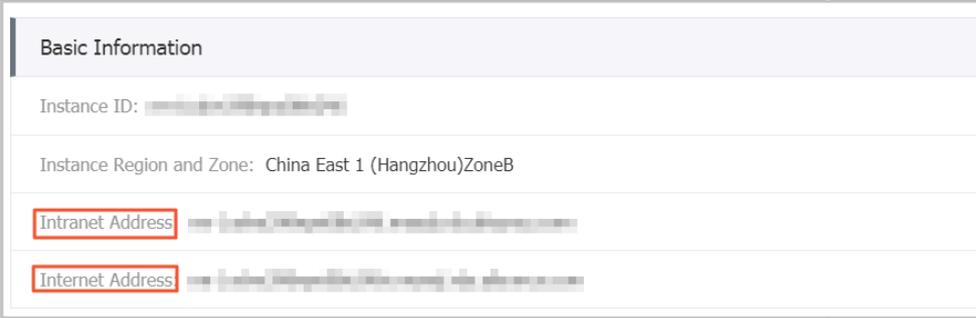
You have [created an RDS for MariaDB TX instance](#), [configured a whitelist](#), and [Created accounts](#).

### Use a database client to connect to an RDS instance

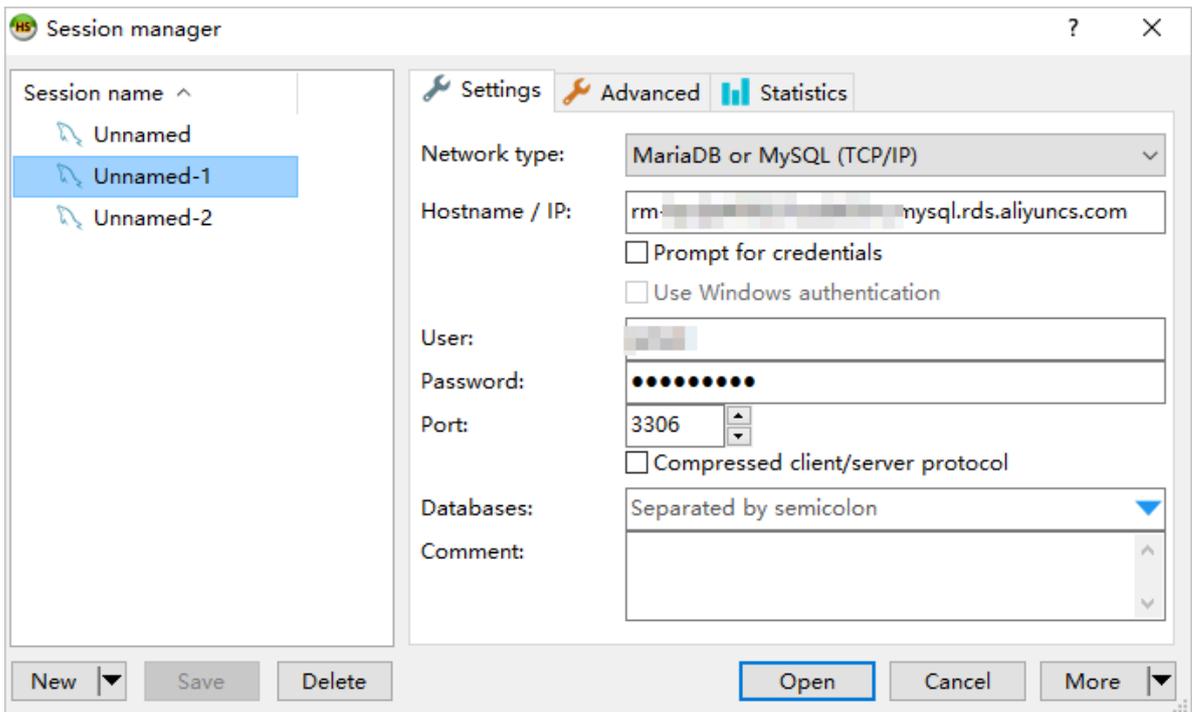
ApsaraDB RDS for MySQL is fully compatible with MySQL. You can connect to an RDS instance from any general-purpose database client in the similar way you connect to a MySQL database. This section describes how to use [HeidiSQL](#) to connect to an RDS instance.

1. Start HeidiSQL.
2. In the lower-left area of the Session manager dialog box, click New.
3. Enter the information of the RDS instance to be connected. The following table describes the parameters.

Parameter	Description
Network type	The method of connecting to the RDS instance. Select MariaDB or MySQL (TCP/IP).

Parameter	Description
<p>Hostname/IP</p>	<p>Enter the private or public IP address of the RDS instance.</p> <ul style="list-style-type: none"> <li>· If your database client is deployed in an ECS instance that is in the same region and has the same network type as the RDS instance, you can use the private IP address of the RDS instance. For example, if the ECS and RDS instances are both in a VPC located in the China (Hangzhou) region, then you can use the private IP address of the RDS instance to create a secure, efficient connection.</li> <li>· In the other situations, use the public IP address of the the RDS instance.</li> </ul> <p>You can obtain the private and public IP addresses of the RDS instance by completing the following steps:</p> <ol style="list-style-type: none"> <li>a. Log on to the <a href="#">RDS console</a>.</li> <li>b. In the upper-left corner of the page, select the region where the RDS instance is located.</li> <li>c. Find the RDS instance and click its ID.</li> <li>d. On the displayed Basic Information page, find the private and public IP addresses and their corresponding port numbers.</li> </ol>  <p>The screenshot shows the 'Basic Information' section of the RDS console. It includes fields for Instance ID, Instance Region and Zone (China East 1 (Hangzhou)ZoneB), Intranet Address, and Internet Address. The 'Intranet Address' and 'Internet Address' fields are highlighted with red boxes.</p>
<p>User</p>	<p>The username of the account that you use to access the RDS instance.</p>
<p>Password</p>	<p>The password of the account that you use to access the RDS instance.</p>

Parameter	Description
Port	The port for the RDS instance to establish a connection . If you use the private IP address of the RDS instance to establish a connection, enter the private port number. If you use the public IP address of the RDS instance to establish a connection, enter the public port number.



4. Click Open.

If the entered information is correct, the RDS instance can be connected.

