Alibaba Cloud ApsaraDB for RDS

RDS for PPAS User Guide

Issue: 20191021

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

Alibaba Cloud ApsaraDB for RDS (short for Relational Database Service) is a stable, reliable, and scalable online database service. Based on Alibaba Cloud distributed file system and high-performance SSD storage, ApsaraDB for RDS supports the MySQL, SQL Server, PostgreSQL, and PPAS (compatible with Oracle) database engines and provides a portfolio of solutions to disaster tolerance, backup, recovery, monitoring, and migration to facilitate database operation and maintenance. For information about the benefits of ApsaraDB for RDS, see *#unique_4*.

This document describes how to configure and manage RDS through the *RDS console* , helping you better understand the features and functions of ApsaraDB for RDS. Additionally, you can configure and manage RDS through API and SDK.

If you need technical support, you can call 95187. Alternatively, you can open the *RDS console* and in the upper-right corner choose More > Support > Open a new ticket. If your business is complex, you can purchase a *support plan* to obtain your exclusive support service from IM enterprise groups, technical service managers (TAM), and service managers.

For more information about ApsaraDB for RDS, visit *ApsaraDB RDS for MySQL*.

Disclaimer

Some product features or services described in this document may be unavailable for certain regions. See the relevant commercial contracts for specific Terms and Conditions. This document serves as a user guide only. No content in this document can constitute any express or implied warranty.

Terms

- **Instance: A database service process that takes up physical memory independen tly. You can specify the memory size, disk space, and database type of an instance, but only the memory specification determines the performance of the**

instance. After an instance is created, you can delete it or change its configurat ion as needed.

- Database: A logical unit created in an instance. Multiple databases that each have a unique name can be created in one instance.
- Region and zone: A region is a physical data center. A zone is a physical area that has independent power supply and network in a region. For more information, visit *Alibaba Cloud's Global Infrastructure*.

Concepts

Item	Description
On-premises database	A database that is deployed in your on-premises equipment room or on a cloud other than ApsaraDB for RDS.
RDS for XX (XX is MySQL, SQL Server, PostgreSQL, or PPAS.)	A type of RDS instance. For example , RDS for MySQL refers to the type of RDS instance that runs in the MySQL database engine.

2 Limits of RDS for PPAS

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

The following table describes the limits of RDS for PPAS.

Operation	Description
Modify database parameter settings	Currently not supported
Database root permission	RDS does not offer the superuser permission to users.
Database backup	You can back up data only through pg_dump.
Data migration to the cloud	You can only use psql to restore data backed up by pg_dump.
Set up database replication	· You do not need to set up data replication because the system has automatically set up PPAS stream replication based the HA mode. · The PPAS slave node is invisible to users, and cannot be used directly for access.
Restart an RDS instance	You must restart an instance through the *RDS console* or APIs.
Network settings	If the *access mode* of the instance is safe connection mode, enabling net.ipv4.tcp_timestamps in SNAT mode is not allowed.

3 Quick start

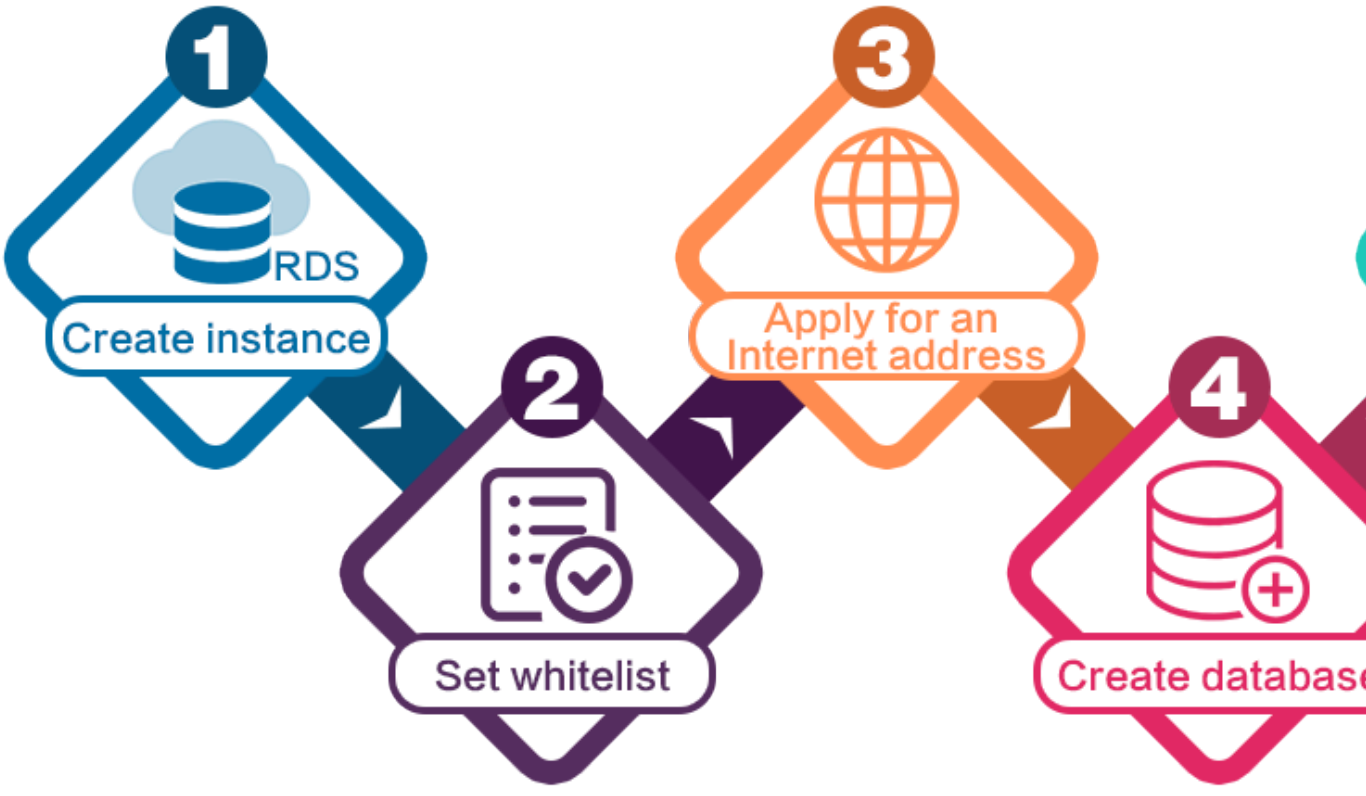
3.1 General process to use RDS for PPAS

This topic describes the general process from purchasing an RDS for PPAS instance to using it, including creating, setting, and connecting an instance.

Quick start flowchart

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

The following flowchart shows the operations you must complete from purchasing an RDS for PPAS instance to using it.



1. *Create an RDS for PPAS instance*
2. *Configure a whitelist for an RDS for PPAS instance*
3. *Apply for a public endpoint for an RDS for PPAS instance*

4. *Create databases and accounts for an RDS for PPAS instance*
5. *Connect to an RDS for PPAS instance*

3.2 Create an RDS for PPAS instance

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

For information about how to create an RDS for MySQL instance by calling an API action, see *CreateDBInstance*.

For information about the pricing of RDS for MySQL instances, 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 *Switch from pay-as-you-go billing to subscription billing*.**
- **By default, each 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.
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.

Parameter	Description
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.
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.

Parameter	Description
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.
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.

Parameter	Description
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*.

APIs

API	Description
#unique_20	Used to create an RDS instance.

3.3 Configure a whitelist for an RDS for PPAS instance

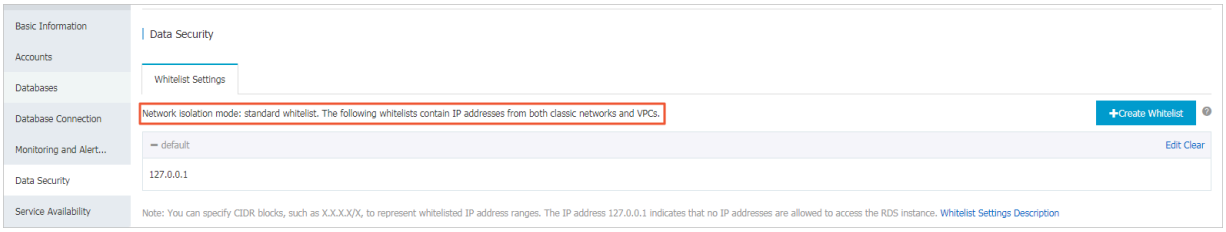
This topic describes how to configure a whitelist for an RDS for PPAS instance.

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 can 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.

Precautions

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



Note:

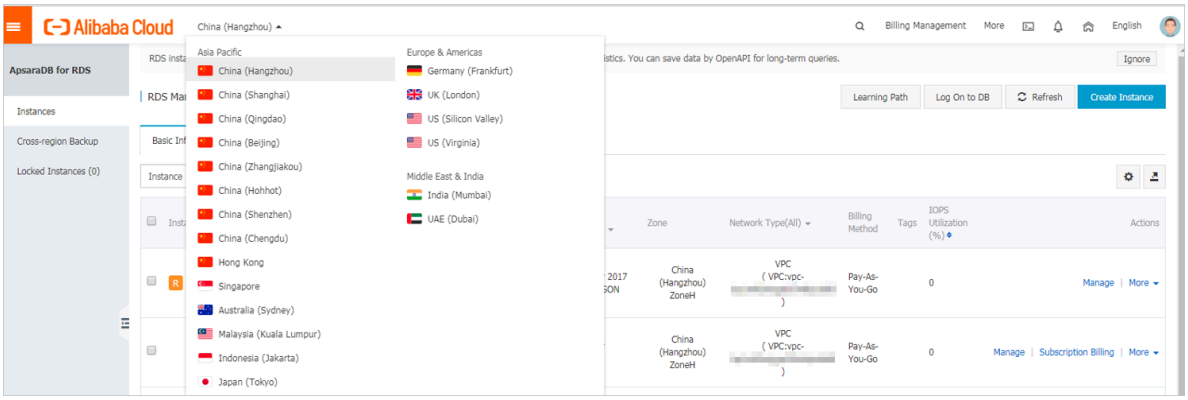
The internal networks to which RDS instances belong are divided into two types: classic network and VPC.

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

Procedure

Enhanced whitelist

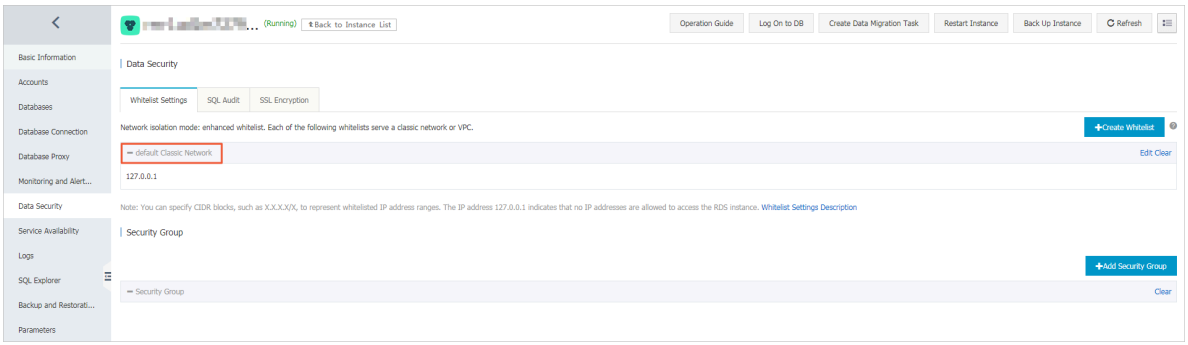
1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Data Security.**
5. **On the Whitelist Settings tab page, follow the following instructions based on your usage scenario:**
   - **Accessing an RDS instance from an ECS located in a VPC: Click Edit next to the `default VPC` whitelist.**
   - **Accessing an RDS instance from an ECS located in a classic network: Click Edit next to the `default Classic Network` whitelist.**
   - **Accessing an RDS instance from an ECS or host located in a public network: Click Edit next to the `default Classic Network` whitelist.**

Note:

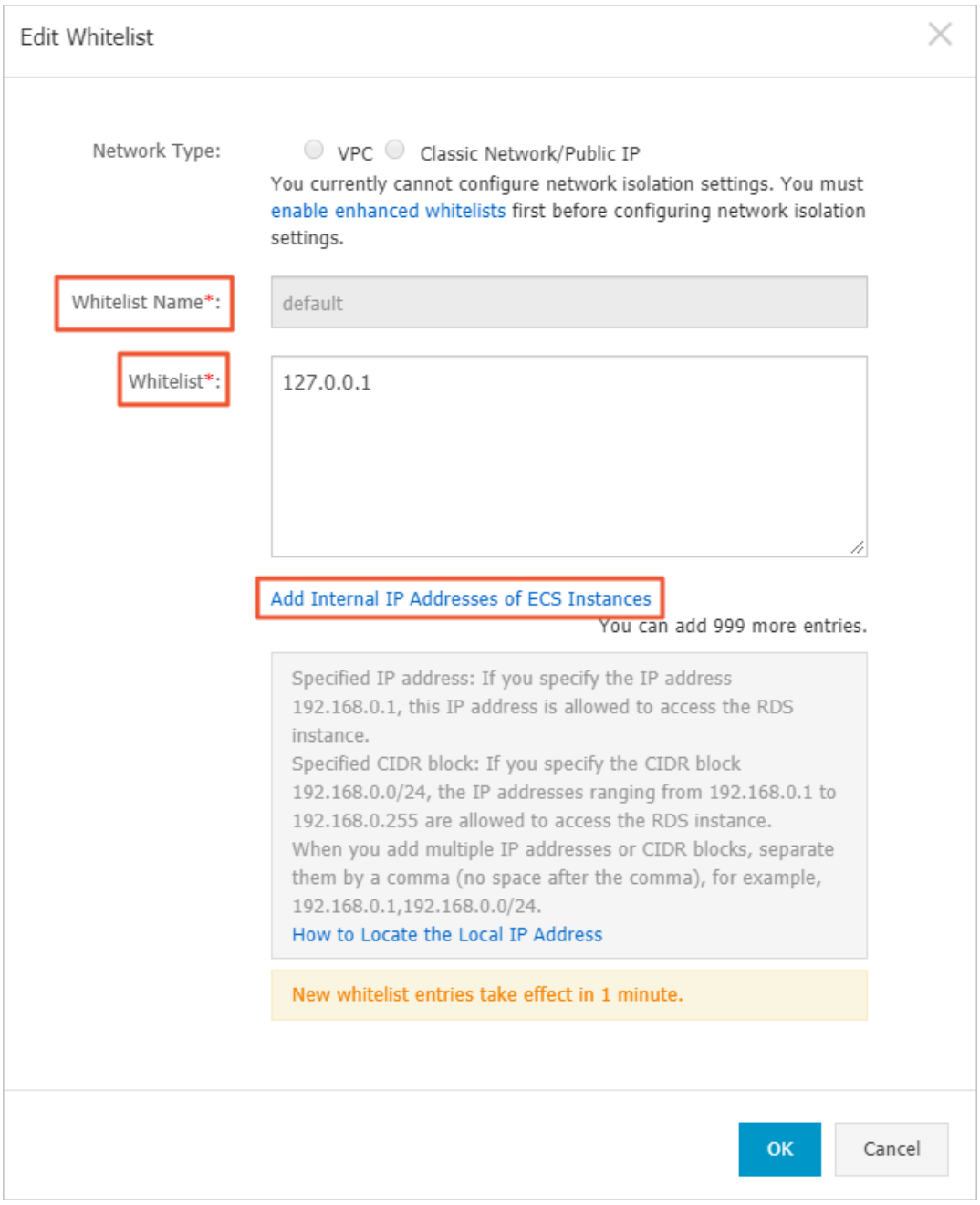
- If the ECS instance accesses the RDS instance by using the VPC or classic network, you must make sure that the two instances are in the same region and have the same *network type*. Otherwise, the connection fails.
- You can also click Create Whitelist. In the displayed Create Whitelist dialog box, select VPC or Classic Network/Public IP.



6. 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:

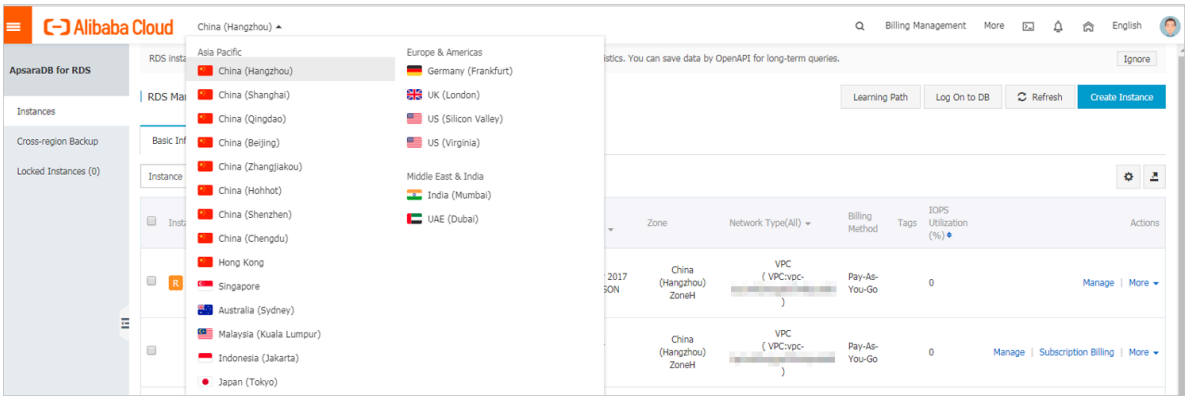
After you add an IP address or CIDR block to the default whitelist, the default address 127.0.0.1 is automatically deleted.



Standard whitelist

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

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



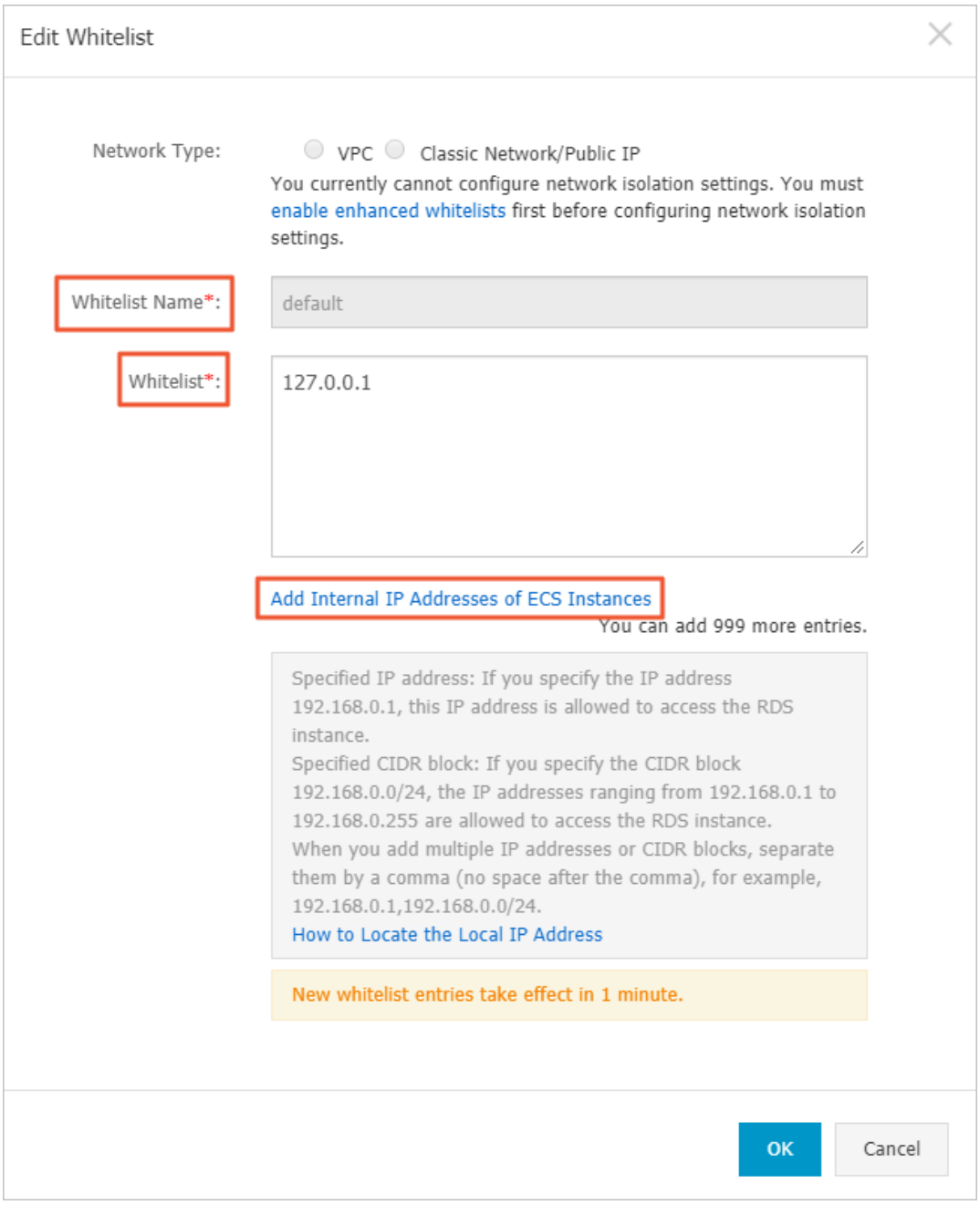
3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Data Security.
5. On the Whitelist Settings tab page, click Edit corresponding to the default whitelist.

> **Note:**
> You can also click Create Whitelist to configure 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 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.



Common errors

- **The default address 127.0.0.1 on the Whitelist Settings tab 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 turn on 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 VPC.**
  - **If the network type is classic network, the internal IP address of the ECS instance is added to the whitelist whose network isolation mode is classic network.**
  - **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 instance or host must be added to the whitelist whose network isolation mode is classic network.**
- **The public IP address that you add to the whitelist may not be the real egress 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 provide wrong IP addresses.**

  For more information, see *#unique_23*

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.**

3.4 Create databases and accounts for an RDS for PPAS instance

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

Before using RDS, you must create databases and accounts for your RDS instance . For PPAS instances, you must create a premier account in the RDS console. And then you can create and manage databases through a client. This topic takes the

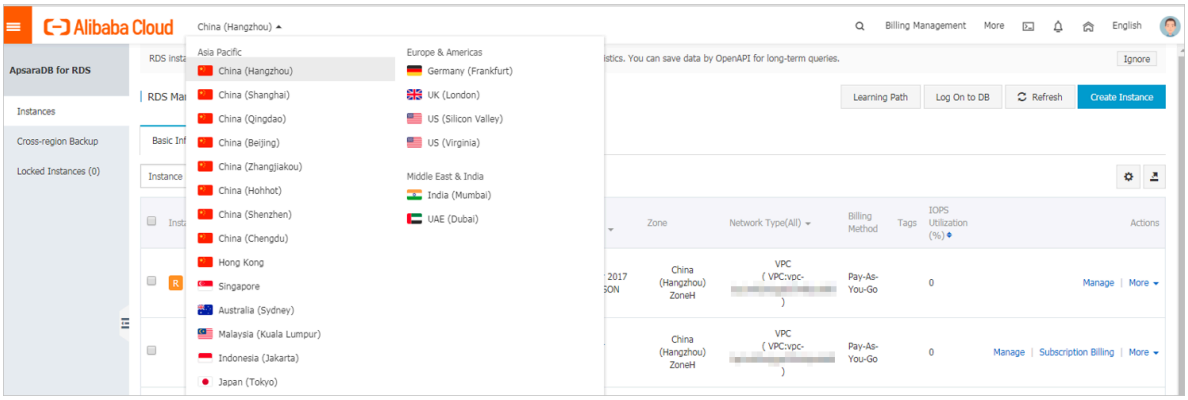
pgAdmin 4 client as an example to introduce how to create databases and accounts for PPAS instances.

Precautions

- Databases under a single instance share all the resources of this instance. Each PPAS instance supports one premier account, countless general accounts, and countless databases. You must create and manage common accounts and databases through SQL statements.
- To migrate your local database to an RDS instance, you must create the same databases and accounts for the RDS instance as your local database.
- When assigning account permissions for each database, follow the minimum permission' principle and consider service roles to create accounts. Alternativ ely, rationally assign read-only and read/write permissions. When necessary, you can split accounts and databases into smaller units so that each account can only access data for its own services. If the account does not need to write data to a database, assign the read-only permission for the account.
- For database security purposes, set strong passwords for the accounts and change the passwords regularly.

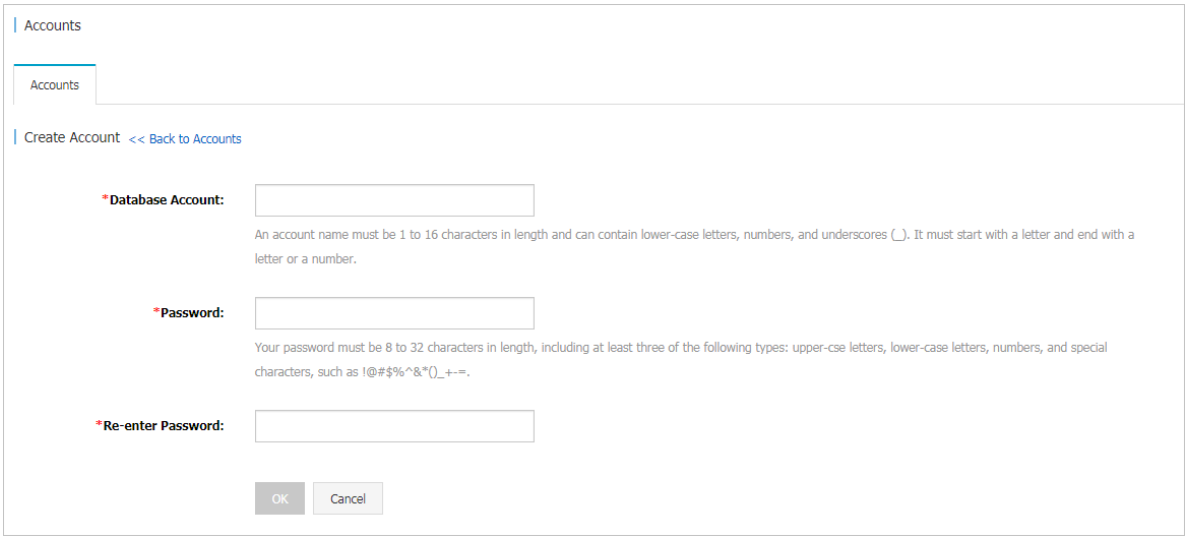
Procedure

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



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

6. Enter the account information.



Parameter description:

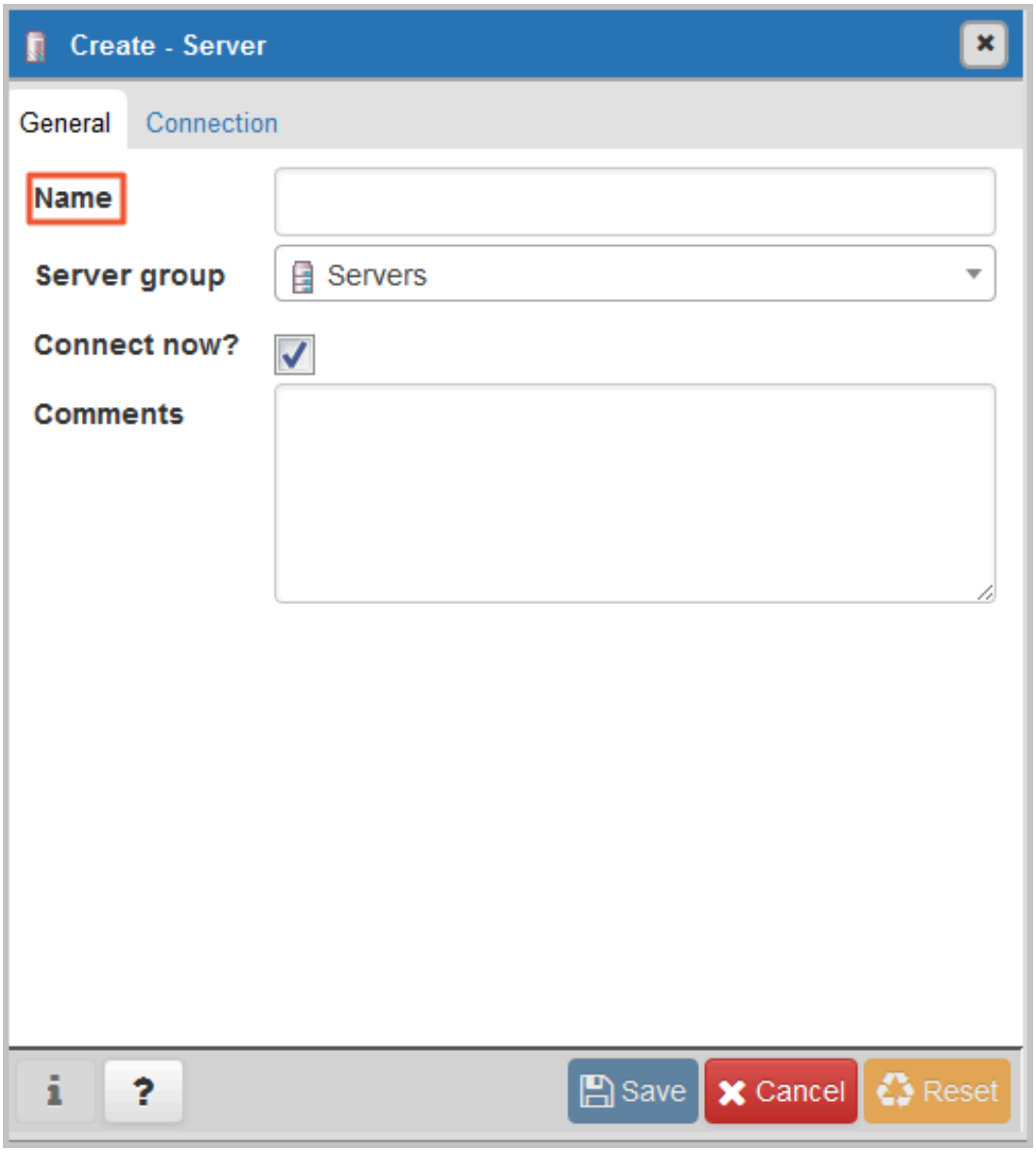
- Database Account: The name of the premier account. The account name must be 2 to 16 characters in length and can contain lowercase letters, numbers, and underscores (_). It must start with a letter and end with a letter or number.
- Password: The password of the premier account. The account password 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.

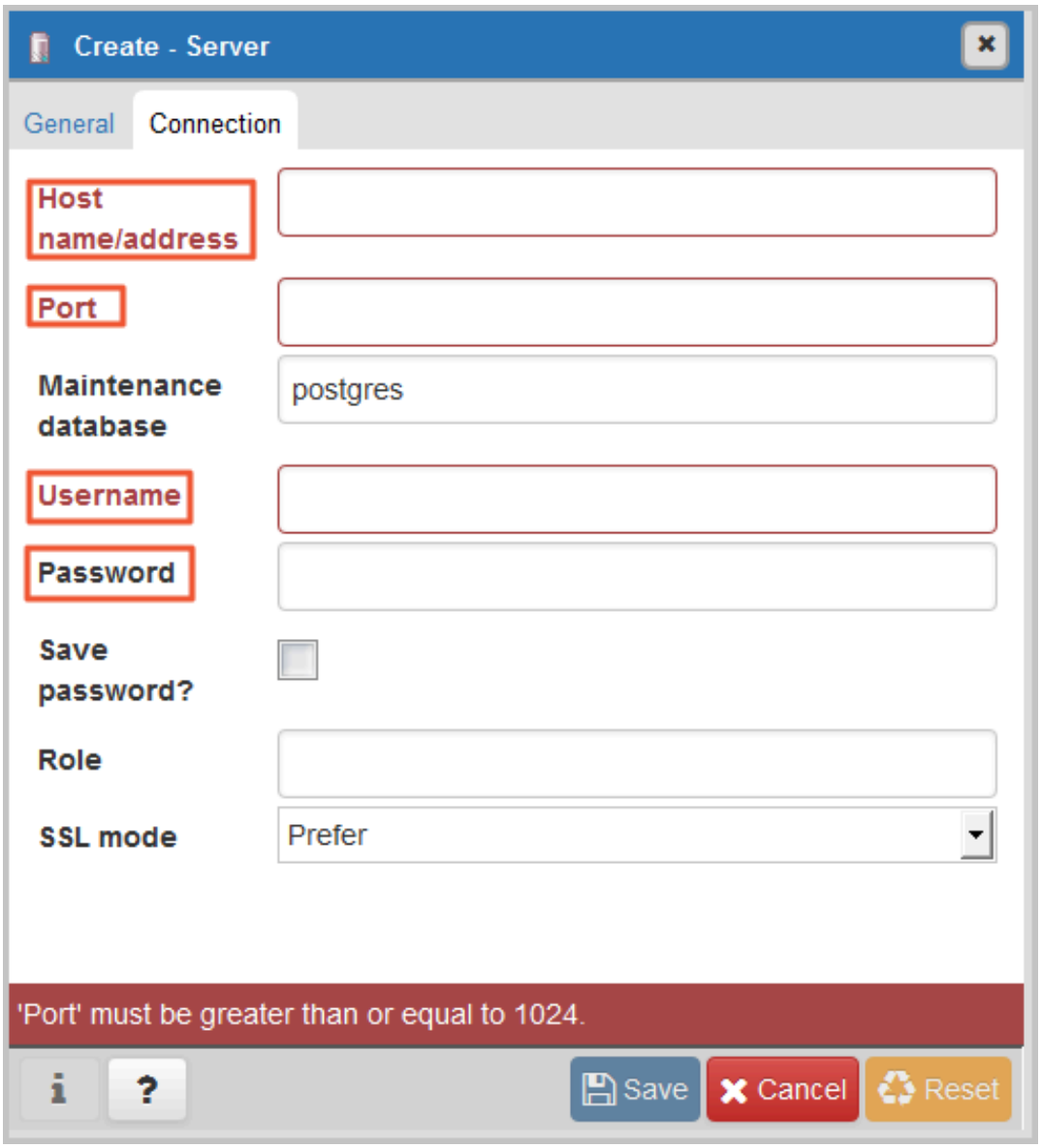
7. Click OK.
8. Add the IP address that is allowed to access the RDS instance to the RDS whitelist. For more information, see *Configure a whitelist for an RDS for PPAS instance*.
9. Start the pgAdmin 4 client.

10. Right-click Servers and choose Create > Server from the shortcut menu.

11. In the Create Server dialog box, click the General tab and enter the server name.



12. Click the Connection tab and enter the information about the RDS instance to be connected.



Parameter description:

- Host name/address: The internal or public endpoint of the RDS instance. To obtain the internal and public endpoints and ports of the RDS instance, follow these steps:
  a. Log on to the *RDS console*.
  b. Select the target region.
  c. Find the target RDS instance and click the instance ID.

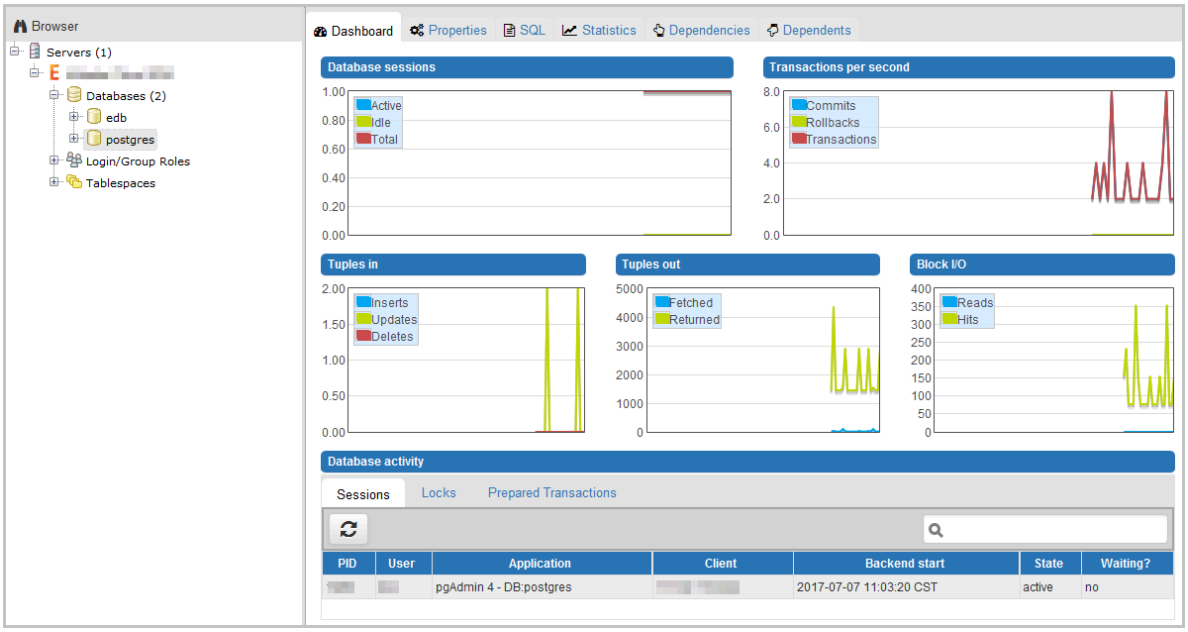
d. On the Basic Information page, find the Basic Information section, where you can obtain the internal and public endpoints and ports of the RDS instance.

- Port: The internal or public port numbr of the RDS instance.
- Username: The username of the premier account for the RDS instance.
- Password The password of the premier account for the RDS instance.

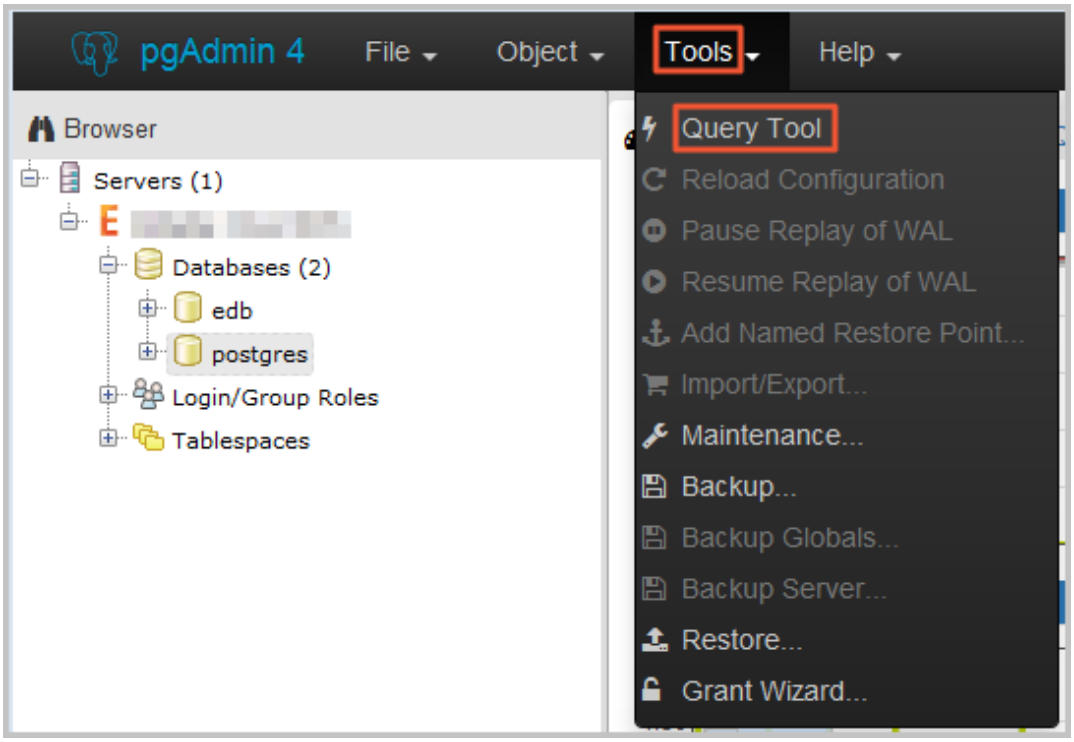
13. Click Save.

14. If the connection information is correct, choose Servers > server name > Databases > edb or postgres. The following page is displayed, which indicates that the connection to the RDS instance is successful.

Note:
postgres is the default system database of the RDS instance. Do not perform any operation in this database.

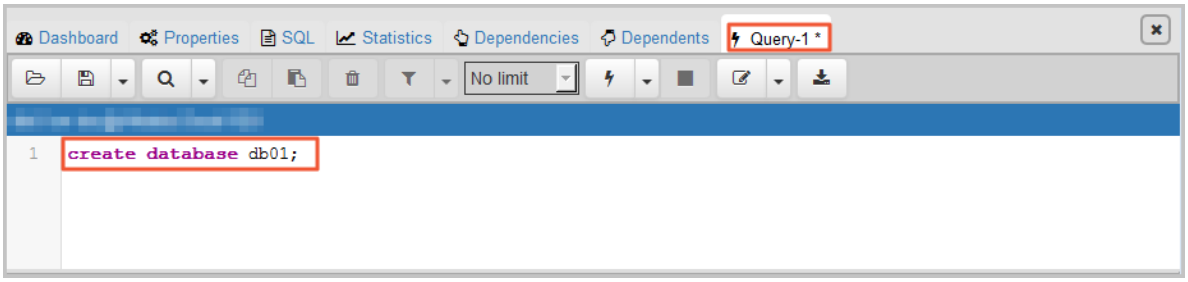


15. Double-click postgres and choose Tools > Query Tool.

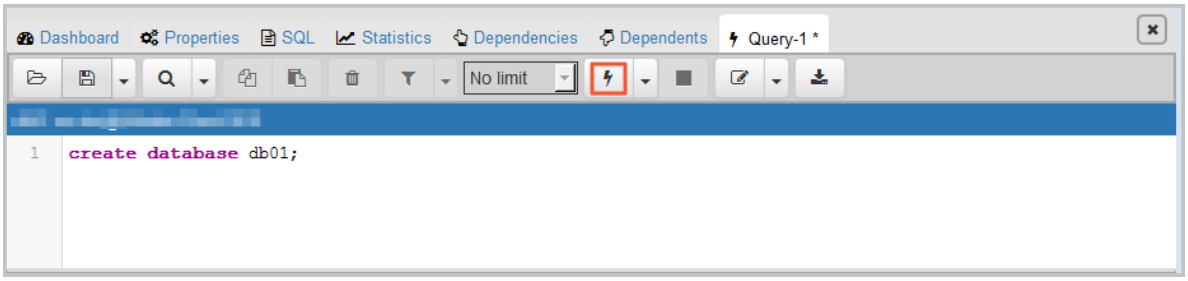


16. Enter the following command on the Query-1 tab page to create a database:

```
create database <database name>;
```

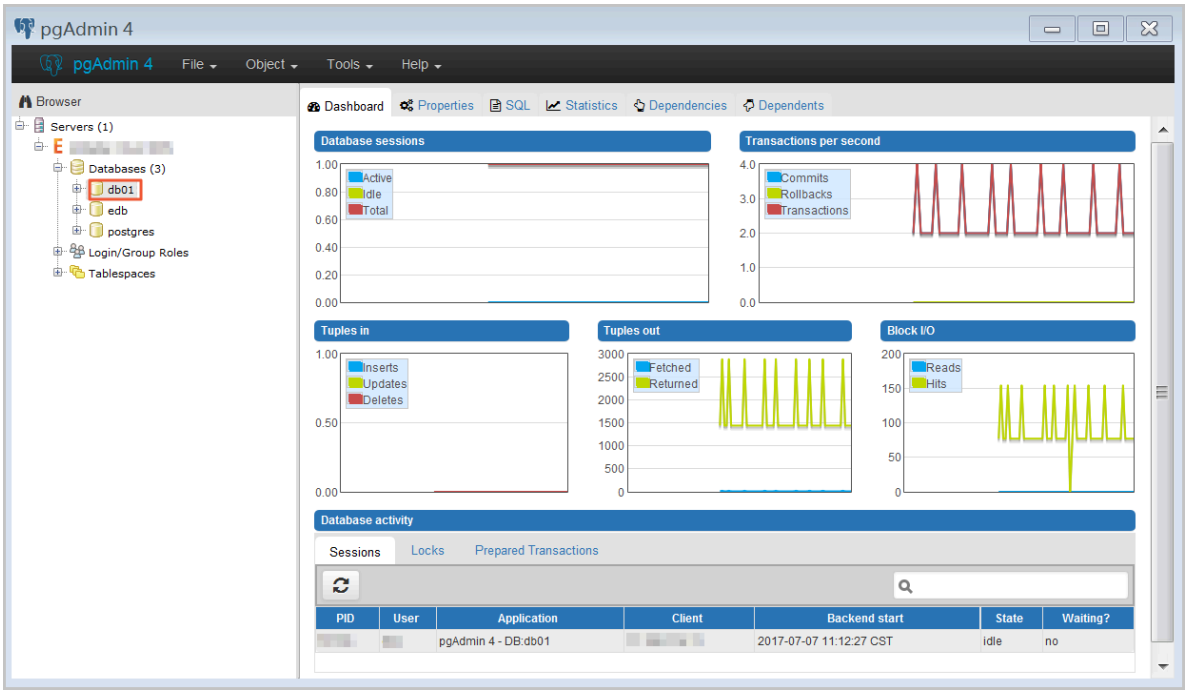


17. Click Execute/Refresh, as shown in the following figure.



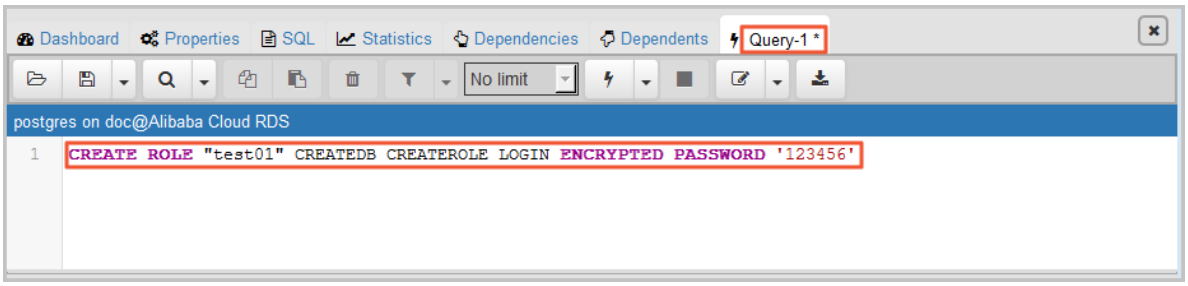
If the execution is successful, the new database is created.

18. Right-click Databases and choose Refresh from the shortcut menu. Then you can find the new database.

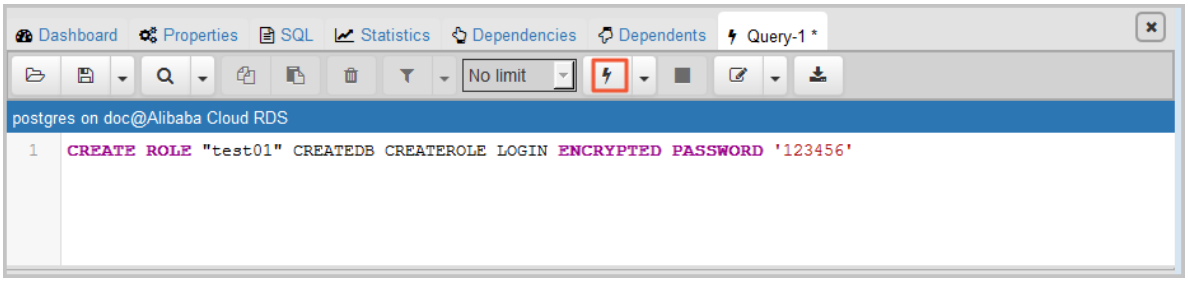


19. Enter the following command on the Query-1 tab page to create an account:

```
CREATE ROLE "username" CREATEDB CREATEROLE LOGIN ENCRYPTED PASSWORD
 'password';
```

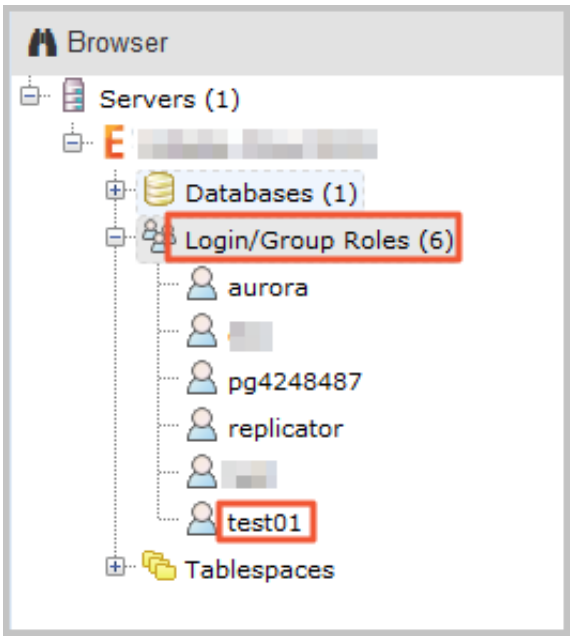


20. Click Execute/Refresh, as shown in the following figure.



If the execution is successful, the new account is created.

21. Right-click Login/Group Roles and choose Refresh from the shortcut menu. Then you can find the new account.



FAQ

Can I use the new account of my RDS instance on the corresponding read-only instances?

The new account will be synchronized to the read-only instances of your RDS instance. However, you cannot manage the account in the read-only instances. The new account only has the read permissions on the read-only instances.

APIs

API	Description
CreateAccount	Used to create an account for an RDS instance.

3.5 Connect to an RDS for PPAS instance

This topic describes how to connect to an RDS for PPAS instance. After completing the initial configuration, you can connect to your RDS instance from an ECS instance or your computer.

You can use a database client or Data Management Service (DMS) to connect to an RDS instance. This topic describes how to connect to an RDS instance by using DMS and the pgAdmin 4 client.

Background information

You can log on to DMS from the *RDS console* and then connect to an RDS instance. *DMS* offers an integrated solution for data and schema management, access security, BI charts, data trends, data tracking, performance optimization, and server management. DMS can be used to manage non-relational databases and relational databases, such as MySQL, SQL Server, PostgreSQL, MongoDB, and Redis. It can also be used to manage Linux servers.

You can also use a database client to connect to an RDS instance. ApsaraDB RDS for PPAS is fully compatible with PPAS. You can connect to RDS in the similar way you connect to an on-premises PPAS server. This topic describes how to use the pgAdmin 4 client to connect to an RDS instance. This topic also serves as a reference if you choose to use other database clients. When you use a client to connect to an RDS instance, you must *set internal and public IP addresses* as follows:

- **If your client is deployed in an ECS instance and the instance is in the same region and has the same network type as the target RDS instance, then you can use the internal IP address. For example, the ECS instance and RDS instance are both in the VPC located in China (Hangzhou). You can use the internal IP address provided to create a secure connection.**
- **Use the public IP address for other situations.**

Use DMS to connect to an RDS instance

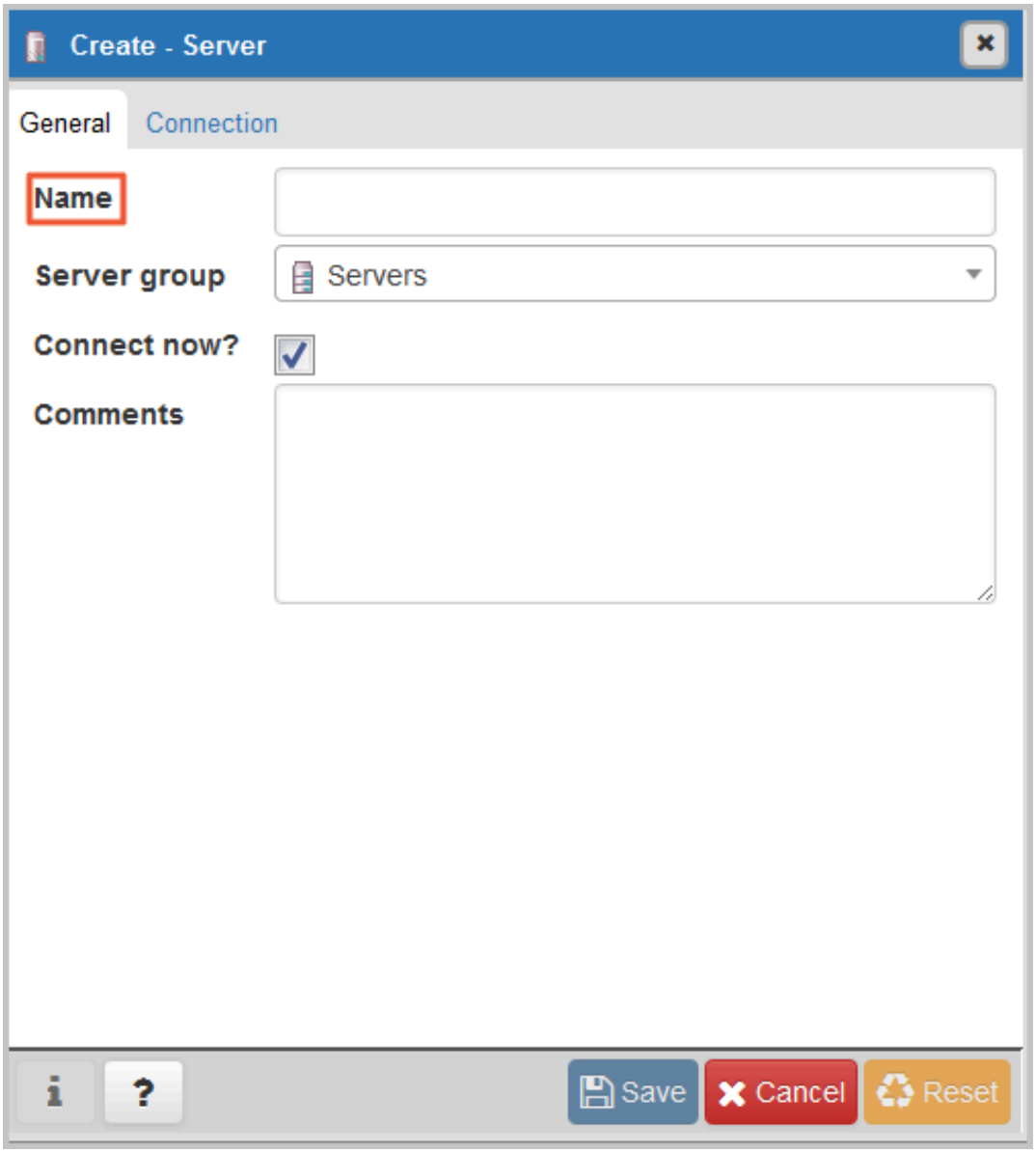
For more information about how to connect to an RDS instance through DMS, see *Log on to the RDS database through DMS*.

Use a client to connect to an RDS instance

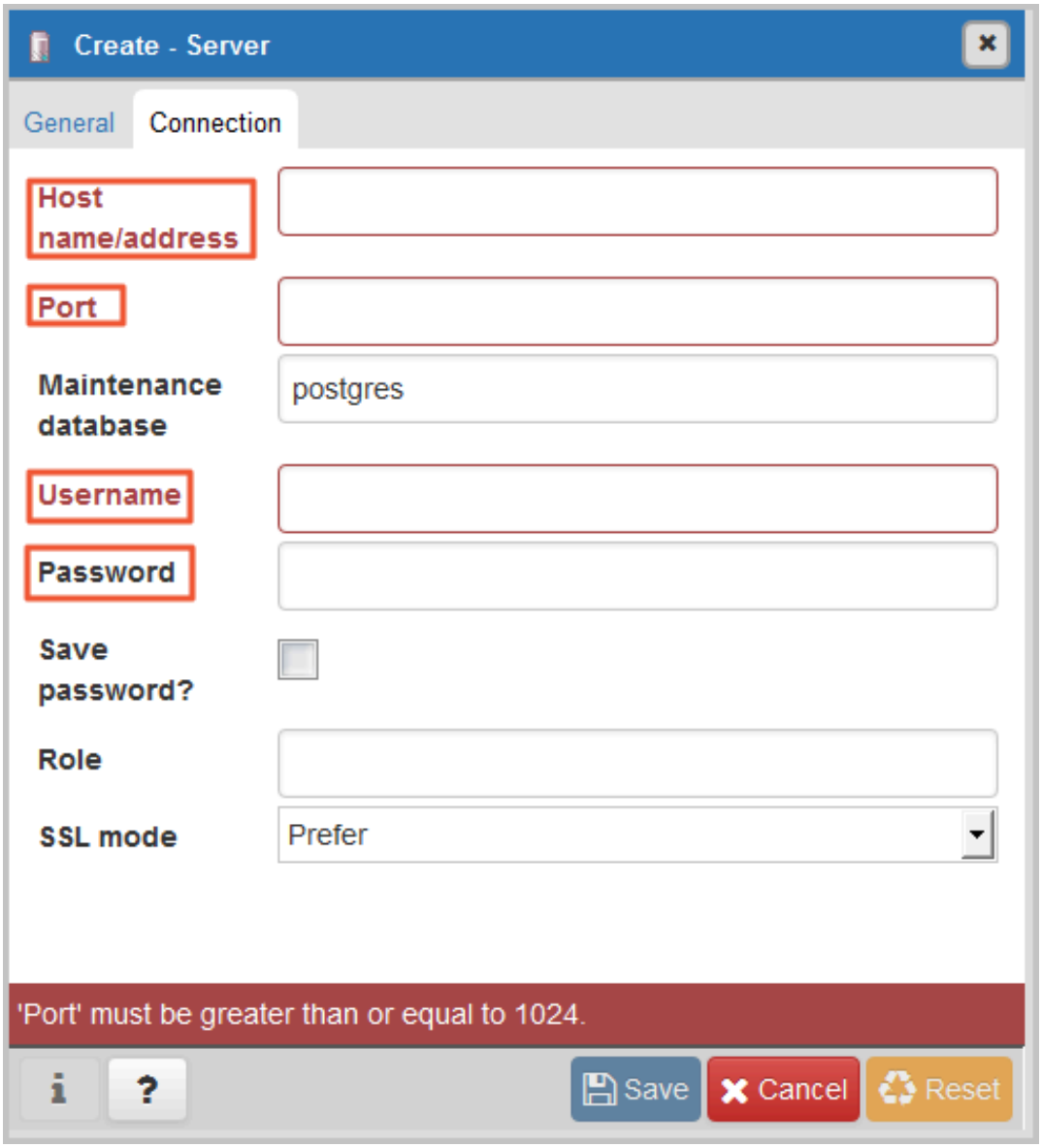
1. **Add the IP address that is used to access the RDS instance to the RDS whitelist. For more information about how to configure a whitelist, see *Configure a whitelist for an RDS for PPAS instance*.**
2. **Start the pgAdmin 4 client.**

3. **Right-click Servers and choose Create > Server from the shortcut menu.**

4. On the General tab of the Create - Server dialog box, enter the name of the server, as shown in the following figure.



5. Click the Connection tab, and enter the information of the target RDS instance, as shown in the following figure.

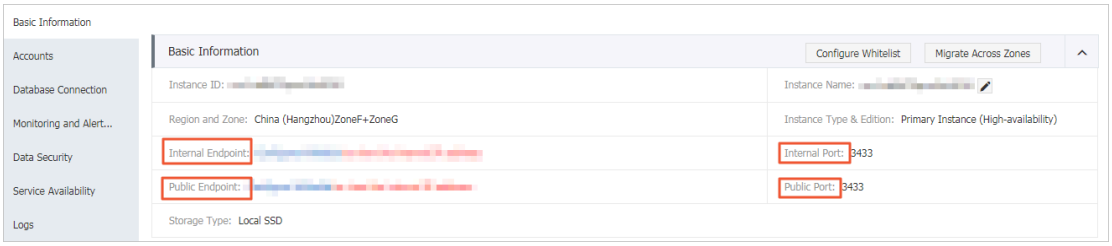


Parameter description:

- Host name/address: the endpoint of the RDS instance. If it is an internal connection, enter the internal endpoint of the RDS instance. If it is an external

connection, enter the public endpoint of the RDS instance. To view the endpoint and the port information of the RDS instance, follow these steps:

a. Log on to the *RDS console*.
b. In the upper-left corner, select the region where the target instance is located.
c. Find the target instance and click its ID.
d. On the Basic Information page, find the internal and public endpoints and port numbers of the RDS instance.

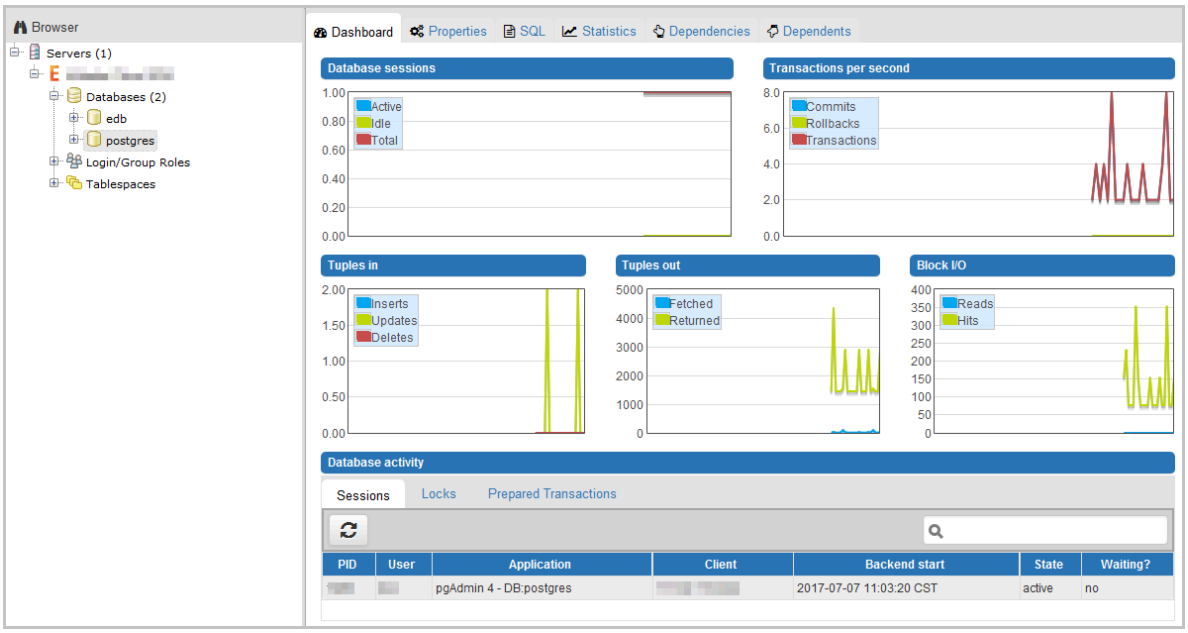


- Port: the port number of the RDS instance. If it is an internal connection, enter the port number for internal connections. If it is an external connection, enter the port number for external connections.
- Username: the name of the premier account for the RDS instance.
- Password: the password of the premier account for the RDS instance.

6. Click Save.
7. If the connection information is correct, choose Servers > Server Name > Databases > edb or postgres. The following page is displayed, which indicates that the connection to the RDS instance is successful.

Note:

Edb and postgres are default system databases of the RDS instance. Do not perform any operation in the two databases.



3.6 Read and write external data files by using the oss_fdw plugin

This topic describes how to read and write external data files by using the oss_fdw plugin. In Alibaba Cloud, you can use this plugin to load data from OSS to an RDS for PostgreSQL or RDS for PPAS instance. You can also write data from an RDS for PostgreSQL or RDS for PPAS instance to OSS.

oss_fdw parameters

Similar to other fdw interfaces, oss_fdw can encapsulate data stored on OSS (external data sources), allowing you to read files on OSS. The process is like reading data from a table. oss_fdw provides unique parameters used for connecting to and parsing file data on OSS.

Note:

- **Currently, oss_fdw can read and write the following file types in OSS: .text/.csv files and .text/.csv files in GZIP format.**
- **The value of each parameter needs to be quoted and cannot contain any useless spaces.**

CREATE SERVER parameters

- `ossendpoint`: **Address (host) used to access OSS from a private network**
- `id`: **OSS account ID**
- `key`: **OSS account key**
- `bucket`: **OSS bucket, assigned after an OSS account is created**

The following parameters are related to error tolerance in import and export modes. If network connectivity is poor, you can reconfigure these parameters to facilitate successful imports and exports.

- `oss_connect_timeout`: **Connection expiration time, measured in seconds. Default value: 10s.**
- `oss_dns_cache_timeout`: **DNS expiration time, measured in seconds. Default value: 60s.**
- `oss_speed_limit`: **Minimum tolerable rate. Default value: 1,024 byte/s (1 Kbit/s).**
- `oss_speed_time`: **Maximum tolerable time. Default value: 15s.**

If the default values of the `oss_speed_limit` and `oss_speed_time` parameters are used, a timeout error occurs when the transmission rate is smaller than 1 Kbit/s for 15 consecutive seconds.

CREATE FOREIGN TABLE parameters

- `filepath`: **File name including a path on OSS.**
  - **A file name contains a path but not a bucket name.**
  - **This parameter matches multiple files in the corresponding path on OSS, and supports file loading to a database.**
  - **Files named in the format of filepath or filepath.*x* can be imported to a database. *x* in filepath.*x* must start from 1 and be consecutive.**

    For example, if there are five files, *filepath*, *filepath.1*, *filepath.2*, *filepath.3*, and *filepath.5*, then the first four files are matched and imported, but the file named *filepath.5* is not.
- `dir`: **Virtual directory on OSS.**
  - **The value of this parameter must end with a slash (/).**
  - **All files (excluding subfolders and files in subfolders) in the virtual directory indicated by this parameter are matched and imported to a database.**

- `prefix`: **Prefix of the path in the data file. Regular expressions are not supported. You can set only one of the these parameters:** `prefix`, `filepath`, **and** `dir`.
- `format`: **File format, which can only be CSV currently.**
- `encoding`: **File data encoding format. It supports common PostgreSQL encoding formats, such as UTF-8.**
- `parse_errors`: **Parsing in error tolerance mode. The errors that occur during the file parsing process are ignored by row.**
- `delimiter`: **Delimiter specified for columns.**
- `quote`: **Quote character for a specified file.**
- `escape`: **Escape character for a specified file.**
- `null`: **Used to nullify the column matching a specified string. For example,** `null 'test'` **is used to set the column whose value is** `test` **to null.**
- `force_not_null`: **Used to un-nullify the value of one or more columns. For example,** `force_not_null 'id'` **is used to set the values of the** `id` **column to empty strings.**
- `compressiontype`: **Used to set whether the file read or written on OSS is compressed and set the compression format. Values:**
  - `none`: **Uncompressed (default value)**
  - `gzip`: **compressed gzip file**
- `compressionlevel`: **Used to set the compression level of the compression format written to OSS. Value range:** `1` **to** `9`**. Default value:** `6`.

Note:

- **The** `filepath` **and** `dir` **parameters need to be specified in the** `OPTIONS` **parameter.**
- **Either the** `filepath` **or** `dir` **parameter must be specified, and they cannot be specified at the same time.**
- **The export mode currently only supports virtual folders, that is, only the** `dir` **parameter is supported.**

Export mode parameters for CREATE FOREIGN TABLE

- `oss_flush_block_size`: **Buffer size for the data written to OSS at a time. Its default value is 32 MB, and the value range is 1 MB to 128 MB.**

- `oss_file_max_size`: **Maximum file size for the data written to OSS (subsequent data is written in another file when the maximum file size is exceeded). Its default value is 1,024 MB, and the value range is 8 MB to 4,000 MB.**
- `num_parallel_worker`: **The number of parallel compression threads in the compression mode in which the OSS data is written, ranging from 1 to 8. Its default value is 3.**

Auxiliary function

FUNCTION oss_fdw_list_file (relname text, schema text DEFAULT 'public')

- **Used to obtain the name and size of the OSS file that an external table matches.**
- **The unit of file size is byte.**

```
select * from oss_fdw_list_file('t_oss');
              name | size

 oss_test/test.gz. 1 | 739698350
 oss_test/test.gz. 2 | 739413041
 oss_test/test.gz. 3 | 739562048
(3 rows)
```

Auxiliary feature

oss_fdw.rds_read_one_file: In read mode, it is used to specify a file that matches the external table. Once it is set, the external table matches only one file that is set during data import.

For example, set oss_fdw.rds_read_one_file = ‘oss_test/example16.csv. 1’;

```
set oss_fdw.rds_read_one_file = 'oss_test/test.gz. 2';
select * from oss_fdw_list_file('t_oss');
              name | size

  oss_test/test.gz. 2 | 739413041
(1 rows)
```

oss_fdw example

```
# (PostgreSQL) Create the plugin
create extension oss_fdw;  ----For PPAS, run: select rds_manage
_extension('create','oss_fdw');
# Create a server instance
CREATE SERVER ossserver FOREIGN DATA WRAPPER oss_fdw OPTIONS
     (host 'oss-cn-hangzhou.aliyuncs.com' ,  id 'xxx',  key 'xxx',
bucket 'mybucket');
# Create an OSS external table
CREATE FOREIGN TABLE ossexample
    (date text,  time text,  open float,
     high float,  low float,  volume int)
     SERVER ossserver
     OPTIONS ( filepath 'osstest/example.csv',  delimiter ', ' ,
```

```
          format 'csv',  encoding 'utf8',  PARSE_ERRORS '100');
# Create a table, to which data is loaded
create table example
        (date text,  time text,  open float,
         high float,  low float,  volume int);
# Load data from ossexample to example.
insert into example select * from ossexample;
# As you can see
# oss_fdw estimates the file size on OSS and formulates a query plan
correctly.
explain insert into example select * from ossexample;
                             QUERY PLAN

 Insert on example (cost=0.00.. 1.60 rows=6 width=92)
   -> Foreign Scan on ossexample (cost=0.00.. 1.60 rows=6 width=92)
         Foreign OssFile: osstest/example.csv. 0
         Foreign OssFile Size: 728
(4 rows)
# Write the data in the example table to OSS.
insert into ossexample select * from example;
explain insert into ossexample select * from example;
                           QUERY PLAN

 Insert on ossexample  (cost=0.00..16.60 rows=660 width=92)
   ->  Seq Scan on example  (cost=0.00..16.60 rows=660 width=92)
(2 rows)
```

oss_fdw usage tips

- **oss_fdw is an external table plugin developed based on the PostgreSQL FOREIGN TABLE framework.**
- **The data import performance is related to the PostgreSQL cluster resources (CPU I/O MEM MET) and OSS.**
- **For expected data import performance, ossendpoint in ossprotocol must match the region where PostgreSQL is located in Alibaba Cloud. For more information, see** *Endpoints*.
- **If the error "oss endpoint userendpoint not in aliyun white list" is triggered during reading of SQL statements for external tables, use these** *regions and endpoints*. **If the problem persists, submit a trouble ticket.**

Error handling

When an import or export error occurs, the error log contains the following information:

- `code`: **HTTP status code of the erroneous request.**
- `error_code`: **Error code returned by OSS.**
- `error_msg`: **Error message provided by OSS.**

- `req_id`: UUID that identifies the request. If you cannot solve the problem, you can seek help from OSS development engineers by providing the req_id.

Timeout errors can be handled by using oss_ext parameters.

For more information about error types, see the following resources:

- *OSS help*
- *PostgreSQL CREATE FOREIGN TABLE*
- *Exception handling*
- *OSS error response*

Hide IDs and keys

If the `id` and `key` parameters for CREATE SERVER are not encrypted, plaintext information is displayed by using `select * from pg_foreign_server`, making the ID and key exposed. The symmetric encryption can be performed to hide the ID and key (use different keys of different instances for further protection of your information). However, to avoid incompatibility with old instances, you cannot use methods similar to GP to add a data type.

Encrypted information:

```
postgres=# select * from pg_foreign_server ;
  srvname  | srvowner | srvfdw | srvtype | srvversion | srvacl |

  srvoptions

-----------+----------+--------+---------+------------+--------
+-----------------------------------------------------------------------------------
----------------------------------
 ossserver |       10 |  16390 |         |            |        | {host
=oss-cn-hangzhou-zmf.aliyuncs.com, id=MD5xxxxxxxx, key=MD5xxxxxxxx,
bucket=067862}
```

The encrypted information is preceded by MD5 (total length: len%8==3). Therefore, encryption is not performed again when the exported data is imported. But you cannot create the key and ID preceded by MD5.

4 Billing management

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

This topic describes how to change the billing method of an RDS for PPAS 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.**

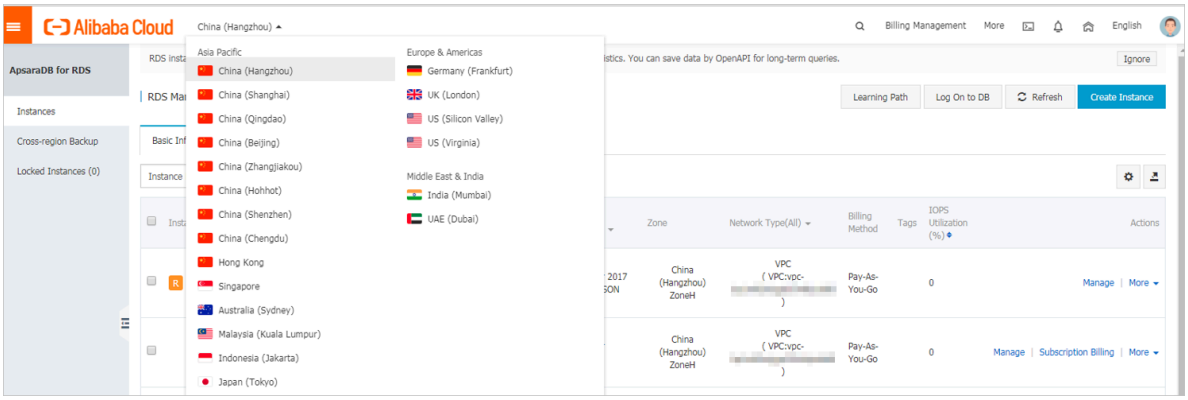
Prerequisites

- **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 PPAS 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.

4.2 Manually renew an RDS for PPAS instance

This topic describes how to manually renew an RDS for PPAS instance. Each subscription-based instance has an expiration date. If an instance is not renewed in time before the instance expires, a service interruption or even data loss may occur.

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

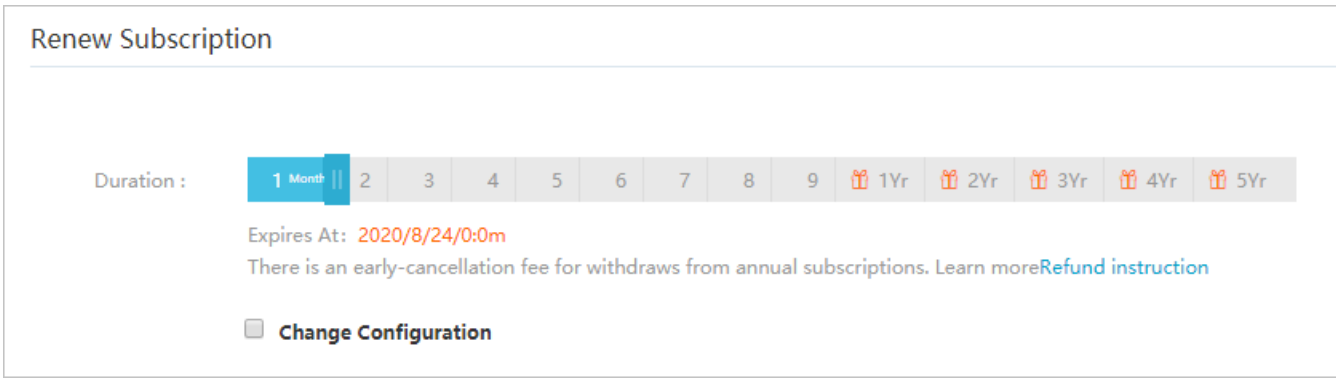
Note:
A pay-as-you-go-based instance does not have an expiration date and no renewal is required.

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 *ApsaraDB for 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 in the Actions column click Renew.**
4. **On the Renew Subscription page, select a duration. The longer the duration, the bigger discount you have.**

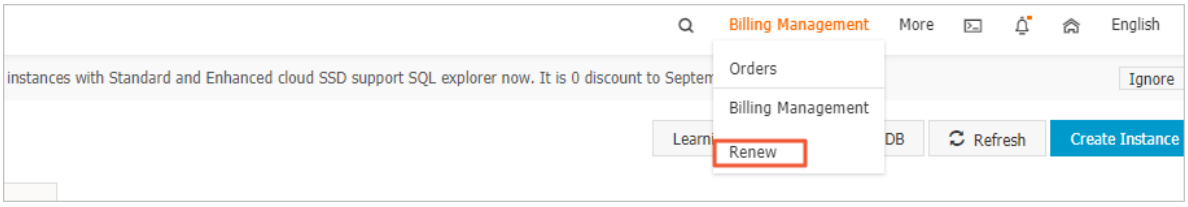


5. **Select Terms of Service, Service Level Agreement, and Terms of Use, and click Pay Now to complete the payment.**

Renew an RDS instance in the Renew console

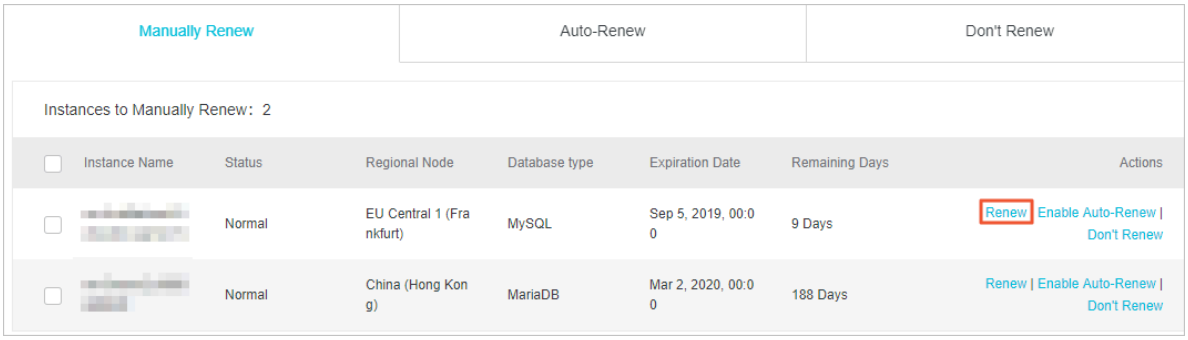
1. **Log on to the *ApsaraDB for RDS console*.**

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, select the service agreement, and click Pay Now to complete the payment.

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 PPAS instance*.

4.3 Automatically renew an RDS for PPAS instance

This topic describes how to automatically renew an RDS for PPAS 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. Enabling auto-renewal guarantees that your business runs smoothly without the need of manual renewal when your instance expires.

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.**

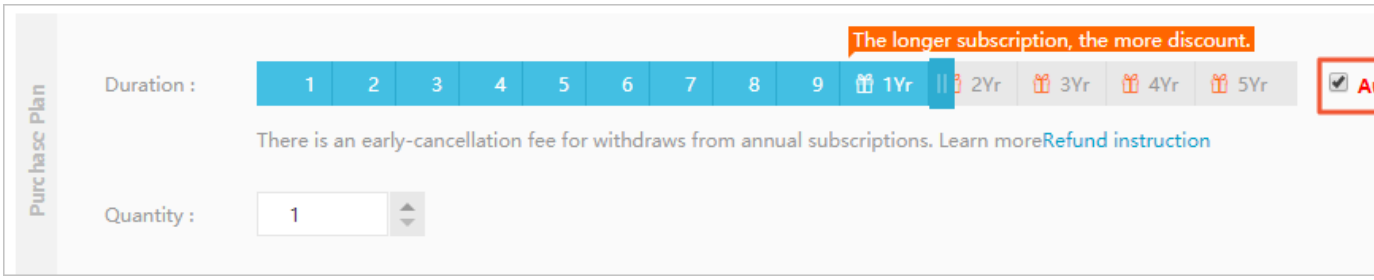
Precautions

- **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 PPAS 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.

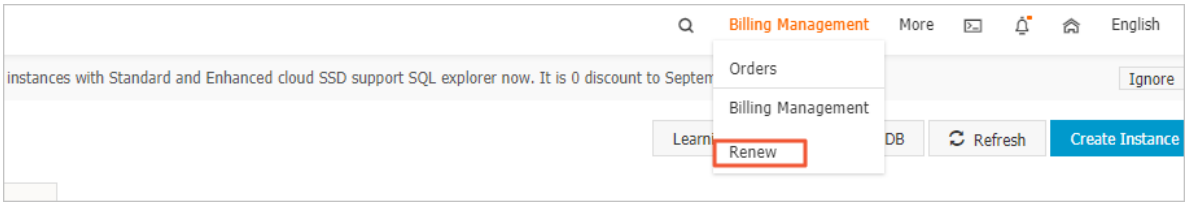


Enable automatic renewal after you purchase an RDS instance

Note:

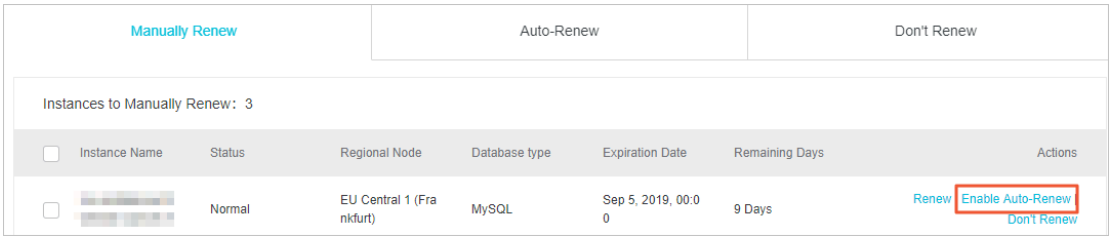
After you enable automatic renewal, the system automatically renews your instance based on the selected renewal duration. For example, if you select a three-month renewal duration, the fees are automatically paid every three months for each renewal.

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.

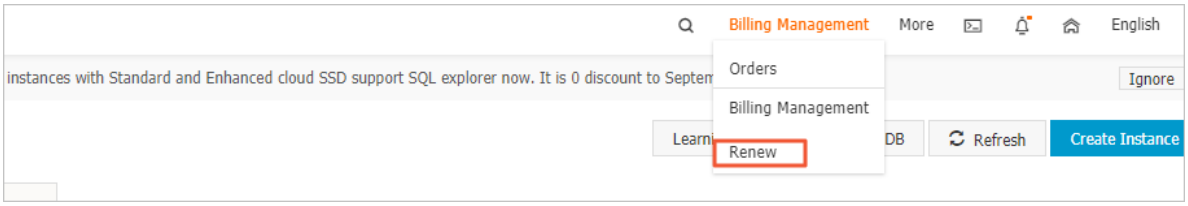


     b. In the displayed dialog box, set Auto-Renew Cycle and click Enable Auto-Renew.
   - Follow these steps to enable auto-renewal for more than one RDS instance:

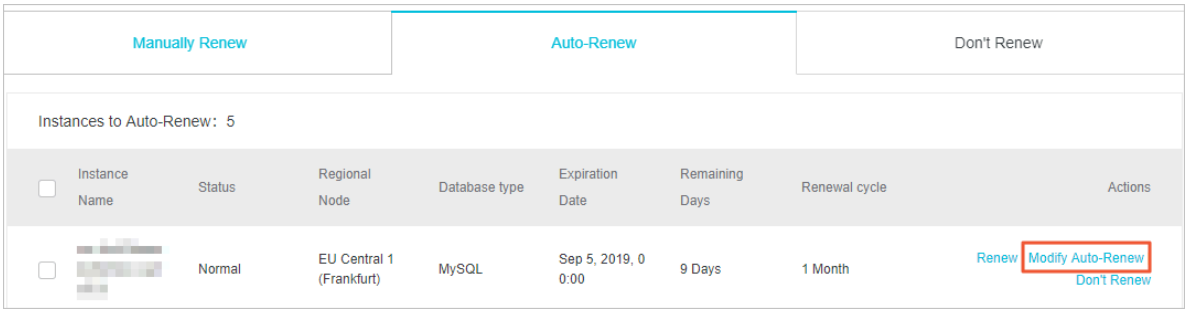
     Select the target RDS instances, and click Enable Auto-Renew below the instance list.
   - In the displayed dialog box, set Auto-Renew Cycle and click Enable Auto-Renew.

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.



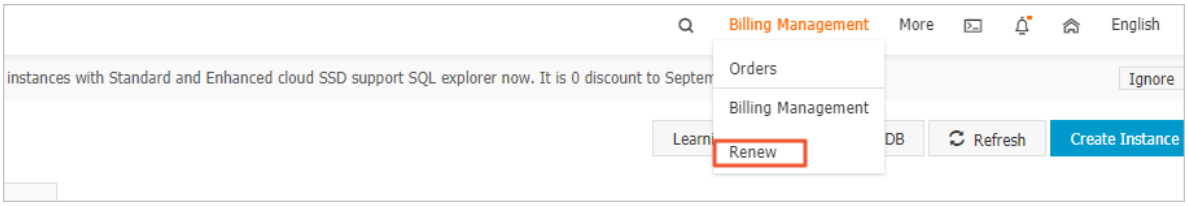
3. In the left-side navigation pane, click ApsaraDB for RDS.
4. On the Auto-Renew tab, find the target RDS instance and in the Actions column click Modify Auto-Renew.



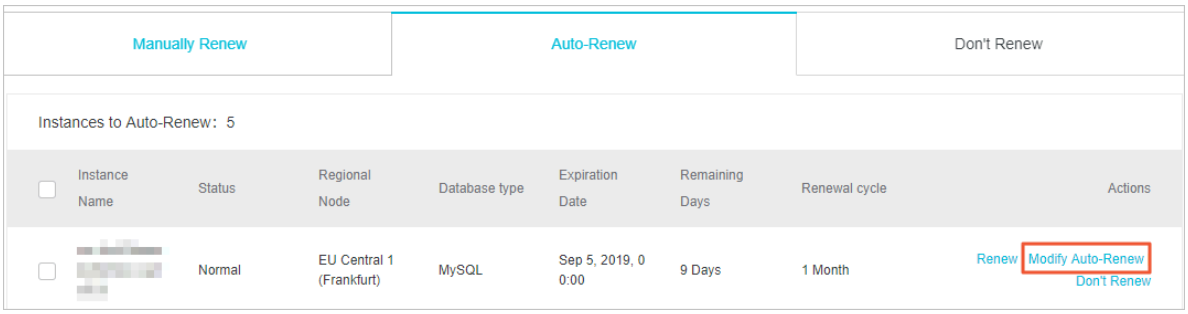
5. **In the displayed dialog box, select Modify Auto-Renew Cycle, select an auto-renew cycle, and click OK.**

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_20	**Used to create an RDS instance.** **Note:** **Automatic renewal is enabled when you create the instance.**
#unique_34	**Used to renew a subscription-based RDS instance.** **Note:** **Automatic renewal is enabled after you create the instance.**

5 Instance management

5.1 Restart an RDS instance

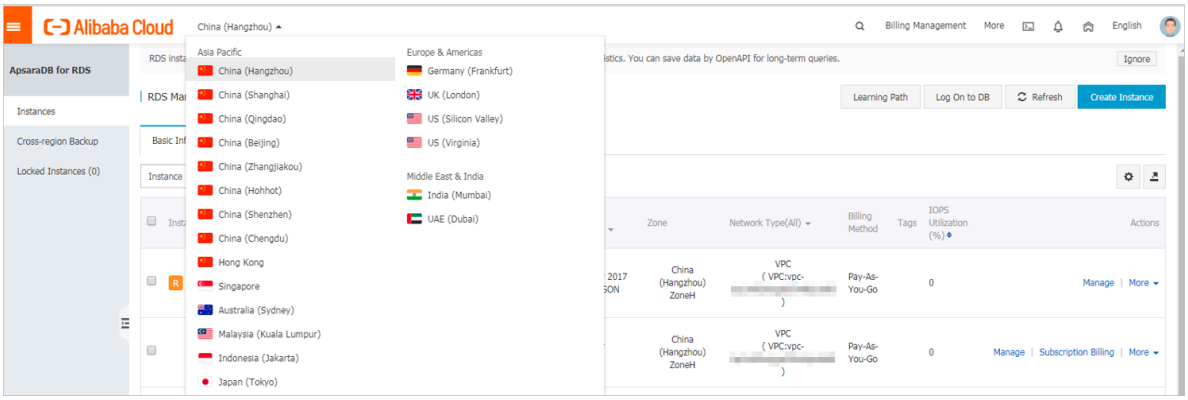
This topic describes how to manually restart an RDS instance in the RDS console if the number of connections exceeds the threshold or any performance issue occurs for the instance.

Impact

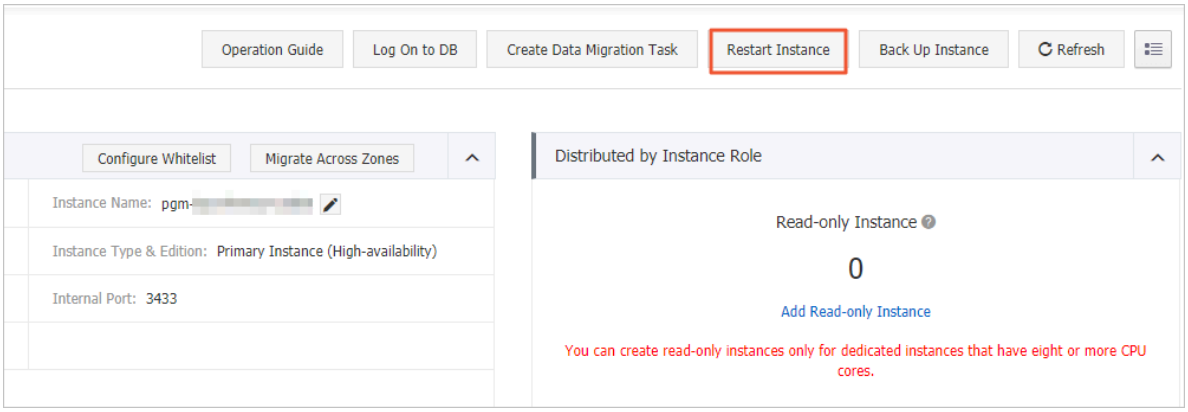
Restarting an RDS instance interrupts connections. Make appropriate arrangements before restarting an RDS instance.

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. 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_37	Used to restart an RDS instance.

5.2 Change the maintenance window of an RDS instance

This topic describes how to change the maintenance window of an RDS instance. To guarantee the stability of ApsaraDB for RDS instances, the back-end system performs maintenance of the instances at irregular intervals. 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.

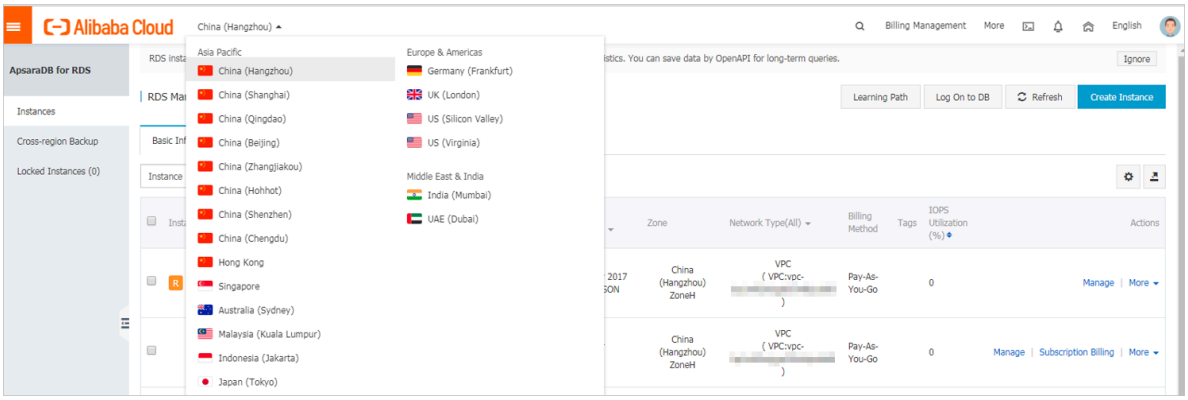
Precautions

- **Before maintenance is performed, ApsaraDB for RDS sends SMS messages and emails to the contacts listed in your Alibaba Cloud accounts.**
- **To guarantee the stability of 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.**

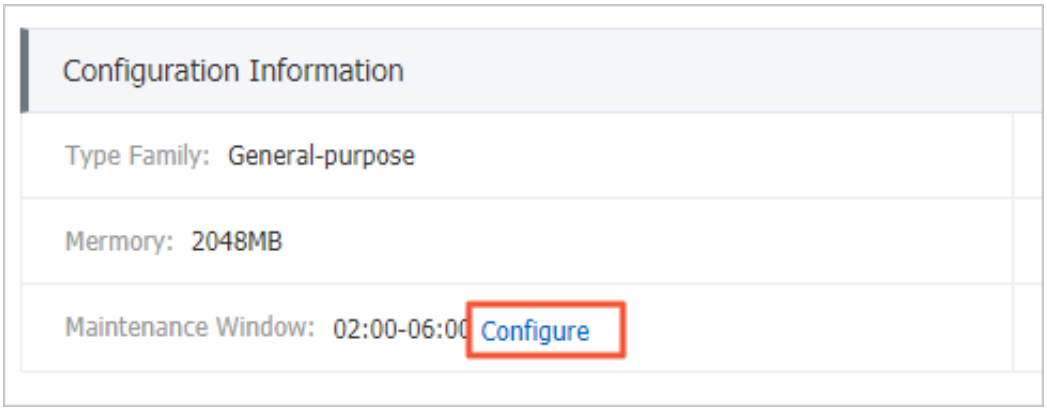
Procedure

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

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



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_39	Used to change the maintenance window of an RDS instance.

5.3 Migrate an RDS for PPAS instance across zones in the same region

This topic describes how to migrate an RDS for PPAS instance across zones in the same region. The attributes, configuration, and connection addresses of the instance remain unchanged after the migration. The time required for the migration varies depending on the data volume of the instance. In typical cases, the migration takes a few hours.

Migration scenarios

Migration scenario	Description
Migrate an RDS instance from one zone to another	**The zone where the RDS instance is located is overloaded or cannot meet the performance requirements of the instance.**
Migrate an RDS instance from one zone to multiple zones	**The master and slave nodes are located in different equipment rooms in different zones to enhance disaster tolerance.** **A multi-zone instance is superior to a single-zone instance because it can survive more disasters. For example, a single-zone instance can survive server and rack faults while a multi-zone instance can survive equipment room faults.**
Migrate an RDS instance from multiple zones to one zone	**This scenario is provided to meet the requirements of specific functions.**

Fees

This function is free of charge. No fee is charged even when you migrate an RDS instance from one zone to multiple zones.

Prerequisites

This function is available only when the region to which your RDS instance belongs has more than one zone.

Precautions

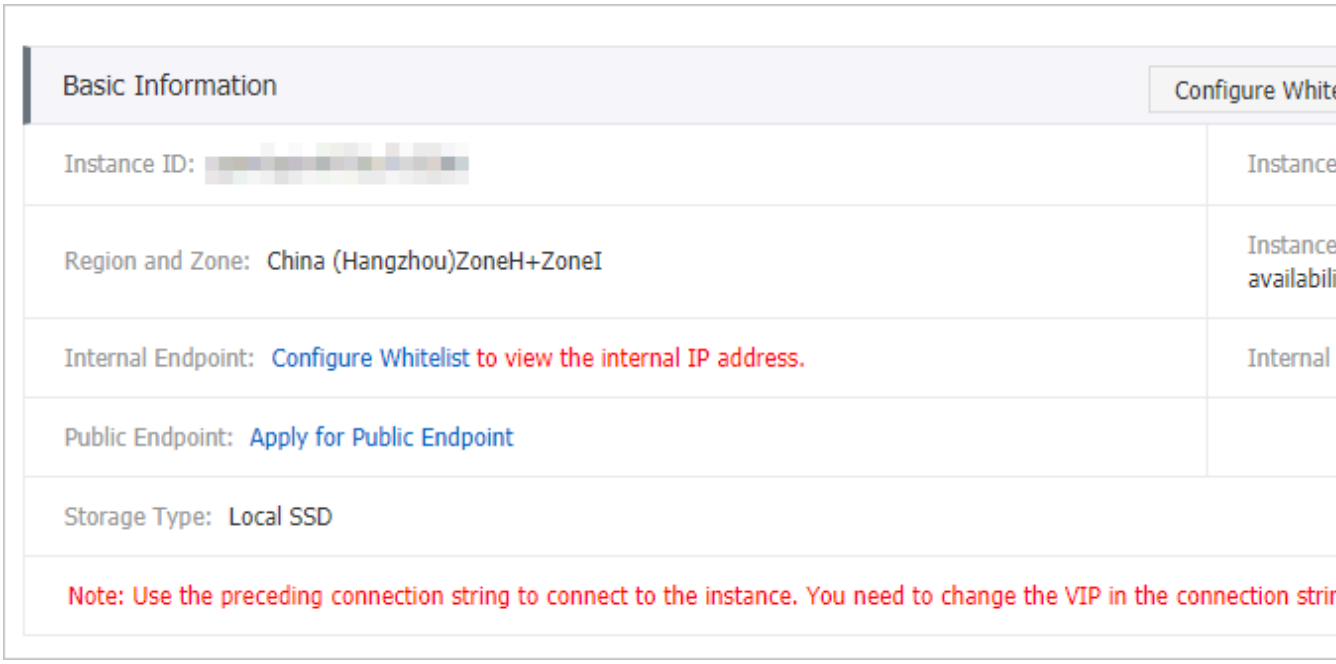
During the migration, the connection to your RDS instance remains unavailable for 30 seconds, and most operations related to databases, accounts, and networks

cannot be performed. Make sure that your application can be automatically reconnected to your RDS instance after the migration. Additionally, perform the migration during off-peak hours.

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 its ID.**
4. **In the Basic Information section of the Basic Information page, click Migrate Across Zones.**

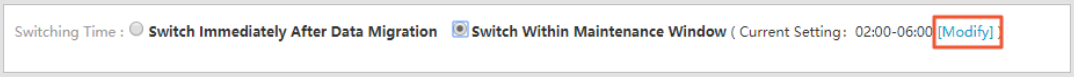


5. In the displayed dialog box, specify the destination zone, VSwitch, and migration time, and click OK.

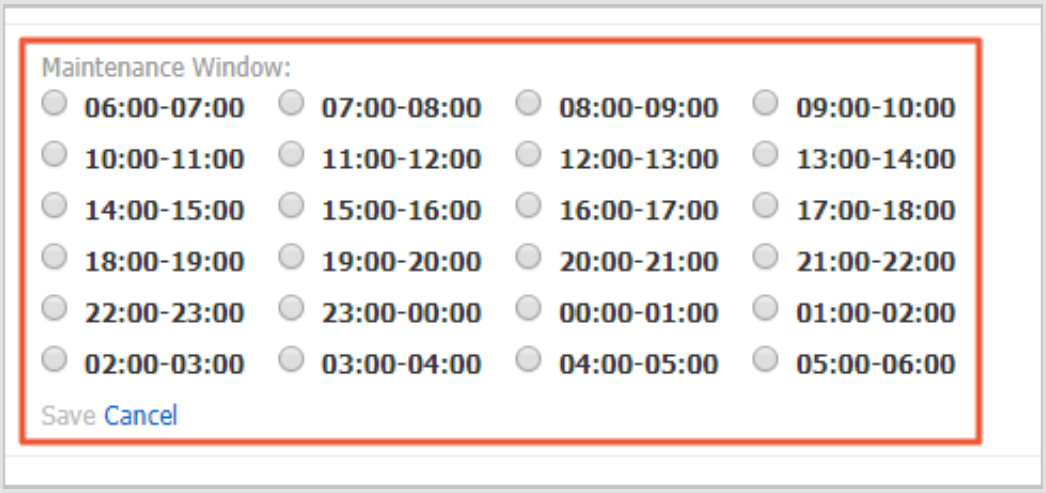
Note:

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

a. Click Change.



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



c. Refresh the page, and perform the migration again.

APIs

API	Description
#unique_41	Used to migrate an RDS instance across zones.

5.4 Switch over services between the RDS for PPAS master and slave instances

This topic describes how to switch over services between the RDS for PPAS master and slave instances.

A High-availability Edition instance has a slave instance, and the data is synchronized between both instances in real time. You can only access the master instance. The slave instance is a backup instance and cannot be accessed. You can switch

your services from the master instance to the slave instance. After the switchover, the original master instance becomes the slave instance.

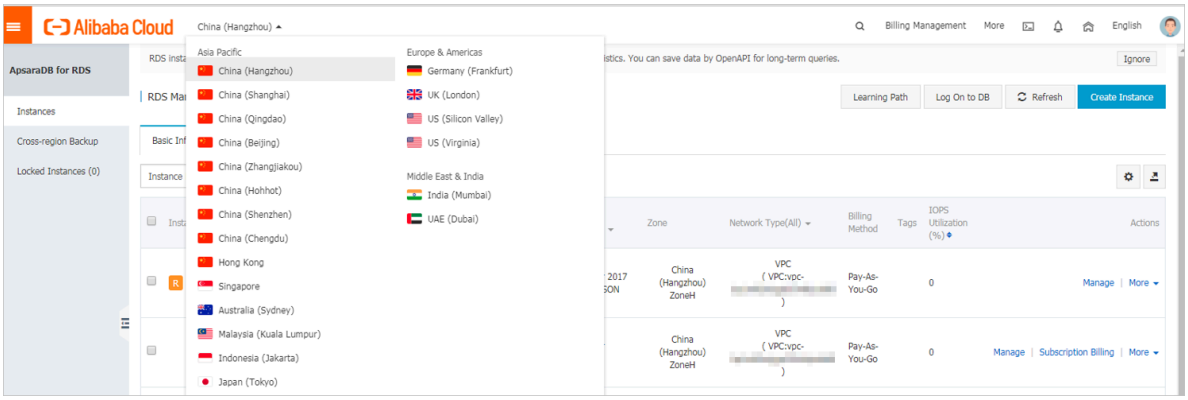
If the master instance cannot be accessed, your business is automatically switched to the slave instance.

Precautions

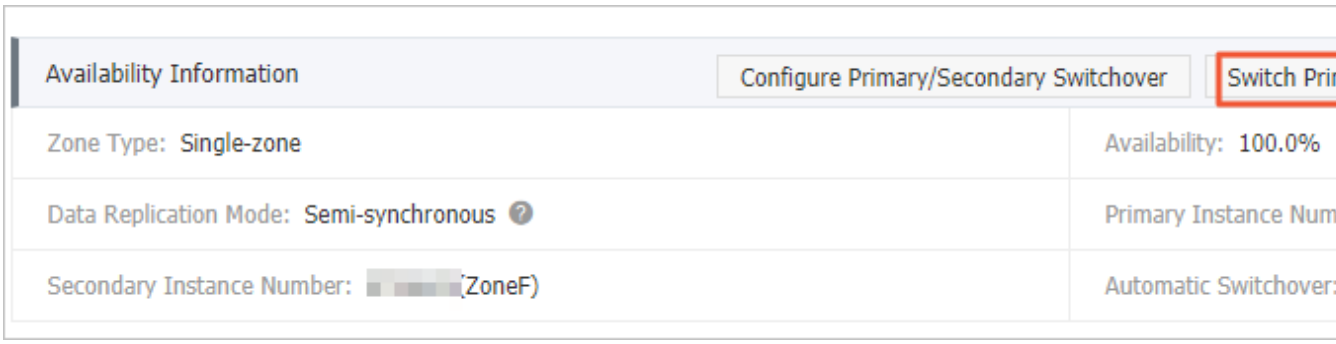
During the switchover, your RDS instance may be disconnected. Make sure that your application can automatically reconnect to your RDS instance after the switchover.

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.

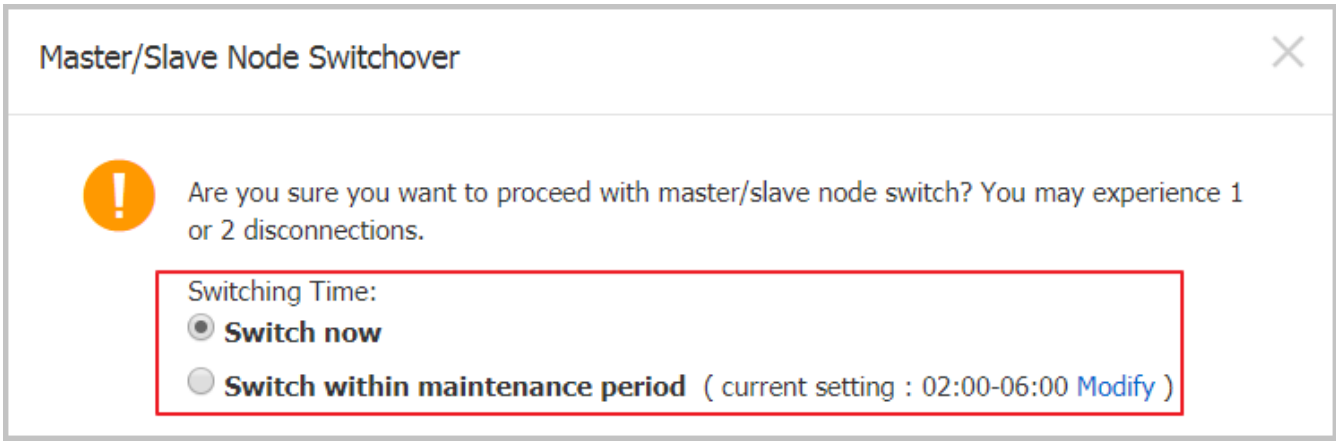


3. Find the instance and click the instance ID.
4. In the left-side navigation pane, click Service Availability.
5. In the `Availability Information` section, click Switch Primary/Secondary Instance.



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

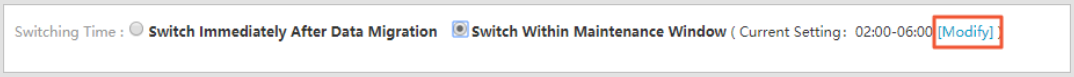
   During the switch, operations such as managing the databases and accounts and switchover the network types cannot be performed. Therefore, we recommend that you select Switch Within Maintenance Window.



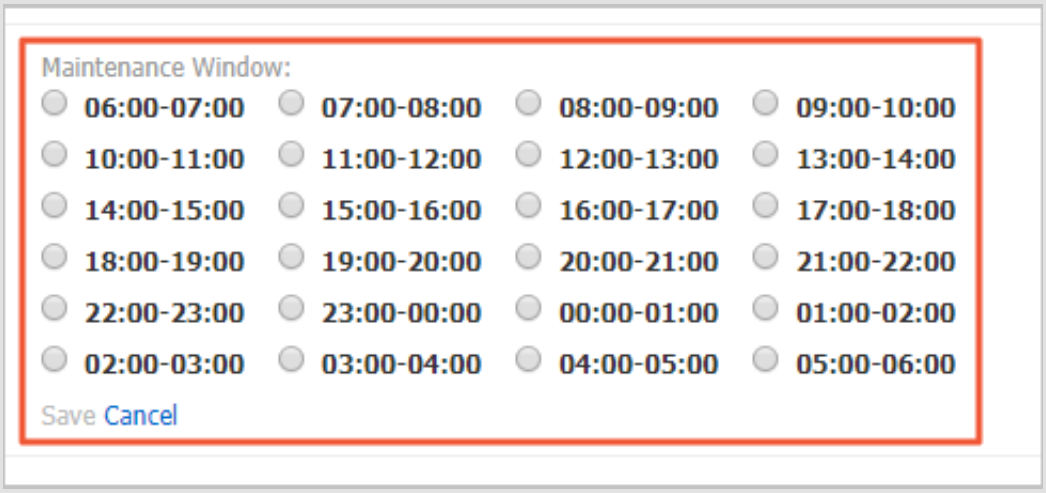
Note:

If you want to change the maintenance window, follow 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	Switches between the master and slave instances.

5.5 Change the network type of an RDS for PPAS instance

This topic describes how to change the network type of an RDS for PPAS instance.

Network types

- **Classic network: Instances in a classic network are not isolated. Access control is implemented for instances by using whitelists.**
- **Virtual Private Cloud (VPC): A VPC is an isolated network environment. We recommend that you use VPC because it is more secure.**

  You can customize the routing table, IP address range, and gateway of the VPC. To smoothly migrate applications to the cloud, you can use a leased line or VPN to connect your own data center to a VPC on the cloud to make a virtual data center.

Note:

- **You can use the classic network or VPC and switch between the network types for free.**
- **For PostgreSQL instances, you must switch the IP whitelist mode to the enhanced whitelist mode before switching the network type. For more information, see** *#unique_45*.

Switch from VPC to classic network

Precautions

- **After the network type of an RDS instance is switched to classic network, the endpoints remain unchanged, but the corresponding IP addresses change.**
- **After the network type of an RDS instance is switched to classic network, ECS instances in VPCs cannot access the RDS instance by using the internal endpoint . Make sure that you change the endpoint on the application.**
- **Switching the network type may result in a disconnection of 30 seconds. To avoid impacts that arise from this operation, we recommend that you perform the**

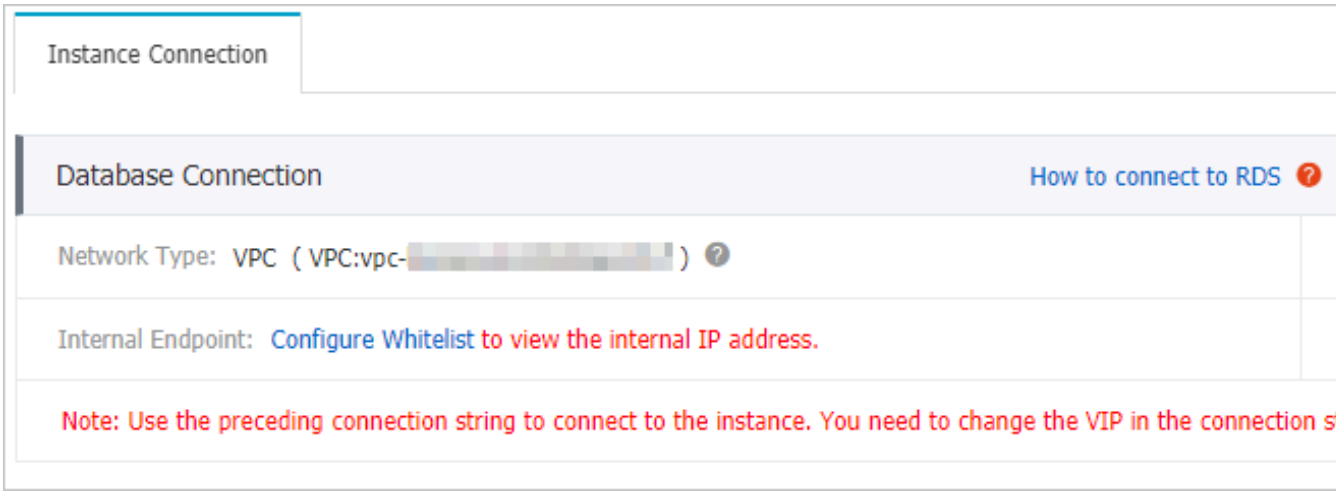
switching during off-peak hours, or configure automatic reconnection policies for your application.

- Instances of PostgreSQL 11 High-availability Edition (cloud disk), PostgreSQL 10 High-availability Edition (cloud disk), and PostgreSQL 10 Basic Edition do not support the classic network. Therefore, you cannot switch these instances to the classic network.

Procedure

1. Log on to the *ApsaraDB for 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. In the Database Connection section, click Switch to Classic Network.



6. In the message that appears, click OK.

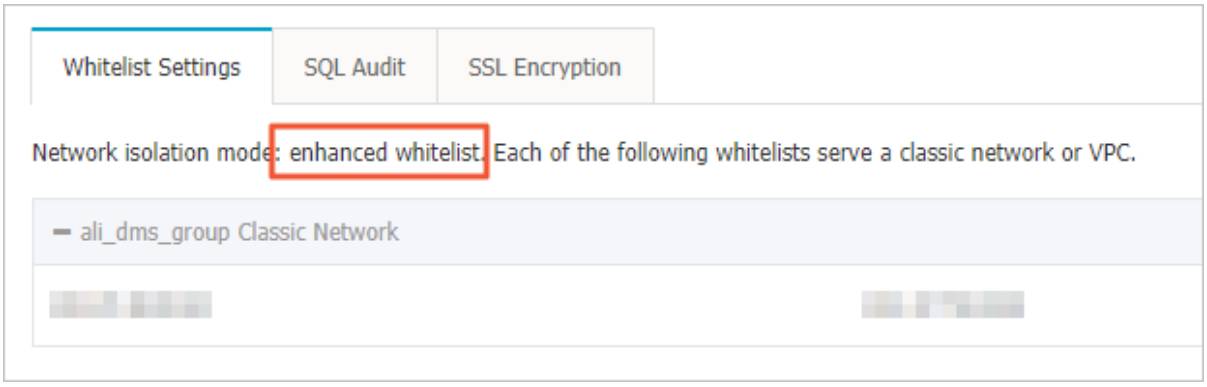
   After the network type is switched, only ECS instances in classic networks can access the RDS instance over the internal network. Make sure that you configure the endpoint of the RDS instance on the ECS instance in the classic network.

7. Configure the whitelist of the RDS instance to allow access from the ECS instance over the internal network.

   - If the RDS instance applies the standard whitelist mode, as shown in the following figure, you must add the internal endpoint of the ECS instance in the classic network to any whitelist of the RDS instance.

   - If the RDS instance applies the *enhanced whitelist mode*, as shown in the following figure, you must add the internal endpoint of the ECS instance in the classic network to the default classic network whitelist of the RDS instance. If there is no classic network whitelist, you must create a new whitelist.

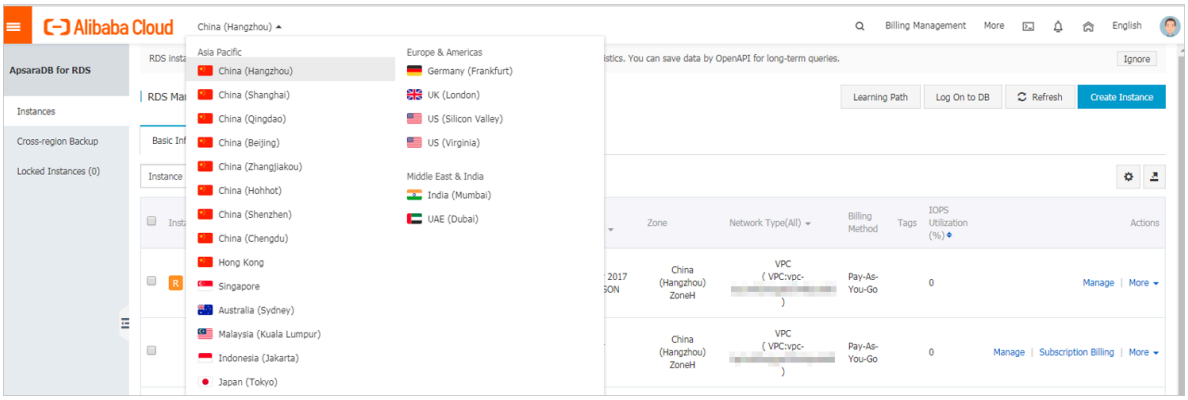
     

Switch from classic network to VPC

Procedure

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

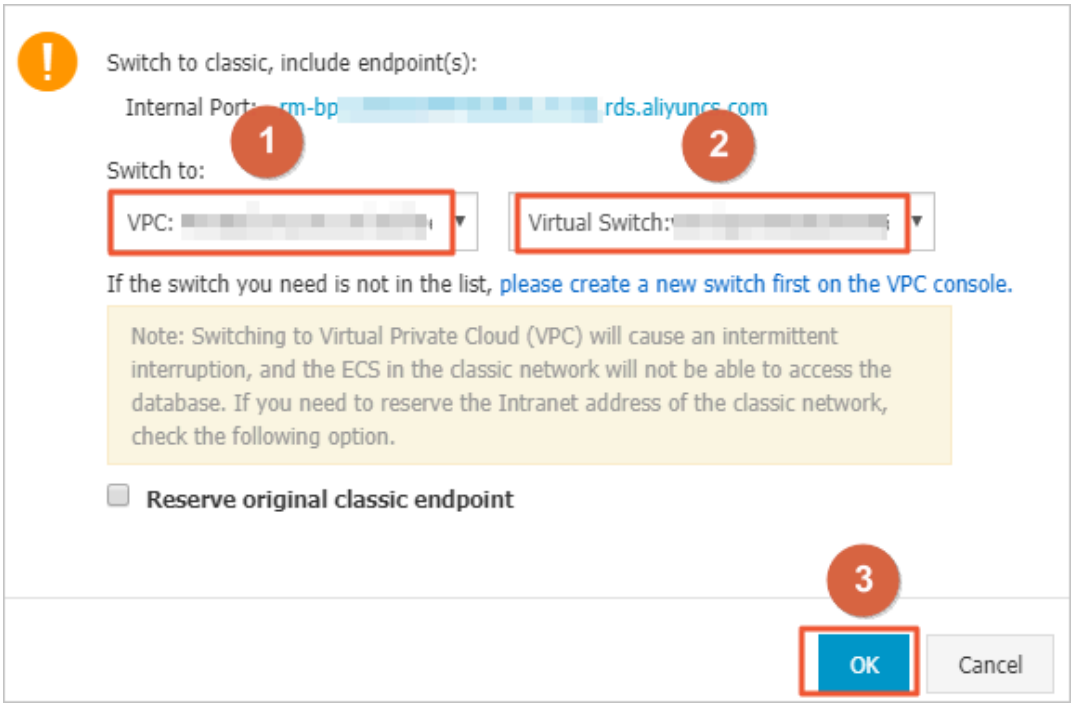
2. In the upper-left corner, select the region where the target RDS instance is located.



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Database Connection .
5. Click Switch to VPC.
6. In the dialog box that appears, select a VPC and a VSwitch, and specify whether to retain the classic network address.
   - Select a VPC. We recommend that you select the VPC where your ECS instance is located. Otherwise, the ECS and RDS instances cannot connect to each other

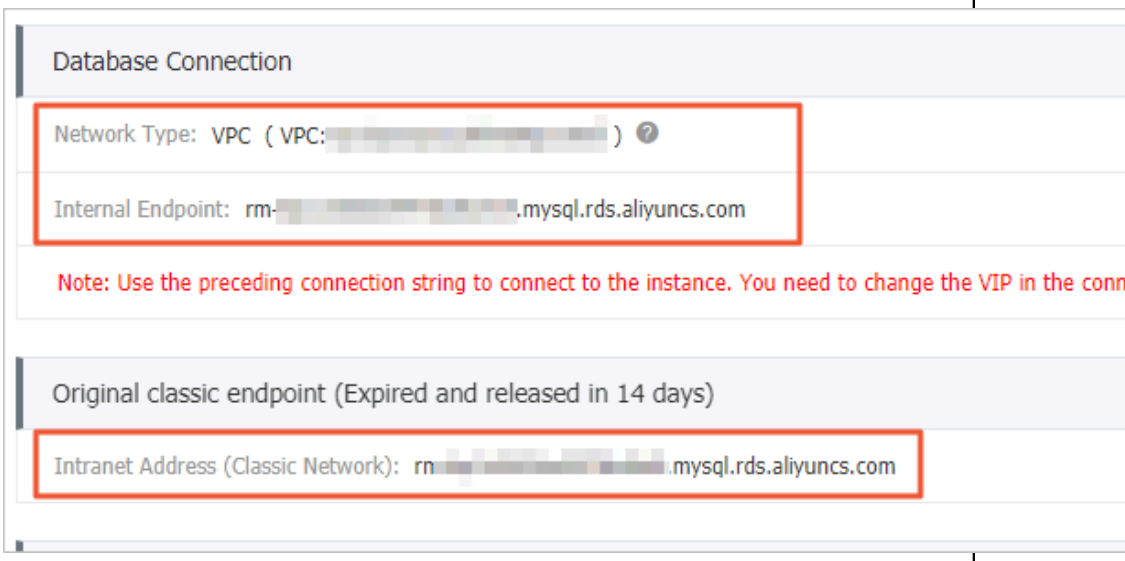
over the internal network unless *Express Connect* or *VPN Gateway* are created to connect the two VPCs.

- Select a VSwitch. If there is no VSwitch in the VPC that you select, as shown in the following figure, you must create a VSwitch in the zone where the instance is located. For more information, see *Manage VSwitches*.



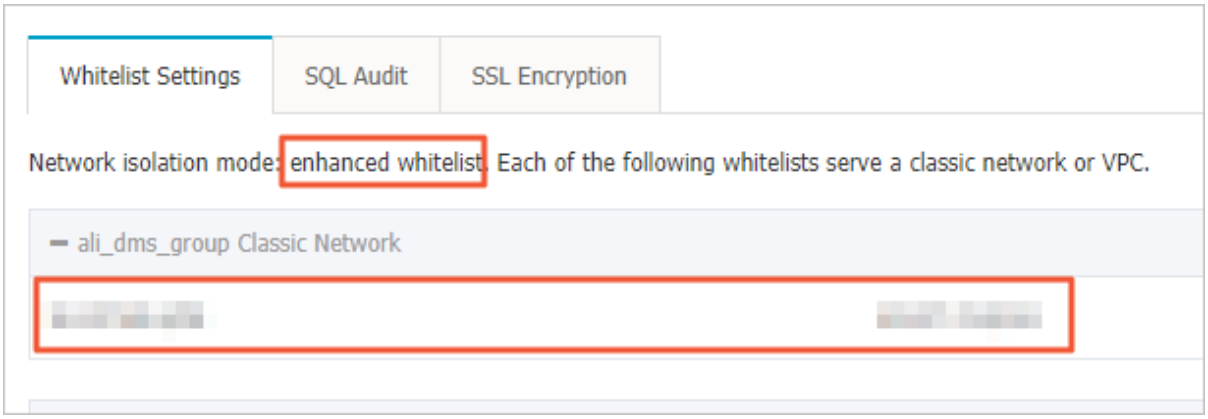
- Select or clear Reserve Original Classic Endpoint as needed. The following table describes the details.

Action	Description
Clear	The classic network address is not retained. The original classic network address is changed to the VPC address. If you do not retain the classic network address, the RDS instance will be disconnected for 30 seconds, and the access from the ECS instance in the classic network to the RDS instance over the internal network is immediately disconnected when you switch the network type.

Action	Description
Select	The classic network address is retained, and a new VPC address is generated, as shown in the following figure. It indicates that the *hybrid access mode* is enabled, and the RDS instance can be accessed by ECS instances in both a classic network and a VPC. If you retain the classic network address, the RDS instance will not be disconnected when you switch the network type. The internal access from the ECS instance in the classic network to the RDS instance is only disconnected when the classic network address expires. Before the classic network address expires, make sure that the VPC address has been configured in the ECS instance in the VPC to smoothly migrate your services to the VPC. The system will send an SMS message to the phone number bound to your Alibaba Cloud account every day in the seven days before the classic network address expires.  For more information, see *Configure a hybrid access solution to smoothly migrate an RDS instance from the classic network to a VPC*.

7. Add the internal IP address of the ECS instance in the VPC to the VPC whitelist of the RDS instance, so that the ECS instance can access the RDS instance over the

internal network, as shown in the following figure. If there is no VPC whitelist, you must create a new whitelist.



8. Perform one of the following operations as needed:
   - If you retain the classic network address, you must configure the VPC address of the RDS instance in the ECS instance that is in the VPC.
   - If you do not retain the classic network address, the access from the ECS instance in the classic network to the RDS instance over the internal network is immediately disconnected when you switch the network type. You must configure the VPC address of the RDS instance in the ECS instance that is in the VPC.

> **Note:**
> If you need to use the ECS instance in the classic network to access the RDS instance in the VPC, you can use the *ClassicLink* function or migrate the ECS instance to the VPC.

APIs

API	Description
#unique_52	Used to change the network type of an RDS instance.

5.6 Release an RDS for PPAS instance

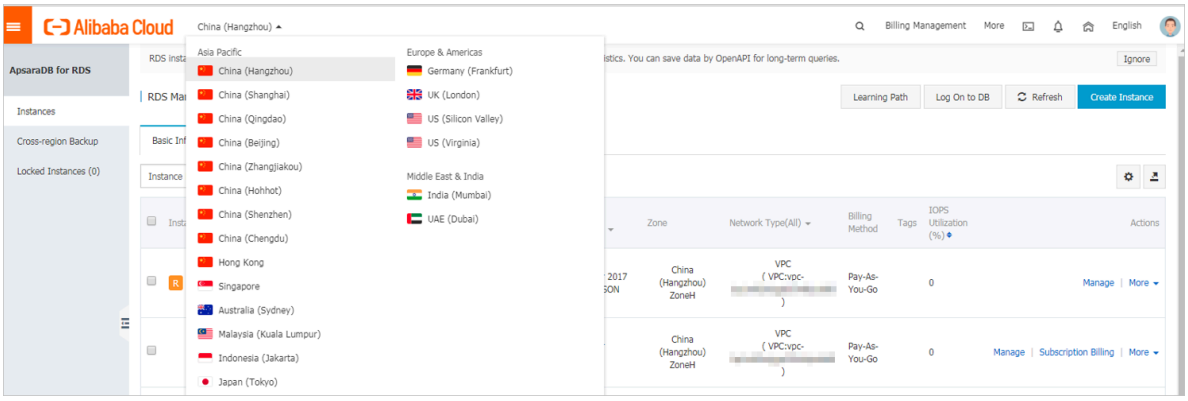
This topic describes how to release an RDS for PPAS instance, which can use the pay-as-you-go or subscription billing method.

> **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:**

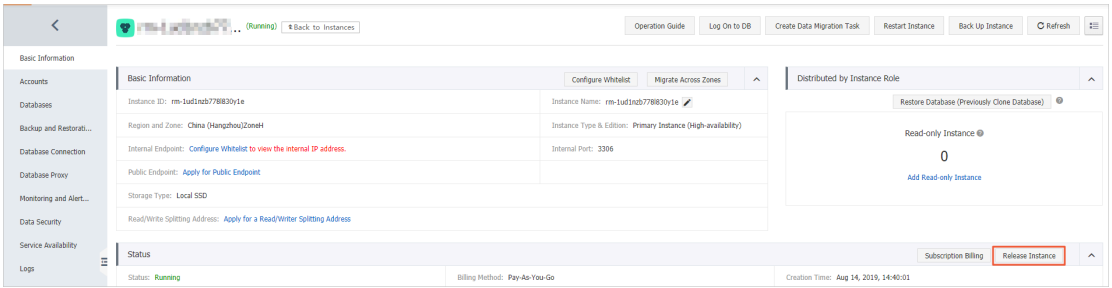
   - **Method 1:**

     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.)

5.7 Change the configuration of an RDS for PPAS instance

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

You can upgrade or downgrade the configuration of an RDS for PPAS 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

If you want to horizontally scale the read capability of an RDS for PPAS instance, you can create read-only instances. For more information, see *#unique_55* and *#unique_56*.

Configuration item	Description
CPU and Memory	All PPAS DB engine versions and editions support the CPU and memory change.

Configuration item	Description
Capacity	All PPAS DB engine versions and editions allow you to increase storage capacity. You can only decrease the storage capacity of a subscription 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_58*.

Prerequisites

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

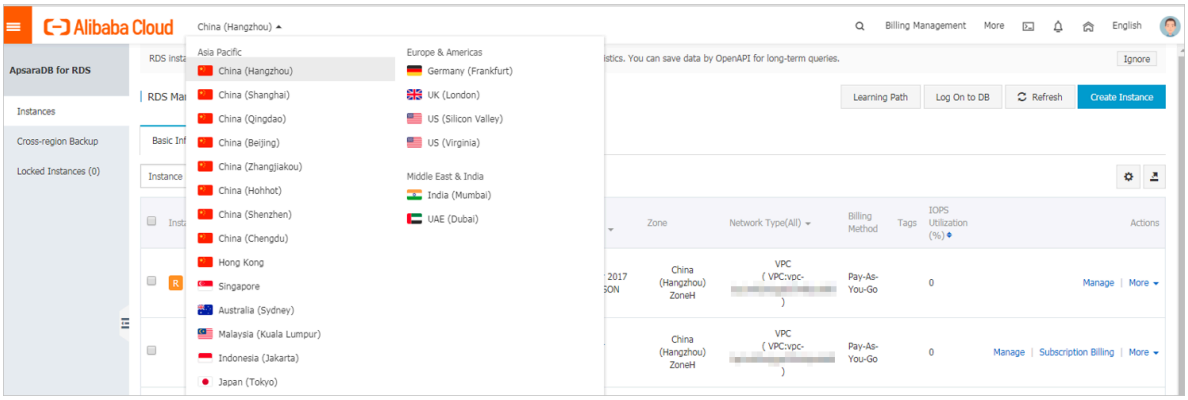
Precautions

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.

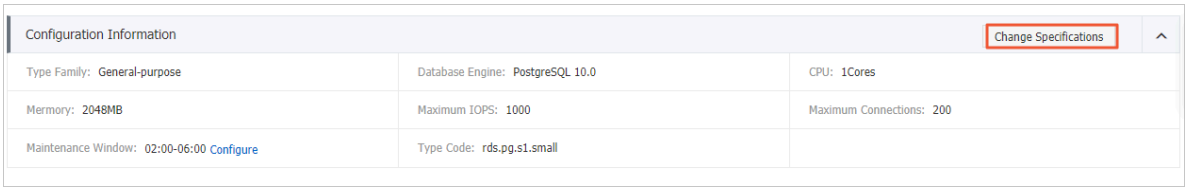
Procedure

1. Log on to the *RDS console*.

2. 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 Configuration Information section and click Change Specifications.

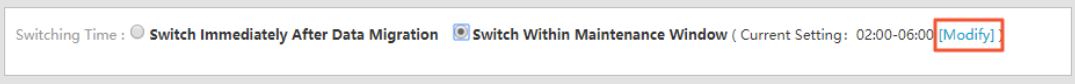


5. Optional. If the RDS instance uses the subscription billing method, click Next in the displayed dialog box.
6. On the Change Specifications page, change the instance configuration. For more information, see *Configuration items*.
7. Specify the time at which you want to change the configuration.
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

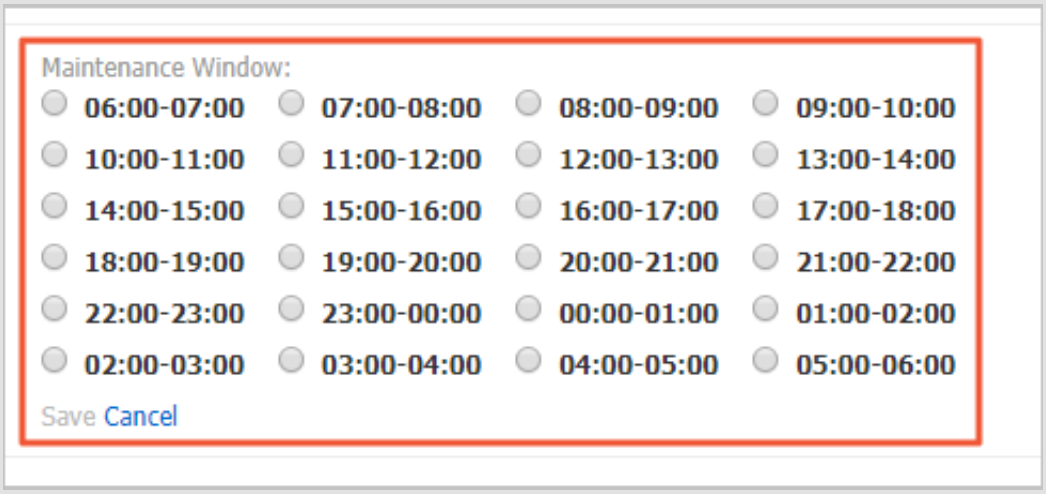
Note:

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.

5.8 Reconfigure parameters for an RDS for PPAS instance

This topic describes how to use the console or API to view and reconfigure some parameters for an RDS for PPAS 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.

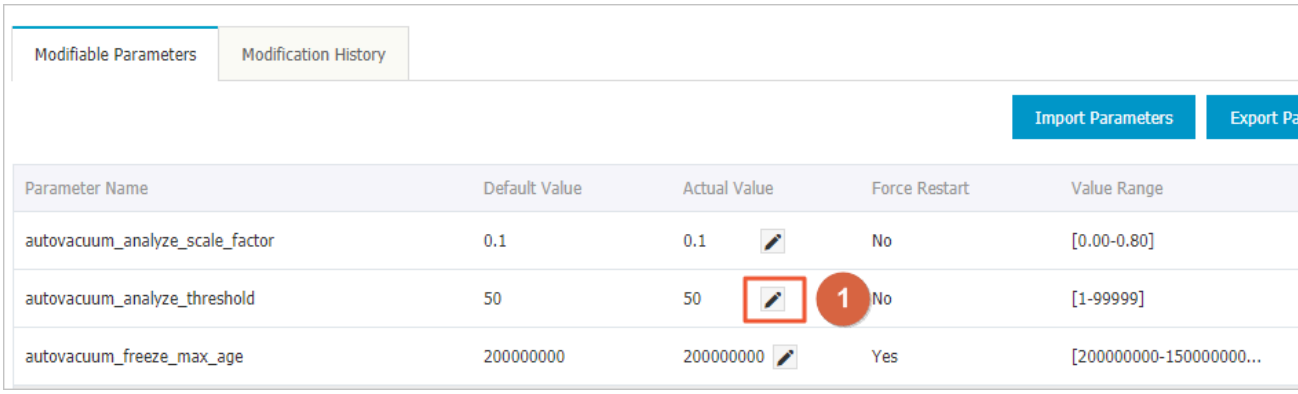
   - To reconfigure only one parameter of the RDS instance, follow these steps:

     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:

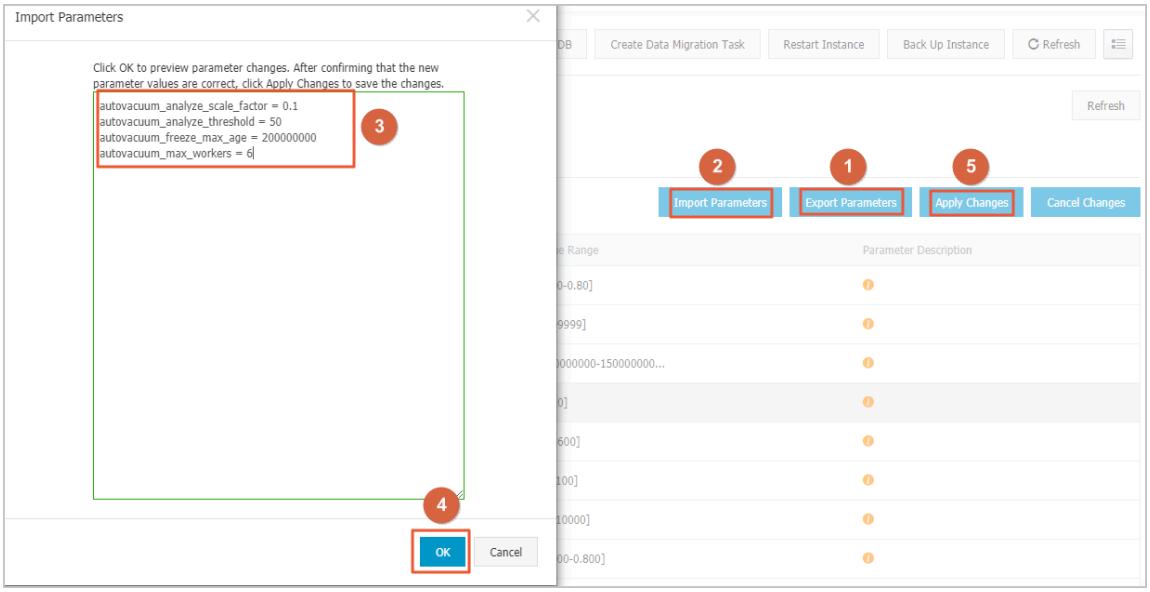
     a. In the upper-right corner, click Export Parameters to export the parameters as a file to your computer.

     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_60*
- *#unique_61*
- *#unique_62*

Parameter reference

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

5.9 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.**

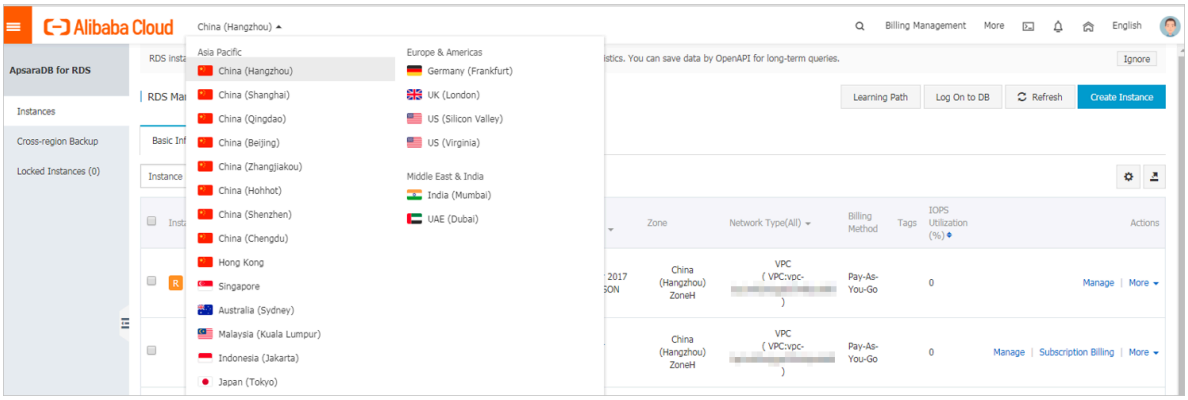
   The instance is unlocked after renewal.

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.**

6 Account management

6.1 Create an account for an RDS for PPAS instance

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

Before using an RDS for PPAS instance, you must create a premier account for it in the RDS console. Then, you can create and manage databases by using the premier account in the DMS console.

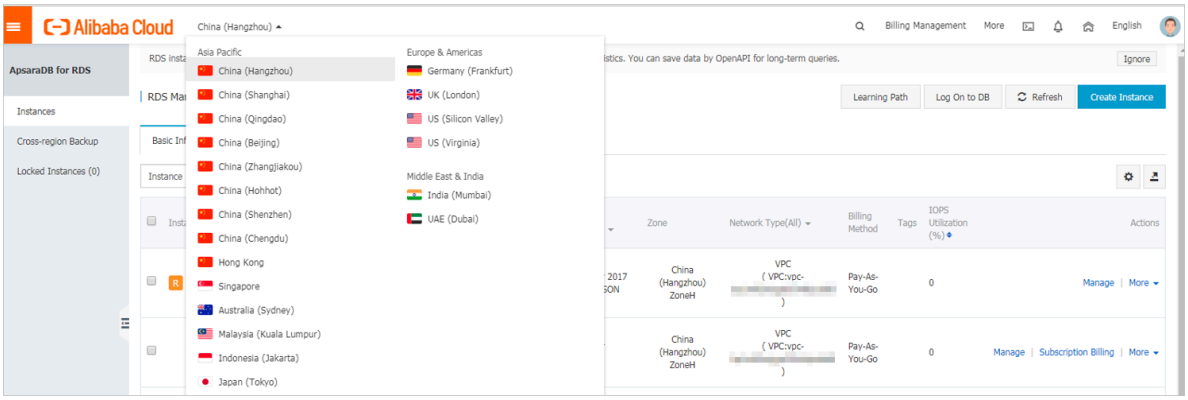
Precautions

- **The databases in an RDS instance share all resources provided by the instance . You can create and manage one premier account and more than one standard account by using SQL statements.**
- **If you want to migrate an on-premises database to an RDS instance, you must create the same accounts and databases in the RDS instance as those in the on-premises database.**
- **When assigning account permissions for each database, follow the minimum permission' principle and consider service roles to create accounts. Alternativ ely, rationally assign read-only and read/write permissions. When necessary, you can split accounts and databases into smaller units so that each account can only access data for its own services. If the account does not need to write data to a database, assign the read-only permission for the account.**
- **For database security purposes, set strong passwords for the accounts and change the passwords regularly.**
- **The premier account cannot be deleted after it is created.**

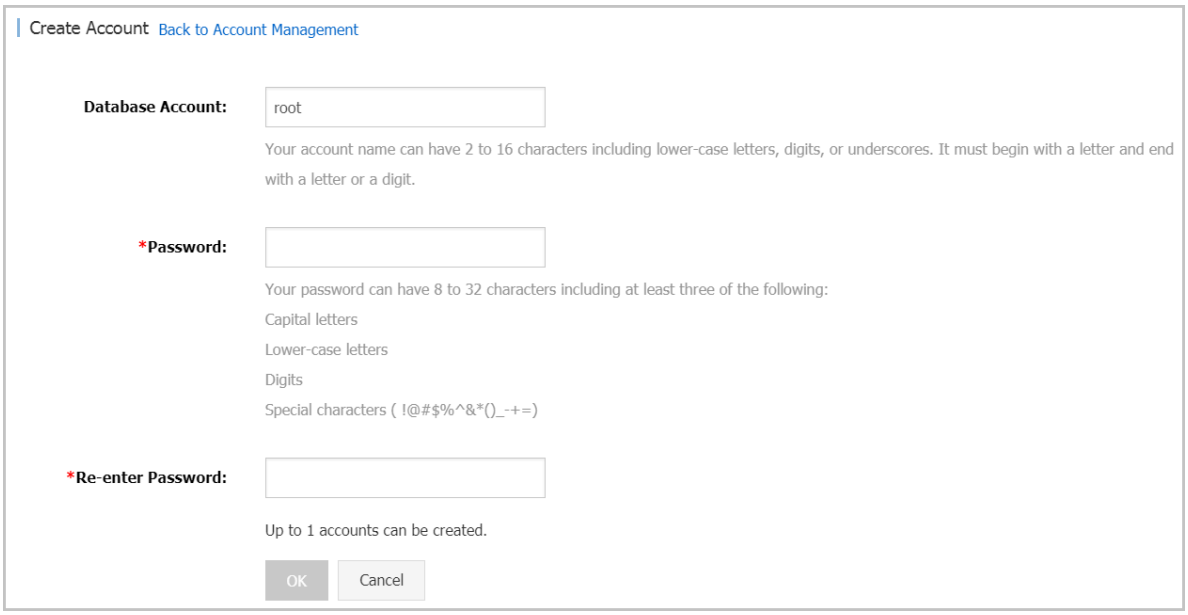
Procedure

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 its ID.
4. In the left-side navigation pane, click Accounts.
5. Click Create Initial Account.
6. Enter the account information.



Parameter description:

- **Database Account: The name of the premier account. It contains 2 to 16 characters including the lowercase letters, digits, and underscores (_). It must begin with a letter and end with a letter or digit.**
- **Password: The password of the premier account. It contains 8 to 32 characters including at least three of the following types of characters: uppercase**

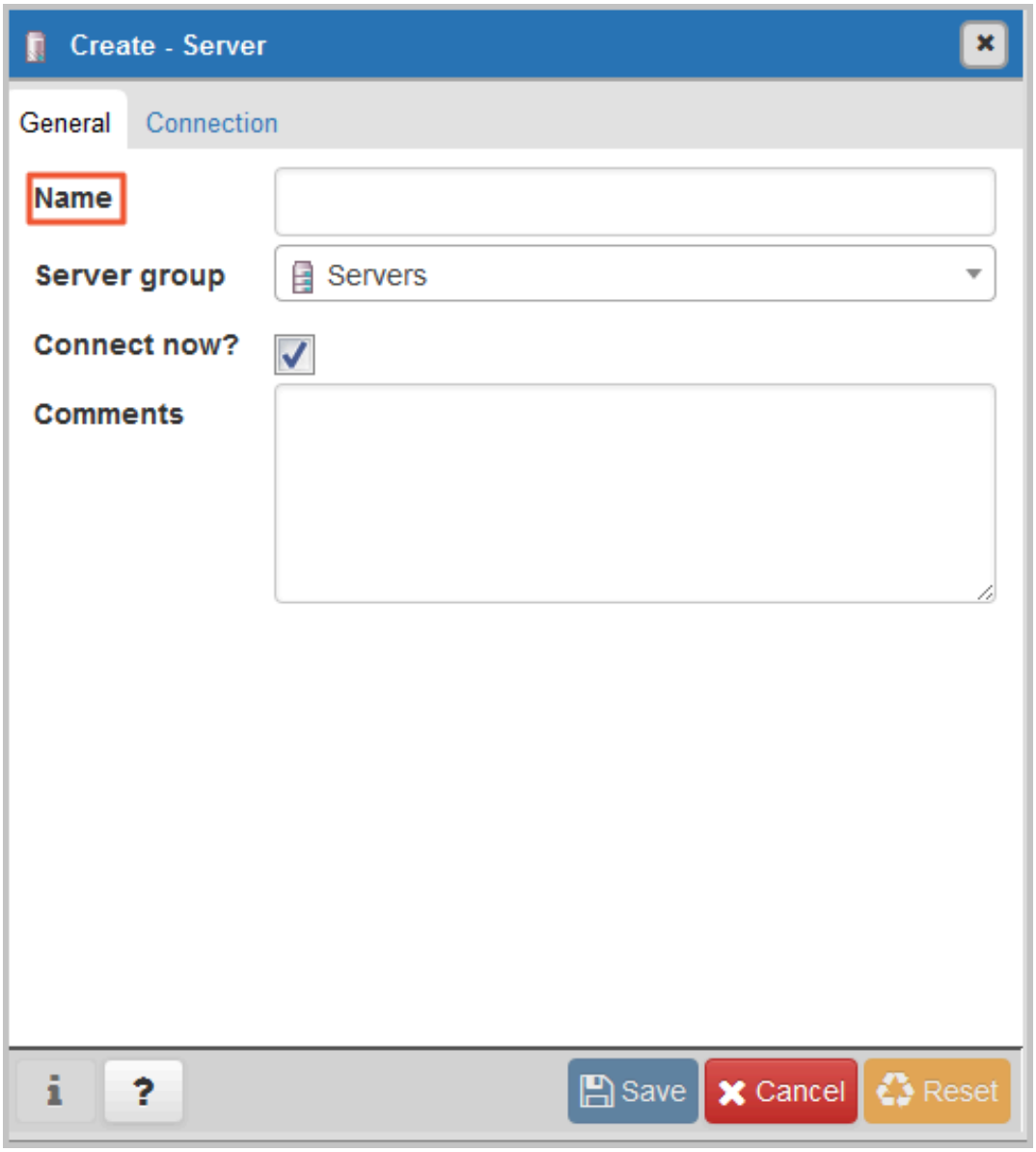
letters, lowercase letters, digits, and special characters. The allowed special characters are as follows:

! @ # $ % ^ & * ( ) _ + - =

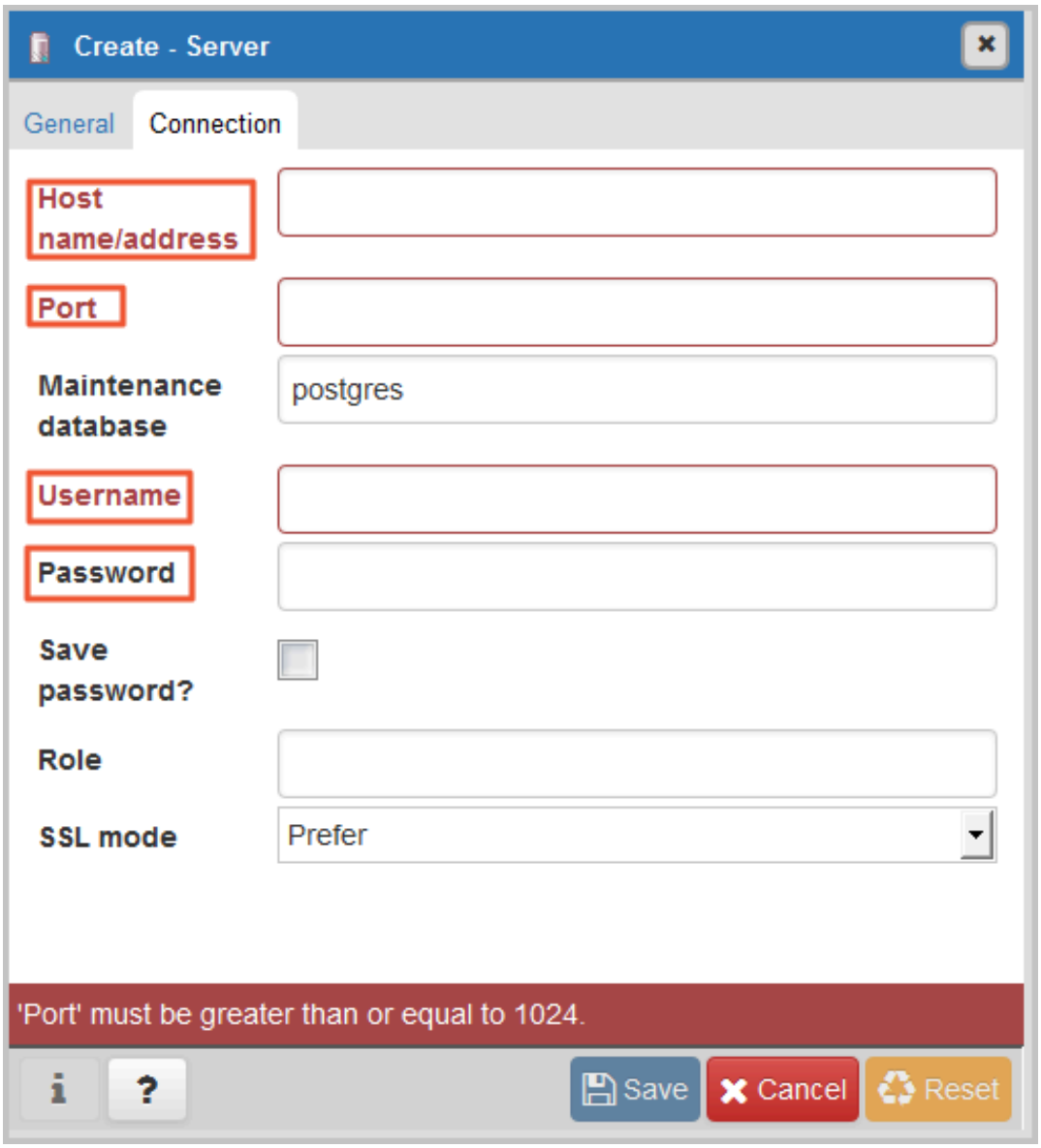
- Re-enter Password: Re-enter the password to make sure that the password is entered correctly.

7. Click OK.
8. Add the IP address that is allowed to access the RDS instance to the RDS whitelist. For more information, see *Configure a whitelist for an RDS for PPAS instance*.
9. Start the pgAdmin 4 client.
10. Right-click Servers and choose Create > Server from the shortcut menu.

11. In the Create Server dialog box, click the General tab and enter the server name.



12. Click the Connection tab and enter the information about the instance to be connected.



Parameter description:

- Host name/address: The internal or public endpoint of the RDS instance. To obtain the internal and public endpoints and ports of the RDS instance, follow these steps:
  a. Log on to the *RDS console*.
  b. In the upper-left corner, select the region where the target RDS instance is located.
  c. Find the target RDS instance and click the instance ID.

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

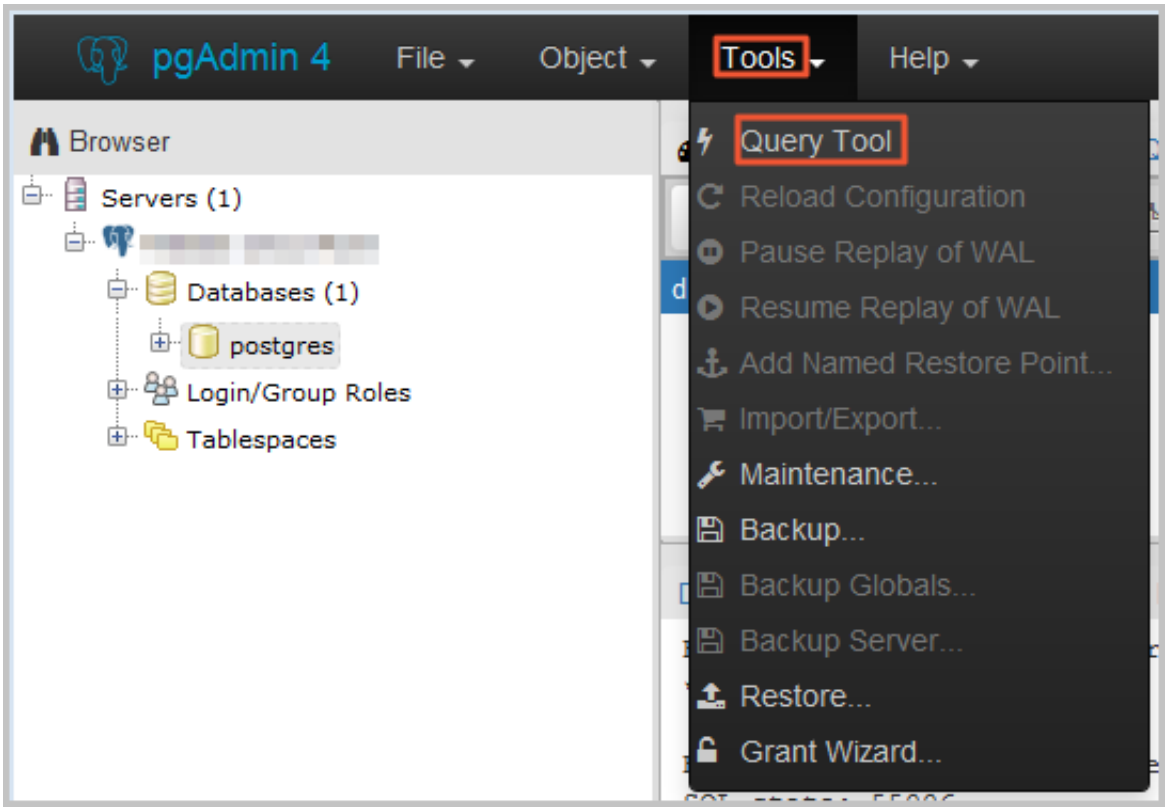
- Port: The internal or public port numbr of the RDS instance.
- Username: The username of the premier account for the RDS instance.
- Password The password of the premier account for the RDS instance.

13. Click Save.

14. Choose Servers > *Server name* > Databases > postgres. If the connection information is correct, the page shown in the following figure is displayed, indicating that a connection is established.

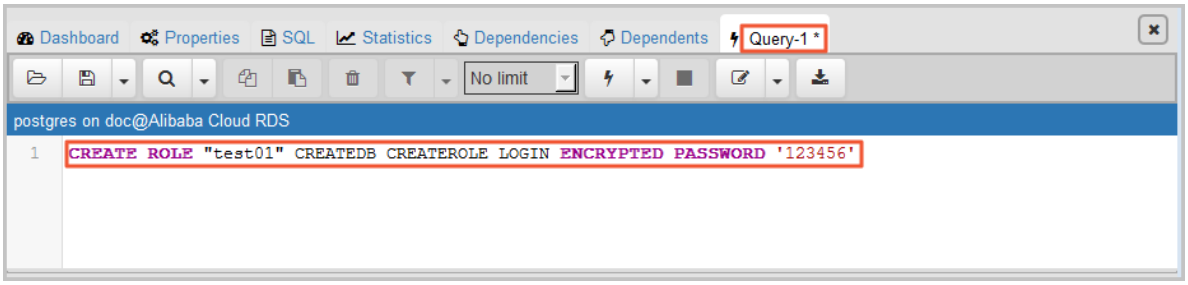
Note:
postgres is the default database of the RDS instance. Do not perform any operation in this database.

15. Select postgres and choose Tools > Query Tool.

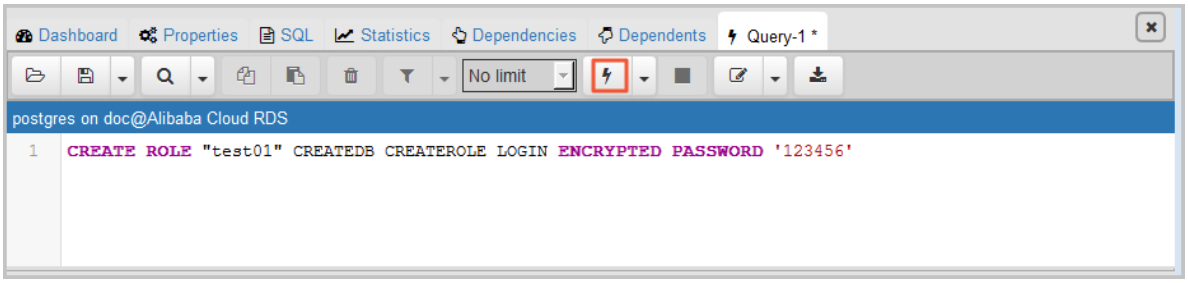


16. On the Query-1 tab, enter the following command to create an account:

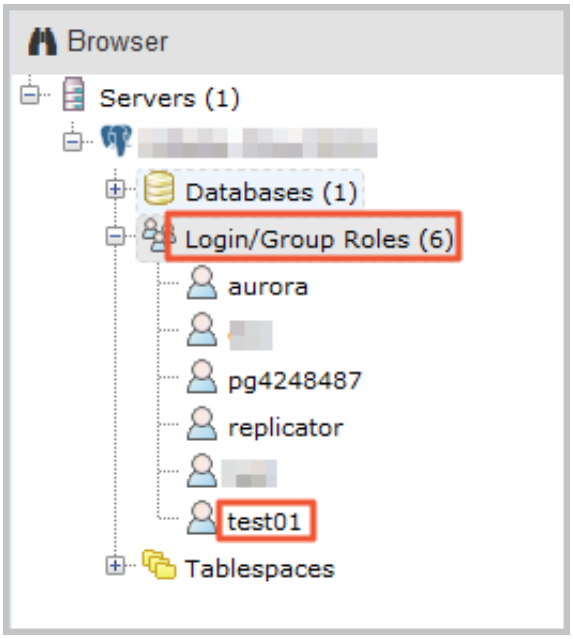
```
CREATE ROLE "username" CREATEDB CREATEROLE LOGIN ENCRYPTED PASSWORD
 'password';
```



17. Click the execute or refresh button.



18. When the command is executed successfully, indicating that the account is created, right-click Login/Group Roles and choose the refresh button to view the new account.



APIs

API	Description
#unique_26	Used to create an account for an RDS instance.

6.2 Reset the password of an account for an RDS for PPAS instance

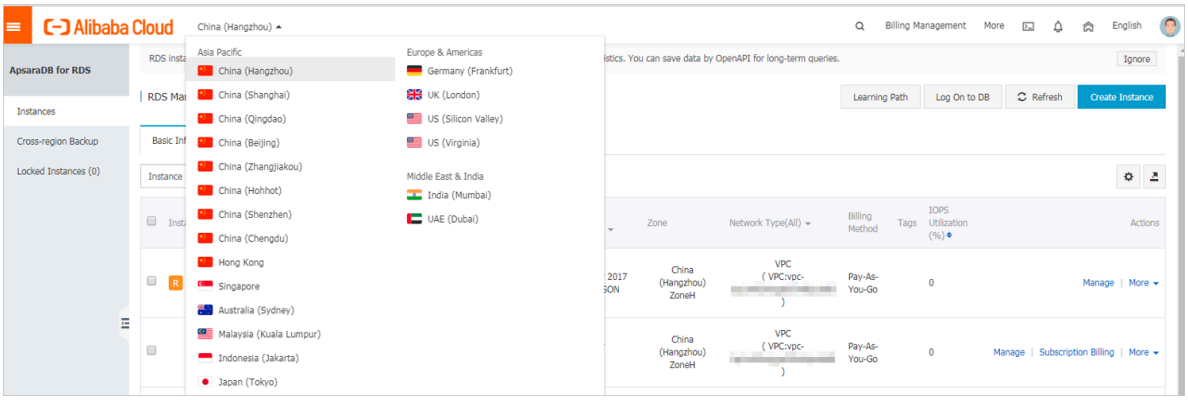
This topic describes how to reset the password of an account for an RDS for PPAS instance in case that the password is lost.

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

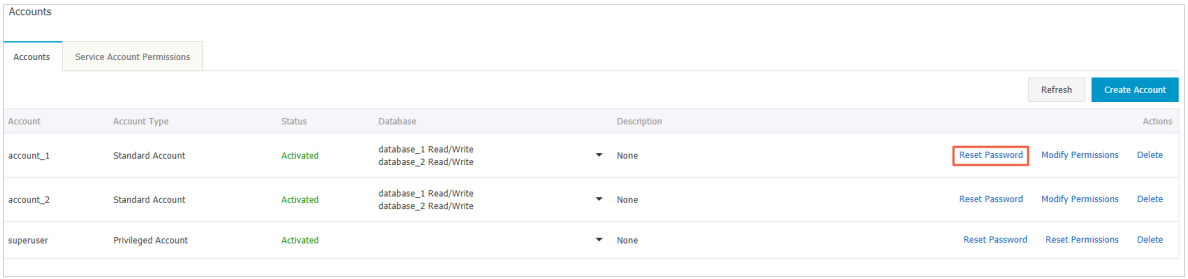
Procedure

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_68	Used to reset the password of a database account.

7 Database management

7.1 Create a database for an RDS for PPAS instance

This topic describes how to create a database for an RDS for PPAS instance.

Before using an RDS for PPAS instance, you must create a premier account for it in the RDS console, and then create and manage databases by using the premier account in the DMS console.

Precautions

- **The databases in an RDS instance share all resources provided by the instance. You can create and manage more than one database by using SQL statements.**
- **If you want to migrate an on-premises database to an RDS instance, you must create the same accounts and databases in the RDS instance as those in the on-premises database.**

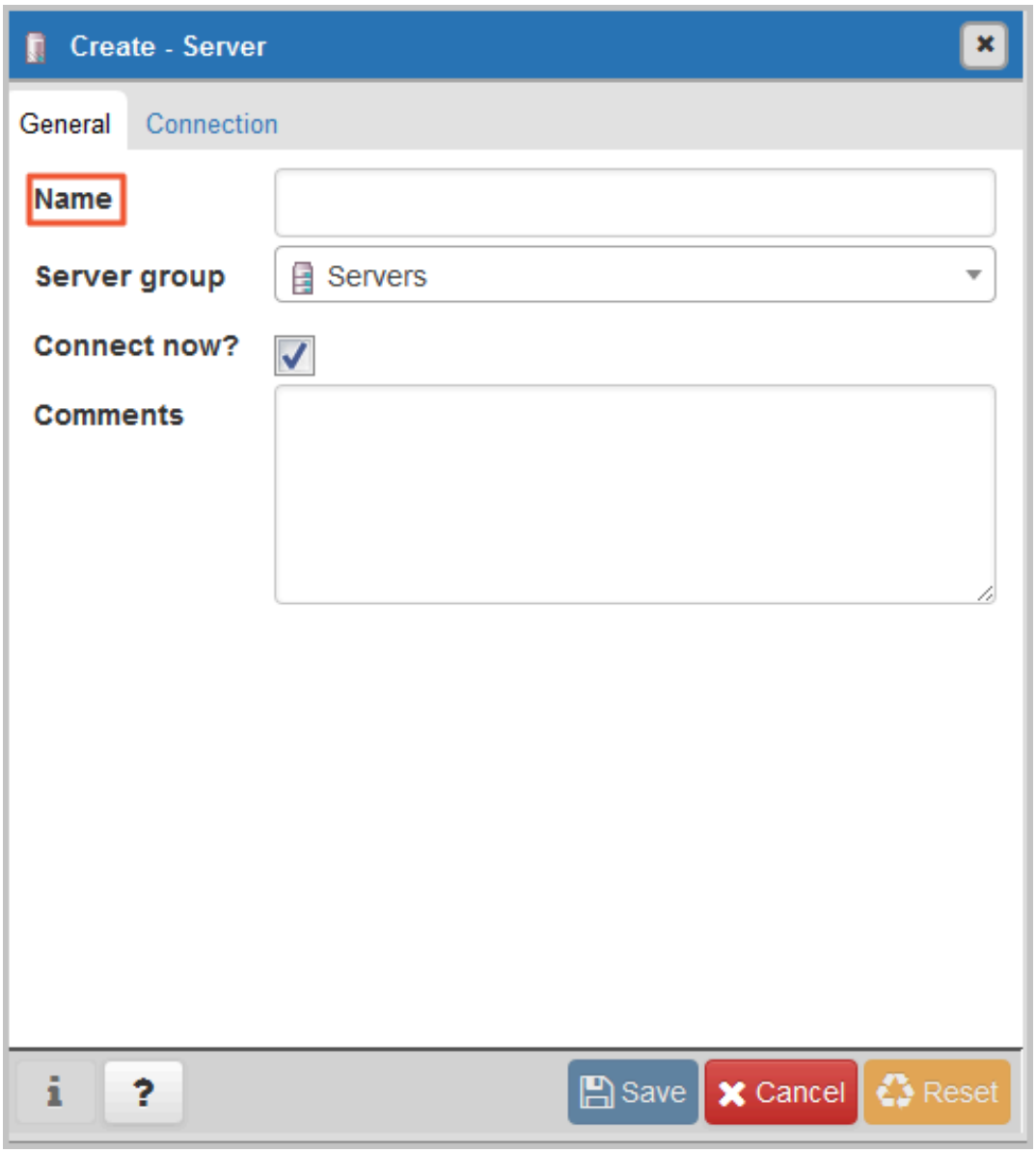
Procedure

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

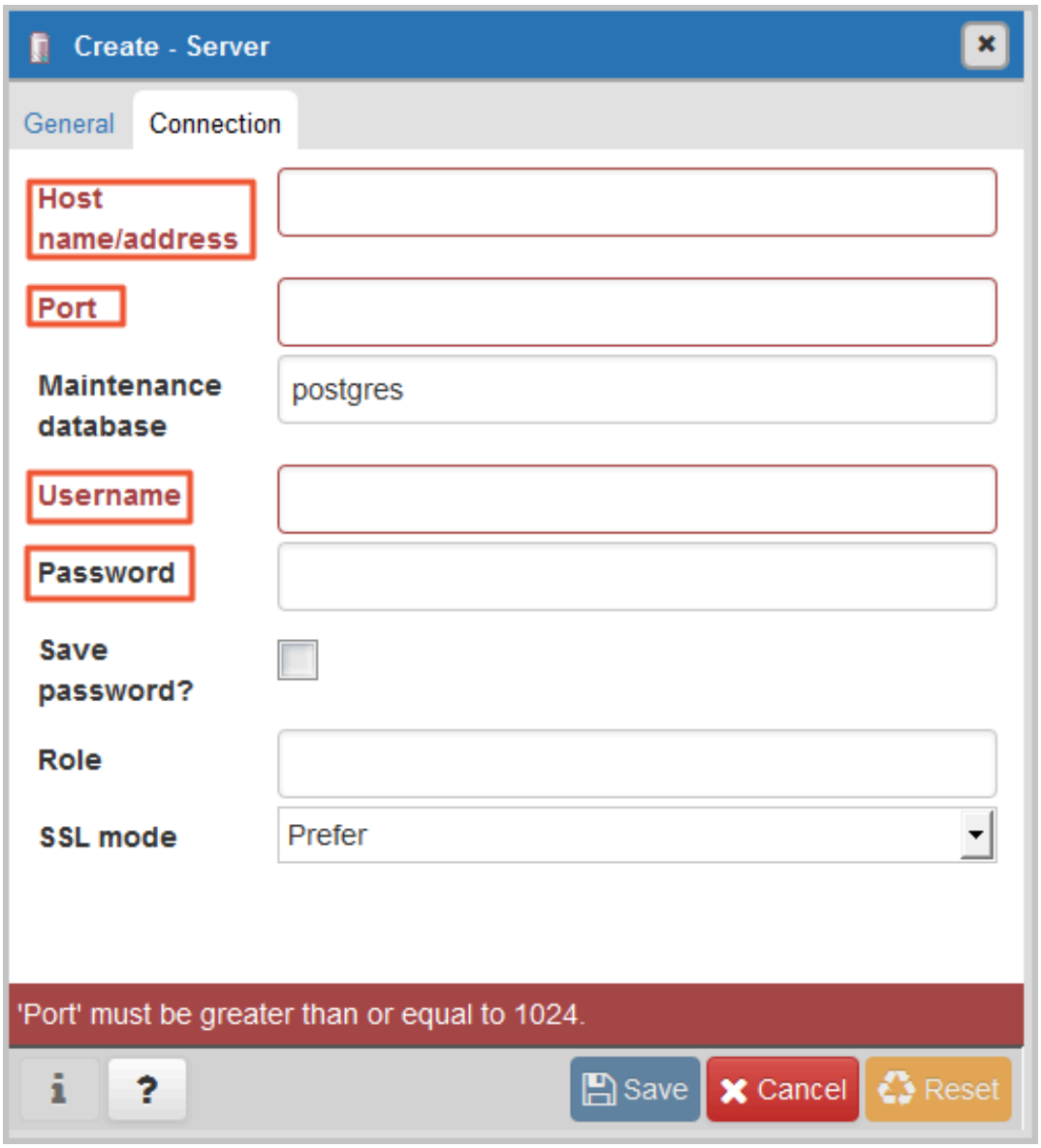
3. **Find the target RDS instance and click the instance ID.**
4. **Add the IP addresses of the devices that are to access the RDS instance to a whitelist of the RDS instance. For more information, see *Configure a whitelist for an RDS for PPAS instance*.**
5. **Start the pgAdmin 4 client.**

6. In the left-side navigation pane, right-click Servers and choose Create > Server.

7. **In the Create - Server dialog box, click the General tab and enter the server name.**



8. Click the Connection tab and enter the information about the RDS instance to be connected.



Parameter description:

- Host name/address: The internal or public endpoint of the RDS instance. To obtain the internal and public endpoints and ports of the RDS instance, follow these steps:
  a. Log on to the *RDS console*.
  b. In the upper-left corner, select the region where the target RDS instance is located.
  c. Find the target RDS instance and click the instance ID.

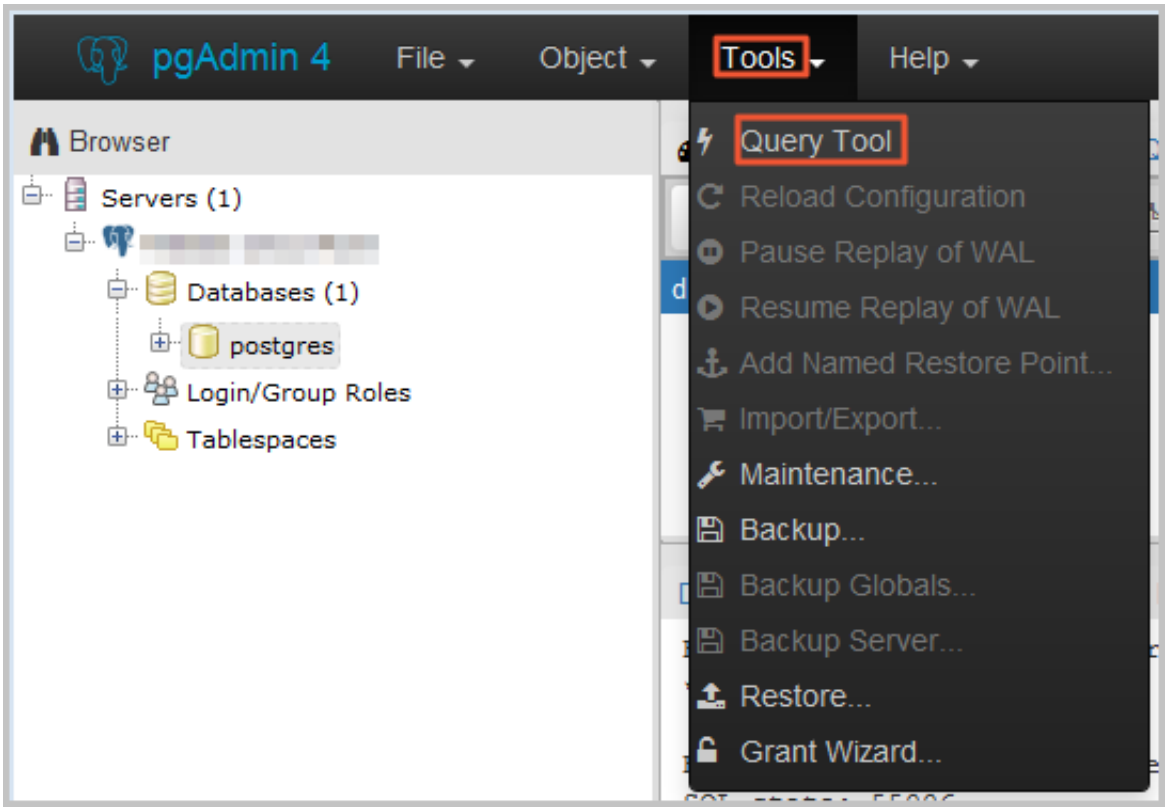
d. On the Basic Information page, find the Basic Information section, where you can obtain the internal and public endpoints and ports of the RDS instance.

- Port: The internal or public port numbr of the RDS instance.
- Username: The username of the premier account for the RDS instance.
- Password The password of the premier account for the RDS instance.

9. Click Save.
10. Choose Servers > *Server name* > Databases > postgres. If the connection information is correct, the page shown in the following figure is displayed, indicating that a connection is established.

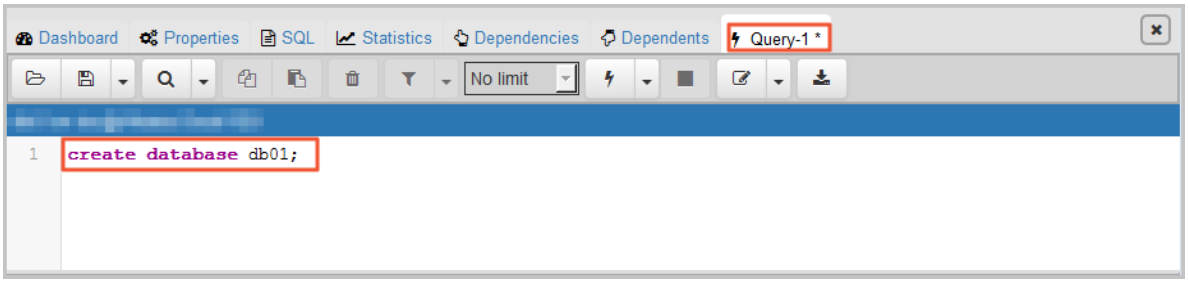
Note:
postgres is the default database of the RDS instance. Do not perform any operation in this database.

11. Select postgres and choose Tools > Query Tool.

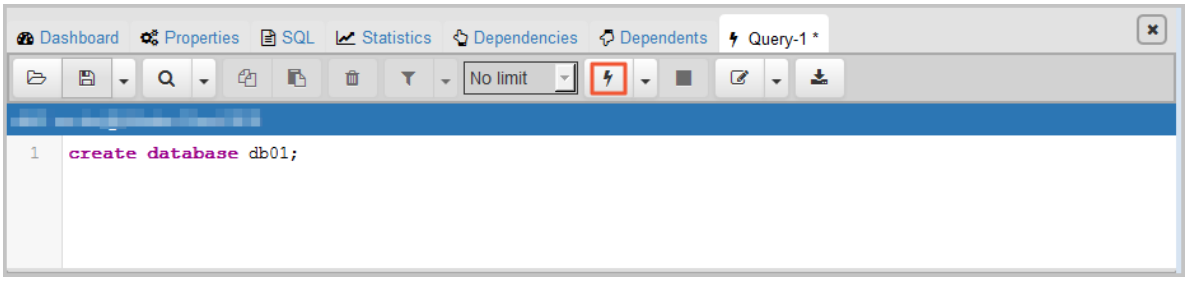


12. On the Query-1 tab, enter the following command to create a database:

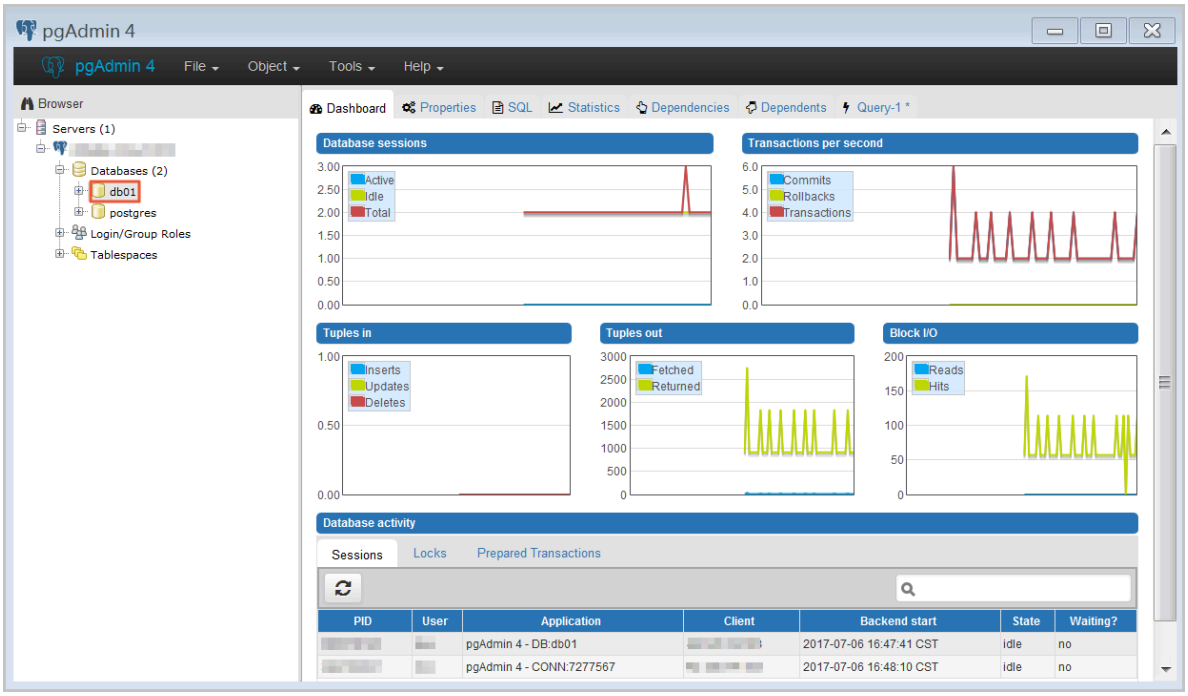
```
create database <database name>;
```



13. Click the execute or refresh button.



14. When the command is executed successfully, indicating that the database is created, right-click Databases and choose the refresh button to view the new database.



7.2 Delete a database for an RDS for PPAS instance

This topic describes how to delete a database from an RDS for PPAS instance by using SQL commands.

The procedure is as follows:

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

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

8 Database connection

8.1 Configure a hybrid access solution to smoothly migrate an RDS instance from the classic network to a VPC

This topic describes how to configure a hybrid access solution to smoothly migrate an RDS instance from the classic network to a VPC. To meet the increasing needs of migration between different network types, ApsaraDB for RDS introduces the hybrid access solution. This solution enables a smooth migration from the classic network to a VPC without any transient disconnections or service interruptions. The solution also offers the option to migrate a primary instance and its read-only instances separately without any interference with each other.

Background information

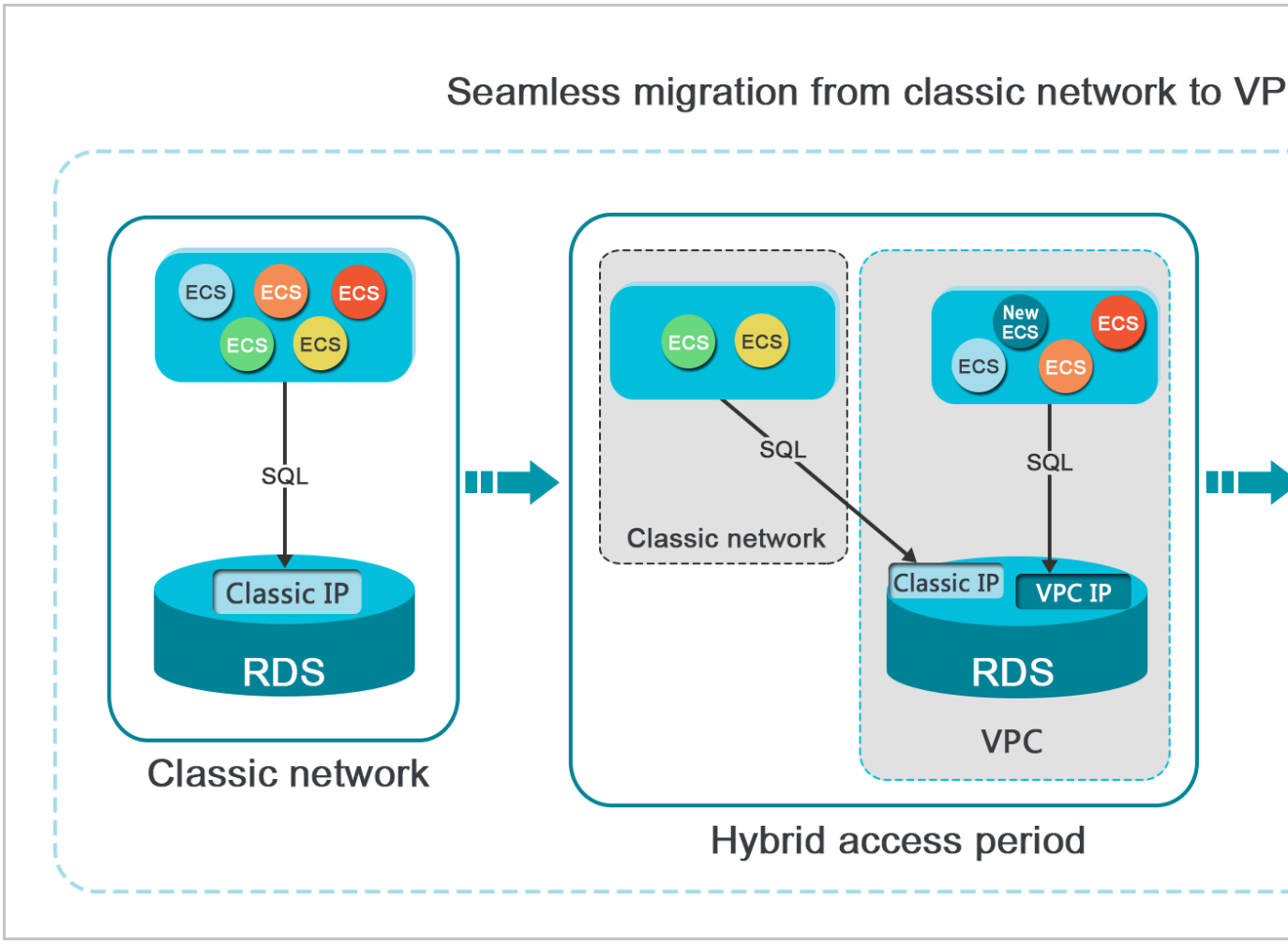
In the past, when migrating an RDS instance from the classic network to a VPC, the internal endpoint of the RDS instance changes. The connection string of the RDS instance remains the same but the IP address bound to the connection string is changed to the corresponding IP address in the VPC. This change will cause a 30-second transient disconnection, and the ECS in the classic network cannot access the RDS instance through the internal endpoint within this period. To migrate the RDS instance across different networks in a smooth manner, ApsaraDB for RDS introduces the hybrid access solution.

Hybrid access refers to the ability of an RDS instance to be accessed by ECS on both the classic network and VPC. During the hybrid access period, the RDS instance reserves the original internal endpoint of the classic network and adds an internal endpoint of VPC. This prevents transient disconnections during the RDS database migration.

For better security and performance, we recommend that you use the internal endpoint of VPC only. Therefore, hybrid access is available for a limited period of time. The internal endpoint of the classic network is released when the hybrid access period expires. In that case, your applications cannot access the RDS database by using the internal endpoint of the classic network. You must configure the internal endpoint of VPC in all your applications during the hybrid access

period. This can guarantee smooth network migration and minimize the impact on your services.

For example, your company wants to use the hybrid access solution to migrate RDS instances from the classic network to a VPC. During the hybrid access period, some applications can access the database through the internal endpoint of the VPC, and the other applications can access the database through the original internal endpoint of the classic network. When all the applications access the database through the internal endpoint of the VPC, the internal endpoint of the classic network can be released. The following figure illustrates the scenario.



Limits

During the hybrid access period, the instance has the following limits:

- Switching to the classic network is not supported.
- Migrating the RDS instance to another zone is not supported.

Prerequisites

- **The network type of the instance is the classic network.**
- **Available VPCs and VSwitches exist in the zone where the RDS instance is located. For more information about how to create VPCs and VSwitches, see *Manage VPCs*.**

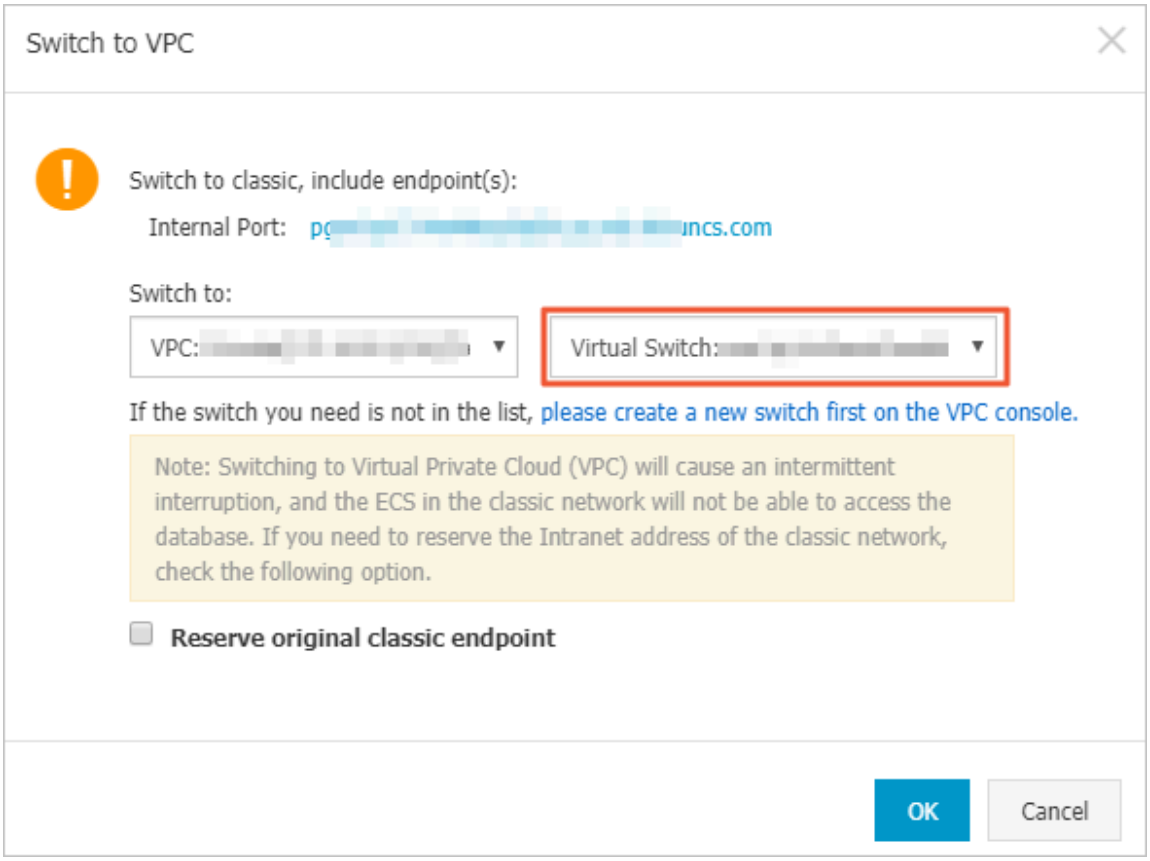
Migrate the RDS instance from the classic network to a VPC

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 Database Connections.**
5. **Click Switch to VPC.**
6. **In the dialog box that appears, select a VPC and VSwitch, and select whether to retain the internal and public endpoints of the classic network.**
   - **Select a VPC. We recommend that you select the VPC where your ECS instance is located. Otherwise, the ECS instance and RDS instance cannot communicate**

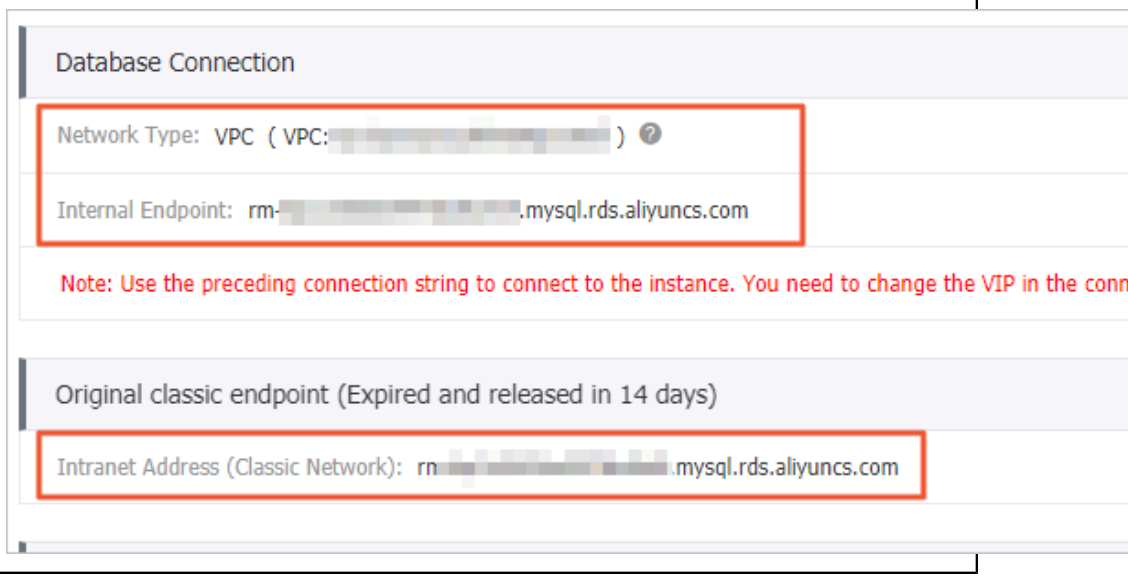
through the internal connections unless you create an express connection or gateway. For more information, see *Express connection* and *VPN gateway*.

- Select a VSwitch. If no VSwitch exists in the selected VPC (as shown in the following figure), create a VSwitch in the same zone as the instance. For more information, see *Manage VSwitches*.



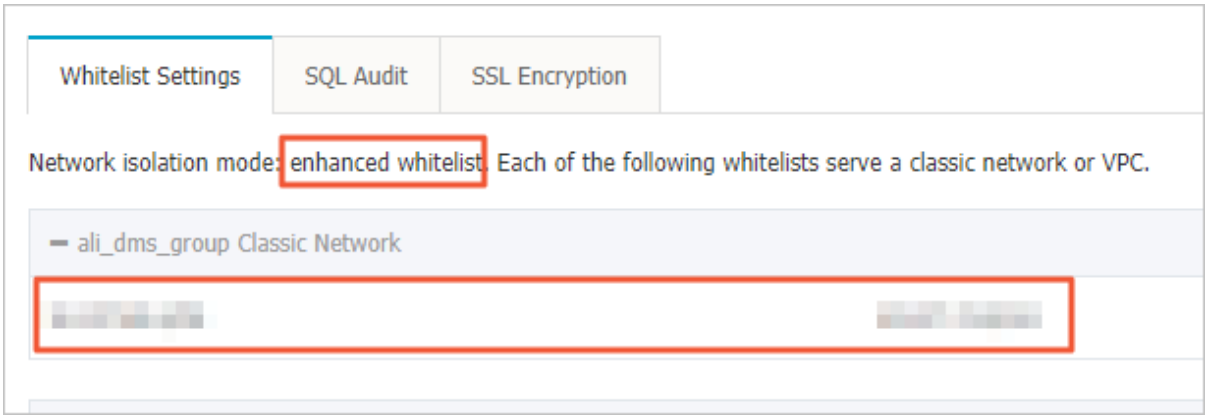
- Decide whether to select Retain Classic Network. The following table describes the different actions.

Action	Description
Clear	The endpoint of the classic network is not retained. The original endpoint is changed to the endpoint of the VPC. If the endpoint of the classic network is not retained, a 30-second transient disconnection will occur to the RDS instance when the network type is changed. The internal access to the RDS instance from the ECS instance that is located in the classic network will be immediately disconnected.

Action	Description
Select	The endpoint of the classic network is retained, and a new endpoint of the VPC is added. Indicates that the hybrid access mode is used and RDS can be simultaneously accessed by ECS instances both in the classic network and VPC through the internal endpoints. If the endpoint of the classic network is retained, the RDS instance will not be immediately disconnected when the network type is changed. The ECS instances in the classic network will not be disconnected from the internal access to the RDS instance until the internal endpoint of the classic network expires. Before the endpoint of the classic network expires, add the endpoint of the VPC to the ECS instance that is located in the same VPC. This makes sure that your business is smoothly migrated to the VPC. Within seven days before the endpoints of the classic network expire, the system will send a text message to the mobile phone bound to your account every day. 

7. Add the internal IP address of the ECS instance in the VPC to the VPC whitelist group of the RDS instance. This makes sure that the ECS instance can access the

RDS instance through the internal network. If no VPC whitelist group exists, create a new group.



8. · **If you select Retain Classic Network, add the endpoint of the VPC to the ECS instance before the endpoint of the classic network expires.**
   · **If you clear Retain Classic Network, the internal connection from the ECS instance in the VPC to the RDS instance is immediately disconnected after the network type is changed. You must add the RDS endpoint of the VPC to the ECS instance.**

> **Note:**
> **To connect an ECS instance in the classic network to an RDS instance in a VPC through the internal network, you can use *ClassicLink* or switch the network type to VPC.**

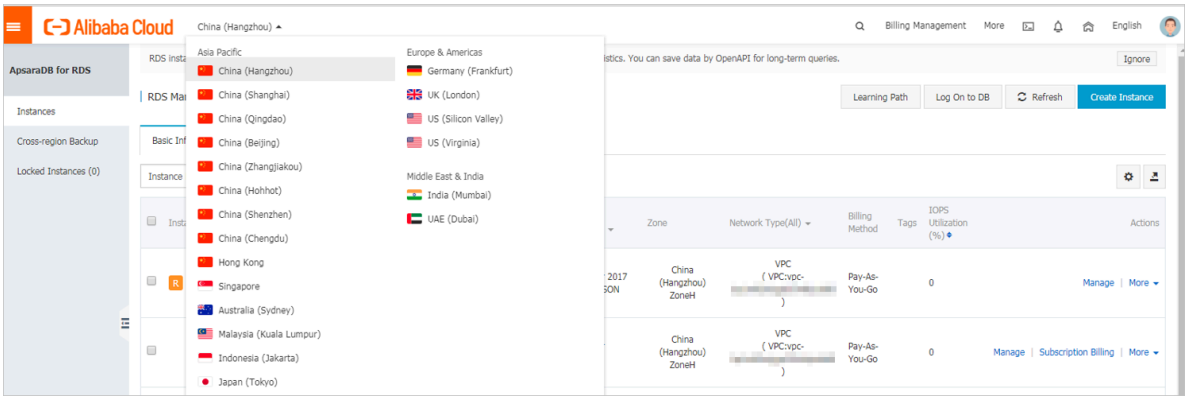
Change the expiration time for the original internal endpoint of the classic network

During the hybrid access period, you can change the retention period for the original internal endpoint of the classic network at any time as needed. The system will update the expiration date based on the modified date. For example, if the original internal endpoint of the classic network is set to expire on August 18, 2017, and you change the expiration time to "14 days later" on August 15, 2017. The internal endpoint of the classic network is released on August 29, 2017.

Follow these steps to change the expiration time:

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 Database Connections.
5. On the Instance Connection tab, click Change Expiration Time, as shown in the following figure.

6. On the Change Expiration Time page that appears, select an expiration time and click OK.

8.2 Configure endpoints for an RDS for PPAS instance

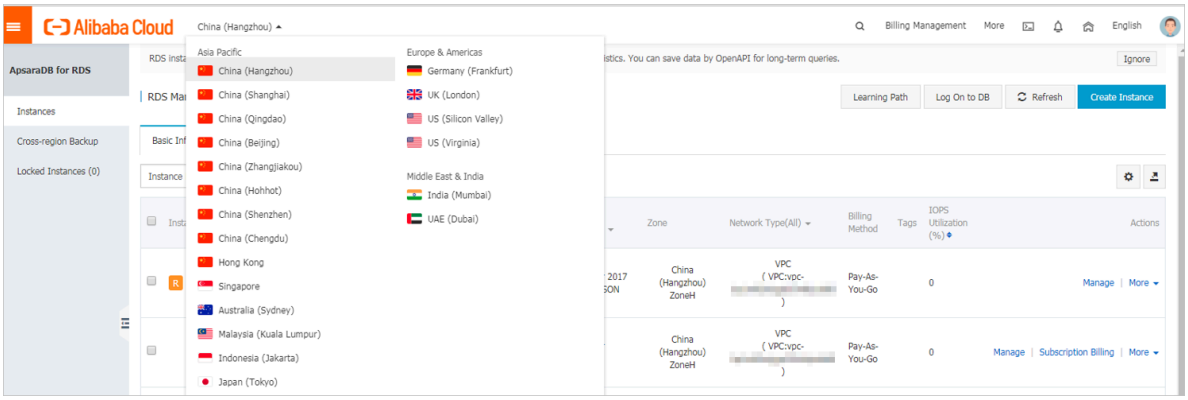
This topic describes how to configure endpoints for an RDS for PPAS instance, including applying for, changing, and releasing the endpoints. ApsaraDB for RDS provides two types of endpoints: internal endpoints and public endpoints.

Internal and public endpoints

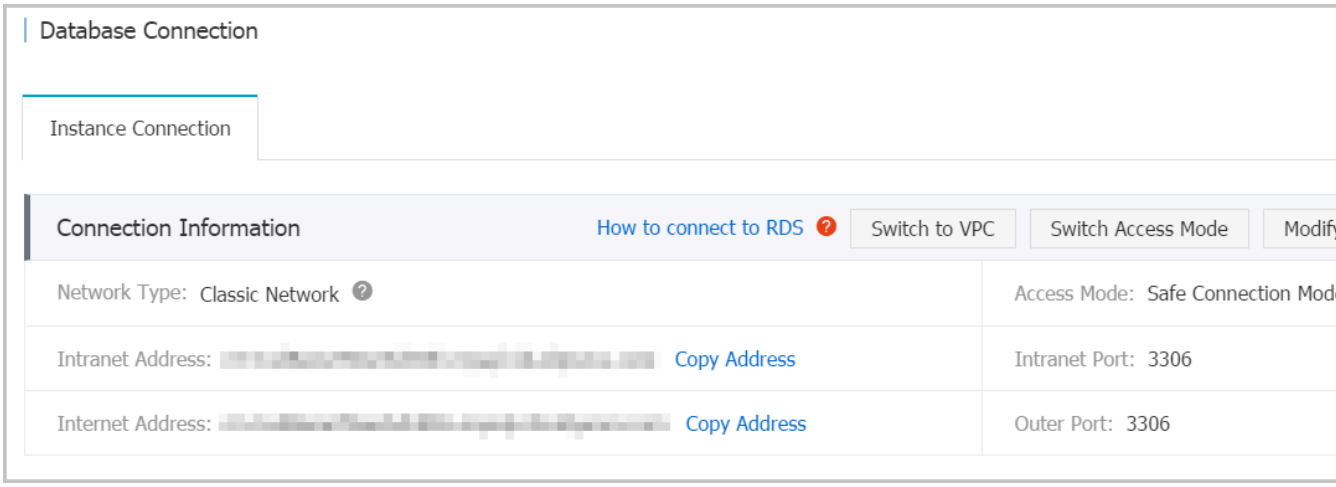
Endpoint type	Description
Internal endpoint	· The internal endpoint is provided by default. You do not need to apply for it and cannot release it. However, you can change the network type. · If your application is deployed on an ECS instance that is in the same region and has the same *network type* as the RDS instance, 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.

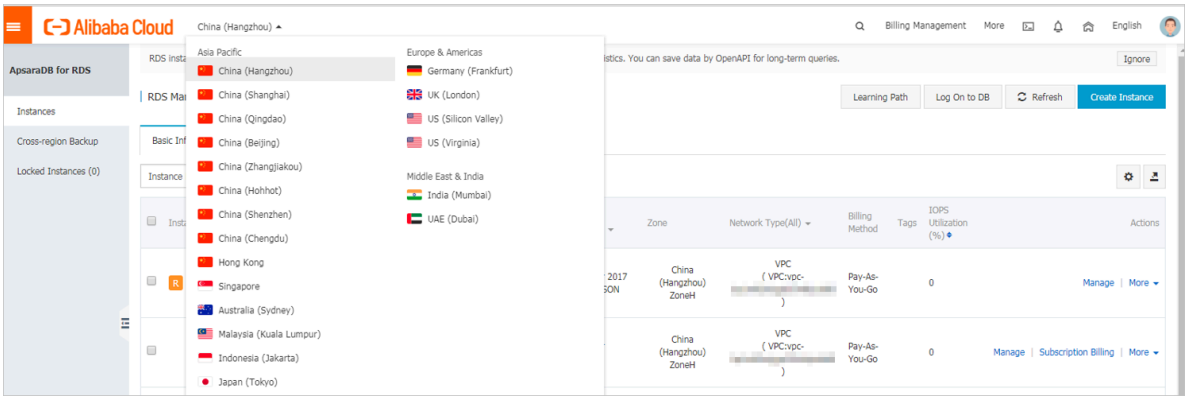


6. **In the message box that appears, click OK.**

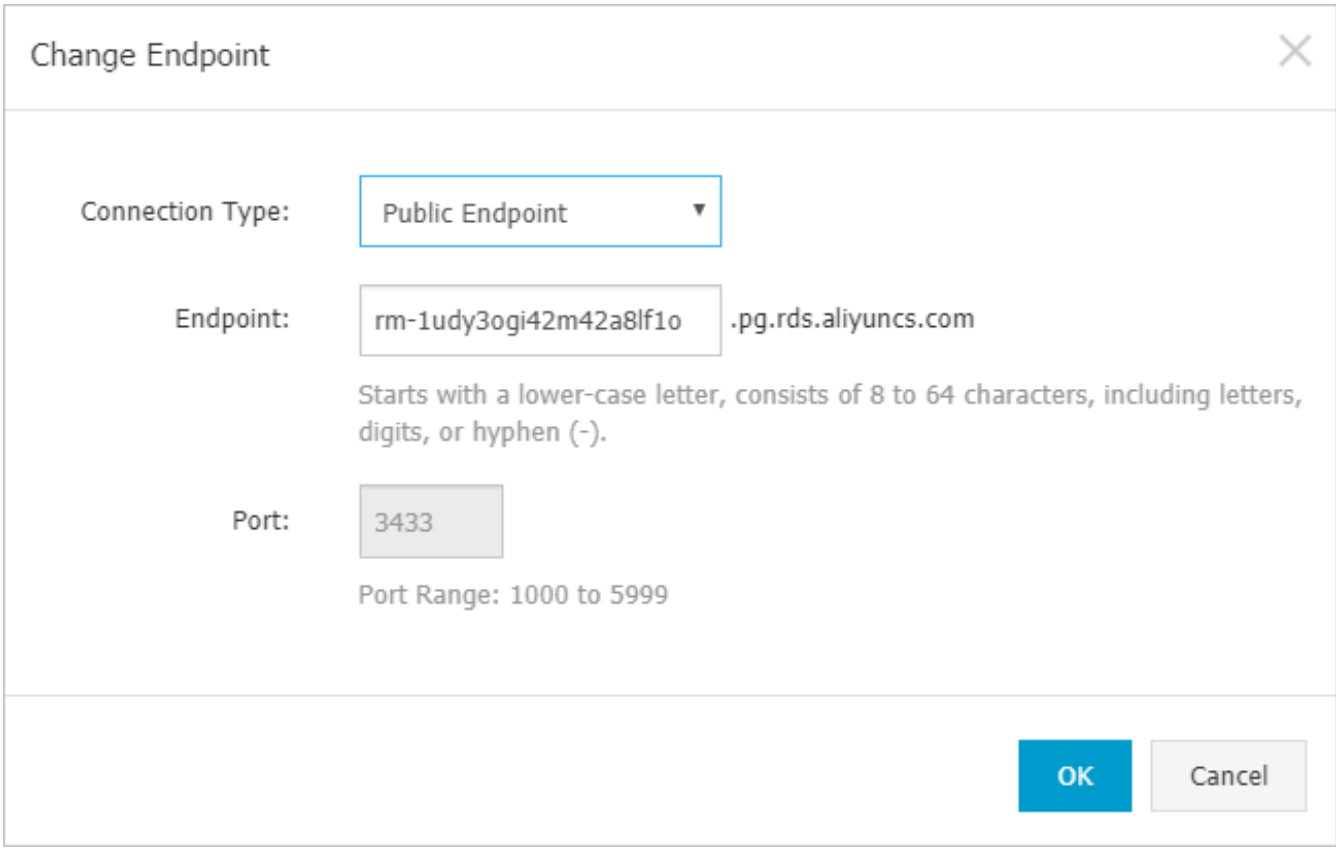
Change the internal and public endpoints

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

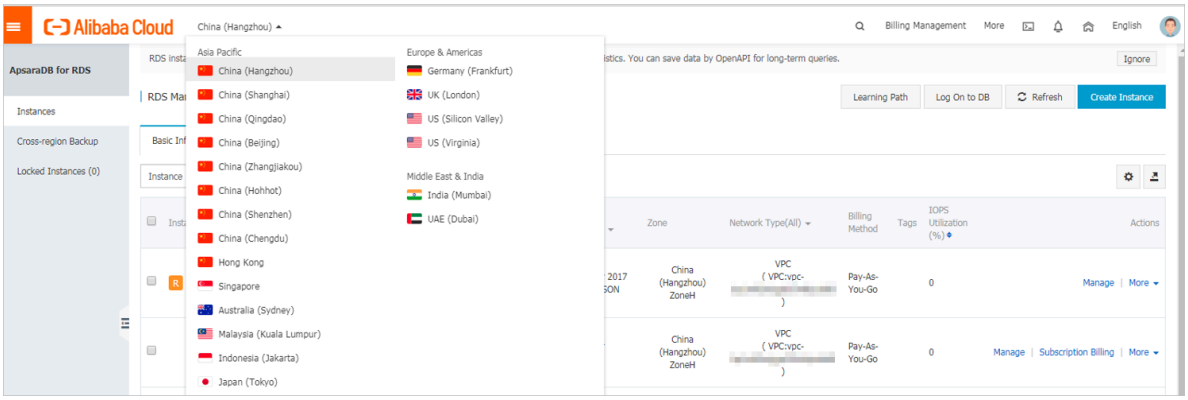
Operation	Description
#unique_78	Used to apply for a public endpoint for an RDS instance.
#unique_79	Used to release the public endpoint of an RDS instance.

8.3 View the internal and public endpoints and ports of an RDS for PPAS instance

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

Procedure

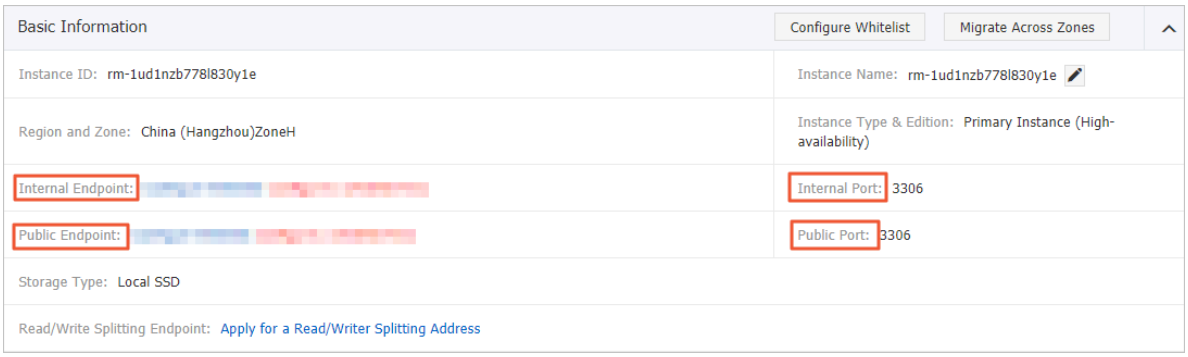
1. Log on to the *RDS console*.
2. In the upper-left corner, select the region where the target RDS instance is located.



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.



8.4 Apply for a public endpoint for an RDS for PPAS instance

This topic describes how to apply for a public endpoint for an RDS for PPAS 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.

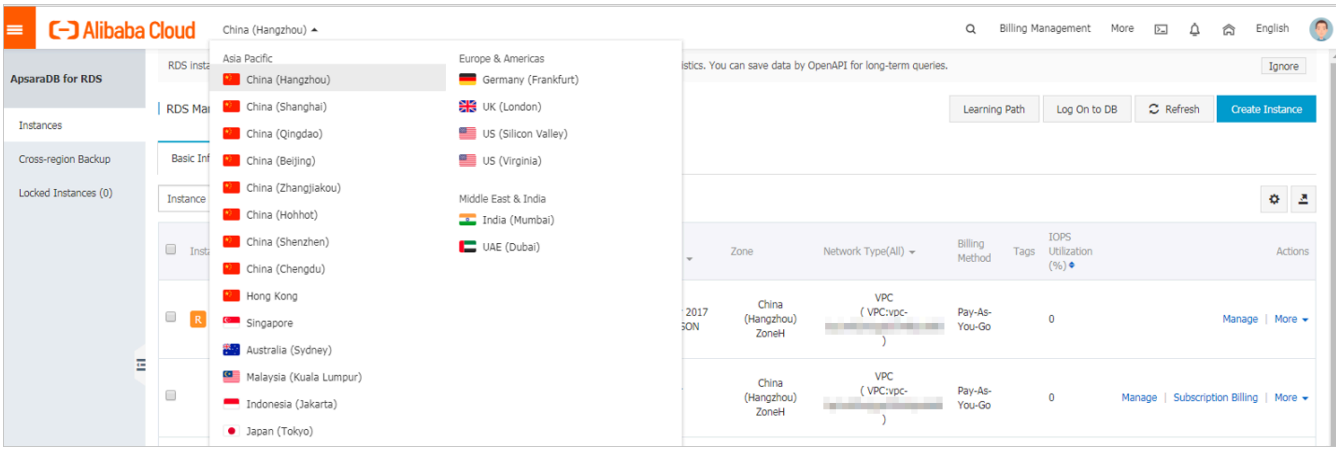
Internal and public endpoints

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.

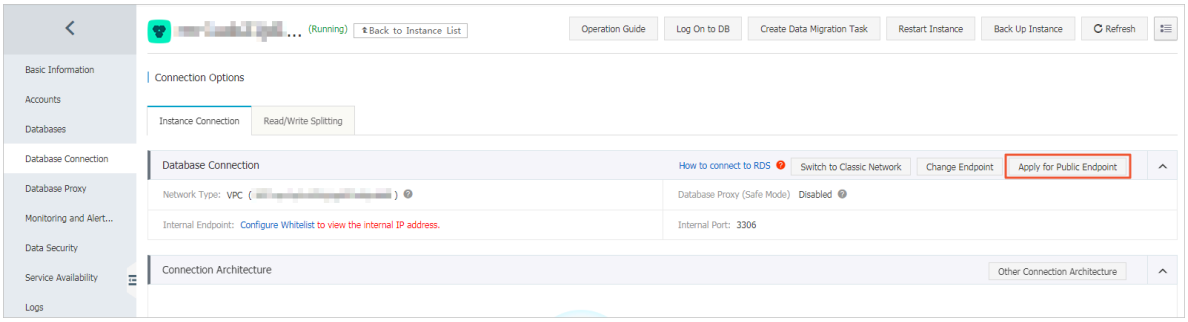
Procedure

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



3. Find the target RDS instance and click the instance ID.
4. 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.

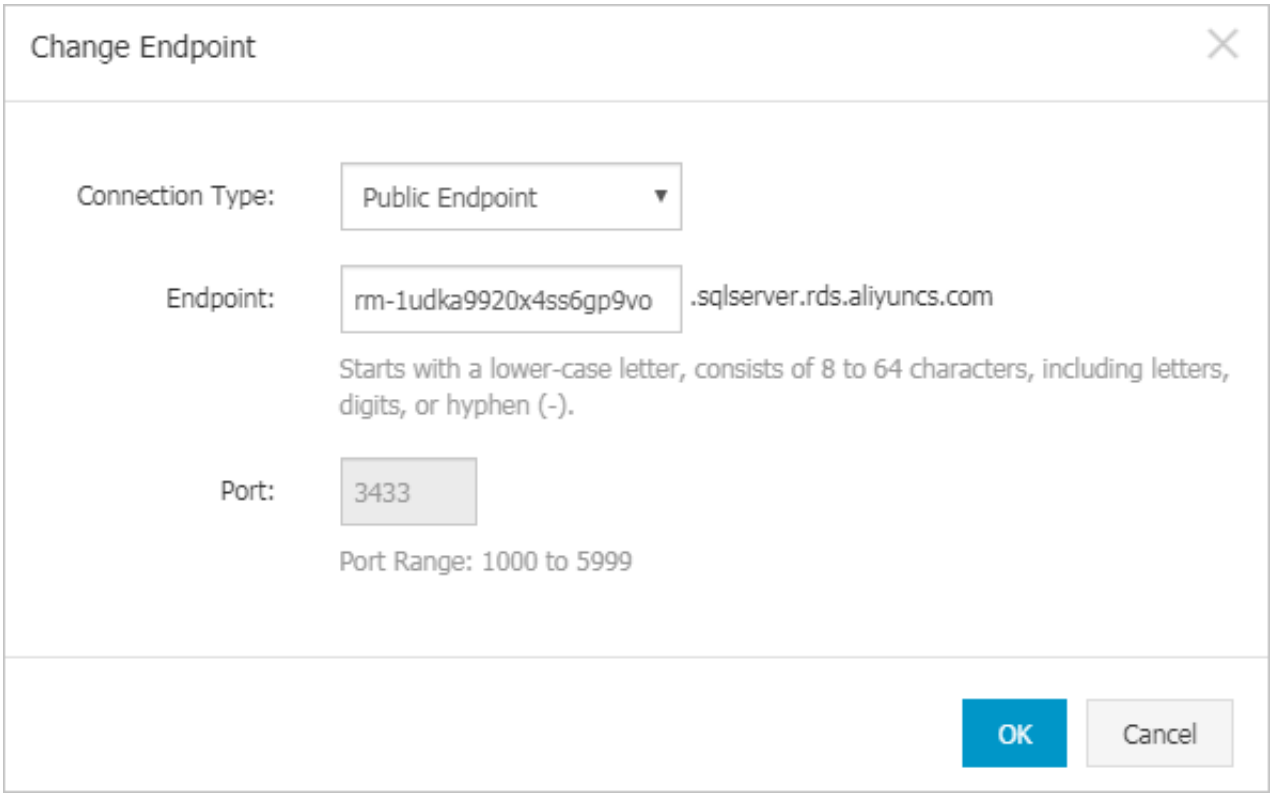
7. Optional. If you want to change the public endpoint or port number, click Change Endpoint. In the displayed dialog box, set the public endpoint and port number and click OK.

   - Connection Type: Select Public Endpoint.

     Note:

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

- **Endpoint: The endpoint must be 8 to 64 characters in length and can contain letters, numbers, and hyphens (-). It must start with a lowercase letter.**
- **Port: You can change the port number only when the network type of the RDS instance is classic network.**



APIs

API	Description
#unique_78	**Used to apply for a public endpoint for an RDS instance.**

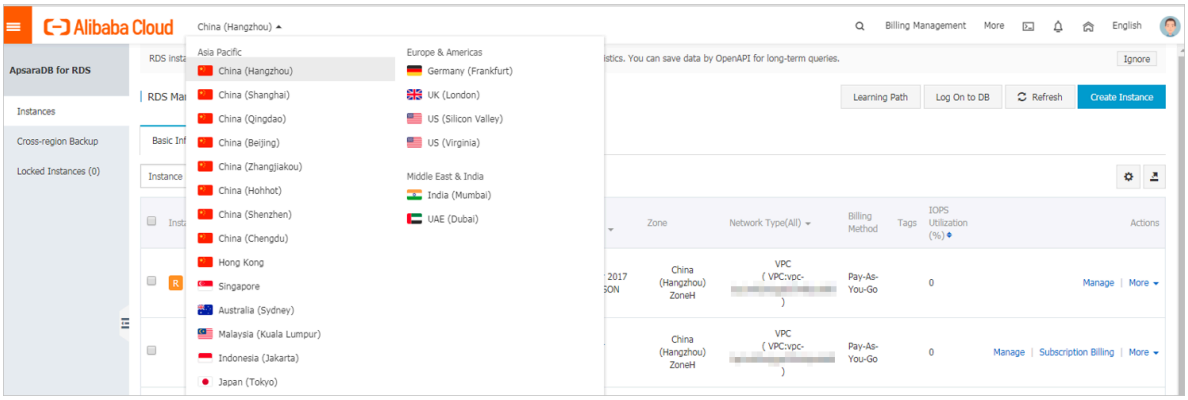
9 Monitoring and alerts

9.1 View resource monitoring data

This topic describes how to view the resource and engine monitoring data of an RDS for PPAS 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, specify the time range. The following table describes the monitoring metrics.**

Metric	Description
Disk Space (MB)	The disk space usage of the RDS instance. Unit: MByte.
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.

Metric	Description
Total Connections	The total number of connections to the RDS instance .

9.2 Set the monitoring frequency

This topic describes how to set the monitoring frequency for an RDS for PPAS 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

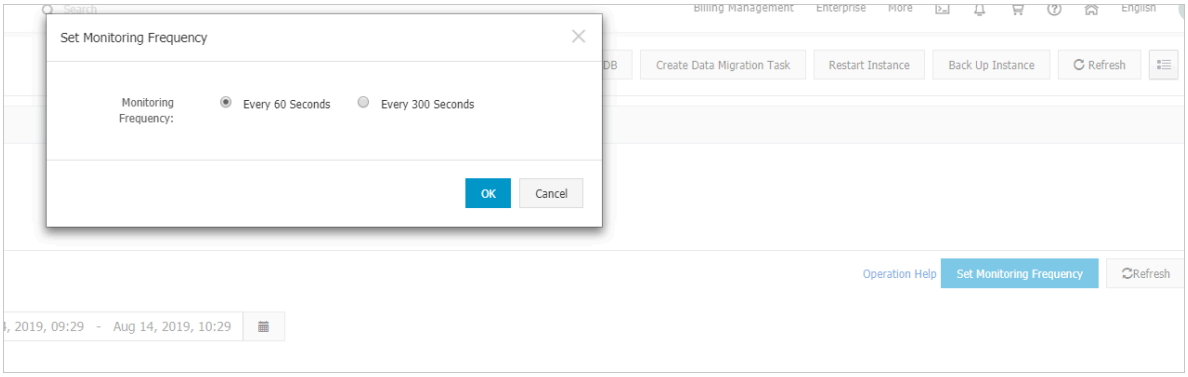
1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**

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 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.



APIs

API	Description
#unique_85	Used to query the monitoring data of an RDS instance.

9.3 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.

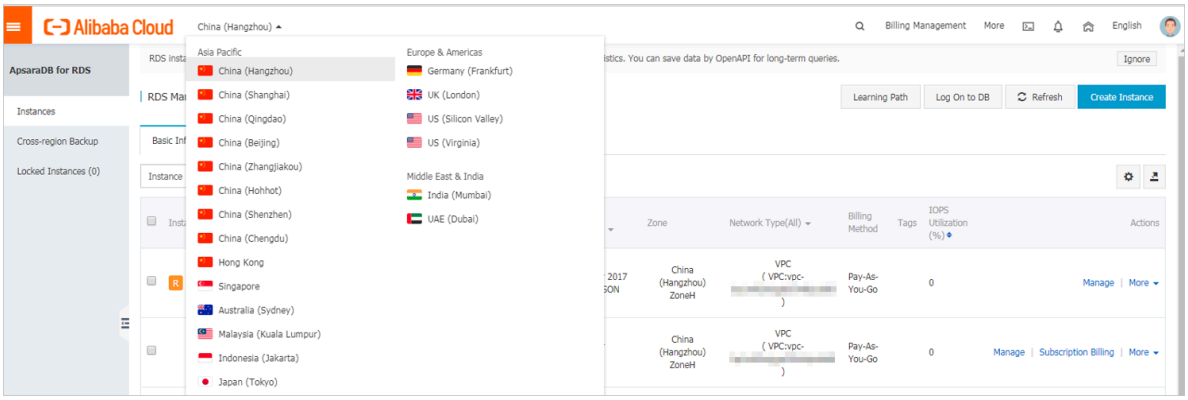
Background information

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.

10 Data security

10.1 Switch to the enhanced whitelist mode for an RDS for PPAS instance

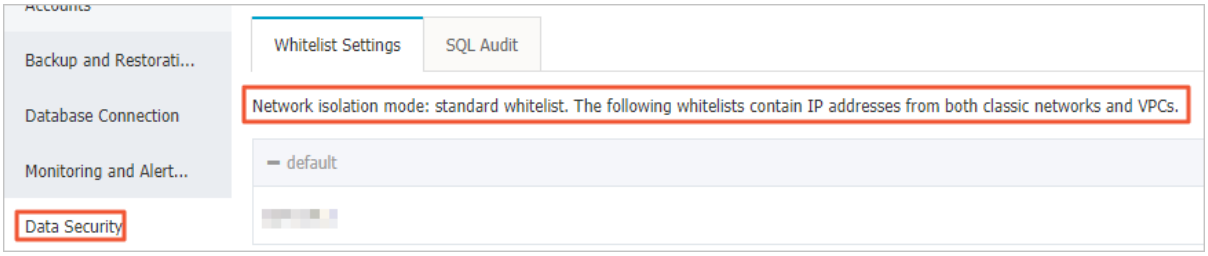
This topic describes how to switch from the standard whitelist mode the enhanced whitelist mode for an RDS for PPAS instance.

IP whitelist modes

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

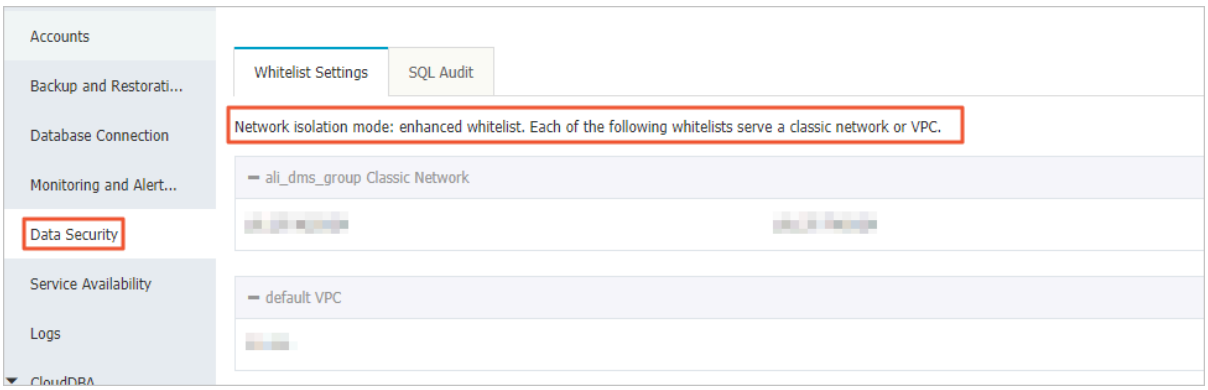
- **Standard whitelist mode**

  In this mode, the IP addresses in the whitelist do not distinguish between classic networks and VPCs. The IP addresses in the whitelist can access the RDS instance both in classic networks 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 the network type of the instance is VPC, a new whitelist of the VPC is generated and contains the same IP addresses in the original whitelist. The new IP whitelist group only applies to VPCs.**
- **If the instance network type is classic network, a new whitelist group is generated and contains the same IP addresses in the original whitelist. The new IP whitelist group only applies to classic networks.**
- **If the instance is in the *hybrid access mode*, two new whitelist groups are generated and each contains the same IP addresses in the original whitelist. One of the whitelist group applies to VPCs and the other applies to classic networks.**

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

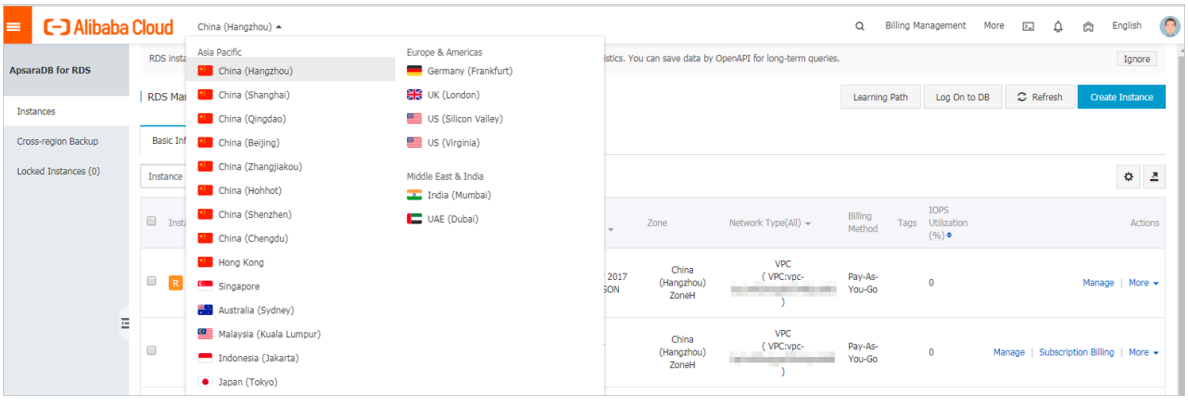
Precautions

- **You can switch from the standard whitelist mode to the enhanced whitelist mode . However, you cannot switch from the enhanced whitelist mode to the standard whitelist mode.**
- **In the enhanced whitelist 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, 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.

10.2 Configure a whitelist for an RDS for PPAS instance

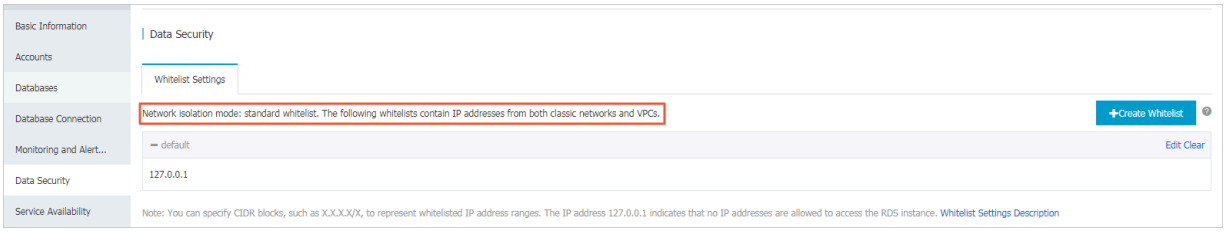
This topic describes how to configure a whitelist for an RDS for PPAS instance.

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 can 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.

Precautions

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



Note:

The internal networks to which RDS instances belong are divided into two types: classic network and VPC.

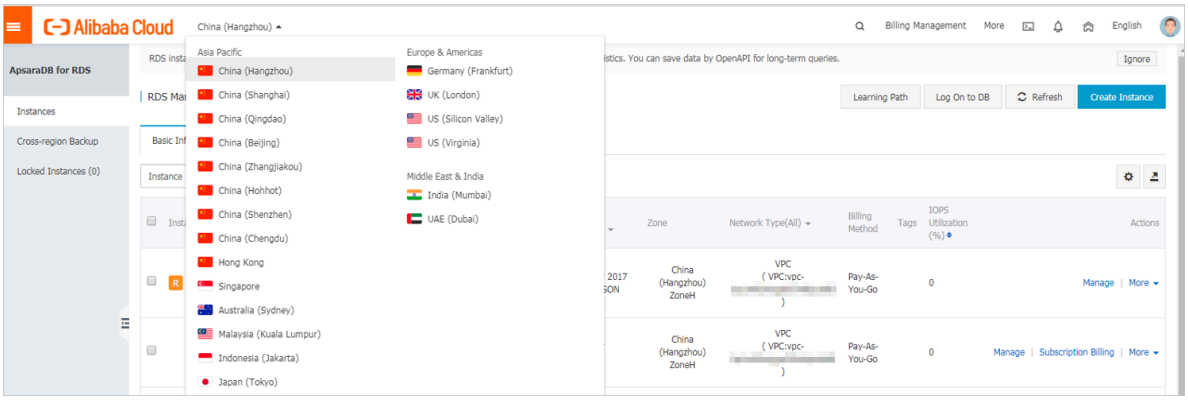
- **Classic network: Alibaba Cloud allocates IP addresses automatically. Users only need to perform simple configurations. This network type is suitable for new users.**
- **VPC: Users customize the network topology and IP addresses. It supports leased line connection, and is suitable for advanced users.**

Procedure

Enhanced whitelist

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

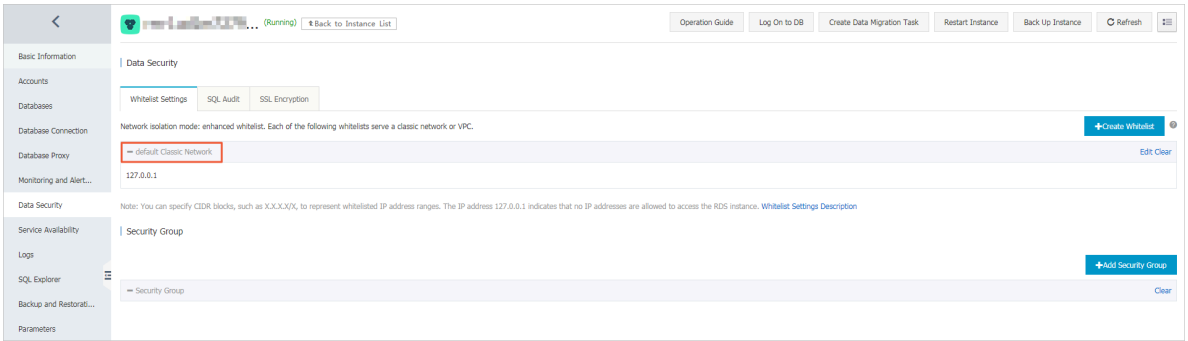
2. In the upper-left corner, select the region where the target RDS instance is located.



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

   - Accessing an RDS instance from an ECS located in a VPC: Click Edit next to the `default VPC` whitelist.
   - Accessing an RDS instance from an ECS located in a classic network: Click Edit next to the `default Classic Network` whitelist.
   - Accessing an RDS instance from an ECS or host located in a public network: Click Edit next to the `default Classic Network` whitelist.

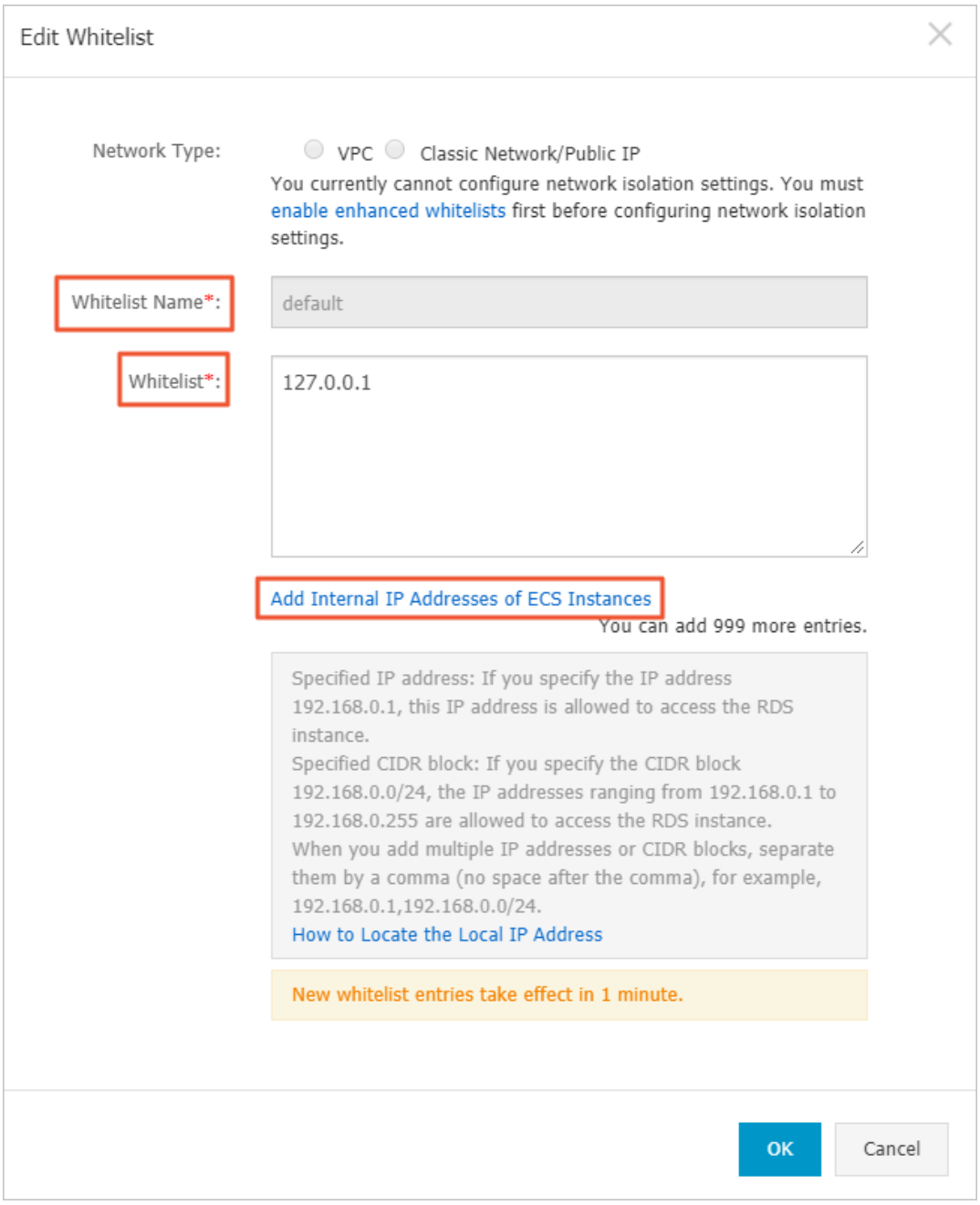
> **Note:**
>
> - If the ECS instance accesses the RDS instance by using the VPC or classic network, you must make sure that the two instances are in the same region and have the same *network type*. Otherwise, the connection fails.
> - You can also click Create Whitelist. In the displayed Create Whitelist dialog box, select VPC or Classic Network/Public IP.



6. **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:

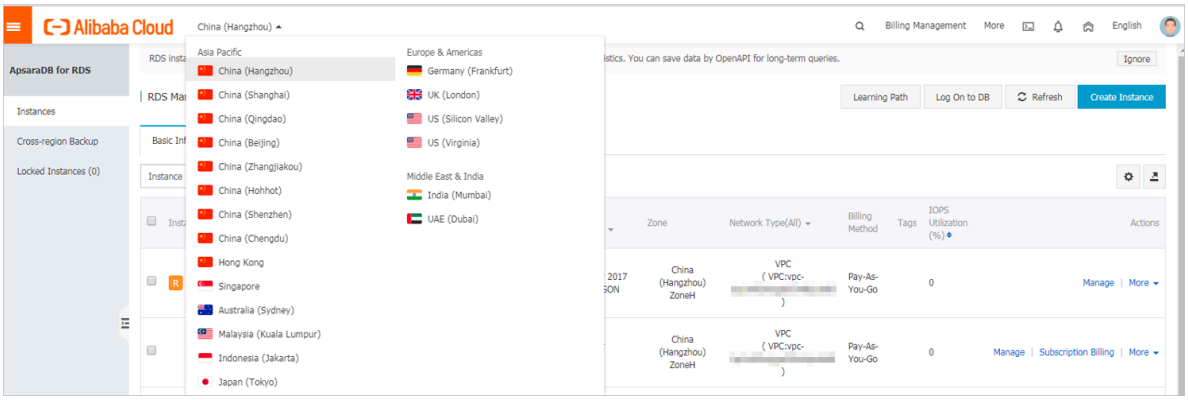
After you add an IP address or CIDR block to the default whitelist, the default address 127.0.0.1 is automatically deleted.



Standard whitelist

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

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



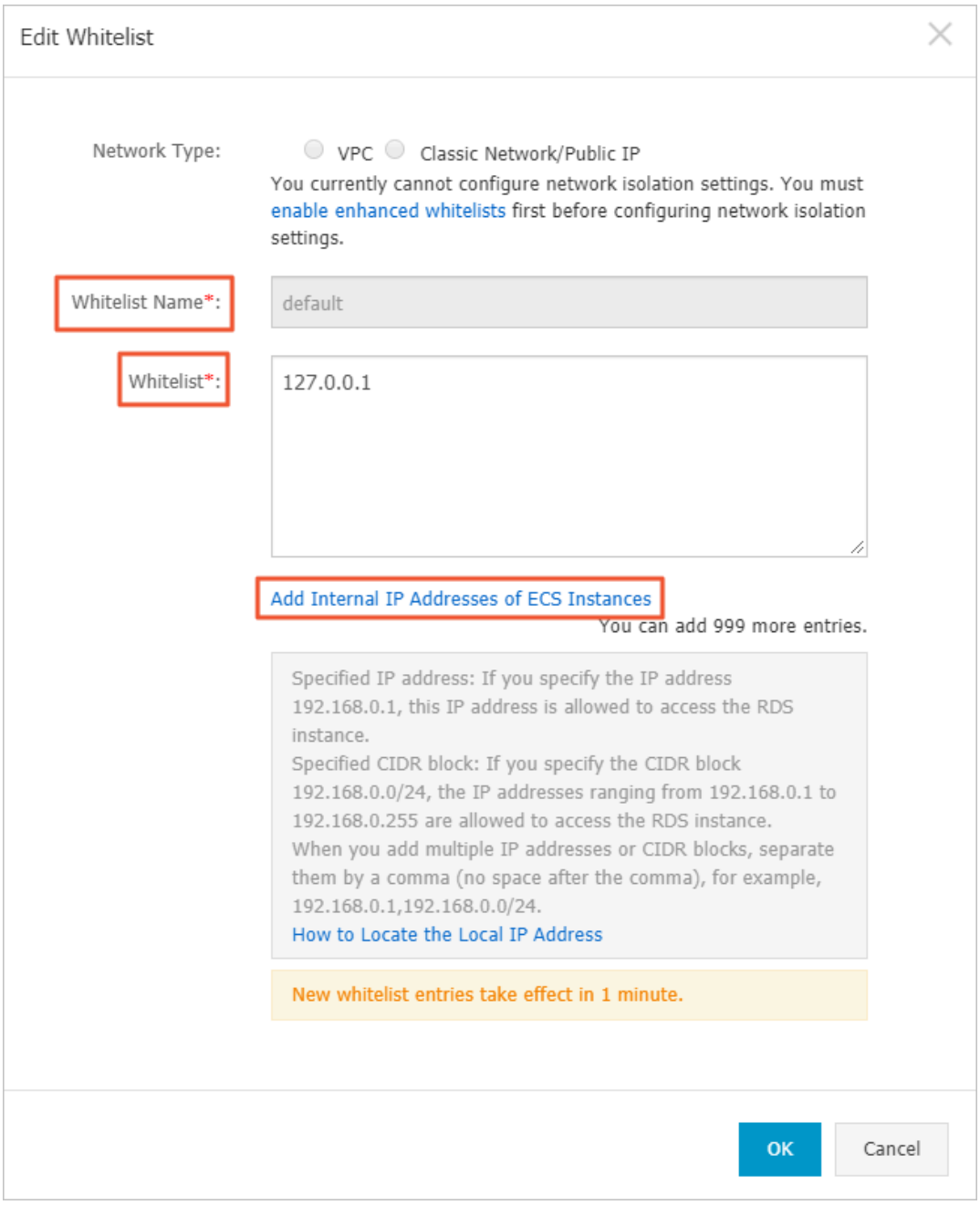
3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Data Security.
5. On the Whitelist Settings tab page, click Edit corresponding to the default whitelist.

> **Note:**
> You can also click Create Whitelist to configure 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 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.



Common errors

- **The default address 127.0.0.1 on the Whitelist Settings tab 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 turn on 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 VPC.**
  - **If the network type is classic network, the internal IP address of the ECS instance is added to the whitelist whose network isolation mode is classic network.**
  - **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 instance or host must be added to the whitelist whose network isolation mode is classic network.**
- **The public IP address that you add to the whitelist may not be the real egress 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 provide wrong IP addresses.**

  For more information, see *#unique_91*

APIs

API	Description
#unique_92	**Used to view the IP address whitelist of an RDS instance.**
#unique_93	**Used to modify the IP address whitelist of an RDS instance.**

11 Data backup

11.1 Back up the data of an RDS for PPAS instance

This topic describes how to back up the data of an RDS for PPAS instance. You can specify a data and log backup cycle, according to which the system automatically backs up data and logs. Alternatively, you can manually back up the instance data.

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 PPAS 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
PPAS	Supports full physical backup.	A WAL file (16 MB/file) is compressed and uploaded immediately after it is generated. You must delete the file from your computer within 24 hours.

Set a backup policy for automatic backup

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

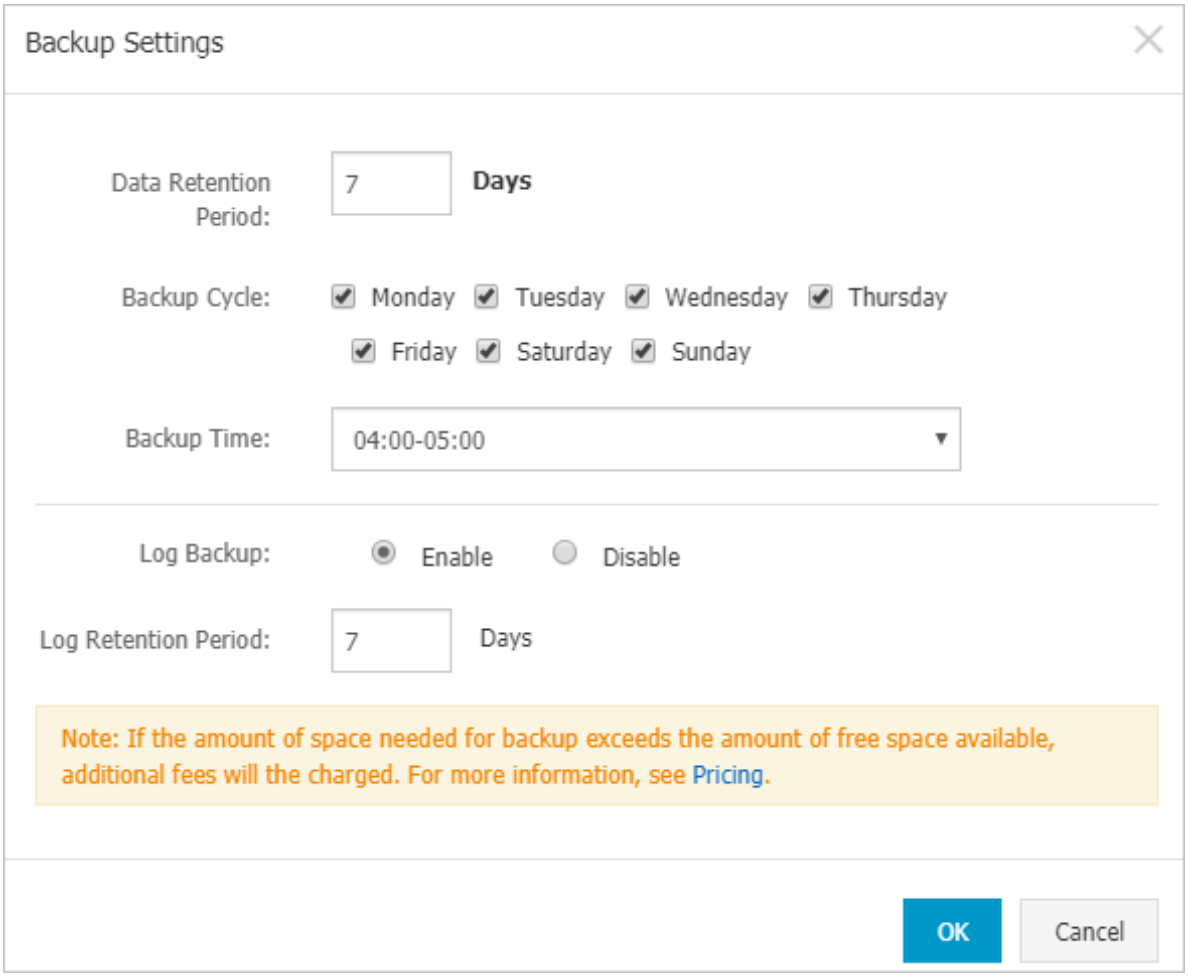
1. Log on to the *RDS console*.
2. In the upper-left corner, select the region where the target RDS instance is located.

3. Find the target RDS instance and click its ID.
4. In the left-side navigation pane, click Backup and Restoration.
5. 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 11-1: 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.

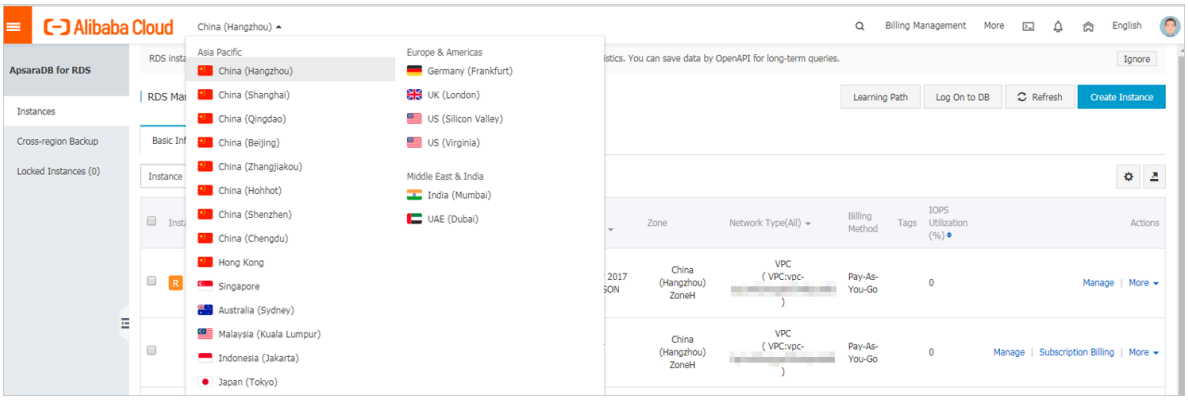
Parameter	Description
Log Backup	The status of the log backup function. **Notice:** If you disable the log backup function, all log backup files are deleted and the time-based data restoration function becomes unavailable.
Log Retention Period	· The number of days in which log backup files are retained. 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.



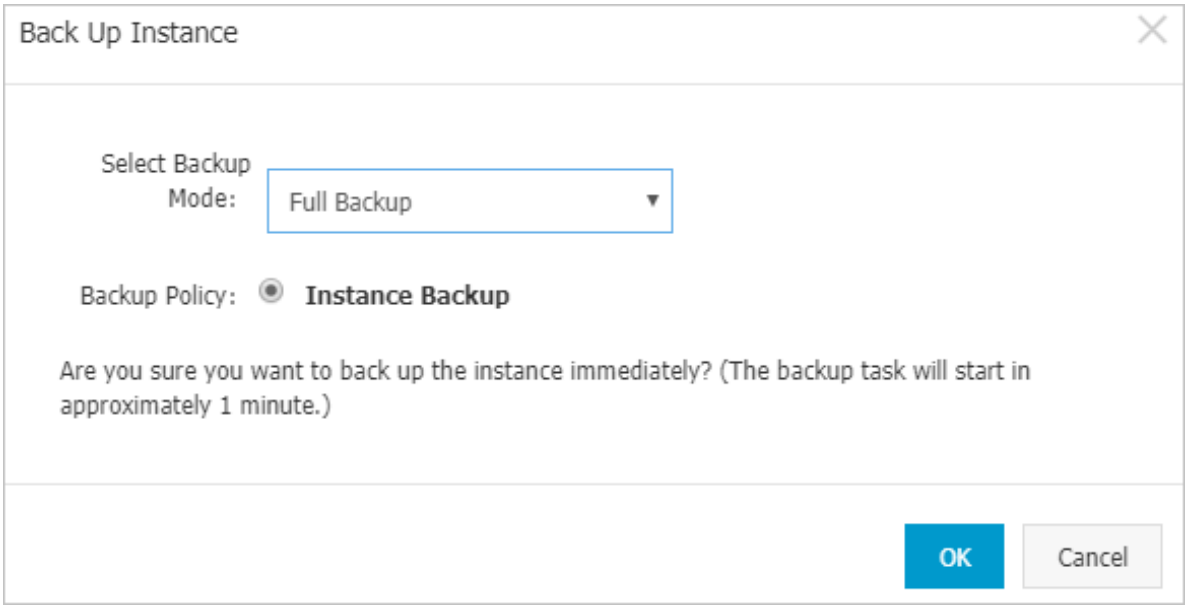
Manually back up data

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 upper-right corner of the Basic Information page, click Back Up Instance.



5. In the Back Up Instance dialog box, set the backup parameters and click OK.

FAQ

1. Can I disable the data backup function for an RDS for PPAS instance?

   No. The data backup function must be enabled. However, you can lower the backup frequency to at least two times a week. The backup file retention period ranges from 7 days to 730 days.

2. Can I disable the log backup function for an RDS for PPAS instance?

   Yes. You can disable the log backup function as needed.

APIs

API	Description
#unique_97	**Used to create a backup file for an RDS instance.**
#unique_98	**Used to view the list of backup files for an RDS instance.**
#unique_99	**Used to view the backup settings of an RDS instance.**
#unique_100	**Used to modify the backup settings of an RDS instance.**
#unique_101	**Used to delete the data backup files of an RDS instance.**
#unique_102	**Used to obtain the list of backup tasks for an RDS instance.**
#unique_103	**Used to obtain the log backup files of an RDS instance.**

11.2 View the quota of free backup space for an RDS for PPAS instance

This topic describes how to calculate and view the quota of free backup space for an RDS for PPAS 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)

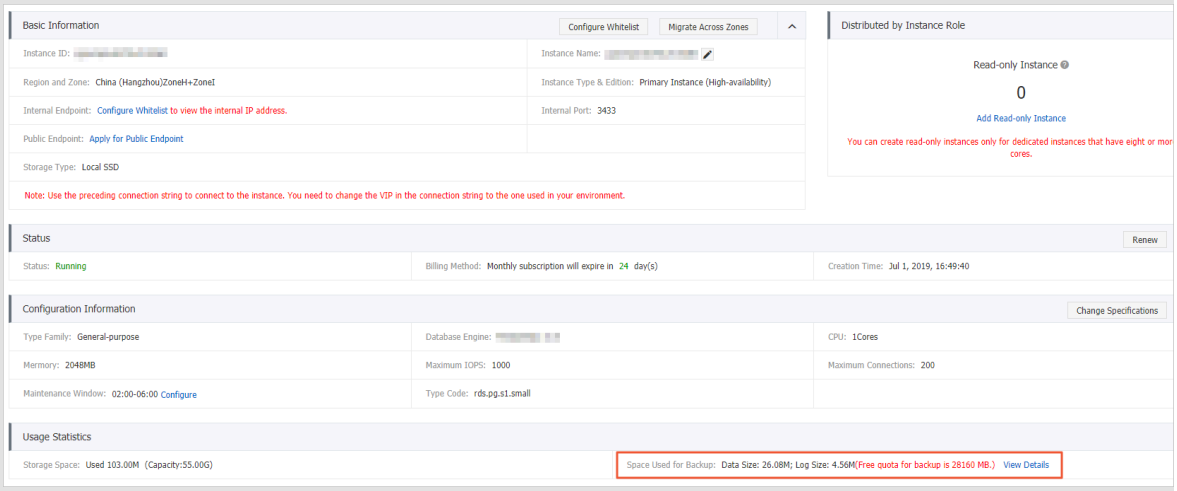
Backup space beyond the quota = Backup data size + Backup log size - Round up (50 % × Storage space purchased for the RDS instance) (Unit: GB)

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)
```

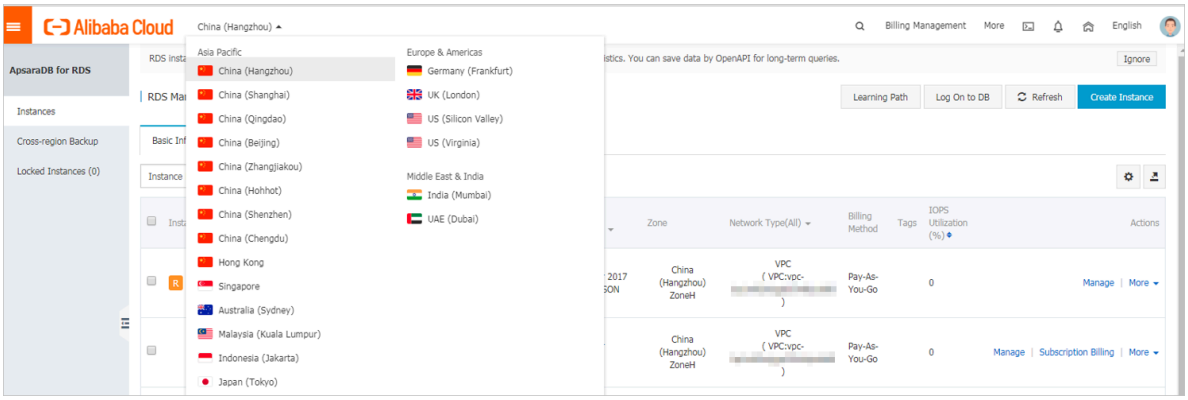
Note:

- **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.

11.3 Download the backup files of an RDS for PPAS instance

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

> **Note:**
> An RDS for PPAS instance does not support the download of data backup files. You can *restore the data of an RDS for PPAS instance* or migrate data from RDS for PPAS to an on-premises database.

Limits

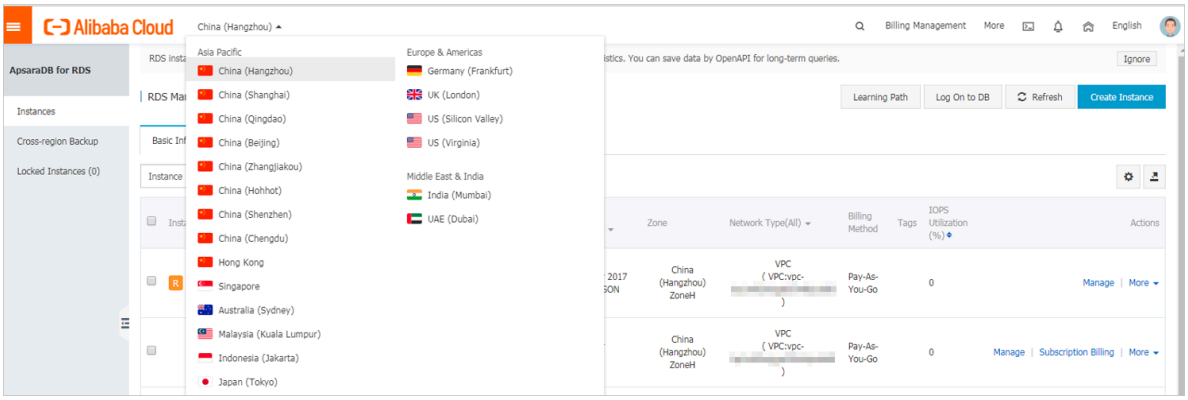
A RAM user who has only the read-only permissions cannot download backup files. You can add the required permissions to a RAM user in the RAM console. For more information, see *#unique_106*.

DB engine	Data backup download	Log backup download
PPAS	Not supported.	Supported by all versions.

Procedure

1. Log on to the *RDS console*.

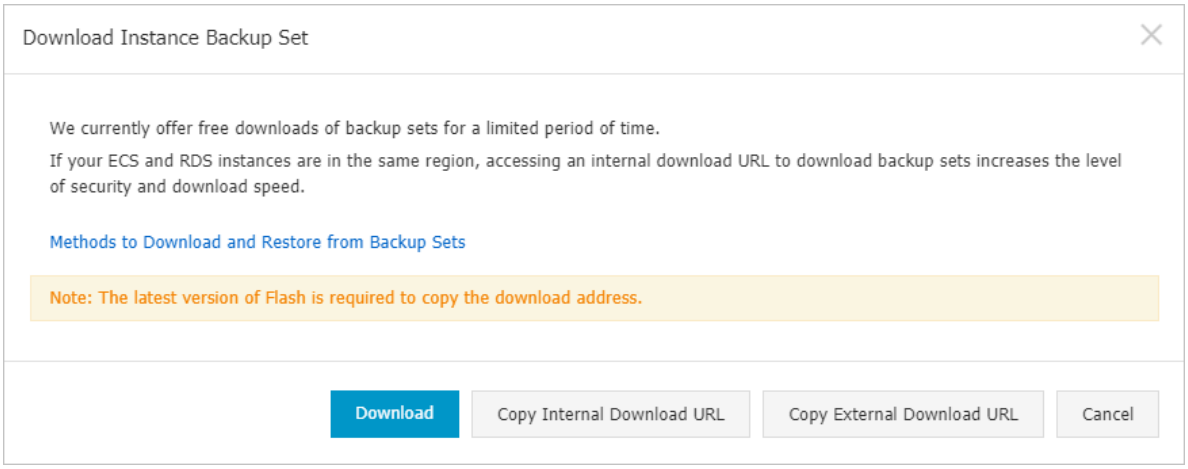
2. In the upper-left corner, select the region where the target RDS instance is located.



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 Archive List tab, select a time range and click Search. In the log backup file list, find the target log backup file and in the Actions colum 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 No. 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.
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 log 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 Data restoration

12.1 Restore the data of an RDS for PPAS instance

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

You can restore the data of an RDS for PPAS 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

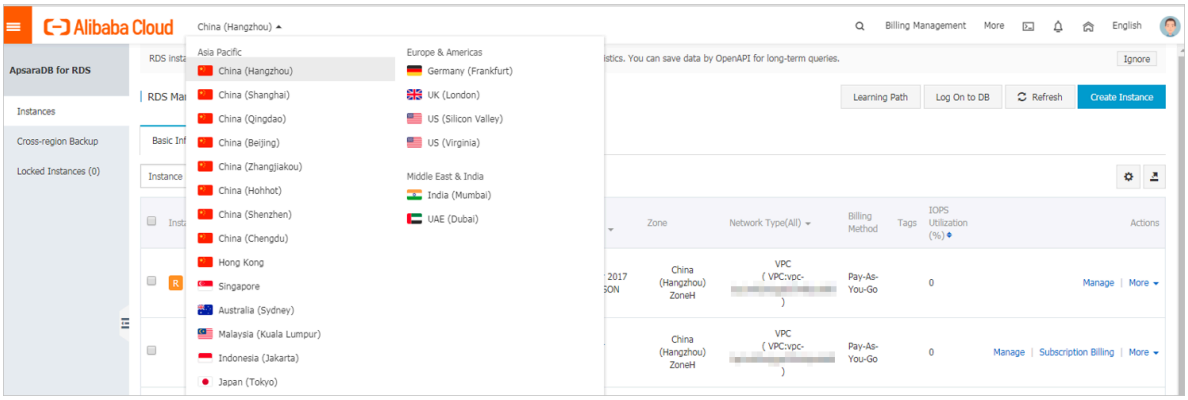
The original RDS instance must meet the following conditions:

- **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 *Back up the data of an RDS for PPAS 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 *Connect to an RDS for PPAS instance*.

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:

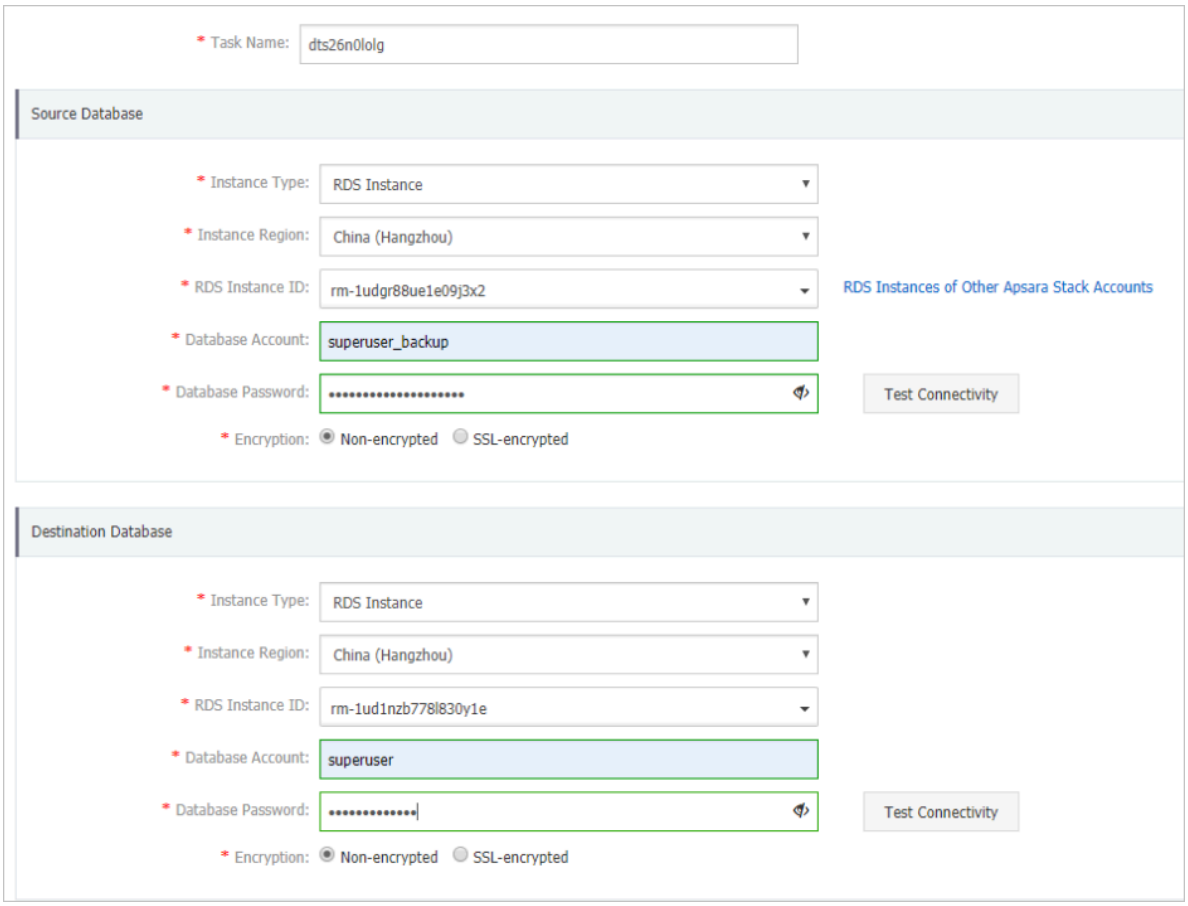
   - **Task Name: By default, DTS automatically generates a name for each migration task. You can change the name as needed.**
   - **Source Database**
     - **Instance Type: Select RDS Instance.**
     - **Instance Region: Select the region where the new RDS instance is located.**
     - **RDS Instance 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.**

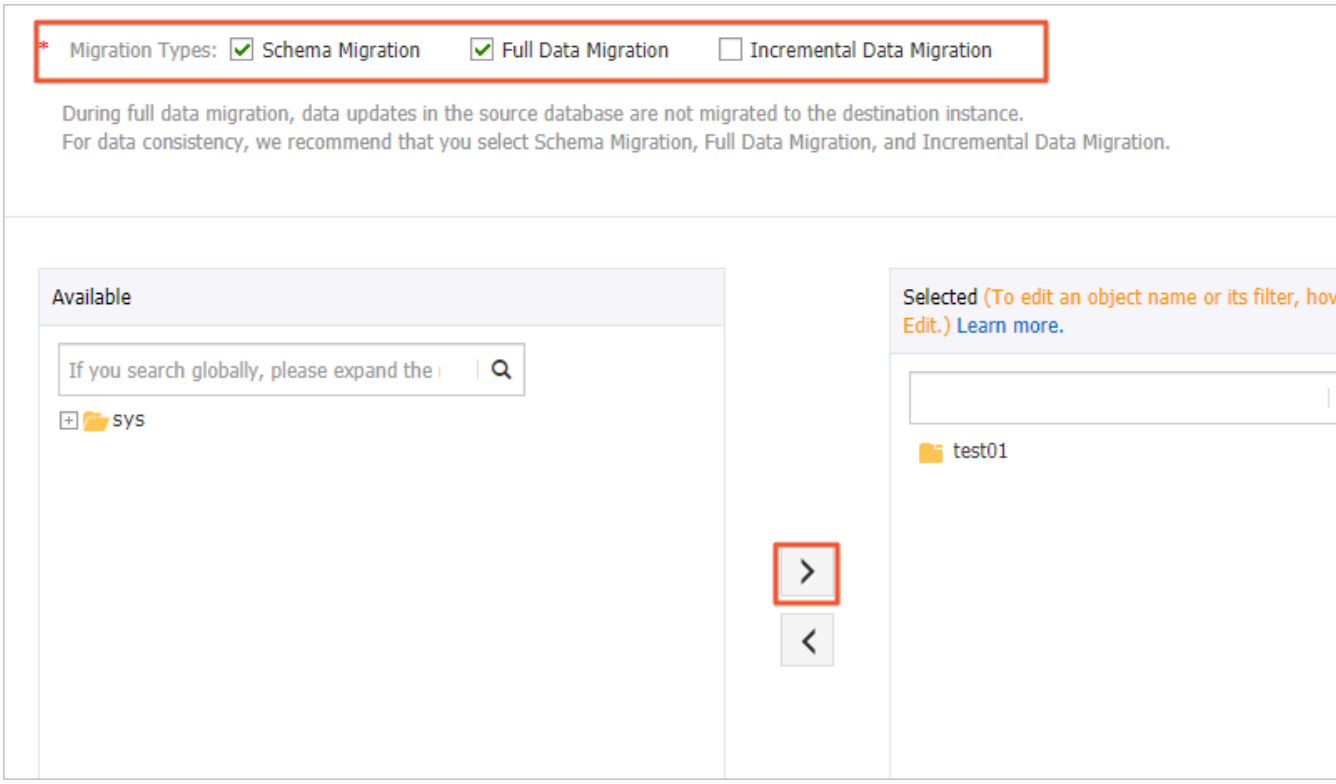
Note:

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:

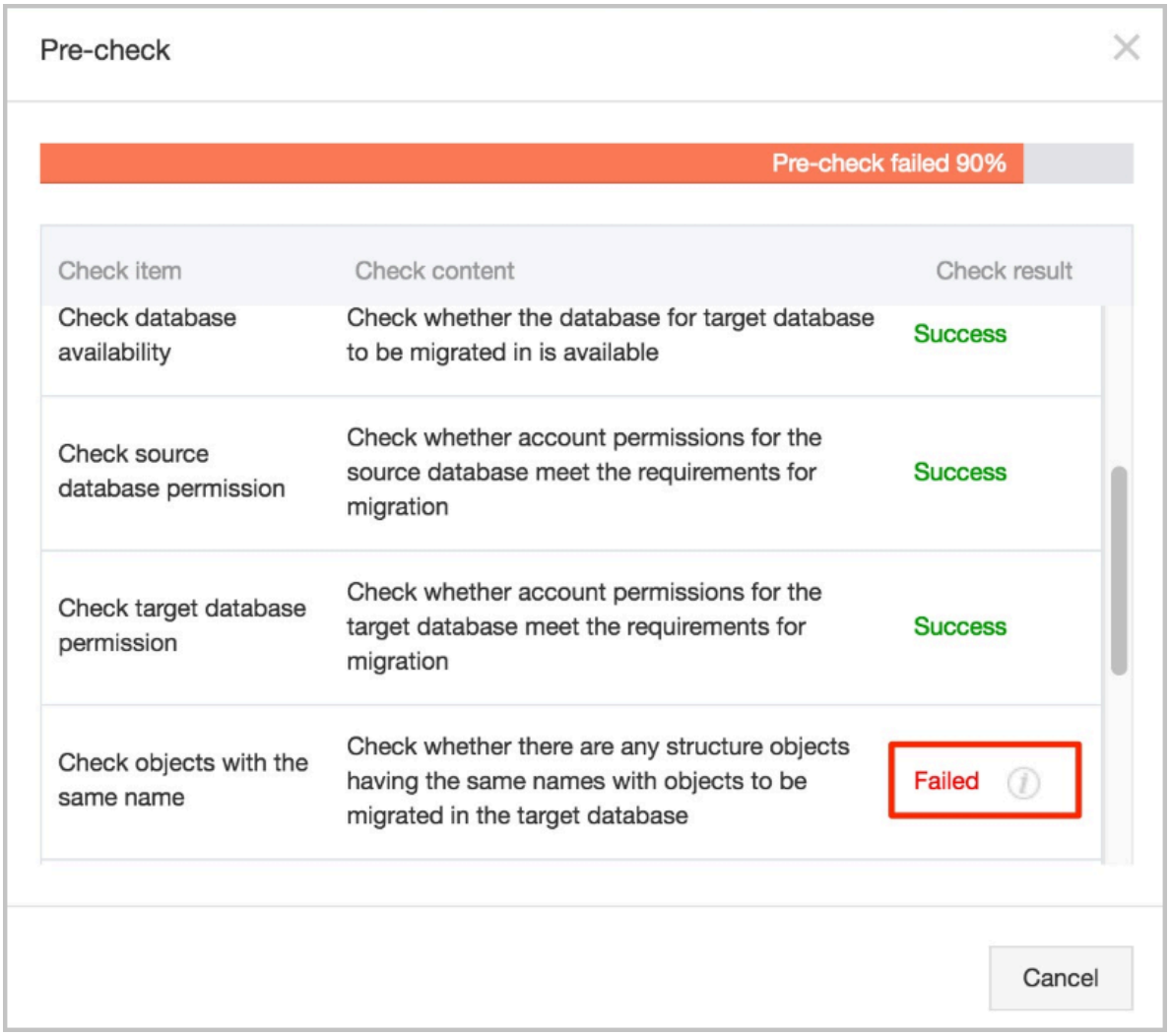
- **In the Selected section, move the pointer over the object whose name you want to change, click Edit, and in the displayed dialog box enter the new object name.**

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

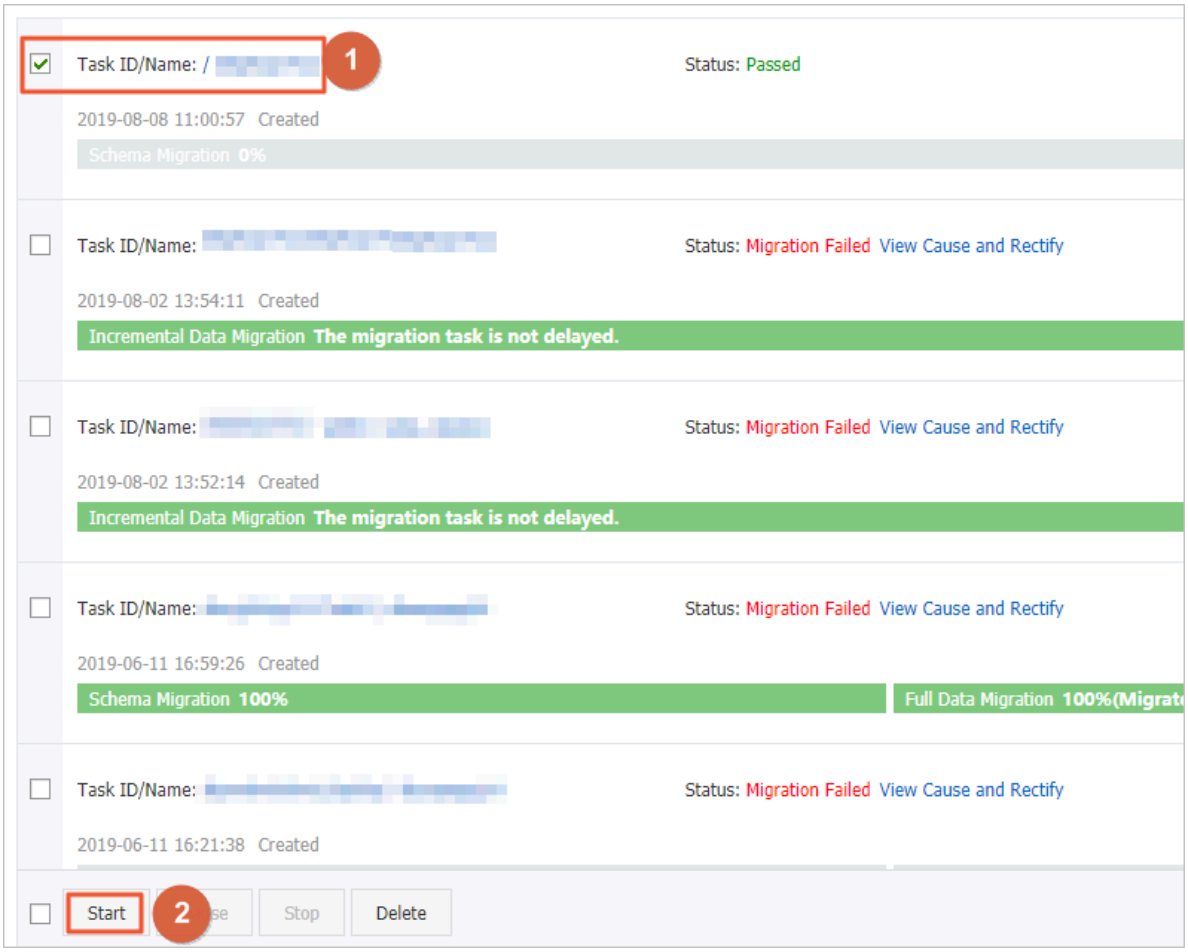


8. **Click Precheck.**

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.

13 Disable the database proxy mode

This topic describes how to disable the database proxy mode for an RDS for PPAS instance. Disabling the database proxy mode means switching to the standard mode, which helps improve the performance of the RDS instance.

Notice:
The database proxy mode may cause service instability in certain circumstances. For smooth service operation, we recommend that you upgrade the network connection mode of your RDS instance as soon as possible. For more information, see *#unique_110*.

Precautions

- **In the database proxy mode, the multi-statement function is enabled by default at the protocol layer. Therefore, after you disable the database proxy mode, if you do not enable the multi-statement function but run multiple SQL statements, the system reports errors in the SQL statements. To prevent this problem, you must check and add connection parameters in advance. For example, you can add the `allowMultiQueries` parameter to JDBC as follows:**

```
dbc:mysql:///test?allowMultiQueries=true
```

- **You can only disable the database proxy mode (that is, switch from the database proxy mode to the standard mode). You cannot enable the database proxy mode (that is, switch from the standard mode to the database proxy mode).**
- **Switching the access mode may cause a 30-second transient disconnection. Therefore, we recommend that you switch the access mode during off-peak hours or make sure that your application can automatically reconnect to the RDS instance.**

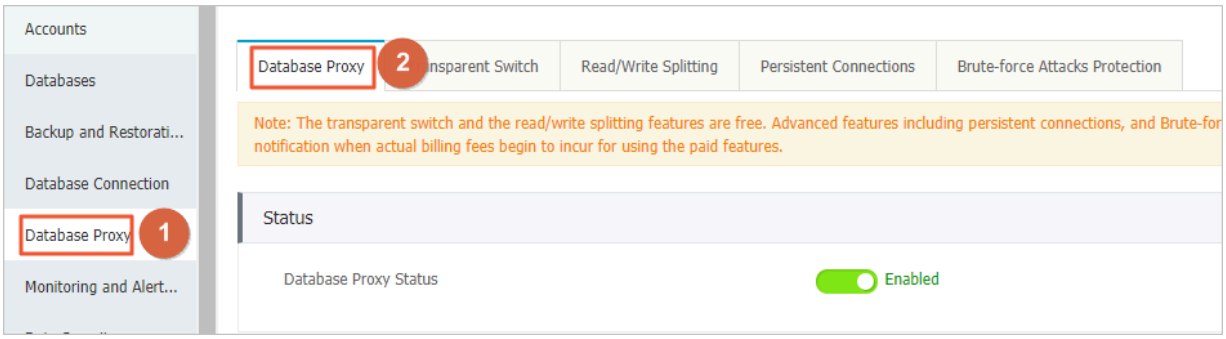
Prerequisites

The database proxy mode is enabled for your RDS instance.

Note:

- **If the Database Proxy tab is displayed, the database proxy mode is enabled and you can proceed with the operations described in this topic.**

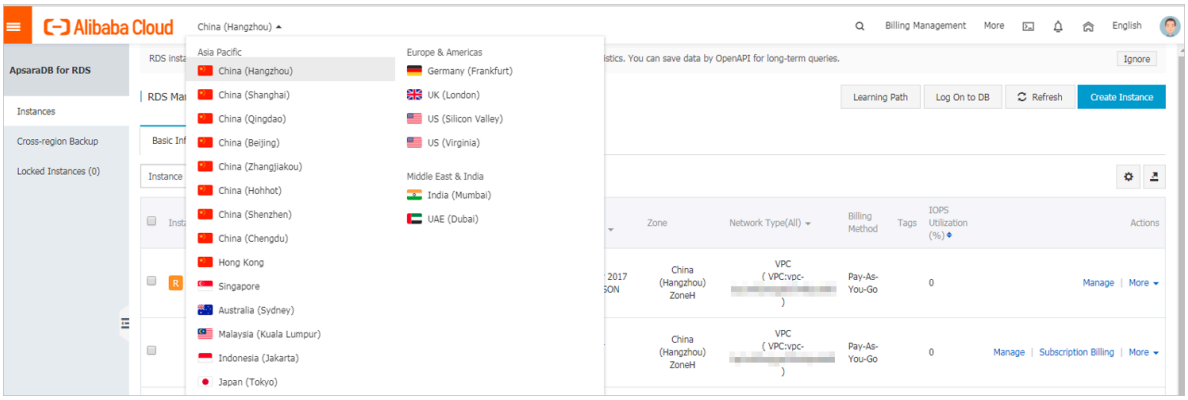
- **If the Database Proxy tab is not displayed, the database proxy mode is not displayed and you can skip this topic.**



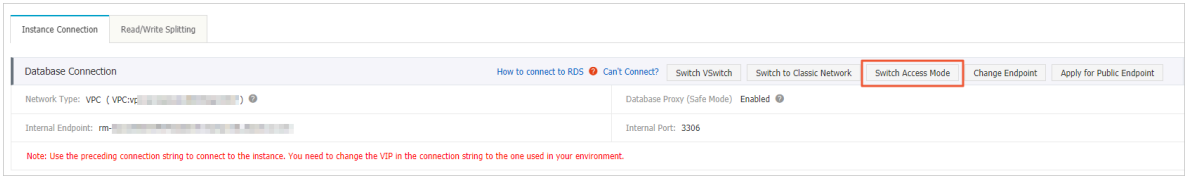
Procedure

Method 1

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 Switch Access Mode and in the displayed dialog box, click Confirm.**



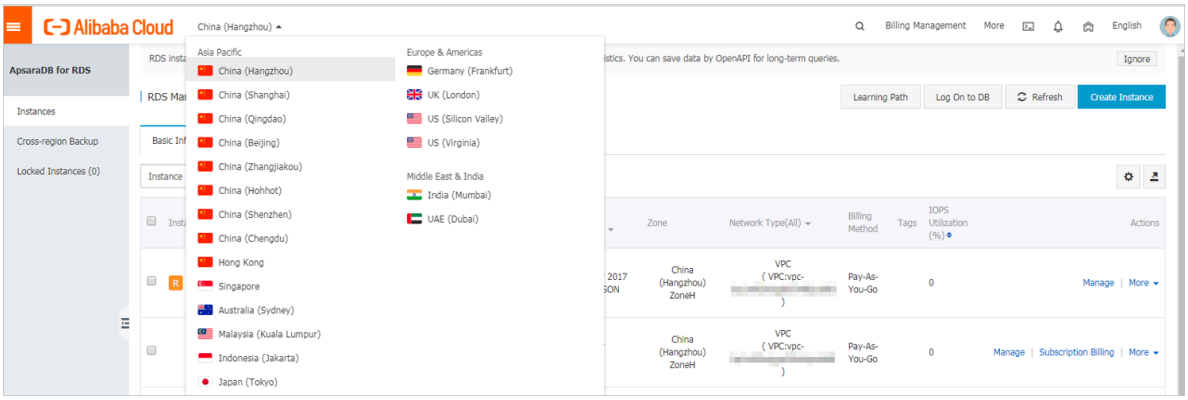
Note:

This button is available only when you have enabled the database proxy mode.

Method 2

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 Proxy.
5. On the Database Proxy tab, click the slider next to the database proxy status and in the displayed dialog box, click Confirm.

> **Note:**
> This tab page is available only when you have enabled the database proxy mode.

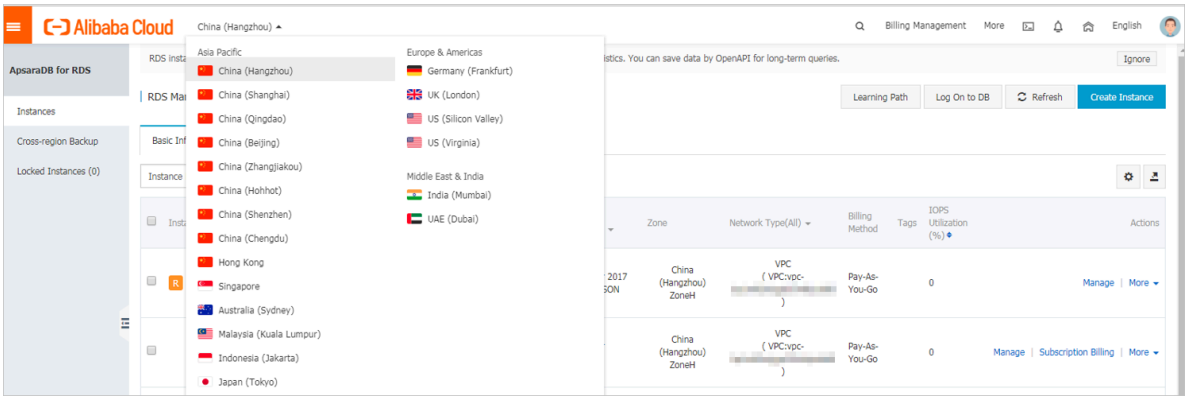
14 Manage logs

This topic describes how to manage logs through the RDS console or by using SQL statements. You can query error logs and slow query logs. The log query results help you to locate faults. All RDS for PPAS instances support log management.

- **For information about log backup policies and rules, see** *Back up the data of an RDS for PPAS instance*.
- **For information about how to download log backup files, see** *Download the backup files of an RDS for PPAS instance*.
- **For information about how to restore data through log backup files, see** *Restore the data of an RDS for PPAS 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 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. Similar SQL statements are displayed once only.
Primary/Secondary Instance Switch Log	Records logs related to the switchovers between the master and slave instances within the last one month.

Note:

For each RDS instance in the China (Zhangjiakou) region, the system retains only the error logs, slow query logs, and slow query log summary generated within the last nine days.

15 Tag management

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.

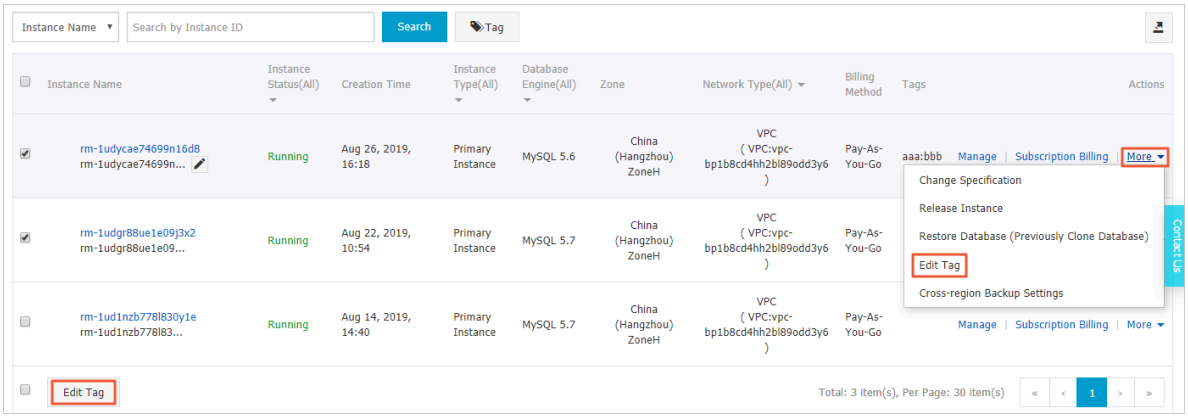
Limits

- **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

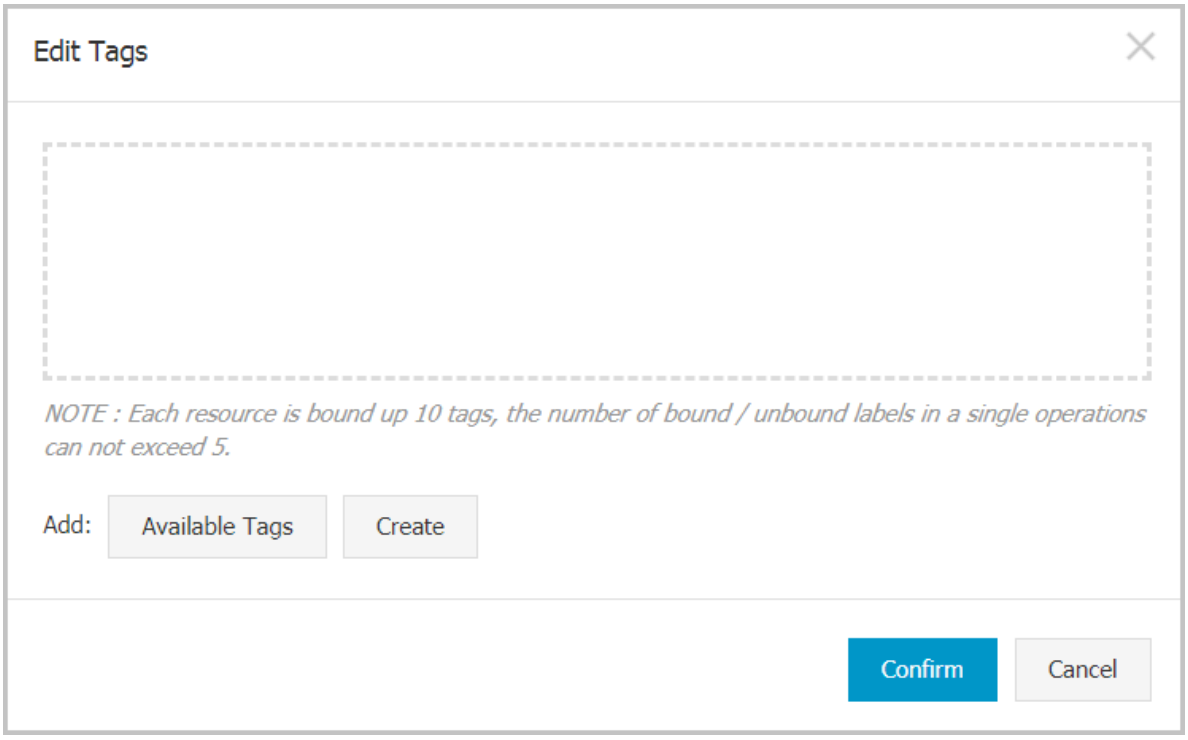
1. **Log on to the *RDS console* and in the left-side navigation pane, click Instances.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**

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

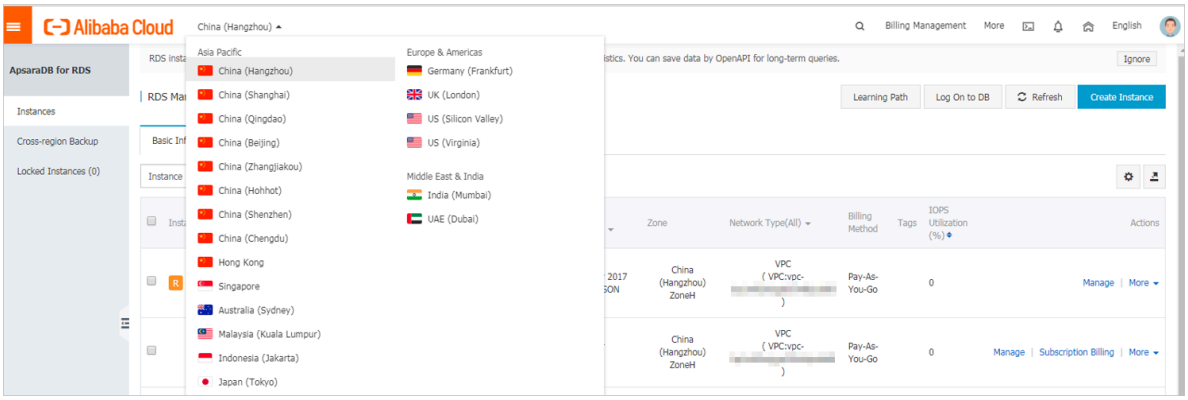
This topic describes how to delete tags from an RDS instance when you no longer need the tags or due to adjustments to the instance.

Limits

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

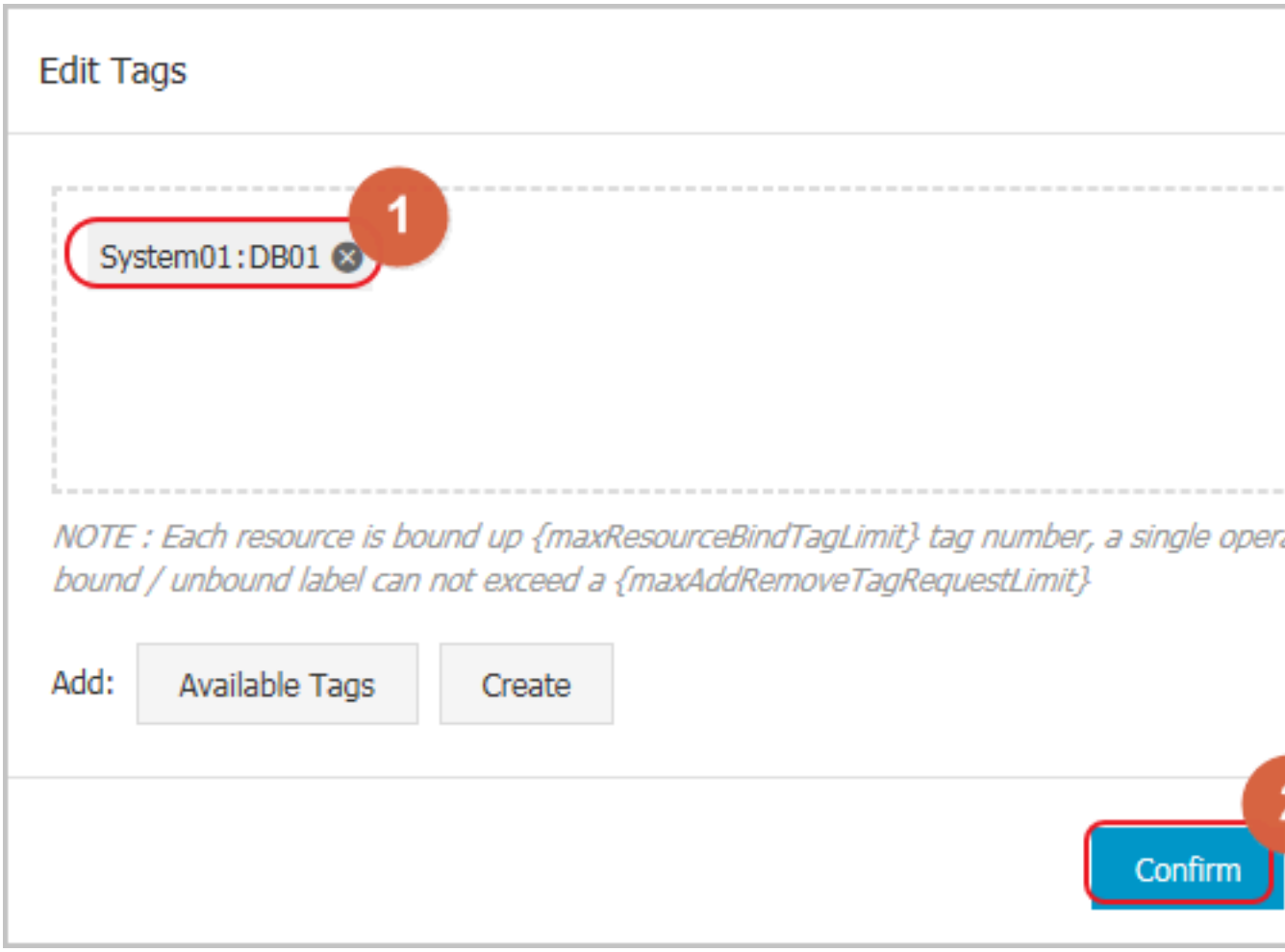
Procedure

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

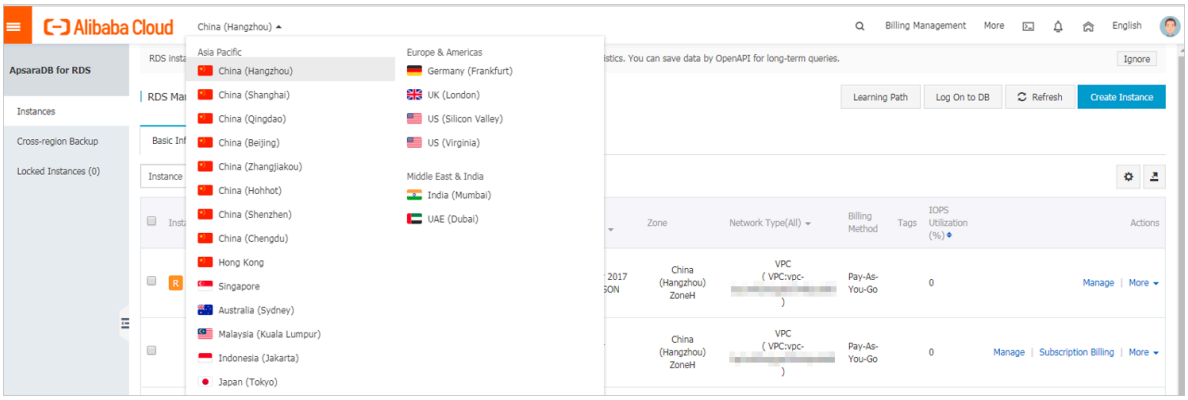
API	Description
#unique_116	**Used to unbind a tag from an RDS instance.**

15.3 Filter RDS instances by tag

This topic describes how to filter RDS instances by tag.

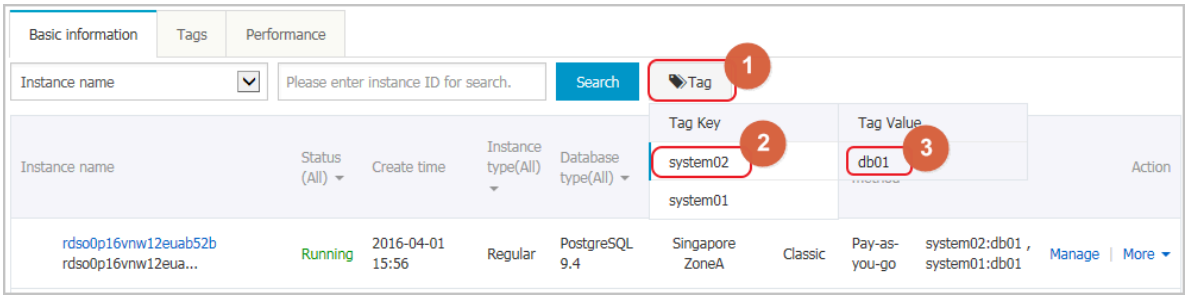
1. **Log on to the** *RDS console*.

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.