

Alibaba Cloud ApsaraDB for MySQL

Quick Start for MySQL

Issue: 20190828

Legal disclaimer

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

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

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

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

Generic conventions

Table -1: Style conventions

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

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

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Limits.....	1
2 General process.....	3
3 Create an RDS for MySQL instance.....	4
4 Initial configuration.....	8
4.1 Configure a whitelist.....	8
4.2 Apply for an Internet address.....	16
4.3 Create accounts and databases.....	19
5 Connect to an RDS for MySQL instance.....	28
6 Scale instances.....	33
6.1 Read-only instance.....	33
6.1.1 Introduction to MySQL read-only instances.....	33
6.1.2 Create an RDS for MySQL read-only instance.....	35

1 Limits

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

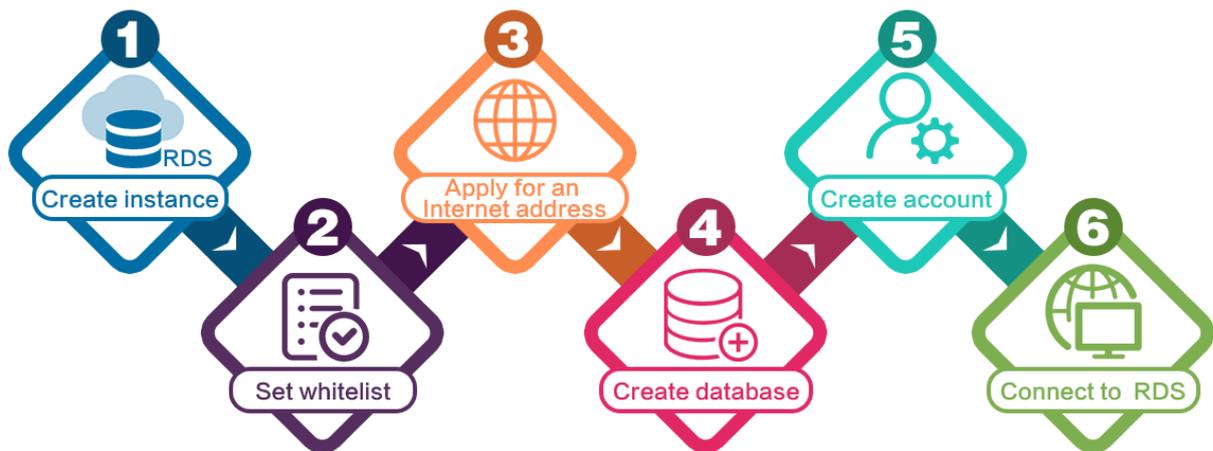
Items	Restrictions
Parameter modification	The RDS console or APIs must be used to modify database parameters. But some parameters cannot be modified. For more information, see #unique_4 .
Root permission	The root or sa permission is not provided.
Backup	<ul style="list-style-type: none"> Command lines or graphical interfaces can be used for logical backup. For physical backup, the RDS console or APIs must be used.
Restoration	<ul style="list-style-type: none"> Command lines or graphical interfaces can be used for logical restoration. For physical restoration, the RDS console or APIs must be used.
Migration	<ul style="list-style-type: none"> Command lines or graphical interfaces can be used for logical import. You can use the MySQL command line tool or Data Transmission Service (DTS) to migrate data.
MySQL storage engine	<ul style="list-style-type: none"> Currently only InnoDB and TokuDB are supported. The MyISAM engine has defects and may cause data loss. If you create MyISAM engine tables, they are automatically converted to InnoDB engine tables. For more information, see Why does RDS for MySQL not support the MyISAM engine? The InnoDB storage engine is recommended for performance and security requirements. The Memory engine is not supported. If you create Memory engine tables, they are automatically converted to InnoDB engine tables.
Replication	MySQL provides a dual-node cluster based on the master/slave replication architecture, so you manual deployment is not required . The slave instance in the architecture is invisible to you, and your application cannot access to the slave instance directly.
Restarting RDS instances	Instances must be restarted through the RDS console or APIs.

Items	Restrictions
User, password, and database management	By default, RDS console is used to manage users, passwords, and databases, including operations such as instance creation, instance deletion, permission modification, and password modification. MySQL also allows you to create a master account for finer-grained management.
Common account	<ul style="list-style-type: none">• Does not support customized authorization.• The account management and database management interfaces are provided on the RDS console.• Instances that support common accounts also support master accounts.
Master account	<ul style="list-style-type: none">• Support customized authorization.• SQL statements can be used for management.
Network settings	If a MySQL 5.5/5.6 instance is in a classic network and its access mode is safe connection mode, do not enable <code>net.ipv4.tcp_timestamps</code> in SNAT mode.

2 General process

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

Quick Start flowchart



1. [#unique_7](#)
2. [#unique_8](#)
3. [#unique_9](#)
4. [#unique_10](#)
5. [#unique_11](#)

3 Create an RDS for MySQL instance

You can use the RDS console or APIs to create an RDS for MySQL instance. For more information about instance pricing, see [#unique_13](#). This topic describes how to use the RDS console to create an instance. To use APIs to create an RDS for MySQL instance, see [CreateDBInstance](#).

Prerequisites

You have registered an Alibaba Cloud account.

Precautions

- Subscription instances cannot be converted to Pay-As-You-Go instances.
- Pay-As-You-Go instances can be converted to Subscription instances. For operation instructions, see [#unique_15](#).
- An Alibaba Cloud account can create up to 30 Pay-As-You-Go RDS instances. You can open a ticket to apply for increasing the limit.

Procedure

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

4. Set the following parameters.

Parameter	Description
Region	<p>Indicates the location of the RDS instance you want to purchase. You cannot change the region once you confirm your order.</p> <ul style="list-style-type: none"> • Select the region closest to your users to increase the access speed. • Select the region where your ECS instance is located so that the ECS instance can access the RDS instance through the intranet. If the ECS instance and RDS instance are located in different regions, they can communicate only through the Internet and hence performance is degraded.
Database Engine	<p>The supported database engines are MySQL, Microsoft SQL Server, PostgreSQL, PPAS (compatible with Oracle), and MariaDB TX.</p> <p>In this example, select MySQL.</p> <div style="background-color: #f0f0f0; padding: 5px;">  Note: The available database engines vary depending on the region you select. </div>
Version	<p>For RDS for MySQL, the supported versions are MySQL 5.5, 5.6, 5.7, and 8.0.</p> <div style="background-color: #f0f0f0; padding: 5px;">  Note: The available versions vary depending on the region you select. </div>
Edition	<ul style="list-style-type: none"> • Basic: This edition provides a single node and separates computing from storage. It is extremely cost-effective. • High-availability: This edition adopts the high-availability architecture with one master node and one slave node. It is applicable to over 80% of scenarios. <div style="background-color: #f0f0f0; padding: 5px;">  Note: The available product series vary depending on the region you select. For more information on the product series, see #unique_16. </div>

Parameter	Description
Zone	<p>A zone is a physical area within a region. Different zones in the same region are basically the same.</p> <p>You can deploy the master and slave nodes of your RDS instance in the same zone or in different zones.</p>
Network Type	<ul style="list-style-type: none"> • 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. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  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. </div>
Type	<p>Indicates the specifications of the RDS instance. Each instance type supports a specific number of CPU cores, memory size, maximum number of connections, and maximum IOPS. For more information, see #unique_17.</p> <p>RDS for MySQL supports the following instance type families:</p> <ul style="list-style-type: none"> • 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: owns dedicated CPU, memory, storage, and I/O resources. • Dedicated host: owns all the CPU, memory, storage, and I/O resources on the server where it is located. <p>For example, 8 Cores 32 GB (Basic) indicates a general-purpose instance, and 8 Cores 32 GB (Dedicated) indicates a dedicated instance.</p>
Capacity	<p>Used for storing data, system files, binlog files, and transaction files.</p>

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



Note:

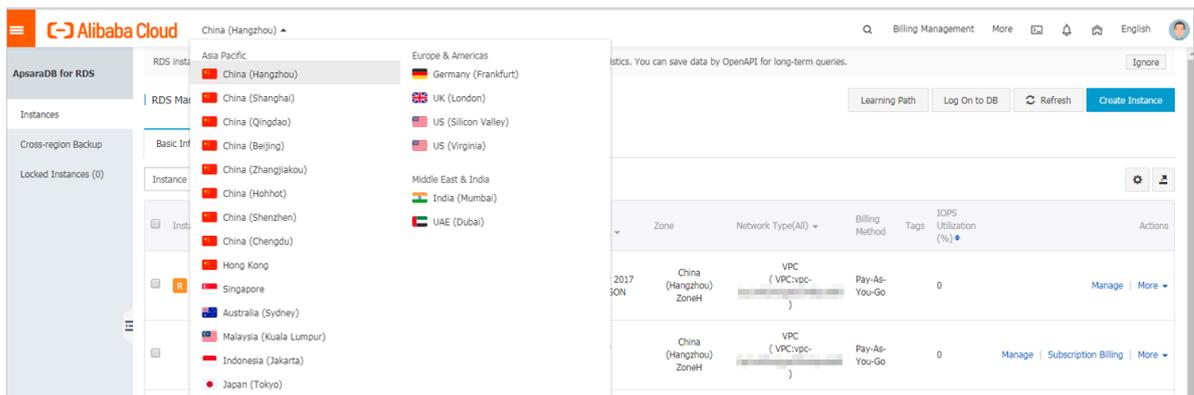
For a Subscription instance, you can:

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

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

What to do next

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



2. [#unique_8](#).
3. [Create accounts](#).
4. [#unique_9](#) (if you want to access the RDS instance through the Internet).
5. [Connect to the RDS instance](#).

FAQ

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

See [Manage RDS permissions by using RAM](#).

APIs

API	Description
#unique_18	Used to create an RDS instance.

4 Initial configuration

4.1 Configure a whitelist

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

To configure a whitelist, follow these steps:

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

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

Configure an IP address whitelist

Precautions

- The default IP whitelist can only be edited or cleared, but cannot be deleted.
- If you log on to DMS but the DMS server IP address has not been added to the whitelist, DMS prompts you to add the IP address and automatically generates a whitelist containing the IP address.
- You must confirm which network isolation mode your RDS instance is in before configuring the whitelist. See the corresponding operations based on the network isolation mode.





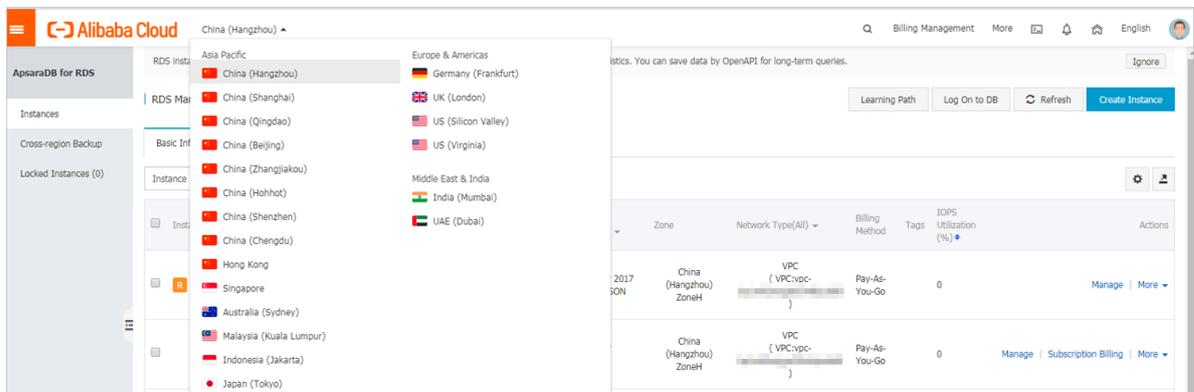
Note:

The private networks to which RDS instances belong are divided into two types: Classic Network and VPC.

- **Classic network:** Alibaba Cloud automatically allocates IP addresses. Users only need to perform simple configurations. This network type is suitable for new users.
- **VPC:** You can customize the network topology and IP addresses. It supports leased line connection, and is suitable for advanced users.

If the network isolation mode is enhanced whitelist mode

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



3. Find the target instance and click its ID.
4. In the left-side navigation pane, click Data Security.

5. On the Whitelist Settings tab page, follow these instructions based on your scenario:

- To access the RDS instance from an ECS instance located within a VPC, click Edit for default VPC whitelist.
- To access the RDS instance from an ECS instance located within the classic network, click Edit for the default Classic Network whitelist.
- To access the RDS instance from a server or computer located in a public network, click Edit for the default Classic Network whitelist.



Note:

- To allow ECS to access RDS through the intranet (VPC or classic network), 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 to create a new whitelist. In the displayed Create Whitelist dialog box, select a network type: VPC or Classic Network/Public IP.

The screenshot shows the 'Whitelist Settings' page in the ApsaraDB for MySQL console. The page is divided into several sections: 'Basic Information', 'Accounts', 'Databases', 'Database Connection', 'Database Proxy', 'Monitoring and Alert...', 'Data Security', 'Service Availability', 'Logs', 'SQL Explorer', 'Backup and Restorati...', and 'Parameters'. The 'Data Security' section is expanded, showing 'Whitelist Settings', 'SQL Audit', and 'SSL Encryption'. The 'Whitelist Settings' section displays the network isolation mode as 'enhanced whitelist' and lists the following whitelists: 'Default Classic Network' (highlighted with a red box) and '127.0.0.1'. A 'Create Whitelist' button is visible in the top right corner. The 'Security Group' section is also visible, showing a 'Security Group' entry with an 'Add Security Group' button.

6. In the displayed Edit Whitelist dialog box, add the IP addresses that need to access the instance, and then click OK.

- If you add an IP address range, such as 10.10.10.0/24, any IP address in the 10.10.10.X format can access the RDS instance.
- To add multiple IP addresses or IP address ranges, separate them with a comma (without spaces), for example, 192.168.0.1,172.16.213.9.
- You can click Add Internal IP Addresses of ECS Instances to display the IP addresses of all the ECS instances under your Alibaba Cloud account, and add to the whitelist.



Note:

After you add any IP address to the default whitelist, the default IP address 127.0.0.1 is automatically removed.

Edit Whitelist

Network Type: VPC Classic Network/Public IP

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

Whitelist Name*: default

Whitelist*: 127.0.0.1

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

You can add 999 more entries.

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

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

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

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

New whitelist entries take effect in 1 minute.

OK Cancel

If the network isolation mode is standard whitelist mode

1. Log on to the [RDS console](#).
2. In the upper-left corner of the page, 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 for the default whitelist.



Note:

You can also click Create Whitelist to create another whitelist.



6. In the displayed Edit Whitelist dialog box, add the IP addresses that need to access the instance, and then click OK.

- If you add an IP address range, such as 10.10.10.0/24, any IP address in the 10.10.10.X format can access the RDS instance.
- To add multiple IP addresses or IP address ranges, separate them with a comma (without spaces), for example, 192.168.0.1,172.16.213.9.
- You can click Add Internal IP Addresses of ECS Instances to display the IP addresses of all the ECS instances under your Alibaba Cloud account, and add to the whitelist.



Note:

After you add any IP address to the default whitelist, the default address 127.0.0.1 is automatically removed.

Edit Whitelist ✕

Network Type: VPC Classic Network/Public IP

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

Whitelist Name*: default

Whitelist*: 127.0.0.1

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

You can add 999 more entries.

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

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

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

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

New whitelist entries take effect in 1 minute.

OK Cancel

Common incorrect settings

- If the IP address whitelist contains only the default address 127.0.0.1, 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 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 the [enhanced whitelist](#) mode is enabled, check the following:
 - To connect to the RDS instance through the VPC address of the RDS instance, make sure that the private IP address of the ECS instance is added to the default VPC whitelist.
 - To connect to the RDS instance through the classic network address of the RDS instance, make sure that the private IP address of the ECS instance is added to the default Classic Network whitelist.
 - To connect to the RDS instance through [ClassicLink](#), make sure that the private IP address of the ECS instance is added to the default VPC whitelist.
 - To connect to the RDS instance through the public address of the RDS instance, make sure that the public IP address of the device is added to the default Classic Network whitelist.
- The public IP address that you add to the whitelist may not be the real outbound IP address. The reasons are as follows:
 - The public IP address is not fixed and may dynamically change.
 - The tools or websites used to query the public IP addresses may provide wrong IP addresses.

For more information, see [#unique_23](#).

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 the 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

- RDS versions that support an ECS security group are MySQL 5.6 and 5.7.
- You can configure both the IP address whitelists and an ECS security group. The IP addresses in the whitelists 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 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.



Note:

Security groups with a VPC tag are within VPCs.

6. Select a security group and click OK.

APIs

API	Description
#unique_24	Used to view the IP address whitelist of an RDS instance.
#unique_25	Used to modify the IP address whitelist of an RDS instance.

4.2 Apply for an Internet address

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

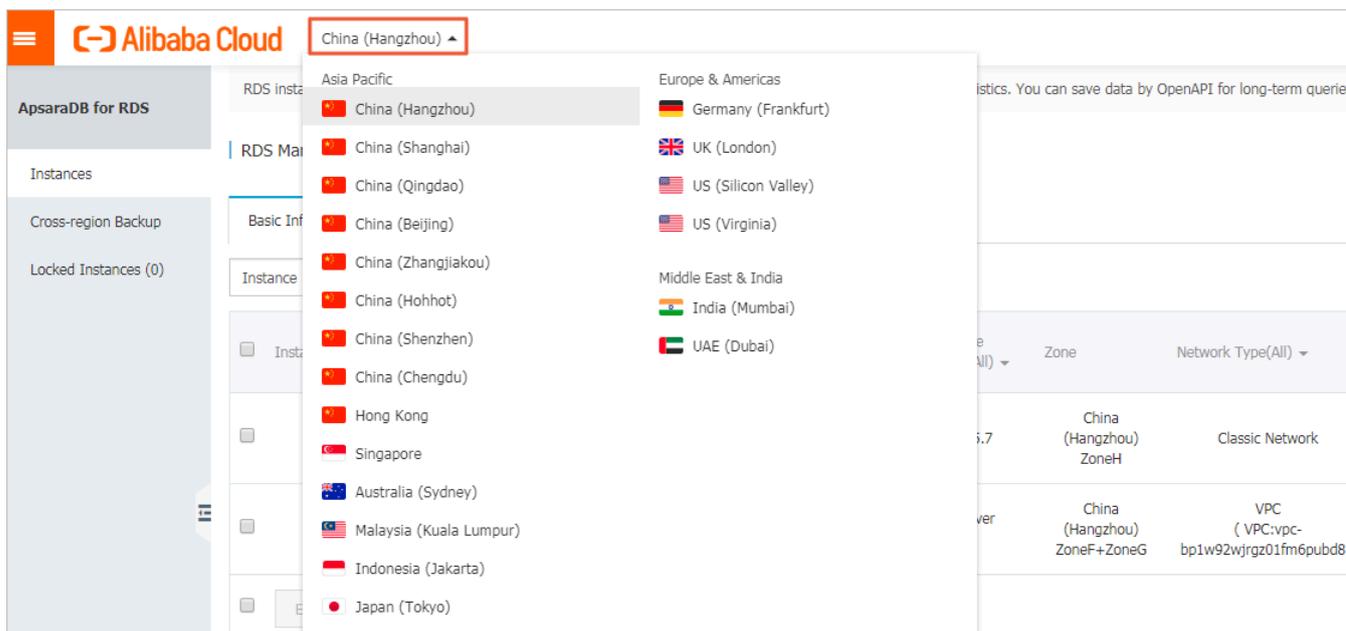
Intranet and Internet addresses

Address Type	Description
Intranet address	<p>The intranet address is generated by default.</p> <p>Use the intranet address if all of the following conditions are met:</p> <ul style="list-style-type: none"> · 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. <p>The intranet address is recommended because accessing RDS through the intranet is most secure and delivers optimal performance.</p>

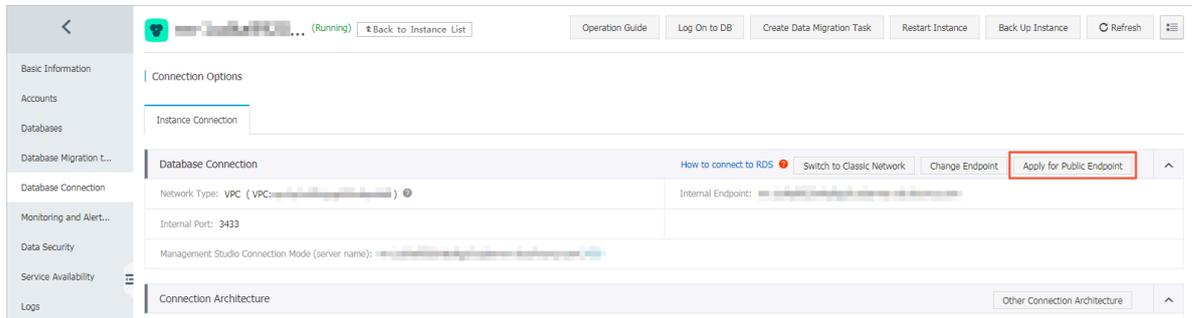
Address Type	Description
Internet address	<p>You need to manually apply for the Internet address. You can also release it anytime.</p> <p>Use the Internet address if you cannot access RDS through the intranet. Specific scenarios are as follows:</p> <ul style="list-style-type: none"> · An ECS instance 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. <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p> Note:</p> <ul style="list-style-type: none"> · The Internet address and traffic are currently free of charge. · Using the Internet address reduces security. Please exercise caution. · To ensure high security and performance, we recommend that you migrate your application to an ECS instance that is in the same region and has the same network type as your RDS instance and then use the intranet address. </div>

Apply for an Internet address

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



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



6. In the displayed dialog box, click OK.

The Internet address is generated.

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

- Connection Type: Select Public Endpoint.



Note:

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

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

Change Endpoint
✕

Connection Type: Internal Endpoint ▼

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

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

Port: 3433

Port Range: 1000 to 5999

OK
Cancel

APIs

API	Description
#unique_28	Used to apply for an Internet address.

4.3 Create accounts and databases

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

Account types

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

Account Type	Description
Superuser account	<ul style="list-style-type: none"> Can only be created and managed through the console or API. Each instance can have only one superuser account, which can be used to manage all databases and standard accounts. Has more 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	<ul style="list-style-type: none"> 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.

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

Differences between the superuser account permissions and SUPER permissions

Superuser account permissions

- Can manage all databases and standard accounts. [Account permissions](#) lists the permissions of the superuser account.
- Can terminate the connections established by other accounts.
- Running the `show processlist` command shows only the processes of the current account, excluding processes on the control level.

SUPER permissions

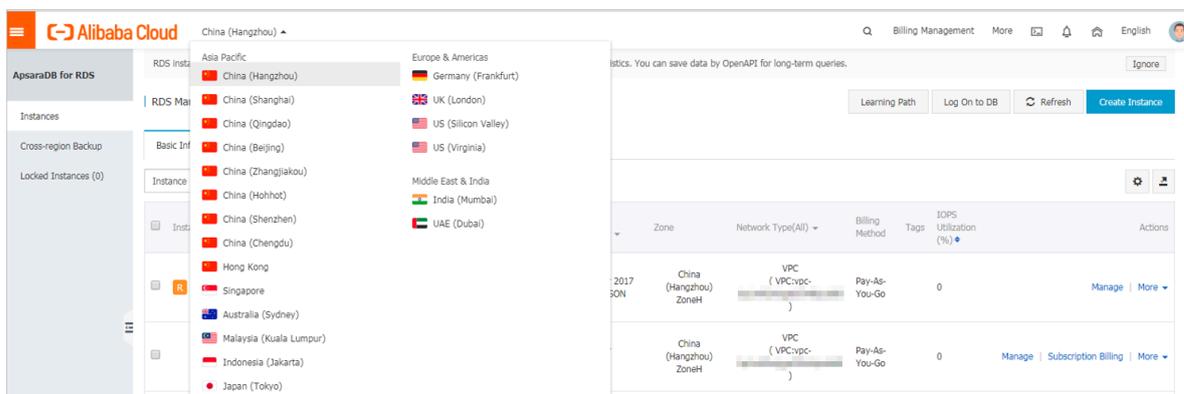
To prevent potential incorrect operations, RDS for MySQL does not provide the SUPER permissions.

- Can terminate any connections.

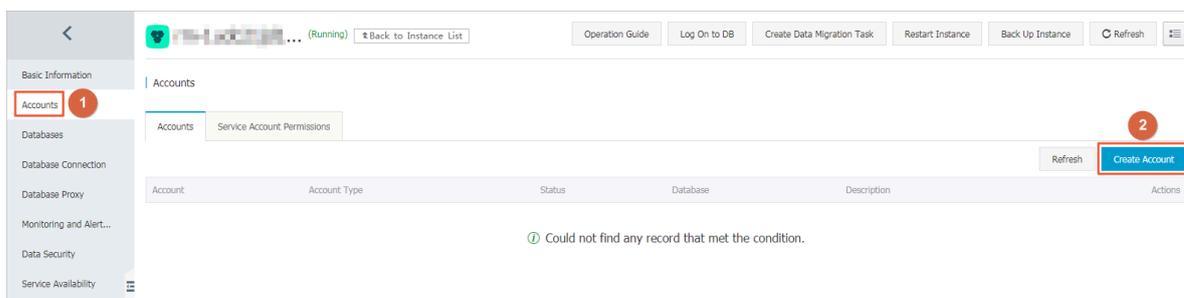
- Running the `show processlist` command shows all processes, including processes on the control level.
- Can use the `SET` statement to modify any global variables.
- Can use the `CHANGE MASTER` and `PURGE MASTER LOGS` commands.
- Can perform operations on files stored on the host.

Create the superuser account

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



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



6. Set the following parameters.

Parameter	Description
Database Account	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 Superuser Account.

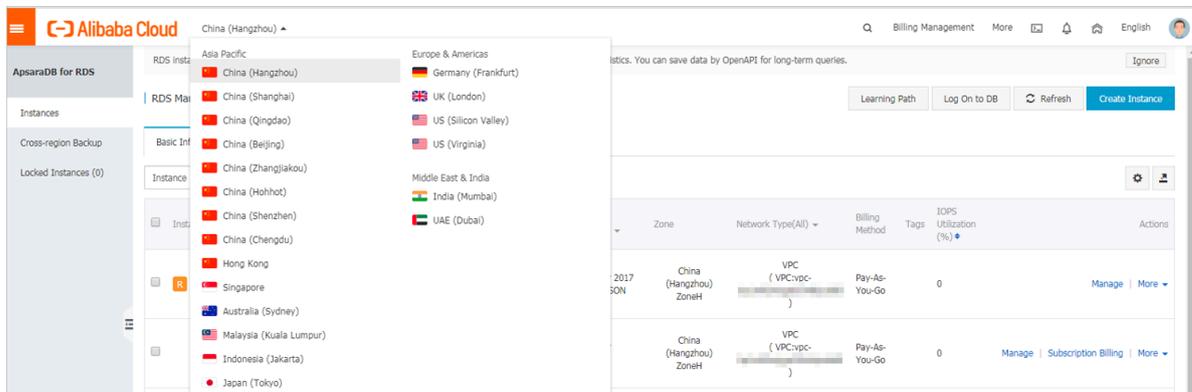
Parameter	Description
Password	The password contains 8 to 32 characters, including at least three of the following types of characters: uppercase letters, lowercase letters, digits, and special characters. The allowed special characters are as follows: ! @ # \$ % ^ & * () _ + - =
Re-enter Password	Enter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

7. Click OK.

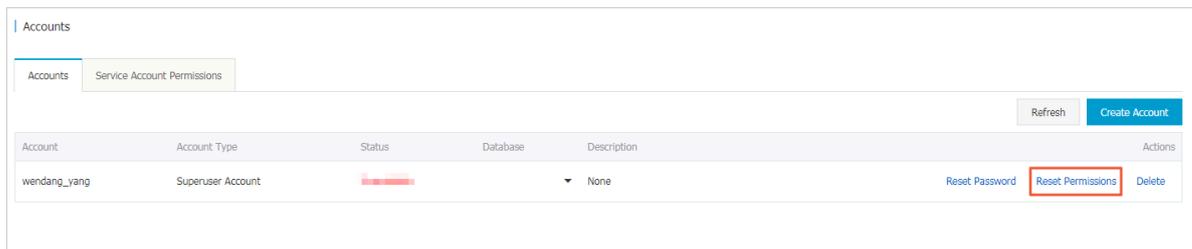
Reset the permissions of the superuser account

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

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



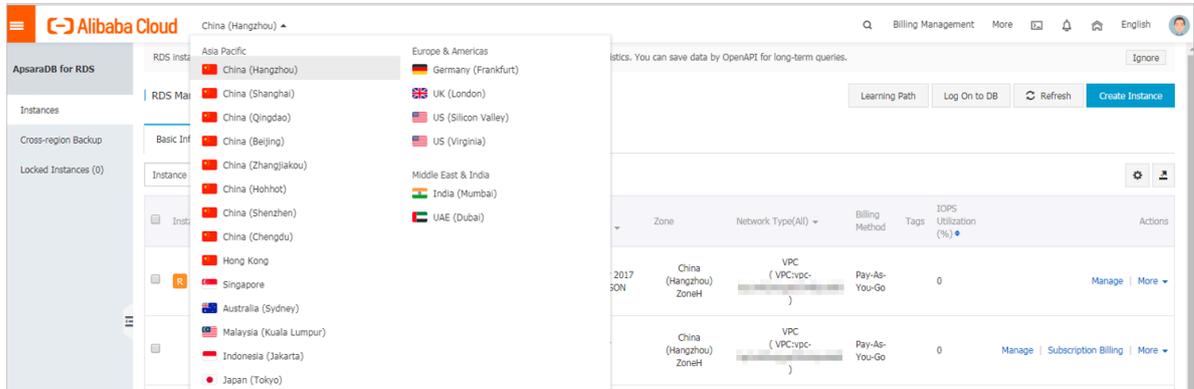
3. Find the target instance and click its ID.
4. In the left-side navigation pane, click Accounts.
5. Find the superuser account, and click Reset Permissions in the Actions column.



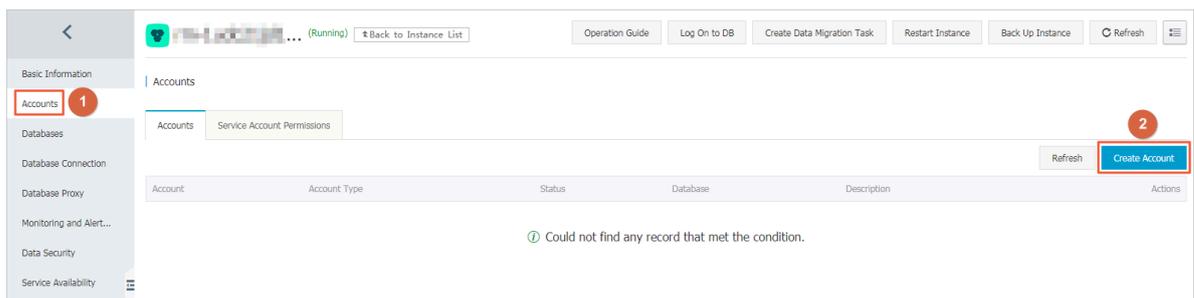
6. Enter the password of the superuser account and click OK.

Create a standard account

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



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



6. Set the following parameters.

Parameter	Description
Database Account	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.

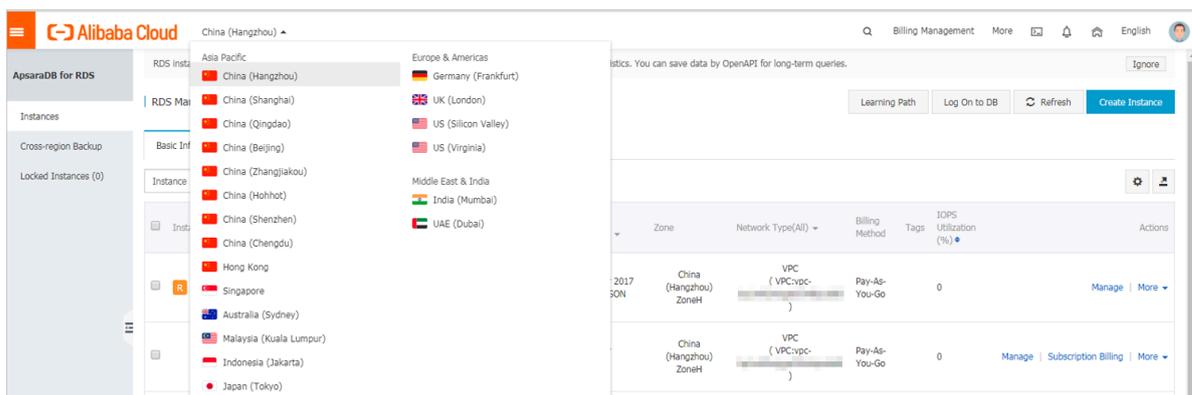
Parameter	Description
Authorized Databases	<p>Grant permissions on one or more databases to the account. This parameter is optional. You can choose to grant permissions to the account after the account is created.</p> <ol style="list-style-type: none"> Select one or more databases from the left area and click Authorize > to add them to the right area. In the right area, click Read/Write, Read-only, DDL Only, or DML Only. <p>If you want to grant the permissions for multiple databases in batches, select all the databases and in the upper-right corner click the button such as Full Control Read/Write.</p> <div style="background-color: #f0f0f0; padding: 5px;">  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. </div>
Password	<p>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:</p> <p>! @ # \$ % ^ & * () _ + - =</p>
Re-enter Password	Enter the password again.
Note	Optional. Enter the other account information that helps to better manage the account. You can enter up to 256 characters.

7. Click OK.

Create a database

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

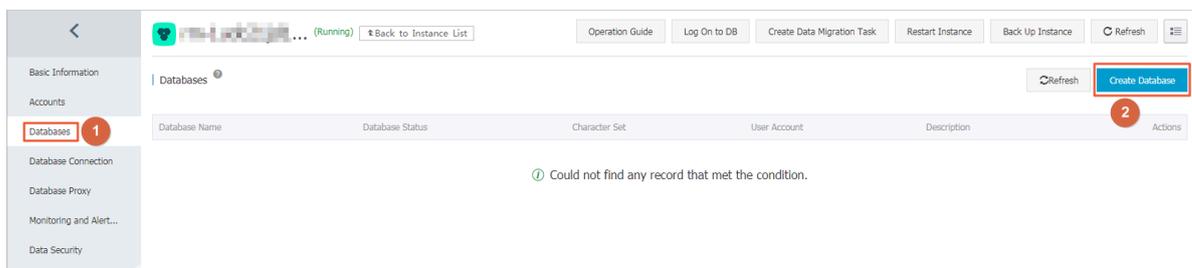
2. In the upper-left corner of the page, select the region where the instance is located.



3. Find the target instance and click its ID.

4. In the left-side navigation pane, click Databases.

5. Click Create Database.



6. Set the following parameters.

Parameters	Description
Database Name	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. If you need another character set, select all and then select the character set from the list.
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. <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p> Note: Only standard accounts are displayed, because the superuser account has all permissions for all databases.</p> </div>
Account Type	Select Read/Write, Read-only, DDL only, or DML only.

Parameters	Description
Remarks	Optional. Enter the other account information that helps to better manage the account. You can enter up to 256 characters.

7. Click OK.

Account permissions

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

Account type	Permission type	Permission				
		PROCESS	REPLICATION SLAVE	REPLICATION CLIENT	N/A	N/A
	DML only	SELECT	INSERT	UPDATE	DELETE	CREATE TEMPORARY TABLES
		LOCK TABLES	EXECUTE	SHOW VIEW	EVENT	TRIGGER
		PROCESS	REPLICATION SLAVE	REPLICATION CLIENT	N/A	N/A

FAQ

Can I use an account that I create to operate read-only instance?

An account created in your master RDS instance will be synchronized to the read-only instances attached to the master instance. However, you cannot manage the account in the read-only instances. The account only has the read permissions for the read-only instances.

APIs

API	Description
#unique_30	Used to create an account.
#unique_31	Used to create a database.

5 Connect to an RDS for MySQL instance

After completing the initial configurations, you can use Data Management Service (DMS), a database client, or the CLI to connect to ApsaraDB RDS for MySQL.

Background information

After you [create an instance](#), [configure a whitelist](#), and [create an account](#), you can use DMS, a database client, or CLI to connect to your RDS instance. You can also set the IP address, port, and account information in applications to connect.

Use DMS to connect to an RDS instance

DMS is a graphical data management service provided by Alibaba Cloud. It can be used to manage non-relational databases and relational databases, and supports data and schema management, user authorization, security audit, data trends, data tracking, BI charts, and performance and optimization.

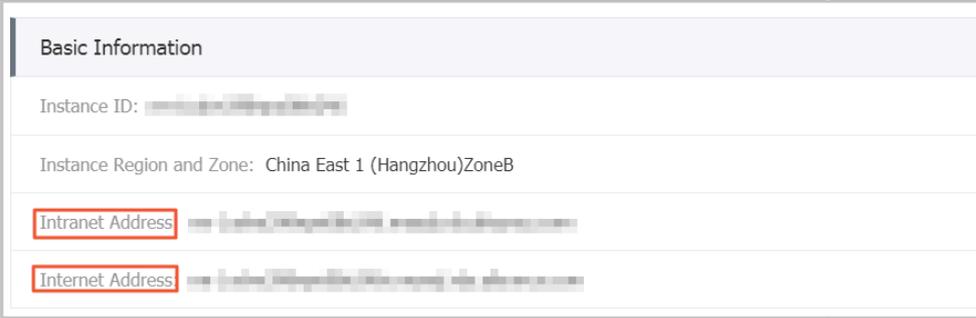
For more information, see [Use DMS to log on to an RDS instance](#).

Use a database client to connect to an RDS instance

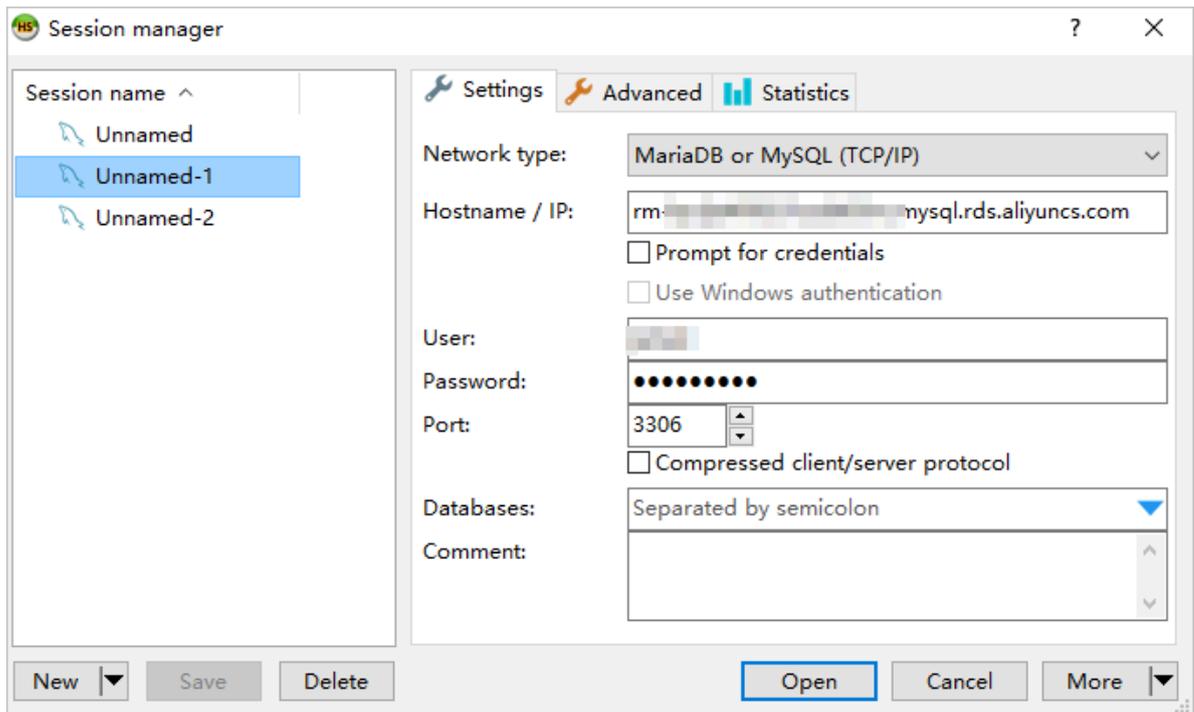
ApsaraDB RDS for MySQL is fully compatible with MySQL. You can connect to an RDS instance from any general-purpose database client in the similar way you connect to a MySQL database. This section describes how to use [HeidiSQL](#) to connect to an RDS instance.

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

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

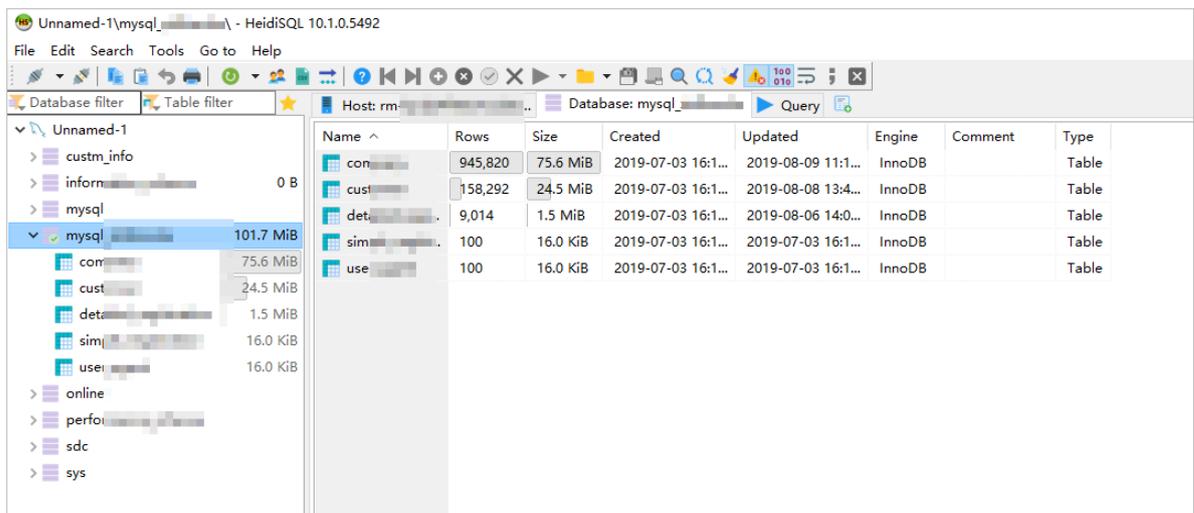
Parameter	Description
<p>Hostname/IP</p>	<p>Enter the private or public IP address of the RDS instance.</p> <ul style="list-style-type: none"> · If your database client is deployed in an ECS instance that is in the same region and has the same network type as the RDS instance, you can use the private 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. <p>You can obtain the private and public IP addresses of the RDS instance by completing the following steps:</p> <ol style="list-style-type: none"> 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.  <p>The screenshot shows the 'Basic Information' tab of an RDS instance. It displays the Instance ID, Instance Region and Zone (China East 1 (Hangzhou)ZoneB), Intranet Address, and Internet Address. The Intranet and Internet Address fields are highlighted with red boxes.</p>
<p>User</p>	<p>The username of the account that you use to access the RDS instance.</p>
<p>Password</p>	<p>The password of the account that you use to access the RDS instance.</p>

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



4. Click Open.

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



Use the CLI to connect to an RDS instance

If MySQL is installed on your server, you can use the CLI to connect to an RDS instance as follows:

```
mysql -h < Host name > -P < Port number > -u < Username > -p < Password > -D < RDS instance name >
```

Field	Description	Example
-h	The private or public IP address of the RDS instance. For more information, see #unique_36 .	<code>rm - bpxxxxxxxx xxxxxx . mysql . rds . aliyuncs . com</code>
-P	<p>The port for the RDS instance to establish a connection.</p> <ul style="list-style-type: none"> · 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. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  Note: <ul style="list-style-type: none"> · The default port number is 3306. · If the port used by the RDS instance to establish a connection is Port 3306, you can retain the default value. </div>	3306
-u	The username of the account that you use to access the RDS instance.	root

Field	Description	Example
-p	<p>The password of the account that you use to access the RDS instance.</p> <p> Note: This field is optional.</p> <ul style="list-style-type: none"> · If you do not enter the password in this field, the system prompts you to enter the password during subsequent operations. · If you enter the password in this field, note that no spaces are allowed between <code>- p</code> and the entered password. 	password23 3
-D	<p>The name of the RDS instance you want to access.</p> <p> Note:</p> <ul style="list-style-type: none"> · This field is optional. · You can enter only the RDS instance name with <code>- D</code> removed. 	mysql

Figure 5-1: Example of connecting to an RDS instance through CLI

```
[root@ ~]# mysql -hrm-bp-3.mysql.rds.aliyuncs.com -uroot -p mysql
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 196
Server version: 5.7.25-log Source distribution

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

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

MySQL [mysql]>
```

6 Scale instances

6.1 Read-only instance

6.1.1 Introduction to MySQL read-only instances

Scenario

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

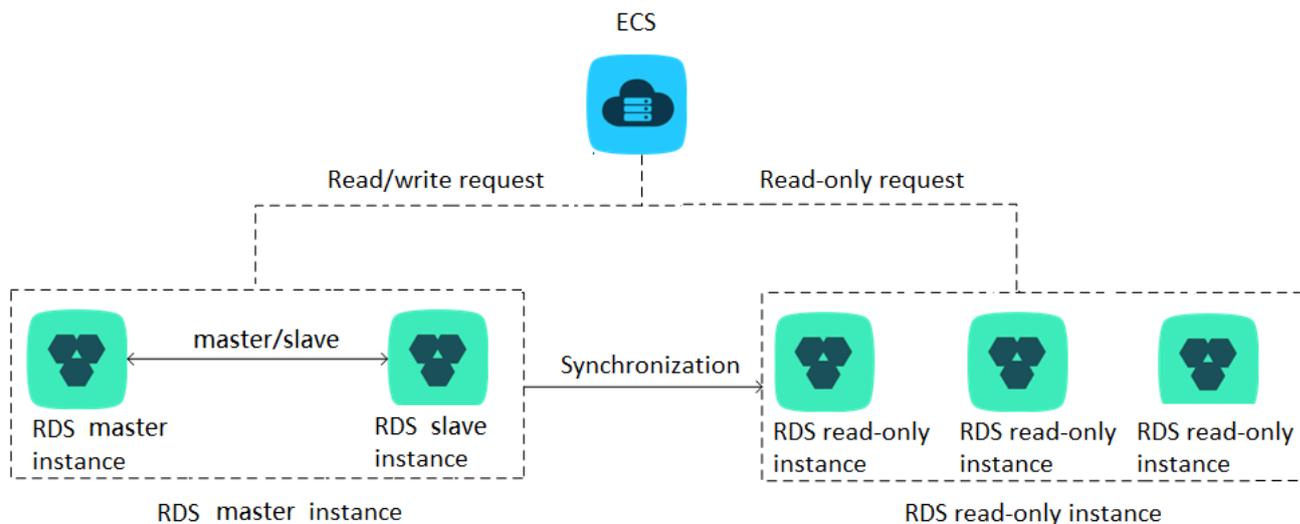
Overview

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



Note:

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



Pricing

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



Note:

For information about data retention policies for read-only instances, see [#unique_40](#).

Features

Read-only instances offer the following features:

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

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

- Read-only instances provide optimization suggestions.

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

Restrictions

- Quantity of read-only instances

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

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

FAQs

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

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

6.1.2 Create an RDS for MySQL read-only instance

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

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

Prerequisites

The version of your RDS master instance is as follows:

- MySQL 8.0 High-availability Edition (with local SSD)
- MySQL 5.7 High-availability Edition (with local SSD)
- MySQL 5.6

Precautions

- You can create read-only instances in your master RDS instance. However, you cannot switch an existing instance to a read-only instance.
- Creating a read-only instance does not affect your master RDS instance because the read-only instance copies data from the slave instance.
- A read-only instance does not inherit the parameter settings of your master RDS instance. Instead, default parameter settings are generated. You can modify the parameter settings of a read-only instance on the RDS console.
- The quantity of read-only instances is as follows.

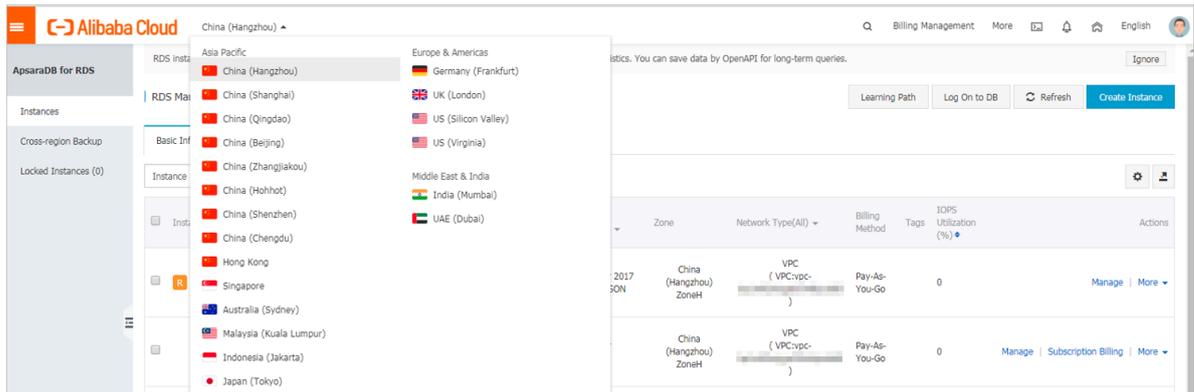
Database type	Memory	Max number of read-only instances
MySQL	≥ 64 GB	10
	< 64 GB	5

- A read-only instance is charged according to the Pay-As-You-Go billing method. Specifically, the fees for a read-only instance are deducted once per hour depending on the instance specifications. For more information, see the "Read-Only Instances" part at [Pricing](#).

Create a read-only instance

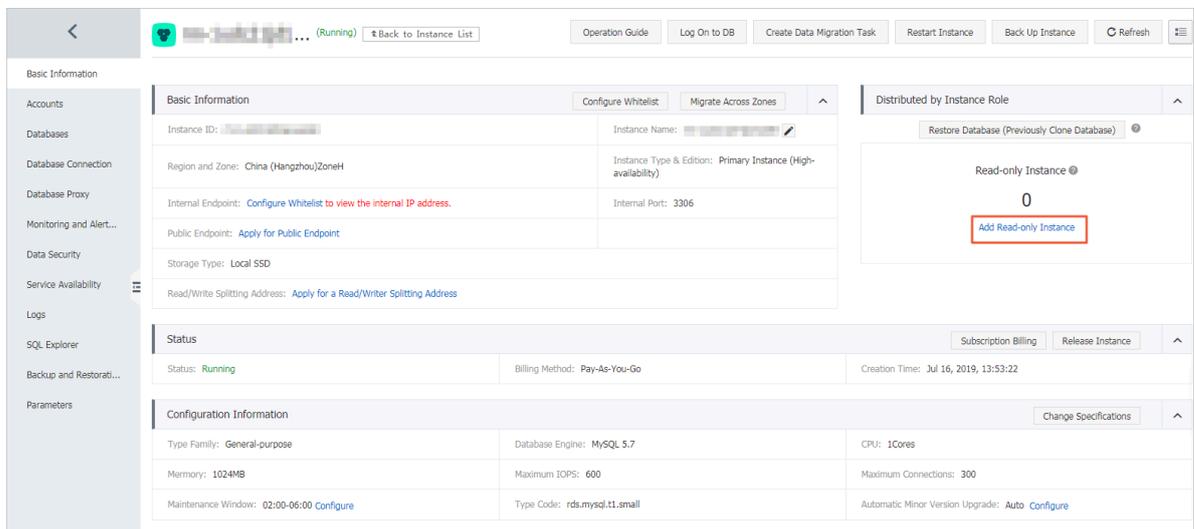
1. Log on to the [RDS console](#).

2. Select the region where the target instance is located.



3. Find the target instance and click its ID.

4. Click Add Read-only Instance.



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



Note:

- We recommend that the read-only instance and the master instance be in the same VPC.
- To guarantee sufficient I/O for data synchronization, we recommend that the configuration of the read-only instance (the memory) is greater than or equal to that of the master instance.
- We recommend that you purchase multiple read-only instances based on your business needs to improve availability.

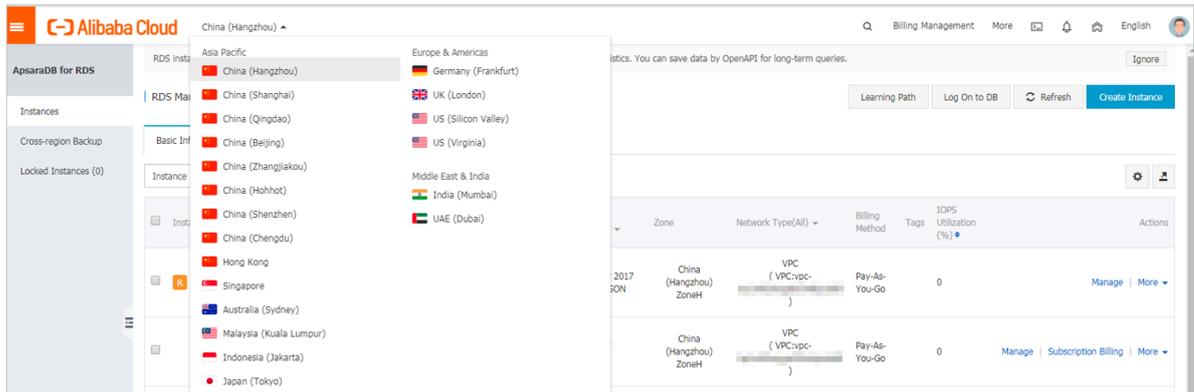
- On the Order Confirmation page, review the order information, select the terms and agreements as prompted, click Pay Now, and complete the payment.

The instance creation takes a few minutes.

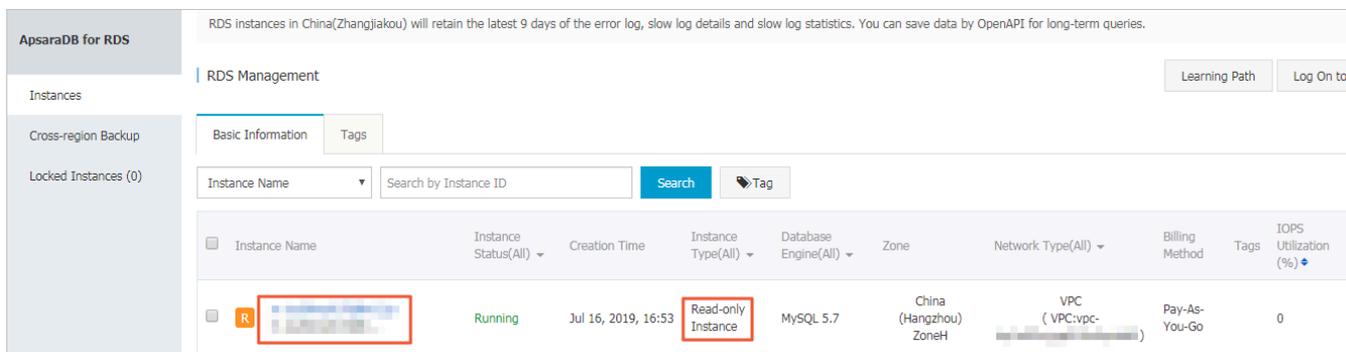
View a read-only instance

View a read-only instance in the instance list

- Log on to the [RDS console](#).
- Select the region where the read-only instance is located.



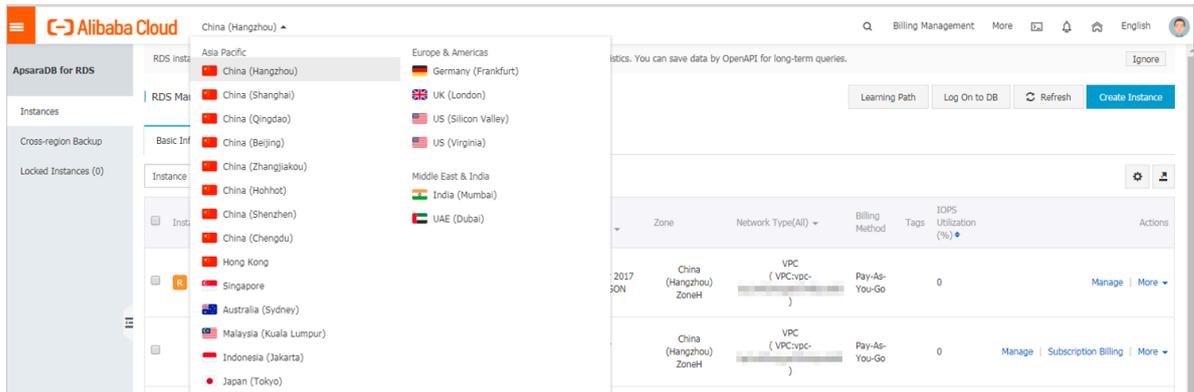
- In the instance list, find the read-only instance and click its ID.



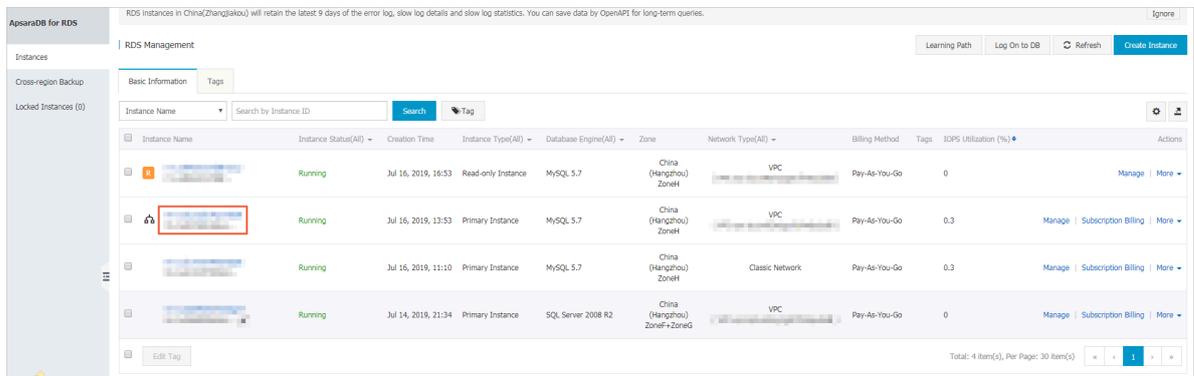
View a read-only instance on the Basic Information page for the master instance

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

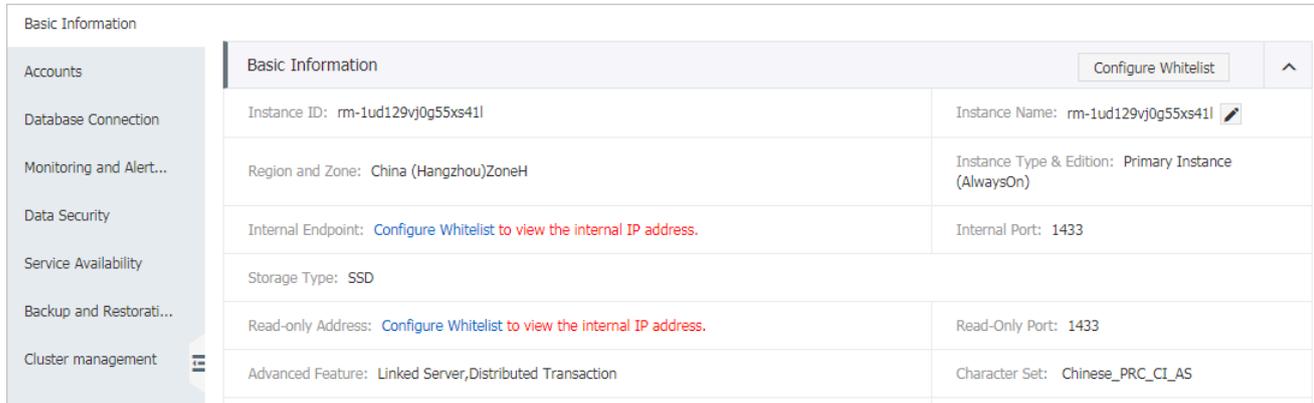
2. Select the region where the master instance is located.



3. In the instance list, find the master instance and click its ID.

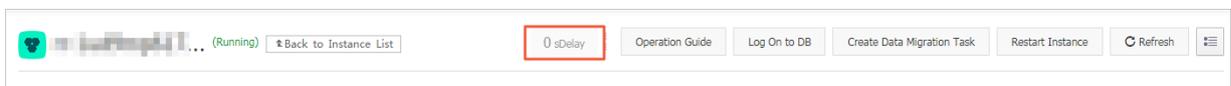


4. On the Basic Information page of the master instance, move the pointer over the number below Read-only Instance and click the ID of the read-only instance.



View the delay time of a read-only instance

When a read-only instance synchronizes data from the master instance, the read-only instance may lag behind the master instance by a small amount of time. You can view the delay on the Basic Information page of the read-only instance.



APIs

API	Description
#unique_42	Used to create an RDS read-only instance.