Alibaba Cloud ApsaraDB for RDS

RDS for MariaDB TX Database

Issue: 20191127

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, consequent**

ial, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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.**

Document conventions

Style	Description	Example
	A danger notice 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.
	A warning notice 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 restart an instance.
	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 **Notice:** If the weight is set to 0, the server no longer receives new requests.
	A note indicates supplemental instructions, best practices, tips, and other content.	 **Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type.
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands.	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *`Instance_ID`*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`

Style	Description	Example
{} or {a|b}	**This format is used for a required value, where only one item can be selected.**	`switch {active|stand}`

Contents

1 Preface

This topic provides an overview of RDS for MySQL, including a disclaimer, terms, and concepts.

Overview

ApsaraDB for RDS offers stable, reliable, and scalable cloud database services. Based on Apsara Distributed File System and high-performance storage (SSD), ApsaraDB for RDS supports the following database engines: MySQL, SQL Server, PostgreSQL, and PPAS (high compatibility with Oracle). ApsaraDB for RDS also provides solutions for disaster recovery, backup, database restoration, monitoring, and migration to simplify the database operations and maintenance. For more information about the benefits of ApsaraDB for RDS, see *Benefits*.

This document describes how to configure ApsaraDB for RDS through the *ApsaraDB for RDS console* to help you know more about its features and functions. You can also manage ApsaraDB for RDS through APIs and SDKs.

For further assistance, you can contact a customer service representative at +86 95187. You can also log on to the *ApsaraDB for RDS console*, click More in the top navigation bar, and choose Support > Open a new ticket. If your business is complex, you can purchase a *support plan* to obtain support from IM enterprise groups, technical account managers (TAMs), and service managers.

For more information about ApsaraDB for RDS, see *Product Details*.

Disclaimer

Some product features or services described in this document may be unavailable in certain regions. See the actual commercial contracts for specific Terms and Conditions. This document serves as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby states that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly.

Terms

- **Instance: A database service process that takes up physical memory independently. You can set different memory size, disk space, and database type, where the memory size determines the performance of the instance. After the instance is created, you can change the configuration or delete the instance at any time.**
- **Database: A database is a logical unit created in an instance. The name of each database under the same instance must be unique.**
- **Region and zone: Each region is a separate geographic area. Each region has many isolated locations known as zones. The power supply and network of each zone are independent. For more information, see *Alibaba Cloud Global Infrastructure*.**

General terms

Term	Description
On-premise database	Refers to the database deployed in the local server room or the database not on the ApsaraDB for RDS.
ApsaraDB RDS for XX (XX represents one of the following database engines: MySQL, SQL Server, PostgreSQL, and PPAS.)	Indicates the ApsaraDB for RDS of a specific database engine. For example, ApsaraDB RDS for MySQL means the database engine of the instance enabled on the RDS is MySQL.

2 Limits of RDS for MariaDB

This topic describes the limits of RDS for MariaDB. To guarantee stability and security, you must understand the limits.

The following table describes the limits of common actions and configurations in RDS for MariaDB.

Item	Limit description
Parameter modification	The *RDS console* or supported API actions can be used to modify database parameters. But For security parameters, some parameters cannot be modified. For more information, see *#unique_6*.
Database root permission	The root and sa permissions are not provided.
Database backup	· Supported CLIs or GUIs can be used for logical data backup. · For physical data backup, the *RDS console* or supported API actions must be used.
Data restoration	· Supported CLIs or GUIs can be used for logical data restoration . · For physical data restoration, the *RDS console* or supported API actions must be used.
MariaDB storage engine	· InnoDB and MyRocks are supported. · For performance and security purposes, we recommend that you use InnoDB. · Memory is not supported. If you create Memory engine tables, they are automatically converted to InnoDB engine tables.
Database replication	MySQL provides a dual-node cluster based on the master/slave replication architecture. The slave instance in the architecture is invisible to you, and your application cannot access to the slave instance directly.
Instance restart	Instances must be restarted through the *RDS console* or supported API actions.

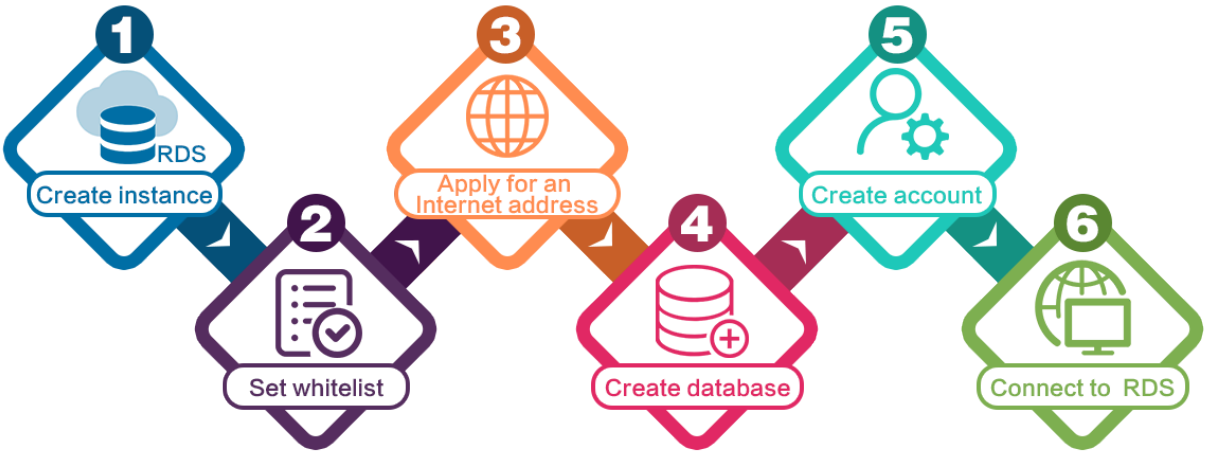
3 Quick start

3.1 General workflow to use RDS for MariaDB

This topic describes the general workflow for how to create and use an RDS for MariaDB instance.

If this is the first time that you use RDS for MariaDB, read *Limits of RDS for MariaDB* **before you purchase an RDS for MariaDB instance.**

The following flowchart shows the general workflow.



1. *Create an RDS for MariaDB instance.*
2. *Configure a whitelist for the RDS for MariaDB instance.*
3. *Apply for a public endpoint for the RDS for MariaDB instance.*
4. *Create databases and accounts for the RDS for MariaDB instance.*
5. *Connect to the RDS for MariaDB instance.*

3.2 Create an RDS for MariaDB instance

This topic describes how to create an RDS for MariaDB instance through the RDS console.

For information about how to create an RDS for MariaDB instance by calling an API action, see *#unique_14*.

For more information about instance pricing, see *#unique_15*.

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_16*.
- An Alibaba Cloud account can create up to 30 pay-as-you-go RDS instances. You can *open a ticket* to apply for an increase to 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 must 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	Select the region in which the RDS instance to be purchased will be located. The region cannot be changed after the instance is created. We recommend that you: - Select the same region as the corresponding ECS instance to avoid incurring charges for Internet traffic usage and guarantee fast access. - Check whether the selected region supports your required MySQL version and whether multi-zone support is available.

Parameter	Description
Database Engine	Select a DB engine. In this example, select MySQL. **Note:** The available DB engines vary depending on the region you select.
Version	Select a version of MySQL. You can select MySQL 5.5, 5.6, 5.7, or 8.0. **Note:** The available versions vary depending on the region you select.
Edition	Select an RDS edition. Valid values: · Basic: The DB system has only one instance. In this edition, computation is separated from storage, which is cost-effective. However, we recommend that you do not use this edition in production environments. · High-availability: The DB system has two instances: one master instance and one slave instance. The two instances work in a classic high-availability architecture. · Enterprise Edition: The DB system has three instances: one master instance and two slave instances. The three instances are located in three different zones in the same region to guarantee service availability. This edition is available to the China (Hangzhou), China (Shanghai), China (Shenzhen), and China (Beijing) regions. **Note:** The available editions vary depending on the DB engine version you select. For information about the RDS editions, see *#unique_17*.

Parameter	Description
Storage Type	Select a storage type. Valid values: · Local SSD: An SSD that is located on the same node as the DB engine. Storing data to local SSDs reduces I/O latency. · Standard SSD: An elastic block storage device that is designed based on a distributed storage architecture. Storing data to cloud SSDs makes separation between computation and storage possible. · Enhanced SSD: An SSD that is designed based on the new-generation distributed block storage architecture and the 25 GB and RDMA technologies to reduce single-link latency. Each enhanced SSD can process up to 1,000,000 random read and write requests. For more information, see *#unique_18*.
Zone	Select a 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 and slave instances in the same zone or in different zones. Multi-zone deployment is more secure because it provides zone-level disaster tolerance.
Network Type	Select a network type. Valid values: · Classic Network: indicates a traditional network. · VPC (recommended): short for Virtual Private Cloud. A VPC is an isolated network environment and therefore provides higher security and performance than a classic network. **Note:** 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.

Parameter	Description
Type	Select an RDS instance type. The RDS instance type specifies the specifications of the RDS instance. Each type supports a specific number of CPU cores, memory size, maximum number of connections, and maximum IOPS. For more information, see *#unique_19*. Valid values: · General-purpose instance: provides dedicated memory and I/O resources, but shares the CPU and storage resources with the other general-purpose instances on the same server. · Dedicated instance: provides dedicated CPU, memory, storage, and I/O resources. · Dedicated host: provides all the CPU, memory, storage, and I/O resources on the server where 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. Optional. Set the duration of the billing method for a subscription instance and specify the number of instances to be created. Then, 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 the 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, read and confirm you agree to Terms of Service, Service Level Agreement, and Terms of Use by selecting the checkbox, confirm the order details, and click Pay Now.

What to do next

Log on to the *RDS console*, select the target region, and view the instance details.

After the RDS instance is created, you must *configure whitelists* and *create accounts* for it. If you want to connect to the RDS instance through the Internet, you must also *apply for a public endpoint* for it. After all is done, you can *connect to the RDS instance*.

3.3 Configure a whitelist for an RDS for MariaDB instance

This topic describes how to configure a whitelist for an RDS for MariaDB instance.

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

RDS for PostgreSQL provides two types of whitelists::

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

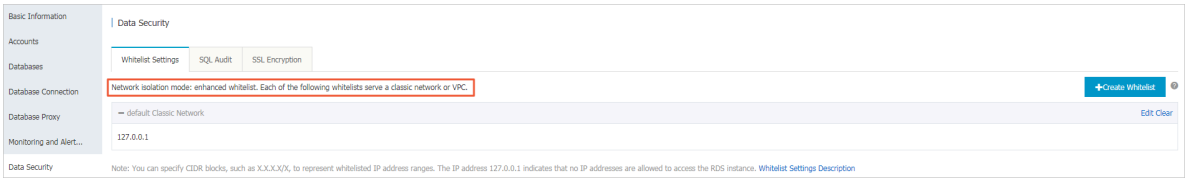
A whitelist can be used to improve the security of your RDS instance. We recommend that you update the whitelist on a regular basis. Configuring a whitelist does not affect the normal operation of your RDS instance.

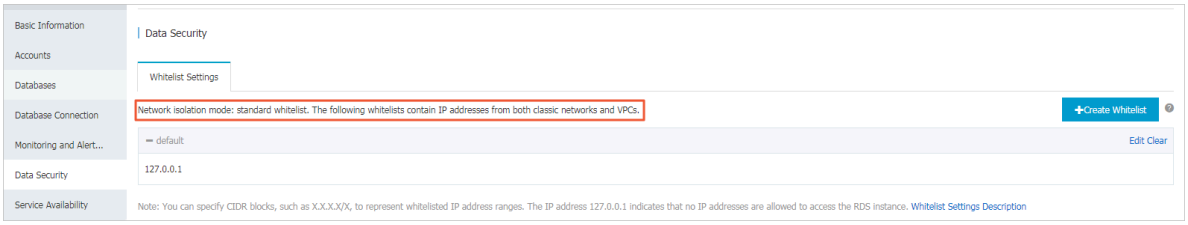
Configure an IP address whitelist

Precautions

- **The default IP whitelist can only be edited or cleared, but cannot be deleted.**

- Each IP whitelist can have up to 1,000 IP addresses or CIDR blocks. If you want to add a large number of IP addresses, we recommend that you group these IP addresses into CIDR blocks, for example, 192.168.1.0/24.
- Before configuring a whitelist, you must confirm which network isolation mode your RDS instance is in, and then perform operations accordingly.



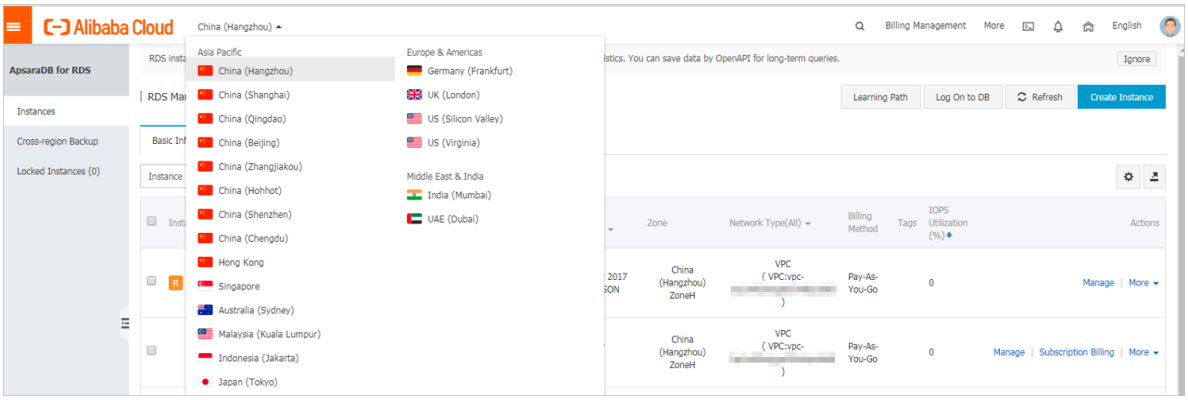


Note:

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

Configure an enhanced whitelist

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

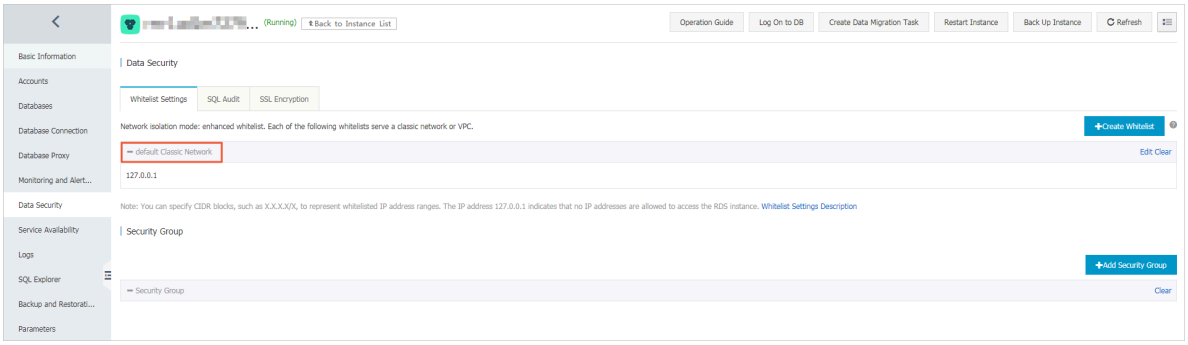


2. Find the target instance and click its ID.
3. In the left-side navigation pane, click Data Security.
4. On the Whitelist Settings tab page, follow these instructions based on your usage scenario:
   - Accessing an RDS instance from an ECS instance located within a VPC: Click Edit next to the `default 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.

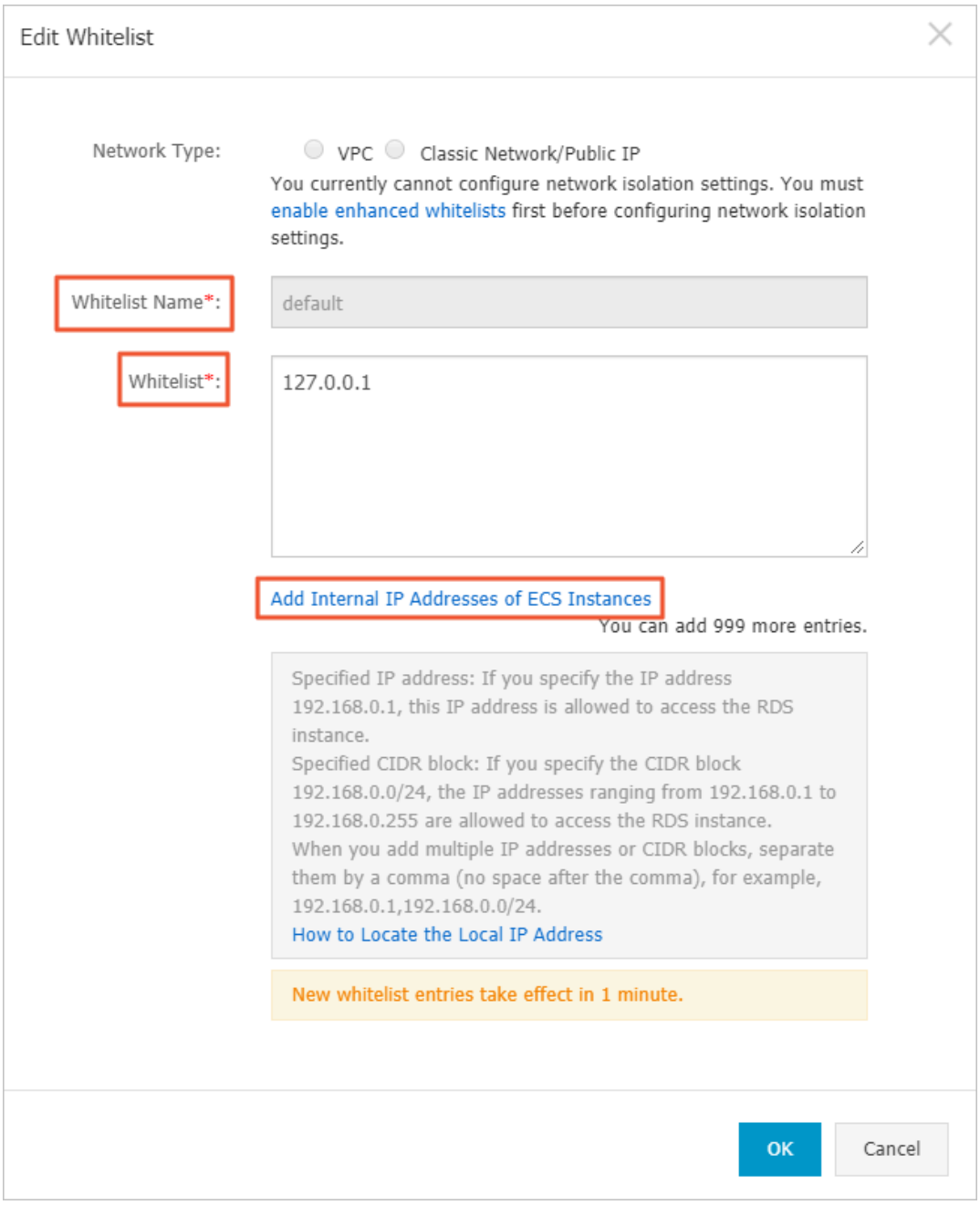


5. In the displayed Edit Whitelist dialog box, specify IP addresses or CIDR blocks used to access the instance, and then click OK.

   - 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:**

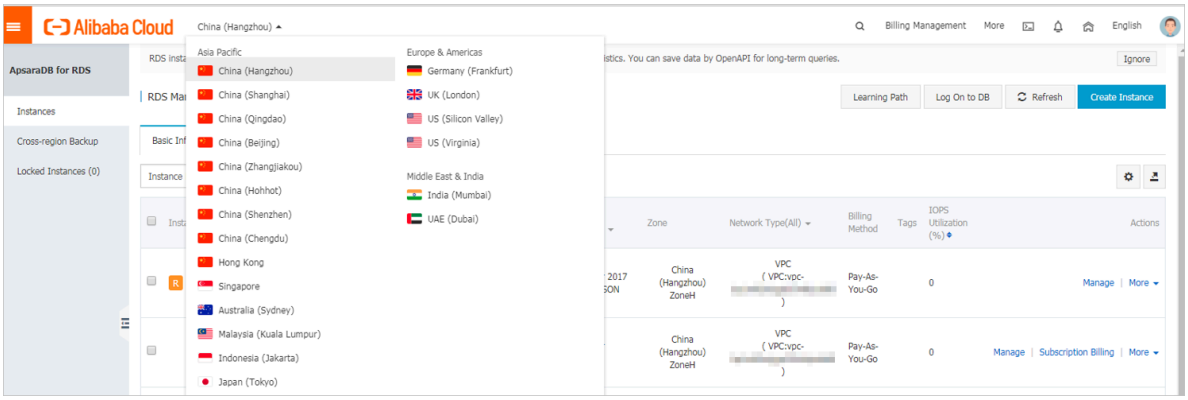
After you add an IP address or CIDR block to the default whitelist, the default address 127.0.0.1 is automatically deleted.



Configure a standard whitelist

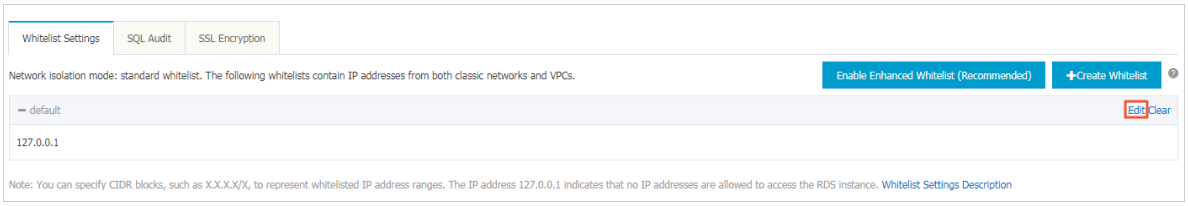
1. **Log on to the** *RDS console*.

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.

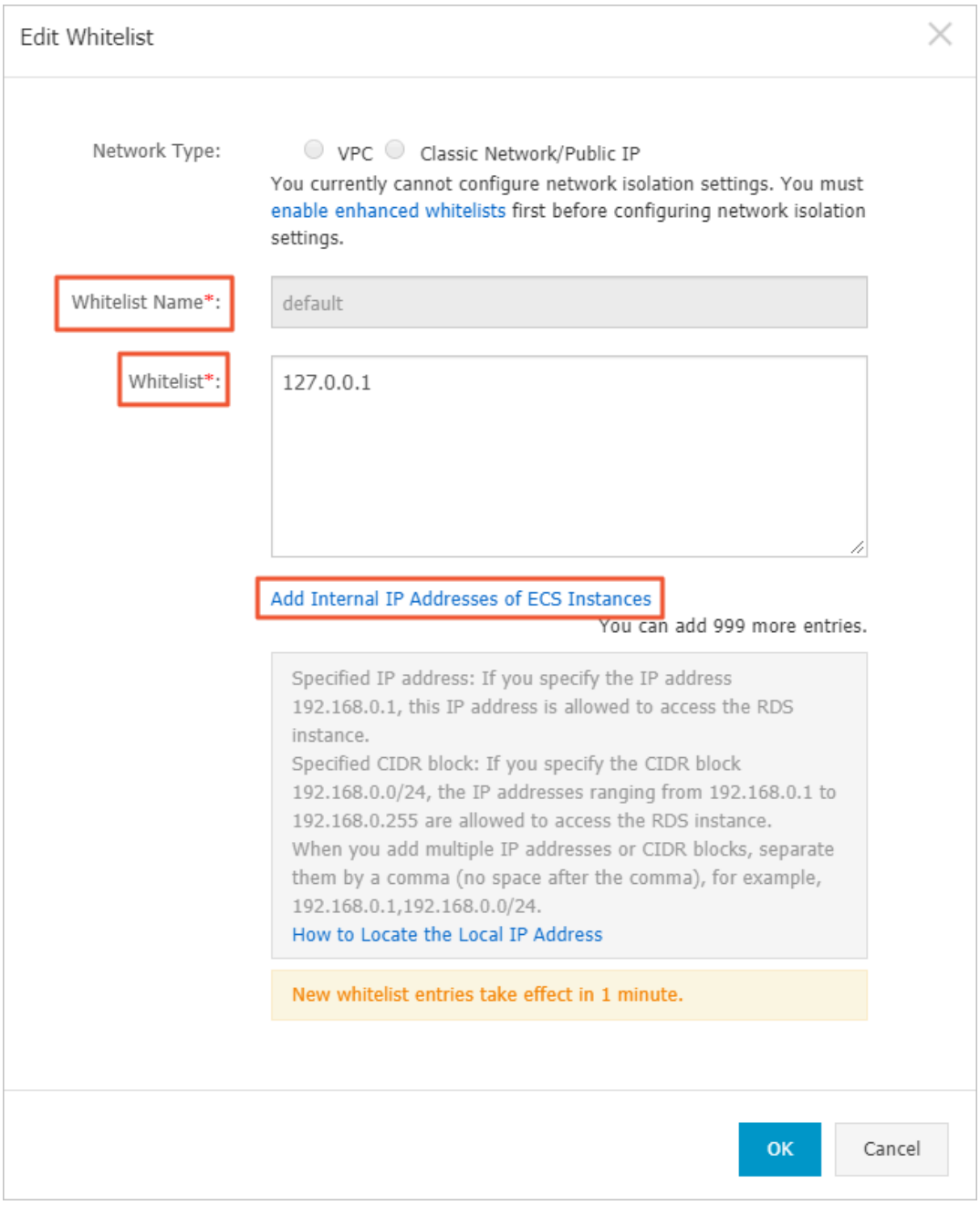
> **Note:**
> You can also click Create Whitelist to create a whitelist.



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.



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 must 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_22*

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.

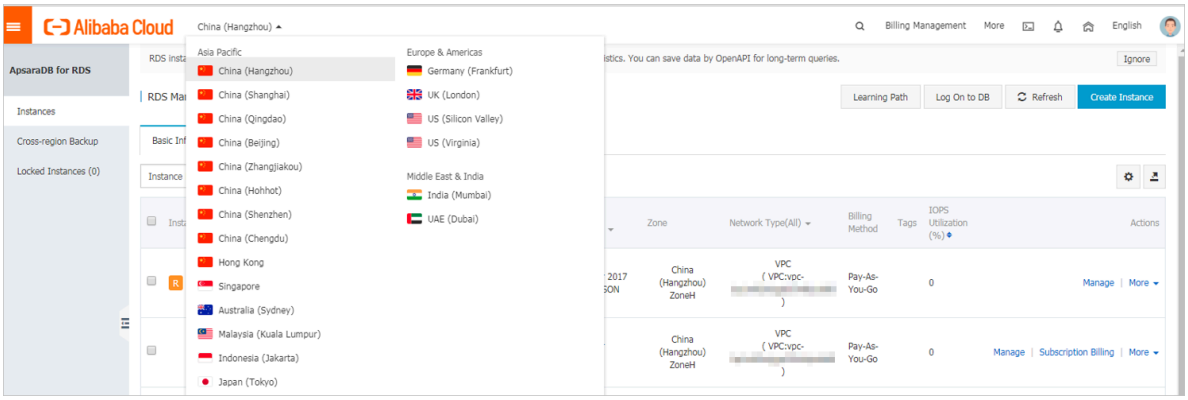
For more information, see *Create a security group*.

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
#unique_23	Used to view the IP address whitelist of an RDS instance.
#unique_24	Used to modify the IP address whitelist of an RDS instance.

3.4 Create accounts and databases for an RDS for MariaDB instance

This topic describes how to create accounts and databases for an RDS for MariaDB instance.

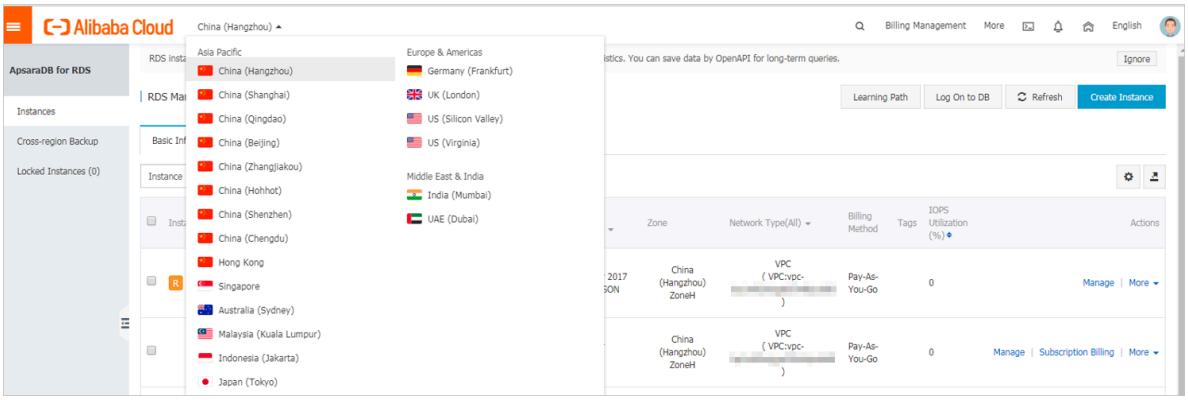
Account types

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

Account type	Description
Premier account	· Can only be created and managed through the RDS console or API. · Each RDS for MariaDB instance can have only one premier account, which can be used to manage all databases and standard accounts. · Has more permissions for fine-grained, personalized management . For example, you can grant the permission of querying different tables to different users. · Has permissions for all databases in the corresponding RDS for MariaDB instance. · Can disconnect the connections established by any other accounts.
Standard account	· Can be created and managed through the RDS console, API, or SQL statements. · Each RDS for MariaDB instance can have more than one standard account, depending on the number of instance cores. · Must be manually authorized with database permissions. · Cannot create or manage other accounts, or terminate the connections established by other accounts.

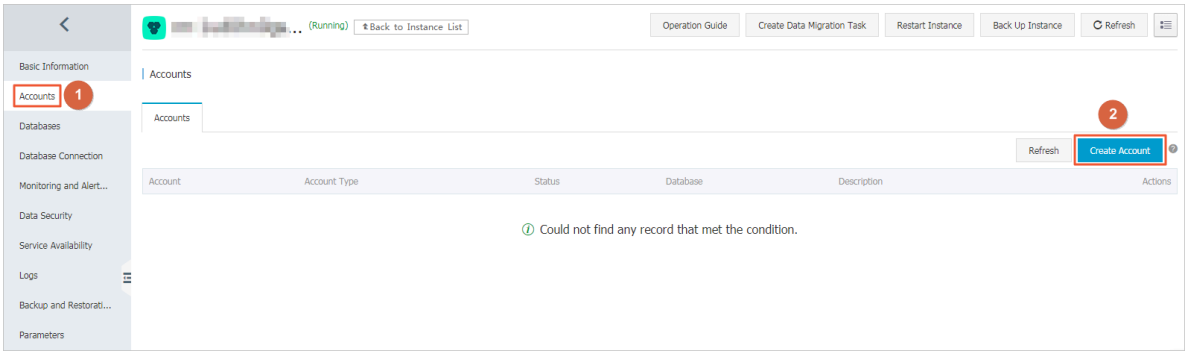
Create a premier account

1. Log on to the *RDS console*.
2. Select the target region.



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Accounts.

5. Click Create Account.



6. Set the following parameters.

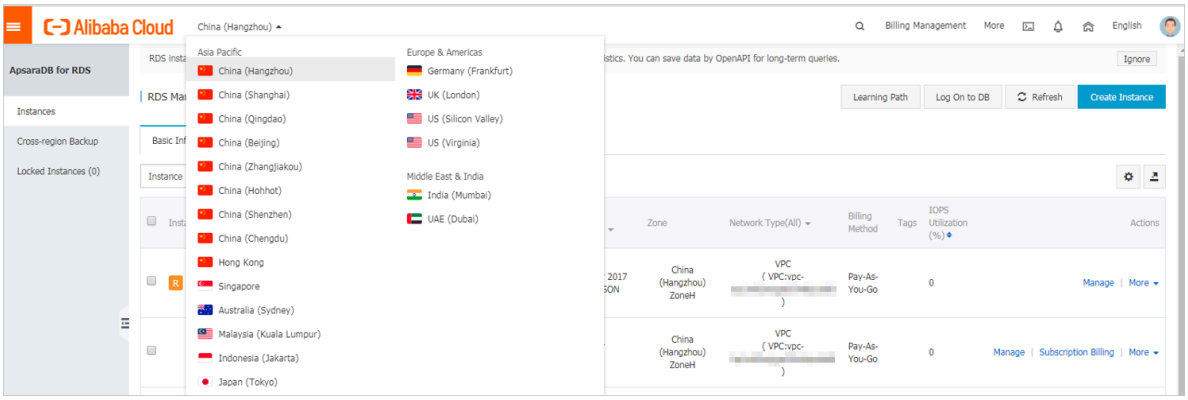
Parameter	Description
Database Account	The account name must be 2 to 16 characters in length and can contain lowercase letters, numbers, and underscores (_). It must start with a letter and end with a letter or number. **Note:** If the name of the premierr account to be created is the same as that of an existing standard account, the standard account is replaced with the premier account.
Account Type	Select Premier Account.
Password	The account password must be 8 to 32 characters in length and contain at least three of the following types of characters : uppercase letters, lowercase letters, numbers, and special characters. The allowed special characters are as follows: ! @ # $ % ^ & * ( ) _ + - =
Re-enter Password	Enter the password again.
Note	Optional. Enter details about the premier account to better identify it. You can enter up to 256 characters.

7. Click OK.

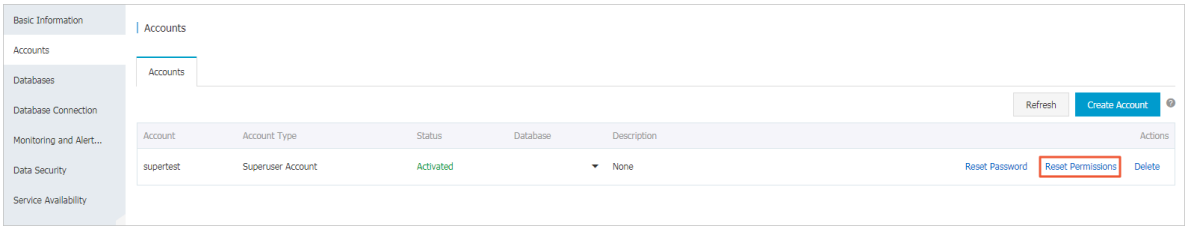
Reset the permissions of a premier account

If the premier account is abnormal (for example, the account permissions are unexpectedly revoked), you can reset the permissions. To do so, follow these steps:

1. **Log on to the *RDS console*.**
2. **Select the target region.**



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



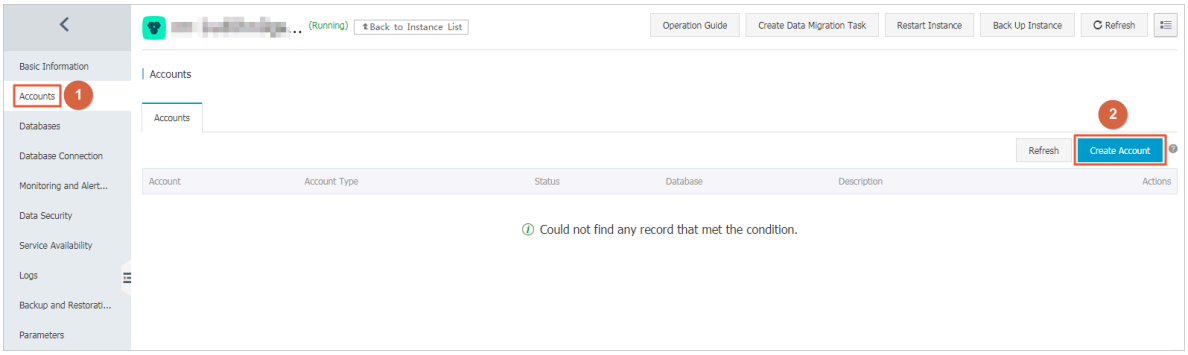
6. **Enter the password of the premier account and click OK.**

Create a standard account

1. **Log on to the *RDS console*.**
2. **Select the target region.**

3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Accounts.**

5. Click Create Account.



6. Set the following parameters.

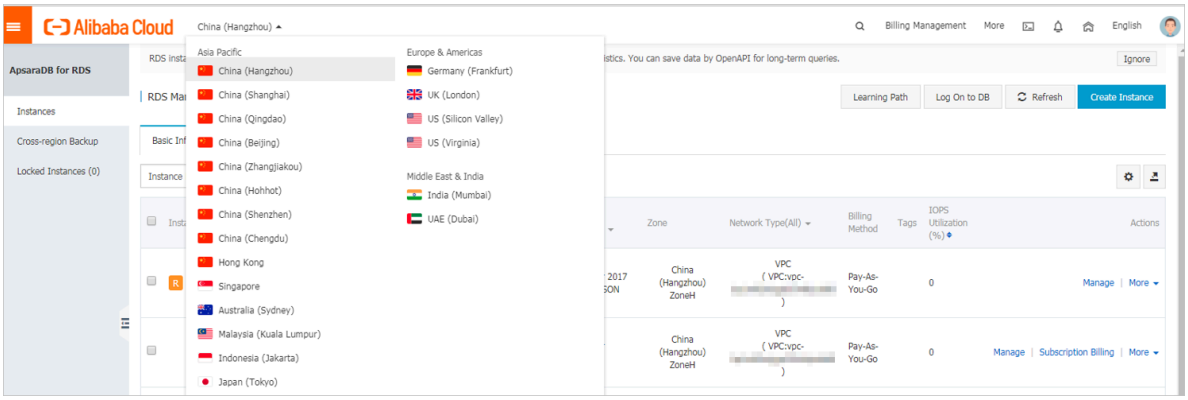
Parameter	Description
Database Account	The account name must be 2 to 16 characters in length and can contain lowercase letters, numbers, and underscores (_). It must start with a letter and end with a letter or number.
Account Type	Select Standard Account.
Authorized Databases	Grant the permissions for one or more databases to the account. This parameter is optional. You can also grant permissions to the account after the account is created. For more information, see *#unique_25*. a. Select one or more databases from the left area and click Add to add the selected databases to the right area. b. In the right area, click Read/Write, Read-only, DDL Only, or DML Only. 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. **Note:** 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.

Parameter	Description
Password	The account password must be 8 to 32 characters in length and contain at least three of the following types of characters : uppercase letters, lowercase letters, numbers, and special characters. The allowed special characters are as follows: ! @ # $ % ^ & * ( ) _ + - =
Re-enter Password	Enter the password again.
Note	Optional. Enter details about the standard account to better identify it. You can enter up to 256 characters.

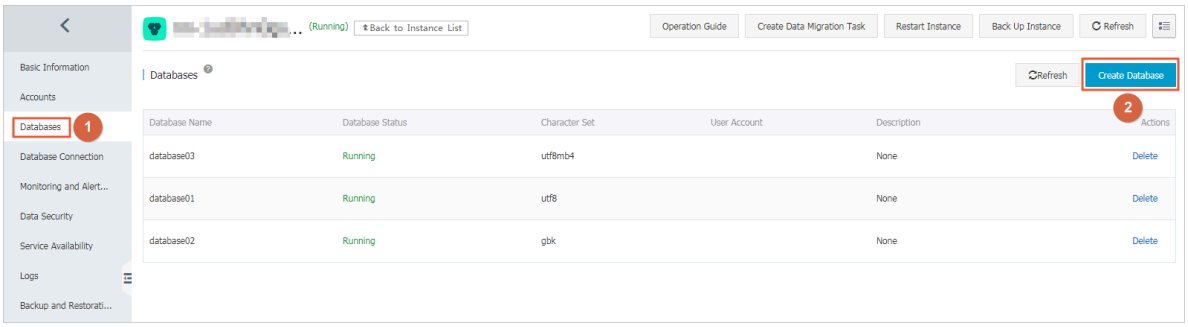
7. Click OK.

Create a database

1. Log on to the *RDS console*.
2. Select the target region.



3. Find the target RDS instance and click the instance 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 must be 2 to 64 characters in length and can contain lowercase letters, numbers, underscores (_), and hyphens (-). It must start with a letter and end with a letter or number.
Supported Character Set	Select utf8, gbk, latin1, or utf8mb4.
Authorized Account	Select the account that needs to access this database. You can also set the authorized account after the database is created. For more information, see *#unique_26*. **Note:** Only standard accounts are displayed because the premier account has all permissions for all databases.
Account Type	Select Read/Write, Read-only, DDL only, or DML only.
Remarks	Optional. Enter details about the database to better identify it. You can enter up to 256 characters.

7. Click OK.

APIs

API	Description
#unique_27	Used to create an account for an RDS instance.
#unique_28	Used to create a database for an RDS instance.

3.5 Connect to an RDS for MariaDB instance

This topic describes how to connect to an RDS for MariaDB instance. After completing the initial configuration, you can use Data Management Service (DMS), a database client, or the CLI to connect to ApsaraDB RDS for MySQL.

You can connect to an RDS for MariaDB TX instance through any MySQL client. This topic uses *MySQL-Front* as an example.

Prerequisites

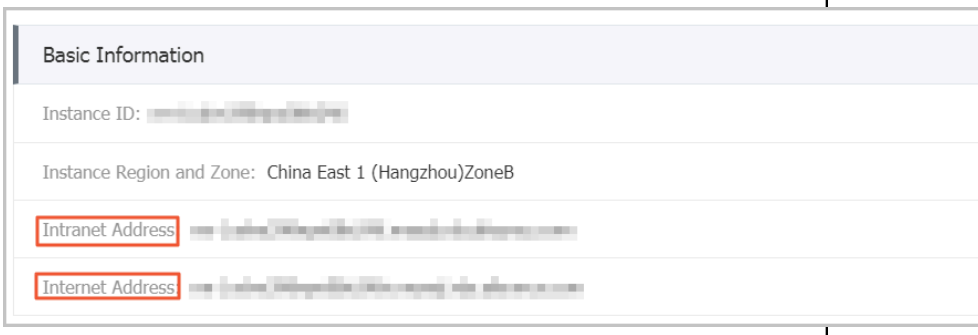
You have *created an RDS for MariaDB TX instance*, *configured a whitelist*, **and** *Created accounts*.

Use a database client to connect to an RDS instance

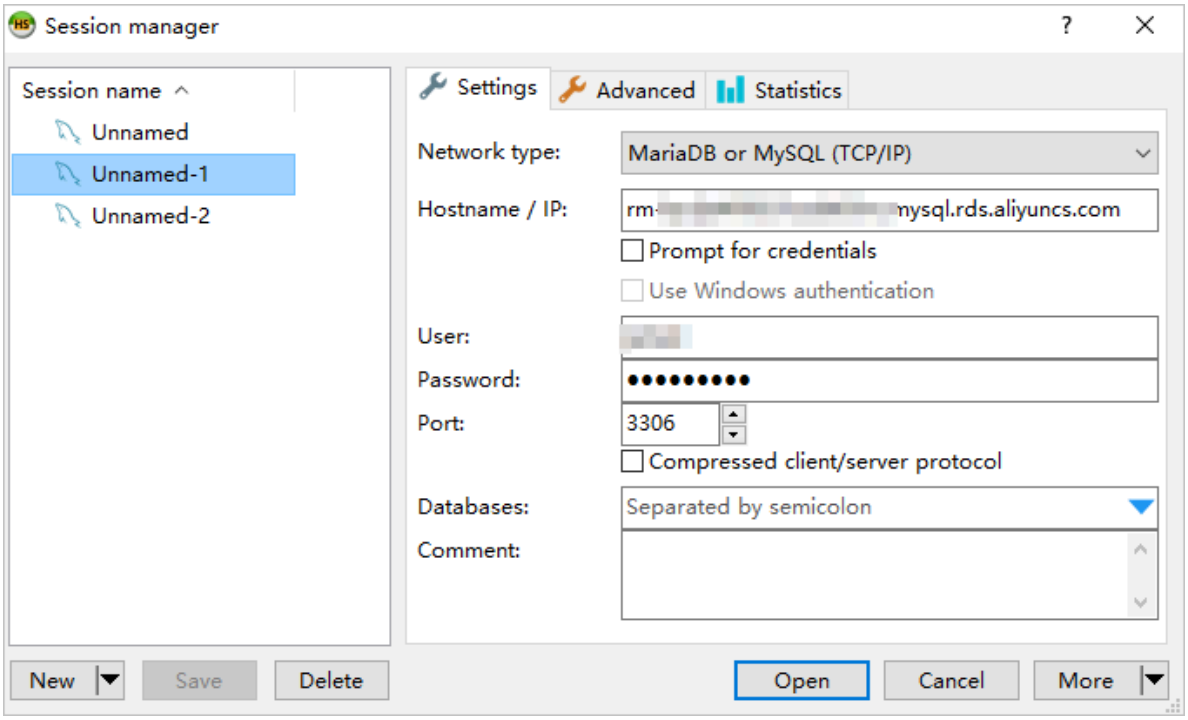
ApsaraDB RDS for MySQL is fully compatible with MySQL. You can connect to an RDS instance from any general-purpose database client in the similar way you connect to a MySQL database. This section describes how to use *HeidiSQL* **to connect to an RDS instance.**

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).

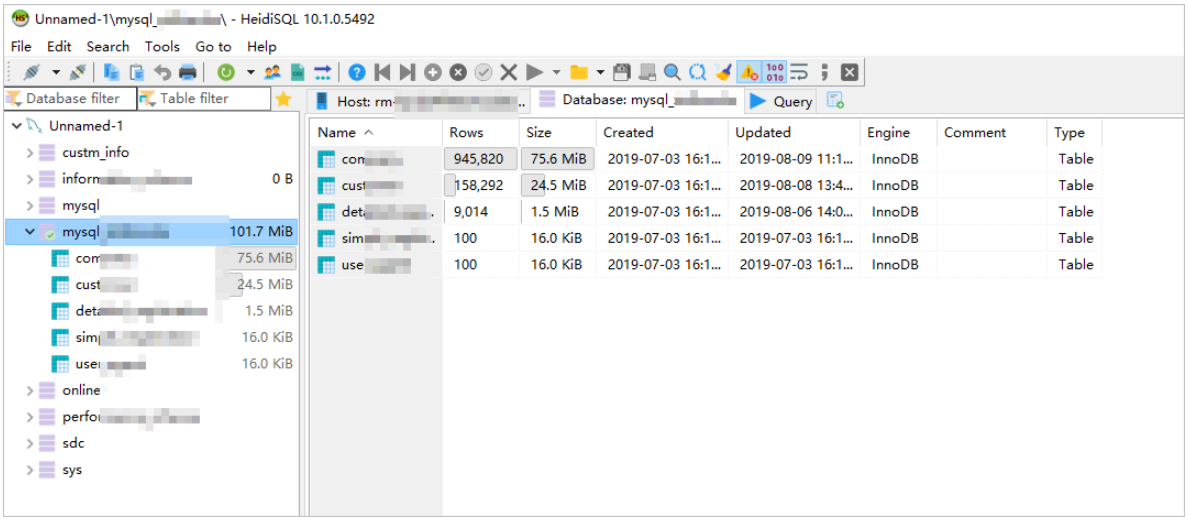
Parameter	Description
Hostname/IP	Enter the private or public IP address of the RDS instance. · If your database client is deployed in an ECS instance that is in the same region and has the same network type as the RDS instance, you can use the private IP address of the RDS instance. For example, if 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. · In the other situations, use the public IP address of the the RDS instance. You can obtain the private and public IP addresses of the RDS instance by completing the following steps: a. Log on to the *RDS console*. b. In the upper-left corner of the page, select the region where the RDS instance is located. c. Find the RDS instance and click its ID. d. On the displayed Basic Information page, find the private and public IP addresses and their corresponding port numbers. 
User	The username of the account that you use to access the RDS instance.
Password	The password of the account that you use to access the RDS instance.

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.



4 Data migration

4.1 Migrate data between RDS for MariaDB instances

DTS cannot be used to migrate data of RDS for MariaDB instances. You can use mysqldump to migrate data between RDS for MariaDB instances. This topic describes the migration procedure.

Background information

The MariaDB 10.3 version is used as an example.

Prerequisites

- **You have installed Linux 7 and MySQL 5.7 on a local host or an Alibaba Cloud ECS instance.**
- **You have configured a whitelist for both of the RDS for MariaDB instances and allowed the public IP address of the host or ECS instance running Linux 7 to access the instances. For more information about how to configure a whitelist, see** *Configure a whitelist for an RDS for MariaDB instance***.**
- **You have applied for public IP addresses for both of the RDS for MariaDB instances. For more information, see** *Apply for a public endpoint for an RDS for MariaDB instance***.**

Procedure

1. **Use a client tool to** *log on to the destination RDS for MariaDB instance* **and create a database.**
2. **Log on to the host or ECS instance running Linux 7, and use the mysqldump tool to export the data of the source RDS for MariaDB instance as a data file.**

```
mysqldump -h <Public IP address of the source instance> -P <Port of
 the source instance> -u <Privileged account of the source instance
> -p<Privileged account password of the source instance> --opt --
default-character-set=utf8 --hex-blob <Name of the database to
```

```
be migrated> --skip-triggers > /tmp/<Name of the database to be
migrated>.sql
```

Example:

```
mysqldump -h rm-xxx.mariadb.rds.aliyuncs.com -P 3306 -u test -
pTestxxx --opt --default-character-set=utf8 --hex-blob testdb --skip
-triggers > /tmp/testdb.sql
```

Note:

Do not update data during the export process. This step only exports data. It does not export stored procedures, triggers, or functions.

3. **Use mysqldump to export stored procedures, triggers, and functions.**

```
mysqldump -h <Public IP address of the source instance> -P <Port of
 the source instance> -u <Privileged account of the source instance
> -p<Privileged account password of the source instance> --opt --
default-character-set=utf8 --hex-blob <Name of the database to be
migrated> -R > /tmp/<Name of the database to be migrated>trigger.sql
```

Example:

```
mysqldump -h rm-xxx.mariadb.rds.aliyuncs.com -P 3306 -u test -
pTestxxx --opt --default-character-set=utf8 --hex-blob testdb -R > /
tmp/testdbtrigger.sql
```

Note:

Skip this step if no stored procedures, triggers, or functions are used in the database.

4. **Run the following statements to import data files, stored procedures, triggers, and functions to the destination RDS for MariaDB instance:**

```
mysql -h <Public IP address of the destination instance> -P <Port of
 the destination instance> -u <Privileged account of the destinatio
n instance> -p<Privileged account password of the destination
instance> <Database name of the destination instance> < /tmp/<Name
of the database to be migrated>.sql
mysql -h <Public IP address of the destination instance> -P <Port of
 the destination instance> -u <Privileged account of the destinatio
n instance> -p<Privileged account password of the destination
instance> <Database name of the destination instance> < /tmp/<Name
of the database to be migrated>trigger.sql
```

Examples:

```
mysql -h rm-xxx.mariadb.rds.aliyuncs.com -P 3306 -u test2 -pTest2xxx
 test001 < /tmp/testdb.sql
```

```
mysql -h rm-xxx.mariadb.rds.aliyuncs.com -P 3306 -u test2 -pTest2xxx
 test001 < /tmp/testdbtriggertrigger.sql
```

4.2 Use mysqldump to migrate data to an RDS for MariaDB TX instance

This topic describes how to use the mysqldump client to migrate data to an RDS for MariaDB TX instance.

Background information

RDS is fully compatible with native database services. The process of migrating data from native databases to RDS instances is similar to that of migrating data from a MariaDB server to another.

This topic takes an on-premises server running Linux 7 and MariaDB 10.2.4 as an example to describe how to migrate data from an on-premises database to an RDS for MariaDB TX instance.

Precautions

The name of the table after migration is case-insensitive and displayed in lowercase letters.

Prerequisites

The RDS instance has a whitelist and a public endpoint. For more information, see *Configure a whitelist for an RDS for MariaDB instance* **and** *Apply for a public endpoint for an RDS for MariaDB instance*.

Procedure

1. **Use a remote access tool to** *log on to the RDS for MariaDB TX instance* **and create a database.**
2. **Log on to the on-premises Linux server and use the mysqldump tool to export the on-premises database data as a data file.**

```
mysqldump -h localhost -u root -p<root account password> --opt --
default-character-set=utf8 --hex-blob <Name of the database to
be migrated> --skip-triggers > /tmp/<Name of the database to be
migrated>.sql
```

Note:

Do not update data during the export process. This step only exports data. It does not export stored procedures, triggers, or functions.

3. **Use mysqldump to export stored procedures, triggers, and functions.**

```
mysqldump -h localhost -u root -p<root account password> --opt --
default-character-set=utf8 --hex-blob <Name of the database to be
migrated> -R | sed -e 's/DEFINER[ ]*=[ ]*[^*]*\*/\*/' > /tmp/<Name
of the database to be migrated>trigger.sql
```

Note:

Skip this step if no stored procedures, triggers, or functions are used in the database. When exporting stored procedures, triggers, and functions, you must remove the DEFINER clause to guarantee compatibility with RDS.

4. **Run the following statements to import data files and stored procedure files to the destination RDS instance:**

```
mysql -h <Public IP address of the RDS instance> -u <Privileged
account of the RDS instance> -p<Privileged account password of the
RDS instance> < /tmp/<Name of the database to be migrated>.sql
mysql -h <Public IP address of the RDS instance> -u <Privileged
account of the RDS instance> -p<Privileged account password of the
 RDS instance> < /tmp/<Name of the database to be migrated>trigger.
sql
```

5. **Refresh the data query page of the remote access tool and view the table. If data exists in the table, the migration is successful.**

5 Billing

5.1 Switch from pay-as-you-go billing to subscription billing

This topic describes how to change the billing method of an RDS for MariaDB instance from pay-as-you-go to (monthly or annual) subscription.

Impacts

Changing the billing method does not interrupt the running of your RDS instance.

Precautions

- **You cannot change the billing method of an RDS instance from subscription to pay-as-you-go. To optimize your cost plan, you must evaluate your usage model thoroughly before you change the billing method of your RDS instance.**
- **If an RDS instance has an unpaid subscription order, the subscription order becomes invalid after you upgrade the instance type. In such case, you must first go to the *Orders* page in the RDS console to cancel the subscription order, and then change the billing method to subscription again.**

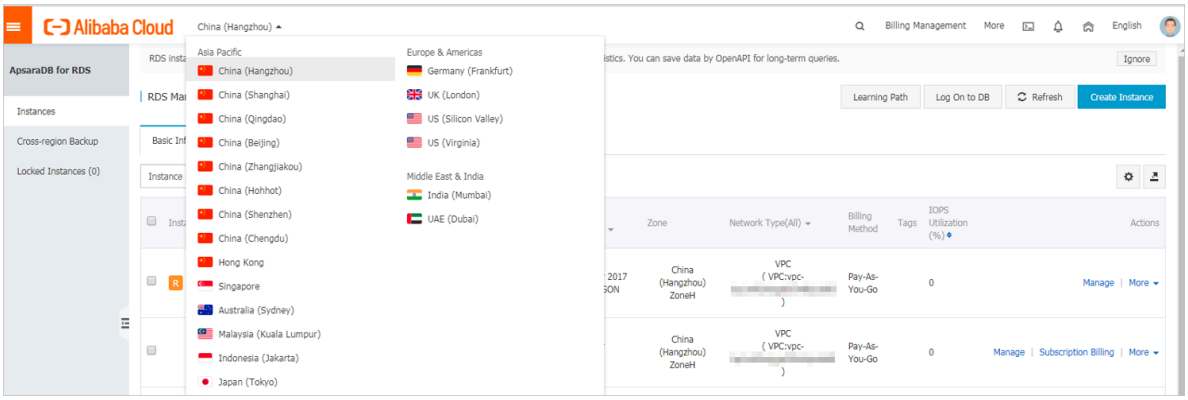
Prerequisites

- **The instance type cannot be a historical one, which means that the instance type must be available for sale. For more information about historical instance types, see *#unique_19*. Before you change the billing method of a historical-type RDS instance to subscription, you must change the instance type to one that is available for sale. For detailed steps, see *Change the configuration of an RDS for MariaDB instance*.**
- **The RDS instance uses the pay-as-you-go billing method.**
- **The RDS instance is in the Running state.**
- **The RDS instance does not have an unpaid subscription order.**

Procedure

1. **Log on to the *RDS console*.**

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



3. Find the target RDS instance and use one of the following two methods to open the Switch to Subscription Billing page.

   - In the Actions column, click Subscription Billing.
   - Click the instance ID. Then in the Status section of the Basic Information page, click Subscription Billing.

4. Select a duration of purchase.
5. Select Terms of Service, Service Level Agreement, and Terms of Use. Then click Pay Now.

> **Note:**
> The system generates a subscription order. If this order is not paid or canceled, you cannot change the billing method of this RDS instance from pay-as-you-go to subscription or purchase a new RDS instance. You can go to the *Orders* page to pay for or cancel this order.

6. Complete the payment.

5.2 Manually renew an RDS for MariaDB instance

This topic describes how to manually renew an RDS for MariaDB instance that is charged by using subscription billing. If a subscription RDS instance expires and is not renewed in time, services will be stopped and data may be permanently deleted.

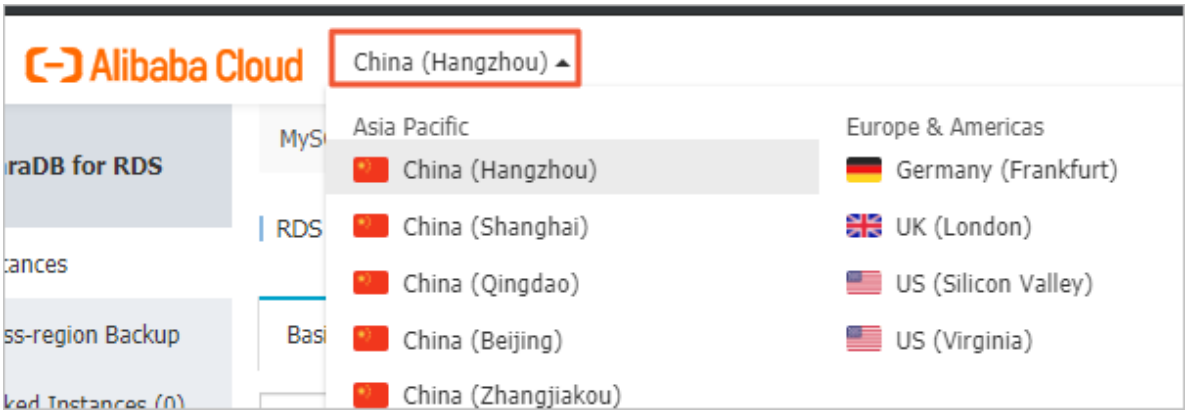
For more information about the impacts, see *Expiration and overdue policy*.

Note:
A pay-as-you-go-based instance does not have an expiration date and no renewal is required.

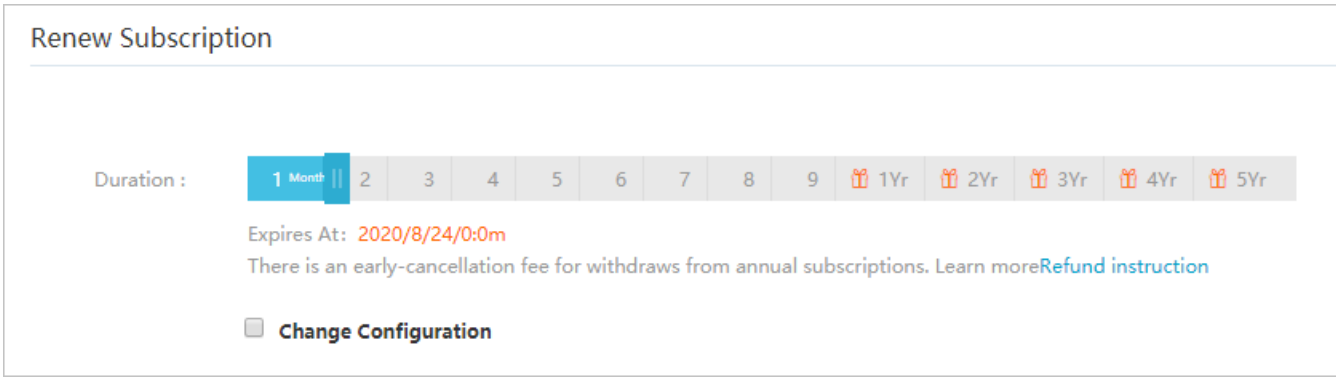
You can manually renew a subscription-based instance before it expires or within 15 days after it expires.

Method 1: Renew an RDS instance in the RDS console

1. **Log on to the *RDS console*.**
2. **Select the target region.**



3. **Find the target RDS instance and in the Actions column click Renew.**
4. **On the Renew Subscription page, select a duration. The longer the duration, the bigger discount you have.**

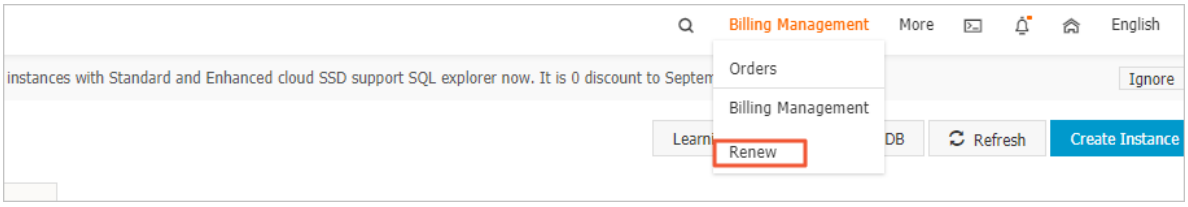


5. **Read and confirm you agree to Terms of Service, Service Level Agreement, and Terms of Useby selecting the checkbox, confirm the order details, and click Pay Now**

Renew an RDS instance in the Renew console

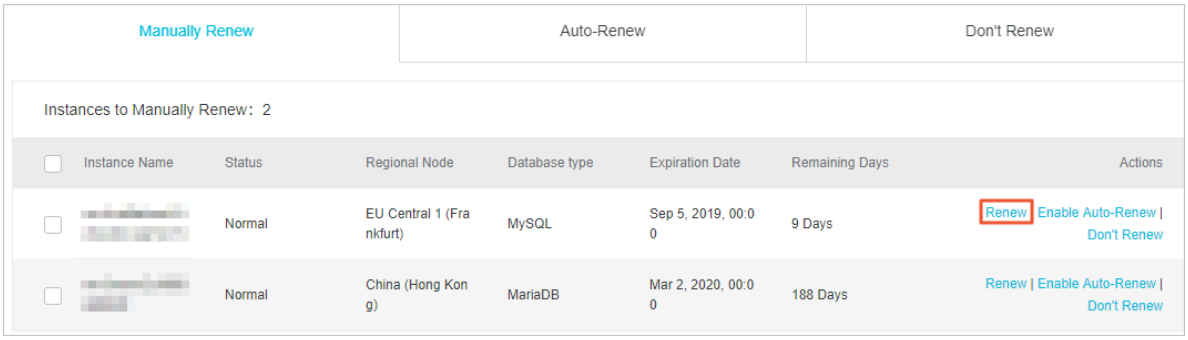
1. **Log on to the *RDS console*.**

2. In the upper-right corner of the page, choose Billing Management > Renew.



3. In the left-side navigation pane, click ApsaraDB for RDS.
4. On the Manually Renew tab, find the target RDS instance and in the Actions column click Renew

> **Note:**
>
> - If the target RDS instance is on the Don't Renew tab, you can click Enable Manual Renew in the Actions column to restore the instance to manual renewal.
> - If the target RDS instance is on the Auto-Renew tab, you can click Modify Auto-Renew in the Actions column, and then in the displayed dialog box select Disable Auto-Renew and click OK to restore the instance to manual renewal.



5. Select a duration, read and confirm you agree to Terms of Service, Service Level Agreement, and Terms of Use by selecting the checkbox, confirm the order details, and click Pay Now.

Auto-renewal

Enabling auto-renewal guarantees that your business runs smoothly without the need of manual renewal when your instance expires. For more information, see *Automatically renew an RDS for MariaDB instance*.

5.3 Automatically renew an RDS for MariaDB instance

This topic describes how to automatically renew an RDS for MariaDB instance.

Each subscription-based instance has an expiration date. If an instance is not renewed in time when the instance expires, a service interruption or even data loss may occur. For more information about the impacts, see *Expiration and overdue policy*. Enabling auto-renewal guarantees that your business runs smoothly without the need of manual renewal when your instance expires.

> **Note:**
> **A pay-as-you-go-based instance does not have an expiration date and no renewal is required.**

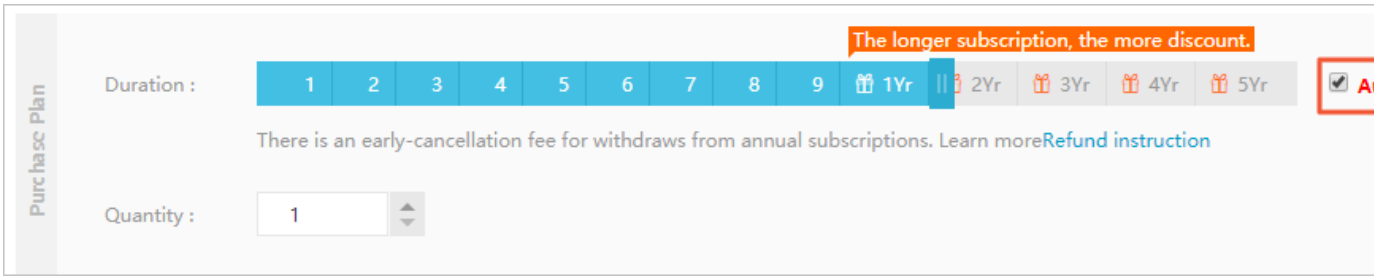
Precautions

- **If you have enabled automatic renewal for your subscription-based instance, a payment will be deducted three days before the expiration date. You can pay the fees by credit cards or coupons. Make sure that your credit card has sufficient balance.**
- **If you manually renew an instance before the automatic deduction date, the system will automatically renew the instance before the next expiration date.**
- **The automatic renewal function takes effect the next day after you enable it. If your instance expires the next day, renew it manually to prevent service interruption. For more information, see *Manually renew an RDS for MariaDB instance*.**

Enable automatic renewal when you purchase an RDS instance

> **Note:**
> **After you enable automatic renewal, the system automatically renews your instance based on the specified Duration when the instance expires. For example, if you have purchased a three-month subscription-based instance and selected Auto-renewal, the fees are automatically paid every three months for each renewal.**

When you *purchase a subscription-based instance*, you can select Auto Renewal on the purchase page.

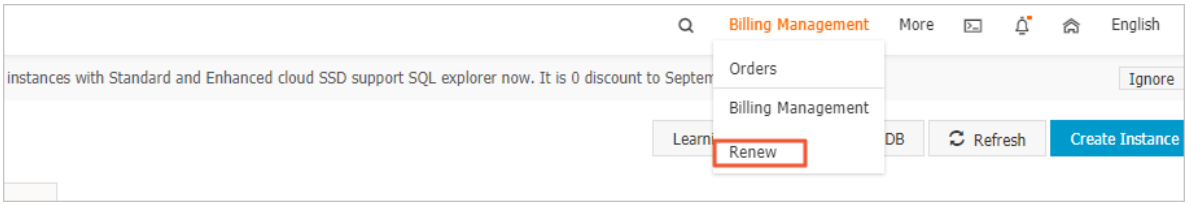


Enable automatic renewal after you purchase an RDS instance

Note:

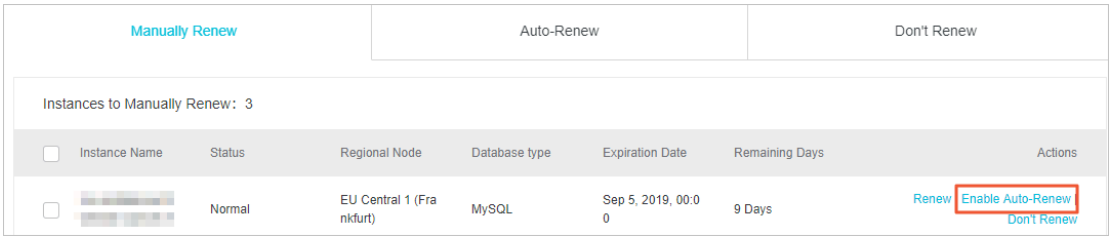
After you enable automatic renewal, the system automatically renews your instance based on the selected renewal duration. For example, if you select a three-month renewal duration, the fees are automatically paid every three months for each renewal.

1. **Log on to the *RDS console*.**
2. **In the upper-right corner, choose Billing Management > Renew.**



3. **In the left-side navigation pane, click ApsaraDB for RDS.**

4. On the Manually Renew or Auto-Renew tab, find the target RDS instance. You can enable automatic renewal for one or more RDS instances at a time.
   - Follow these steps to enable automatic renewal for one RDS instance:
     a. Find the target RDS instance and in the Actions column click Enable Auto-Renew.

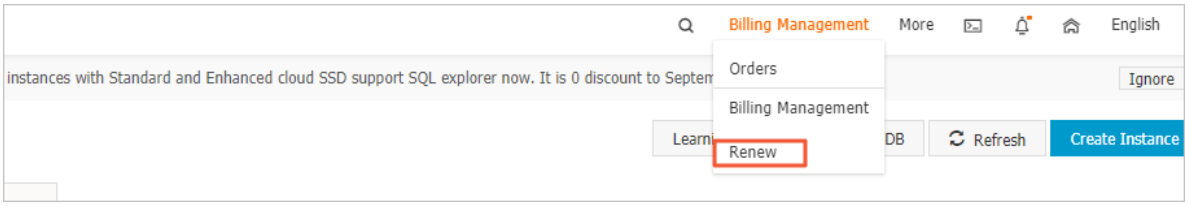


     b. In the displayed dialog box, set Auto-Renew Cycle and click Enable Auto-Renew.
   - Follow these steps to enable auto-renewal for more than one RDS instance:

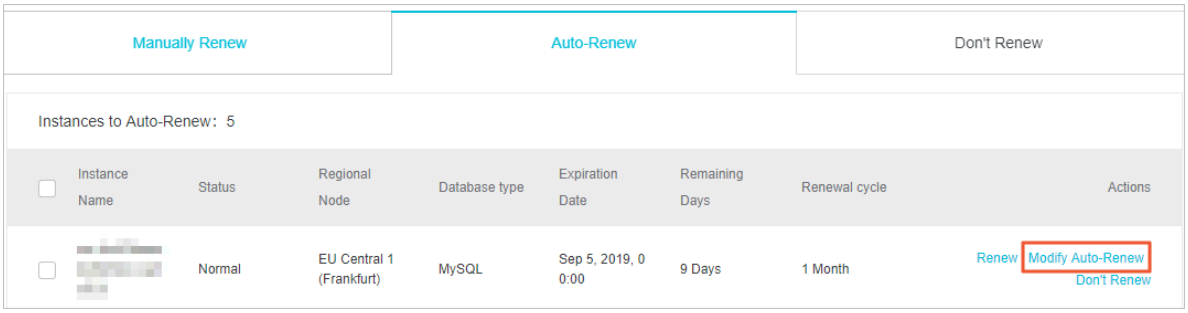
     Select the target RDS instances, and click Enable Auto-Renew below the instance list.
   - In the displayed dialog box, set Auto-Renew Cycle and click Enable Auto-Renew.

Change the auto-renew cycle of an RDS instance

1. Log on to the *RDS console*.
2. In the upper-right corner, choose Billing Management > Renew.



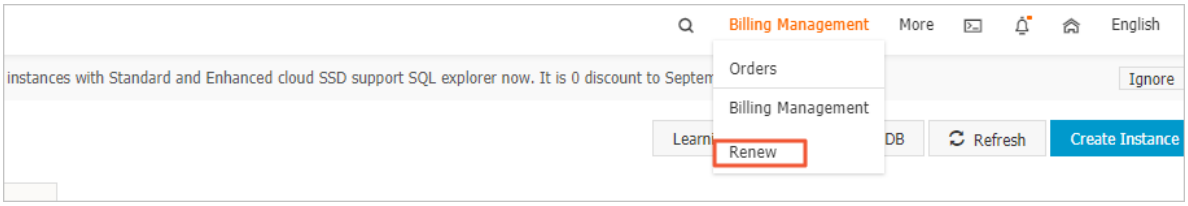
3. In the left-side navigation pane, click ApsaraDB for RDS.
4. On the Auto-Renew tab, find the target RDS instance and in the Actions column click Modify Auto-Renew.



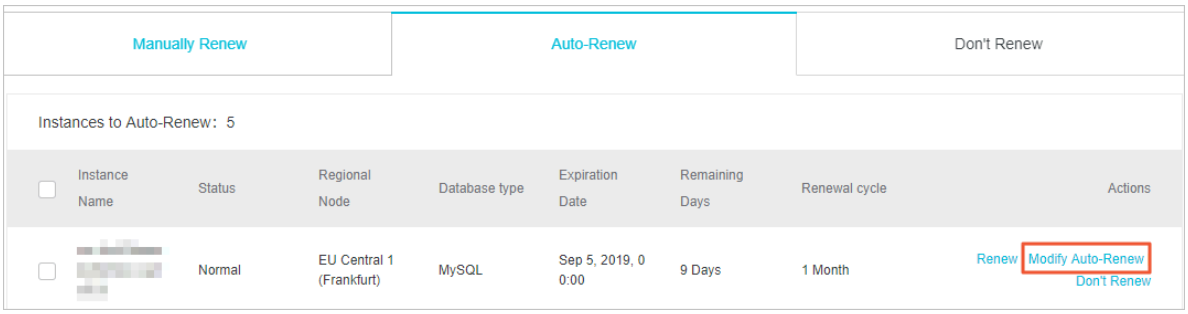
5. **In the displayed dialog box, select Modify Auto-Renew Cycle, select an auto-renew cycle, and click OK.**

Disable automatic renewal for an RDS instance

1. **Log on to the *RDS console*.**
2. **In the upper-right corner, choose Billing Management > Renew.**



3. **In the left-side navigation pane, click ApsaraDB for RDS.**
4. **On the Auto-Renew tab, find the target RDS instance and in the Actions column click Modify Auto-Renew.**



5. **In the displayed dialog box, select Disable Auto-Renew and click OK.**

APIs

Operation	Description
#unique_14	**Used to create an RDS instance.** **Note:** **Automatic renewal is enabled when you create the instance.**
#unique_38	**Used to renew a subscription-based RDS instance.** **Note:** **Automatic renewal is enabled after you create the instance.**

6 Instance

6.1 Restart an RDS for PPAS instance

This topic describes how to restart an RDS for PPAS instance in the RDS console if the number of connections exceeds its upper limit or any performance issue occurs for the instance.

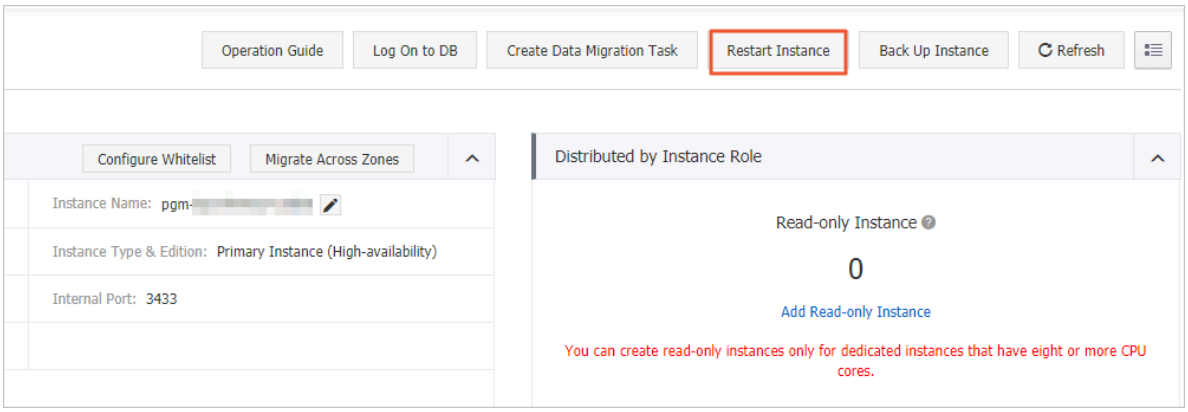
Impact

Restarting an RDS instance may interrupt its connections and impact your services. Exercise caution when performing this action.

Procedure

1. **Log on to the *RDS console*.**
2. **Select the target region.**

3. **Find the target RDS instance. Then, click the instance ID or in the Actions column click Manage.**
4. **In the upper-right corner of the Basic Information page, clickRestart Instance.**



5. In the displayed dialog box, click Confirm.

APIs

API	Description
#unique_41	Used to restart an RDS instance.

6.2 Set the maintenance window of an RDS for PPAS instance

This topic describes how to set the maintenance window of an RDS for PPAS instance so that RDS for PPAS can perform regular maintenance operations as needed according to a defined schedule. The default maintenance window is from 02:00 to 06:00. You can set the maintenance window to the off-peak period of your business to avoid impacts on business.

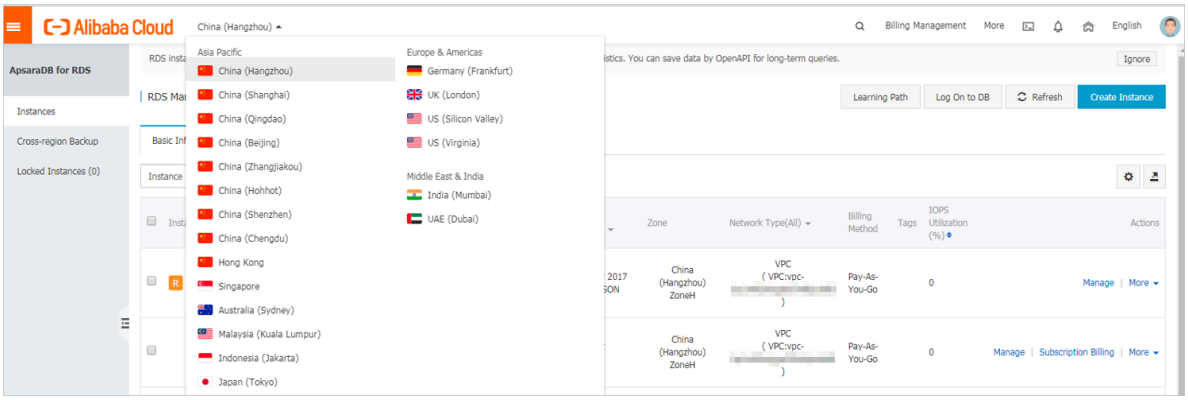
Precautions

- Before maintenance is performed, ApsaraDB for RDS sends SMS messages and emails to the contacts listed in your Alibaba Cloud accounts.
- To guarantee service stability during the maintenance process, the instance enters the Instance Maintaining state before the maintenance time on the day of maintenance. When the instance is in this state, access to data in the database and query operations such as performance monitoring are not affected. However, apart from account and database management and IP address whitelist configuration, modification operations such as upgrade, downgrade, and restart are temporarily unavailable.
- During the maintenance window, the instance is disconnected once or twice. Make sure that you configure automatic reconnection policies for your applicatio ns to avoid service disruptions.

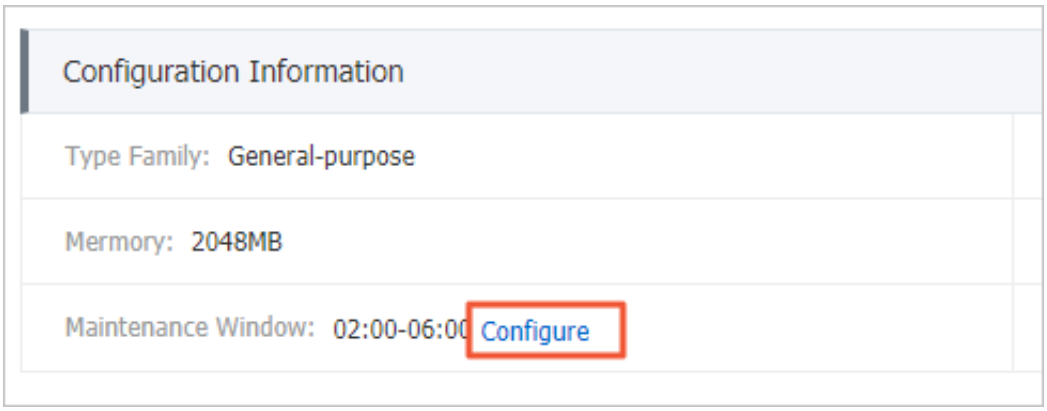
Procedure

1. Log on to the *RDS consoleRDS console*.

2. Select the target region.



3. Find the target RDS instance. Then, click the instance ID, or in the Actions column click Manage.
4. On the Basic Information page, find the Configuration Information section and click Configure to the right of Maintenance Window.



5. Select a maintenance window and click Save.

Note:
The maintenance window is in China Standard Time (UTC +8).

APIs

API	Description
#unique_43	Used to change the maintenance window of an RDS instance.

6.3 Automatically or manually switch over services between the master and slave RDS for MariaDB instances

This topic describes how to automatically or manually switch over services between the master and slave RDS for MariaDB instances. After the switchover, the master instance becomes the salve instance.

In the High-availability Edition, each instance (the master instance) has a slave instance, and data is synchronized between both instances in real time. You can only access the master instance. The slave instance works as a backup and cannot be accessed.

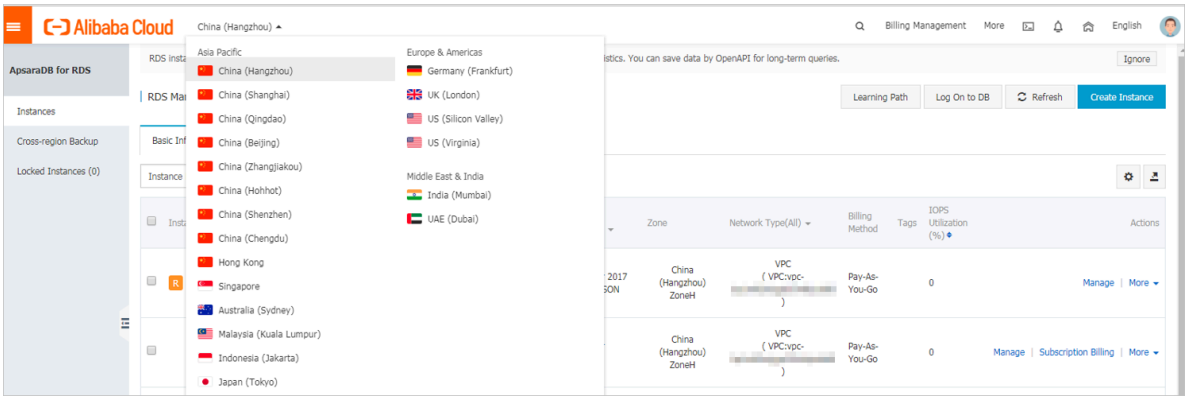
If the master instance cannot be accessed, your business is automatically switched over to the slave instance.

Precautions

During the switchover, your RDS instance may be disconnected. Make sure that your application can automatically reconnect to your RDS instance after the switchover.

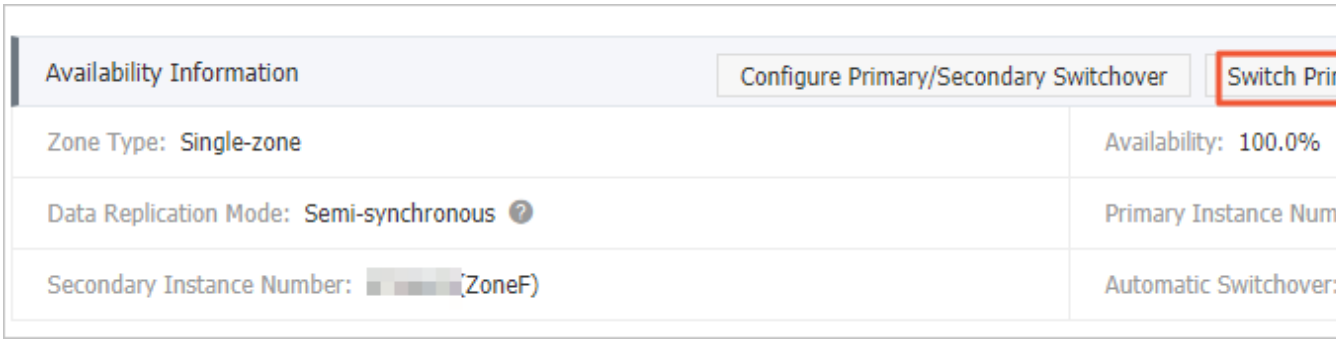
Procedure

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



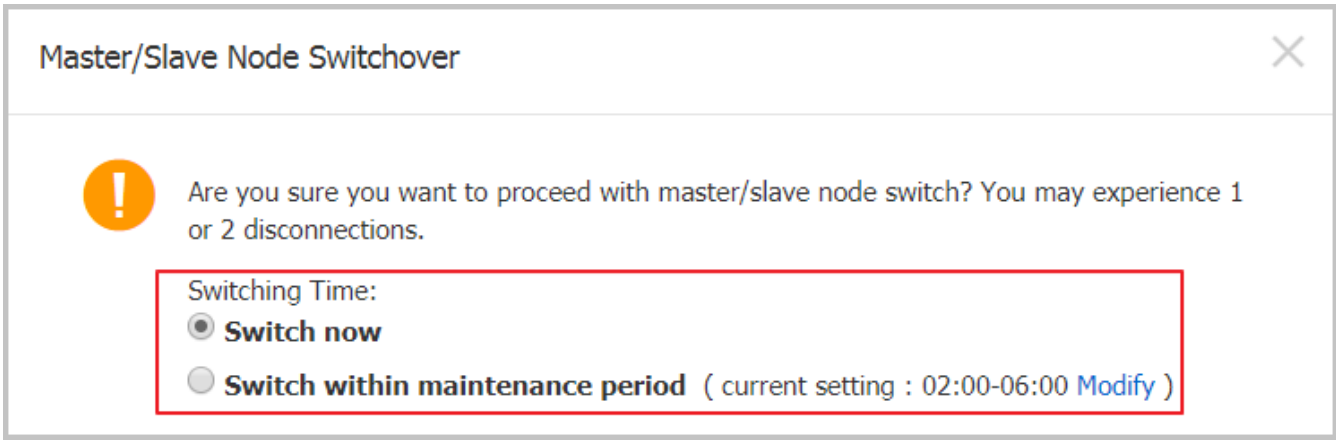
3. **Find the instance and click the instance ID.**
4. **In the left-side navigation pane, click Service Availability.**

5. **In the `Availability Information` section, click Switch Primary/Secondary Instance.**



6. **Select an appropriate time to perform the switch, and click OK.**

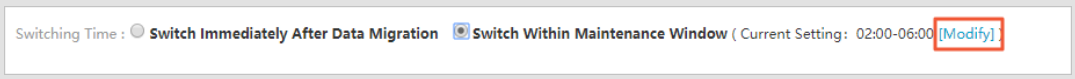
   During the switch, operations such as managing the databases and accounts and switchover the network types cannot be performed. Therefore, we recommend that you select Switch Within Maintenance Window.



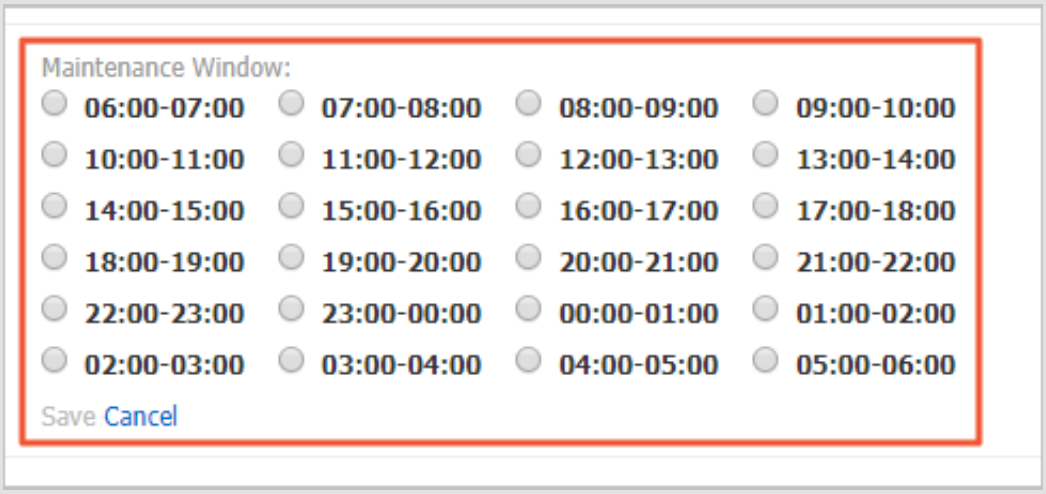
Note:

If you want to change the maintenance window, following these steps:

a. Click Change.



b. In the Configuration Information section, select a maintenance window and click Save.



c. Return to the Service Availability page, refresh the page, and perform the steps to switch the service.

APIs

Operation	Description
SwitchDBInstanceHA	Used to switch over services between the RDS master and slave instances.

6.4 Release an RDS for MariaDB instance

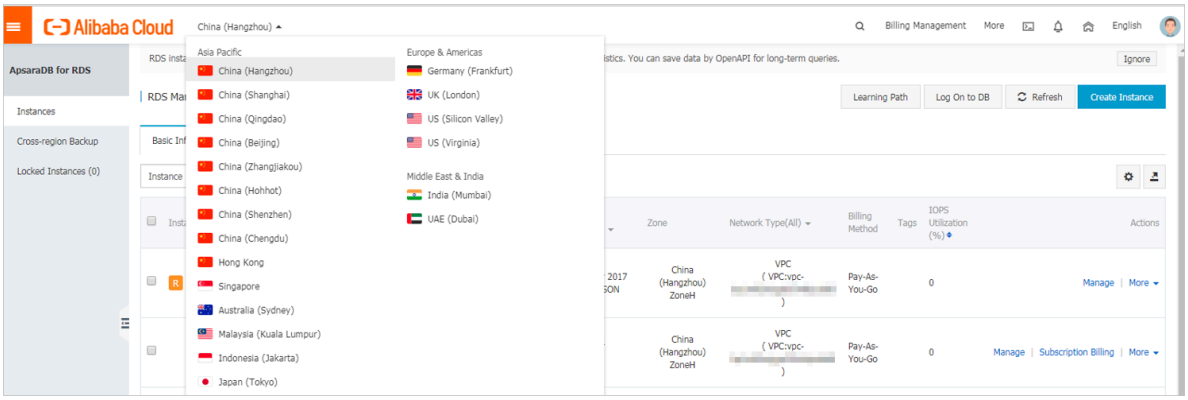
This topic describes how to release an RDS for MariaDB instance, which can use the pay-as-you-go or subscription billing method.

Note:
After an RDS instance is released, its data is deleted immediately. We recommend that you back up the instance data before you release the instance.

Release a pay-as-you-go-based RDS instance

1. Log on to the *RDS console*.

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



3. Use one of the following two methods to open the Release Instance dialog box:

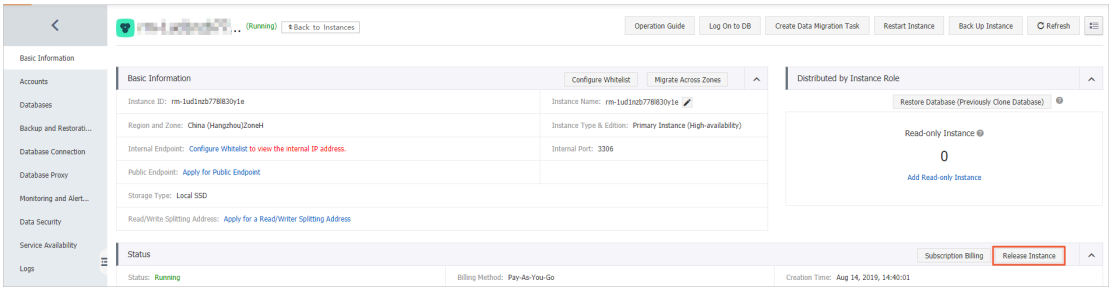
   - Method 1:

     Find the target RDS instance and in the Actions column choose More > Release Instance.

   - Method 2:

     a. Find the target RDS instance and click the instance ID.

     b. On the Basic Information page, find the Status section and click Release Instance.



4. In the Release Instance dialog box, click Confirm.

Release a subscription RDS instance

You can *open a ticket* to apply for releasing a subscription RDS instance.

APIs

API	Description
DeleteDBInstance	Used to release a pay-as-you-go-based RDS instance. (A subscription-based RDS instance cannot be released by calling an API action.)

6.5 Change the configuration of an RDS for MariaDB instance

This topic describes how to change the configuration of an RDS for MariaDB instance, including changing the edition, specifications, storage capacity, storage class, and zone.

You can upgrade or downgrade the configuration of an RDS for MariaDB instance at any time regardless of whether the instance uses the subscription or pay-as-you-go billing method. The new configuration takes effect immediately after you complete the configuration upgrade or downgrade.

Configuration items

Configuration item	Description
CPU and Memory	All MariaDB DB engine versions and editions support the CPU and memory change.
Capacity	All MariaDB DB engine versions and editions allow you to increase storage capacity. You can only decrease the storage capacity of a subscription-based instance with local SSDs during *instance renewal*. **Note:** · For information about the capacity range, see *#unique_19*. · You cannot decrease the storage capacity if the RDS instance uses cloud SSDs. · If the storage capacity range of the current specifications cannot meet your requirements, you can change the specifications.

> **Note:**
> **Changing the preceding configuration does not change the endpoints of the RDS instance.**

Billing

For more information, see *#unique_49*.

Prerequisites

Your Alibaba Cloud account does not have an unpaid renewal order.

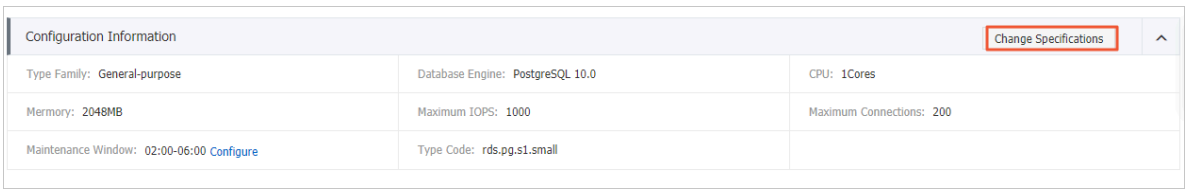
Precautions

When the new configuration is taking effect, the RDS instance may be disconnected for about 30 seconds and most operations related to databases, accounts, and networks cannot be performed. Therefore, we recommend that you change the configuration during off-peak hours or make sure that your application can automatically reconnect to the RDS instance.

Procedure

1. **Log on to the *RDS console*.**
2. **Select the target region.**

3. **Find the target RDS instance and click the instance ID.**
4. **On the Basic information page, find the Configuration Information section and click Change Specifications.**

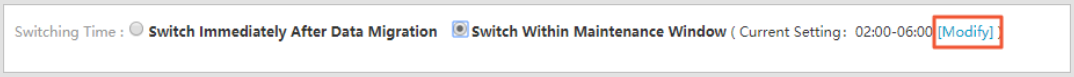


5. Optional. If the RDS instance uses the subscription billing method, click Next in the displayed dialog box.
6. On the Change Specifications page, change the instance configuration. For more information, see *Configuration items*.
7. Specify the time at which you want to change the configuration.
   - Switch Immediately After Data Migration: Change the configuration immediately after the data migration.
   - Switch Within Maintenance Window: Change the configuration during the *maintenance window*.

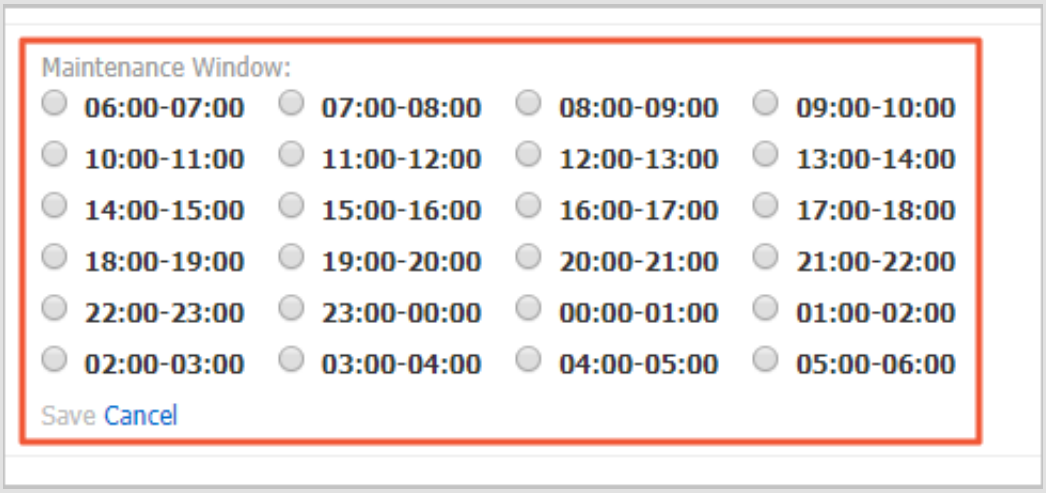
   Note:

   To change the maintenance window, follow these steps:

   a. Click Modify.

   b. In the Configuration Information section, select a maintenance window and click Save.

   c. Go back to the Change Specifications page, refresh the page, and change the configuration again.
8. Select Terms of Service, Service Level Agreement, and Terms of Use and click Confirm.

FAQ

Do I need to migrate data if I only want to expand the storage capacity of an RDS instance?

Check whether the server where the RDS instance is located provides sufficient storage capacity for expansion. If yes, you do not need to migrate data and can directly expand the storage capacity. If no, you must migrate data to a server that provides sufficient storage capacity before you expand the storage capacity.

6.6 Reconfigure parameters for an RDS for MariaDB instance

This topic describes how to use the console or API to view and reconfigure some parameters for an RDS for MariaDB instance. You can also use the console to query the parameter reconfiguration history.

Precautions

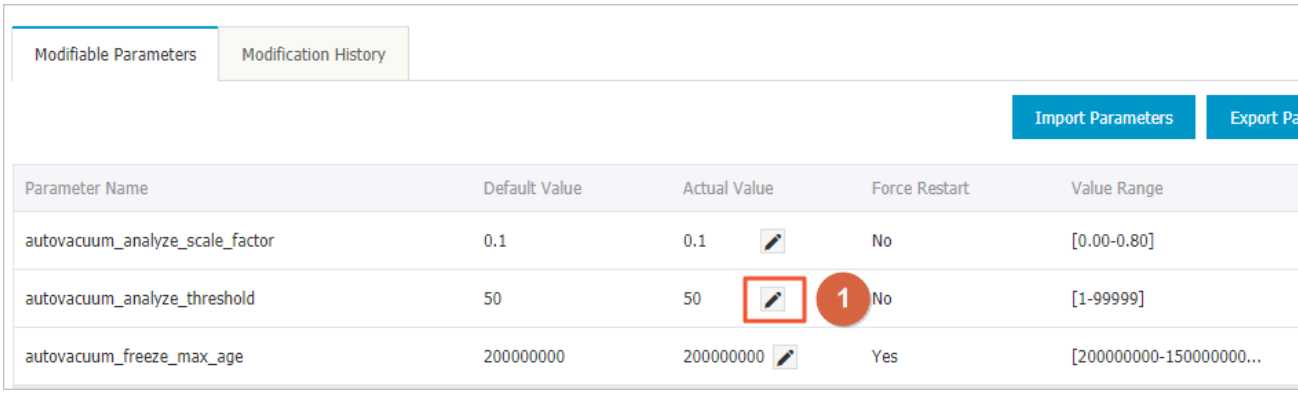
- **When you reconfigure parameters on the Parameters page, see the Value Range column corresponding to each parameter.**
- **After you reconfigure certain parameters, you must restart the RDS instance for the changes to take effect. For more information, see the Restart column on the Parameters page. A restart disconnects the RDS instance. We recommend that you make appropriate service arrangements before you restart an RDS instance. Proceed with caution.**

Reconfigure parameters

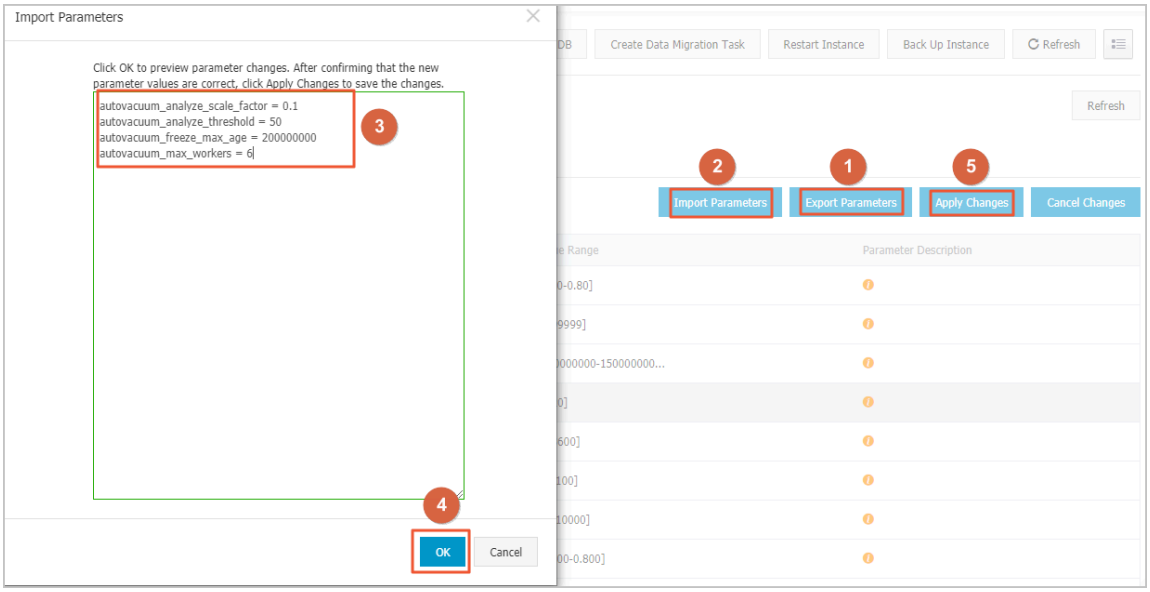
1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**

3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Parameters.**

5. On the Modifiable Parameters tab, reconfigure one or more parameters as needed.
   - To reconfigure only one parameter of the RDS instance, follow these steps:
     a. Find the parameter you want to reconfigure, and in the Actual Value column click  .
     b. In the displayed dialog box, enter a new value within the value range and click Confirm.
     c. In the upper-right corner, click Apply Parameters.
     d. In the displayed dialog box, click Confirm.



   - To reconfigure more than one parameter of the RDS instance, follow these steps:
     a. In the upper-right corner, click Export Parameters to export the parameters as a file to your computer.
     b. Open the parameter file on your computer and reconfigure the parameters.
     c. In the upper-right corner, click Import Parameters.
     d. Copy the parameters and their values from the parameter file and paste them to the Import Parameters dialog box, then click OK.
     e. Verify the parameter values, and click Apply Changes.



View the parameter reconfiguration history

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

3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Parameters.**
5. **Click the Modification History tab.**
6. **Select a time range and click Search.**

APIs

- *#unique_51*
- *#unique_52*
- *#unique_53*

Parameter reference

For more information, see *RDS for MariaDB instance parameters*.

6.7 Instance recycle bin

This topic describes the instance recycle bin and the related operations.

RDS instances are locked when they expire or have overdue payments. You can unlock, recreate, or release instances in the recycle bin.

Renew and unlock an instance

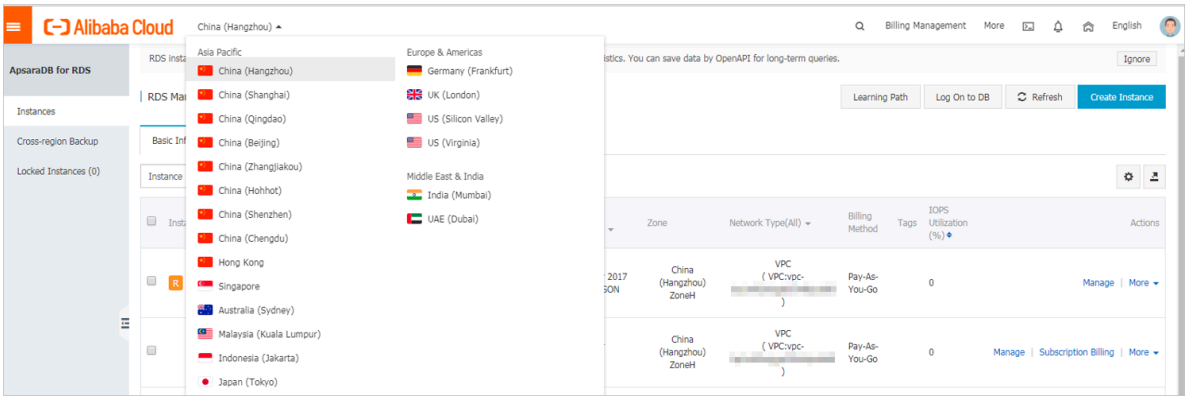
When an RDS instance is locked due to expiration or overdue payments, you can go to the recycle bin to renew and unlock the instance.

Instances that have been locked due to expiration or overdue payment are described as follows:

- **Subscription instances are locked and cannot be accessed within seven days after they expire.**
- **Pay-as-you-go instances cannot be accessed from the second to eighth day after your Alibaba Cloud account incurs overdue payments.**

The procedure is as follows:

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



3. **In the left-side navigation pane, click Locked Instances.**
4. **Find the locked instance and click Unlock to renew the instance.**

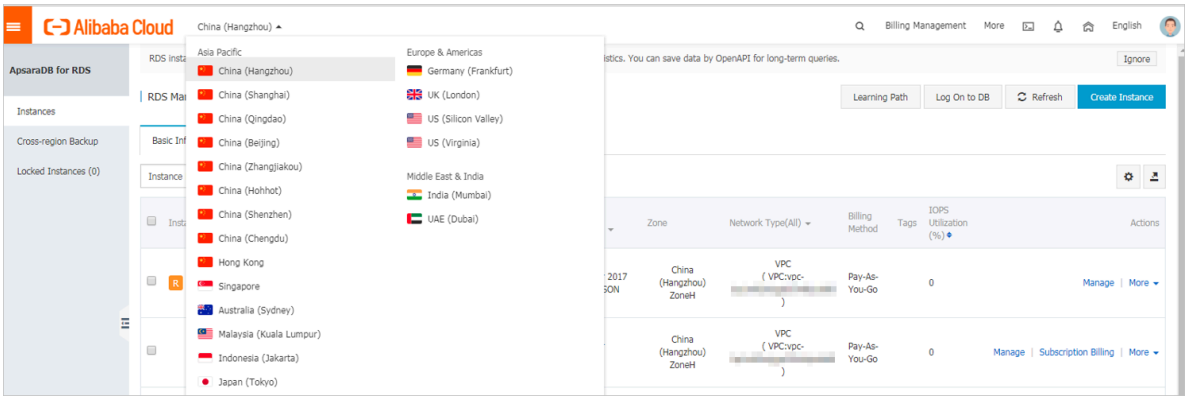
   The instance is unlocked after renewal.

Release an instance

When an RDS instance is locked due to expiration or overdue payments, you can release the instance in the recycle bin.

The procedure is as follows:

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



3. **In the left-side navigation pane, click Locked Instances.**
4. **Find the instance and click Destroy.**

7 Account

7.1 Create an account for an RDS for MariaDB instance

This topic describes how to create an account for an RDS for MariaDB instance.

Account types

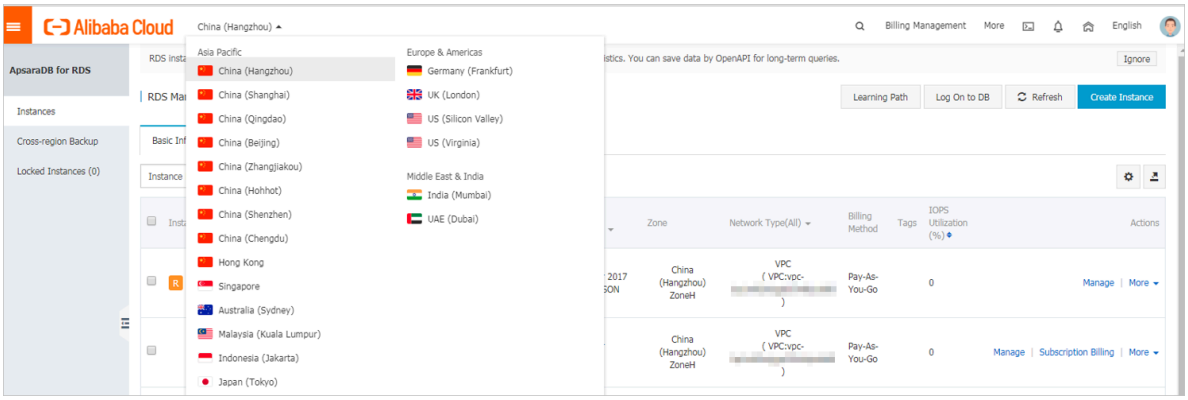
RDS for MariaDB supports two types of database accounts: premier accounts and standard accounts. You can manage all your accounts and databases in the console.

Account type	Description
Premier account	· Can only be created and managed through the console or API. · Each instance can have only one premier account, which can be used to manage all databases and standard accounts. · Has more permissions than standard accounts and can manage permissions at a more fine-grained level. For example, it can assign table-level query permissions 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 permissions. · Cannot create or manage other accounts, or terminate the connections established by other accounts.

Create a premier account

1. **Log on to the** *RDS console*.

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



3. Find the target RDS 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 Premier Account.
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.

Reset the permissions of a premier account

If the premier account of an RDS instance 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 RDS instance is located.

3. Find the target RDS instance and click its ID.
4. In the left-side navigation pane, click Accounts.
5. Find the premier account and in the Actions column click Reset Permissions.
6. Enter the password of the premier account and click OK.

Create a standard account

1. Log on to the *RDS console*.
2. In the upper-left cornere, select the region where the target RDS instance is located.

3. Find the target RDS 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, or underscores (_). It must begin with a letter and end with a letter or digit.
Account Type	Select Standard Account.
Authorized Databases	Grant permissions on one or more databases to the account. This parameter is optional. You can choose to grant permissions to the account after the account is created. a. Select one or more databases from the left area and click Authorize > to add them to the right area. b. In the right area, click Read/Write, Read-only, DDL Only, or DML Only. 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. Note: 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.
Password	The password must contain 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.

APIs

API	Description
#unique_27	**Used to create an account for an RDS instance.**

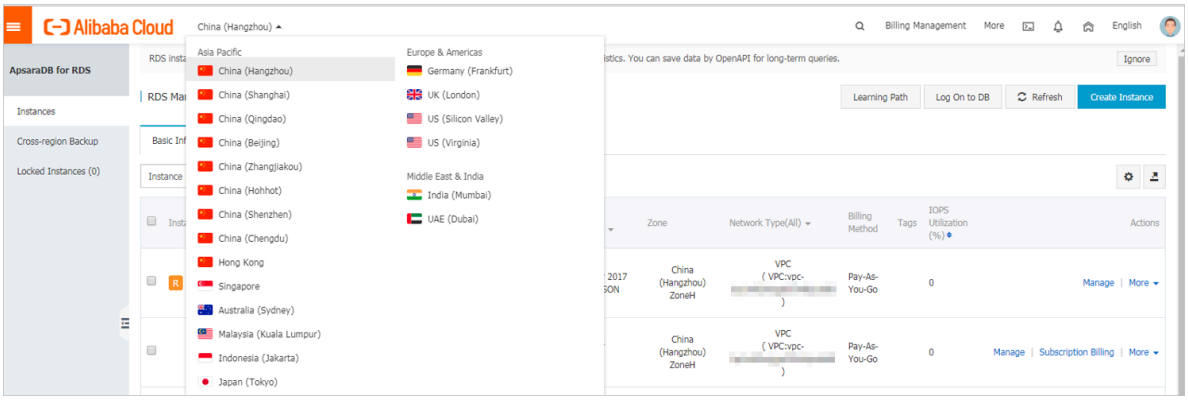
7.2 Reset the password of an account for an RDS for MariaDB instance

This topic describes how to reset the password of an account for an RDS for MariaDB instance in case that the password is lost.

> **Note:**
> **For data security purposes, we recommend you change the password on a regular basis.**

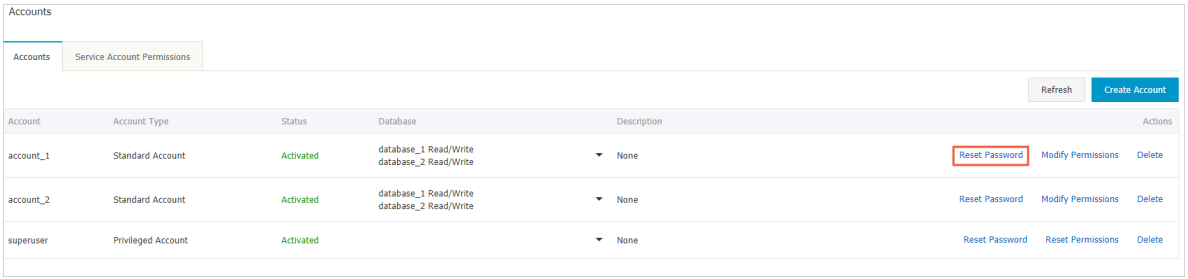
Procedure

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



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Accounts.**

5. On the Accounts tab, select the account whose password you want to reset, and in the Actions column click Reset Password.



6. In the Reset Account Password dialog box, enter a new password and confirm it, then click OK. The password consists of 6 to 32 characters including letters, digits, hyphen (-), or underscores (_). A previously used password is not recommended.

APIs

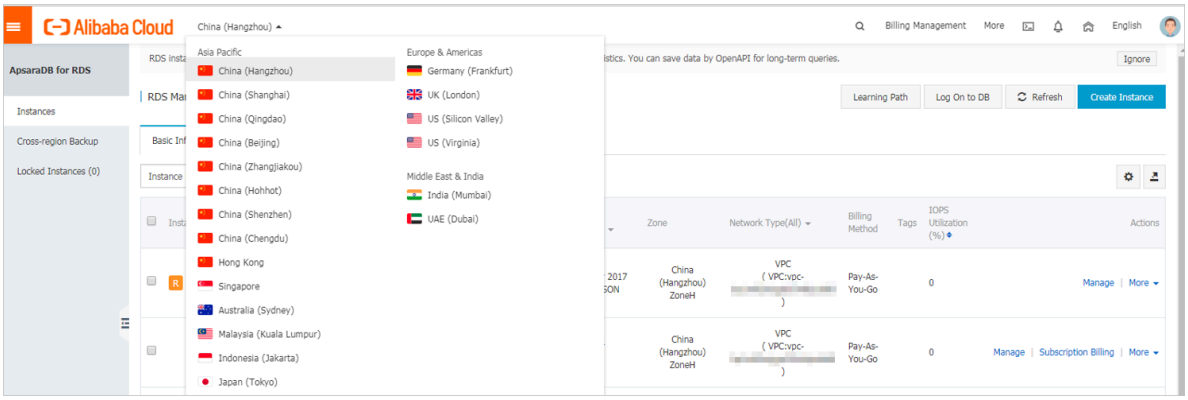
API	Description
#unique_58	Used to reset the password of a database account.

7.3 Change the permissions of an account for an RDS for MariaDB instance

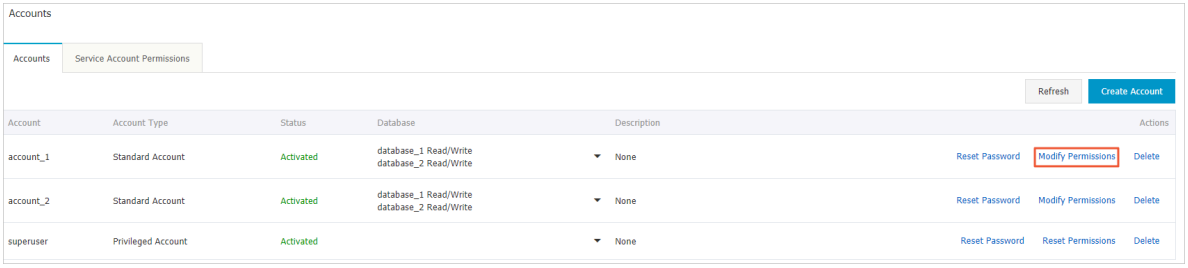
This topic describes how to change the permissions of a standard account for an RDS for MariaDB instance. The permissions of the premier account cannot be changed. You can only reset the premier account if needed.

Procedure

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



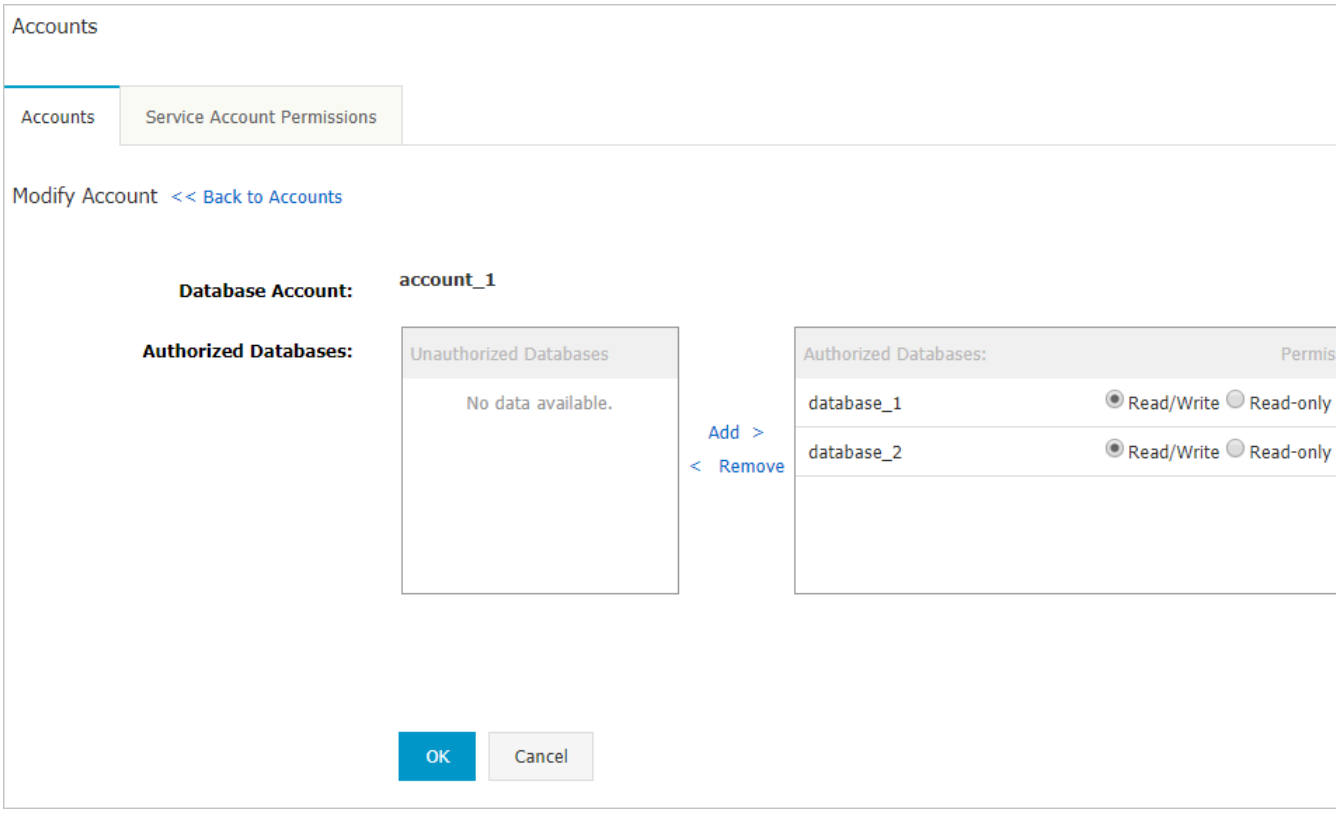
3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Accounts.
5. On the Accounts tab, find the target account and in the Actions column click Modify Permissions.



6. Change the account permissions and click OK.
   - Add an authorized database: Select a database in the Unauthorized Databases section and then click Add > to add it to the Authorized Databases section.
   - Delete an authorized database: Select a database in the Authorized Databases section and then click < Remove to add it to the Unauthorized Databases section.
   - Change the permissions of an authorized database: Find the database in the Authorized Databases section and select Read/Write, Read-only, DDL Only, or DML Only. To change the permissions of more than one authorized database in batches, you can click Full Control Read/Write, Full Control Ready-only, Full Control DDL Only, or Full Control DML Only in the upper-right corner of the Authorized Databases section.

Note:

Either of them is displayed at a time.



7.4 Delete an account for an RDS for MariaDB instance

This topic describes how to delete an account from an RDS for MariaDB instance in the RDS console.

Procedure

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

3. **Find the target RDS instance and click the instance ID.**

4. In the left-side navigation pane, click Accounts.
5. On the Accounts tab, find the account you want to delete, and in the Actions column click Delete.
6. In the displayed dialog box, click Confirm.

APIs

API	Description
#unique_61	Used to delete an account for an RDS instance.

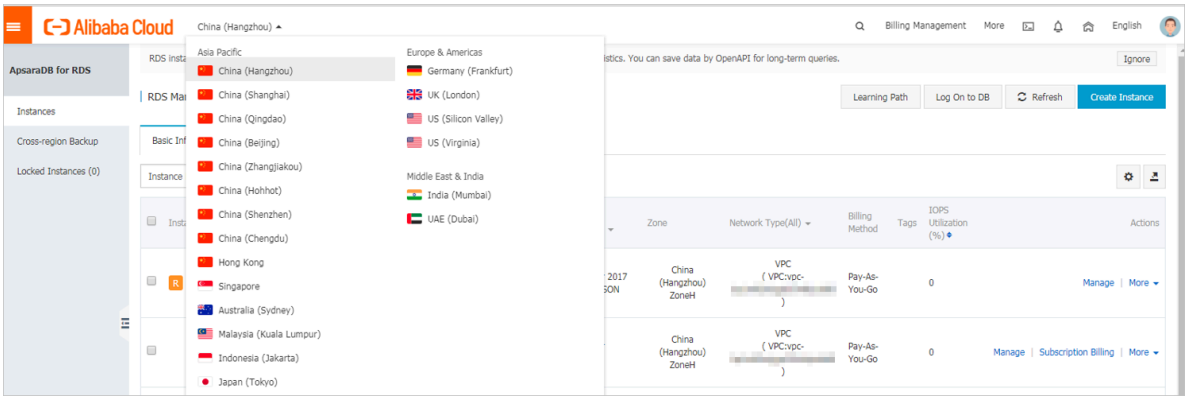
8 Database

8.1 Create a database for an RDS for MariaDB instance

This topic describes how to crate a database for an RDS for MariaDB instance.

Procedure

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



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Databases.**
5. **Click Create Database.**
6. **Set the following parameters.**

Parameters	Description
Database Name	The account name contains 2 to 16 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.

Parameters	Description
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. Note: Only standard accounts are displayed, because the premier account has all permissions for all databases.
Account Type	Select Read/Write, Read-only, DDL only, or DML only.
Description	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
CreateDatabase	Used to create a database for an RDS instance.

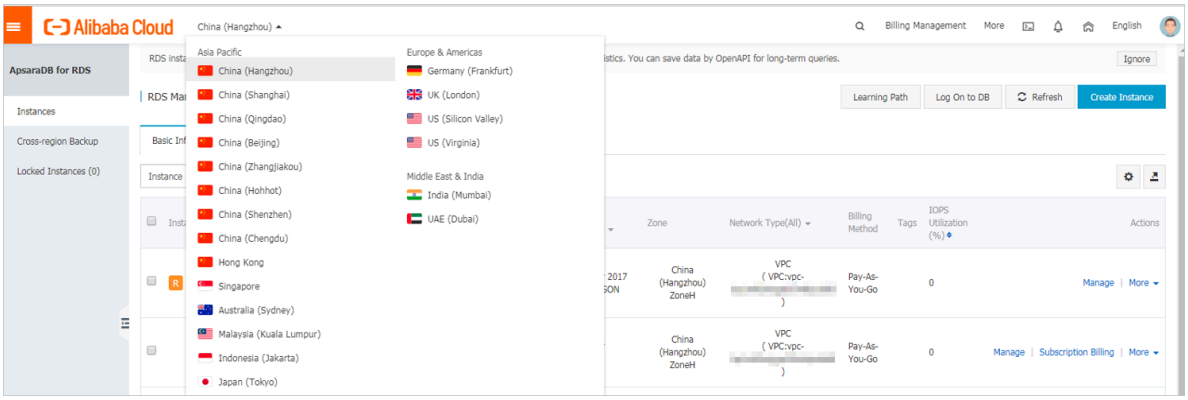
8.2 Delete a database for an RDS for MariaDB instance

This topic describes how to use the RDS console or run an SQL statement to delete a database for an RDS for MariaDB instance. Each method applies to different types of instances. You can choose a suitable method based on the RDS instance whose database you want to delete.

Use the RDS console to delete a database

1. Log on to the *RDS console*.

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



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Databases.
5. Find the database you want to delete, and in the Actions column click Delete.
6. In the displayed dialog box, click Confirm.

Run an SQL statement to delete a database

1. Use a database client to connect to your RDS instance. For more information, see *Connect to an RDS for MariaDB instance*.
2. Run the following command to delete a database:

```
drop database <database name>;
```

APIs

API	Description
#unique_66	Used to delete a database for an RDS instance.

9 Database connection

9.1 Connect to an RDS for MariaDB instance

This topic describes how to connect to an RDS for MariaDB instance. After completing the initial configuration, you can use Data Management Service (DMS), a database client, or the CLI to connect to ApsaraDB RDS for MySQL.

You can connect to an RDS for MariaDB TX instance through any MySQL client. This topic uses *MySQL-Front* as an example.

Prerequisites

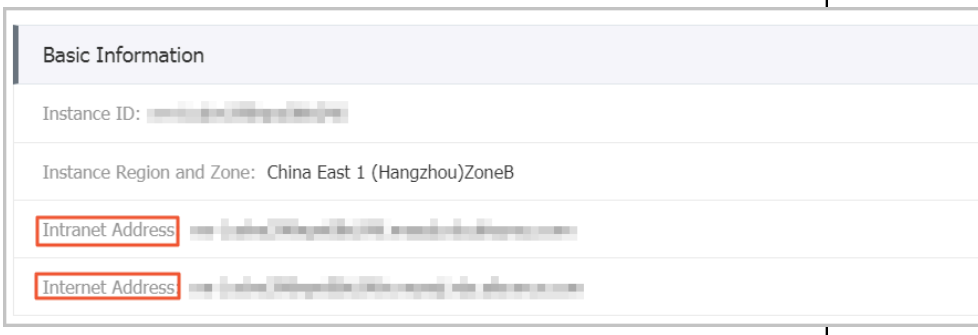
You have *created an RDS for MariaDB TX instance*, *configured a whitelist*, and *Created accounts*.

Use a database client to connect to an RDS instance

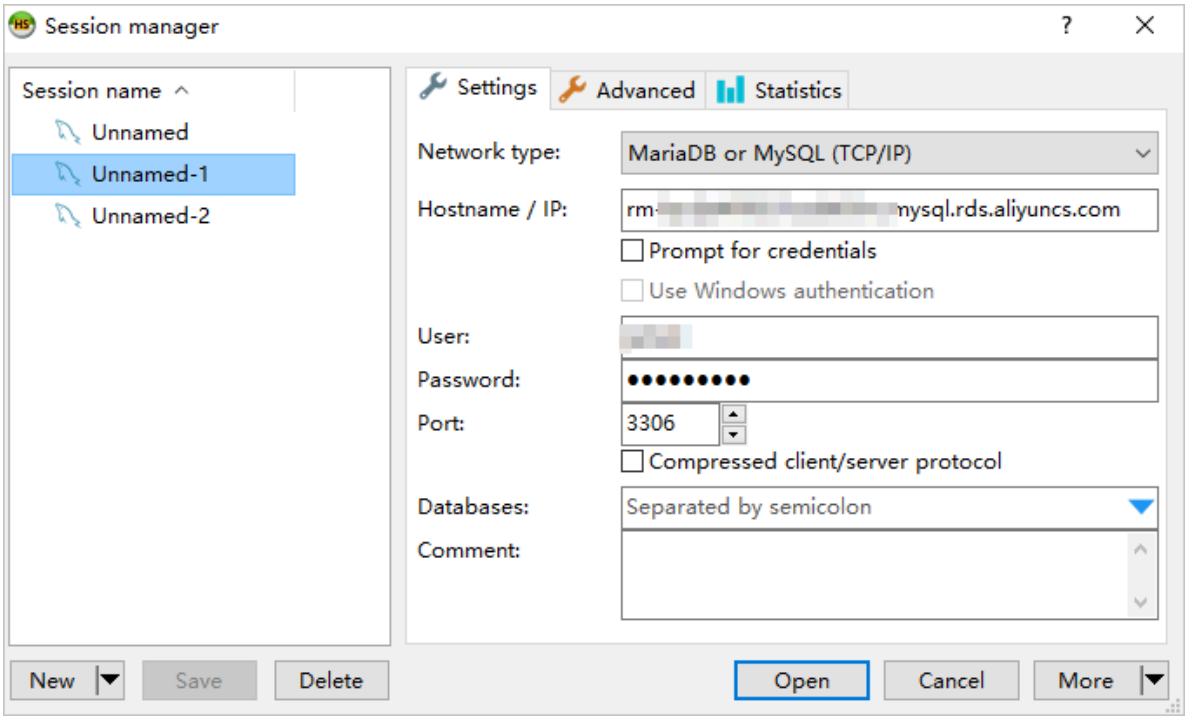
ApsaraDB RDS for MySQL is fully compatible with MySQL. You can connect to an RDS instance from any general-purpose database client in the similar way you connect to a MySQL database. This section describes how to use *HeidiSQL* to connect to an RDS instance.

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).

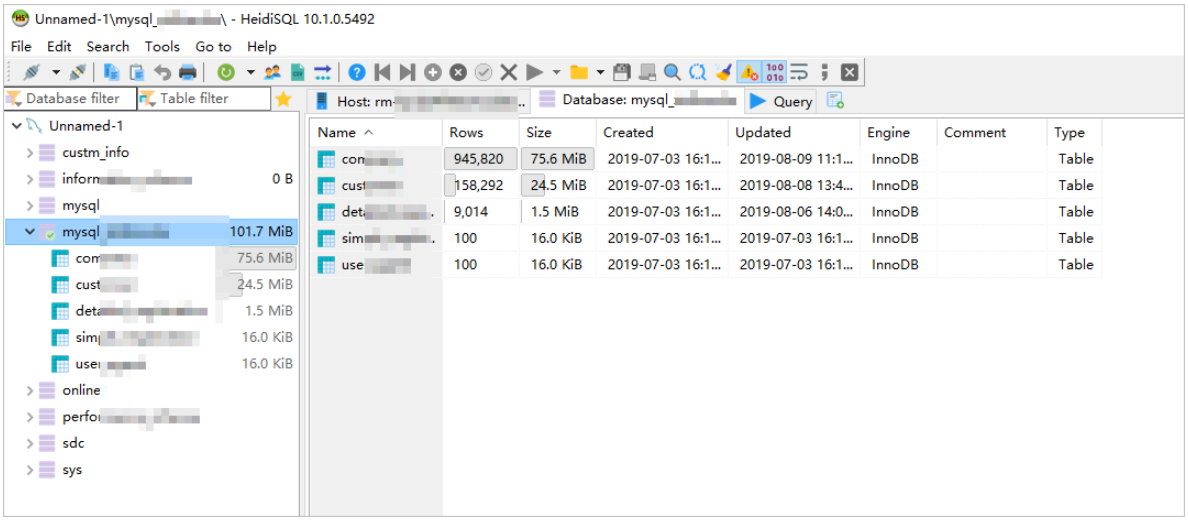
Parameter	Description
Hostname/IP	Enter the private or public IP address of the RDS instance. · If your database client is deployed in an ECS instance that is in the same region and has the same network type as the RDS instance, you can use the private IP address of the RDS instance. For example, if 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. · In the other situations, use the public IP address of the the RDS instance. You can obtain the private and public IP addresses of the RDS instance by completing the following steps: a. Log on to the *RDS console*. b. In the upper-left corner of the page, select the region where the RDS instance is located. c. Find the RDS instance and click its ID. d. On the displayed Basic Information page, find the private and public IP addresses and their corresponding port numbers. 
User	The username of the account that you use to access the RDS instance.
Password	The password of the account that you use to access the RDS instance.

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.



9.2 Configure endpoints for an RDS for MariaDB instance

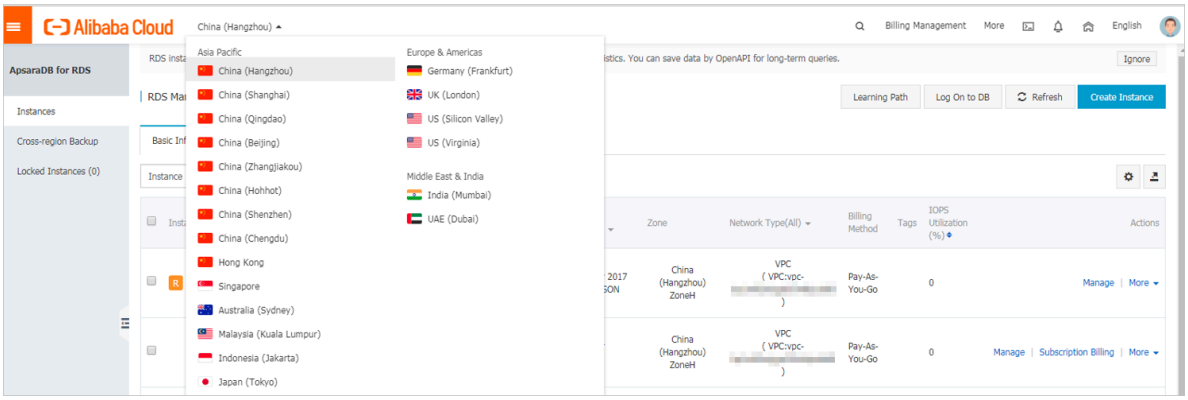
This topic describes how to configure endpoints for an RDS for MariaDB instance. ApsaraDB for RDS provides two types of endpoints: internal endpoints and public endpoints.

Internal and public endpoints

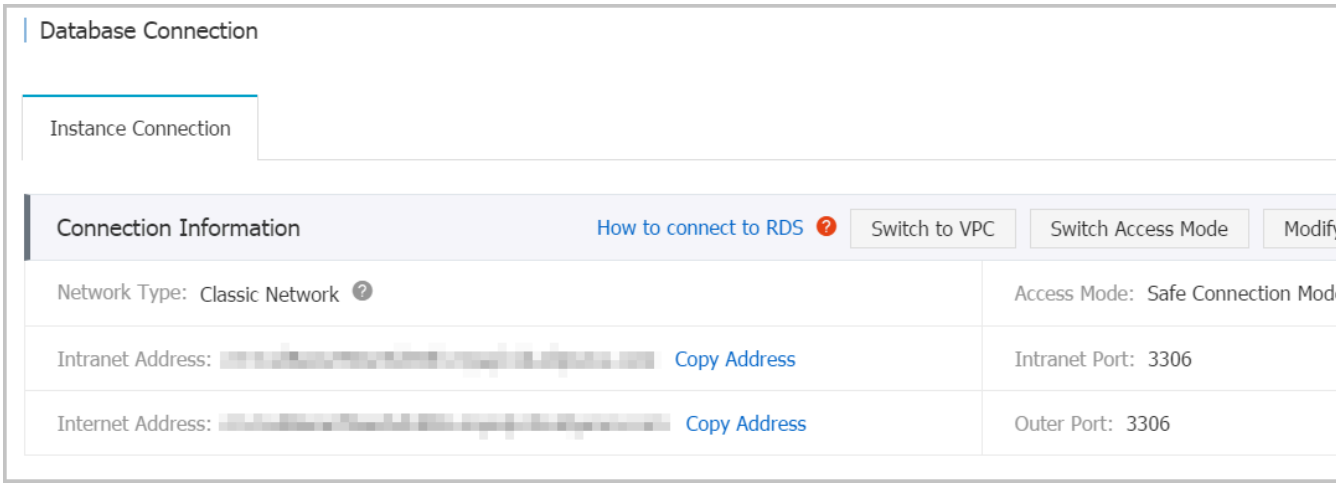
Endpoint type	Description
Internal endpoint	· The internal endpoint is provided by default. You do not need to apply for it and cannot release it. However, you can change the network type. · If your application is deployed on an ECS instance that is in the same region and the network types of the ECS and RDS instances are both VPC, the ECS and RDS instances can communicate with each other by default. You do not need to apply for a public endpoint for the RDS instance. · Accessing an RDS instance through the internal endpoint achieves the high security and performance of the RDS instance.
Public endpoint	· You must manually apply for a public endpoint. You can release the public endpoint if you do not need it. · When you cannot access an RDS instance through the internal endpoint, you must apply for a public endpoint. The specific scenarios are as follows: - When you access an RDS instance from an ECS instance, where the ECS instance and RDS instance are located in different regions, and their network types are different. - When you access an RDS instance from the third-party services or applications. **Note:** · For security purposes, exercise caution when you access your RDS instance through a public endpoint. · We recommend that you migrate your application to an ECS instance in the same region and with the same network type as your RDS instance, and then use the internal endpoint to access your application. This helps to improve transmission speed and data security.

Apply for or release a public endpoint

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



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Database Connection.**
5. · **If you have not applied for a public endpoint, click Apply for Public Endpoint.**
   · **If you have applied for a public endpoint, click Release Public Endpoint.**

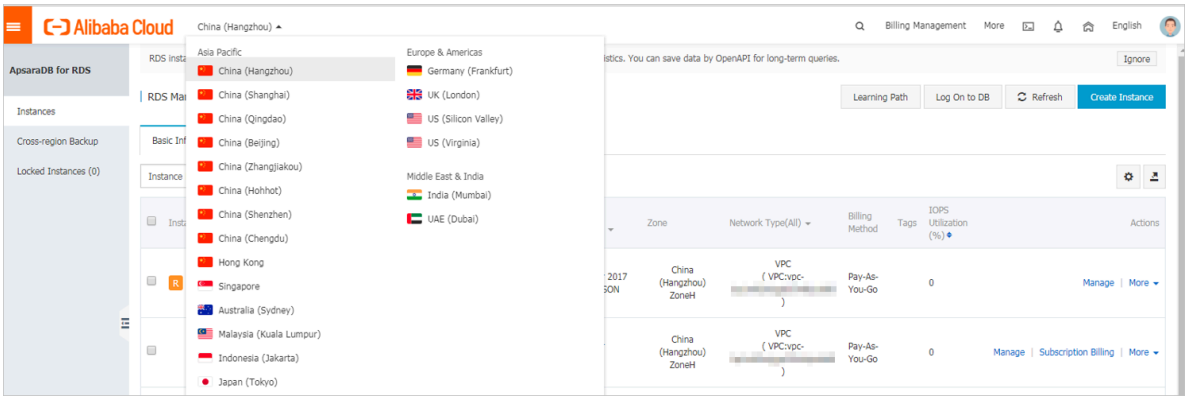


6. **In the message box that appears, click OK.**

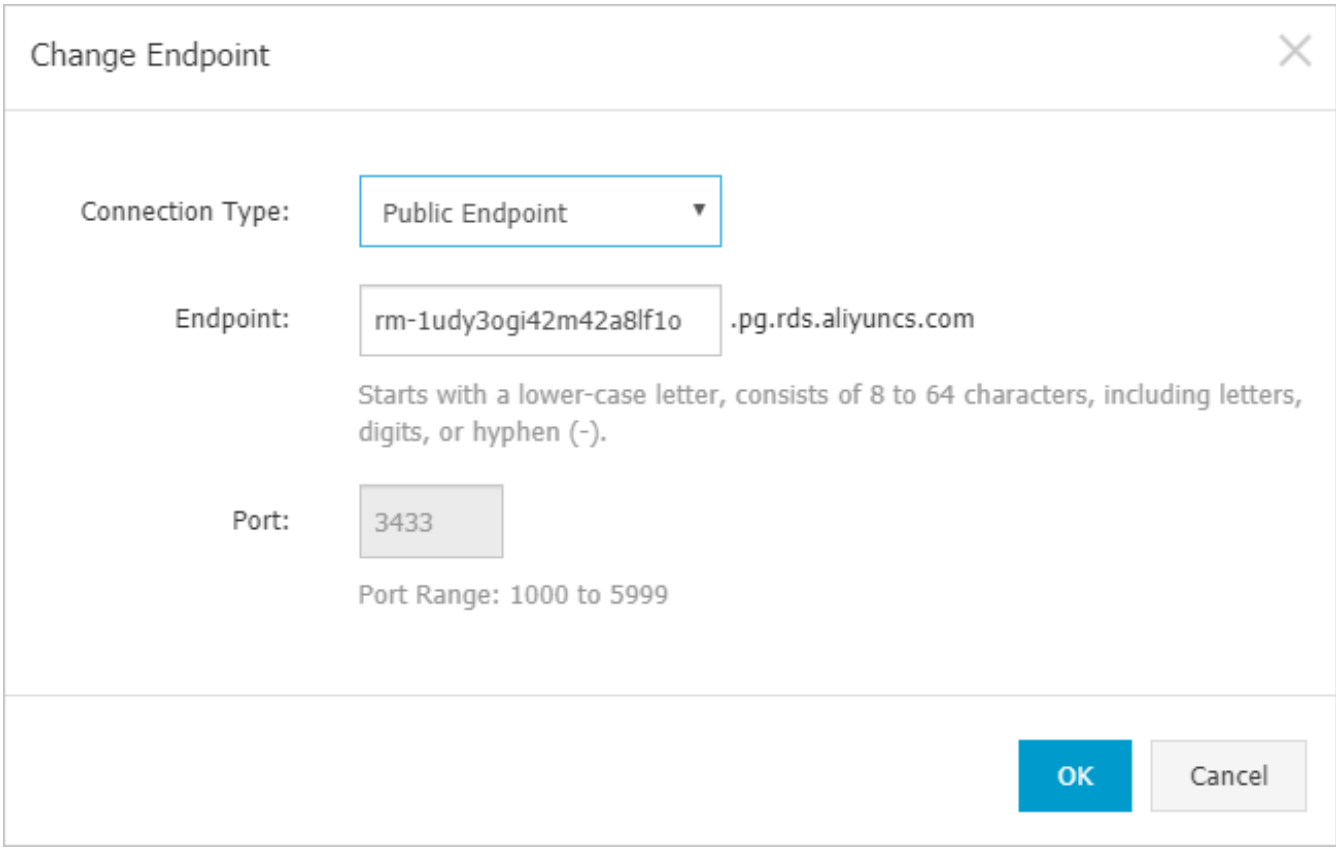
Change the internal and public endpoints

1. **Log on to the *RDS console*.**

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



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Database Connection.
5. Click Change Endpoint.
6. In the dialog box that appears, specify the internal and public endpoints, and click OK.



Note:

- The prefix of the endpoint must be 8 to 64 characters in length and can contain letters, numbers, and hyphens (-). It must start with a lowercase letter.
- In a VPC, either the internal port number or public port number cannot be changed.
- In a classic network, either the internal port number or public port number can be changed.

APIs

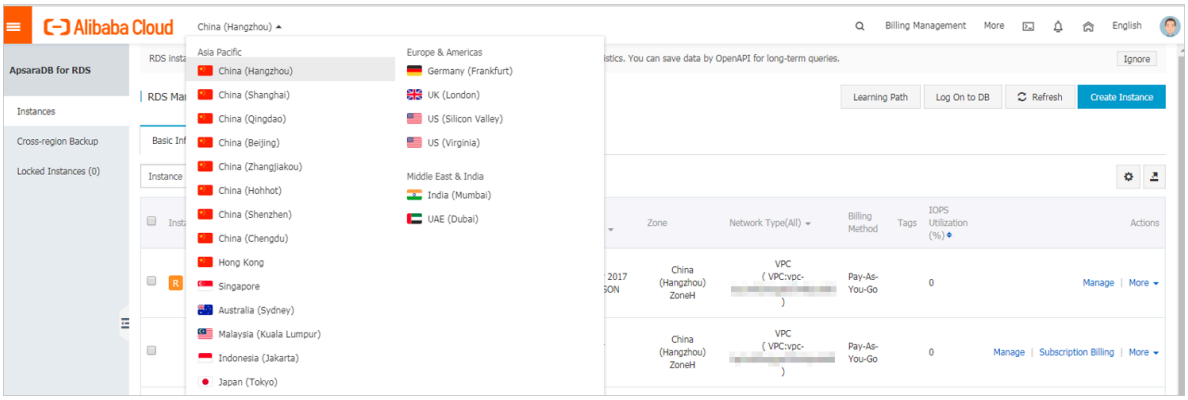
Operation	Description
#unique_69	Used to apply for a public endpoint for an RDS instance.
#unique_70	Used to release the public endpoint of an RDS instance.

9.3 View the internal and public endpoints and ports of an RDS for MariaDB instance

This topic describes how to view the internal and public endpoints and ports of an RDS for MariaDB instance. When connecting to an RDS instance, you must enter its internal or public endpoint and port number.

Procedure

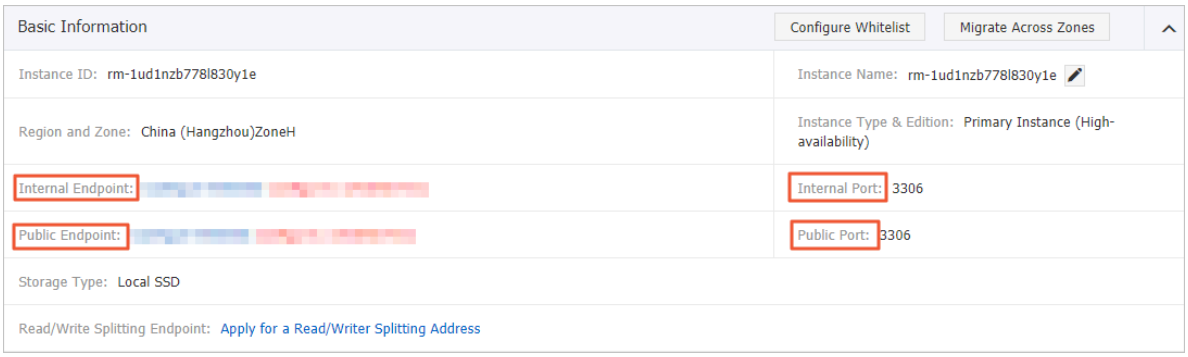
1. Log on to the *RDS console*.
2. In the upper-left corner, select the region where the target RDS instance is located.



3. Find the target RDS instance and click the instance ID.

4. On the Basic Information page, find the Basic Information section, where you can view the internal and public endpoints and ports of the RDS instance.

> **Note:**
>
> - The internal and public endpoints are displayed only after you configure a whitelist.
> - The public endpoint is displayed only after you apply for it.



9.4 Apply for a public endpoint for an RDS for MariaDB instance

This topic describes how to apply for a public endpoint for an RDS for MariaDB instance. Apsara for RDS supports two types of endpoints: internal endpoints and public endpoints. By default, the system provides you with an internal endpoint for connecting to your RDS instance. If you want to connect to your RDS instance through the Internet, you must apply for a public endpoint.

Internal and public endpoints

Endpoint type	Description
Internal endpoint	The internal endpoint is generated by default. Use the internal endpoint 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. We recommend that you use the internal endpoint to access your RDS instance because this is more secure and delivers optimal performance.

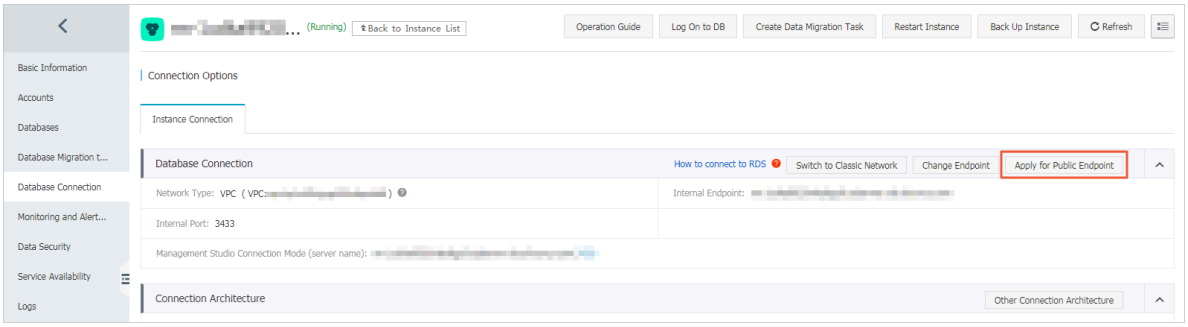
Endpoint type	Description
Public endpoint	You must manually apply for a public endpoint. You can also release it anytime. Use the public endpoint if you cannot access RDS through the intranet. Specific scenarios are as follows: · An ECS instance accesses your RDS instance but the ECS instance is located 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 public endpoint and traffic are currently free of charge. · Using the public endpoint reduces security. Please exercise caution. · To guarantee 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 public endpoint.

Apply for a public endpoint

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

3. Find the target RDS instance and click the instance 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.

   A public endpoint is generated successfully.

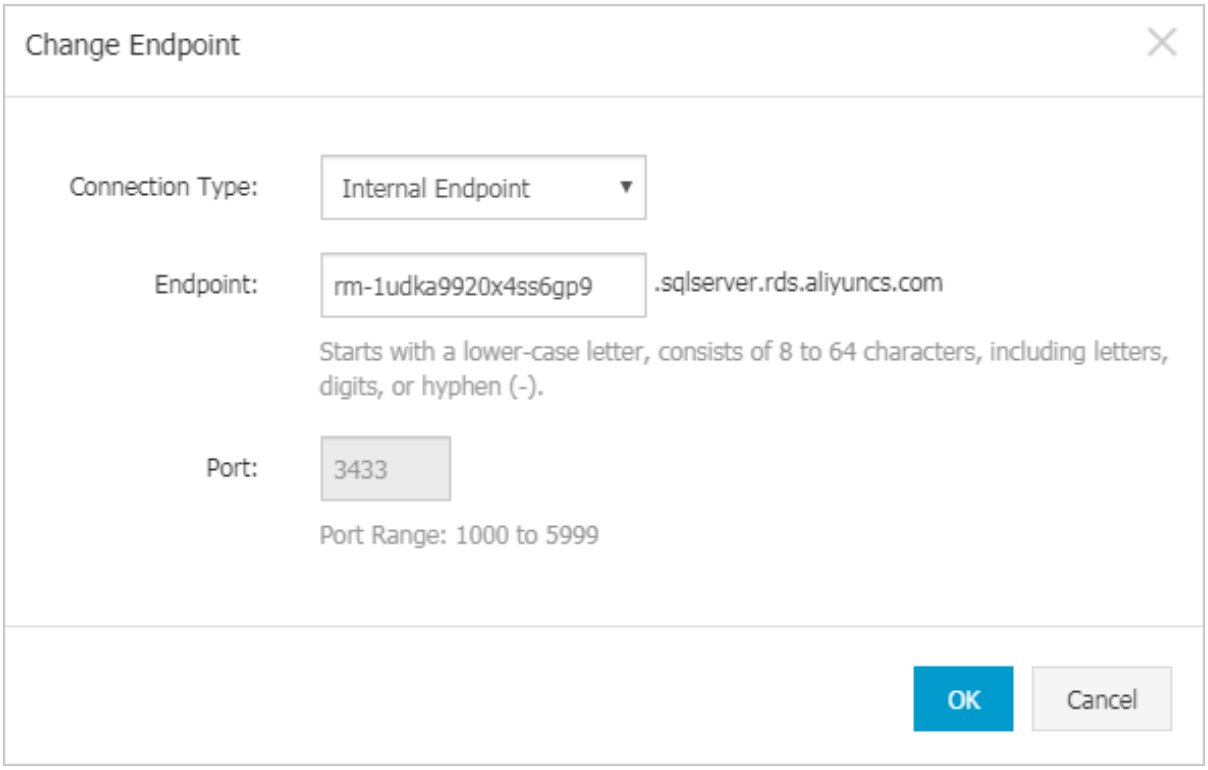
7. Optional. If you want to change the public endpoint or port number, click Change Endpoint. In the displayed dialog box, set the public endpoint and port number and click OK.

   - Connection Type: Select Public Endpoint.

   Note:

The Public Endpoint option is available only after you have applied for a public endpoint.

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



APIs

API	Description
#unique_69	**Used to apply for a public endpoint for an RDS instance.**

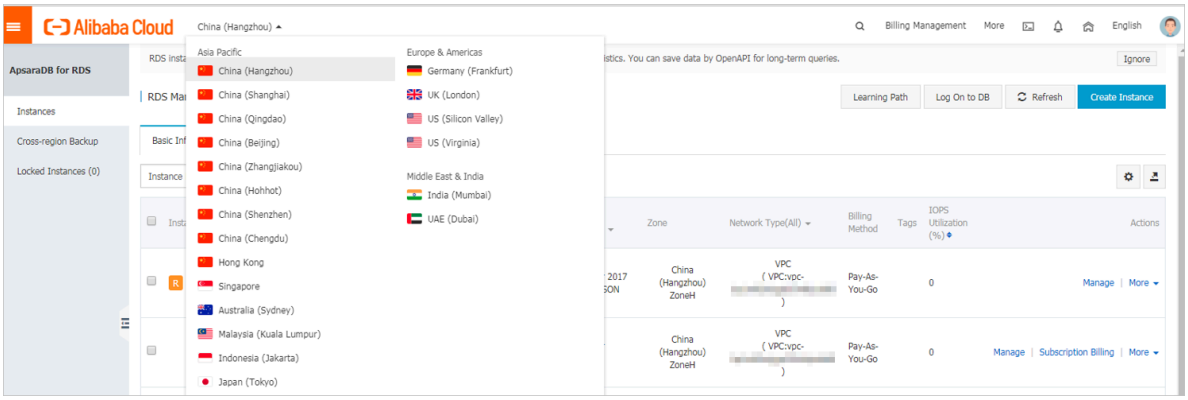
10 Monitoring and alerts

10.1 View resource and engine monitoring data

This topic describes how to view the resource and engine monitoring data of an RDS for MariaDB instance. ApsaraDB for RDS provides a wide range of performance metrics for you to view in the RDS console.

Procedure

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



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Monitoring and Alerts.**
5. **On the Monitoring tab, select the Resource Monitoring or Engine Monitoring monitoring type and specify the time range. The following table describes the monitoring metrics.**

Monitoring type	Metric	Description
Resource Monitoring	IOPS (Input/Output Operations per Second)	The number of I/O requests to the data disk per second and the number of I/O requests to the log disk per second for the RDS instance. Unit: Number/second.
	Memory Usage (%)	The memory usage of the RDS instance.
	CPU Utilization (%)	The CPU usage of the RDS instance.

Monitoring type	Metric	Description
	Total Connections	The total number of connections to the RDS instance.
	Network Traffic (KB)	The input and output traffic of the RDS instance per second. Unit: KB.
Engine Monitoring	TPS (Transactions per Second)/ QPS (Queries per Second)	The average number of transactions per second and the average number of SQL statements executed per second.
	InnoDB Buffer Pool Read Hit Ratio, Usage Ratio, and Dirty Block Ratio (%)	The read hit ratio, usage, and proportion of dirty blocks for the InnoDB buffer pool.
	InnoDB Read/ Write Volume (KB)	The amount of data that is read and written by InnoDB per second. Unit: KB.
	InnoDB Buffer Pool Read/Write Frequency	The number of read and write operations that are performed by InnoDB per second.
	InnoDB Log Read/ Write/fsync	The average frequency of physical writes to log files per second by InnoDB, the log write request frequency, and the average frequency of fsync () writes to log files.
	Number of Temporary Tables Created Automatically on the Hard Disk when MySQL Statements Are Being Executed	The number of temporary tables that are automatically created on the hard disk when the instance runs SQL statements.

Monitorin type	Metric	Description
	MySQL_COMDML	The number of SQL statements that are executed by the RDS instance per second, including: · Insert · Delete · Insert_Select · Replace · Replace_Select · Select · Update
	MySQL_RowDML	The number of operations that are performed by InnoDB per second, including: · The average number of physical writes to log files per second · The number of rows that are read/updated /deleted/inserted from InnoDB tables per second.
	MyISAM Read/ Write Frequency	The number of read/write operations that are performed by MyISAM on the buffer pool per second and the number of read/write operations that are performed by MyISAM on the hard disk per second.
	MyISAM Key Buffer Read/Write /Usage Ratio (%)	The read hit ratio, write hit ratio, and usage of the MyISAM key buffer per second.

10.2 Set the monitoring frequency

This topic describes how to set the monitoring frequency for an RDS for MariaDB instance.

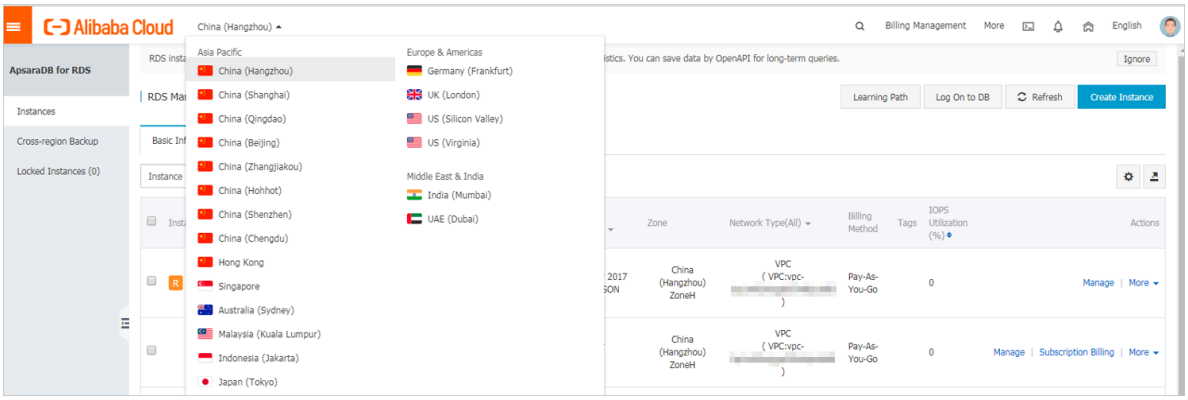
Background information

RDS for PPAS supports two monitoring frequencies:

- **Once per 60 seconds (monitoring period: 30 days)**
- **Once per 300 seconds (monitoring period: 30 days)**

Procedure

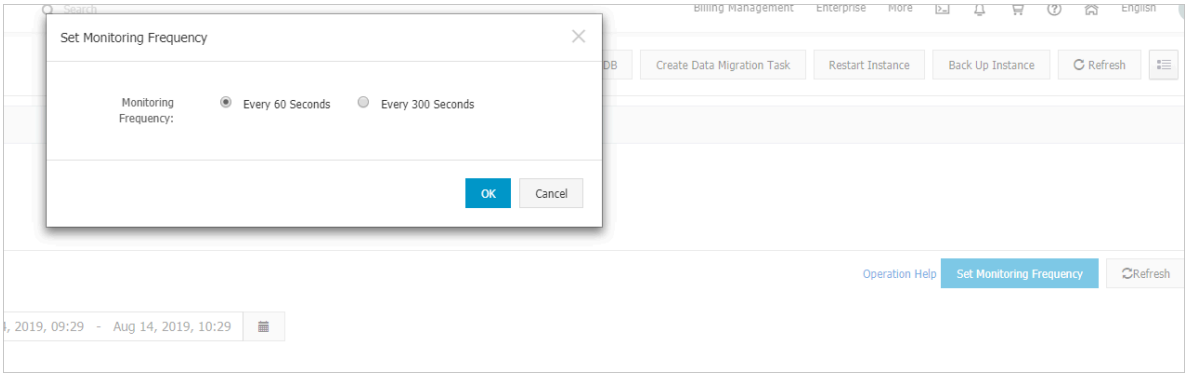
1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Monitoring and Alerts.**

> **Note:**
> **For information about the monitoring metrics supported by the instance, see *View resource and engine monitoring data*.**

5. **Click the Monitoring tab.**
6. **Click Set Monitoring Frequency.**
7. **In the Set Monitoring Frequency dialog box, select the monitoring frequency and click OK.**



10.3 Set an alert rule

This topic describes how to set an alert rule for an RDS instance. ApsaraDB for RDS offers the instance monitoring function, and sends messages to you after

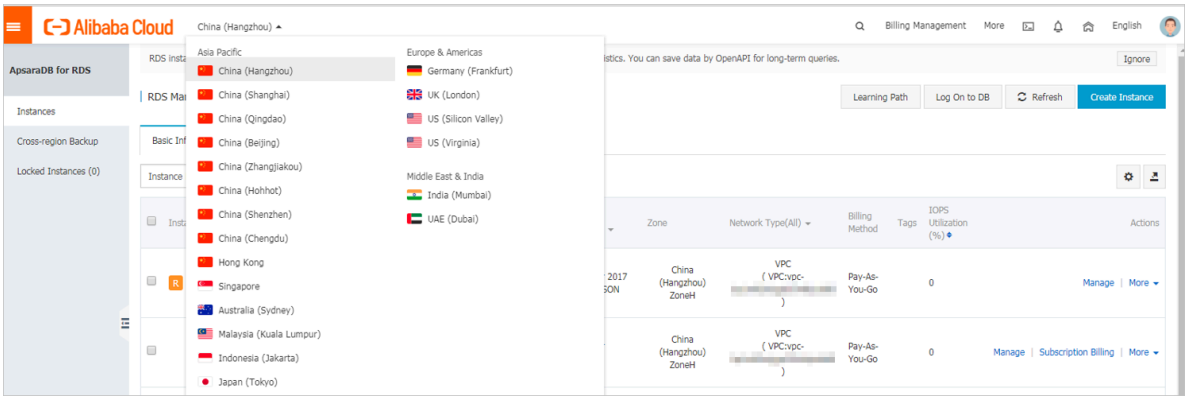
detecting an exception in an instance. In addition, when the instance is locked due to insufficient disk space, the system sends a message to you.

Background information

Alibaba CloudMonitor offers monitoring and alarming. CloudMonitor helps you set alarm rules for metrics. You must add alarm contacts while set a contact group. The alarm contacts and the contact group are notified immediately when an alarm is triggered in the event of exceptions. You can create an alarm contact group using a related metric.

Procedure

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



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Monitoring and Alerts.
5. Click the Alerts tab.
6. Click Set Alert Rule.

   You are directed to the CloudMonitor console.

   Note:
   You can click Refresh to manually refresh the current status of the alert metrics.
7. In the left-side navigation pane, choose Alarms > > Alarm Contacts to open the Alarm Contact Management page.

   Note:
   When alert rules are set for the first time, if the alert notification object is not a contact of the Alibaba Cloud account of RDS, the alarm contact and alarm

contact group must be created first. If you have already set the alarm contact and the alarm contact group, go to Step 10.

8. Click Create Alarm Contact.
9. In the Set Alarm Contact dialog box, enter the alarm contact information and click Send verification code. Then, enter the verification code sent to your mailbox, and click Save.

> Note:
>
> - We recommend that you perform the next step to create the alarm contact group after you add all alarm notification objects.
> - You can click Edit to modify a contact, or click Delete to delete a contact.

10. On the Alarm Contact Management page, click the Alarm Contact Group tab.
11. Click Create Alarm Contact Group.
12. Set `Group Name` and `Description`, select a contact from Existing Contacts, click  to add the contact to `Selected Contacts`, and click OK.

> Note:
> On the Alarm Contact Group page, you can click  to modify a contact group, click X to delete a contact group, or click Delete to delete a contact in the contact group.

13. After creating the alarm contact group, choose Cloud Service Monitoring > ApsaraDB for RDS from the left-side navigation pane.
14. Select the region of RDS for which the alert rule is to be set.
15. Find the target instance and click Alarm Rules in the Actions column.

    The system displays the metrics of the current alert.
16. Click Create Alarm Rule to add a new alert rule.

> Note:
> You can click Modify, Disable, or Delete for the metrics as needed.

11 Data security

11.1 Configure a whitelist for an RDS for MariaDB instance

This topic describes how to configure a whitelist for an RDS for MariaDB instance.

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

RDS for PostgreSQL provides two types of whitelists::

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

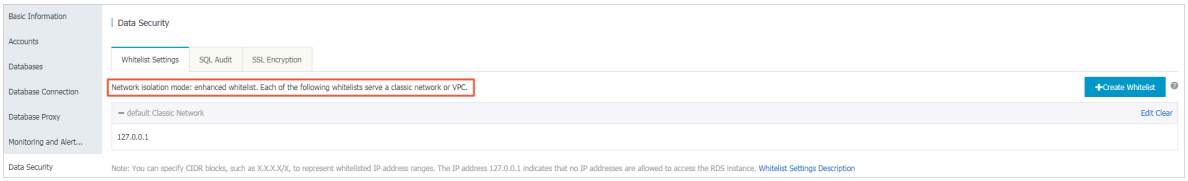
A whitelist can be used to improve the security of your RDS instance. We recommend that you update the whitelist on a regular basis. Configuring a whitelist does not affect the normal operation of your RDS instance.

Configure an IP address whitelist

Precautions

- **The default IP whitelist can only be edited or cleared, but cannot be deleted.**
- **Each IP whitelist can have up to 1,000 IP addresses or CIDR blocks. If you want to add a large number of IP addresses, we recommend that you group these IP addresses into CIDR blocks, for example, 192.168.1.0/24.**

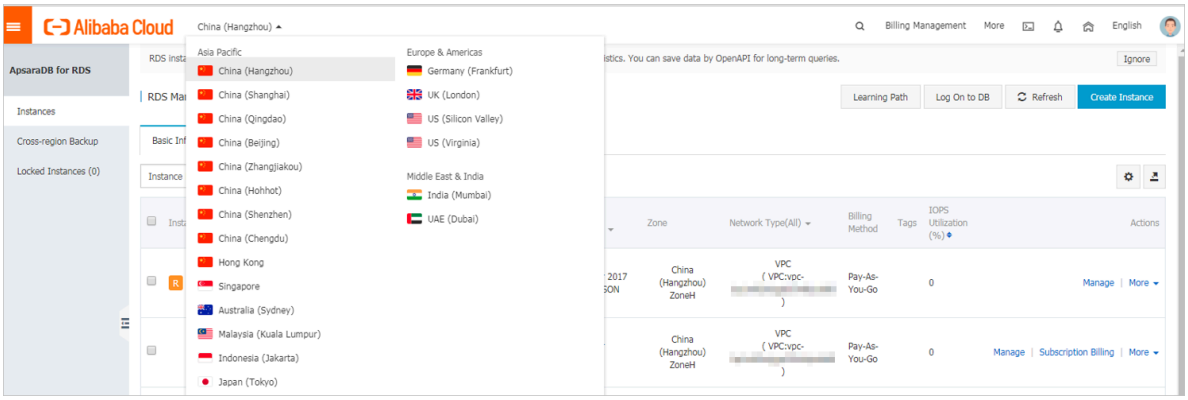
- **Before configuring a whitelist, you must confirm which network isolation mode your RDS instance is in, and then perform operations accordingly.**



> **Note:**
> **The intranet where an RDS for MariaDB instance is located must be a VPC.**

Configure an enhanced whitelist

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



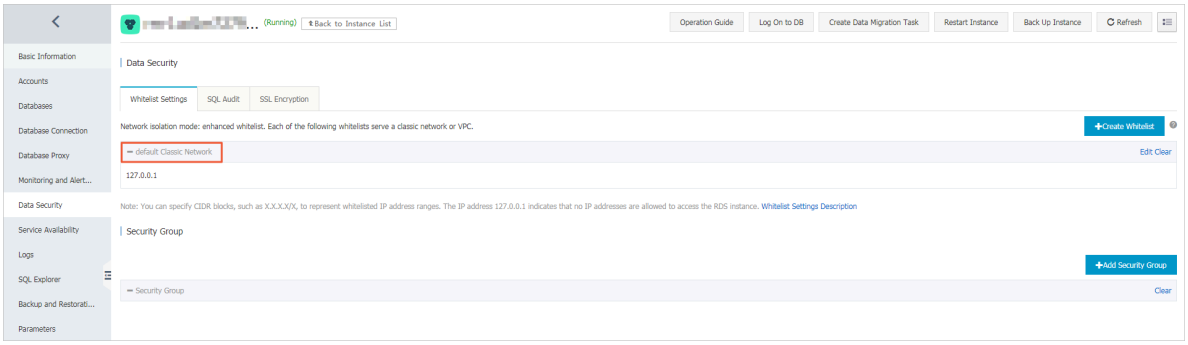
2. **Find the target instance and click its ID.**
3. **In the left-side navigation pane, click Data Security.**
4. **On the Whitelist Settings tab page, follow these instructions based on your usage scenario:**

   - **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.

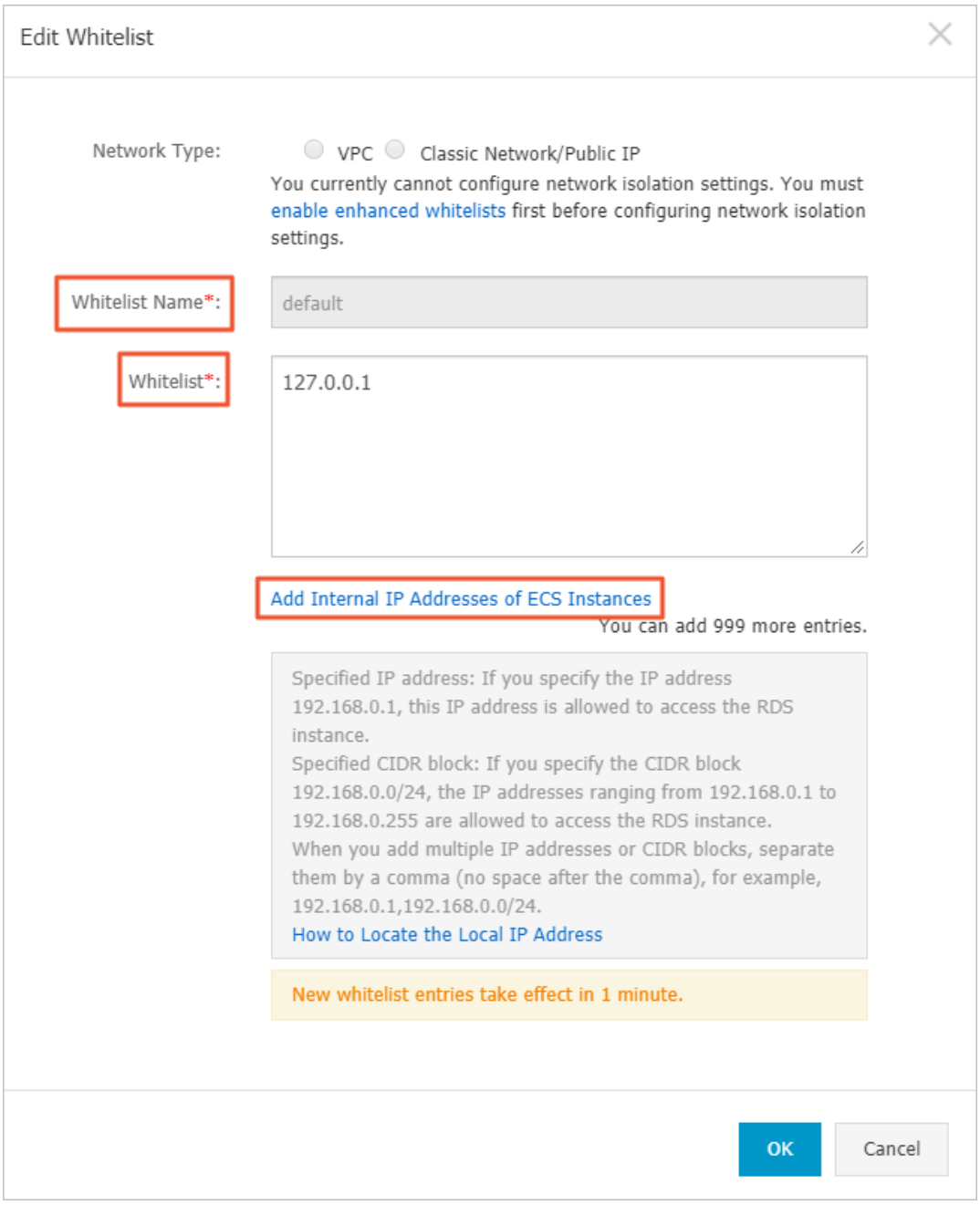


5. In the displayed Edit Whitelist dialog box, specify IP addresses or CIDR blocks used to access the instance, and then click OK.

   - 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:**

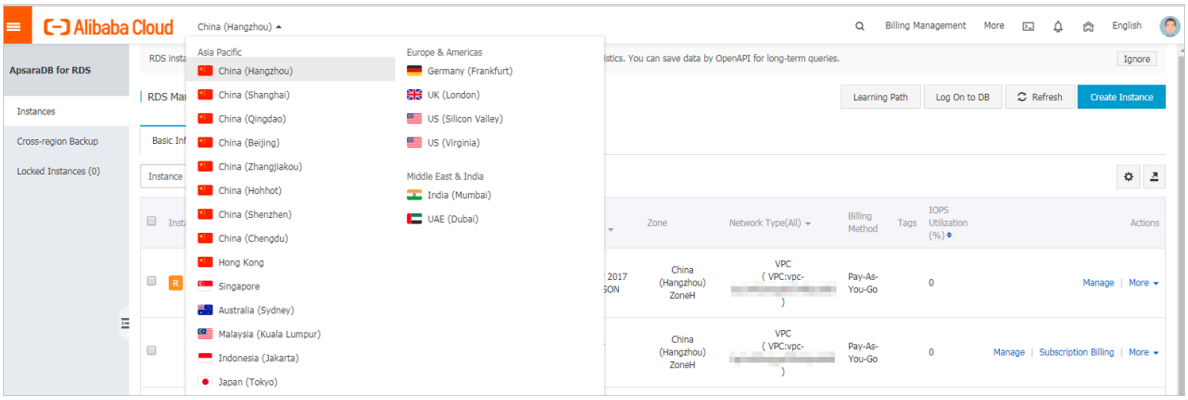
After you add an IP address or CIDR block to the default whitelist, the default address 127.0.0.1 is automatically deleted.



Configure a standard whitelist

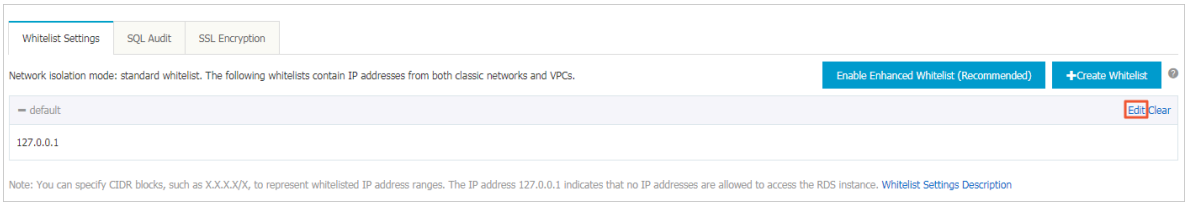
1. **Log on to the** *RDS console*.

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.

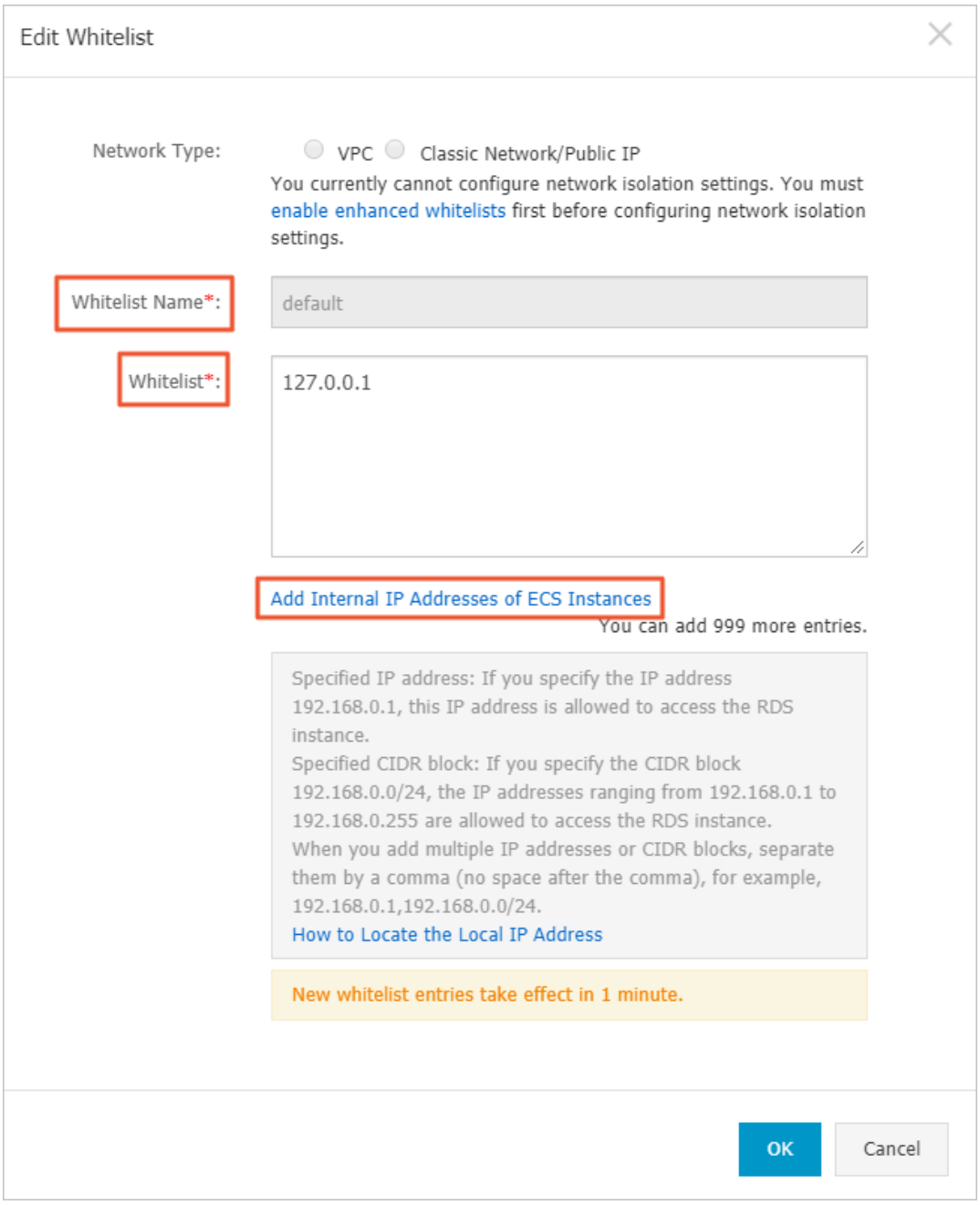
> **Note:**
> You can also click Create Whitelist to create a whitelist.



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.



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 must 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_22*

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.

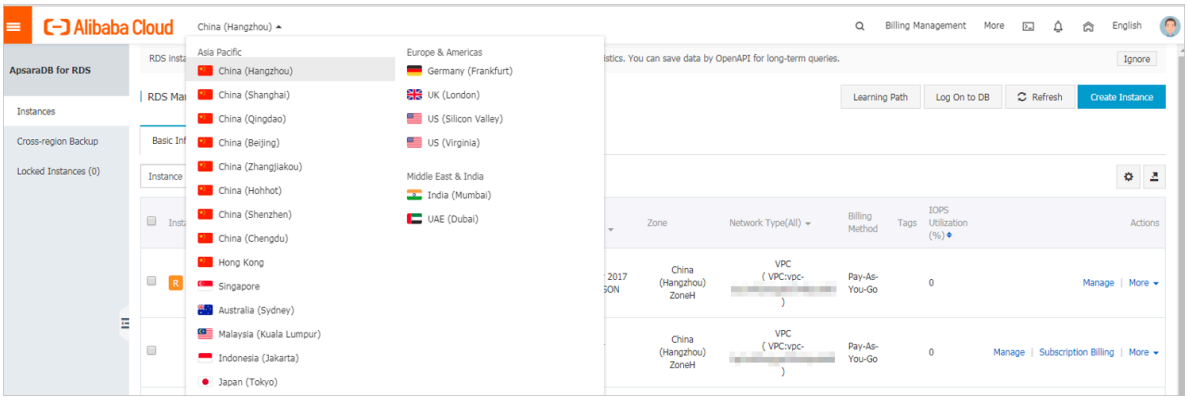
For more information, see *Create a security group*.

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
#unique_23	Used to view the IP address whitelist of an RDS instance.
#unique_24	Used to modify the IP address whitelist of an RDS instance.

11.2 Switch to the enhanced whitelist mode for an RDS for MariaDB instance

This topic describes how to switch to the enhanced whitelist mode for an RDS for MariaDB instance.

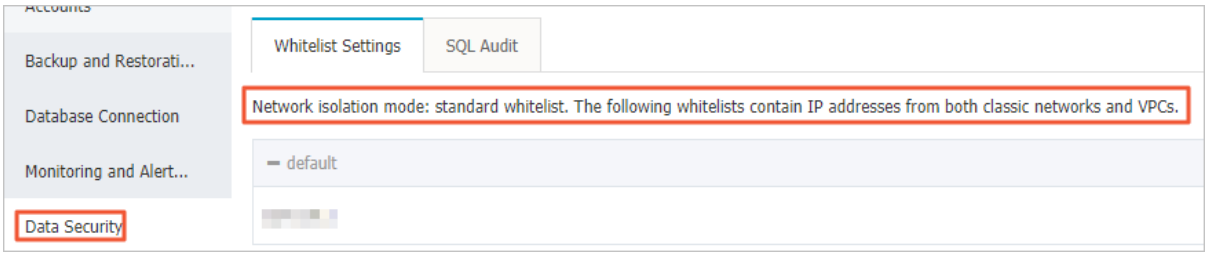
> **Note:**
> Currently the enhanced whitelist mode is unavailable due to a network link upgrade. Notifications are given when the enhanced whitelist mode is available.

IP whitelist modes

ApsaraDB for RDS instances provide the following two IP whitelist modes:

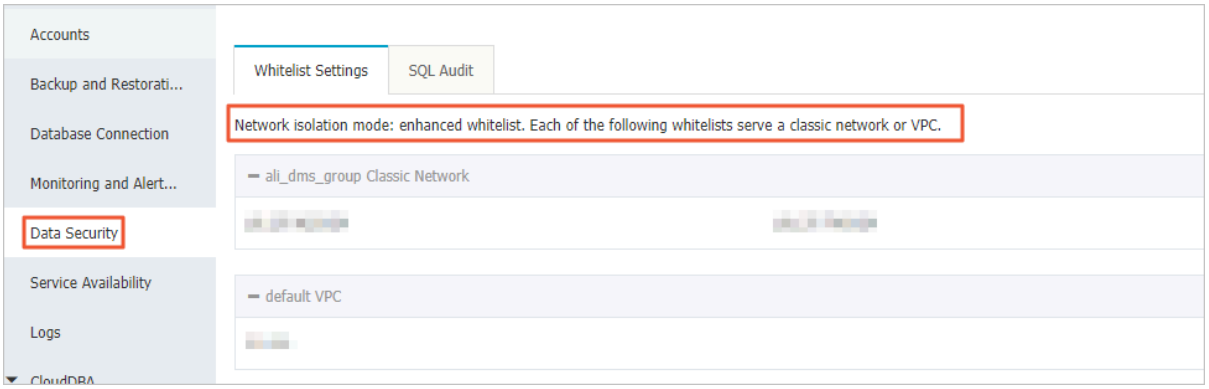
- **Standard whitelist mode**

  In this mode, the IP addresses in the whitelist do not distinguish between the classic network and VPCs. The IP addresses in the whitelist can access the RDS instance both in the classic network and VPCs. We recommend that you switch from the standard whitelist to the enhanced whitelist.



- **Enhanced whitelist mode**

  In this mode, the whitelist is classified into two IP whitelist groups by network type: the classic-network whitelist group and the VPC whitelist group. When you create an IP whitelist, you must specify a network type.



Changes after switching to the enhanced whitelist mode

If your RDS instance is in a VPC, the original IP address whitelists of your RDS instance are replicated to a new IP address whitelist that is suitable to VPC.

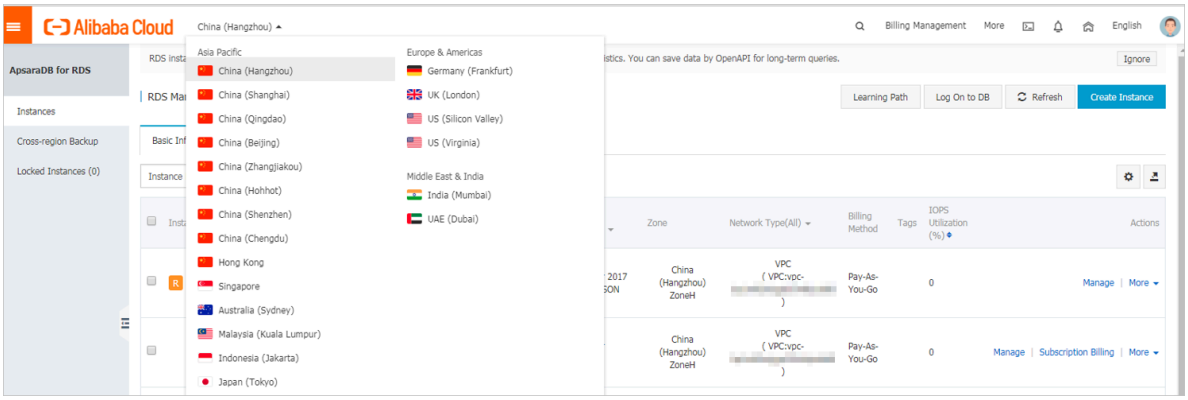
Note:
Switching to the enhanced whitelist mode does not affect the ECS instances that are in the *ECS security group whitelist*.

Precautions

- **You can switch from the standard whitelist to the enhanced whitelist. However, you cannot switch from the enhanced whitelist to the standard whitelist.**
- **In the enhanced mode, the classic-network whitelist group also applies to accesses from a public network. If you want to access the RDS instance from an instance, host, or application in the public network, you must add the public IP address to the classic-network whitelist group.**

Procedure

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



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Data Security.**
5. **On the Whitelist Settings tab, click Switch to Enhanced Whitelist (Recommended).**

6. **In the message box that appears, click OK.**

12 Data backup

12.1 View the quota of free backup space for an RDS for MariaDB instance

This topic describes how to calculate and view the quota of free backup space for an RDS for MariaDB instance. The quota varies depending on the used DB engine version and edition. Additionally, this topic describes how to calculate the backup space beyond the quota.

Backup files occupy backup space. Each RDS instance has a specific quota of free backup space. If the total size of backup files exceeds the quota, additional fees are incurred.

Calculate the quota of free backup space and the backup space beyond the quota

Quota of free backup space = Round up (50% × Storage space purchased for the RDS instance) (Unit: GB)

Backup space beyond the quota = Backup data size + Backup log size - Round up (50 % × Storage space purchased for the RDS instance) (Unit: GB)

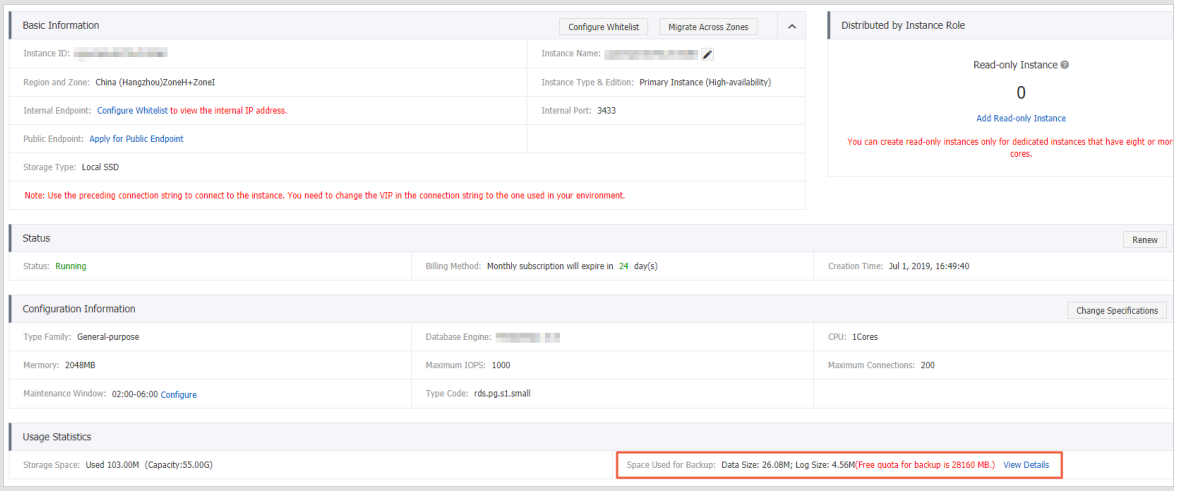
For example, the backup data size is 30 GB, the backup log size is 10 GB, and the storage space is 60 GB, then you must pay for 10-GB storage space every hour:

```
Hourly fees = 30 + 10 - 50% × 60 = 10 (GB)
```

Note:

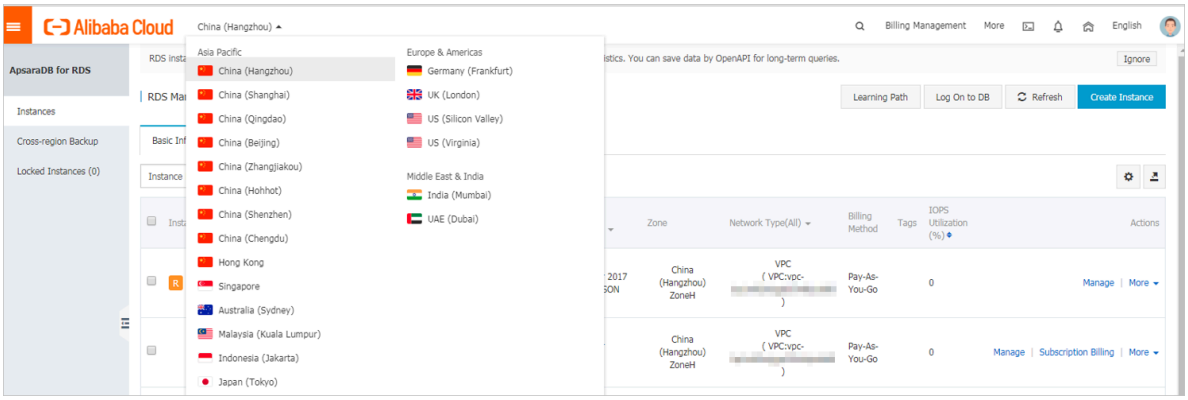
- **For more information about the hourly fees for the backup space beyond the quota, see** *ApsaraDB RDS for MySQL pricing*.

- **The Basic Editions of some DB engines store backup files generated within the last seven days for free. For more information, log on to the RDS console.**



View the quota of free backup space in the RDS console

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



3. **Find the target RDS instance and click its ID.**
4. **In the Usage Statistics section of the Basic Information page, view the data size next to Space Used for Backup. The data size is the quota of free backup space.**

> **Note:**
> **The quota of free backup space varies depending on the instance type. The following figure is only an example.**

12.2 Download the log backup files of an RDS for MariaDB instance

This topic describes how to download the log backup files of an RDS for MariaDB instance. The downloaded log backup files are not encrypted.

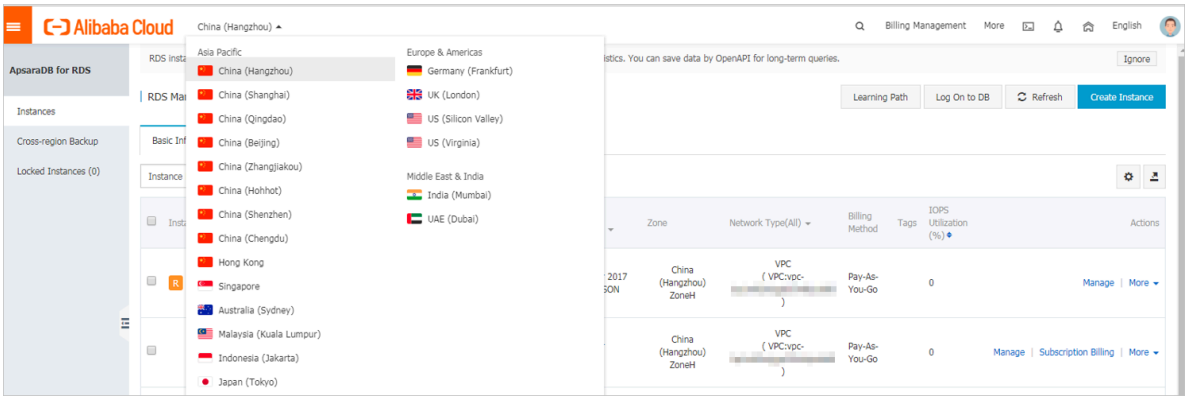
Limits

A RAM user who has only the read-only permissions cannot download backup files. You can add the required permissions to a RAM user in the RAM console. For more information, see *#unique_83*.

DB engine	Data backup download	Log backup download
MariaDB	Not supported. You can only use the restoration function to restore data to a new RDS instance or to the original RDS instance.	Supported.

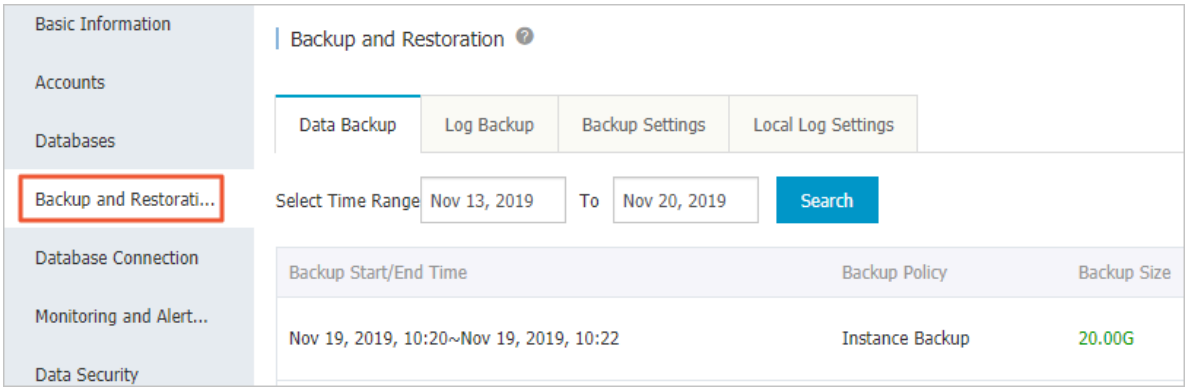
Procedure

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



3. **Find the target RDS instance and click the instance ID.**

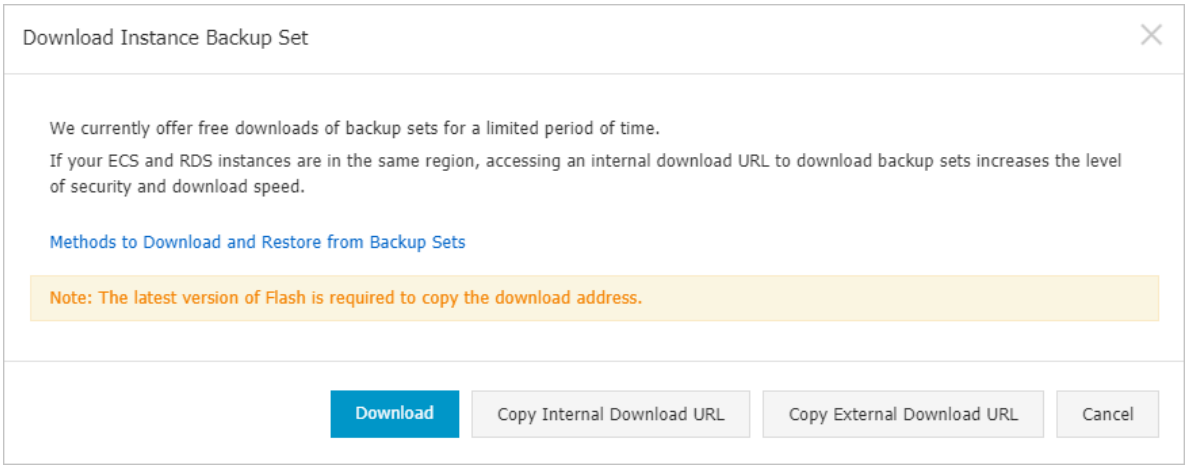
4. In the left-side navigation pane, click Backup and Restoration.



5. On the Log Backup tab, select a time range and click Search. In the log backup file list, find the target log backup file and in the Actions column click Download.

> **Note:**
> If the log backup file is used to restore the RDS instance to an on-premises database, note the following:
>
> - The instance ID of the log backup file must the same as that of the corresponding data backup file.
> - The start time and end time of the log backup file must be later than the selected backup time point and earlier than the time point from which you want to restore data.

6. In the Download Instance Backup Set or Download Binary Log dialog box, select a download method.



Download method	Description
Download	To download the backup file through the public connection address.

Download method	Description
Copy Internal Download URL	To copy the internal download URL only. When your ECS instance is located in the same region as the RDS instance, you can log on to your ECS instance and then use the internal download URL to download the backup file. This is faster and more secure.
Copy External Download URL	To copy the external download URL only. This method is suitable when you download the backup file by using other tools.

Note:

In a Linux operating system, you can run the following command to download a data backup file:

```
wget -c '<Download URL of the log backup file>' -O <User-defined
file name>.tar.gz
```

- **The `-c` parameter is used to enable resumable download.**
- **The `-O` parameter is used to save the downloaded result as a file with the specified name (the file extension is .tar.gz or .xb.gz as included in the URL).**
- **If you enter more than one download URL, then you must include each download URL in a pair of single quotation marks ('). Otherwise, the download fails.**

12.3 Automatically back up the data of an RDS for MariaDB instance

This topic describes how to set backup policies for an RDS for MariaDB instance. The system backs up the instance data according to the backup policies. MariaDB TX does not support manual backup.

Precautions

- **The backup files occupy the backup space of the RDS instance. If the used backup space exceeds the quota of free backup space, additional fees are incurred. For more information, see** *View the quota of free backup space for an RDS for MariaDB instance*.

- For information about the billing method and billable items, see *#unique_15*.
- For information about the pricing of backup space, see *ApsaraDB RDS for MySQL pricing*.
- Do not perform DDL operations during the backup. Otherwise, tables are locked and consequently the backup fails.
- Back up data and logs during off-peak hours.
- If the data volume is large, the backup may take a long time.
- Backup files are retained for a specified time period. Download the backup files to your computer before they are deleted.

Overview

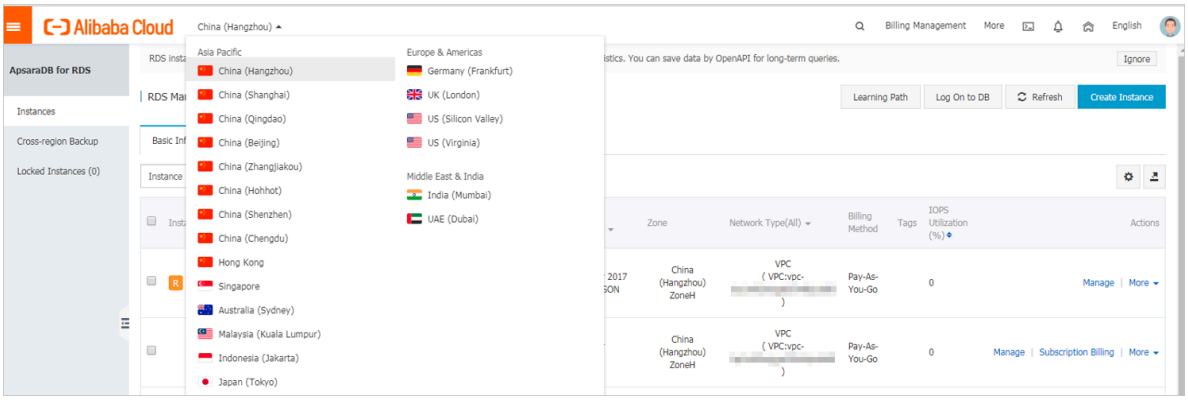
DB engine	Data backup	Log backup
MariaDB	Supports snapshot backup, but does not support physical backup or logical backup.	· Binary log files occupy the disk space of the RDS instance. · When the size of the existing binary log file reaches 500 MB or the duration of data write into the existing binary log file reaches 6 hours, the system starts to write data into a new binary log file. The earlier binary log file then is uploaded asynchronously. · You can uploaded binary log files to buckets in *OSS*. **Note:** You cannot access the buckets for storing the uploaded binary log files in OSS.

Procedure

ApsaraDB for RDS can automatically back up databases according to the backup policy you set.

1. Log on to the *RDS console*.

2. Select the target region.

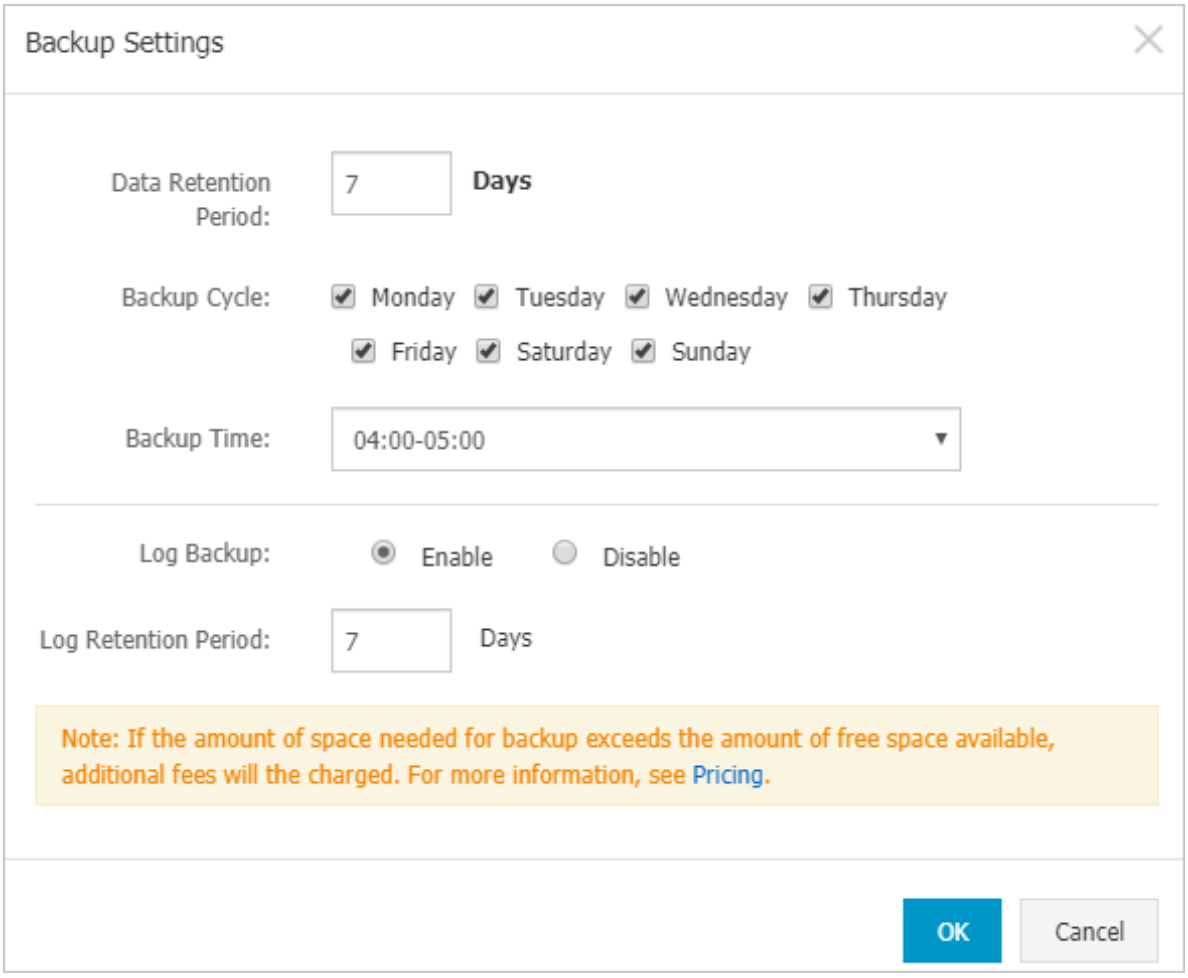


3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Backup and Restoration.
5. On the Backup and Restoration page, click the Backup Settings tab. On the Backup Settings tab, click Edit.
6. In the Backup Settings dialog box, set the backup parameters and click OK. The following table describes the parameters.

Table 12-1: Backup parameters

Parameter	Description
Data Retention Period	The data retention period spans from 7 days to 730 days. The default retention period is 7 days. **Note:** For MySQL 5.7 Basic Edition (with SSDs), the data retention period is 7 days and cannot be changed.
Backup Cycle	Select one or more workdays.
Backup Time	You can select any time period, which is measured in the unit of hour. We recommend that you select a time period during off-peak hours.
Log Backup	The status of the log backup function. **Notice:** If you disable the log backup function, all log backup files are deleted and the time-based data restoration function becomes unavailable.

Parameter	Description
Log Retention Period	· The number of days in which log backup files are retained. The default retention period is 7 days. · The log retention period spans from 7 days to 730 days and must be shorter than or equal to the data retention period. **Note:** For MySQL 5.7 Basic Edition (with SSDs), the log retention period is 7 days and cannot be changed.



FAQ

1. **Can I disable the data backup function for an RDS for MariaDB TX instance?**

   No, the data backup function must be enabled, and the backup file retention period ranges from 7 days to 730 days.

2. **Can I disable the log backup function for an RDS for MariaDB TX instance?**

   Yes, you can disable the log backup function as needed.

APIs

API	Description
#unique_85	**Used to create a backup file for an RDS instance.**
#unique_86	**Used to view the list of backup files for an RDS instance.**
#unique_87	**Used to view the backup settings of an RDS instance.**
#unique_88	**Used to modify the backup settings of an RDS instance.**
#unique_89	**Used to obtain the list of backup tasks for an RDS instance.**
#unique_90	**Used to obtain the log backup files of an RDS instance.**

13 Data restoration

13.1 Restore the data of an RDS for MariaDB instance

This topic describes how to restore the data of an RDS for MariaDB instance by using a data backup.

You can restore the data of an RDS for MariaDB instance by backup set or time. The process is as follows:

1. **Restore data to a new RDS instance.**
2. **Verify data in the new RDS instance.**
3. **Migrate data to the original RDS instance.**

Precautions

- **The whitelist settings, backup settings, and parameter settings of the new RDS instance must be the same as those of the original RDS instance.**
- **The data information of the new RDS instance must be the same as that of the used backup file or that from the specified time point.**
- **The new RDS instance carries the account information in the used backup file or that from the specified time point.**

Fees

For more information, see *ApsaraDB RDS for MySQL pricing*.

Prerequisites

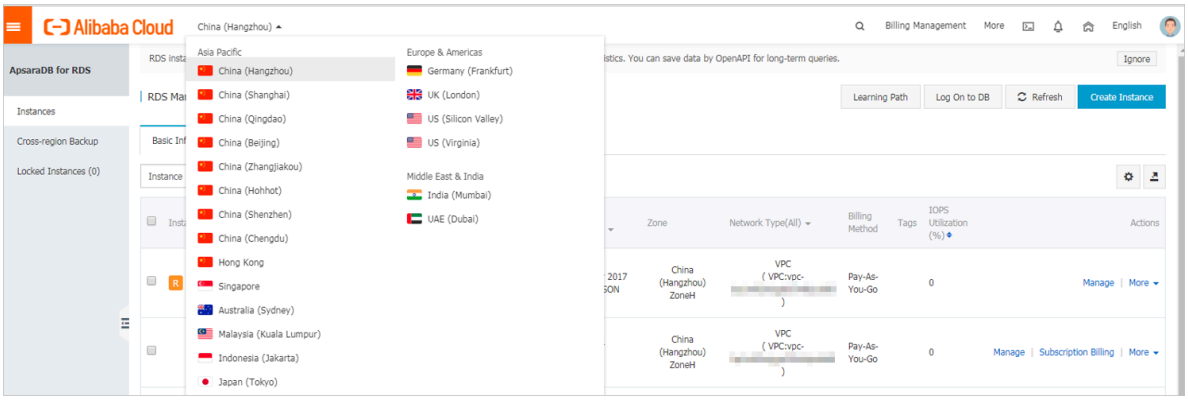
The original RDS instance must meet the following conditions:

- **The instance is in the Running state and is not locked.**
- **No migration task is being performed for the instance.**
- **If you want to restore the data from a time point, the log backup function is enabled.**
- **If you want to restore the data from a backup set, at least one backup set is available for the instance.**

Restore data to a new RDS instance

1. **Log on to the** *RDS console*.

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



3. Find the target RDS instance and click its ID.
4. In the left-side navigation pane, click Backup and Restoration.
5. In the upper-right corner, click Restore Database (Previously Clone Database).
6. On the displayed Restore Database (Previously Clone Instance) page, select a billing method:
   - Pay-As-You-Go: Fees are calculated by hour according to the actual job size. This billing method is suitable to a short-term RDS instance, which can be released immediately after you finish the data restoration.
   - Subscription: Fees are estimated in advance, and the relevant usage allocation is paid for when you create an RDS instance. This billing method is suitable to a long-term RDS instance, which is cheaper than a pay-as-you-go instance. Additionally, a longer duration of purchase indicates a higher discount rate.

> **Note:**
> You can change the billing method of an RDS instance from pay-as-you-go to subscription but not from subscription to pay-as-you-go.

7. Set the parameters of the new RDS instance.

Parameter	Description
Restore Mode	· By Time: You can select any time point within the specified log backup retention period. For more information about how to view or change the log backup retention period, see *Automatically back up the data of an RDS for MariaDB instance*. · By Backup Set **Note:** The By Time option is available only when the log backup function is enabled.
Zone	A zone is a physical area within a region. Different zones in the same region are basically the same. You can create an RDS instance in the same or different zone from the corresponding ECS instance. **Note:** The new RDS instance must be located in the same region as the original RDS instance.

Parameter	Description
CPU and Memory	The type (including the CPU and memory specifications) of the new RDS instance. The CPU, memory, and storage capacity specifications of the new RDS instance must be higher than hose of the original RDS instance. Otherwise, the data restoration may take a long time. Each instance type supports a specific number of CPU cores, memory size, maximum number of connections, and maximum IOPS. For more information, see *#unique_19*. RDS instances fall into the following three type families: · General-purpose instance: A general-purpose instance owns dedicated memory and I/O resources, but shares CPU and storage resources with the other general-purpose instances on the same server. · Dedicated instance: A dedicated instance owns dedicated CPU, memory, storage, and I/O resources. · Dedicated host: A dedicated-host instance owns all the CPU, memory, storage, and I/O resources on the server where it is located. For example, 8 Cores, 32 GB indicates a general-purpose instance, 8 Cores, 32 GB (Dedicated Instance) indicates a dedicated instance, and 30 Cores, 220GB (Dedicated Host)30 Cores, 220 GB (Dedicated Host) indicates a dedicated-host instance.
Capacity	Used for storing data, system files, binlog files, and transaction files.
Network Type	· Classic Network: a classic network. · VPC (recommended): A VPC is an isolated network environment that provides better security and performance than a classic network.

8. Optional. If the new RDS instance uses the subscription billing method, set the Duration and Quantity parameters.
9. Click Buy Now.
10. On the Order Confirmation page, select Terms of Service, Service Level Agreement, and Terms of Use, then click Pay Now to complete the payment.

Verify data in the new RDS instance

For more information, see *#unique_93*.

Migrate data to the original RDS instance

After verifying the data in the new RDS instance, you can migrate the data to the original RDS instance.

Data migration refers to migrating data from one RDS instance (the source RDS instance) to another (the destination RDS instance). The data migration operation does not interrupt the source RDS instance.

Precautions

Do not perform DDL operations during the data migration. Otherwise, the data migration may fail.

Procedure

1. **Log on to the** *DTS console*.
2. **In the left-side navigation pane, click Data Migration.**
3. **In the upper-right corner, click Create Migration Task.**

4. **Enter the migration task name, source database information, and destination database information.**

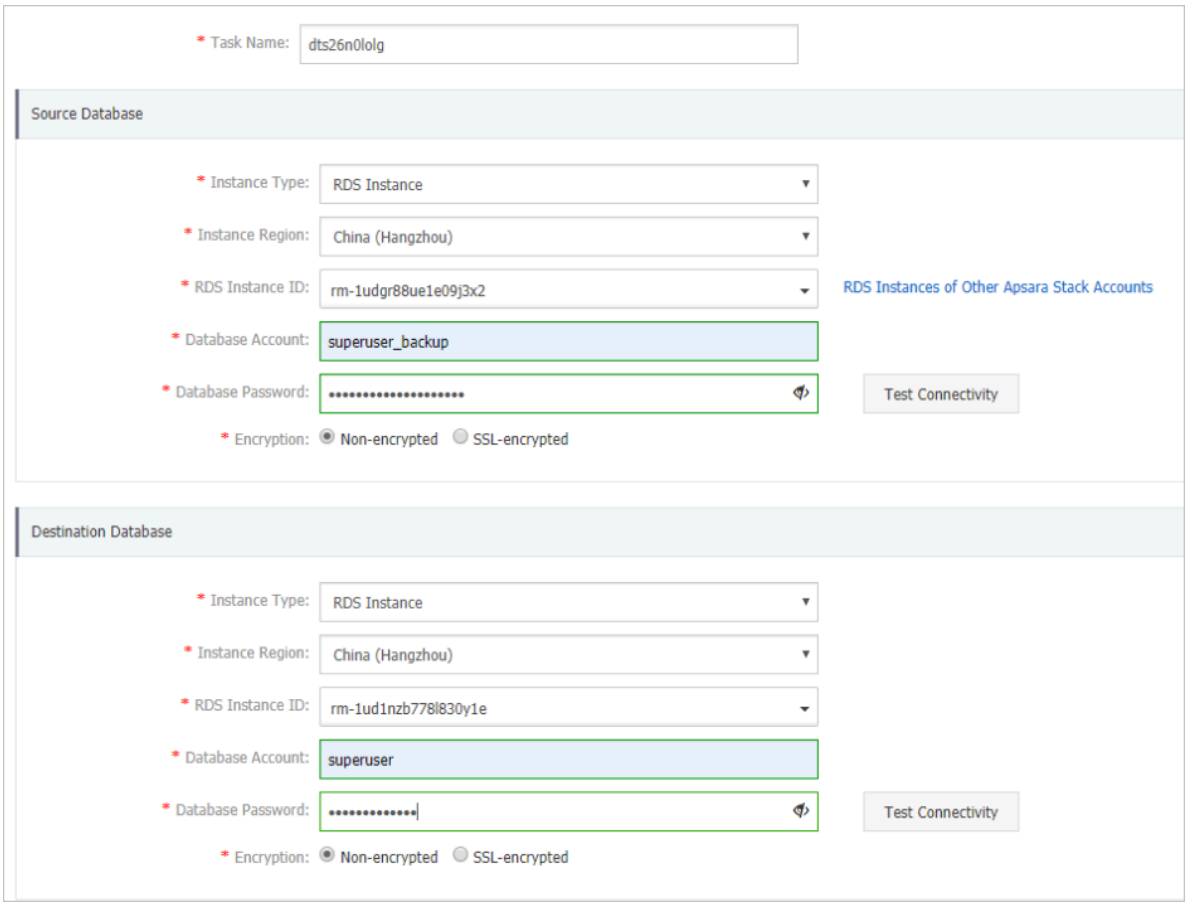
   Parameter description:

   - **Task Name: By default, DTS automatically generates a name for each migration task. You can change the name as needed.**
   - **Source Database**
     - **Instance Type: Select RDS Instance.**
     - **Instance Region: Select the region where the new RDS instance is located.**
     - **RDS Instance ID: Select the ID of the new RDS instance.**
     - **Database Account: Enter the username of the account for the new RDS instance.**
     - **Database Password: Enter the password of the account for the new RDS instance.**
     - **Connection: Select Non-encrypted. If the new RDS instance supports *SSL encryption* and has SSL encryption enabled, then you must select SSL-encrypted.**

     Note:
     The values of the Instance Type and RDS Instance ID parameters determine which of the other parameters are displayed.
   - **Destination Database**
     - **Instance Type: Select RDS Instance.**
     - **Instance Region: Select the region where the original RDS instance is located.**
     - **RDS Instance ID: Select the ID of the original RDS instance.**
     - **Database Account: Enter the username of the account for the original RDS instance.**
     - **Database Password: Enter the password of the account for the original RDS instance.**
     - **Connection: Select Non-encrypted. If the original RDS supports *SSL encryption* and has SSL encryption enabled, then you must selectSSL-encrypted.**

     Note:

The values of the Instance Type and RDS Instance ID parameters determine which of the other parameters are displayed.



5. **Click Set Whitelist and Next.**
6. **Select Schema Migration and Full Data Migration next to Migration Types.**
7. **In the Available section, select the objects you want to migrate. Then click > to move the selected objects to the Selected section.**

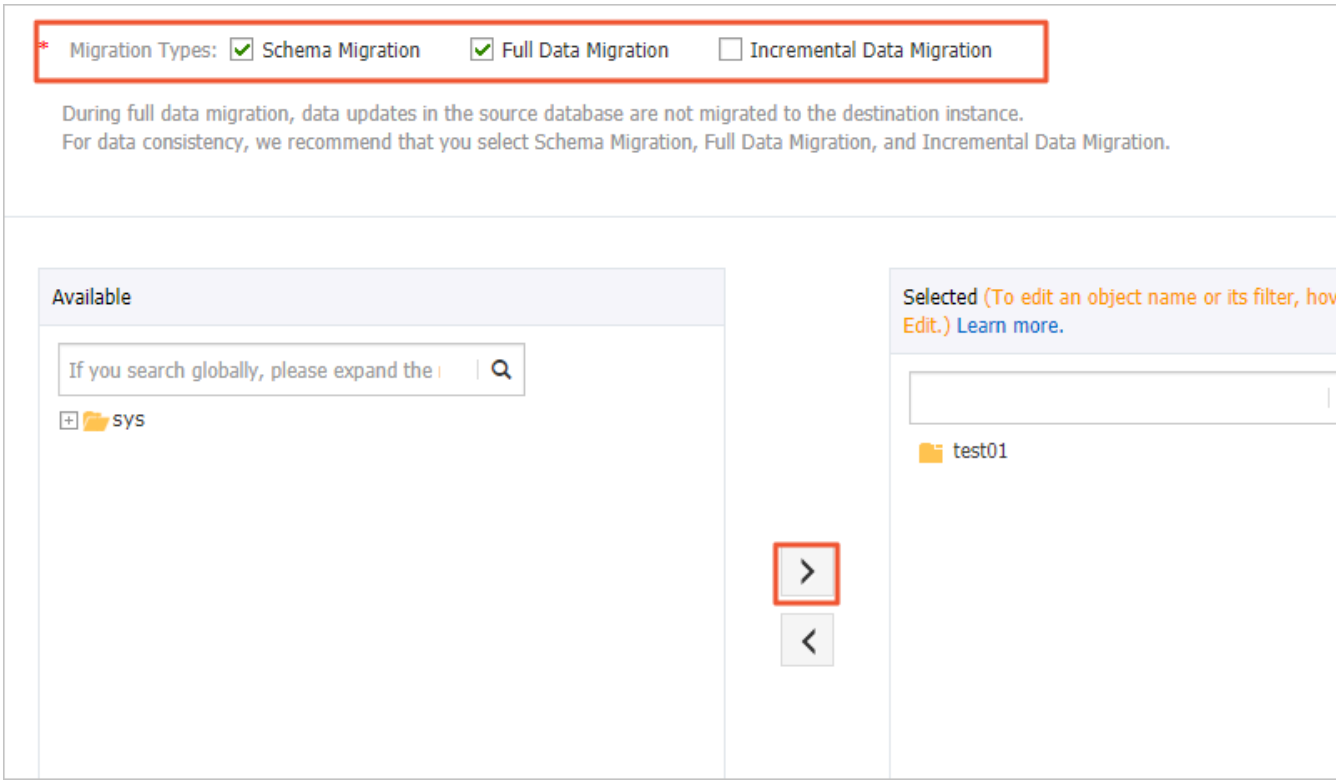
Note:

DTS checks for objects that have the same name. If the destination RDS instance has an object whose name is the same as the name of an object to be migrated, the data migration fails.

In such case, take one of the following two operations:

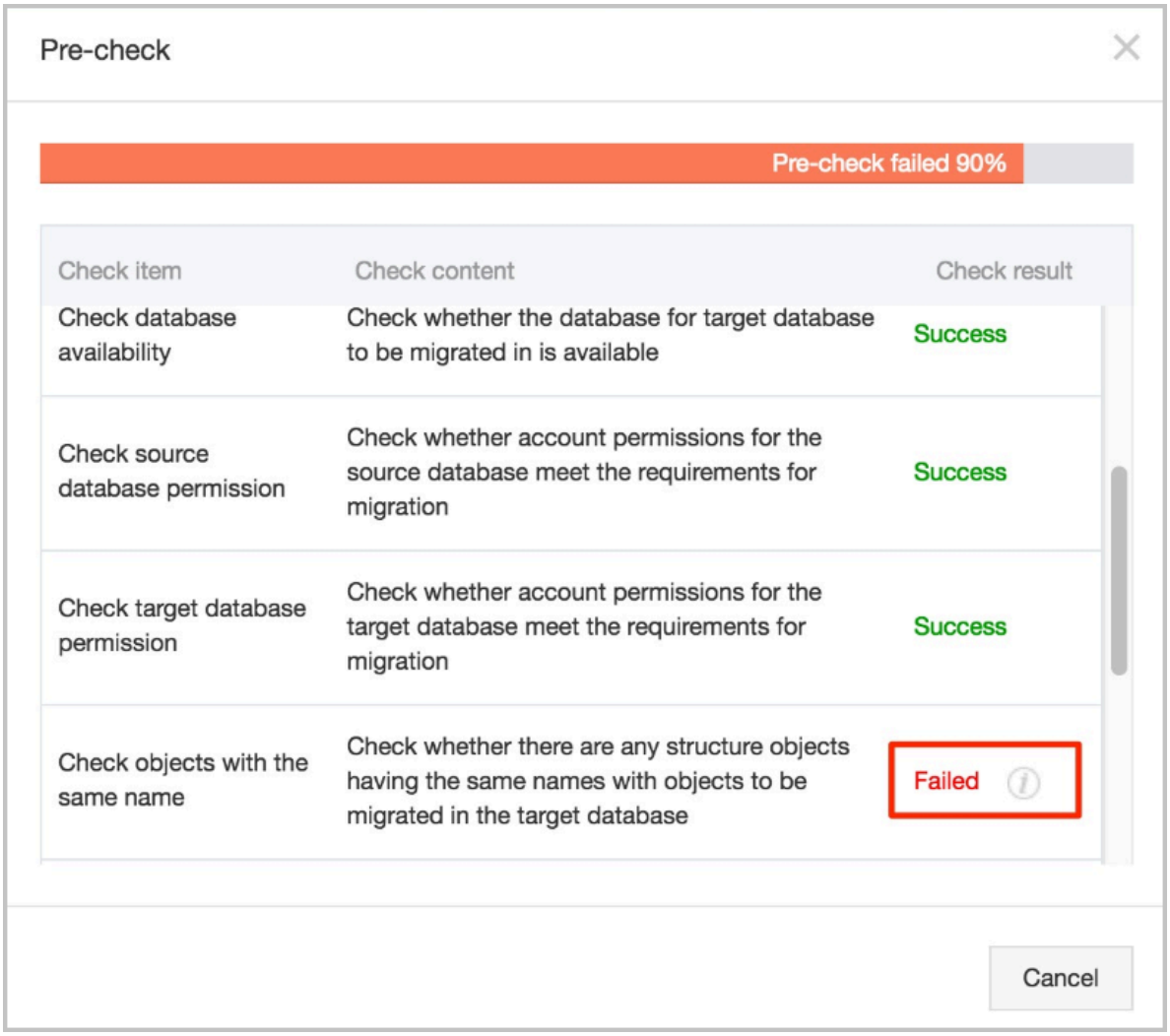
- **In the Selected section, move the pointer over the object whose name you want to change, click Edit, and in the displayed dialog box enter the new object name.**

- **Rename the object in the destination RDS instance.**

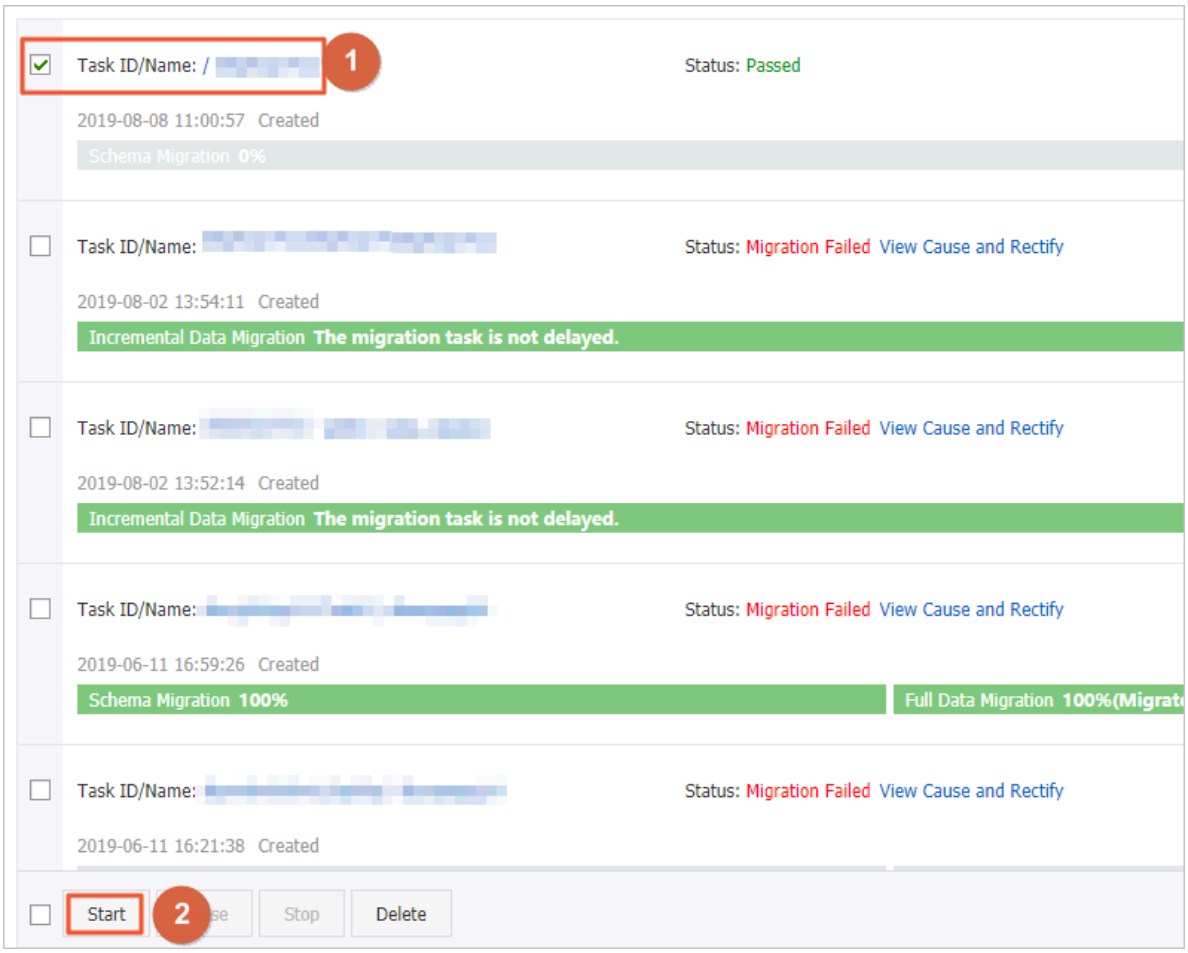


8. **Click Precheck.**

9. **Optional. If the migration task fails the precheck, click ⓘ next to the check item whose Result is Failed, and resolve the problem according to the failure information.**



10. On the page that displays migration tasks, select the migration task you created, then click Start.



11. When the migration task passes the precheck, click Next.

12. In the Confirm Settings dialog box, confirm the configuration, select Data Transmission Service (Pay-As-You-Go) Service Terms, and click Buy and Start.

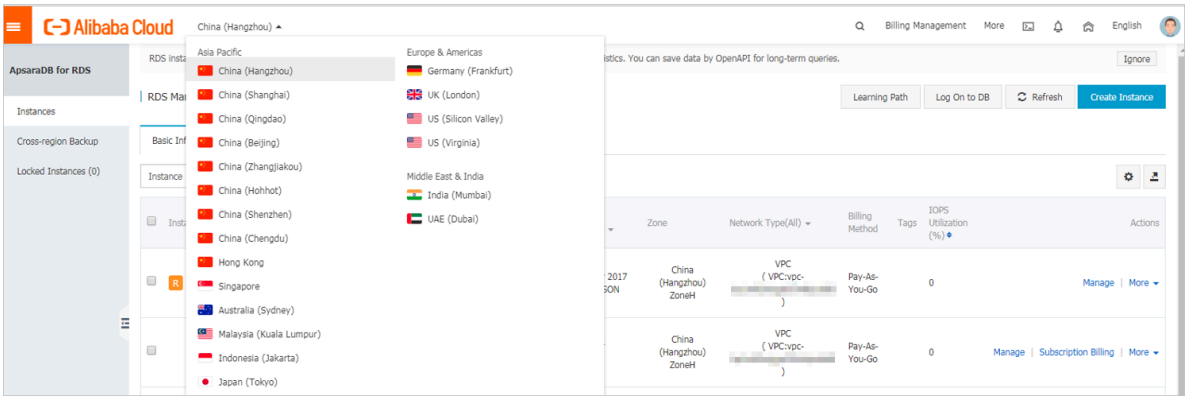
14 Manage logs

This topic describes how to manage the logs of an RDS for MariaDB instance in the RDS console.

- **For information about log backup policies and rules, see** *Automatically back up the data of an RDS for MariaDB instance*.
- **For information about how to download log backup files, see** *Download the log backup files of an RDS for MariaDB instance*.
- **For information about how to restore data through log backup files, see** *Restore the data of an RDS for MariaDB instance*.

View logs

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



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Log Management.**
5. **On the Log Management page, select Error Log, Slow Query Log, Slow Query Log Summary, or Primary/Secondary Instance Switch Log, select a time range, and click Search.**

Query item	Description
Error Log	Records the SQL statements that are failed to be executed within the last one month.

Query item	Description
Slow Query Log	Records the SQL statements that lasted for more than 1 second within the last one month. (You can reconfigure the `long_query_time` parameter to change this time threshold according to *Reconfigure parameters for an RDS for MariaDB instance*.) Similar SQL statements are displayed once only.
Slow Query Log Summary	Provides statistics and analysis reports for SQL statements that lasted for more than 1 second within the last one month. (You can reconfigure the `long_query_time` parameter to change this time threshold according to *Reconfigure parameters for an RDS for MariaDB instance*.)
Primary/ Secondary Instance Switch Log	Records logs related to the switchovers between the master and slave instances within the last one month.

15 Tag

15.1 Create tags

This topic describes how to create tags for one or more RDS instances. If you have a large number of RDS instances, you can create tags and then bind the tags to the instances so that you can classify and better manage the instances. Each tag consists of a key and a value.

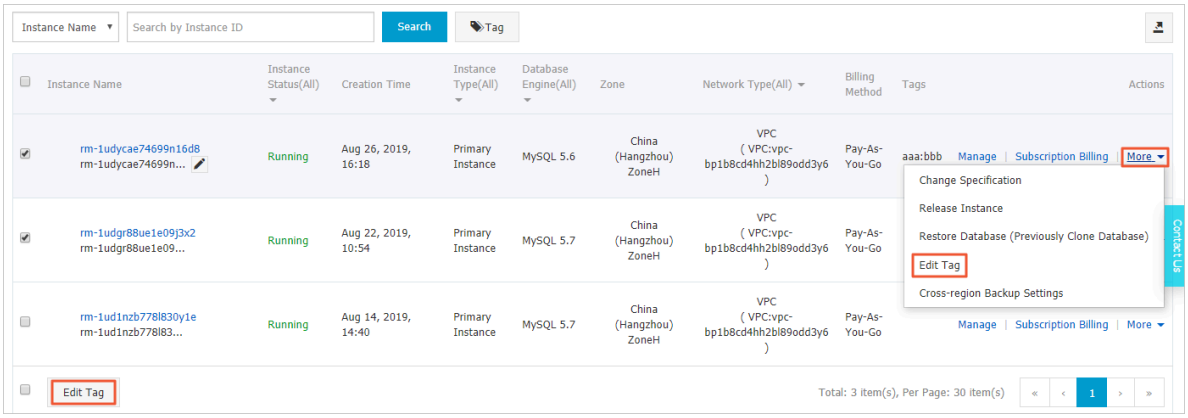
Limits

- **Up to 10 tags can be bound to each RDS instance, and each tag must have a unique key. Tags with the same key are overwritten.**
- **You can bind up to five tags at a time.**
- **Tag information is independent in different regions.**
- **After you unbind a tag from an RDS instance, the tag is deleted if it is not bound to any other RDS instance.**

Procedure

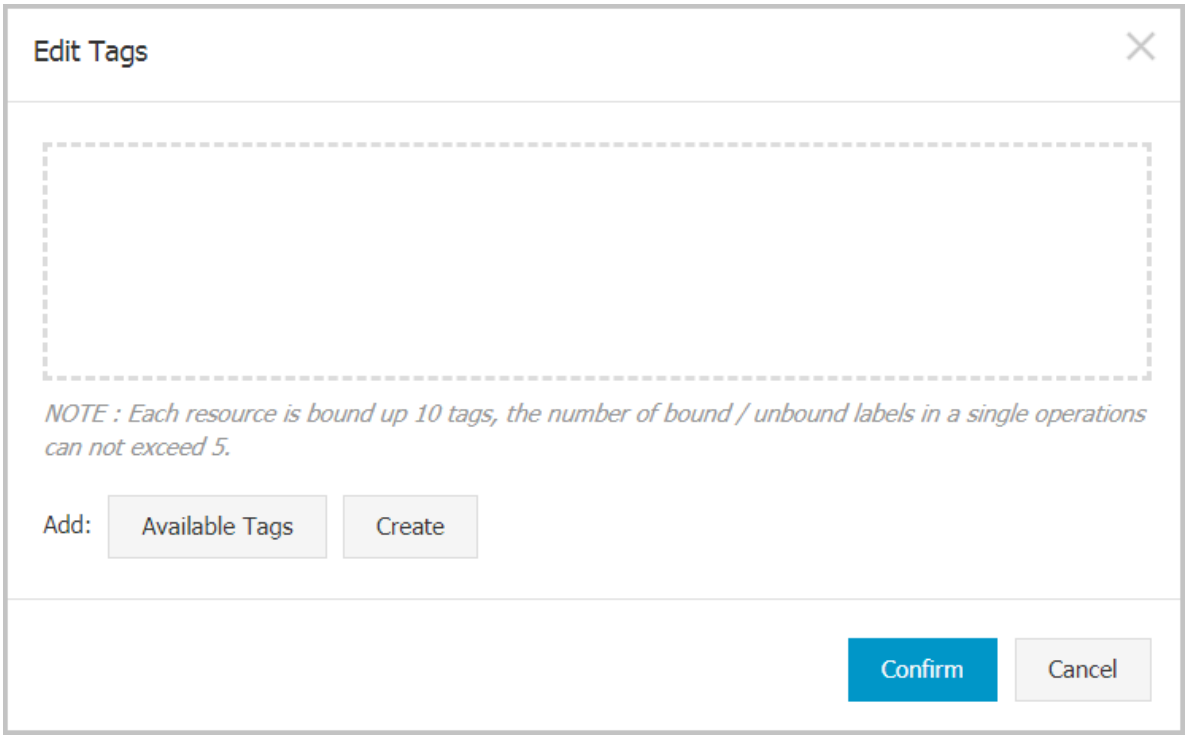
1. **Log on to the *RDS console* and in the left-side navigation pane, click Instances.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**

3. Specify the method of adding tags.
   - If you want to add tags to only one RDS instance, find the RDS instance and in the Actions column choose More > Edit Tag.
   - If you want to add tags to more than one RDS instance, select the RDS instances and click Edit Tag



4. Click Add, enter the Key and Value, and click Confirm.

> **Note:**
> If you have already created tags, you can click Available Tags and select an existing tag.



5. After you add all the tags you need, click Confirm.

APIs

API	Description
AddTagsToResource	Used to bind a tag to RDS instances.

15.2 Delete tags

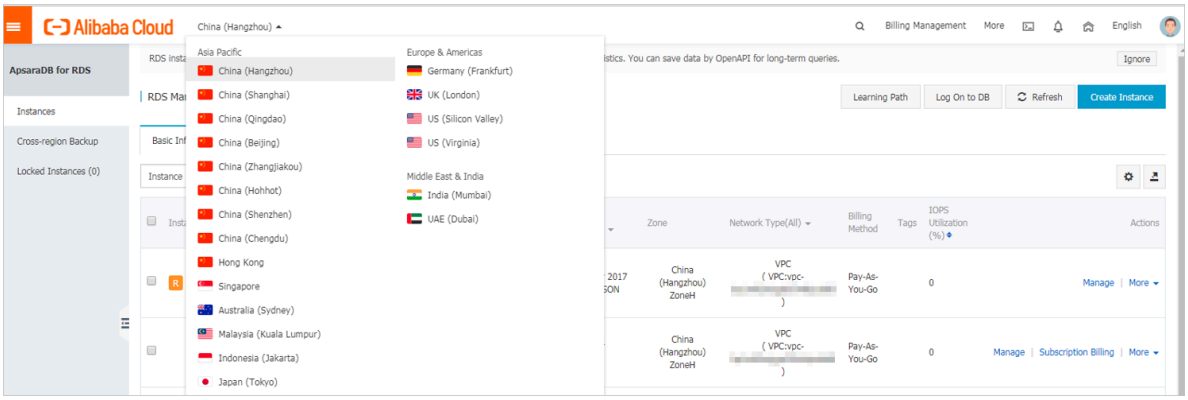
This topic describes how to delete tags from an RDS instance when you no longer need the tags or due to adjustments to the instance.

Limits

After you unbind a tag from an RDS instance, the tag is deleted if it is not bound to any other instance.

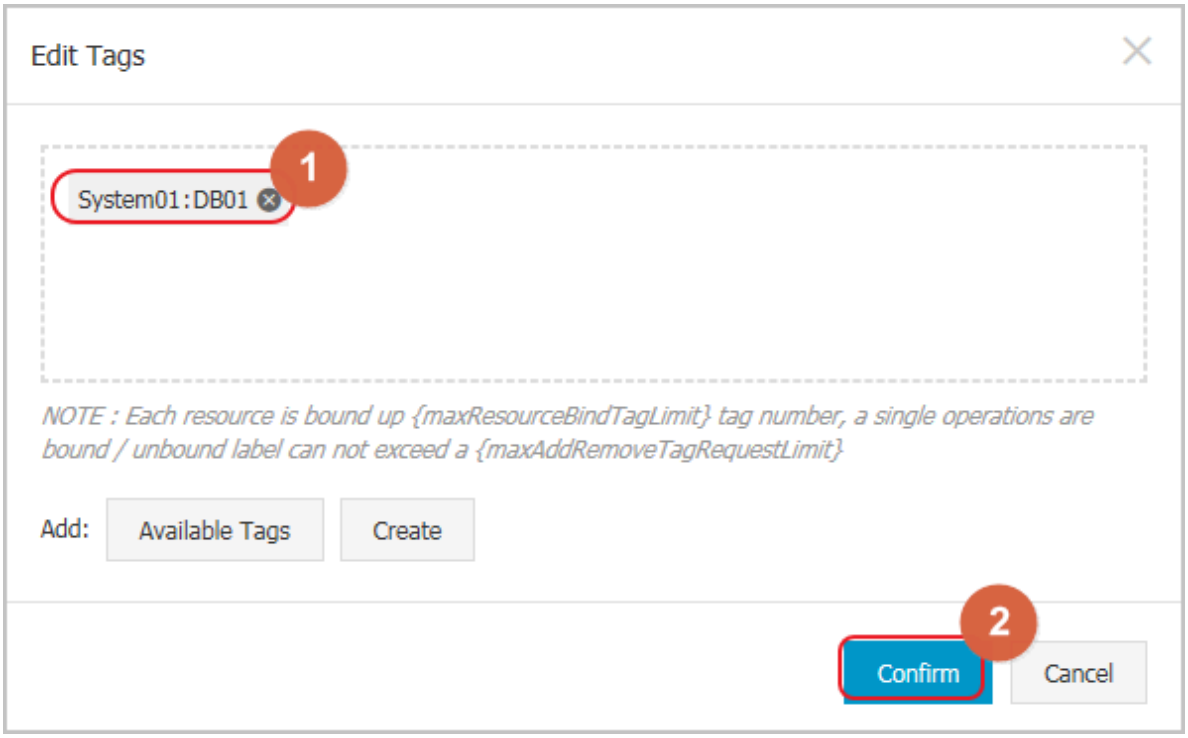
Procedure

1. **Log on to the *RDS console* and in the left-side navigation pane, click Instances.**
2. **In tne upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance and in the Actions column, choose More > Edit Tag.**

4. **Find the tag you want to delete, and click the X button following the tag.**



5. **Click Confirm.**

APIs

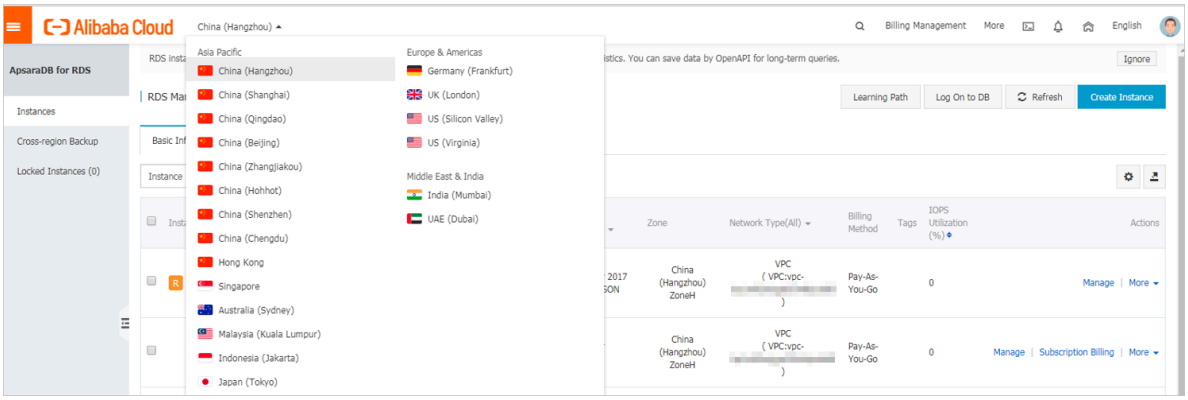
API	Description
#unique_100	**Used to unbind a tag from an RDS instance.**

15.3 Filter RDS instances by tag

This topic describes how to filter RDS instances by tag.

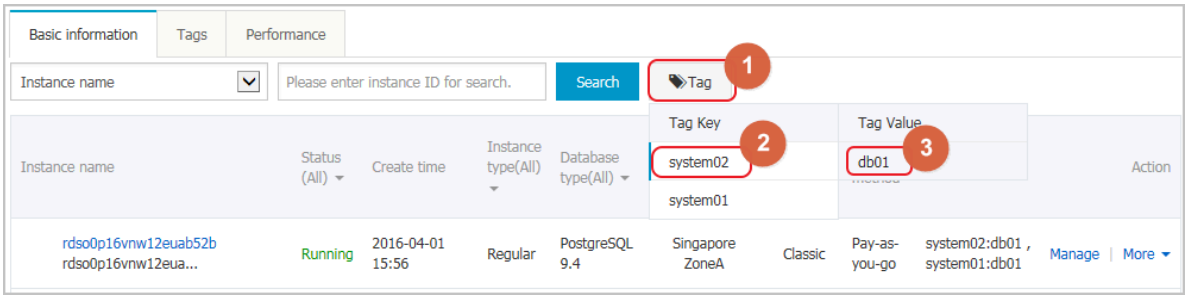
1. **Log on to the** *RDS console*.

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



3. On the Basic Information tab, click the Tag button next to Search and select a tag key and a tag value.

> **Note:**
> You can click the X button following the tag key to cancel the filter operation.



APIs

API	Description
DescribeTags	Used to query tags.