# Alibaba Cloud ApsaraDB for RDS

## RDS for PostgreSQL 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

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

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

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

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

## Disclaimer

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

Terms

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

General terms

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

# 2 Limits of RDS for PostgreSQL

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

**The following table describes the limits of RDS for PostgreSQL.**

| Operations | RDS restrictions |
| --- | --- |
| Modify database parameter settings | Currently it is not supported. |
| Database root permission | RDS does not offer the superuser permission. |
| Database backup | Data backup can only be performed through pg_dump. |
| Data migration | Data backed up through pg_dump can only be restored through psql. |
| Build database replication | The system automatically builds the HA mode based on PostgreSQL stream replication.<br>The PostgreSQL standby node is invisible and cannot be accessed directly. |
| Restart the RDS instance | The instance must be restarted through the RDS console or OpenAPI. |
| Network setting | If the *access mode* of the instance is safe connection mode, enabling net.ipv4.tcp_timestamps in SNAT mode is not allowed. |

# 3 New features

**This topic describes the new product features of ApsaraDB RDS for PostgreSQL.**

July 2019

| Feature | Description | Release date | Available regions | References |
| --- | --- | --- | --- | --- |
| High-performance storage | Supports the ESSD storage type. ESSD is an ultra-high-performance cloud disk product that has the following benefits:<br>· High read/write performance. The maximum IOPS of a single disk is increased from 25 thousand to 1 million.<br>· More storage space. The storage space is increased from 2 TB to 32 TB.<br>· Flexible configuration of storage spaces and specifications. The instance configuration can consist of a 4-core CPU and 32 TB storage space. | July 1, 2019 | China (Qingdao)<br>China (Beijing)<br>China (Zhangjiakou-Beijing Winter Olympic)<br>China (Hohhot)<br>China (Hangzhou)<br>China (Shanghai)<br>China (Shenzhen)<br>China (Hong Kong) | #unique_8 |

| Feature | Description | Release date | Available regions | References |
| --- | --- | --- | --- | --- |
| Risk control | The operations that may trigger risks must be confirmed by a verification code sent from SMS, improving the operation security. | July 1, 2019 | China (Qingdao)<br>China (Beijing)<br>China (Zhangjiakou-Beijing Winter Olympic)<br>China (Hohhot)<br>China (Hangzhou)<br>China (Shanghai)<br>China (Shenzhen)<br>China (Hong Kong) | N/A |

# 4 Quick start

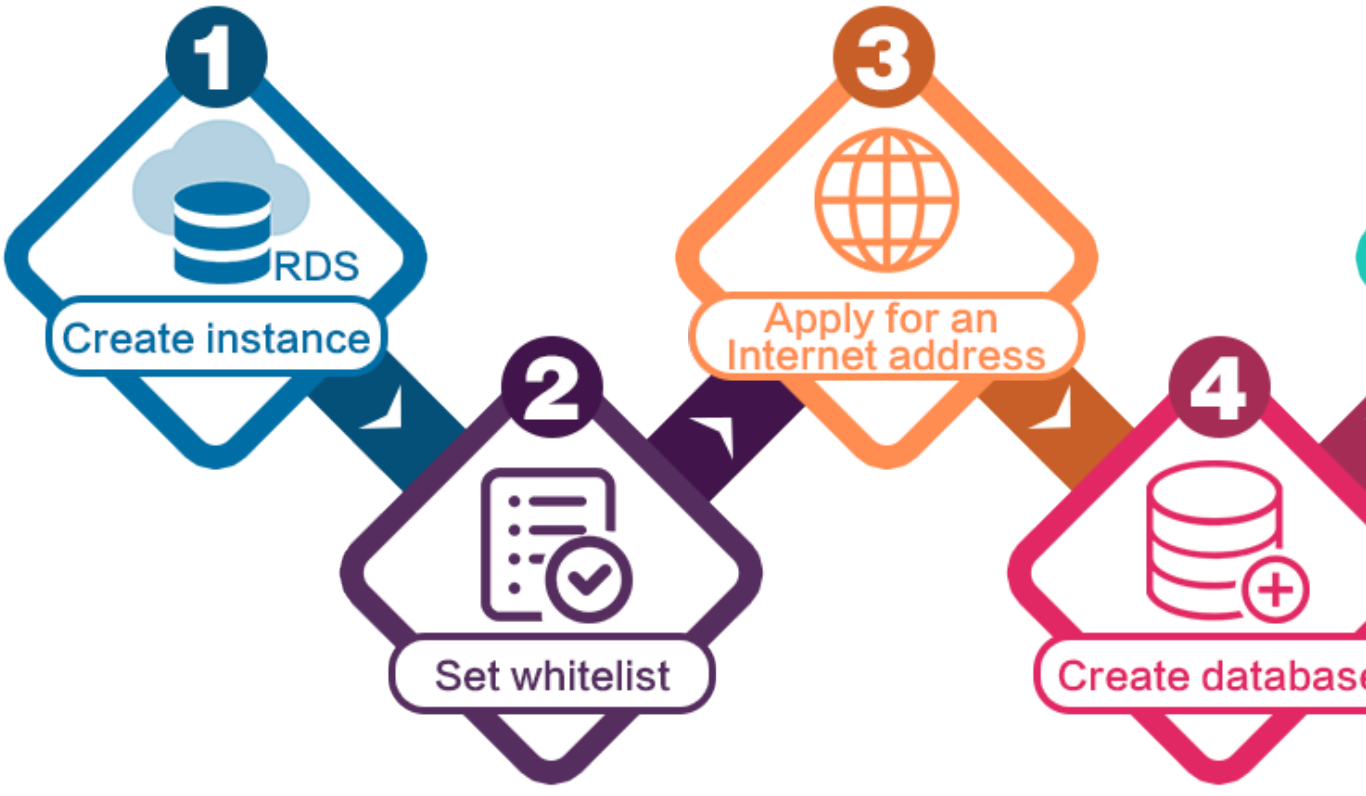
## 4.1 General process to use RDS for PostgreSQL

**This topic describes the general process from purchasing an RDS for PostgreSQL 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 PostgreSQL, read** *Limits of RDS for PostgreSQL* **before you purchase an RDS for PostgreSQL instance.**

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



# 4.2 Create an RDS for PostgreSQL instance

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

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

**For information about the pricing of RDS for PostgreSQL instances, see** *#unique_13*.

## Prerequisites

**You have registered an Alibaba Cloud account.**

**For more information, see** *Sign up with Alibaba Cloud*.

**By**

## 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:<br>· Select the same region as the corresponding ECS instance to avoid incurring charges for Internet traffic usage and guarantee fast access.<br>· Check whether the selected region supports your required MySQL version and whether multi-zone support is available. |
| Database Engine | Select a DB engine.<br>In this example, select MySQL.<br>Note:<br>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.<br>Note:<br>The available versions vary depending on the region you select. |

| Parameter | Description |
| --- | --- |
| Edition | Select an RDS edition. Valid values:<br>· 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.<br>· 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.<br>· 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.<br>Note:<br>The available editions vary depending on the DB engine version you select. For information about the RDS editions, see #unique_15. |
| Storage Type | Select a storage type. Valid values:<br>· Local SSD: An SSD that is located on the same node as the DB engine. Storing data to local SSDs reduces I/O latency.<br>· 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.<br>· 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.<br>For more information, see #unique_8. |

| Parameter | Description |
| --- | --- |
| Zone | Select a zone.<br>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.<br>Multi-zone deployment is more secure because it provides zone-level disaster tolerance. |
| Network Type | Select a network type. Valid values:<br>· Classic Network: indicates a traditional network.<br>· 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.<br>Note:<br>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.<br>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_16*.<br>Valid values:<br>· 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.<br>· Dedicated instance: provides dedicated CPU, memory, storage, and I/O resources.<br>· Dedicated host: provides all the CPU, memory, storage, and I/O resources on the server where it is located.<br>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:**

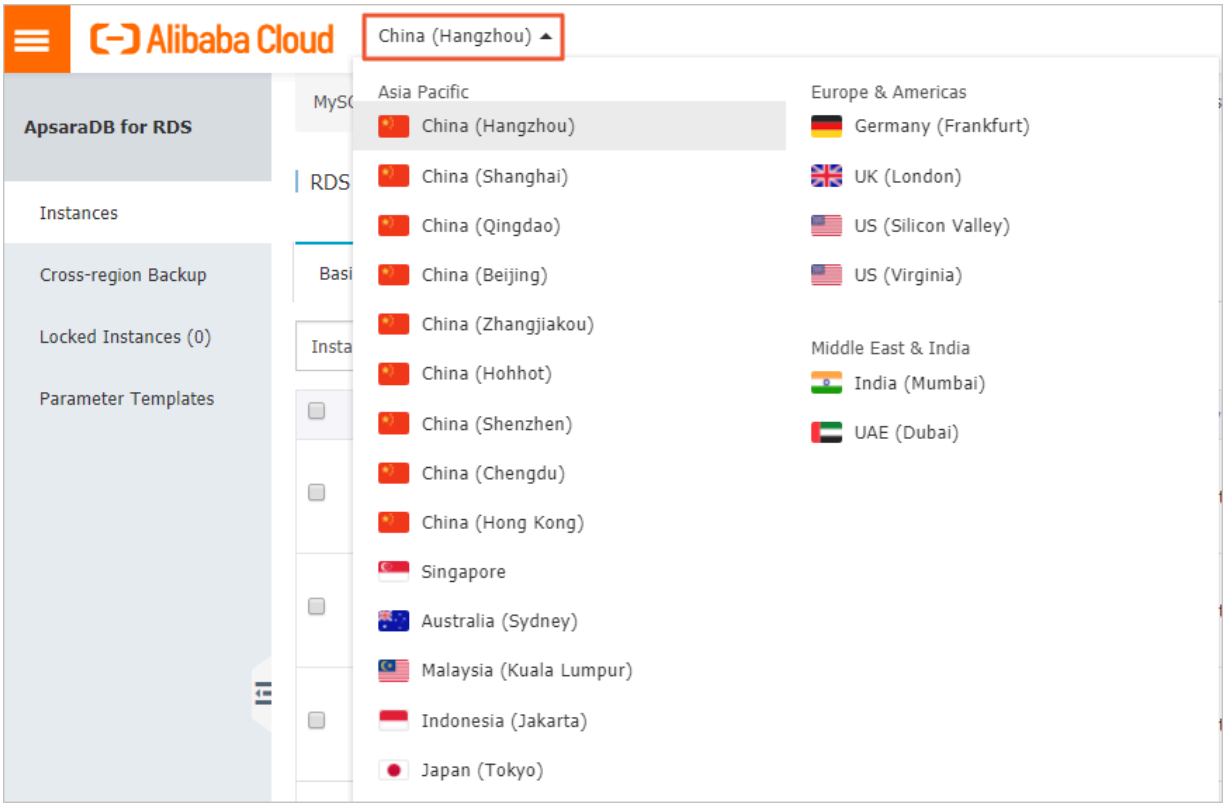
   For a subscription instance, you can:

   - 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_21* | **Used to create an RDS instance.** |

## 4.3 Configure a whitelist for an RDS for PostgreSQL instance

**This topic describes how to configure a whitelist for an RDS for PostgreSQL instance. After you create an RDS instance, you must configure a whitelist for it to allow external devices to access the instance.**

**RDS for PostgreSQL provides two types of whitelists:**

- **IP address whitelist: Add IP addresses to a whitelist so that these IP addresses can access the RDS instance.**

> **Note:**

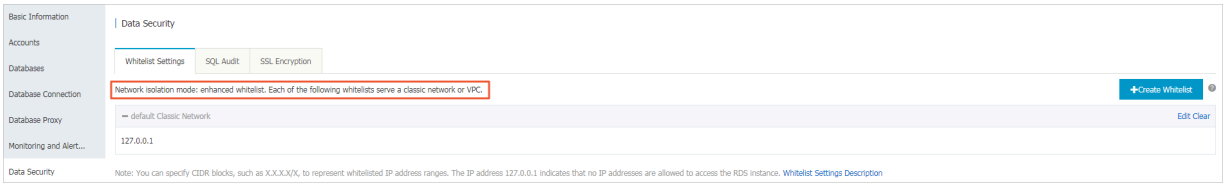
**The default whitelist is an IP address whitelist that contains only the default IP address 127.0.0.1. This default IP address means that no devices can access the RDS instance.**

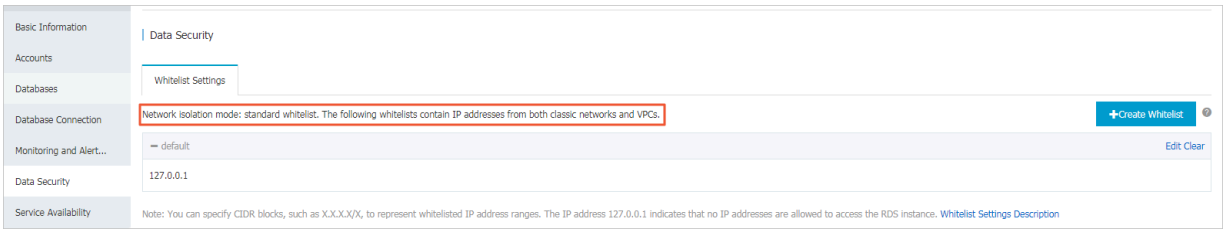
- **VPC security group whitelist: Add a VPC security group to a whitelist so that all ECS instances in the VPC security group can access the RDS instance.**

**We recommend that you periodically check and adjust your whitelists to maintain RDS security. Configuring a whitelist does not affect the normal running of the RDS instance.**

Precautions

- **The default IP address whitelist can be modified or cleared but cannot be deleted .**
- **Up to 1,000 IP addresses or CIDR blocks can be added to each IP address whitelist. If you want to add a large number of IP addresses, we recommend that you merge them into CIDR blocks, for example, 192.168.1.0/24.**
- **If you attempt to connect the RDS instance to DMS without adding the IP address of DMS to a whitelist of the RDS instance, the system displays a message, stating that you can connect to DMS only after you add the IP address of DMS to a whitelist of the RDS instance.**
- **Before configuring a whitelist, you must confirm which network isolation mode the RDS instance works in. Then you can decide which operations you must take accordingly.**



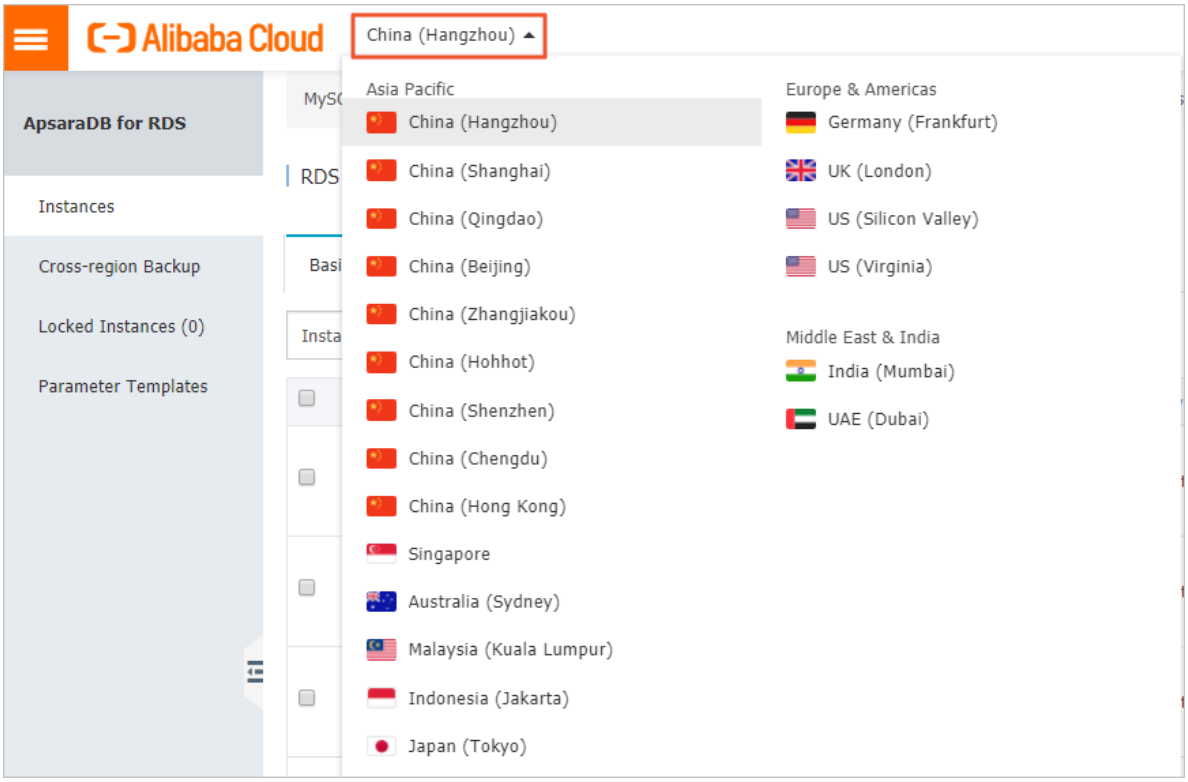




Procedure

**To configure an enhanced whitelist, follow these steps:**

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

2. Select the target region.

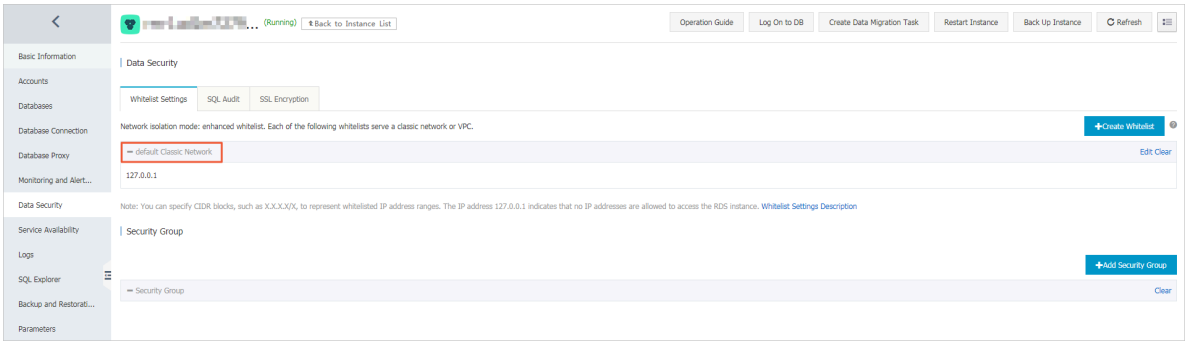



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Data Security.
5. On the Whitelist Settings tab, select the whitelist you want to modify. Detailed steps are as follows:
   - If you want to connect the RDS instance to an ECS instance that is located in a VPC, click Edit in the `default VPC` whitelist.
   - If you want to connect the RDS instance to an ECS instance that is located in a classic network, click Edit in the `default Classic Network` whitelist.
   - If you want to connect the RDS instance to a server or host that is located outside the Alibaba Cloud, click Edit in the `default Classic Network` whitelist.

**Note:**

- If you want to connect the RDS instance to an ECS instance through a private IP address (on a VPC or classic network), make sure that the RDS instance and ECS instance have the same network type. If their network types are different, they cannot communicate. For more information, see *#unique_22*.

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

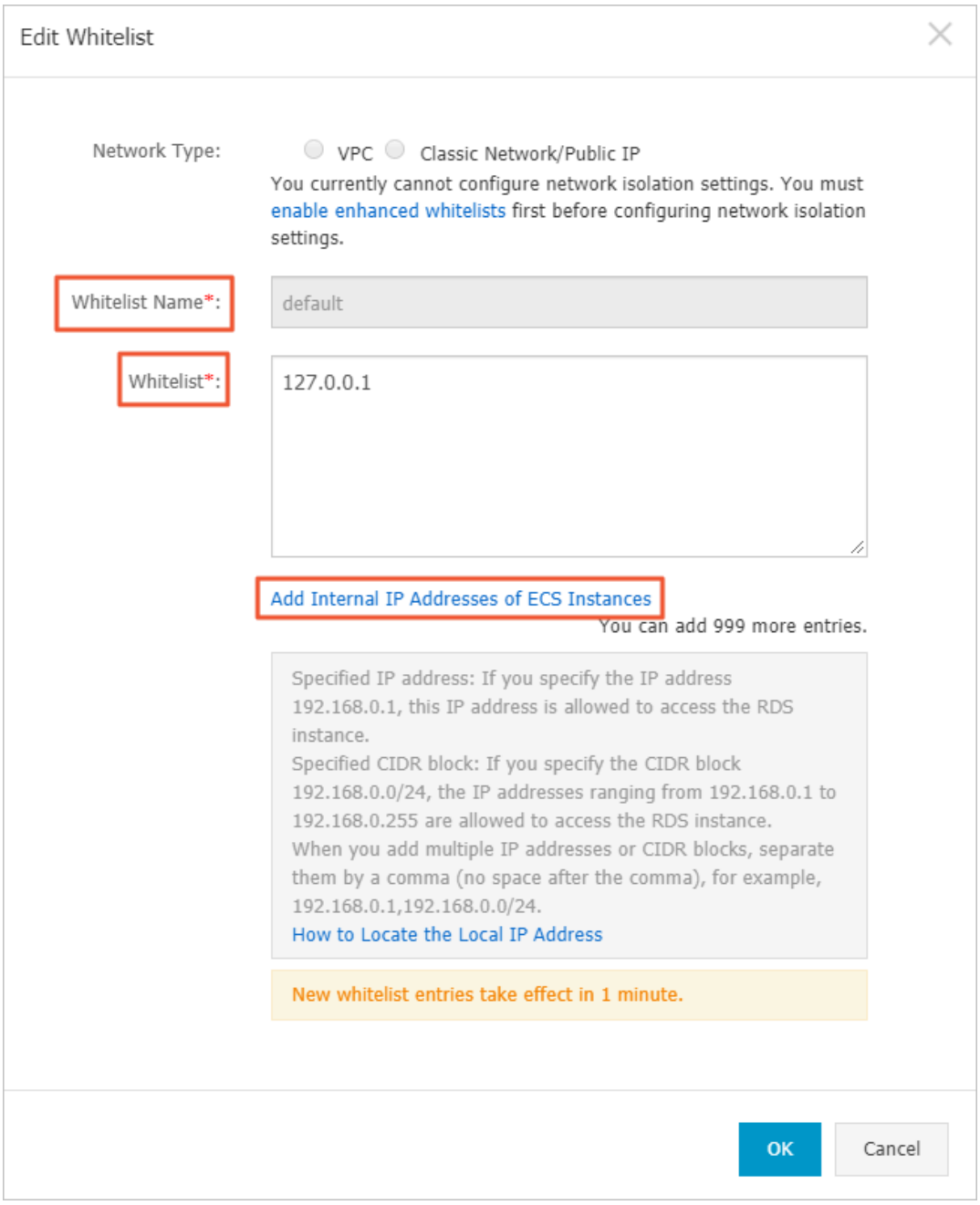



6. In the displayed dialog box, enter IP addresses or CIDR blocks and click OK. Detailed rules are as follows,

   - If you enter a CIDR block, for example, 10.10.10.0/24, then any IP addresses in 10.10.10.*X* format can access the RDS instance.
   - If you want to enter more than one IP address or CIDR block, you must separate them by using commas (,) and leave no spaces preceding or following the commas, for example, 192.168.0.1,172.16.213.9.
   - If you click Add Internal IP Addresses of ECS Instances, then the IP addresses of all ECS instances under your Alibaba Cloud account are displayed in the Whitelist field.

**Note:**

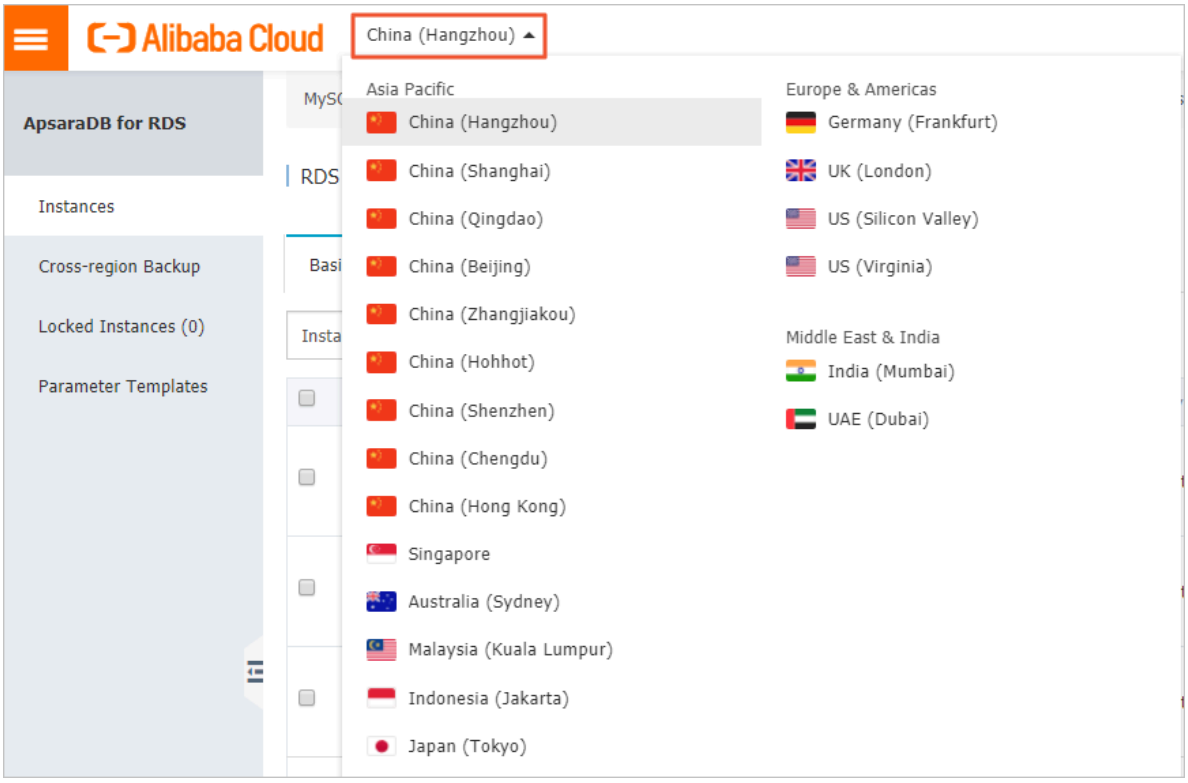
**After you add IP addresses or CIDR blocks to the default whitelist, the system automatically deletes the default IP address 127.0.0.1.**




**To configure a standard whitelist, follow these steps:**

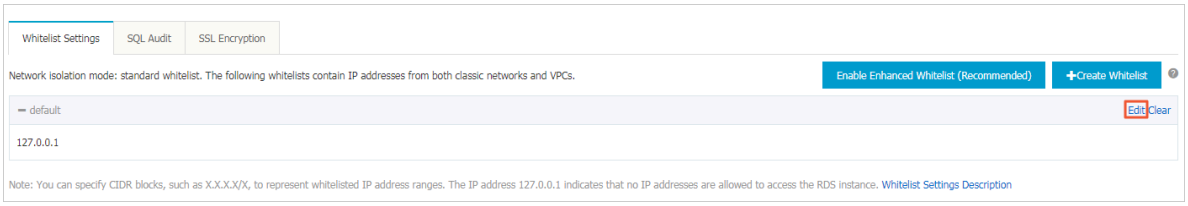
1. **Log on to the** *RDS console*.

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 Edit in the default whitelist.

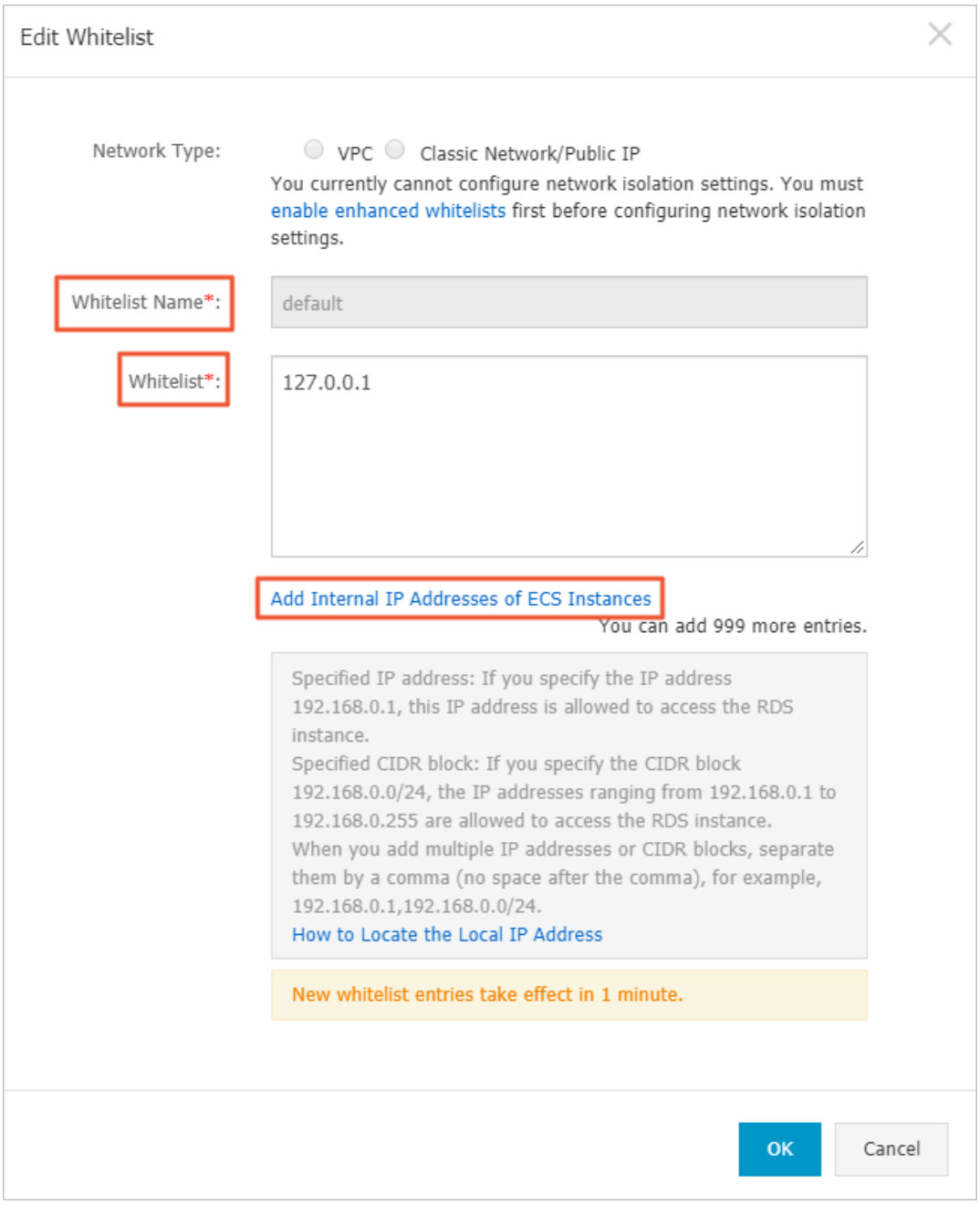
> **Note:**
> You can also click Create Whitelist to create a whitelist.



6. **In the Edit Whitelist dialog box, enter IP addresses or CIDR blocks and click OK. Detailed rules are as follows,**
   - **If you enter a CIDR block, for example, 10.10.10.0/24, then any IP addresses in 10.10.10.*X* format can access the RDS instance.**
   - **If you want to enter more than one IP address or CIDR block, you must separate them by using commas (,) and leave no spaces preceding or following the commas, for example, 192.168.0.1,172.16.213.9.**
   - **If you click Add Internal IP Addresses of ECS Instances, the IP addresses of all ECS instances under your Alibaba Cloud account are displayed in the Whitelist field.**

    **Note:**

**After you add IP addresses or CIDR blocks to the default whitelist, the system automatically deletes the default IP address 127.0.0.1.**




Common configuration errors

- **The whitelist contains only the default IP address 127.0.0.1. The IP address 127.0.0.1 indicates that no devices are allowed to access the RDS instance. Therefore, you must add the IP addresses of the devices to be connected to the RDS instance to the whitelist.**

- **The IP addresses you add to the whitelist are in 0.0.0.0 format, but the correct format is 0.0.0.0/0.**

  **Note:**
  **The entry 0.0.0.0/0 indicates that all devices can access the RDS instance.**

- *The enhanced whitelist mode* **is enabled for the RDS instance, and the IP addresses are added to an inappropriate whitelist. When you add IP addresses:**
  - **If you want the ECS instance to communicate with the RDS instance through a private endpoint in a VPC, make sure that the private IP address of the ECS instance is added to the default VPC whitelist.**
  - **If you want the ECS instance to communicate with the RDS instance through a private endpoint in a classic network, make sure that the private IP address of the ECS instance is added to the default Classic Network whitelist.**
  - **If you use** *ClassicLink* **to access the private endpoint of the RDS instance, make sure that the private IP address of the ECS instance is added to the default VPC whitelist.**
  - **If you want the ECS instance to communicate with the RDS instance through the Internet, make sure that the public IP address of the ECS instance is added to the default Classic Network whitelist. The default VPC whitelist cannot be used for communication through the Internet.**
- **The public IP address you added to a whitelist are invalid. This may occur if the public IP address you added is not the real outbound IP address. Possible reasons are as follows:**
  - **The public IP address dynamically changes.**
  - **The IP address query tool or website yields inaccurate results.**

  **For more information, see** *#unique_24*.

Configure a VPC security group

**A VPC security group is a virtual firewall that is used to set network access control for one or more ECS instances. After a VPC security group is added to a whitelist for the RDS instance, all ECS instances in the VPC security group can access the RDS instance.**

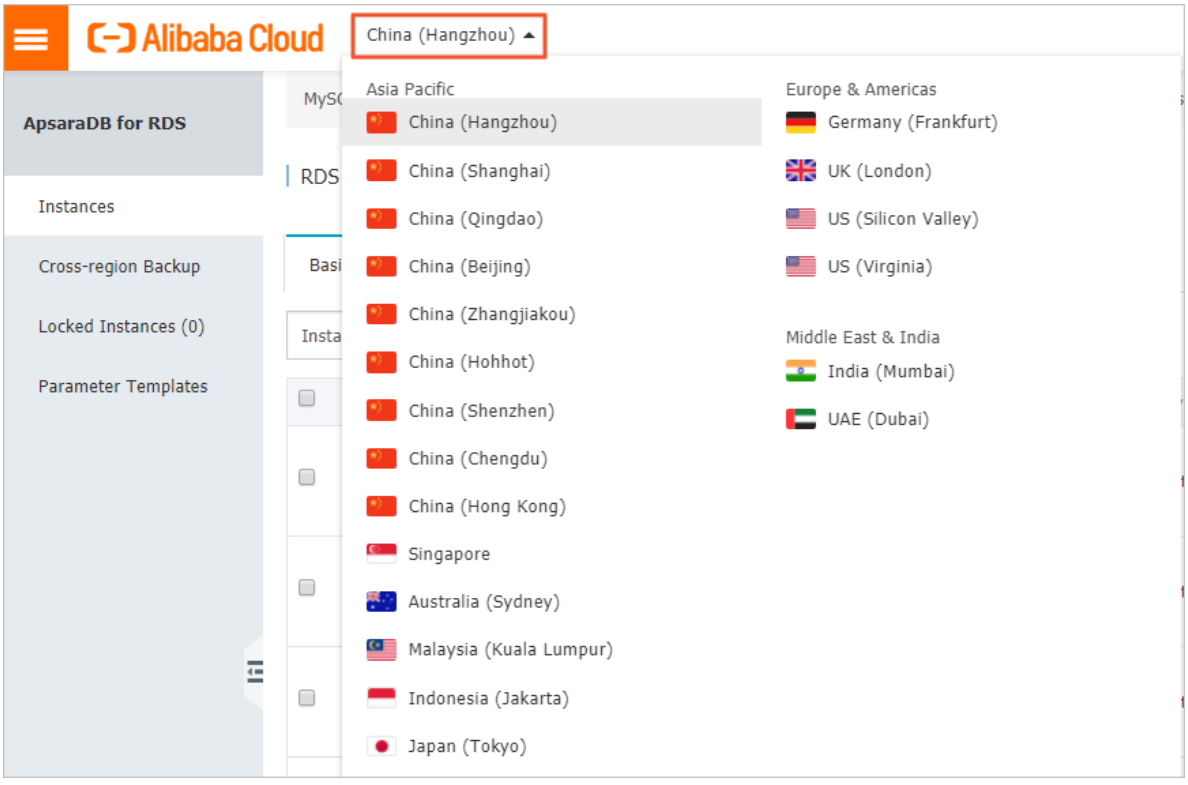
**For more information, see** *Create a security group*.

**Precautions**

- The DB versions and editions that support VPC security groups are PostgreSQL 10 High-availability Edition (with local SSDs), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4.
- The regions that support VPC security groups are China (Hangzhou), China ( Qingdao), and China (Hong Kong).
- You can have one VPC security group whitelist and multiple IP address whitelists . All IP addresses in the IP address whitelists and all ECS instances in the VPC security group whitelist can access the RDS instance.
- One RDS instance supports only one VPC security group whitelist.
- After you update the VPC security group whitelist, the new VPC security group whitelist takes effect immediately.

### 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 Data Security.
5. On the Whitelist Settings tab, click Add Security Group.

**Note:**

An ECS security group with a VPC tag is located in a VPC.

6. Select an ECS security group and click OK.

APIs

| API | Description |
| --- | --- |
| #unique_25 | Used to view the IP address whitelists of an RDS instance. |
| #unique_26 | Used to modify the IP address whitelists of an RDS instance. |

## 4.4 Create databases and accounts for an PostgreSQL instance

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

Before an RDS instance can be used, you must create databases and accounts for it.

Account types

RDS for PostgreSQL support two types of accounts: premier accounts and standard accounts.

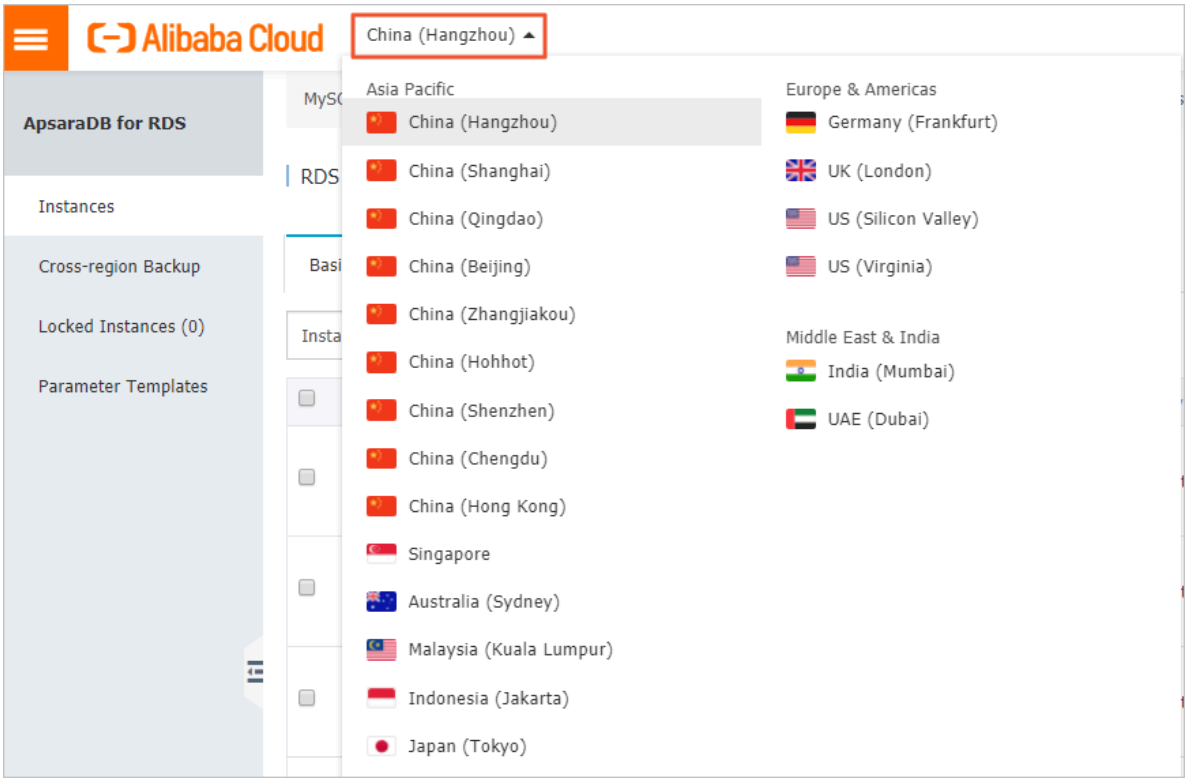
| Account type | Description |
| --- | --- |
| Premier account | · Can only be created and managed through the RDS console or API.<br>· Has only one premier account, which can manage all standard accounts and databases in the RDS for PostgreSQL instance.<br>· Has more permissions for fine-grained, personalized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

Precautions

- **Databases under a single instance share all the resources of this instance. Each RDS for PostgreSQL instance supports one premier account, countless standard accounts, and countless databases. You must create and manage standard accounts and databases through SQL statements.**
- **To migrate your on-premises database to an RDS instance, you must create the same databases and accounts for the RDS instance as your 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, set strong passwords for the accounts and change the passwords regularly.**

Procedure

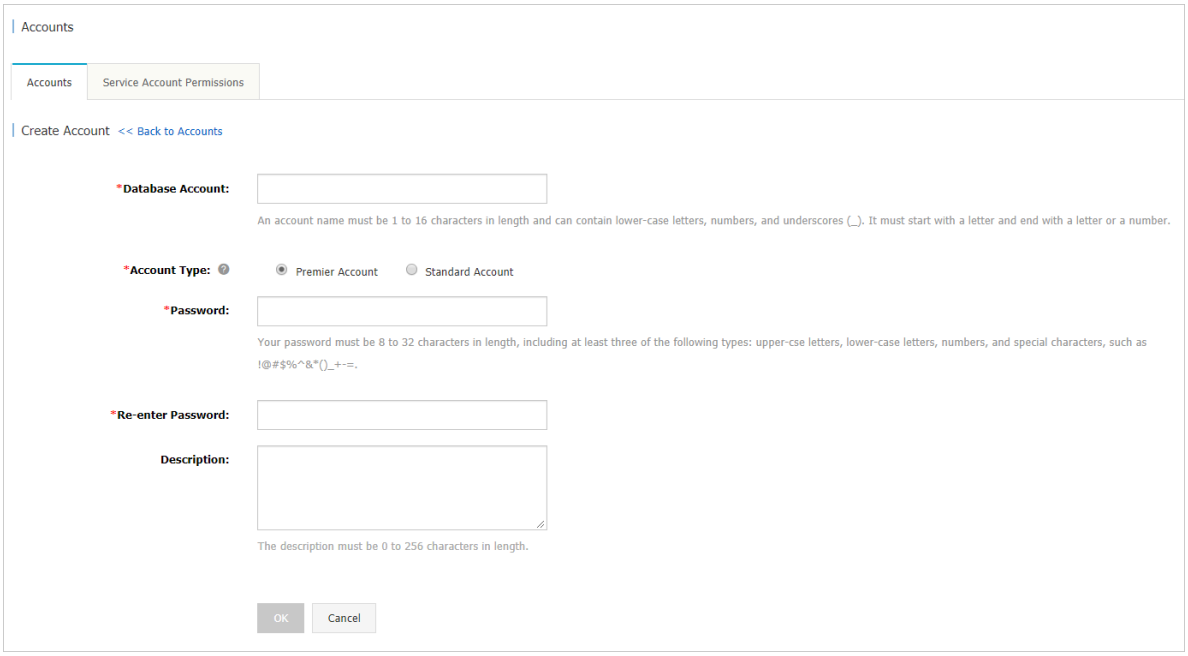
1. **Log on to the *RDS console*.**
2. **Select the target region.**




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

4. In the left-side navigation pane, click Accounts.
5. Click Create Account.
6. Set the following parameters.

| Parameter | Description |
| --- | --- |
| Database Account | The name of the account.<br>· The account name can contain 2 to 16 characters.<br>· The account name can contain lowercase letters, numbers, and underscores (_).<br>· The account name must start with a lowercase letter and end with a lowercase letter or number. |
| Password | The password of the account.<br>· The account password must contain 8 to 32 characters in length.<br>· The account password must contain at least three of the following types of characters: uppercase letters , lowercase letters, numbers, and special characters.<br>· The allowed special characters are as follows:<br>! @ # $ % ^ & * ( ) _ + - = |
| Re-enter Password | Enter the password again. |

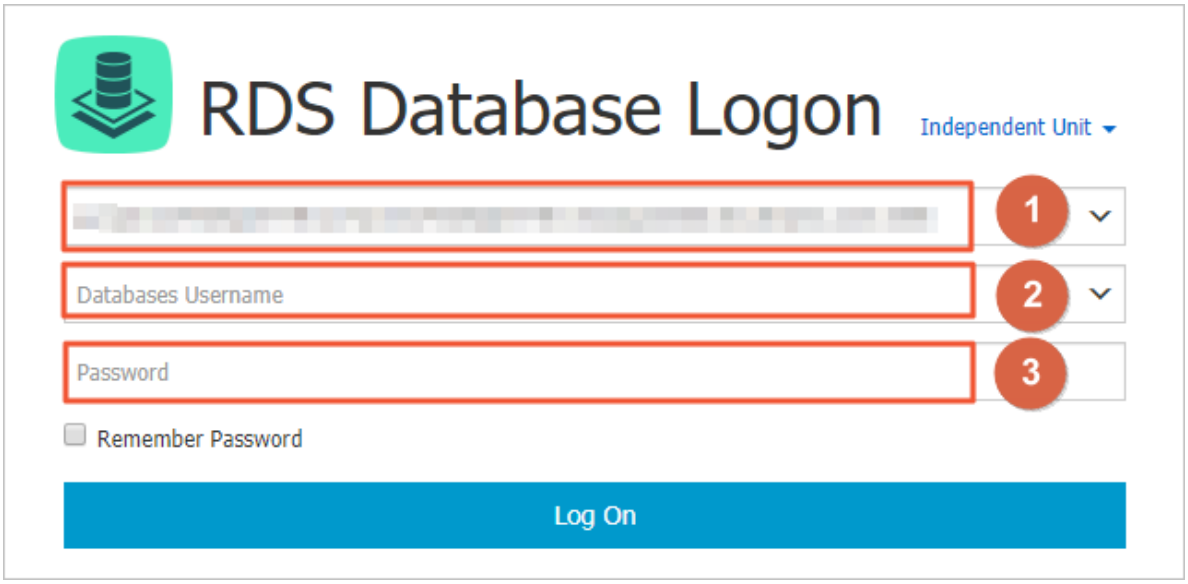



7. Click OK.

8. In the upper-right corner, click Log On to DB.

   You are directed to the RDS Database Logon page in the *Data Management Service console*.

9. Examine the endpoint and port information. If the information is correct, enter the username and password, as shown in the following figure.




| No. | Description |
| --- | --- |
| 1 | The endpoint and port information for the RDS instance. |
| 2 | The name of the account to access the database. |
| 3 | The password of the account to access the database |

10. Click Log On.

> **Note:**
> If you want the browser to remember the password for this account, you can select Remember Password before you click Log On.

11. Optional. If the system prompts you to add the CIDR block where the DMS server is located to the whitelist of the RDS instance, see *#unique_27*.
12. Optional. After the whitelist is properly configured, click Log On.
13. After you log on to the RDS instance, choose SQL Operations > SQL Window from the main menu.
14. In the SQL window, enter the following command to create a database:

```
CREATE DATABASE name
 [ [ WITH ] [ OWNER [=] user_name ]
        [ TEMPLATE [=] template ]
```

```
        [ ENCODING [=] encoding ]
        [ LC_COLLATE [=] lc_collate ]
        [ LC_CTYPE [=] lc_ctype ]
        [ TABLESPACE [=] tablespace_name ]
        [ CONNECTION LIMIT [=] connlimit ] ]
```

**For example, if you want to create a database named test, then run the following command:**

```
Create database test;
```

15. **Click execute to create the database.**
16. **In the SQL window, enter the following command to create a standard account:**

```
CREATE USER name [ [ WITH ] option [ ... ] ]
where option can be:
   SUPERUSER | NOSUPERUSER
 | CREATEDB | NOCREATEDB
 | CREATEROLE | NOCREATEROLE
 | CREATEUSER | NOCREATEUSER
 | INHERIT | NOINHERIT
 | LOGIN | NOLOGIN
 | REPLICATION | NOREPLICATION
 | CONNECTION LIMIT connlimit
 | [ ENCRYPTED | UNENCRYPTED ] PASSWORD 'password'
 | VALID UNTIL 'timestamp'
 | IN ROLE role_name [, ...]
 | IN GROUP role_name [, ...]
 | ROLE role_name [, ...]
 | ADMIN role_name [, ...]
 | USER role_name [, ...]
 | SYSID uid
```

**For example, if you want to create a standard account named test2 with a password of 123456, then run the following command:**

```
create user test2 password '123456';
```

17. **Click execute to create the standard account.**

FAQ

**Can I use the accounts created in a master RDS instance to access the read-only instances attached with this master RDS instance?**

**Yes, the accounts created in a master RDS instance are synchronized to the read-only instances attached with this master RDS instance. However, you cannot manage these accounts in the read-only instances. Additionally, these accounts only have the permissions to read data in the read-only instances.**

APIs

| API | Description |
| --- | --- |
| *#unique_28* | Used to create an account for an RDS instance. |

## 4.5 Connect to an RDS for PostgreSQL instance

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

**You can connect to an RDS for PostgreSQL instance through DMS or a database client such as pgAdmin 4.**

> **Note:**
> **Only the RDS for PostgreSQL instances in PostgreSQL 10 High-availability Edition (with local SSDs), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4 can be connected through DMS.**

Background information

**You can log on to DMS through the RDS console and then access the target RDS instance.**

*DMS* **allows you to manage Linux servers, NoSQL databases, and relational databases such as MySQL, SQL Server, PostgreSQL, MongoDB, and Redis. It is an all-in-one data management service that supports data management, structure management, access security, BI charts, data trends, data trace, performance trends and optimization, and server management.**

**RDS for PostgreSQL is fully compatible with PostgreSQL, so you can connect to RDS in the way you connect to an on-premises PostgreSQL database. This topic takes the pgAdmin 4 client as an example to introduce how to connect to an RDS instance. You can also adopt this method when using other clients. When you connect to an RDS instance through a client, choose to use an** *internal or public endpoint* **as follows:**

- **Use the internal endpoint when your client is installed on an ECS instance that is located in the same region and the same network type as the RDS instance to be connected.**

- **Use the public endpoint for the other situations.**

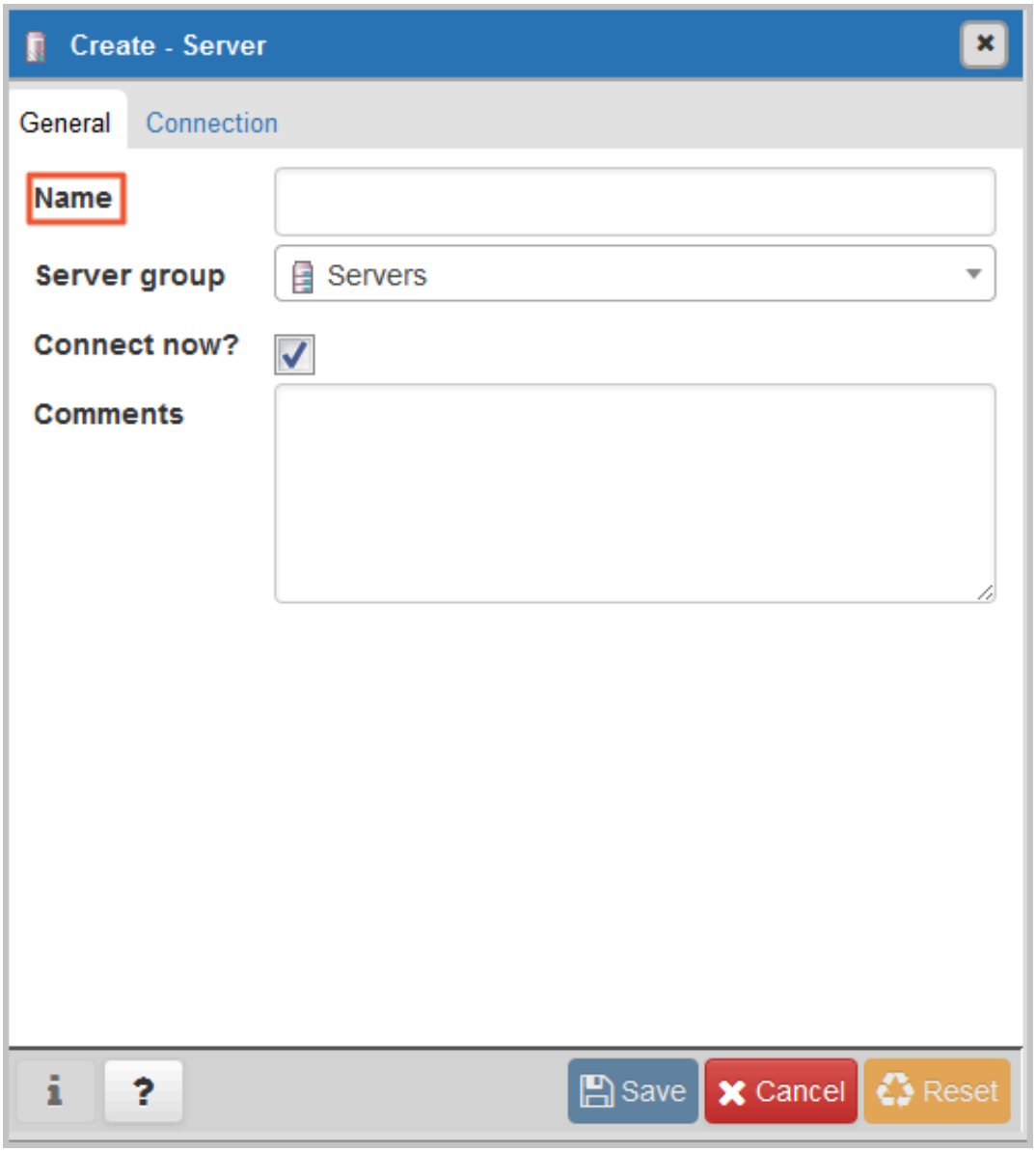
Connect to an RDS instance through DMS

**For more information, see** *#unique_30*.

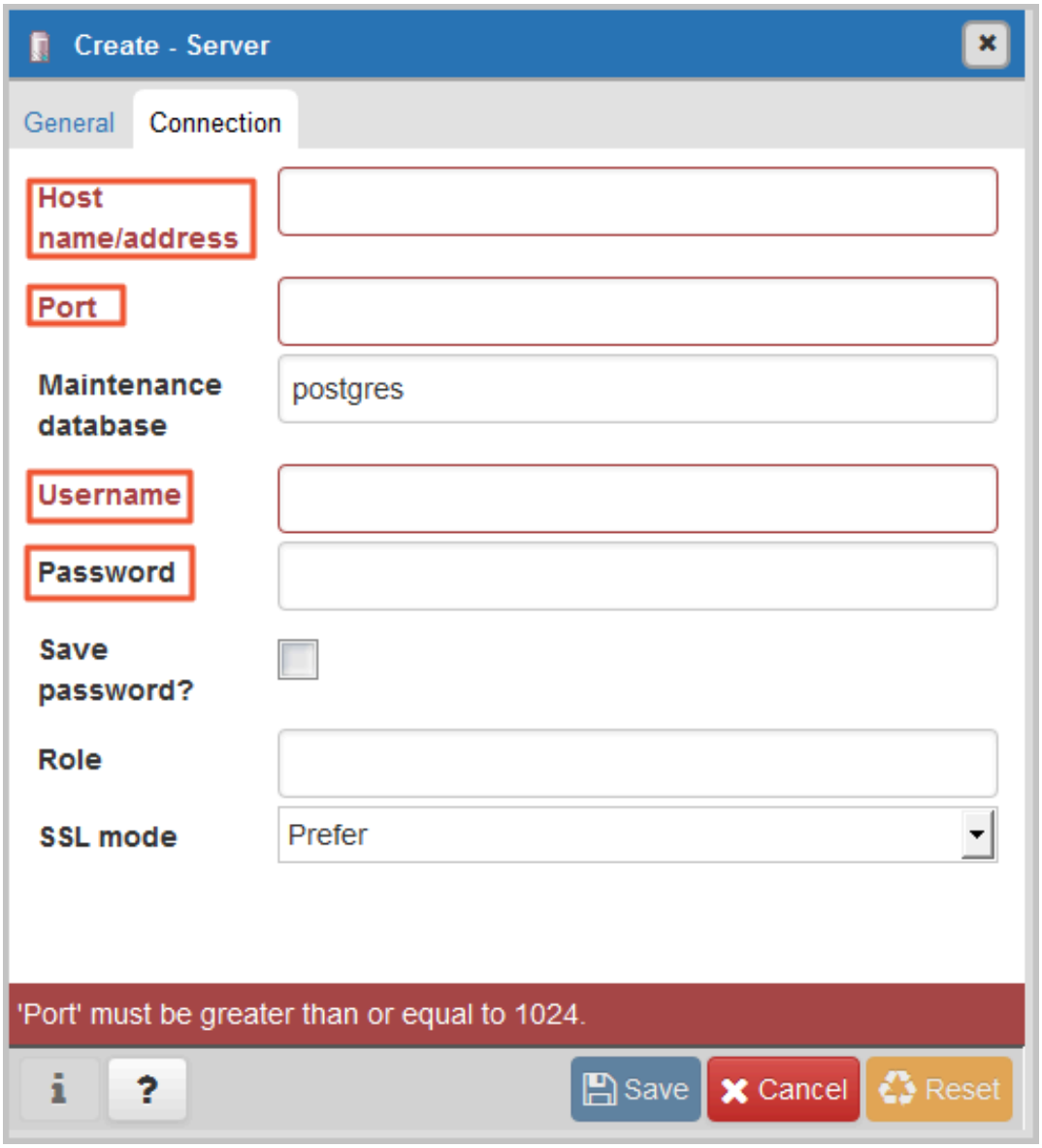
Connect to an RDS instance through a database client

1. **Add the IP address of the device to access the RDS instance to a whitelist of the RDS instance. For more information, see** *#unique_27*.
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 server name.



5. **Click the Connection tab and enter the information of the RDS instance to be connected.**




**Parameter description:**

- `Host name/address`: **to the endpoint of the RDS instance. If your application accesses the RDS instance through a private network, enter the internal endpoint of the RDS instance. If your application accesses the RDS instance**

through the Internet, enter the public endpoint of the RDS instance. To find the endpoints and ports of the RDS instance, follow these steps:

a. Log on to the *RDS console*.
b. Select the region where the target RDS instance is located.
c. Find the target RDS instance and click the instance ID.
d. In the Basic Information section of the Basic Information page, find the endpoints and ports of the RDS instance.

- `Port`: the port number of the RDS instance. If your application accesses the RDS instance through a private network, enter the internal port number of the RDS instance. If your application accesses the RDS instance through the Internet, enter the public port number of the RDS instance.
- `Username`: the name of the premier account you use to connect to the RDS instance.
- `Password`: the password of the premier account you use to connect to the RDS instance.

6. Click Save.
7. If the connection information is correct, choose Servers > server name > Databases > postgres. The following interface is displayed, which indicates that the connection to RDS instance is successful.

**Note:**

**Postgres is the default system database of the RDS instance. Do not perform any operation in this database.**


# 4.6 RDS for PostgreSQL read-only instances

## 4.6.1 Introduction to RDS for PostgreSQL read-only instances

**This topic introduces RDS for PostgreSQL read-only instances. For services that involve a small number of write requests but a large number of read requests, a single RDS instance may not be able to resist the read pressure. As a result, services may be affected. To scale the read ability elastically and share data pressure, you can create one or more read-only instances for your RDS instance. The read-only instances can handle massive read requests and increase the application throughput.**

### Overview

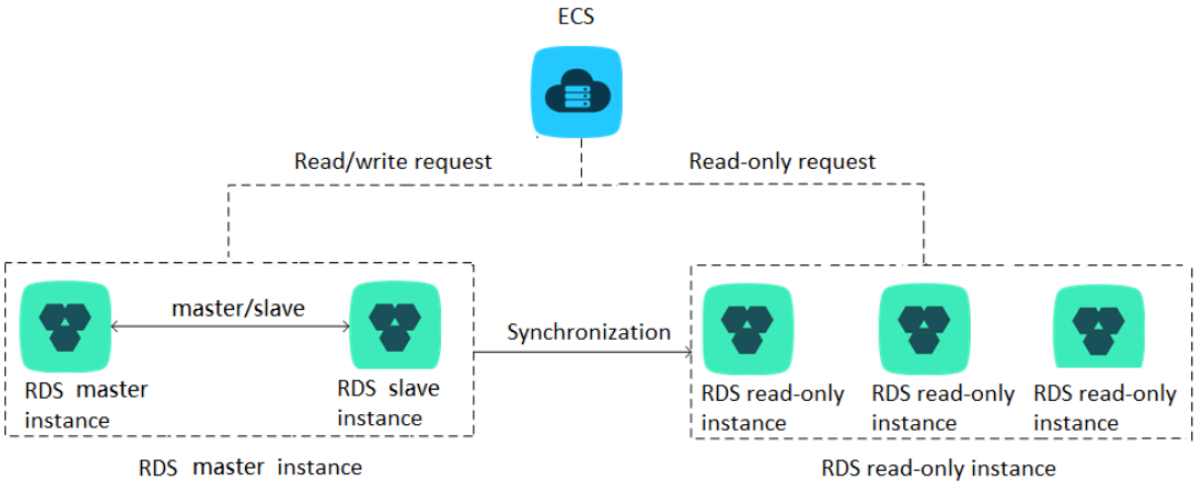
**A read-only instance is a read-only copy of the master instance. Changes to the master instance are automatically synchronized to all relevant read-only instances.**

**Note:**

- **Read-only instances must be PostgreSQL 10.0 High-Availability instances (with local SSDs).**

- The configuration of the master instance must be at least 8-core 32 GB ( dedicated or dedicated-host instance).
- Each read-only instance adopts a single-node architecture (without slave instances).

The following figure shows the topology of read-only instances.




Pricing

Read-only instances use the Pay-As-You-Go billing method. They are charged once every hour.

Features

Read-only instances offer the following features:

- Billing method: Pay-As-You-Go. This method is more flexible and cost-effective.
- Region and zone: A read-only instance must be in the same region as the master instance, but can be in a different zone from the master instance.
- Specifications and storage capacity: The specifications and storage capacity of a read-only instance cannot be lower than those of the master instance.
- *Network type*: The network type of a read-only instance can be different from that of the master instance.
- Account and database management: Users manage accounts and databases through the master instance rather than read-only instances.
- Whitelist: When a read-only instance is created, it automatically copies the whitelists of the master instance, but the whitelists of the read-only instance are independent of those of the master instance. You can modify the whitelists of a read-only instance according to *Configure a whitelist for an RDS for PostgreSQL instance*.

- **Monitoring and alarming: You can monitor system performance metrics, including the disk capacity, IOPS, number of connections, and CPU usage.**

Limits

- **Each master instance can have up to five read-only instances.**
- **Read-only instances do not support backup settings or manual backups.**
- **You cannot migrate data to read-only instances.**
- **You cannot create or delete databases for read-only instances.**
- **You cannot create or delete accounts for read-only instances. Additionally, you cannot authorize accounts or change account passwords for read-only instances.**

FAQ

**Does an account created in the master instance have permissions on read-only instances?**

**The accounts created in the master instance are automatically synchronized to read-only instances. However, you cannot manage the accounts in the read-only instances. The accounts only have the read permissions for the read-only instances.**

## 4.6.2 Create an RDS for PostgreSQL read-only instance

**This topic describes how to create an RDS for PostgreSQL read-only instance. You can create read-only instances to handle a large number of read requests and increase the application throughput. A read-only instance is a read-only copy of the master instance. Changes to the master instance are also automatically synchronized to all relevant read-only instances.**

**For more information, see** *Introduction to RDS for PostgreSQL read-only instances*.

Prerequisites

- **The master instance is an RDS for PostgreSQL 10.0 High-Availability Edition instance.**
- **The configuration of the master instance must be at least 8-core 32 GB (dedicated or dedicated-host instance).**

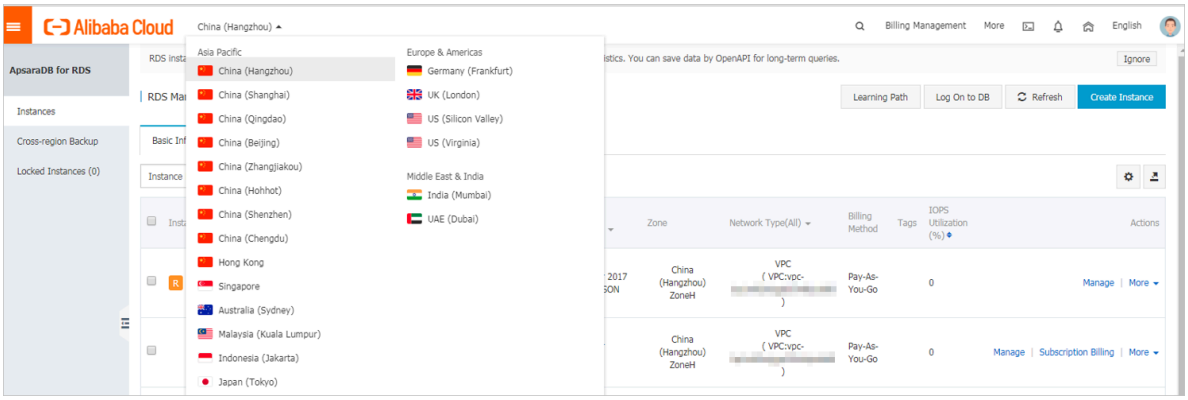
Precautions

- **You can create read-only instances only from a master instance and cannot switch an existing instance to a read-only instance.**

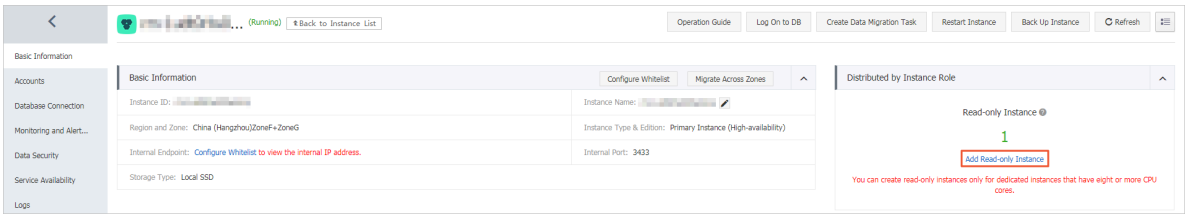
- **Creating a read-only instance does not affect the master instance because the read-only instance copies data from the corresponding slave instance.**
- **Read-only instances do not inherit the parameter settings of the master instance , but use the default parameter settings. You can modify the parameter settings in the console.**
- **The specifications and storage capacity of a read-only instance cannot be lower than those of the master instance.**
- **Each master instance can have up to five read-only instances.**
- **Read-only instances use the Pay-As-You-Go billing method. They are charged once every hour.**

Create a read-only instance

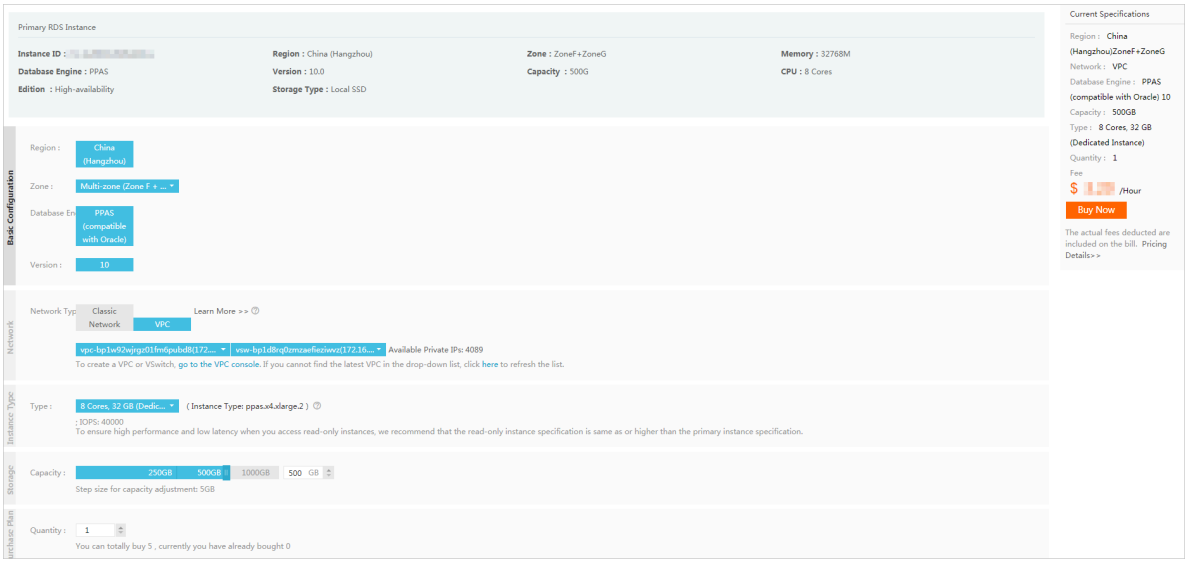
1. **Log on to the *RDS console*.**
2. **Select the target region.**




3. **Find the target RDS instance and click the instance ID.**
4. **Click Add Read-only instance.**



5. On the purchase page, select instance configurations and click Buy Now.




**Note:**

- We recommend that you deploy read-only instances in the same VPC as the master instance .
- The configuration (specifications and storage capacity) of each read-only instance must be greater than or equal to those of the master instance.
- You can deploy up to five read-only instances to improve availability.

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

The instance creation takes a few minutes.

View a read-only instance

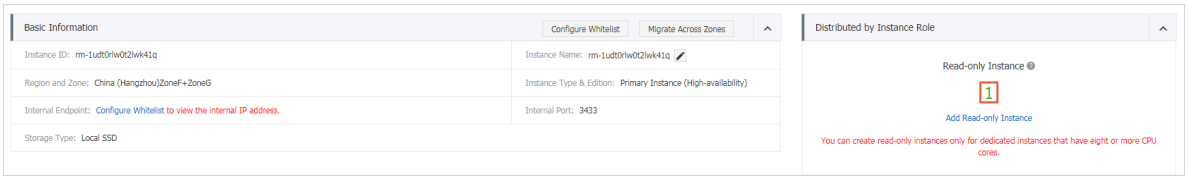
To view a read-only instance in the instance list, follow these steps:

1. Log on to the *RDS console*.
2. Select the region where the read-only instance is located.
3. Find the read-only instance and click the instance ID.

To view a read-only instance on the Basic Information page for the corresponding master instance, follow these steps:

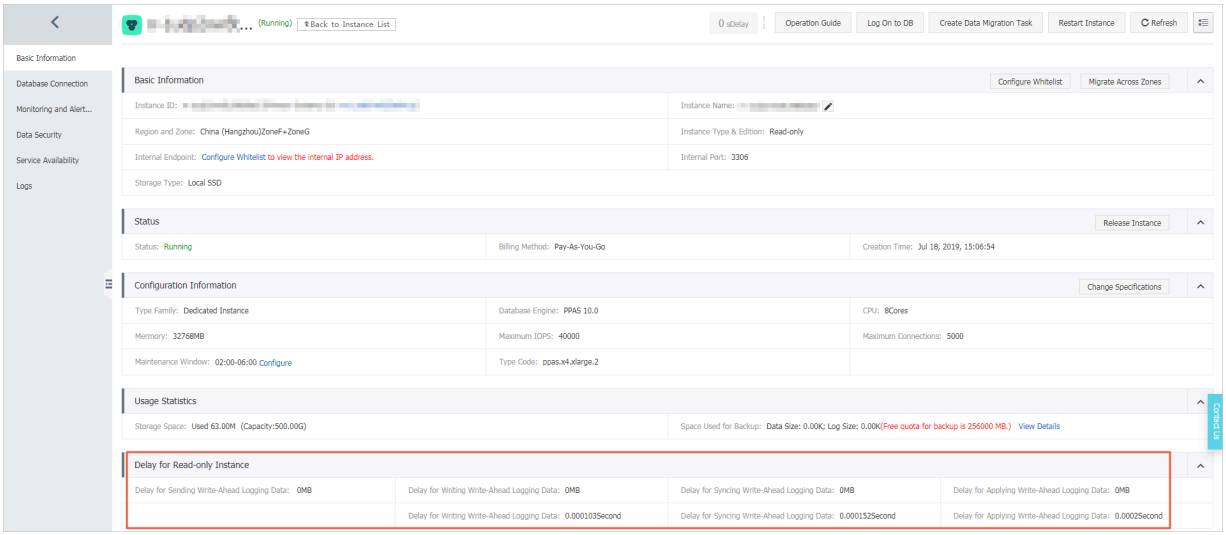
1. Log on to the *RDS console*.
2. Select the target region.
3. Find the master instance and click the instance ID.

4. **On the Basic Information page, move the pointer over the number of read-only instances and click the ID of the read-only instance.**




View the delay of a read-only instance

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




APIs

| API | Description |
| --- | --- |
| *#unique_34* | **Used to create an RDS read-only instance.** |

# 4.7 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.**

# 5 Data Migration

## 5.1 Migrate data between ApsaraDB for RDS instances

**This topic describes how to migrate data between ApsaraDB for RDS instances.**

**You can migrate data from an ApsaraDB for RDS instance to another ApsaraDB for RDS instance to achieve smooth business migration.**

**For more information, see** *Data Migration between ApsaraDB for RDS instances*.

## 5.2 Migrate data from an RDS for PostgreSQL database to an on-premises PostgreSQL database

**Migrating data from ApsaraDB RDS for PostgreSQL to an on-premises database by using logical backup files is supported.**

Procedure

1. **Connect the PostgreSQL client to ApsaraDB RDS for PostgreSQL.**
2. **Run the following command to back up the data.**

   ```
   pg_dump -U username -h hostname -p port databasename -f filename
   ```

   **The following list describes the parameters:**

   - **username: The username to log on to the ApsaraDB RDS for PostgreSQL database.**
   - **hostname: The hostname of the ApsaraDB RDS for PostgreSQL database.**
   - **port: The port number of the ApsaraDB RDS for PostgreSQL database.**
   - **databasename: The ApsaraDB RDS for PostgreSQL database name that you want to back up.**
   - **filename: The name of the backup file to be generated.**

   **For example,**

   ```
   pg_dump -U myuser -h rds2z2tp80v3752wb455.pg.rds.aliyuncs.com -p
   3433 pg001 -f pg001.sql
   ```

3. **Save the** *pg001.sql* **backup file to the target server.**

4. Run the following command to restore data to the on-premises database:

```
psql -U username -h hostname -d desintationdb -p port -f dumpfilena
me.sql
```

The following list describes the parameters:

- username: The username to log on to the on-premises PostgreSQL database.
- hostname: The hostname of the on-premises PostgreSQL database.
- port: The port number of the on-premises PostgreSQL database.
- desintationdb: The database name of the on-premises PostgreSQL database.
- dumpfilename: The name of the backup file to be restored.

For example,

```
psql -U myuser -h localhost -d pg001 -p 5432 -f pg001.sql
```

Due to the permission settings of the ApsaraDB RDS for PostgreSQL database are different from those of the on-premises database, some permission-related warnings or errors may occur during the data import. These warnings and errors can be ignored, for example,

```
WARNING: No privileges could be revoked for "xxxxx".
ERROR: Role "xxxxx" does not exist.
```

## 5.3 Migrate an on-premises PostgreSQL database to ApsaraDB RDS for PostgreSQL by using the psql command tool

This topic describes how to use the psql command to restore the PostgreSQL data backup files to an ApsaraDB for RDS instance.

### Background information

PostgreSQL supports logical backups. To import PostgreSQL data, you can export the logical backup files by using the pg_dump tool and then import the backup files into the ApsaraDB for RDS instance .

### Prerequisites

The database backup of the ApsaraDB for RDS instance has been completed, see *Apply for a public endpoint for an RDS for PostgreSQL instance* and *Create databases and accounts for an PostgreSQL instance*.

Backup data for the on-premises PostgreSQL database

1. **Connect to the on-premises PostgreSQL database through the PostgreSQL client.**
2. **Run the following command to back up the data:**

   ```
   pg_dump -U username -h hostname -p port databasename -f filename
   ```

   **The following list describes the parameters:**

   - **username: The username to log on to the on-premises PostgreSQL database.**
   - **hostname: The hostname of the on-premises database. You can use *localhost* as the hostname if you log on to the local database host.**
   - **port: The port number of the on-premises PostgreSQL database.**
   - **databasename: The name of the on-premises database to be backed up.**
   - **filename: The name of the backup file to be generated.**

   **For example, if you want to back up the on-premises PostgreSQL database using the account William, log on to the PostgreSQL database host and run the following command:**

   ```
   pg_dump -U William -h localhost -p 3433 pg001 -f pg001.sql
   ```

Perform the migration

**Note:**

**We recommend that you restore data to ApsaraDB for RDS through the internal network connection that is more stable and secure. You can upload the data to the ECS and then restore data to the target ApsaraDB for RDS through the internal network connection. If the data file is too large, you must compress the file before uploading. The following example describes how to restore data to ApsaraDB for RDS through the internal network connection.**

1. **Log on to ECS.**

2. **Run the following command through the PostgreSQL client to import the data .**

```
psql -U username -h hostname -d desintationdb -p port -f dumpfilena
me.sql
```

**The following list describes the parameters:**

- **username: The username to log on to the ApsaraDB RDS for PostgreSQL database.**
- **hostname: The hostname of the ApsaraDB RDS for PostgreSQL database.**
- **port: The port number of the ApsaraDB RDS for PostgreSQL database.**
- **desintationdb: The ApsaraDB RDS for PostgreSQL database name.**
- **dumpfilename: The name of the backup file to be restored.**

**For example,**

```
psql -U William -h postgresql.rds.aliyuncs.com -d pg001 -p 3433 -f
pg001.sql
```

**Due to the permission settings of the ApsaraDB RDS for PostgreSQL database are different from those of the on-premises database, some permission-related warnings or errors may occur during the data import. These warnings and errors can be ignored, for example,**

```
WARNING: No privileges could be revoked for "xxxxx".
ERROR: Role "xxxxx" does not exist.
```

# 6 Billing management

## 6.1 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.**

Impact

**Changing billing methods does not impact the performance of your ApsaraDB RDS for PostgreSQL instances.**

Notes

- **You cannot change the billing method from subscription to pay-as-you-go. To optimize your cost plan, evaluate your usage model carefully before you change your billing method.**
- **You cannot upgrade the specifications of a subscription-based instance if the purchase order of the instance has not been paid. Otherwise, the unpaid order will be invalid. You must cancel this order on the *Orders* page and change the billing method again.**

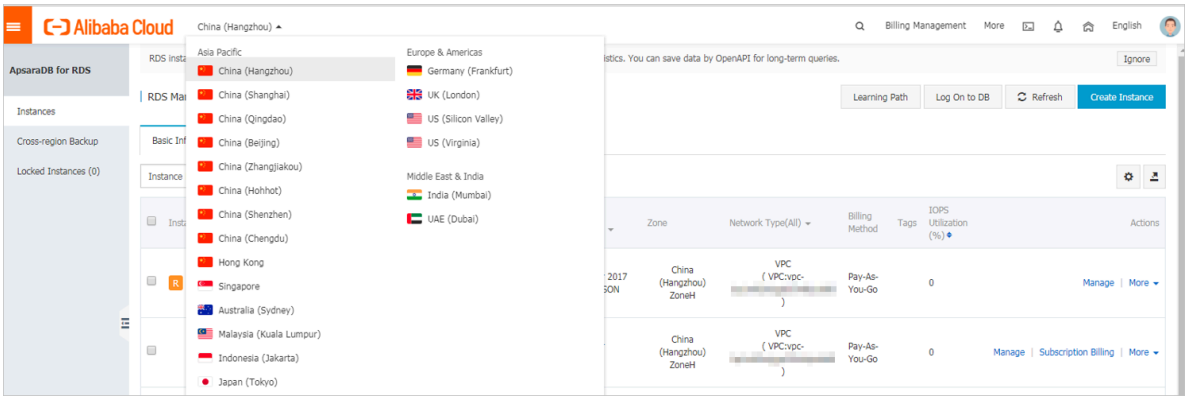
Prerequisites

- **The instance type cannot be an end-of-sales (EOS) instance types that are no longer available for sale. For more information about the EOS instance types, see *End-of-sales instance types*. You must change the instance type from EOS instance type to an available instance type before you change the billing method for the instance to subscription. For more information, see *Change the configuration of an RDS for PostgreSQL instance*.**
- **The billing method of the instance is pay-as-you-go.**
- **The instance is in the Running state.**
- **You do not have an unpaid order of subscription-based instance.**

Procedure

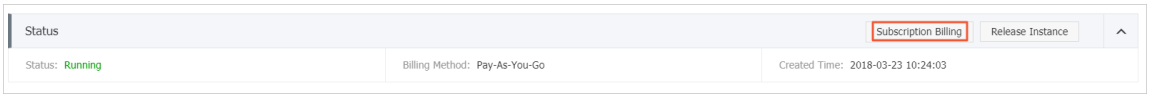
1. **Log on to the *RDS console*.**

2. Select the target region.




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

   - Click Subscription Billing in the Actions column.
   - Click the instance ID to open the Details page. In the Status section, click Subscription Billing, as shown in the following figure.




4. Select the duration of the subscription.
5. Click Pay Now.

> **Note:**
> The system will generate an order for you to switch to the subscription billing method. If this order is not paid or canceled, you cannot purchase new instances or switch the billing method of the instance to subscription. You can pay for or cancel this order on the *Orders* page.

6. Pay the order as prompted.

## 6.2 Manually renew an RDS for PostgreSQL instance

This topic describes how to manually renew an RDS for PostgreSQL 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*.

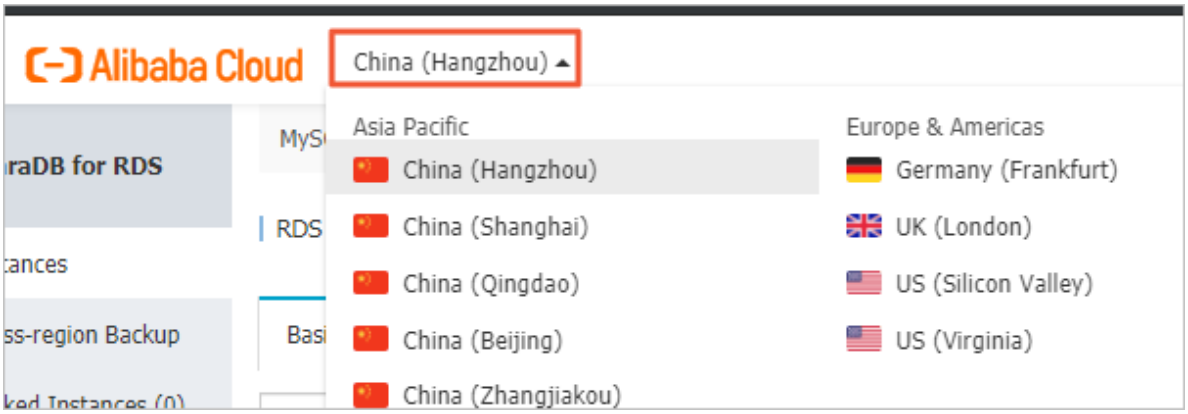
> **Note:**

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

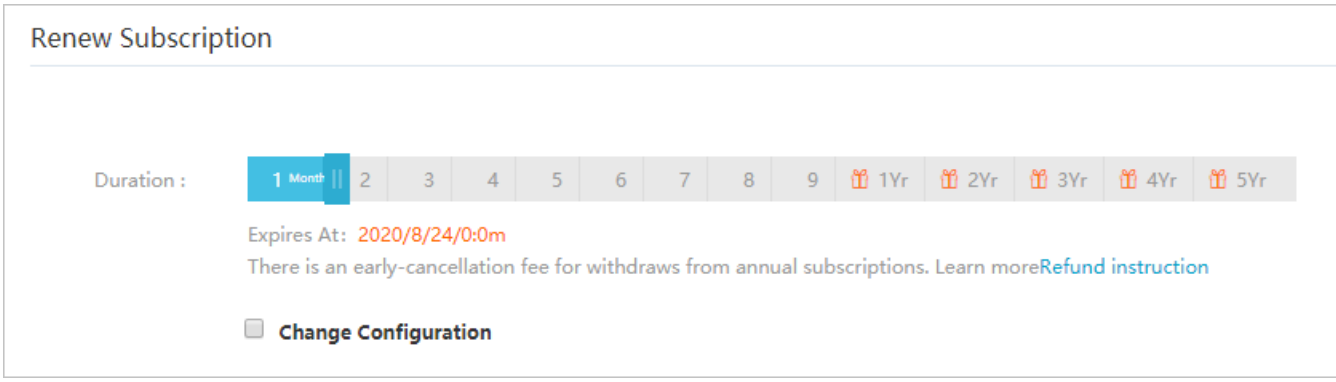
**You can manually renew a subscription-based instance before it expires or within 15 days after it expires.**

Method 1: Renew an RDS instance in the RDS console

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




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

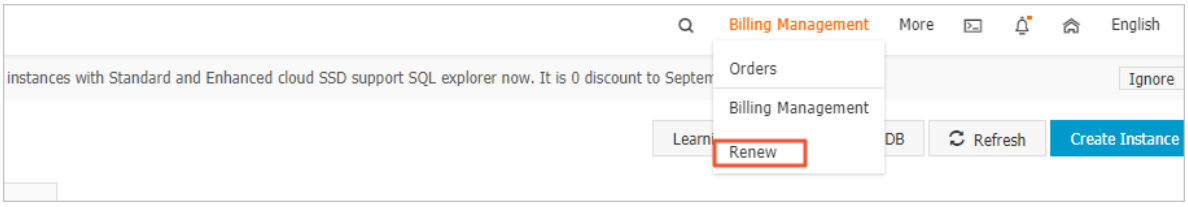



5. **Select Terms of Service, Service Level Agreement, and Terms of Use, and click Pay Now to complete the payment.**

Renew an RDS instance in the Renew console

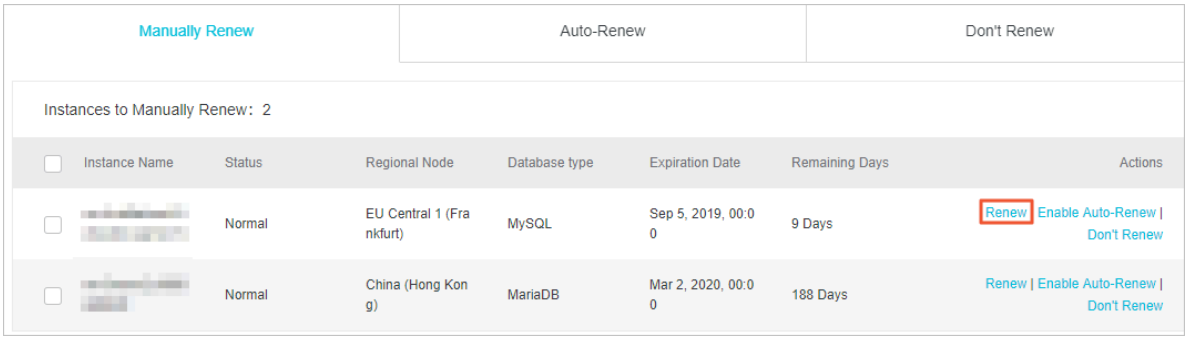
1. **Log on to the *ApsaraDB for RDS console*.**

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 PostgreSQL instance*.

# 6.3 Automatically renew an RDS for PostgreSQL instance

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

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

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

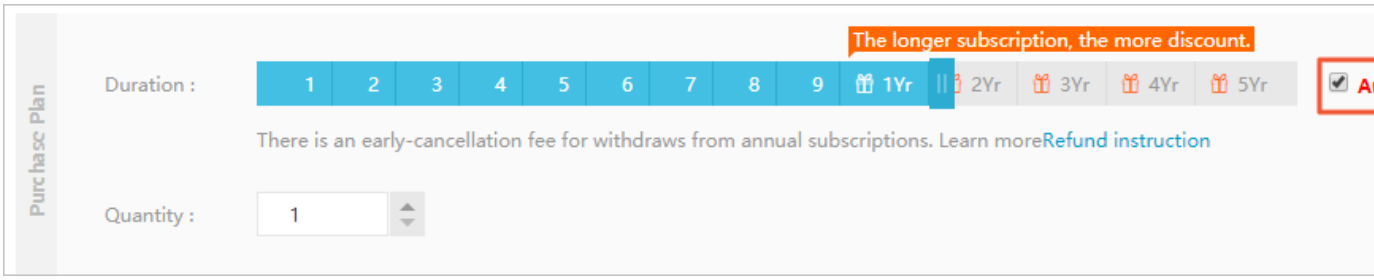
Precautions

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

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.**

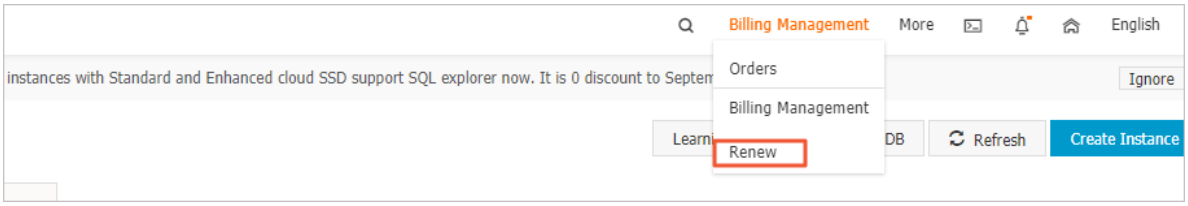



Enable automatic renewal after you purchase an RDS instance

**Note:**

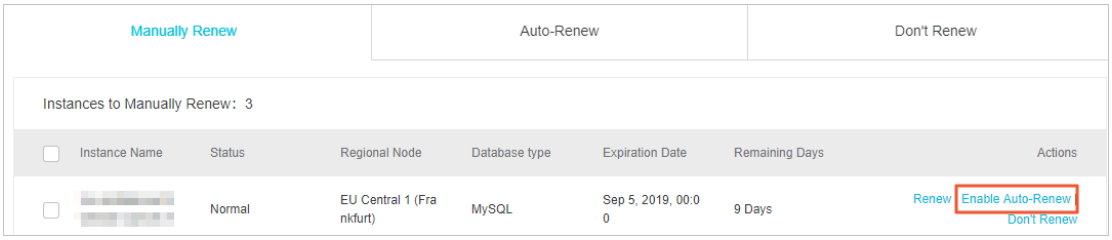
**After you enable automatic renewal, the system automatically renews your instance based on the selected renewal duration. For example, if you select a three-month renewal duration, the fees are automatically paid every three months for each renewal.**

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.

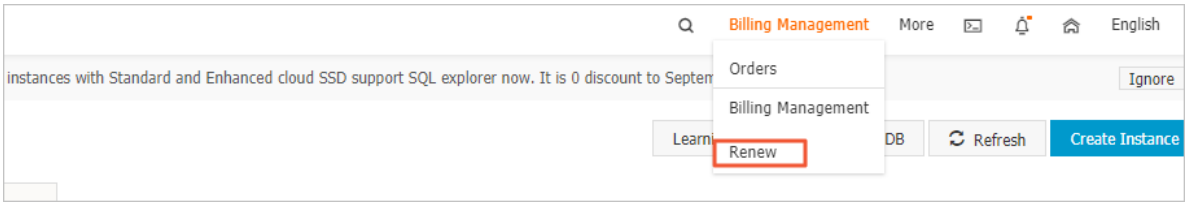



     b. In the displayed dialog box, set Auto-Renew Cycle and click Enable Auto-Renew.
   - Follow these steps to enable auto-renewal for more than one RDS instance:

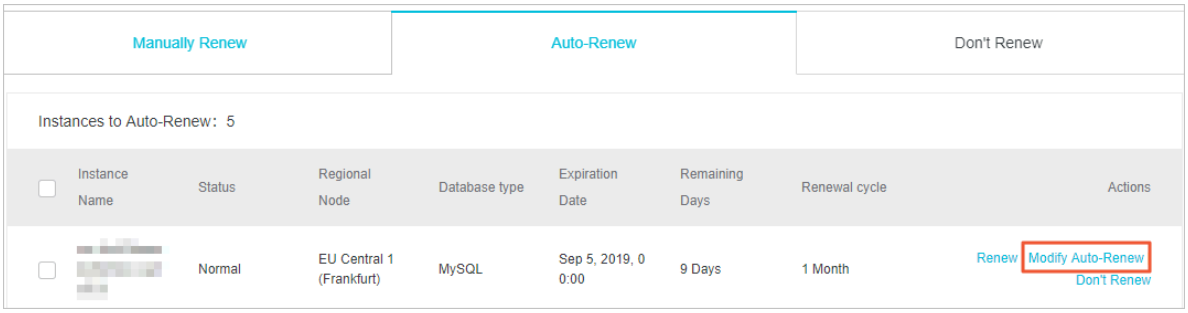
     Select the target RDS instances, and click Enable Auto-Renew below the instance list.
   - In the displayed dialog box, set Auto-Renew Cycle and click Enable Auto-Renew.

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.



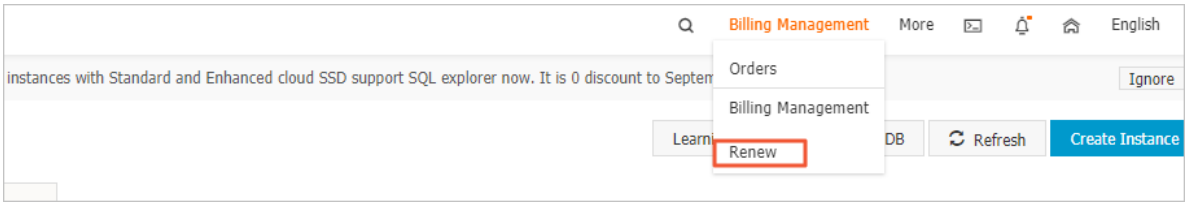

3. In the left-side navigation pane, click ApsaraDB for RDS.
4. On the Auto-Renew tab, find the target RDS instance and in the Actions column click Modify Auto-Renew.



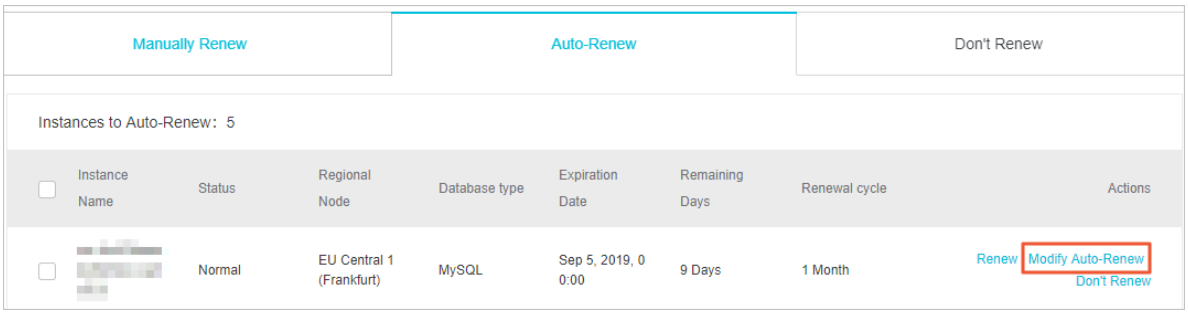
5. In the displayed dialog box, select Modify Auto-Renew Cycle, select an auto-renew cycle, and click OK.

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_21* | Used to create an RDS instance.<br>**Note:**<br>Automatic renewal is enabled when you create the instance. |
| *#unique_45* | Used to renew a subscription-based RDS instance.<br>**Note:**<br>Automatic renewal is enabled after you create the instance. |

# 7 Instance management

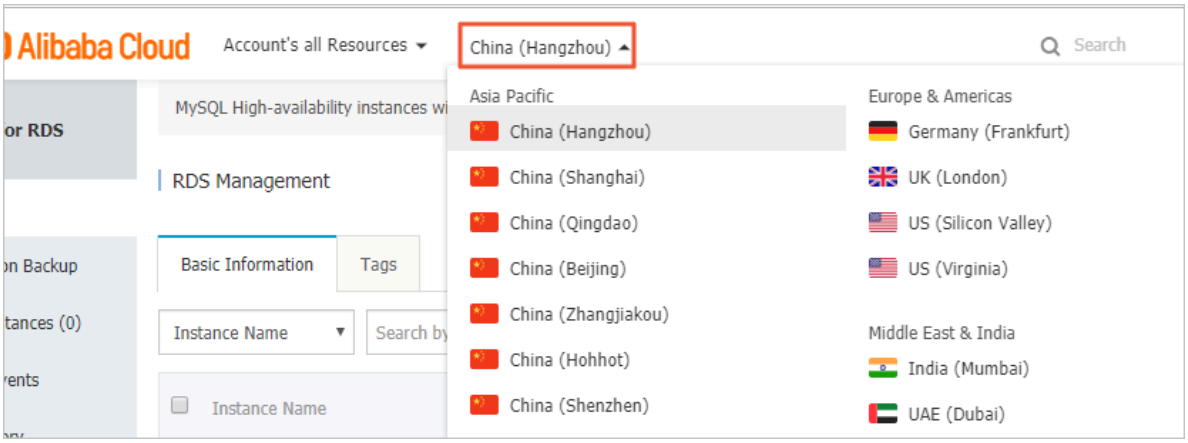
## 7.1 Restart an instance

**This topic describes how to manually restart an RDS instance when the number of connections reaches its upper limit or the instance encounters experience issues.**

> **Note:**
> **A restart incurs disconnections from the RDS instance . We recommend that you make appropriate service arrangements before you restart an instance. Proceed with caution.**

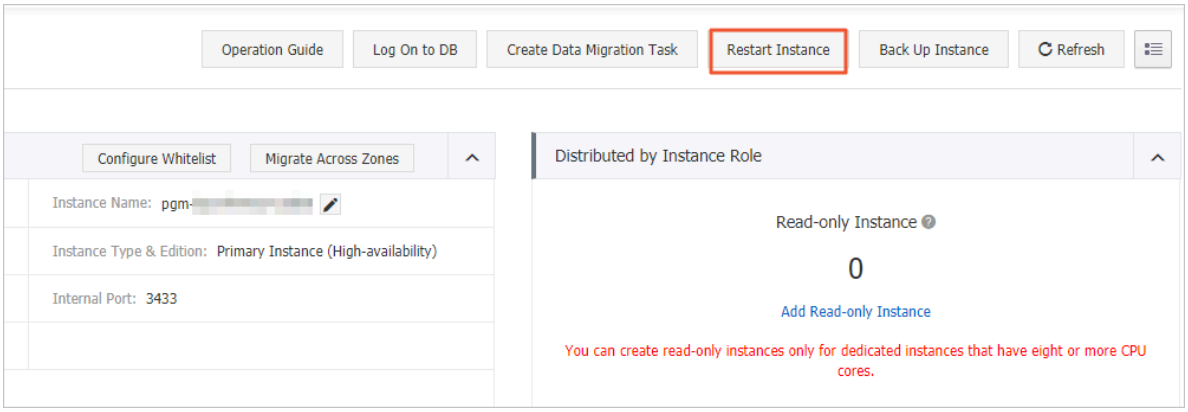
Procedure

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




3. **Find the target RDS instance. Then, click the instance ID or in the Actions column click Management.**

4. In the upper-right corner of the Basic Information page, click Restart Instance.




5. In the message that appears, click OK.

APIs

| API | Description |
| --- | --- |
| *#unique_48* | Used to restart an RDS instance. |

## 7.2 Change the maintenance window

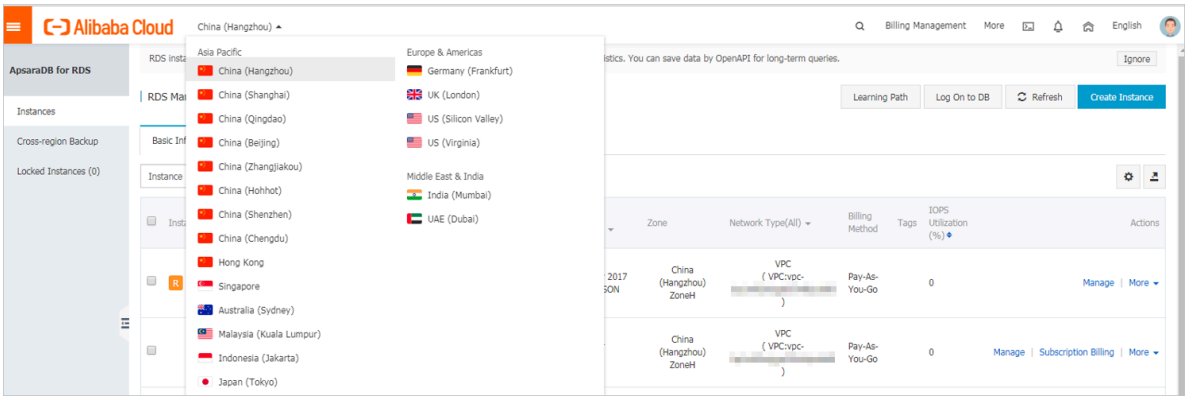
**This topic describes how to change the maintenance window of an RDS for PostgreSQL instance. To guarantee the stability of ApsaraDB for RDS instances, the back-end system performs maintenance of the instances at irregular intervals. The default maintenance window is from 02:00 to 06:00. You can set the maintenance window to the off-peak period of your business to avoid impacts on business.**

Precautions

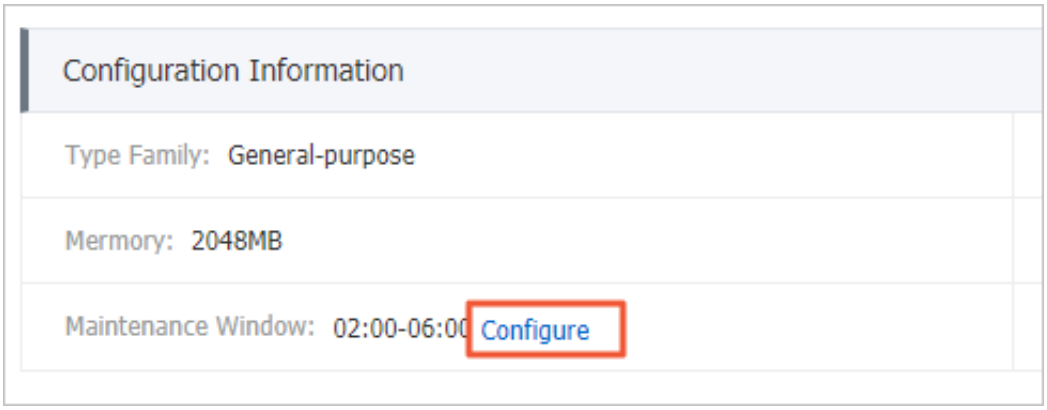
- **Before maintenance is performed, ApsaraDB for RDS sends SMS messages and emails to the contacts listed in your Alibaba Cloud accounts.**
- **To guarantee the stability of the maintenance process, the instance enters the Instance Maintaining state before the maintenance time on the day of maintenance. 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. **Select the target region.**




3. **Find the target RDS instance. Then, click the instance ID or in the Actions column click Management.**
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_50* | **Modifies the maintenance window of the instance.** |

# 7.3 Migrate an RDS for PostgreSQL instance across zones in the same region

**This topic describes how to migrate an RDS for PostgreSQL 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 type | Scenario |
| --- | --- |
| Migrate instances from one zone to another | The capacity of the zone where the instances are located is full, or the performance of the instances is affected due to other reasons. |
| Migrate instances from one zone to multiple zones | Disaster recovery across data centers is required to improve the disaster recovery capability of the instances. The primary and secondary instances are located in different zones.<br>Compared with single-zone instances, multi-zone instances can withstand disasters at higher levels. For example, single-zone instances can tolerate server and rack faults, whereas multi-zone instances can tolerate data center faults. |
| Migrate instances from multiple zones to one zone | Specific features are required. |

## Fees

**This feature is free of charge even if you migrate instances from one zone to multiple zones.**

## Prerequisites

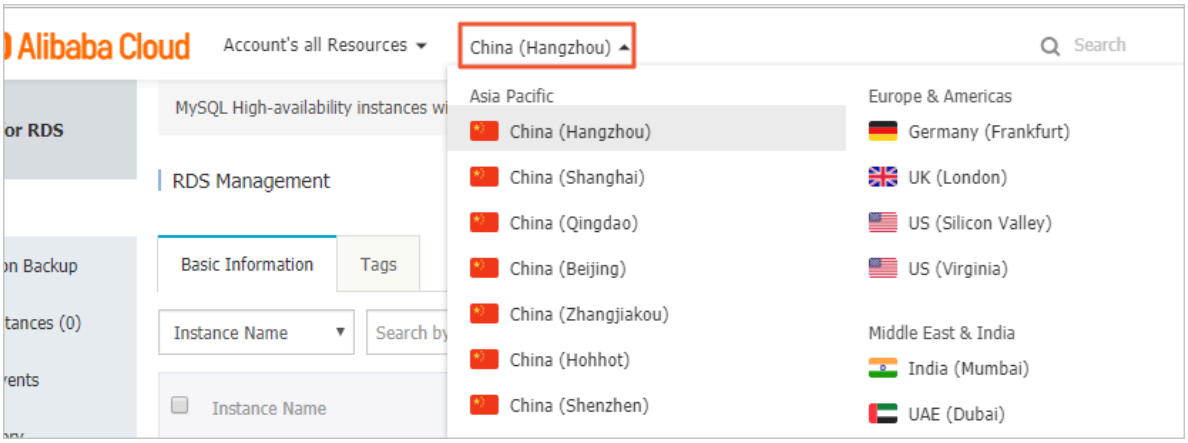
- **Cross-zone migration is available only when the region where the instances are located has multiple zones. For more information about regions and zones, see** *Regions and zones*.
- **The DB engine version and edition are as follows:**
  - **PostgreSQL 10 High-availability Edition (with standard SSDs)**
  - **PostgreSQL 9.4**

Precautions

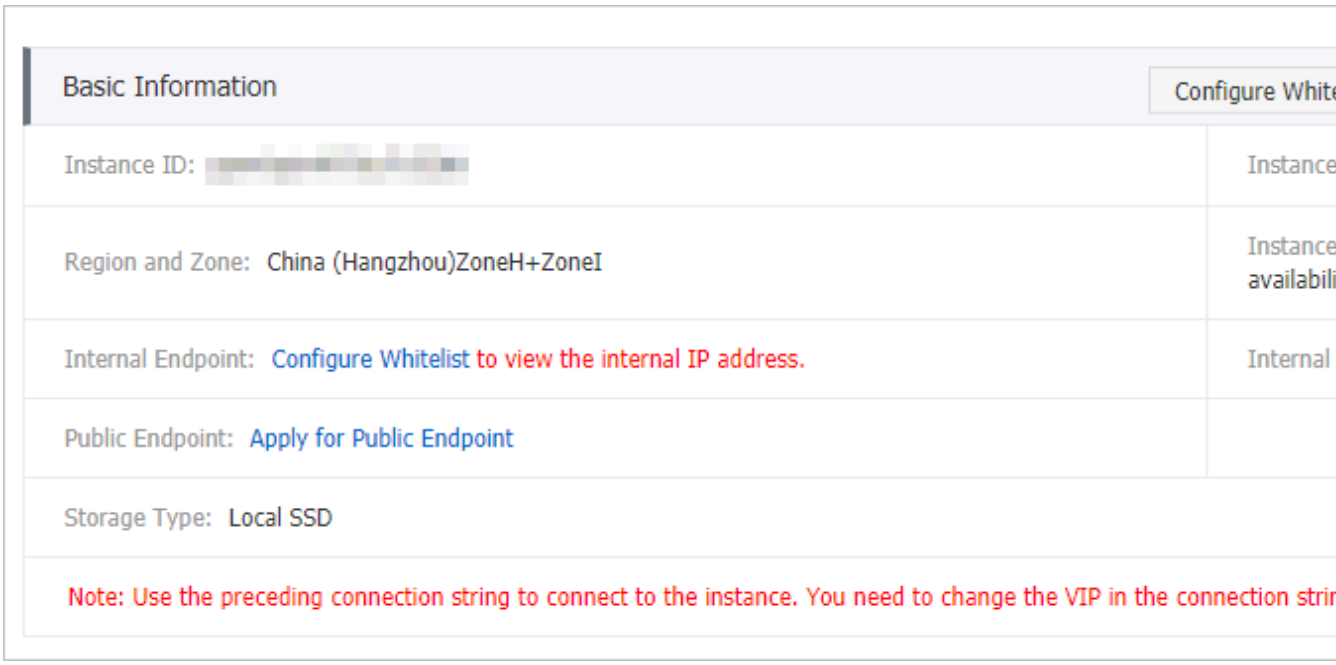
**Services may be disconnected for 30 seconds during cross-zone migration, and most operations related to databases, accounts, and networks cannot be performed. Therefore, make sure that your application is configured with automatic reconnection policies, and migrate instances during off-peak hours.**

Procedure

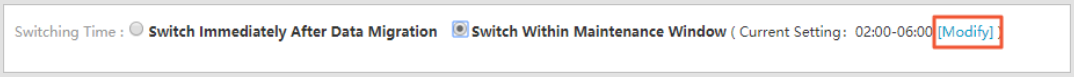
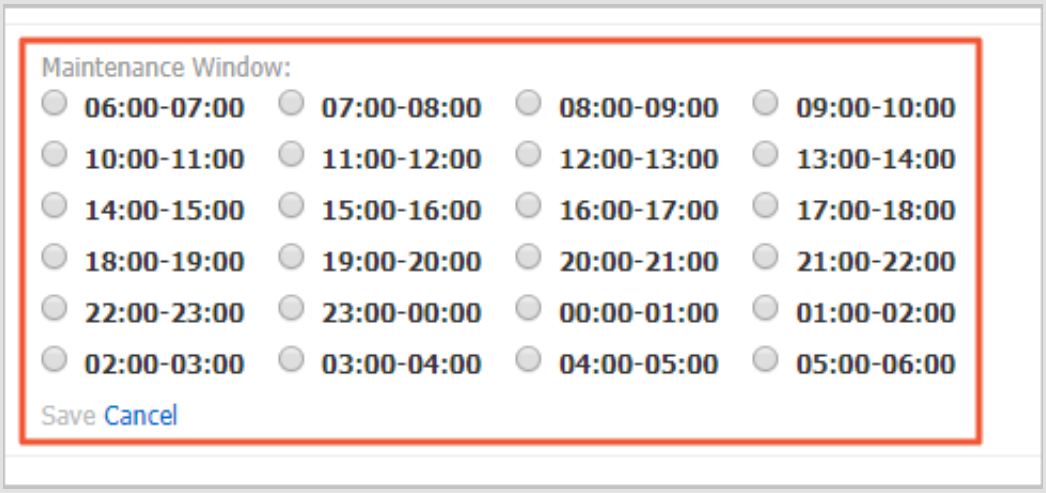
1. **Log on to the *RDS console*.**
2. **Select the target region.**




3. **Find the target instance and click the instance ID.**
4. **Click Migrate Across Zones.**



5. In the dialog box that appears, select the destination zone, VSwitch, and migration time, and then click OK.

> **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 Instance Information page, refresh it, and perform the steps to migrate.

APIs

| API | Description |
| --- | --- |
| *MigrateToOtherZone* | Migrates an RDS instance from one zone to another. |

## 7.4 Switch over services between the RDS for PostgreSQL master and slave instances

This topic describes how to switch over services between the RDS for PostgreSQL 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 over 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.**

Prerequisites

**The instance is a High-availability Edition instance.**

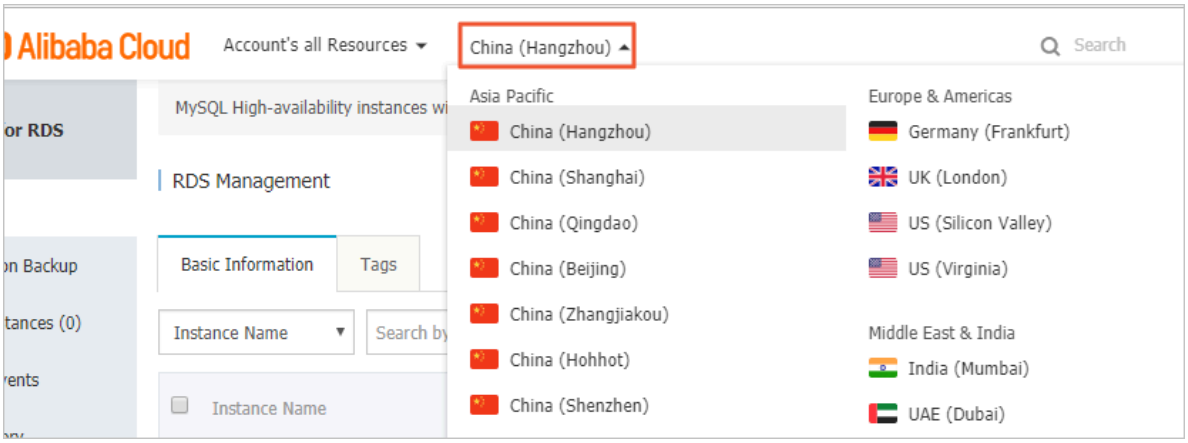
> **Note:**
>
> **Basic Edition instances do not support the switchover because they do not have slave instances.**

Precautions

**Services may be disconnected during the switchover. Make sure that you configure automatic reconnection policies for your applications to avoid loss of services.**

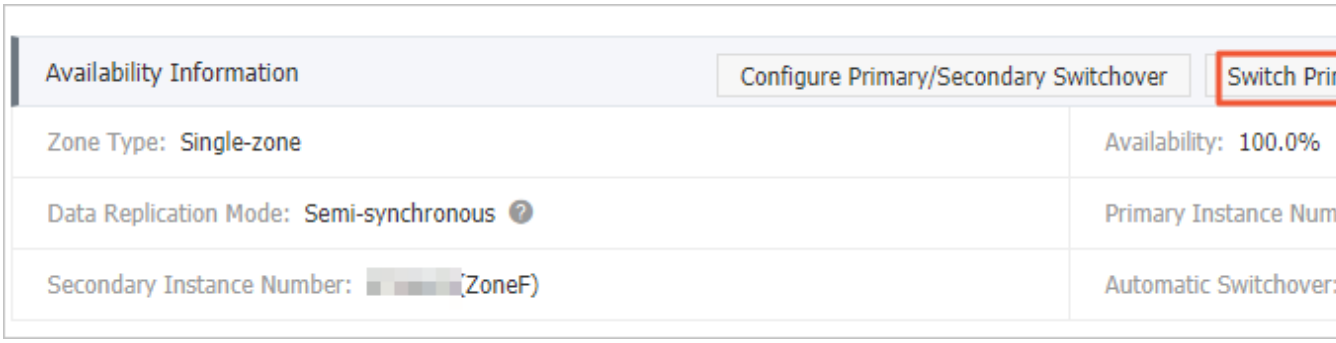
Procedure

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



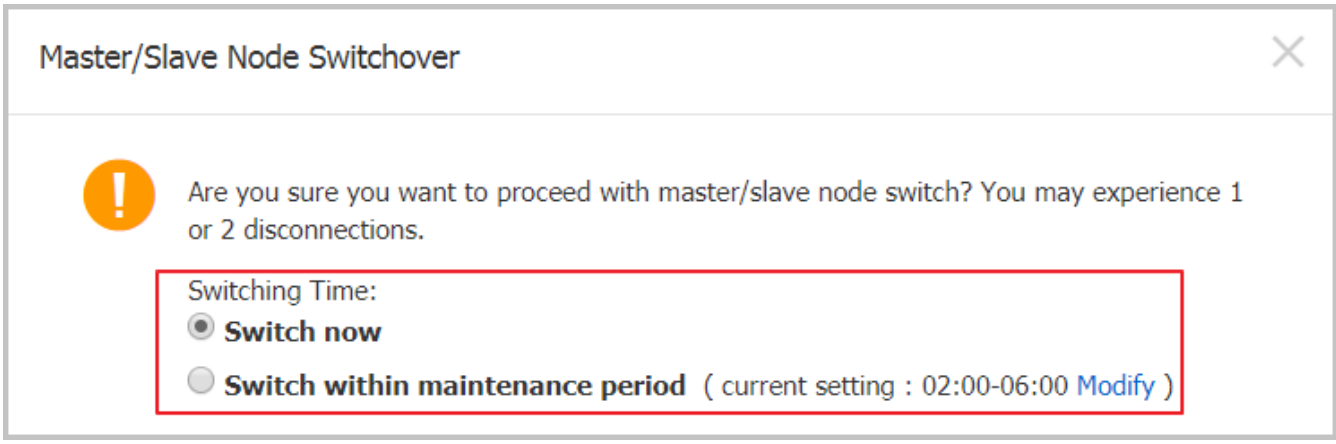

3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Service Availability.**

5. **On the Basic Information page, find the Availability Information section and click Switch Primary/Secondary Instance.**




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

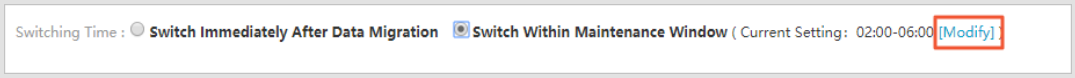
   **During the switch, operations such as managing the databases and accounts and switchover the network types cannot be performed. Therefore, we recommend that you select Switch Within Maintenance Window.**



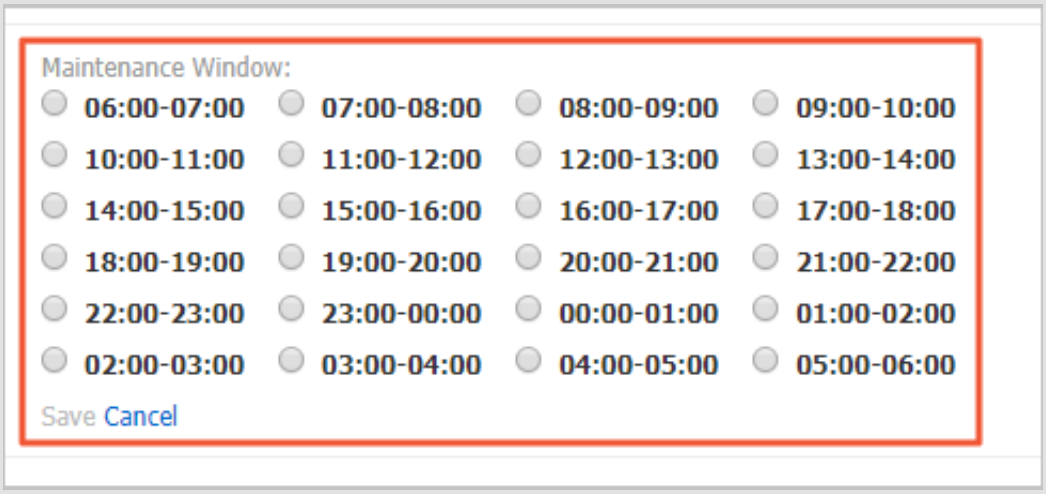

**Note:**

**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 over services between the master and slave instances. |

## 7.5 Change the network type of an RDS for PostgreSQL instance

This topic describes how to change the network type of an RDS for PostgreSQL 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** *Switch from standard IP whitelist to enhanced whitelist*.

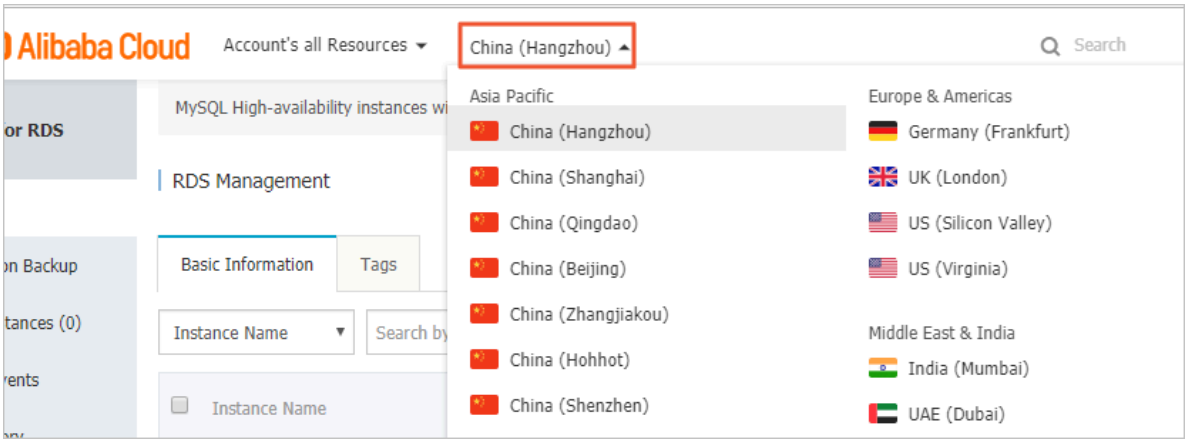
Switch from VPC to classic network

### 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.**

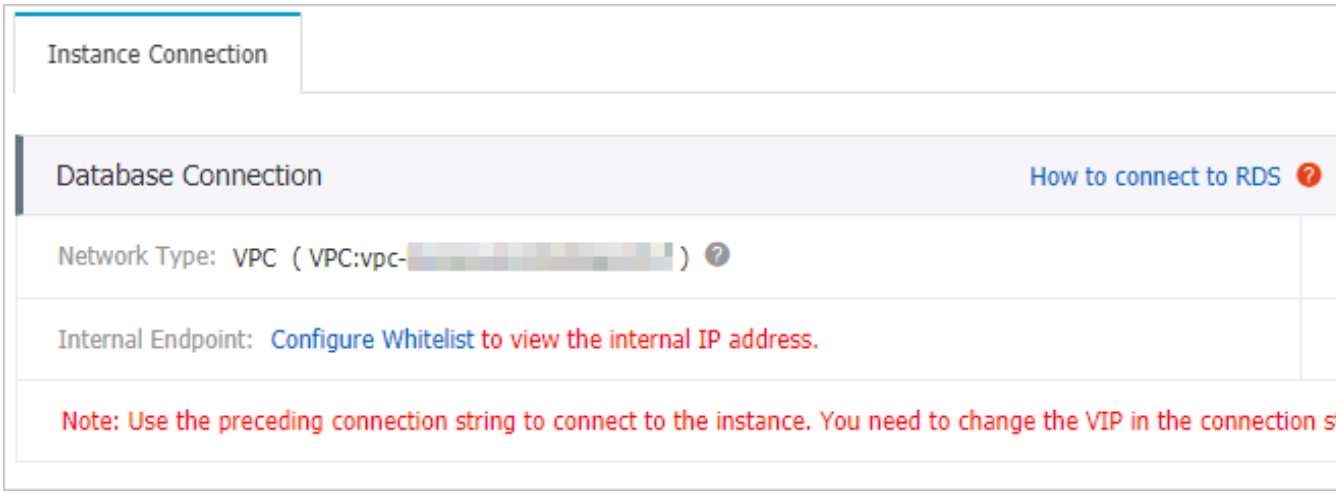
### Procedure

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




3. **Find the target 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.

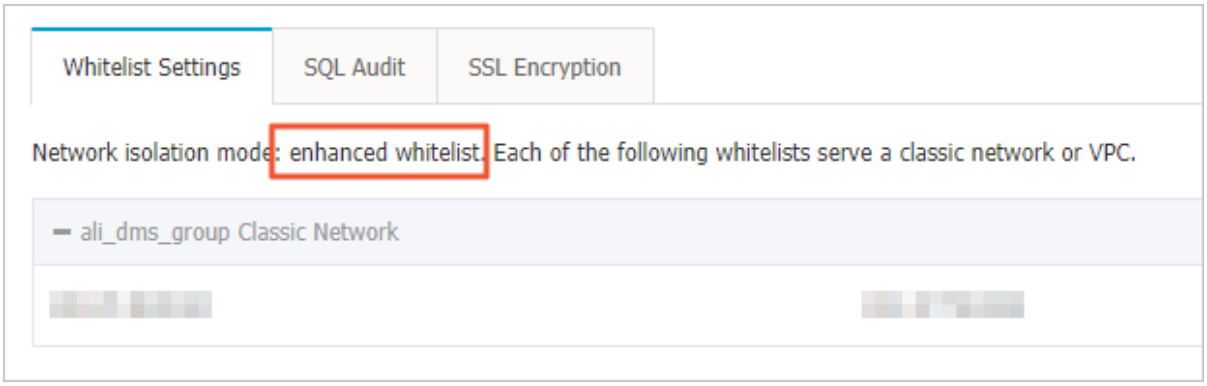



6. In the message that appears, click OK.

   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 IP address of the ECS instance in the classic network to any whitelist of the RDS instance.

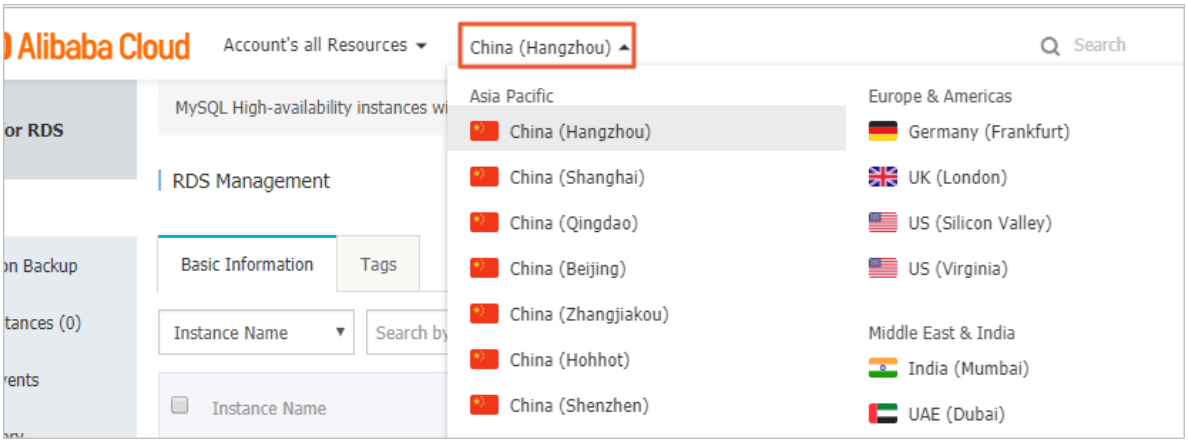

   - If the RDS instance applies the *enhanced whitelist mode*, as shown in the following figure, you must add the internal IP address of the ECS instance in the classic

**network to the default classic network whitelist of the RDS instance. If there is no classic network whitelist, you must create a whitelist.**




Switch from classic network to VPC

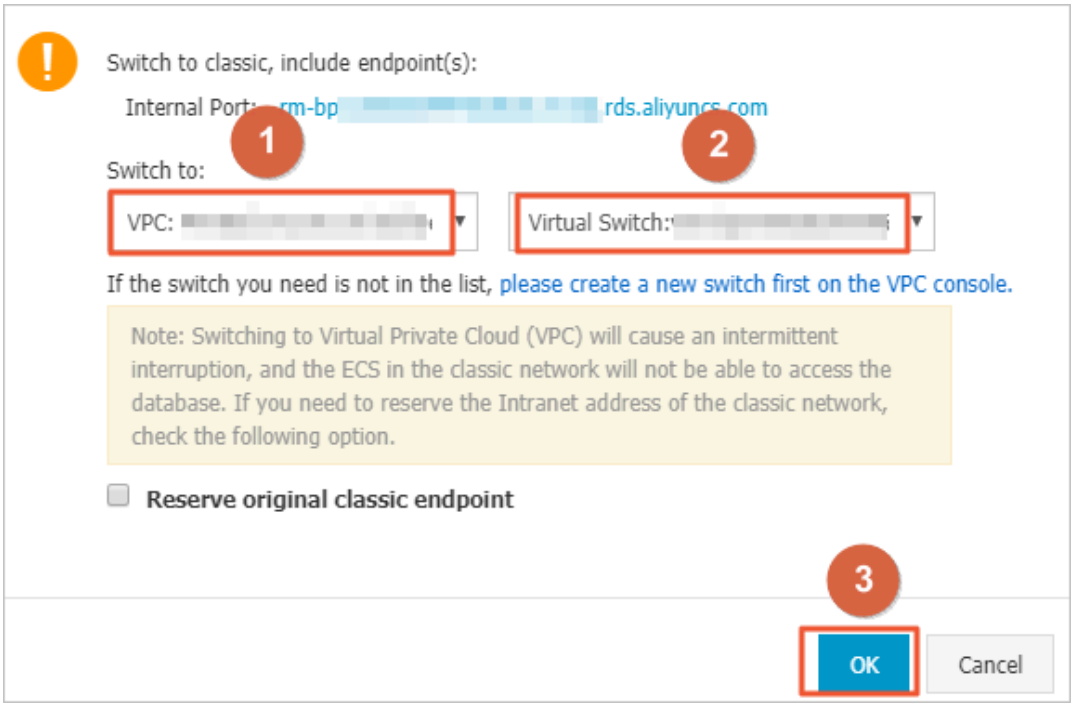
1. **Log on to the *RDS console*.**
2. **Select the target region.**




3. **Find the target 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**

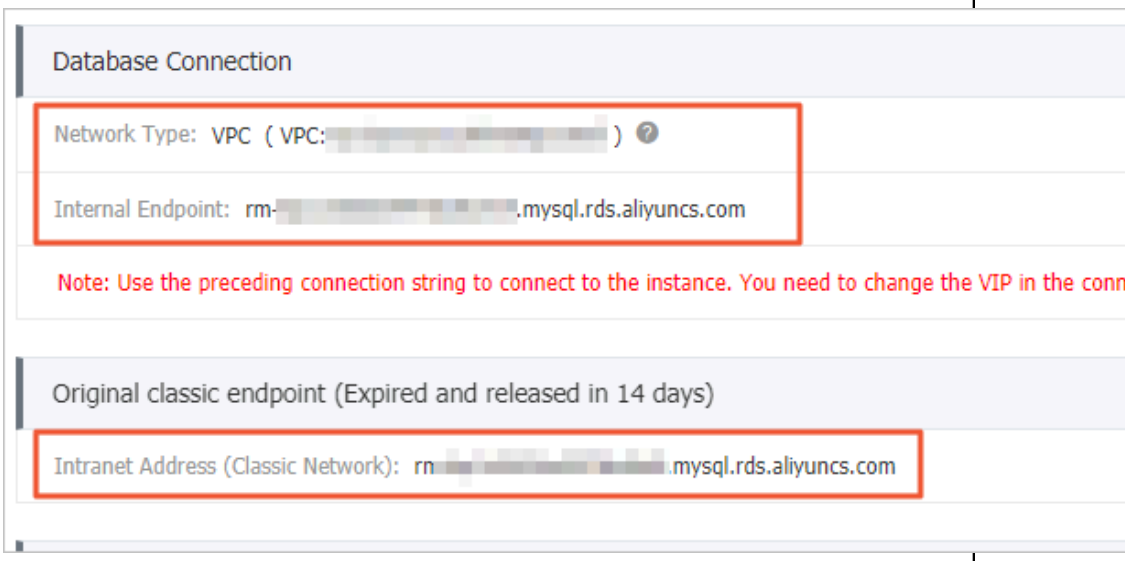
over the internal network unless *Express Connect* or *VPN Gateway* are created to connect the two VPCs.

- 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*.



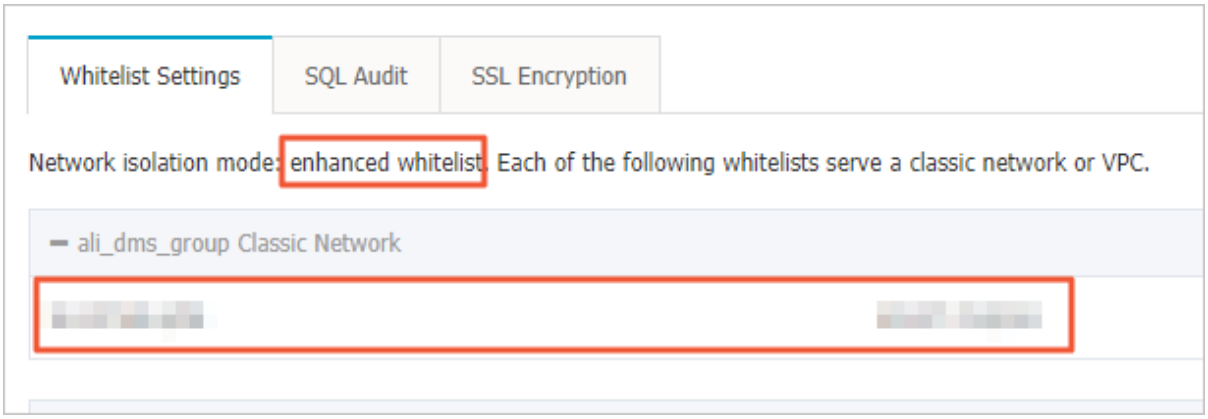

- Select or clear Reserve Original Classic Endpoint as needed. The following table describes the details.

| Action | Description |
| --- | --- |
| Clear | The classic network address is not retained. The original classic network address is changed to the VPC address.<br>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.<br><br>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.<br><br>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.<br><br>  <br><br>For more information, see *Configure a hybrid access solution to smoothly migrate the database from the classic network to a VPC*. |

7. Add the internal endpoint 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. · 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 |
| --- | --- |
| *ModifyDBInstanceNetworkType* | Switches the network type of an RDS instance. |

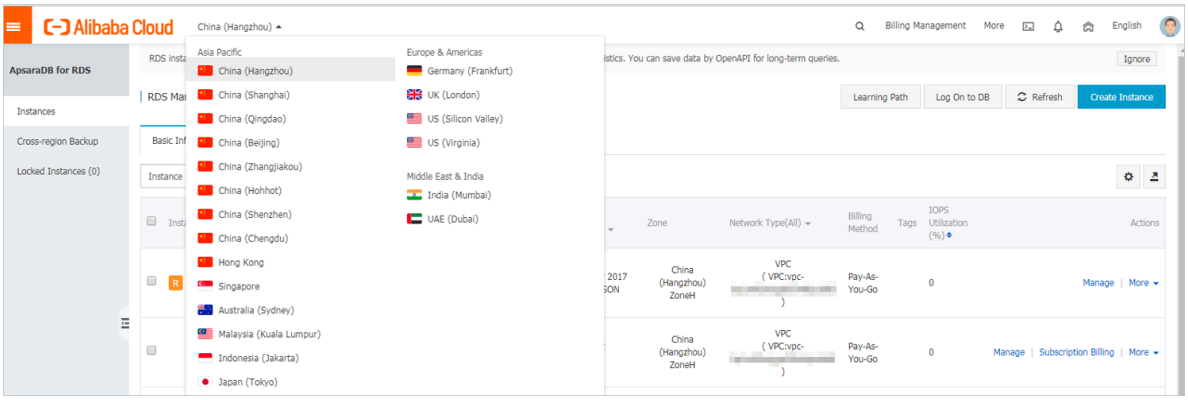
## 7.6 Release an RDS for PostgreSQL instance

This topic describes how to release an RDS for PostgreSQL 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 instance

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

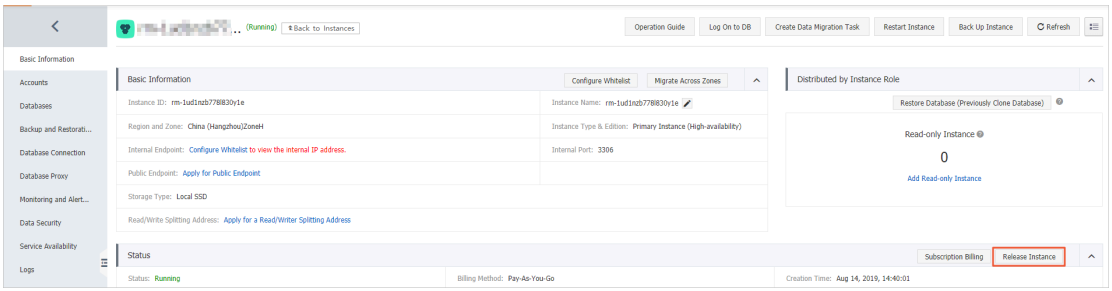



3. **Use one of the following methods to open the Release Instance dialog box:**

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


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

     **b. On the Basic Information page, click Release Instance.**




4. **In the displayed 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* | Releases an RDS instance. |

# 7.7 Change the configuration of an RDS for PostgreSQL instance

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

**You can upgrade or downgrade the configuration of an RDS for PostgreSQL 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.**

## Change items

**If you want to increase the read capability of a database, you can create read-only instances to relieve the pressure. For more information, see** *Introduction to RDS for PostgreSQL read-only instances* **and** *Create an RDS for PostgreSQL read-only instance*.

| Change item | Description |
| --- | --- |
| Instance type | You can modify the specifications of all instance types. |
| Capacity | You can increase the storage capacities of all instances.<br>You can decrease the storage capacity of subscription-based instances that are deployed based on local disks by using the *renewal* method.<br>**Note:**<br>· You cannot specify a storage capacity that exceeds the storage capacity limit of the instance type. For more information, see *#unique_16*.<br>· You cannot decrease the storage capacities of instances that are deployed based on cloud disks.<br>· If the storage capacity of the instance type cannot meet your needs, we recommend that you use a different instance type. |

**Note:**

**Changing the above specifications does not change the endpoint of the instance.**

Billing rules

**For more information, see** *Billing details about configuration change*.

Prerequisites

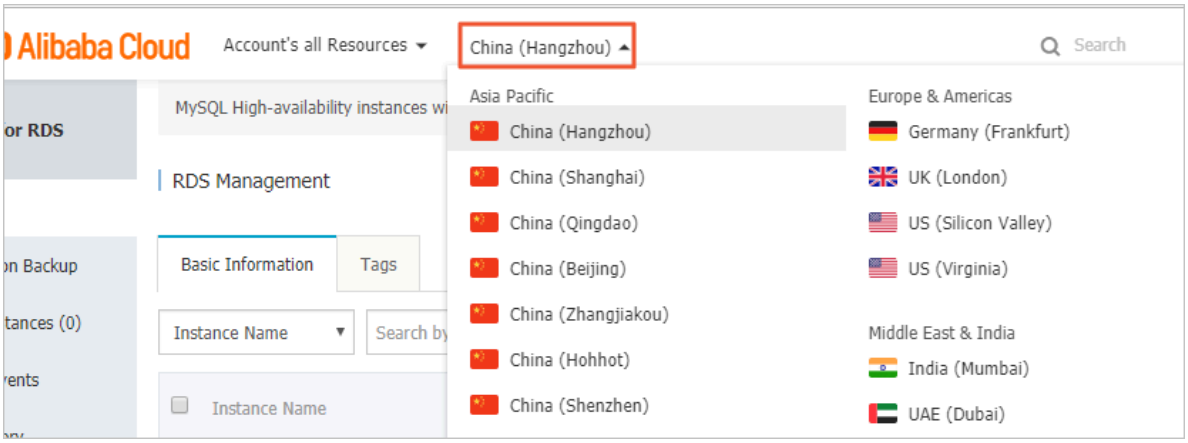
**Your Alibaba Cloud account does not have overdue renewal orders.**

Precautions

- **Your RDS instance may be disconnected for about 30 seconds when the specification changes take effect. During this period, management operations related to databases, accounts, and networks cannot be performed. We recommend that you change the specifications during off-peak hours, or configure automatic reconnection policies for your applications.**
- **In the Basic Edition, your RDS instance is not attached with any slave instances that can serve as hot backups. Therefore, if your RDS instance breaks down unexpectedly or you are changing the instance configuration or upgrading the instance version, your RDS service may remain unavailable for a long period of time. If you have high availability requirements on databases, we recommend that you use other editions such as the High-availability Edition.**

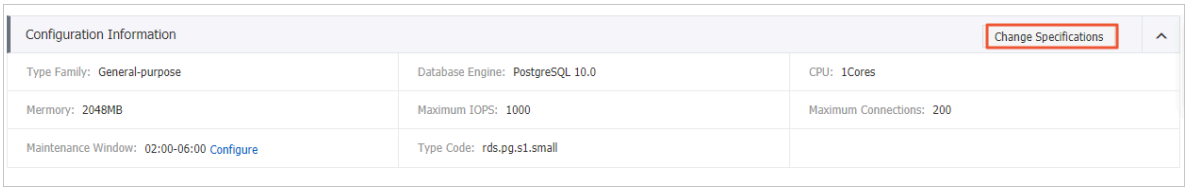
Procedure

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

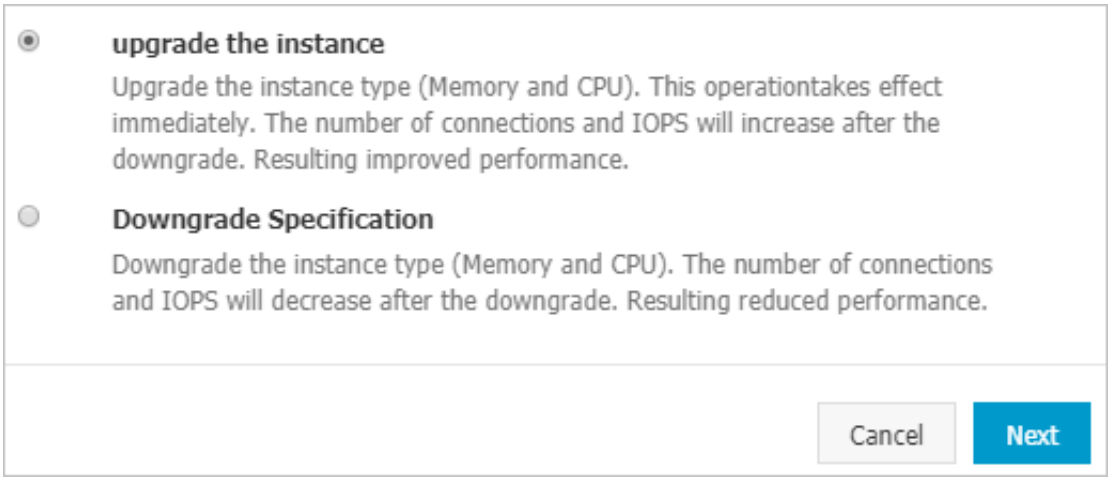



3. **Find the target RDS instance and click the instance ID.**

4. On the Basic Information page that appears, click Change Specifications in the Configuration Information section.




5. In the dialog box that appears, select the change method and click Next. This step is only required for subscription-based instances.

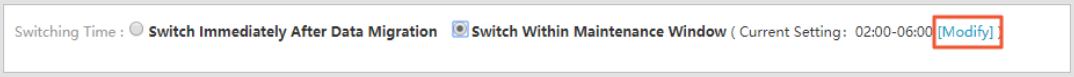



6. Modify Type and Capacity.
7. Specify the time to change the instance specifications.
   - Switch Immediately After Data Migration: Changing the instance specifications involves underlying data migration. You can change the configuration after data migration.
   - Switch Within Maintenance Window: Your RDS instance may be disconnected for about 30 seconds when the specification changes take effect. During this period, management operations related to databases, accounts, and networks cannot be performed. We recommend that you change the configuration within the maintenance window.

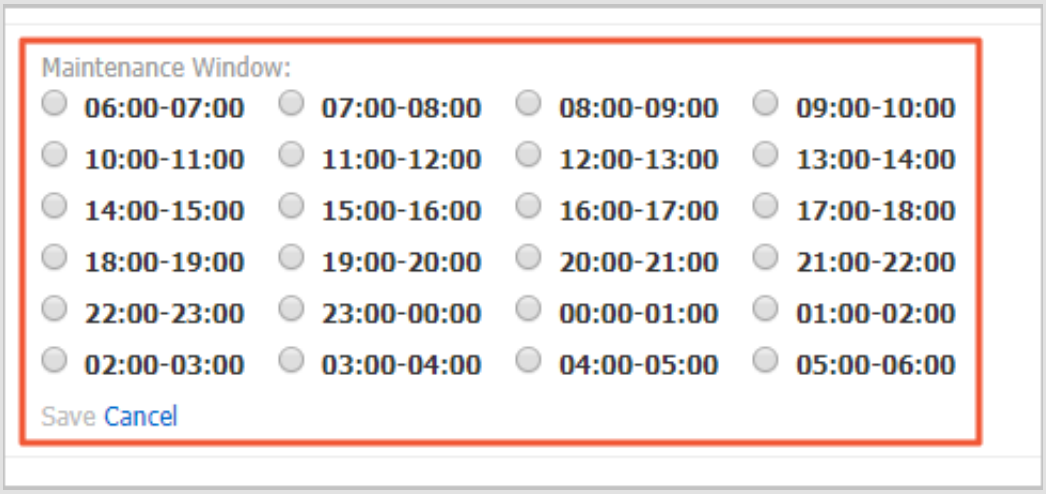
**Note:**

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

a. Click Modify.



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




c. Return to the configuration change page, refresh the page, and change the configuration.

8. On the Change Specifications page, select the Product Terms of Service, click Confirm, and complete the payment.

FAQ

**Do I need to migrate data to a new instance if I only expand the capacity?**

**Check whether there is sufficient storage space on the host where the instance is located for upgrading. If yes, you can upgrade without migrating data. If no, you must migrate data to a host that has enough storage space.**

APIs

| API | Description |
| --- | --- |
| *ModifyDBInstanceSpec* | **Modifies the specifications of an RDS instance.** |

## 7.8 Reconfigure parameters for an RDS for PostgreSQL instance

**This topic describes how to view and reconfigure some parameters for an RDS for PostgreSQL instance through the RDS console or APIs and how to view the parameter reconfiguration history through the RDS console.**

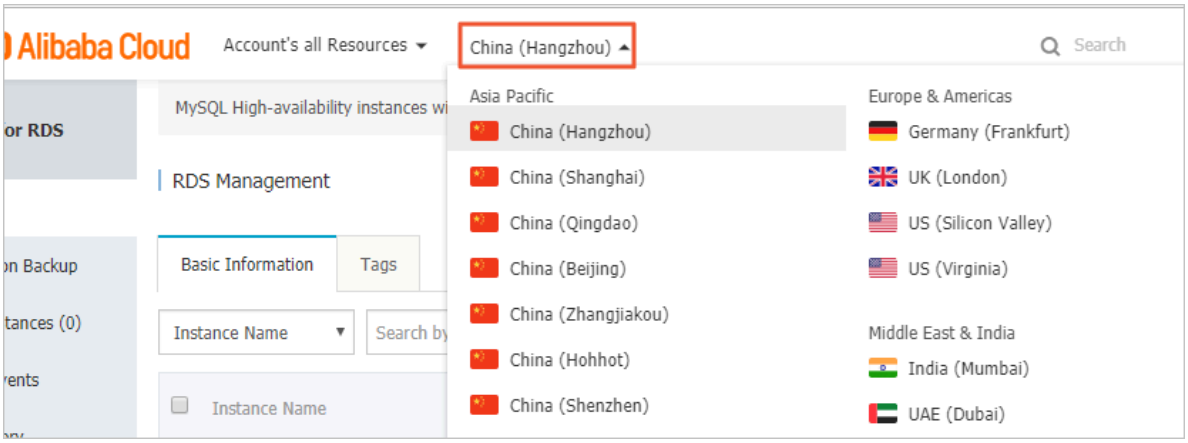
View and reconfigure parameters

**Precautions**

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

**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, select Parameters.

5. On the Modifiable Parameters tab, reconfigure one or more parameters at the same time. The procedure is as follows:

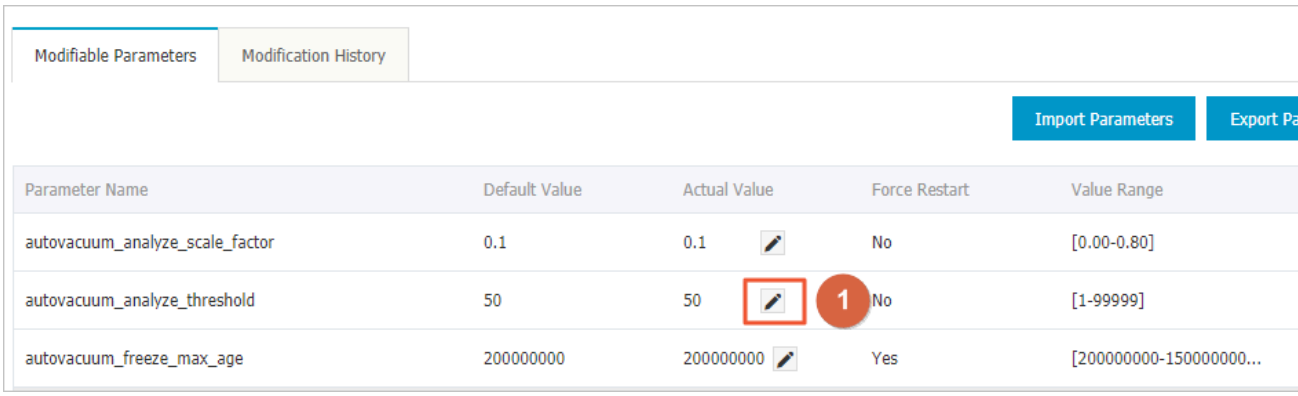
   - Reconfigure a parameter

     a. Click the icon corresponding to the parameter to be reconfigured.

     b. Enter a new value and click Confirm.

     c. Click Apply Changes.

     d. In the message that appears, click Confirm.




   - Reconfigure parameters in batches

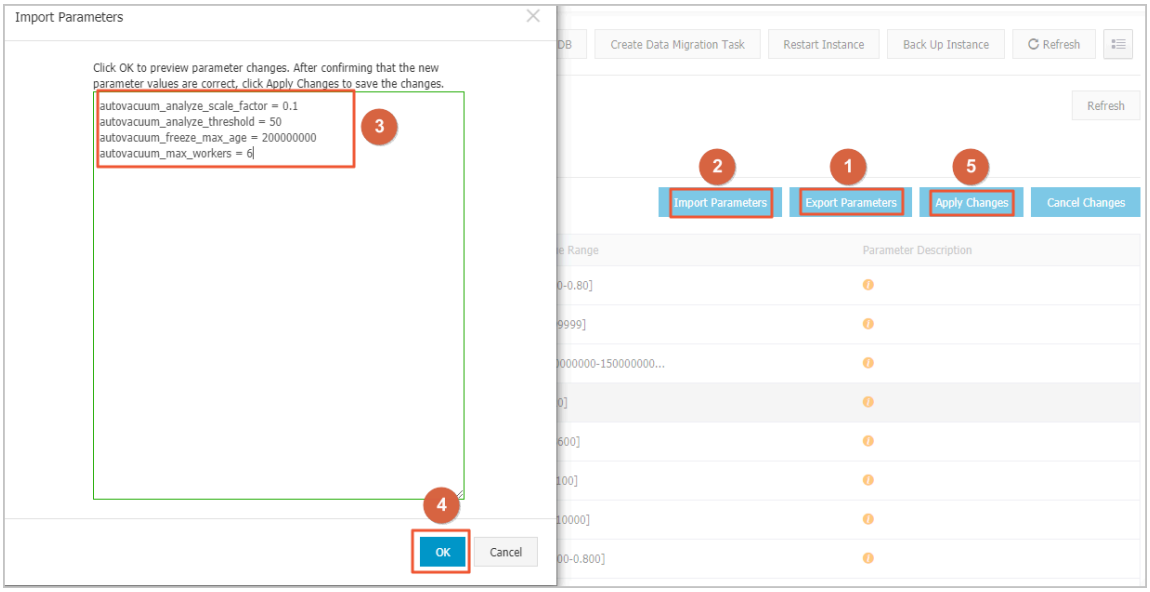
     a. Click Export Parameters to download the parameter file.

     b. Open the file and reconfigure parameters.

     c. After the parameters are reconfigured, click Import Parameters.

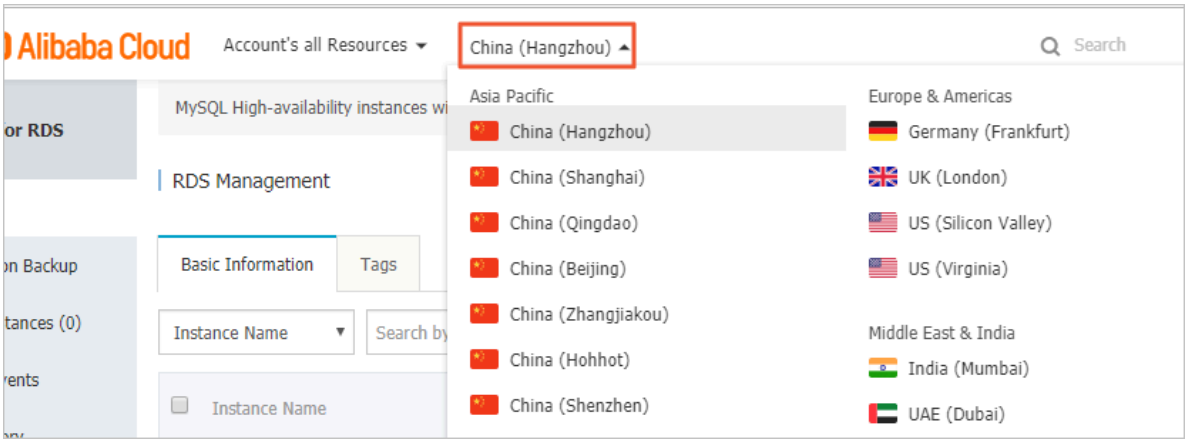
     d. In the Import Parameters dialog box that appears, copy the parameters and their new values in the file and paste in the editing field and click OK.

     e. Confirm the parameters after reconfiguration in the parameter list, and click Apply Changes.




View the parameter reconfiguration history

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




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

APIs

| Operation | Description |
| --- | --- |
| *#unique_69* | **Queries database parameter templates.** |
| *#unique_70* | **Queries the current parameter configurations of an instance.** |

| Operation | Description |
| --- | --- |
| #unique_71 | Reconfigures the parameters of an instance. |

Parameter description

**For more information about parameter settings, see *PostgreSQL Official Documentation*.**

## 7.9 Instance recycle bin

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

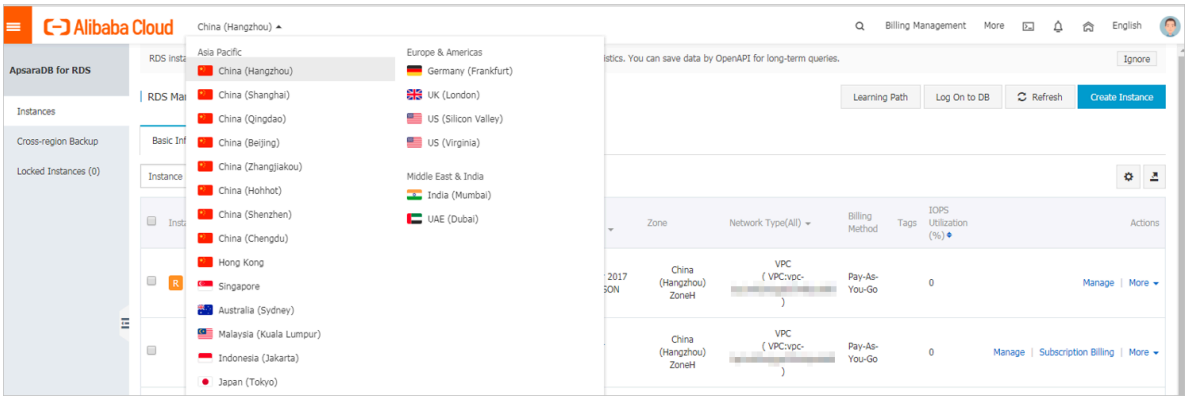
Unlock an RDS instance that has overdue payments

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

Unlock an RDS instance that has expired

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

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




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

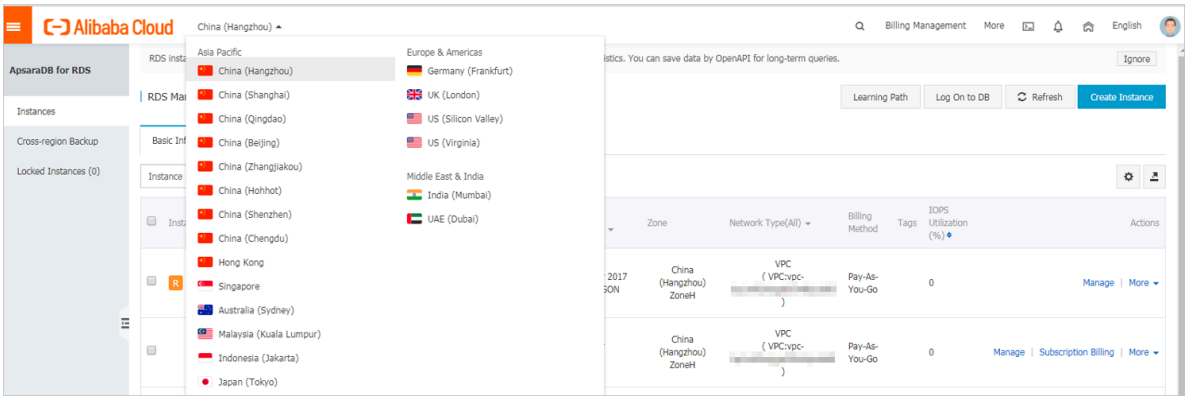
   **The instance is unlocked after renewal.**

Re-create an RDS instance

**After an RDS instance expires, it is released on the eighth day and its data keeps stored in the system for another eight days. Within the eight days, you can restore the instance data to a new instance. On the 16th day counting from the day when**

the RDS instance expired, the instance data is deleted from the system and cannot be retrieved.

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



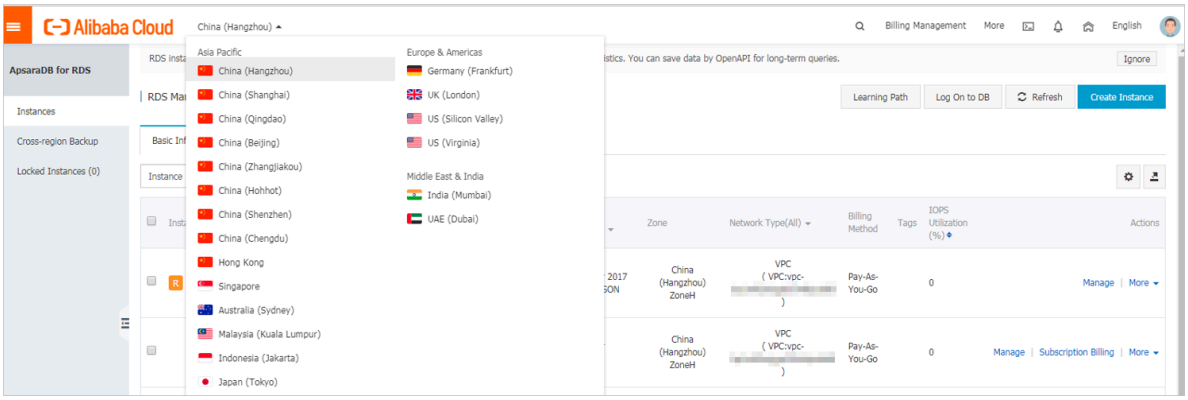

3. In the left-side navigation pane, click Locked Instances.
4. Find the target RDS instance and click the button for re-creating an RDS instance.

   By default, the system creates an RDS instance that has the same specifications and resides in the same zone as the released RDS instance. You can select other zones and specifications as needed.

## Destroy an RDS instance

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

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




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

# 7.10 Release notes

PostgreSQL 10.8

**Release date: 2019-06-12**

**Fixed bugs and security vulnerabilities (CVE-2019-10130). For more information, see** *PostgreSQL Official Documentation*.

# 8 Account management

## 8.1 Create an account

**Before you start to use ApsaraDB for RDS, you must create an account for the RDS instance.**

- **For instances of ApsaraDB RDS for PostgreSQL 11 Cluster Edition (Standard SSD) and PostgreSQL 10 Cluster Edition (Standard SSD), you can directly create a premier account and standard account in the ApsaraDB for RDS console.**
- **For instances of ApsaraDB RDS for PostgreSQL 10 Cluster Edition (Local SSD), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4, you can create a premier account in the ApsaraDB for RDS console.**

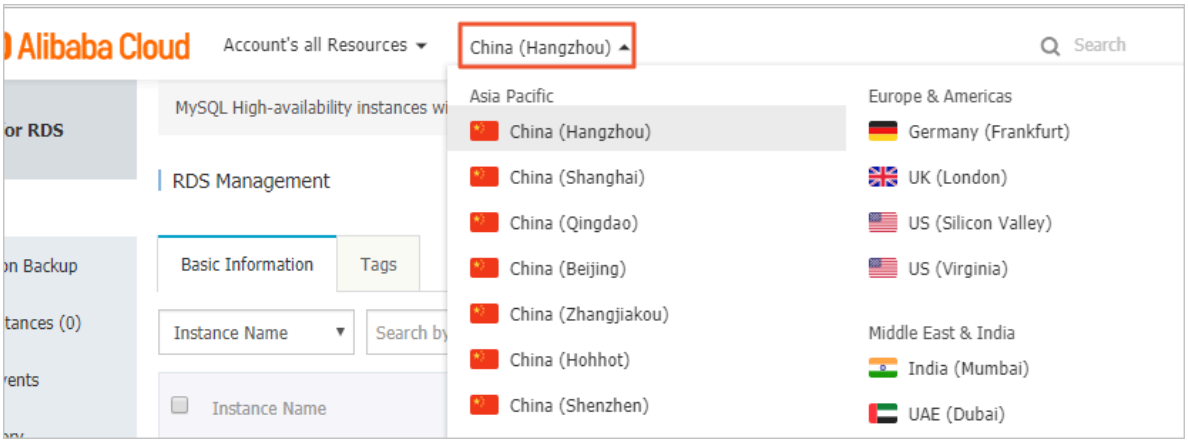
Notes

- **Databases within the same instance share all the resources of the instance. You can create a premier account and multiple standard accounts for each ApsaraDB RDS for PostgreSQL instance. You can also use SQL commands to create and manage accounts.**
- **To migrate the on-premises database to ApsaraDB for RDS, you must create a database and account in the RDS instance consistent with those in the on-premises database.**
- **When you create database accounts, you must assign permissions based on the principle of least privilege and the requirements of the role. You can assign the read-only or read/write permissions to different accounts. When necessary, you can create multiple database accounts and allow each of them only to access data of their own business. If an account does not need to write data to a database, assign read-only permissions to the account.**
- **For database security, you must set strong account passwords and change the passwords regularly.**
- **The premier account cannot be deleted after it is created.**

For PostgreSQL 11 Cluster Edition (Standard SSD) and PostgreSQL 10 Cluster Edition (Standard SSD)

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

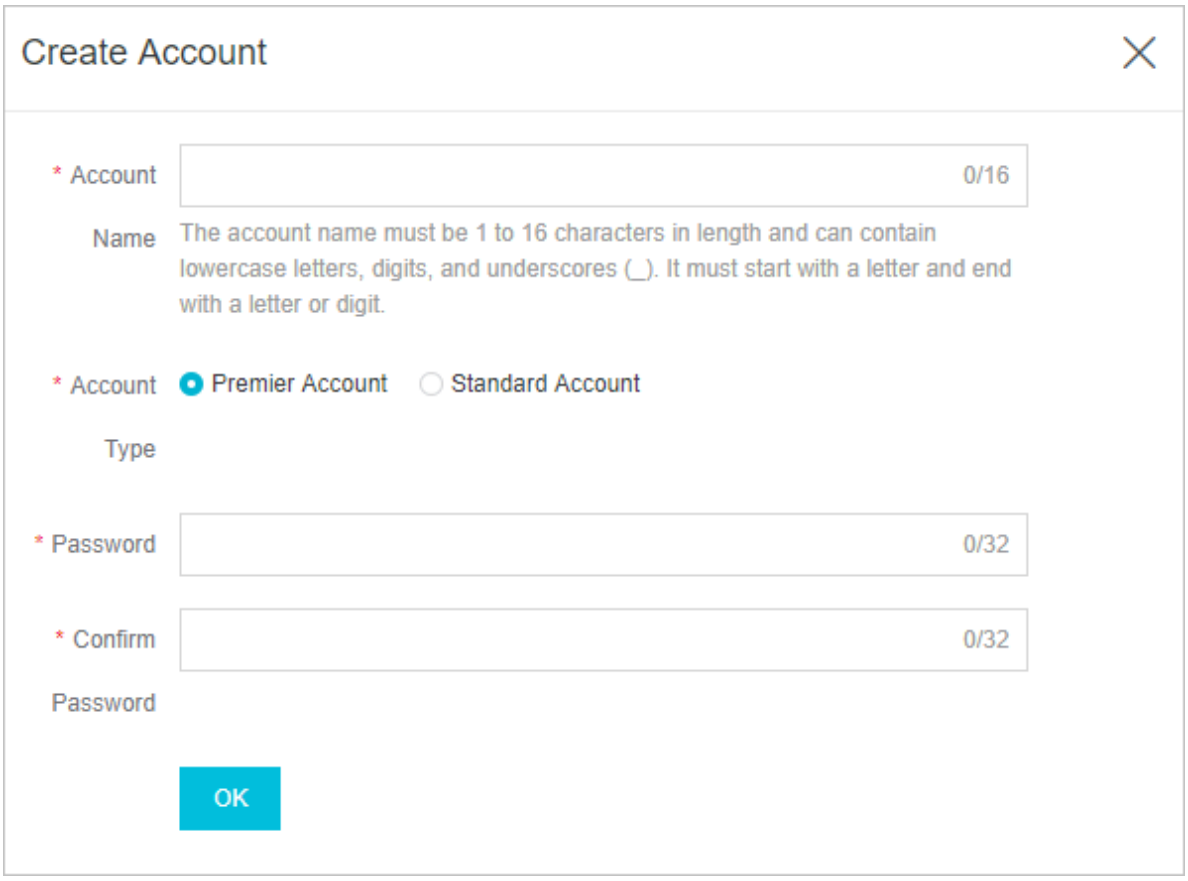
2. In the upper-left corner of the page, select the region where the instance is located.




3. Find the instance and click the instance ID.
4. In the left-side navigation pane, click Accounts.
5. Click Create Account.
6. Configure the following parameters.

| Parameter | Description |
| --- | --- |
| Database account | · The database account must be up to 16 characters in length.<br>· It can contain lowercase letters, digits, and underscores (_).<br>· It must start with a letter and end with a letter or digit. |
| Account type | The account type of your database. You can specify a premier or standard account. |
| Password | · The password must be 8 to 32 characters in length.<br>· It must contain three of the following character types: uppercase letters, lowercase letters, digits, and special characters.<br>· Special characters include ! @ # $ % ^ & * ( ) _ + - = |

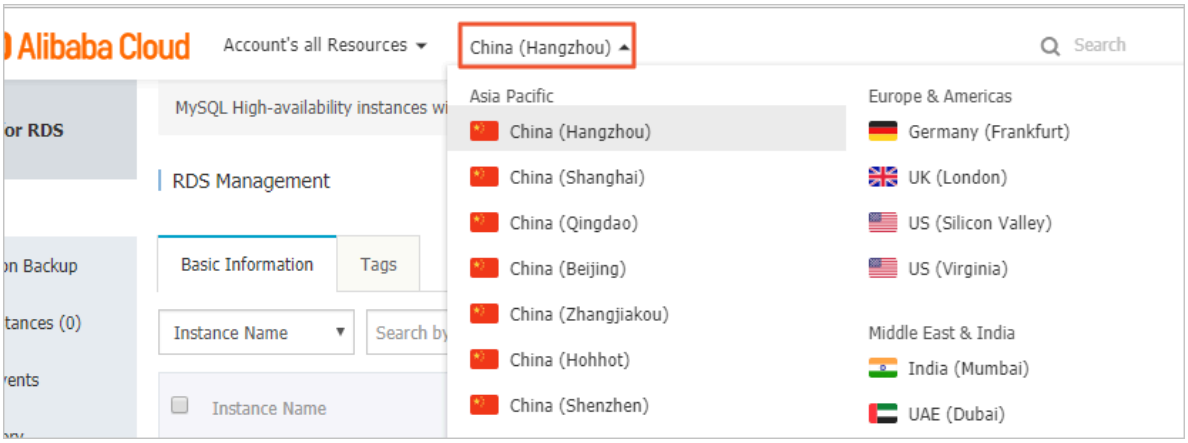
| Parameter | Description |
| --- | --- |
| Re-enter password | Enter the same password again. |




7. **Click OK.**

For PostgreSQL 10 Cluster Edition (Local SSD), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4

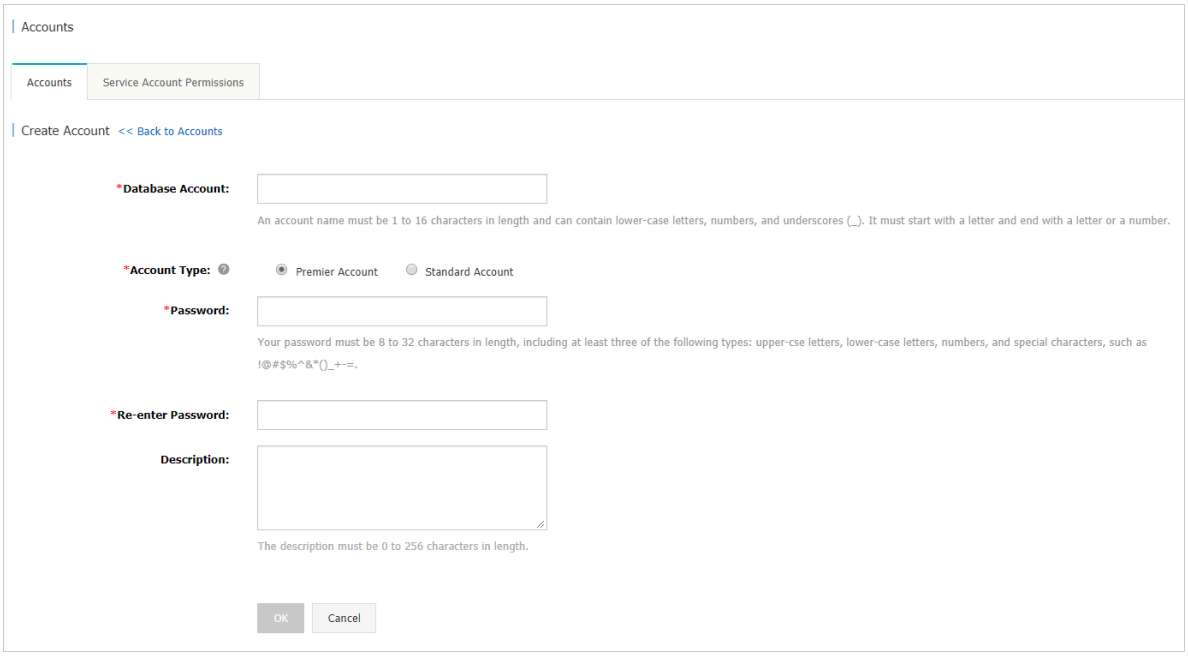
1. **Log on to the** *ApsaraDB for RDS console*.
2. **In the upper-left corner of the page, select the region where the instance is located.**




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

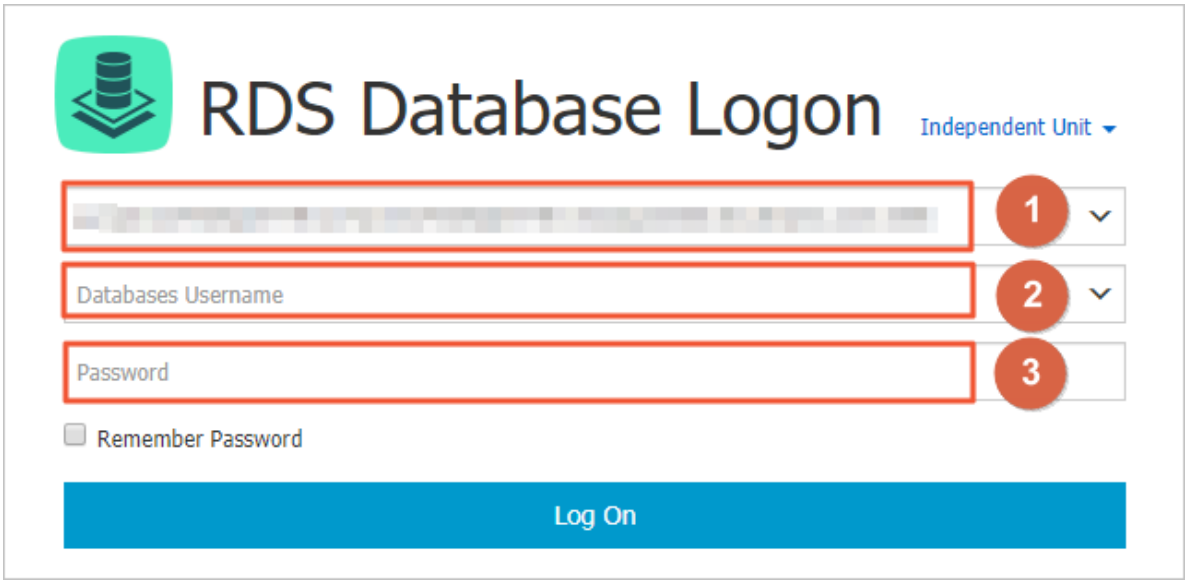
4. In the left-side navigation pane, click Accounts.
5. Click Create Account.
6. Configure the following parameters.

| Parameter | Description |
| --- | --- |
| Database account | · The database account must be 2 to 16 characters in length.<br>· It can contain lowercase letters, digits, and underscores (_).<br>· It must start with a letter and end with a letter or digit. |
| Password | · The password must be 8 to 32 characters in length.<br>· It must contain three of the following character types: uppercase letters, lowercase letters, digits, and special characters.<br>· Special characters include ! @ # $ % ^ & * ( ) _ + - = |
| Re-enter password | Enter the same password again. |




7. Click OK.
8. In the upper-right corner of the page, click Log On to DB to enter the Quick Logon page of the *DMS console*.

9. On the Quick Logon page, check the endpoint and port information displayed on the RDS Database Logon page. If the information is correct, enter the username and password of the database, as shown in the following figure.




| Parameter | Description |
| --- | --- |
| Network address: port | The endpoint and port information to connect to the RDS instance. |
| Database username | The username of the account used to access the database. |
| Password | The password of the account used to access the database. |

10. Click Log On.

> **Note:**
> If you want the Web browser to remember the password, select Remember Password and click Log On.

11. If DMS prompts you to add the IP CIDR block of the DMS server to the RDS address whitelist, click Configure Whitelist. For more information about how to manually configure the whitelist, see *Configure a whitelist*.
12. After the whitelist is configured, click Log On.
13. After you have logged on to the RDS instance, in the top navigation bar, choose SQL Operations > SQL Window.
14. In the SQL window, run the following statement to create a standard account:

```
CREATE USER name [ [ WITH ] option [ ... ] ]
where option can be:
```

```
    SUPERUSER | NOSUPERUSER
  | CREATEDB | NOCREATEDB
  | CREATEROLE | NOCREATEROLE
  | CREATEUSER | NOCREATEUSER
  | INHERIT | NOINHERIT
  | LOGIN | NOLOGIN
  | REPLICATION | NOREPLICATION
  | CONNECTION LIMIT connlimit
  | [ ENCRYPTED | UNENCRYPTED ] PASSWORD 'password'
  | VALID UNTIL 'timestamp'
  | IN ROLE role_name [, ...]
  | IN GROUP role_name [, ...]
  | ROLE role_name [, ...]
  | ADMIN role_name [, ...]
  | USER role_name [, ...]
  | SYSID uid
```

**For example, if you want to create a user account named test2 and the password 123456, run the following command:**

```
create user test2 password '123456';
```

API reference

| Operation | Description |
| --- | --- |
| *CreateAccount* | **You can call this operation to create an account.** |

## 8.2 Reset the password

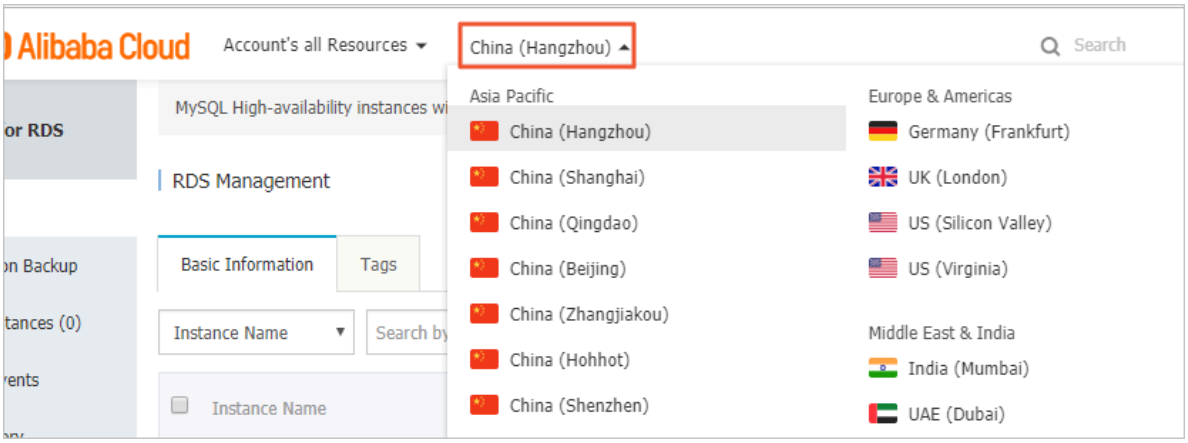
**This topic describes how to reset the password of an account for an RDS for PostgreSQL instance in case that the password is lost.**

**Note:**
**For ApsaraDB RDS for PostgreSQL 10 Cluster Edition (Local SSD), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4 instances, you can only reset the password for the premier accounts.**

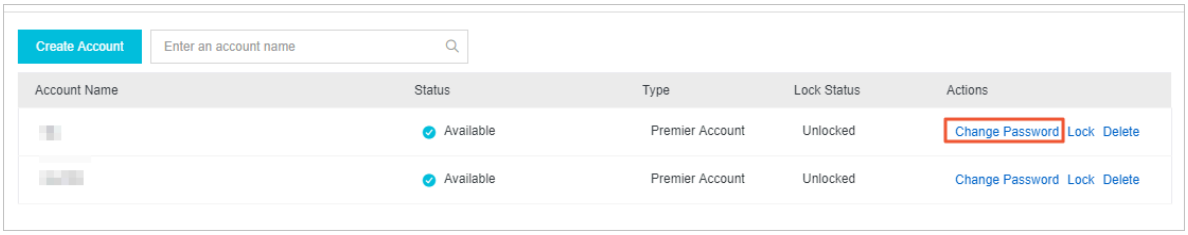
For PostgreSQL 11 Cluster Edition (Standard SSD) and PostgreSQL 10 Cluster Edition (Standard SSD)

1. **Log on to the** *ApsaraDB RDS for PostgreSQL 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 Accounts.**
5. **Find the account that you want to reset the password, and click Reset Password.**



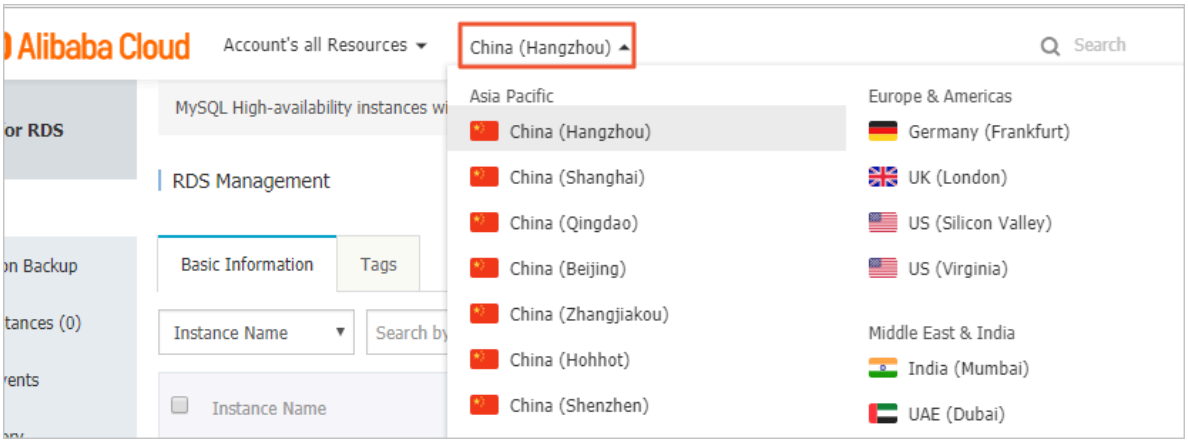

6. **In the dialog box that appears, enter a new password, and click OK.**

> **Note:**
> **The password must meet the following requirements:**
>
> - **The password must be 8 to 32 characters in length.**
> - **It must contain three of the following character types: uppercase letters, lowercase letters, digits, and special characters.**
> - **Special characters include ! @ # $ % ^ & * ( ) _ + - =**

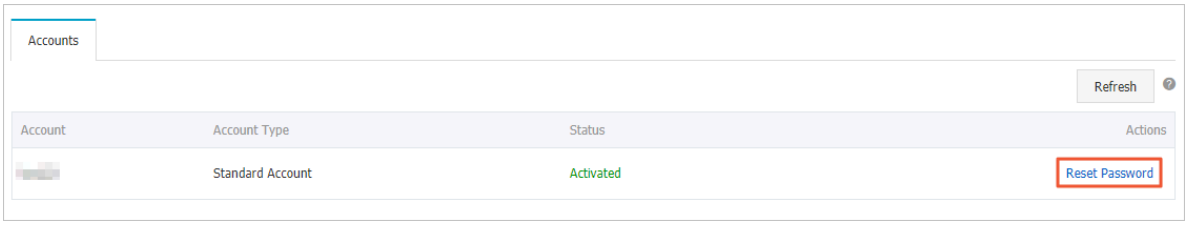
For PostgreSQL 10 Cluster Edition (Local SSD), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4

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 Databases.
5. Find the account that you want to reset the password, and click Reset Password.




6. In the dialog box that appears, enter a new password, and click OK.

**Note:**

The password must meet the following requirements:

- The password must be 8 to 32 characters in length.
- It must contain three of the following character types: uppercase letters, lowercase letters, digits, and special characters.
- Special characters include ! @ # $ % ^ & * ( ) _ + - =

API reference

| Operation | Description |
| --- | --- |
| *ResetAccountPassword* | You can call this operation to reset the password of an account. |

# 9 Database management

## 9.1 Create a database

**Before you start to use ApsaraDB for RDS, you must create a database and account for the RDS instance.**

- **For instances of ApsaraDB RDS for PostgreSQL 11 Cluster Edition (Standard SSD ) and PostgreSQL 10 Cluster Edition (Standard SSD), you can directly create and manage databases in the ApsaraDB for RDS console.**
- **For instances of ApsaraDB RDS for PostgreSQL 10 Cluster Edition (Local SSD), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4, you need to create and manage databases through the Data Management Service (DMS) console or other remote management tools.**

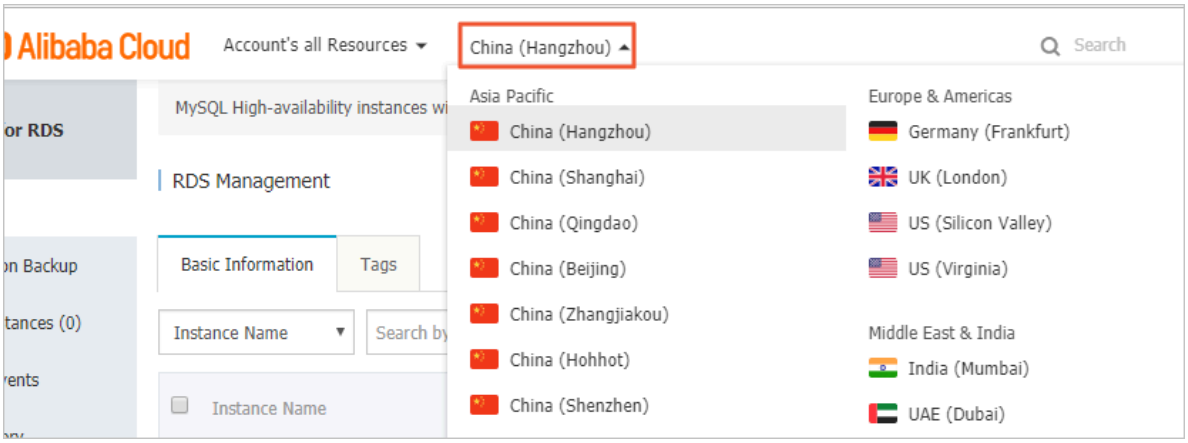
Notes

- **Databases within the same instance share all the resources of the instance. You can create multiple databases for each ApsaraDB RDS for PostgreSQL instance. You can also use SQL commands to create and manage databases.**
- **To migrate the on-premises database to ApsaraDB for RDS, you must create a database and account in the RDS instance consistent with those in the on-premises database.**

For PostgreSQL 11 Cluster Edition (Standard SSD) and PostgreSQL 10 Cluster Edition (Standard SSD)

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

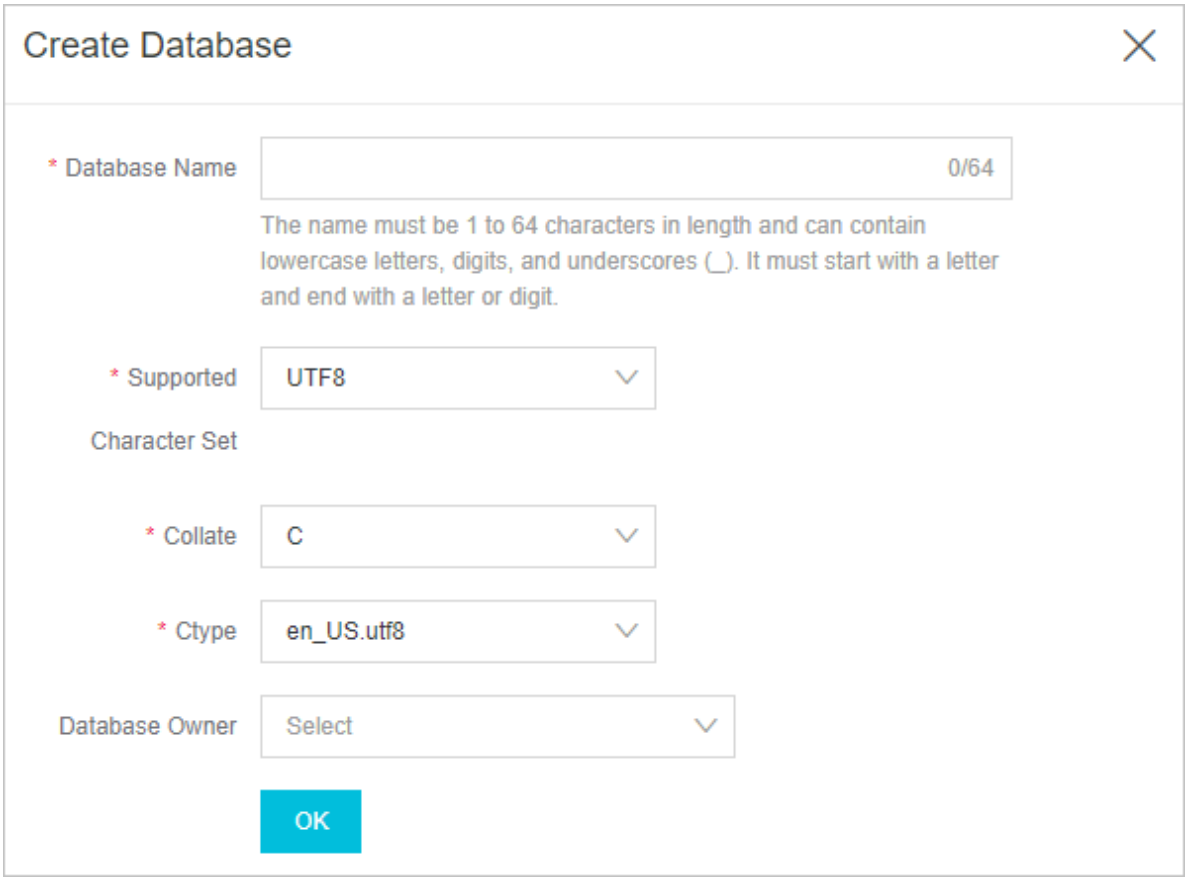
2. In the upper-left corner of the page, select the region where the instance is located.




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

| Parameter | Description |
| --- | --- |
| Database (DB) name | · The name can be up to 64 characters in length.<br>· It can contain lowercase letters, digits, underscores (_), and hyphens (-).<br>· It must start with a letter and end with a letter or digit. |
| Supported character set | The character set that is supported by the database. |
| Collate | The sorting rules of strings. |
| Ctype | The type of characters. |

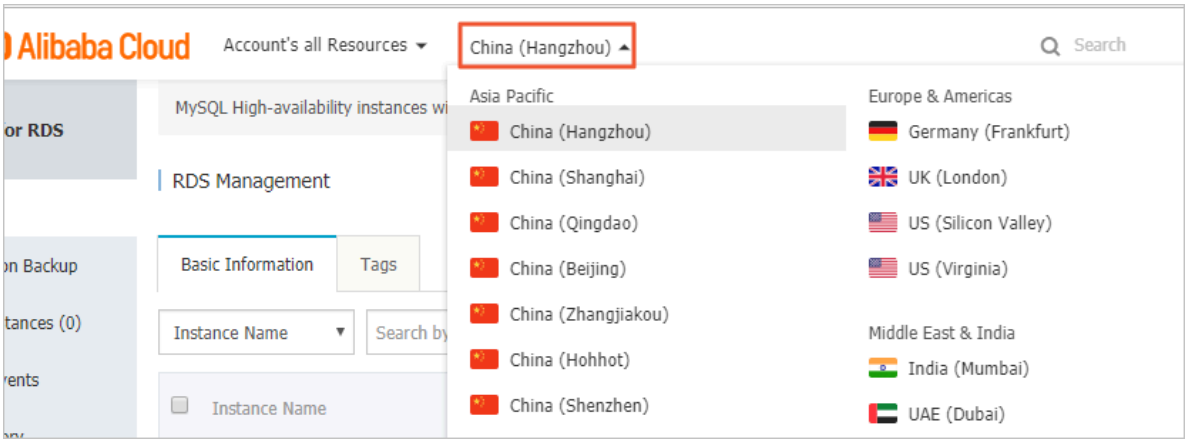
| Parameter | Description |
| --- | --- |
| Database owner | The database owner, who has all permissions on the database. |



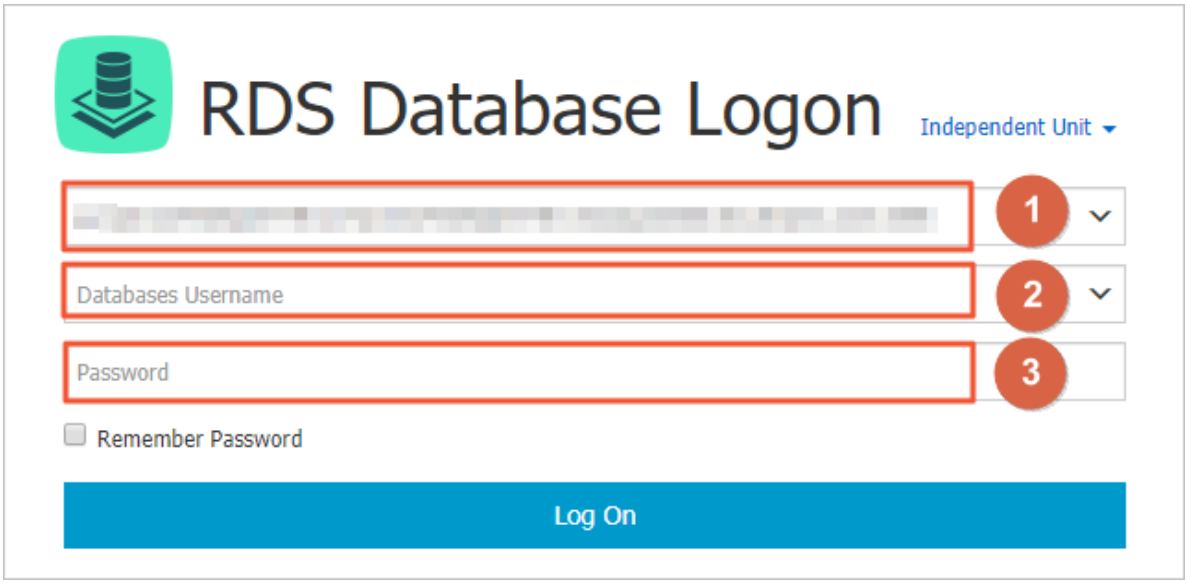

7. **Click OK.**

For PostgreSQL 10 Cluster Edition (Local SSD), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4

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 upper-right corner of the page, click Log On to DB to enter the Quick Logon page of the *DMS console*.
5. On the Quick Logon page, check the endpoint and port information displayed on the RDS Database Logon page. If the information is correct, enter the username and password of the database, as shown in the following figure.




| Parameter | Description |
| --- | --- |
| Network address: port | The endpoint and port information to connect to the RDS instance. |
| Database username | The username of the account used to access the database. |
| Password | The password of the account used to access the database. |

6. If the system prompts you to add the IP CIDR block of the DMS server to the RDS whitelist, click Configure Whitelist. For more information about how to manually configure the whitelist, see *Configure a whitelist*.
7. After the whitelist is configured, click Log On.
8. After you have logged on to the RDS instance, in the top navigation bar, choose SQL Operations > SQL Window.
9. In the SQL window, run the following statement to create a database:

```
CREATE DATABASE name
 [ [ WITH ] [ OWNER [=] user_name ]
        [ TEMPLATE [=] template ]
        [ ENCODING [=] encoding ]
        [ LC_COLLATE [=] lc_collate ]
        [ LC_CTYPE [=] lc_ctype ]
```

```
        [ TABLESPACE [=] tablespace_name ]
        [ CONNECTION LIMIT [=] connlimit ] ]
```

**For example, if you want to create a database named test, run the following command.**

```
create database test;
```

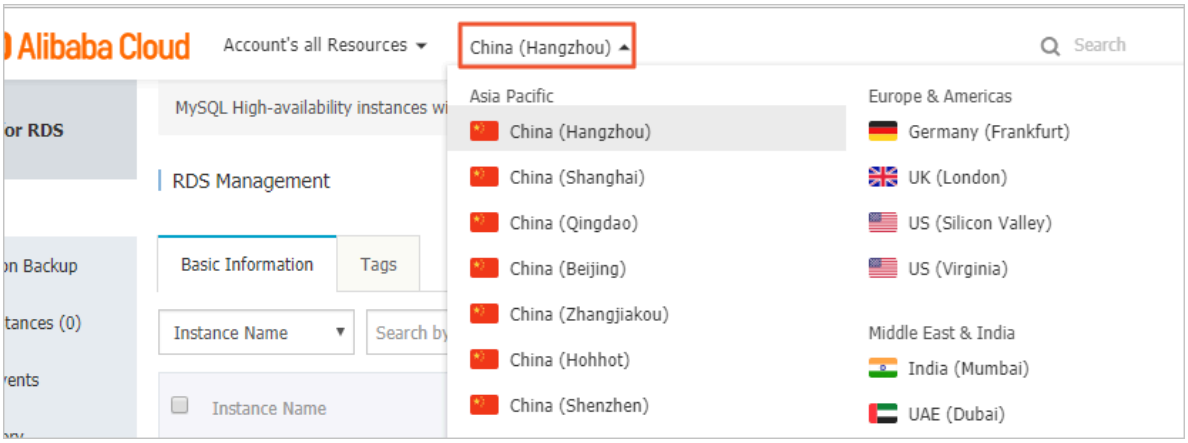
10. **Click OK.**

## 9.2 Delete a database

- **For instances of ApsaraDB RDS for PostgreSQL 10 Cluster Edition (Local SSD ), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4, you can delete a database through the Data Management Service (DMS) console or universal clients.**
- **For instances of ApsaraDB RDS for PostgreSQL 11 Cluster Edition (Standard SSD ) and PostgreSQL 10 Cluster Edition (Standard SSD), you can directly create and manage databases in the ApsaraDB for RDS console.**

For PostgreSQL 11 Cluster Edition (Standard SSD) or PostgreSQL 10 Cluster Edition (Standard SSD)

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

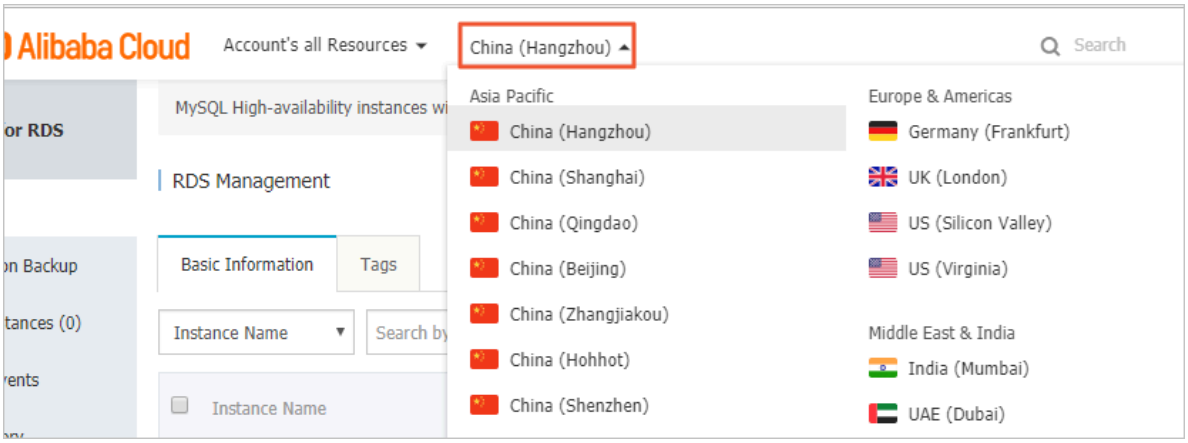



3. **Find the instance and click the instance ID.**
4. **In the left-side navigation pane, click Databases.**
5. **Find the database to be deleted, and click Delete in the Actions column.**
6. **In the dialog box that appears, click OK.**

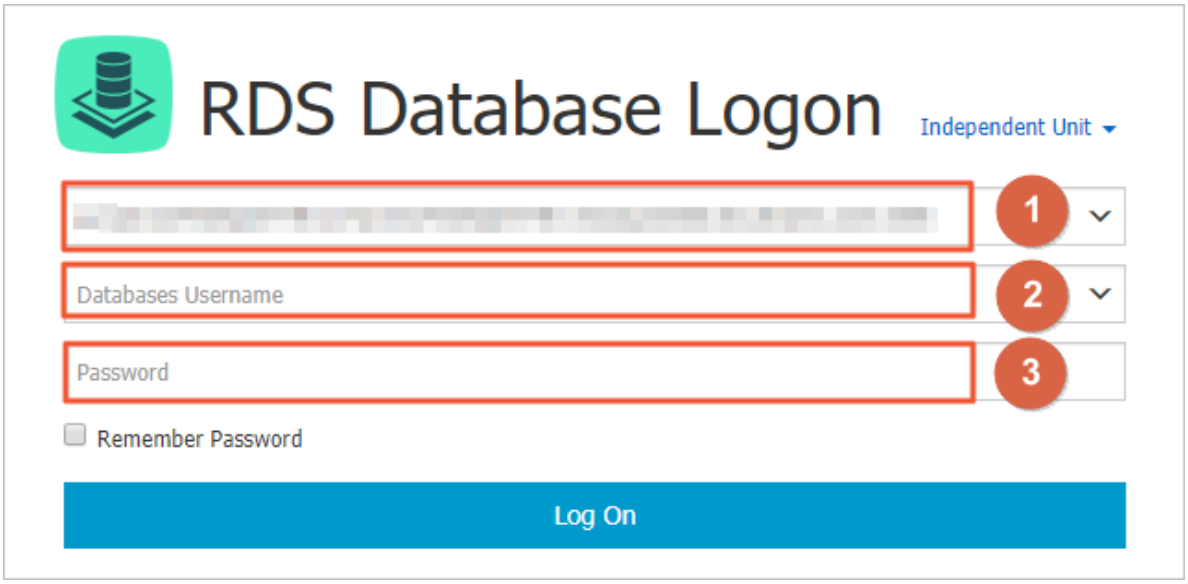
For PostgreSQL 10 Cluster Edition (Local SSD), PostgreSQL 10 Basic Edition, or PostgreSQL 9.4

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. Click Log On to DB in the upper-right corner of the page to enter the Quick Logon page of the *DMS console*.
5. On the Quick Logon page, check the endpoint and port information displayed on the RDS Database Logon page. If the information is correct, enter the username and password of the database, as shown in the following figure.




| Parameter | Description |
| --- | --- |
| Endpoint: port | The endpoint and port information of the instance. |
| Database username | The name of the account to access the database. |
| Password | The password of the account to access the database. |

6. If the system prompts you to add the IP CIDR block of the DMS server to the RDS whitelist, click Configure Whitelist. For more information about how to manually configure the whitelist, see *Configure a whitelist*.
7. Click Log On.
8. In the top navigation bar, choose SQL Operations > SQL Window.
9. Run the following statement to delete the database:

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

10. Click Execute to delete the database.

# 10 Database connections

## 10.1 Configure a hybrid access solution to smoothly migrate the database 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.**

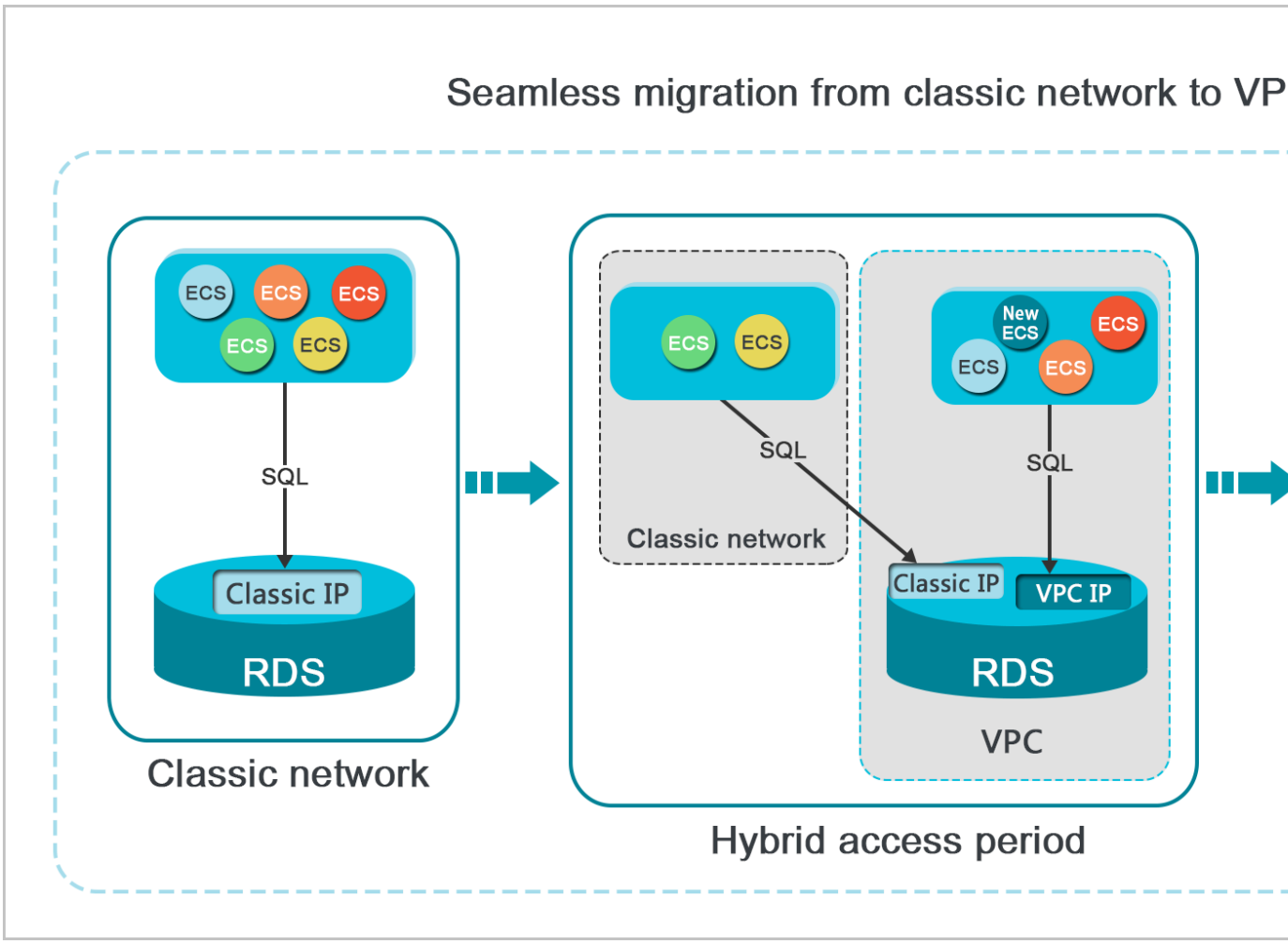
### Background information

**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

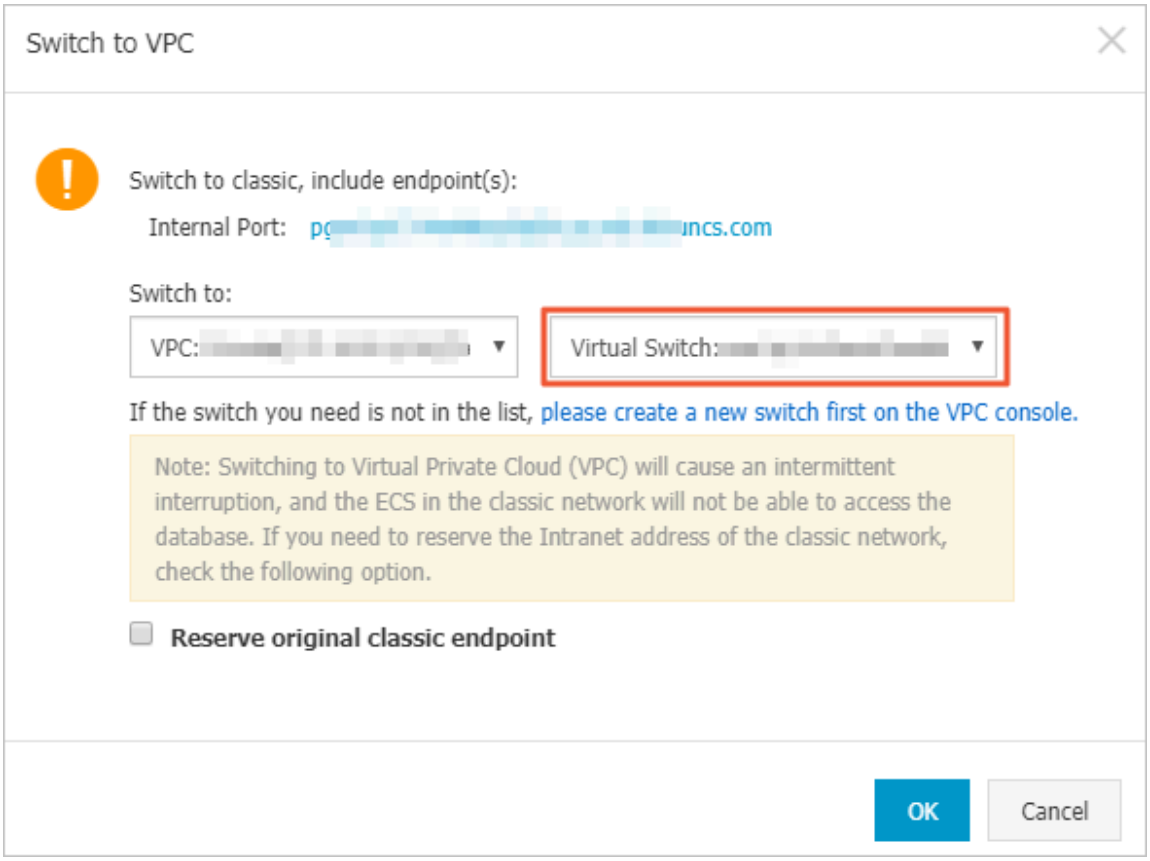
1. **Log on to the *ApsaraDB for RDS console*.**
2. **In the upper-left corner of the page, select the region where the instance is located.**


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**

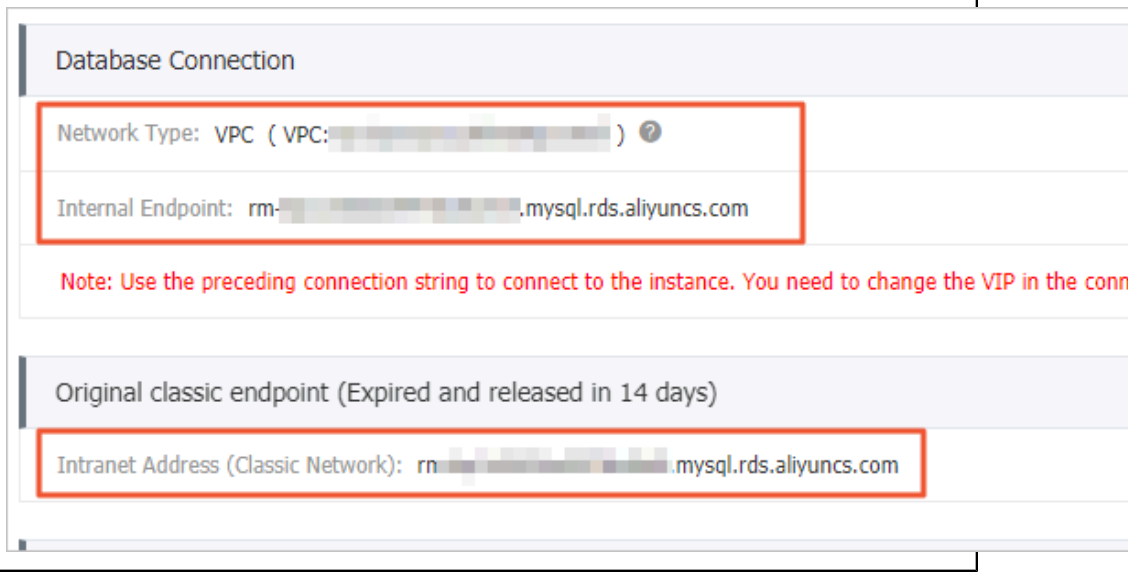
through the internal connections unless you create an express connection or gateway. For more information, see *Express connection* and *VPN gateway*.

- 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*.



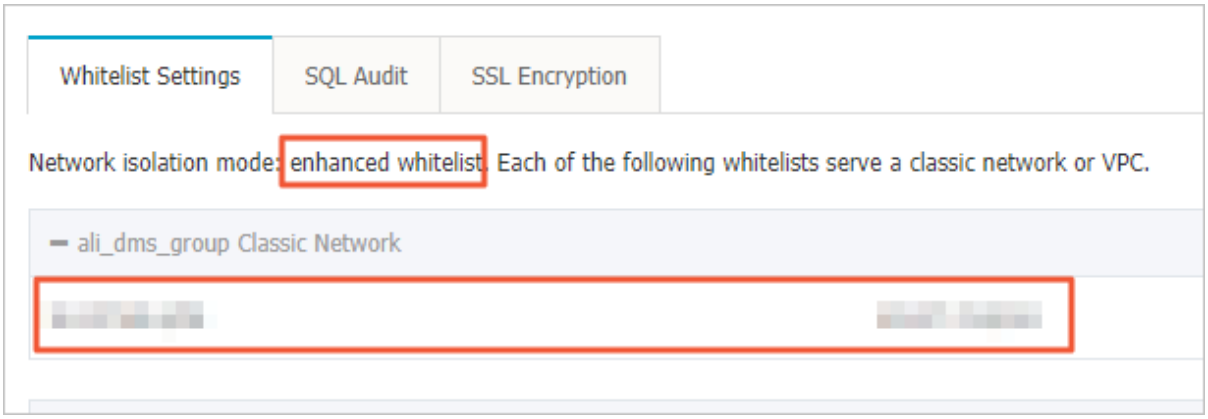

- Decide whether to select Retain Classic Network. The following table describes the different actions.

| Action | Description |
| --- | --- |
| Clear | The endpoint of the classic network is not retained. The original endpoint is changed to the endpoint of the VPC.<br>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.<br><br>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.<br><br>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.<br><br>  |

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.**

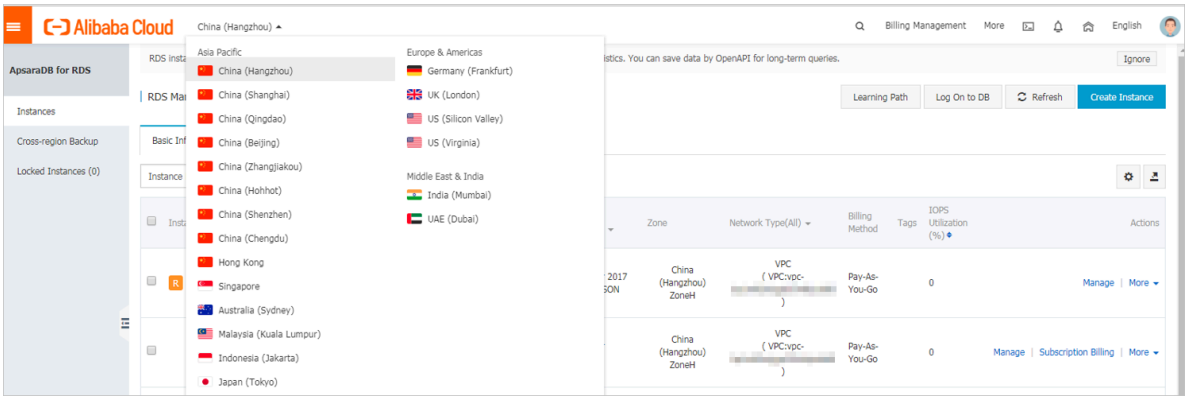
Change the expiration time for the original internal endpoint of the classic network

**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.

## 10.2 Configure endpoints for an RDS for PostgreSQL instance

ApsaraDB for RDS provides two types of endpoints: internal endpoints and public endpoints.

Internal and public endpoints

| Endpoint type | Description |
| --- | --- |
| Internal endpoint | · The internal endpoint is provided by default. You do not need to apply for it and cannot release it. However, you can change the network type.<br>· If your application is deployed to an ECS instance that is in the same region and has the same *network type* as the RDS instance, the RDS instance and the ECS instance can communicate each other by default. You do not need to apply for a public endpoint for the RDS instance.<br>· Accessing an RDS instance through the internal endpoint achieves the high security and performance of the RDS instance. |

| Endpoint type | Description |
| --- | --- |
| Public endpoint | · You must manually apply for a public endpoint. You can release the public endpoint if you do not need it.<br>· When you cannot access an RDS instance through the internal endpoint, you need to apply for a public endpoint. The following section describes the specific scenarios:<br>- When you access an RDS instance from an ECS instance, where the ECS instance and RDS instance are located in different regions, and the *network types* are different.<br>- When you access an RDS instance from the third-party services or applications.<br>**Note:**<br>· For the security of your instance, use caution when you access RDS instances through a public endpoint.<br>· 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 applications. This helps to improve transmission speed and data security. |

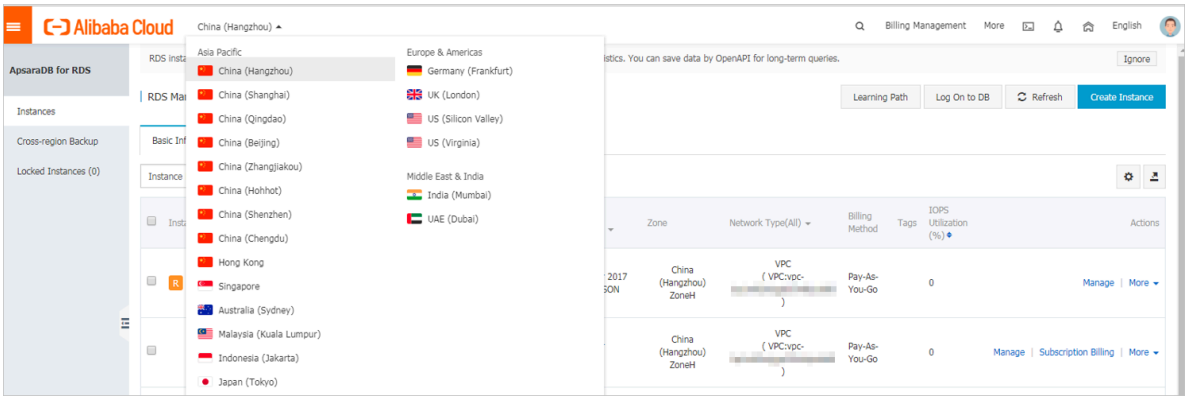
Notes

**For PostgreSQL 11 Cluster Edition (Standard SSD) and PostgreSQL 10 Cluster Edition (Standard SSD) instances, you can only apply for a public endpoint but cannot change or release the public endpoint. For more information, see *Apply for an endpoint*.**

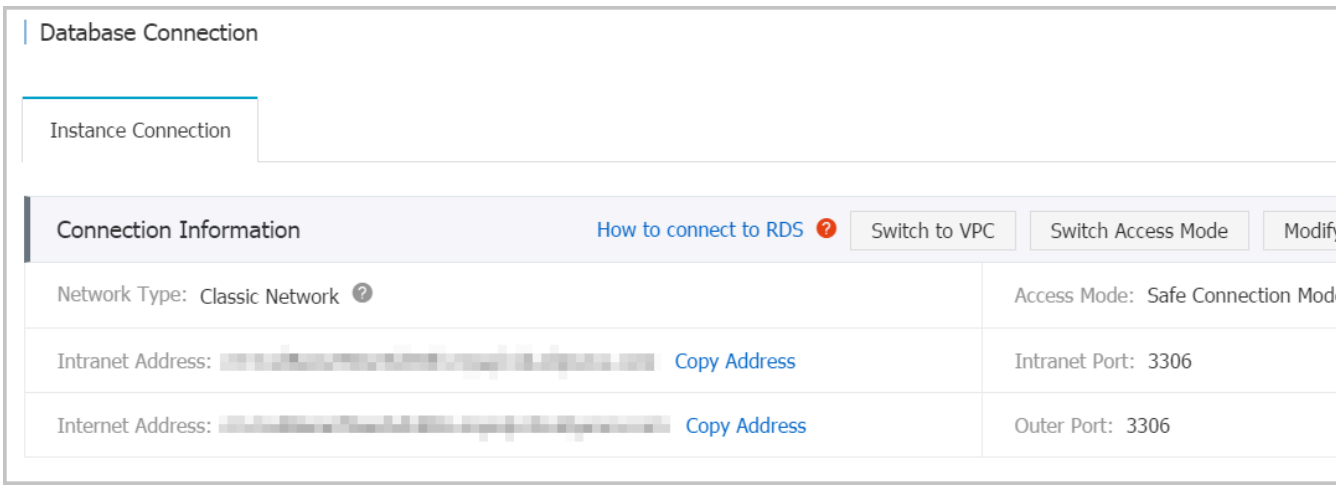
Apply for or release a public endpoint

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, select Database Connections.
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.

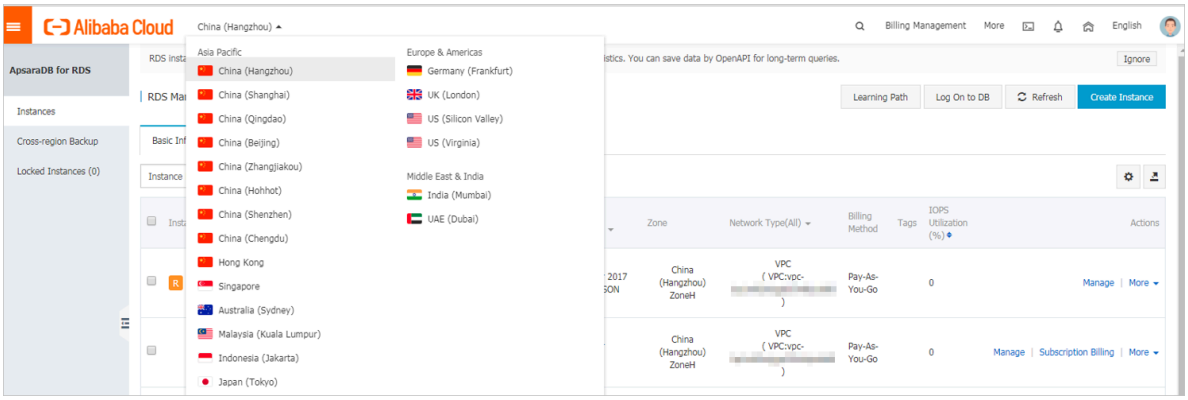




6. In the message box that appears, click OK.

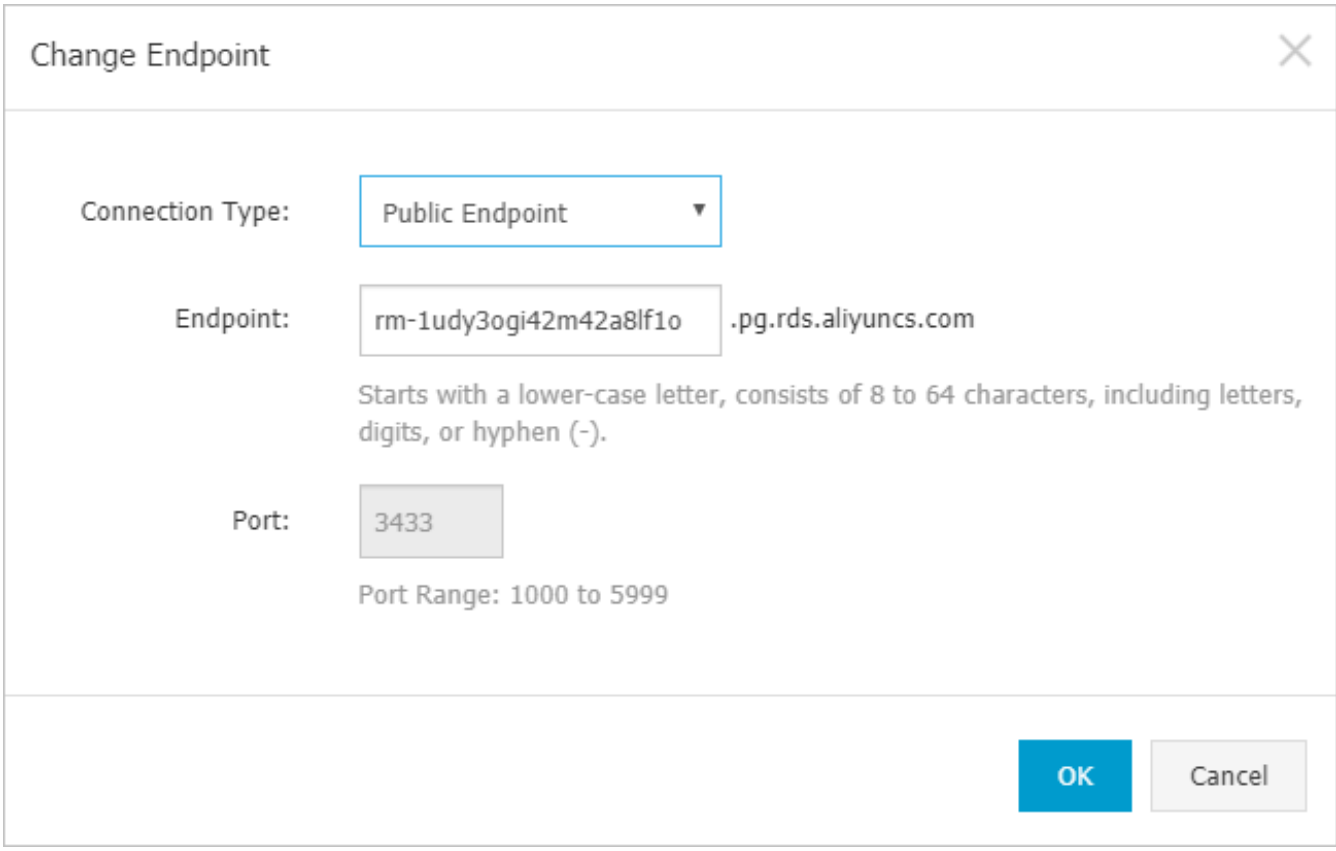
Change a public endpoint

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, select** `Database Connections`.
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_86* | Used to apply for a public endpoint for an RDS instance. |
| *#unique_87* | Used to release the public endpoint of an RDS instance. |

## 10.3 Use DMS to log on to an RDS instance

You can use DMS to log on to an RDS instance. For more information, see *What is DMS ?*. This topic describes how to use DMS to log on to an RDS instance from the RDS console.

Notes

Currently, you can only use an internal endpoint to log on to DMS.

Prerequisites

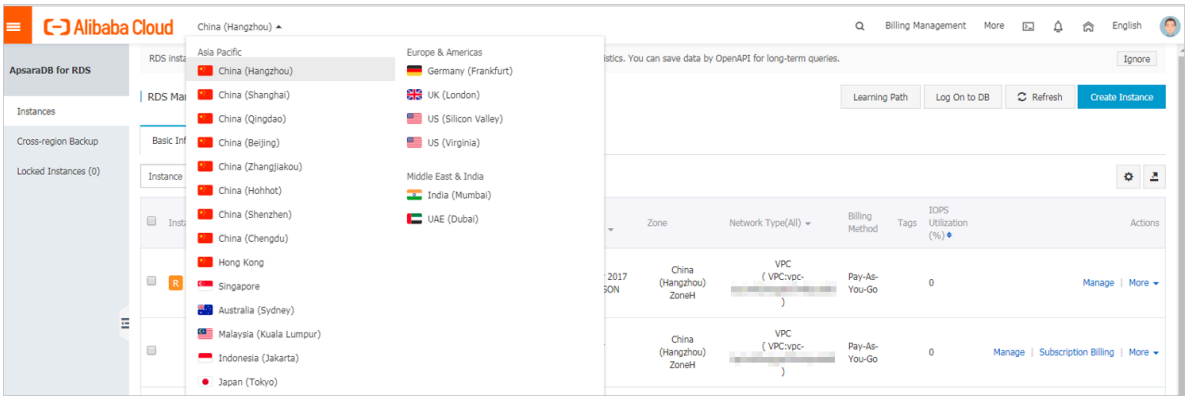
The instance edition must be one of the following editions:

- PostgreSQL 10 Cluster Edition (Local SSD)
- PostgreSQL 10 Basic Edition
- PostgreSQL 9.4

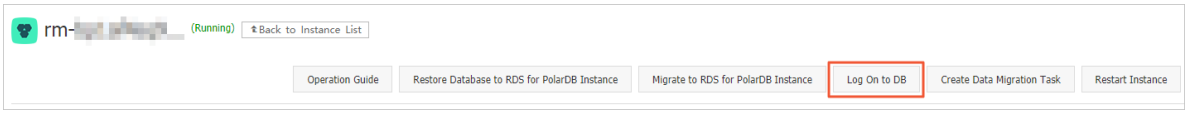
Procedure

1. Log on to the .

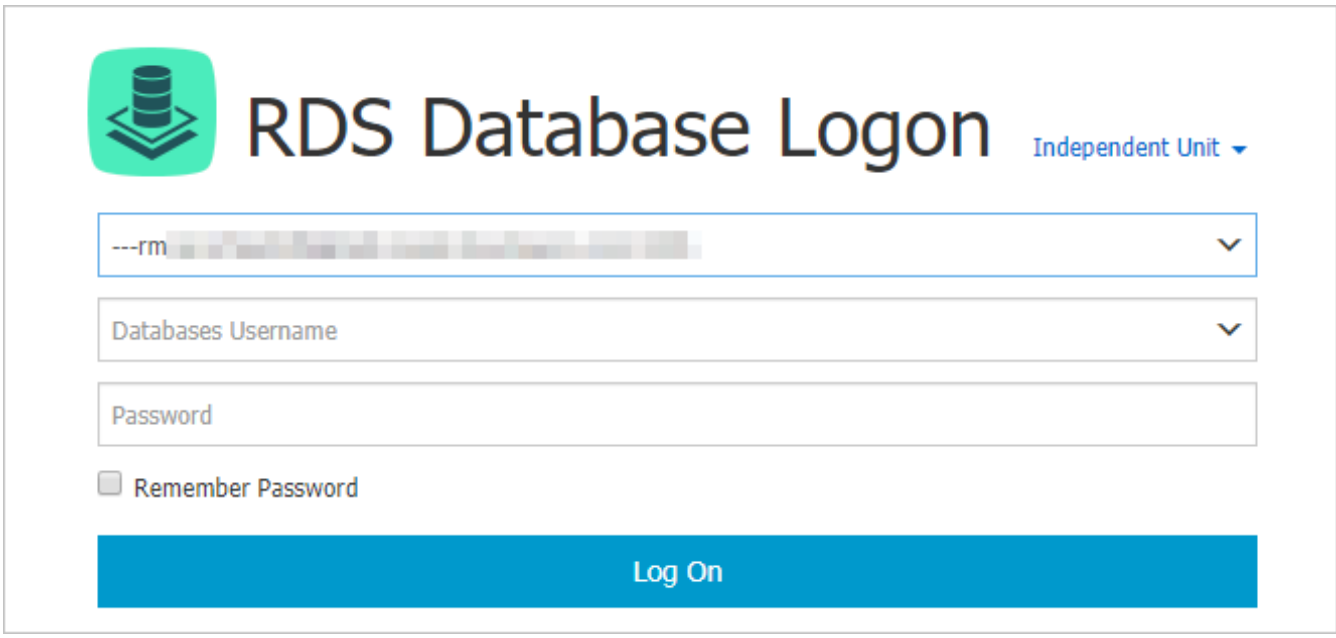
2. In the upper-left corner of the page, select the region where the instance is located.




3. Find the instance and click the instance ID to enter the Basic Information page.
4. Click Log On to DB in the upper-right corner of the page, as shown in the following figure. Enter the Quick Logon page of the *DMS console*.




5. On the Quick Logon page, check the endpoint and port number displayed on the RDS Database Logon page. If the information is correct, enter the username and password of the database, as shown in the following figure.




Configure the following parameters:

- Connection string: the combination of the internal endpoint and port number of an instance, which is in the `<internal endpoint>:<port number>` format.

For information about how to view the internal endpoint and port number of an instance, see *View the internal endpoint and port number*.

- Database username: the account used to access the RDS database.
- Password: the password of the account used to access the RDS database.

6. Click Log On.

> **Note:**
> If you want the Web browser to remember the password, select Remember Password and click Log On.

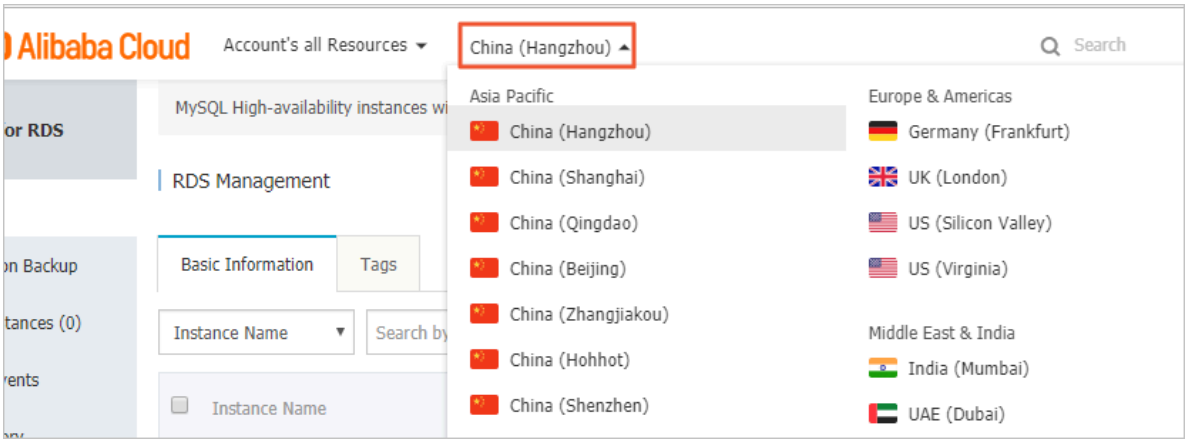
7. If the system prompts you to add the IP CIDR block of the DMS server to the RDS whitelist, click Specify for All Instances or Specify for Current Instance.
8. Click Log On.

## 10.4 View the internal and public endpoints of an instance

When you connect to an RDS instance, you must enter the internal and public endpoints and their corresponding port numbers. This topic describes how to view the internal and public endpoints and their corresponding port numbers in the ApsaraDB for RDS console.

For PostgreSQL 11 Cluster Edition (Standard SSD) and PostgreSQL 10 Cluster Edition (Standard SSD)

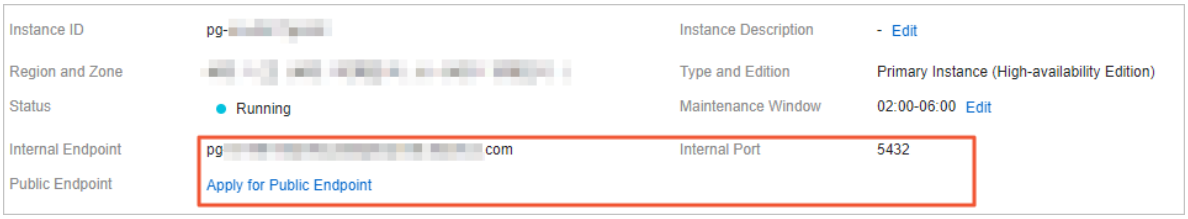
1. Log on to the *ApsaraDB RDS for PostgreSQL console*.
2. In the upper-left corner of the page, select the region where the instance is located.




3. Find the instance and click the instance ID.

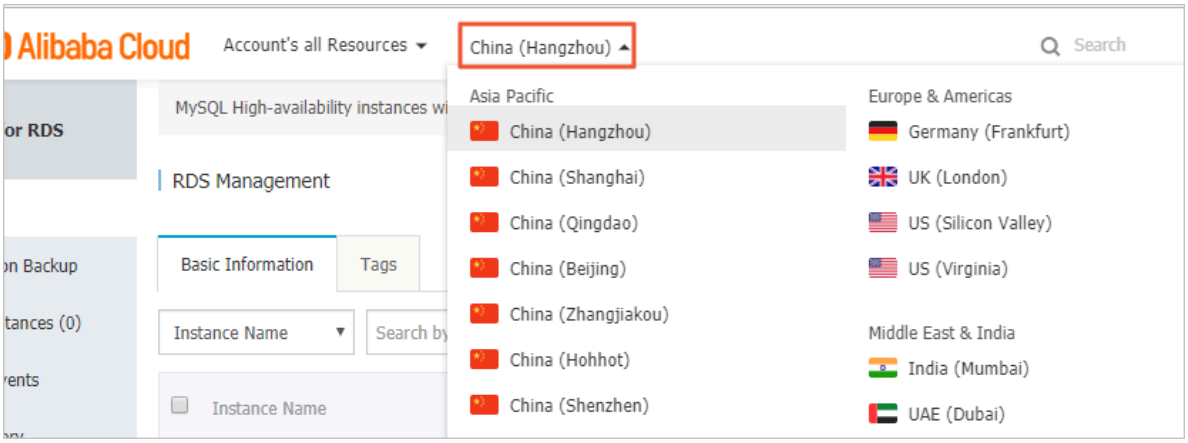
4. **On the Basic Information page that appears, you can view the internal or public endpoints and their corresponding port numbers, as shown in the following figure.**

> **Note:**
>
> - **You must configure the whitelist of the instance to display the endpoint information.**
> - **Only after you have applied for a public endpoint, you can view this information on the Basic Information page.**




For PostgreSQL 10 Cluster Edition (Local SSD), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4

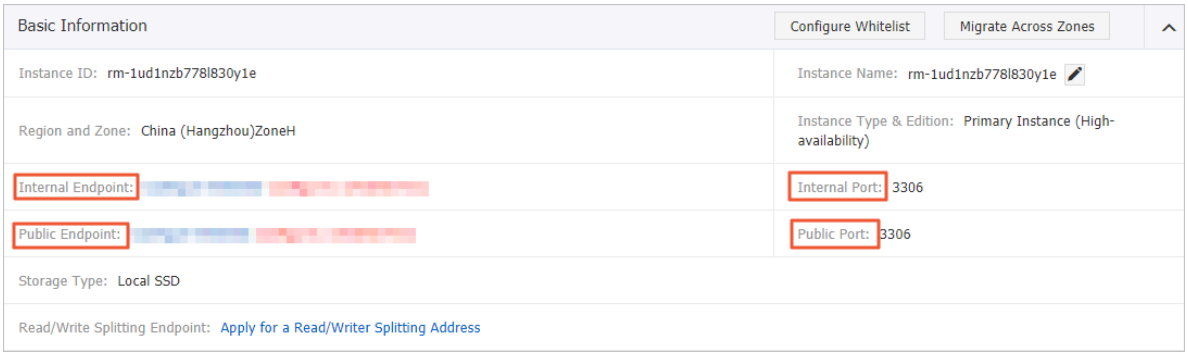
1. **Log on to the *ApsaraDB for RDS console*.**
2. **In the upper-left corner of the page, select the region where the instance is located.**




3. **Find the instance and click the instance ID to enter the Basic Information page.**
4. **On the Basic Information page that appears, you can view the internal and public endpoints and their corresponding port numbers, as shown in the following figure.**

> **Note:**

- **You must configure the whitelist of the instance to display the endpoint information.**
- **Only after you have applied for a public endpoint, you can view this information on the Basic Information page.**




## 10.5 Apply for a public endpoint for an RDS for PostgreSQL instance

**This topic describes how to apply for a public endpoint for an RDS for PostgreSQL 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

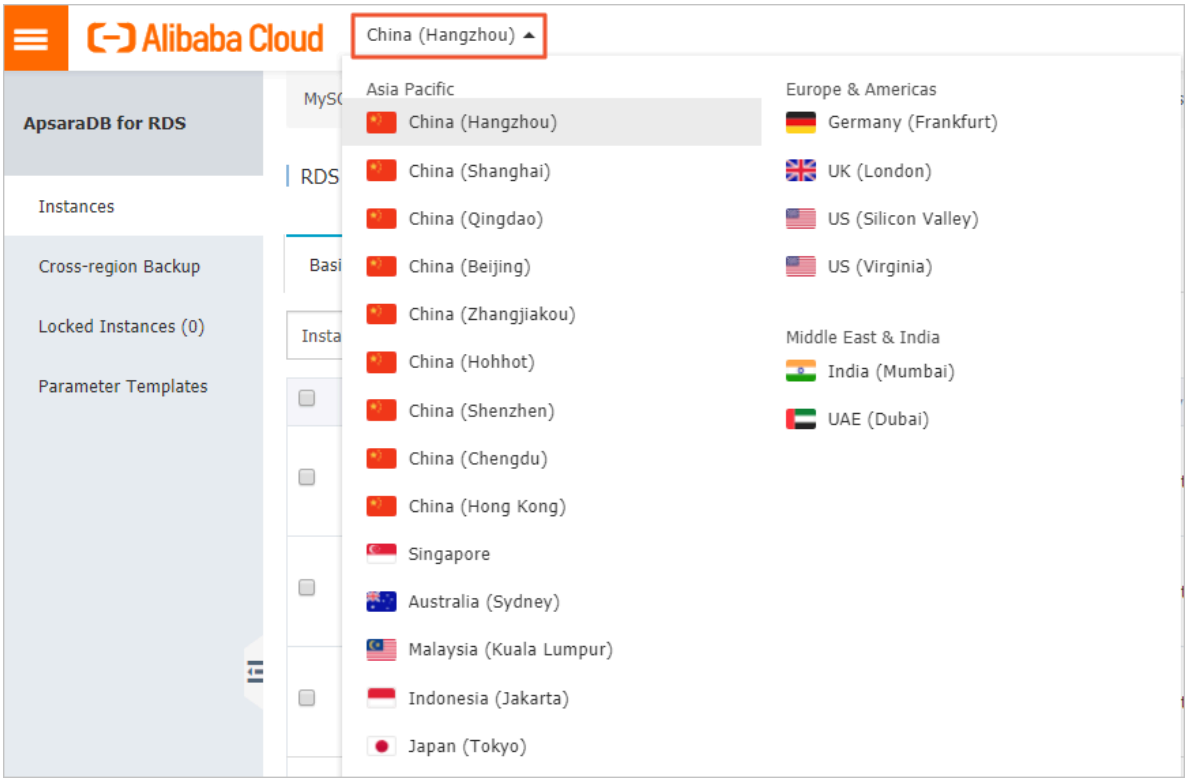
| Endpoint type | Description |
| --- | --- |
| Internal endpoint | · An internal endpoint is generated by default.<br>· If your application is deployed on an ECS instance that is located in the same region as your RDS instance and, at the same time, the ECS instance has the same *network type* as your RDS instance, your RDS instance can communicate with the ECS instance through a private network. In such case, you do not need to apply for a public endpoint.<br>· Accessing your RDS instance through a private network is more secure and helps to maximize RDS performance. |

| Endpoint type | Description |
| --- | --- |
| Public endpoint | · You must manually apply for a public endpoint, which can be released at anytime.<br>· If you cannot access your RDS instance through a private network in one of the following scenarios, you must apply for a public endpoint:<br>- You access your RDS instance from an ECS instance that is located in a different region or has a different *network type* from your RDS instance.<br>- You access your RDS instance from a device outside the Alibaba Cloud.<br>**Note:**<br>· The public endpoint and traffic are currently free of charge.<br>· Using the public endpoint reduces security. Please exercise caution.<br>· To guarantee high security and performance, we recommend that you migrate your application to an ECS instance that is located in the same region and has the same network type as your RDS instance and then use the internal endpoint. |

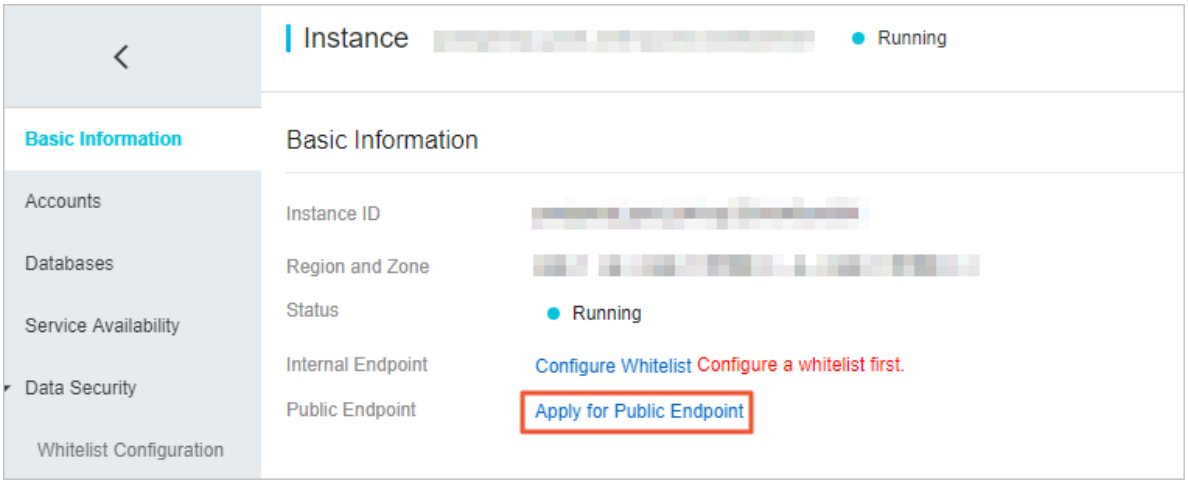
PostgreSQL 11 High-availability Edition (with SSDs) or PostgreSQL 10 High-availability Edition (with SSDs)

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

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



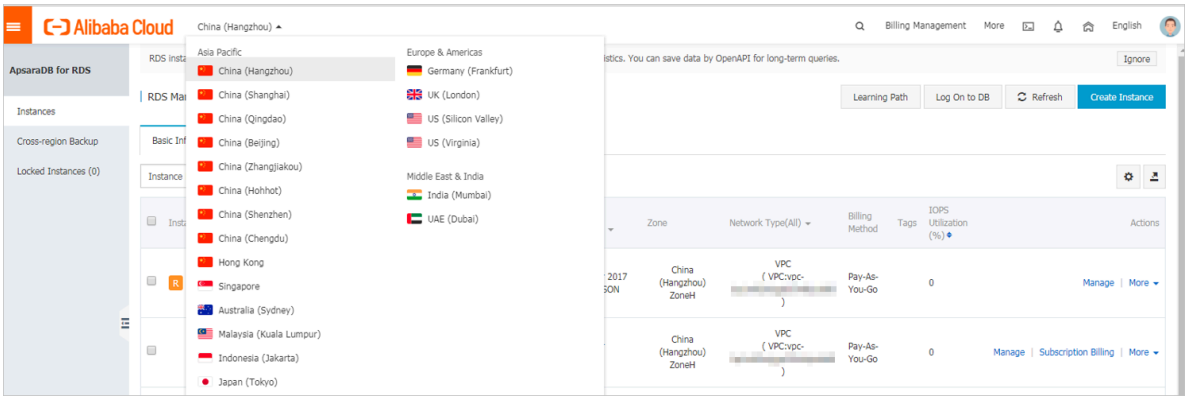

3. **Find the target RDS instance and click the instance ID.**
4. **In the Basic Information section of the Basic Information page, click Apply for Public Endpoint and in the displayed dialog box click OK.**



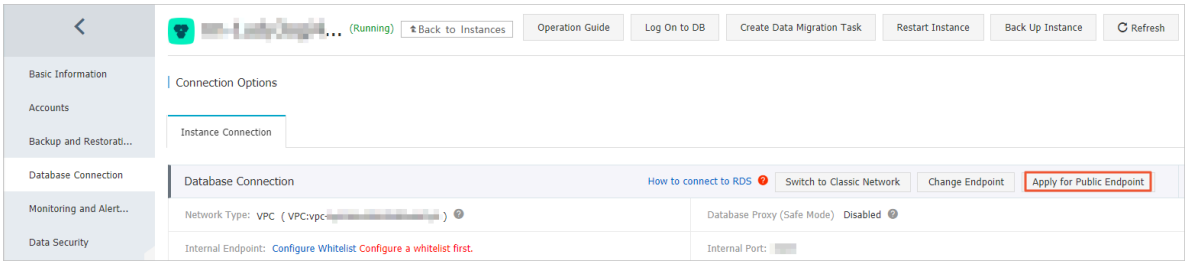

PostgreSQL 10 High-availability Edition (with local SSDs), PostgreSQL 10 Basic Edition, or PostgreSQL 9.4

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 Apply for Public Endpoint.




6. In the displayed dialog box, click OK.

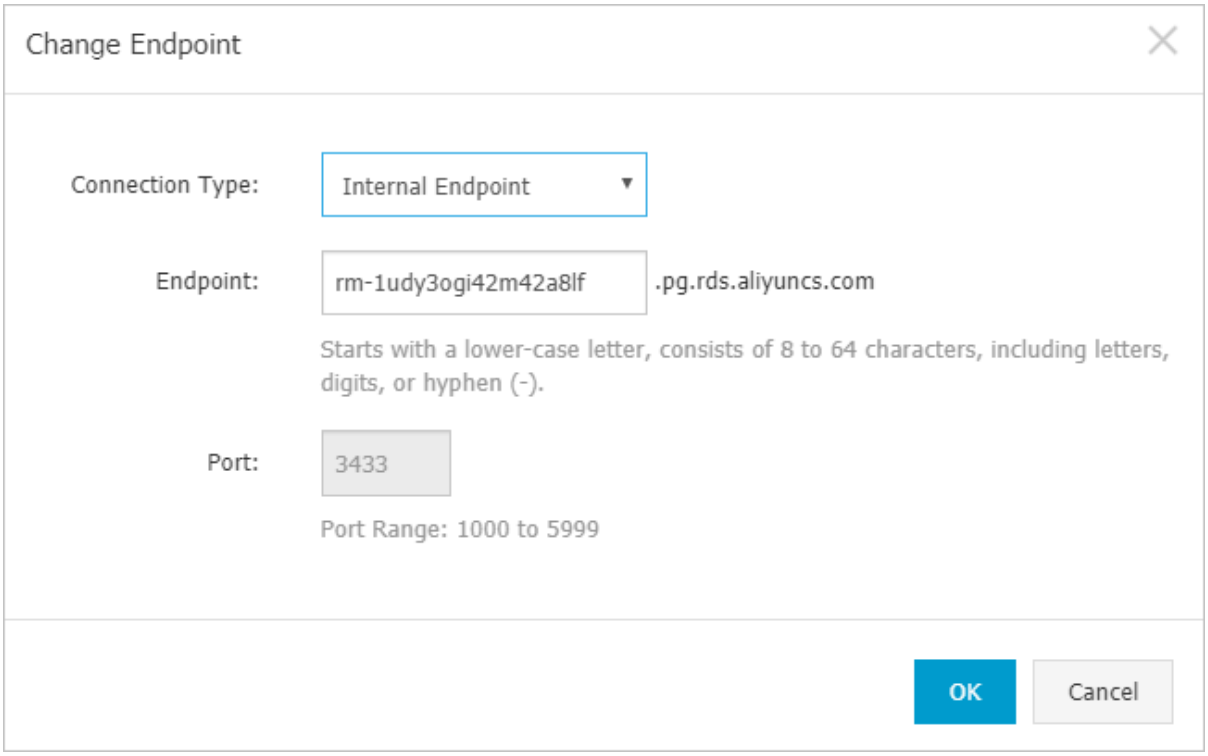
   A public endpoint is generated.

7. Optional. If you want to change the public endpoint or port, click Change Endpoint In the displayed dialog box, select a connection type and click OK.

**Note:**

- The prefix of an endpoint starts with a lowercase letter and contains 8 to 64 characters including letters, digits, and hyphens (-).
- In a VPC, you cannot change the port of an internal or public endpoint.

- **In a classic network, you can change the port of an internal or public endpoint.**




APIs

| API | Description |
| --- | --- |
| *#unique_91* | **Used to apply for an internal endpoint for an RDS instance.** |

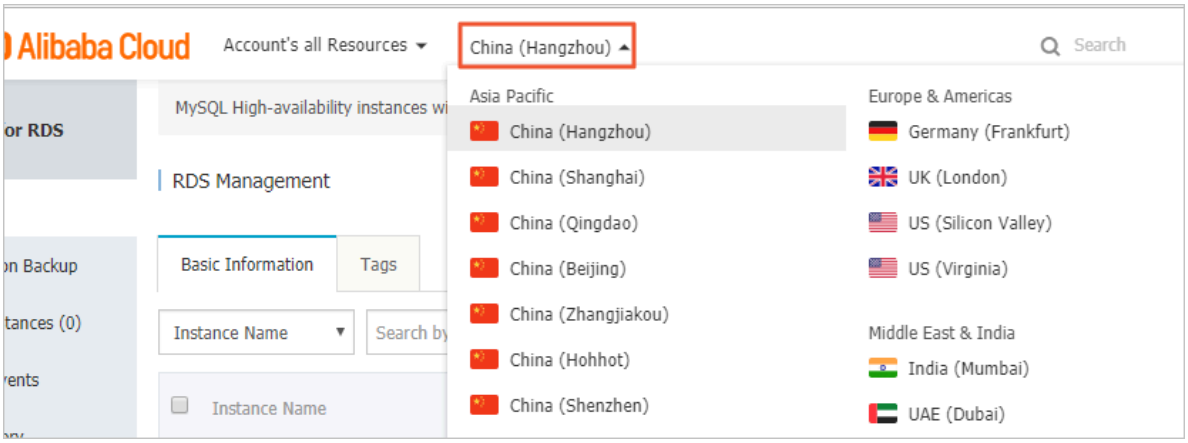
# 11 Monitoring and alerts

## 11.1 View resource monitoring

**ApsaraDB for RDS provides a wide range of performance metrics. You can view resource monitoring in the ApsaraDB for RDS console.**

For PostgreSQL 11 Cluster Edition (Standard SSD) and PostgreSQL 10 Cluster Edition (Standard SSD)

1. **Log on to the *ApsaraDB RDS for PostgreSQL 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, choose Monitoring and Alerts > Basic Monitoring.**
5. **Select the time range to query the corresponding monitoring data. The following table lists the specific monitored metrics.**

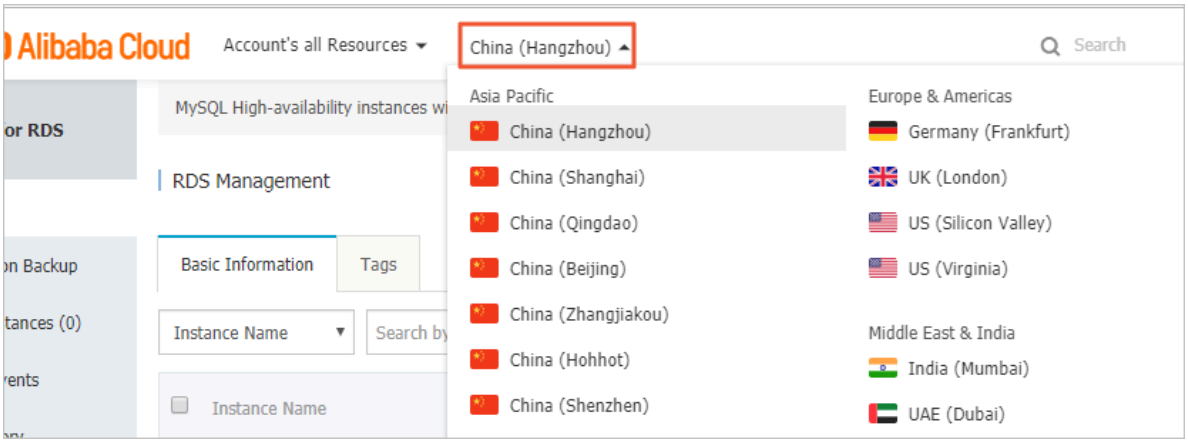
| Monitored metric | Description |
| --- | --- |
| TPS | The number of transactions completed by the instance per second. |
| Operation records | The number of UPDATE, INSERT, DELETE, and other operations of the instance per second. |
| RT | The response time of the instance. Unit: seconds. |
| Connections | Shows the total number of connections, active connections, and idle connections of the instance. |

| Monitored metric | Description |
| --- | --- |
| Longest bloat duration | The time period between the earliest transaction that dead tuples cannot be vacuumed and the monitoring time. |
| Slow queries | The number of SQL statements whose execution time exceed 1 second, 3 seconds, or 5 seconds. |
| Long-running transactions | The number of long-running transactions. It includes the number of transactions whose execution time or idle time exceed 1 second, 3 seconds, or 5 seconds. |
| 2PC | The number of transactions whose execution time exceed 1 second, 3 seconds, or 5 seconds during two-phase commits. |
| Space | The database space and log space of the instance. Unit: MB. |
| Latency | The latency of replication slots and the latency of the secondary database utilization. Unit: Bytes. |
| Data disk IOPS | The number of I/O requests on the data disk per second. |
| Data disk read/write throughput | The throughput of disk reads and writes on the data disk per second. Unit: KB. |
| Data disk usage | The overall usage and iNodes usage of the data disk. |
| Server CPU utilization | The CPU utilization of the instance. |
| Server throughput | The data volume received and sent through the instance NIC per second. Unit: MB. |
| Server memory usage | The memory usage of the instance. |
| Server memory | Shows the memory capacity, used memory size, and free memory size. Unit: MB. |

For PostgreSQL 10 Cluster Edition (Local SSD), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4

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 Monitoring and Alerts.
5. On the Monitoring page, select the time range to query the corresponding monitoring data. The following table lists the specific monitored metrics.

| Monitored metric | Description |
| --- | --- |
| Disk space | The used disk space of the instance. Unit: MB. |
| IOPS | The number of I/O requests of the data disk and log disk per second. |
| Memory usage | The memory usage of the instance. |
| CPU utilization | The CPU utilization of the instance. |
| Total connections | The total number of current connections of the instance. |

## 11.2 Set a monitoring frequency

### Background

Currently, RDS for PostgreSQL provides two monitoring frequencies.

- Every 60 seconds. The monitoring period is 30 days.
- Every 300 seconds. The monitoring period is 30 days.

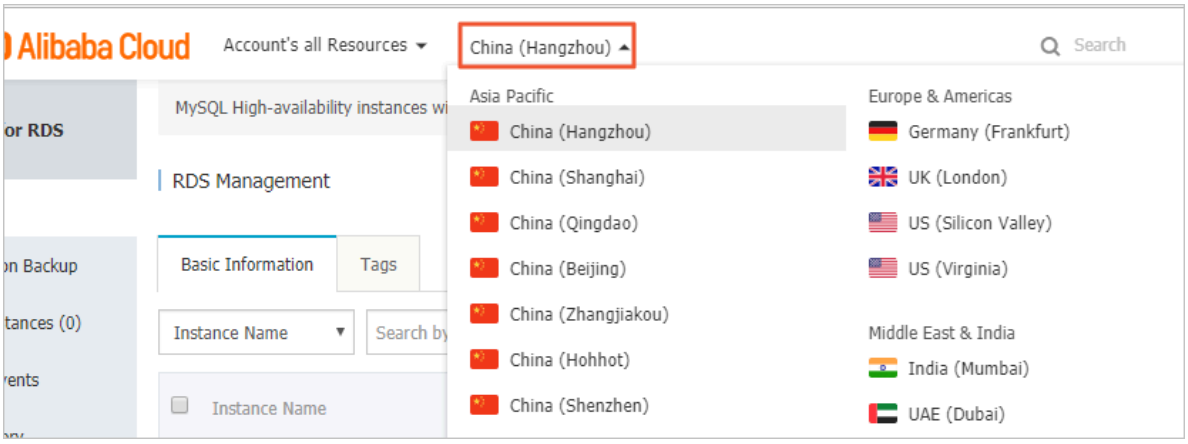
### Prerequisites

The instance editions must be either of the following versions:

- PostgreSQL 10 Cluster Edition (Local SSD)
- PostgreSQL 9.4

Procedure

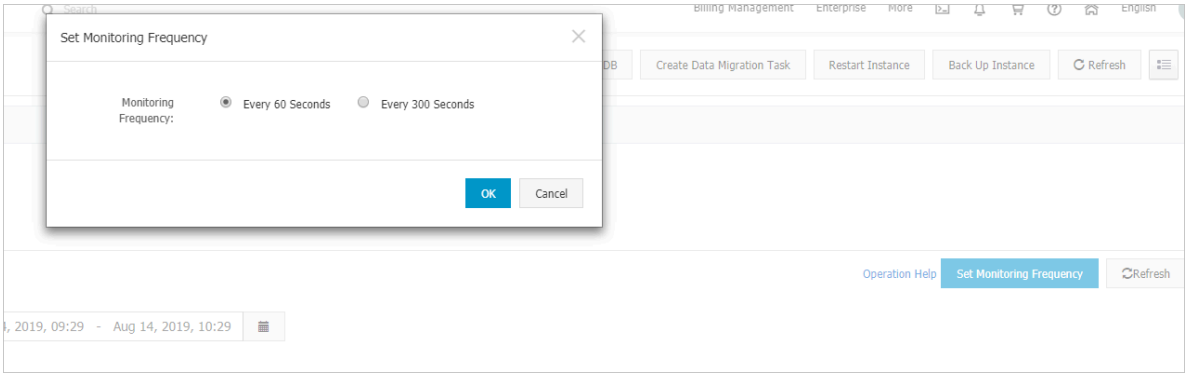
1. **Log on to the *ApsaraDB for RDS console*.**
2. **In the upper-left corner of the page, select the region where the instance is located.**




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

> **Note:**
> **Monitored metrics varies depending on the database engines. For more information, see *View resource monitoring*.**

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




API reference

| Operation | Description |
| --- | --- |
| *DescribeResourceUsage* | You can call this operation to query the resource usage of the instance. |

| Operation | Description |
| --- | --- |
| *DescribeDBInstancePerformance* | You can call this operation to query the instance performance. |
| *DescribeDBInstanceMonitor* | You can call this operation to query the monitoring settings of the instance. |
| *ModifyDBInstanceMonitor* | You can call this operation to change the monitoring settings of an instance. |

## 11.3 Set alert rules

**You can set alert rules for monitoring your system. When the monitored metric meets the conditions, an alert will be triggered and a notification will be sent to the alert contacts.**

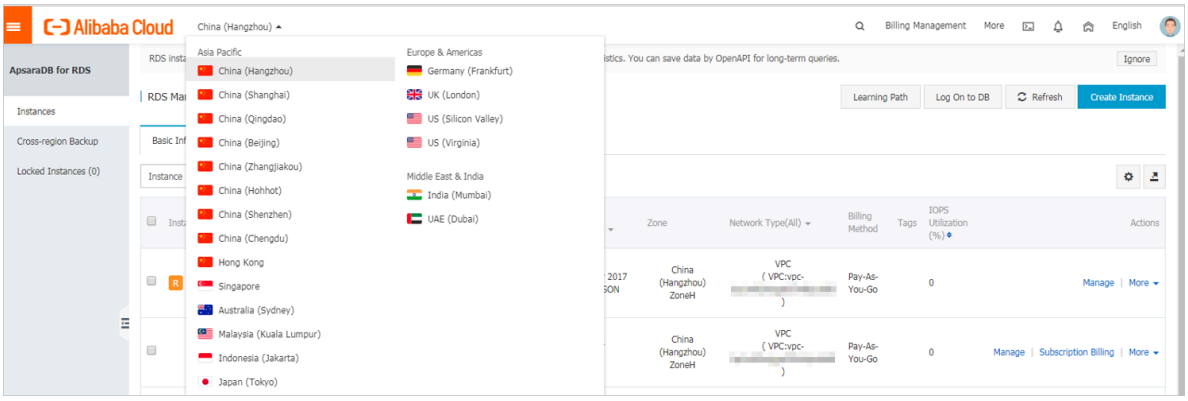
Supported monitored metrics

| ApsaraDB RDS for PostgreSQL edition | Supported monitored metrics |
| --- | --- |
| PostgreSQL 11 Cluster Edition (Standard SSD) and PostgreSQL 10 Cluster Edition (Standard SSD) | IOPS usage |
| | iNode usage |
| | Storage usage |
| | TPS |
| | Connection usage |
| | Average active connections per CPU |
| | Longest bloat duration |
| | CPU utilization |
| | Memory usage |
| PostgreSQL 10 Cluster Edition (Local SSD), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4 | Connection usage |
| | CPU utilization |
| | Latency of read-only instances |
| | Disk usage |
| | IOPS usage |
| | Memory usage |

For PostgreSQL 10 Cluster Edition (Local SSD), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4

### Create alert rules

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 Monitoring and Alerts.
5. Click the Alerts tab.
6. Click Set Alert Rules to open the CloudMonitor console.

> **Note:**
> You can click Refresh to manually refresh the current status of the monitored metrics.

7. Create an alert group. For more information, see *Create alert contacts and alert groups*.
8. Create an alert rule. For more information, see *ApsaraDB for RDS monitoring*.

### Manage alert rules

1. Log on to the *CloudMonitor console for monitoring ApsaraDB for RDS*.
2. Select the region where your instance is located.
3. Find the instance and click the instance ID.

4. On the Alarm Rules tab, find the alert and select one of the following operations:
   - View: views the details of an alert rule.
   - Alarm Logs: views the alert history for a certain period of time.
   - Modify: modifies alert rules. For more information about the parameters, see *Parameter description*.
   - Disable: disables the selected alert rules. If an alert rule is disabled, no alert is triggered even though the monitored metric meets the conditions.
   - Delete: deletes the selected alert rules. An alert rule cannot be restored after you delete the rule. You can only add it again.

# 12 Data security

## 12.1 Switch from standard IP whitelist to enhanced whitelist

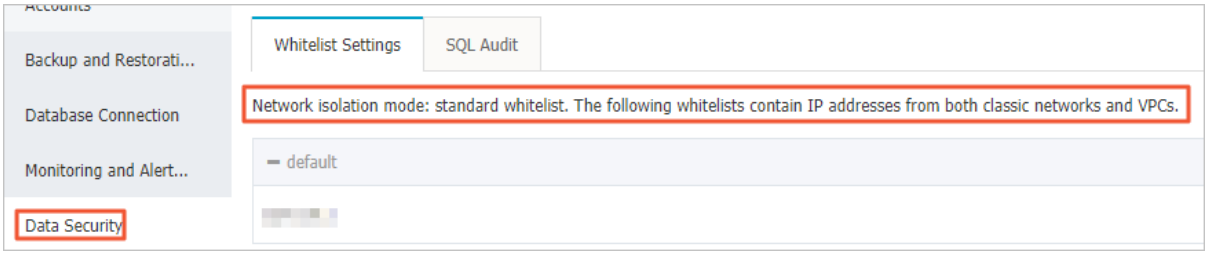
**This topic describes how to switch from the standard whitelist mode the enhanced whitelist mode for an RDS for PPAS instance.**

IP whitelist modes

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

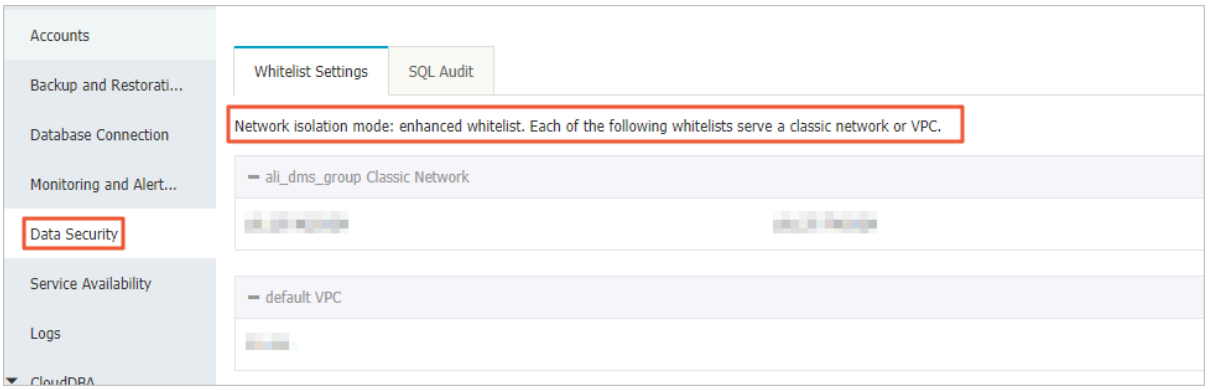
- **Standard whitelist mode**

  **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

- **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 enhanced whitelist mode does not affect the ECS instances that are in the *security group*.**

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.**

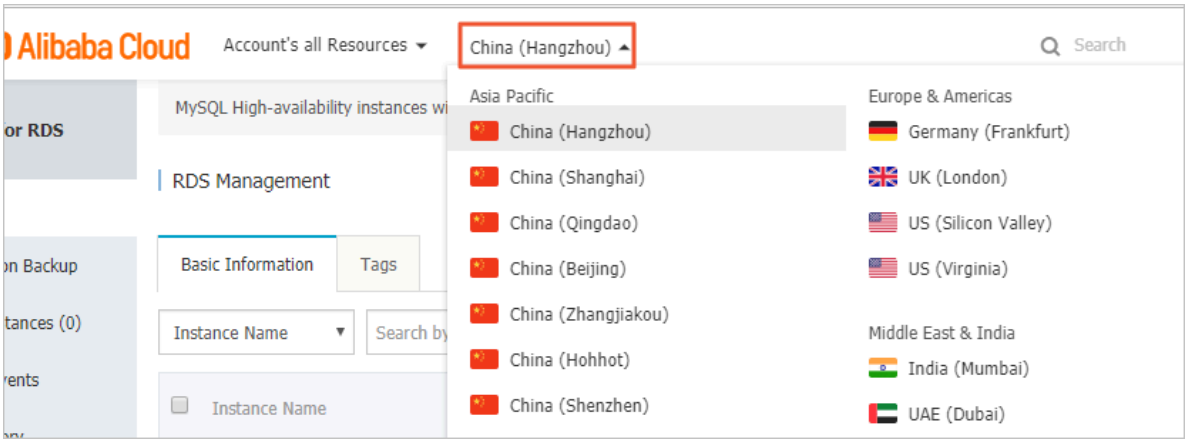
Prerequisites

**The instance edition must be ApsaraDB RDS for PostgreSQL 10 Cluster Edition ( Local SSD).**

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 Data Security.
5. On the Whitelist Settings tab, click Switch to Enhanced Whitelist (Recommended).


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

## 12.2 Configure a whitelist for an RDS for PostgreSQL instance

After you create an RDS instance, you must configure a whitelist to allow other instances, hosts, or applications to access the instance. The default whitelist contains only the IP address 127.0.0.1, which indicates that no other IP addresses are allowed to access the RDS instance.

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

- Configure a whitelist: adds IP addresses to the whitelist to allow them to access the RDS instance.

- **Configure a security group: adds a security group for the RDS instance to allow ECS instances in the group to access the RDS instance.**

  **Note:**
  **Only instances of PostgreSQL 10 Cluster Edition (Local SSD), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4 support security groups.**

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

**This topic describes how to configure a whitelist and avoid common configuration errors:**

- *Configure a whitelist for instances of PostgreSQL 11 Cluster Edition (Standard SSD) or PostgreSQL 10 Cluster Edition (Standard SSD)*
- *Configure a whitelist for instances of PostgreSQL 10 Cluster Edition (Local SSD), PostgreSQL 10 Basic Edition, or PostgreSQL 9.4*
- *Common whitelist configuration errors*
- *Configure a security group*

For PostgreSQL 11 Cluster Edition (Standard SSD) and PostgreSQL 10 Cluster Edition (Standard SSD)

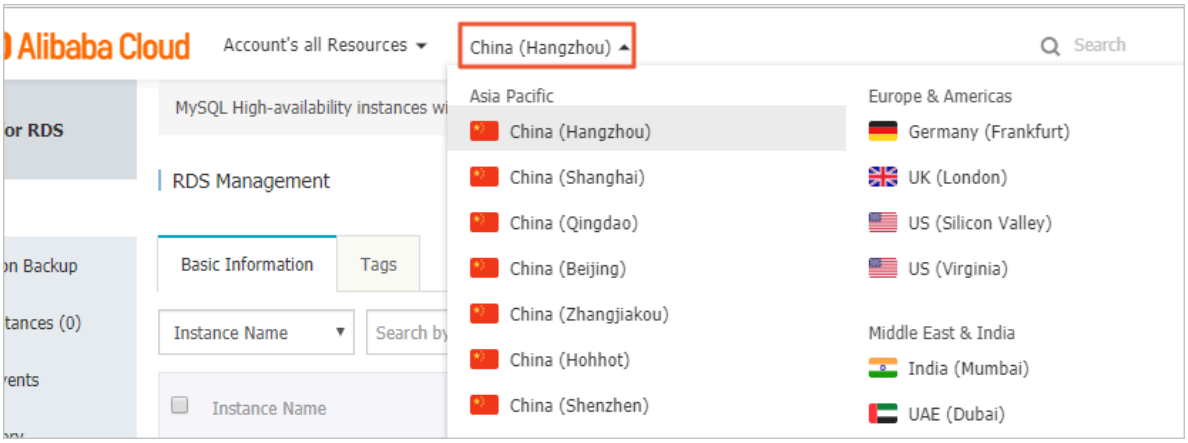
**Notes**

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

**Procedure**

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

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



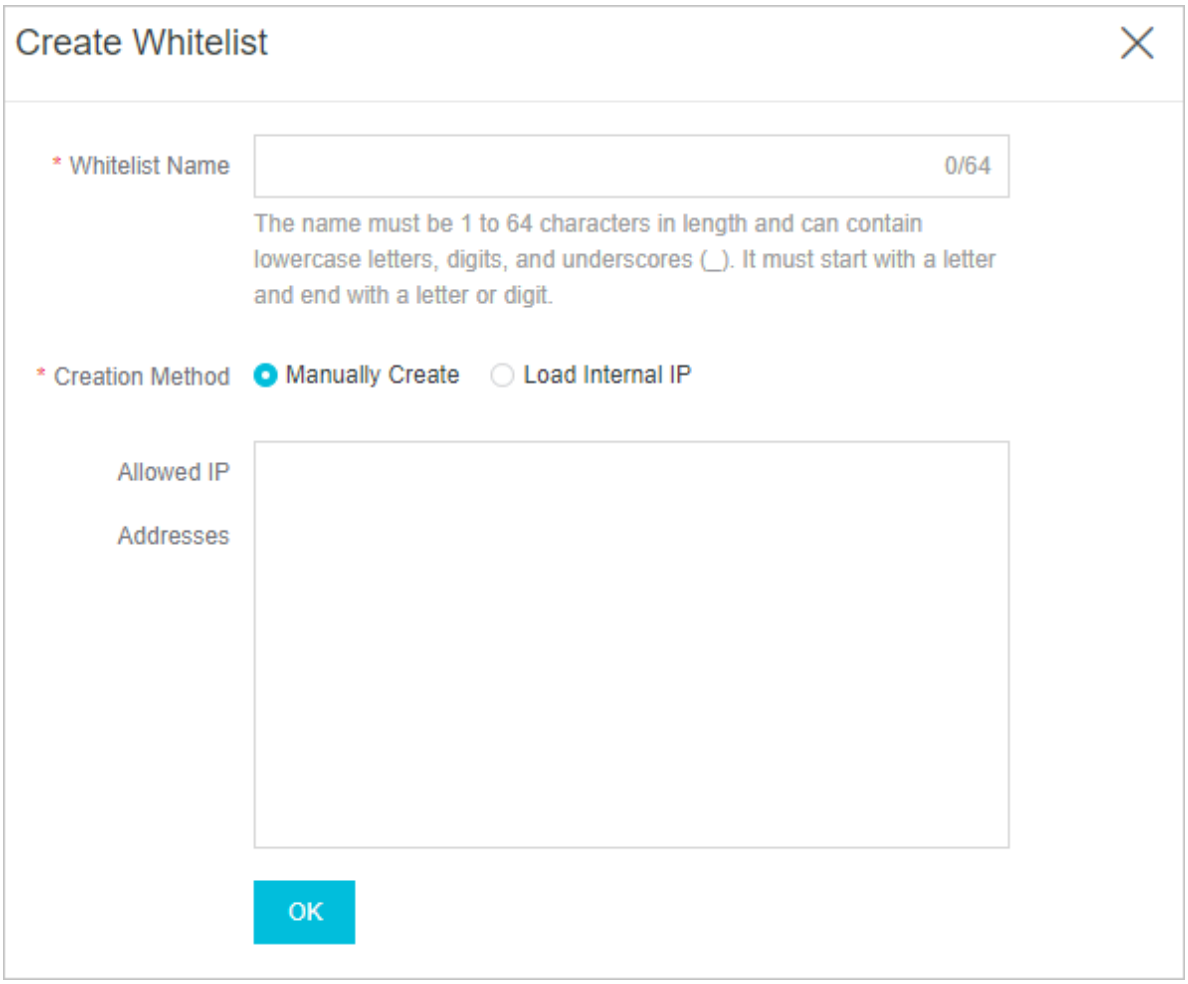

3. Find the instance and click the instance ID.
4. In the left-side navigation pane, choose Data Security > Whitelist Configurations.
5. On the Whitelist Configurations page, click the More icon in the Actions column of the default whitelist and choose Edit, as shown in the following figure.

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


6. In the Edit Whitelist dialog box that appears, specify the IP addresses or CIDR blocks used to access the instance, and then click OK. The following section describes the rules:
   - 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.
   - If you want 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 select Load Internal IP, the IP addresses of all the ECS instances under your Alibaba Cloud account are displayed. You can select the required IP addresses to add into the whitelist.

> **Note:**

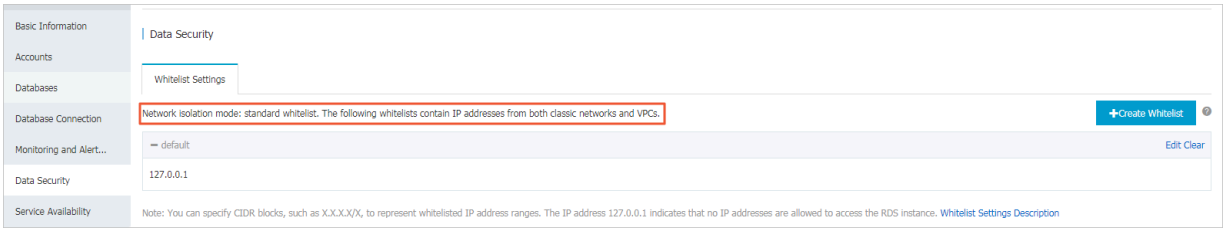
**If you add a new IP address or CIDR block to the default whitelist, the IP address 127.0.0.1 is deleted by default.**




For PostgreSQL 10 Cluster Edition (Local SSD), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4

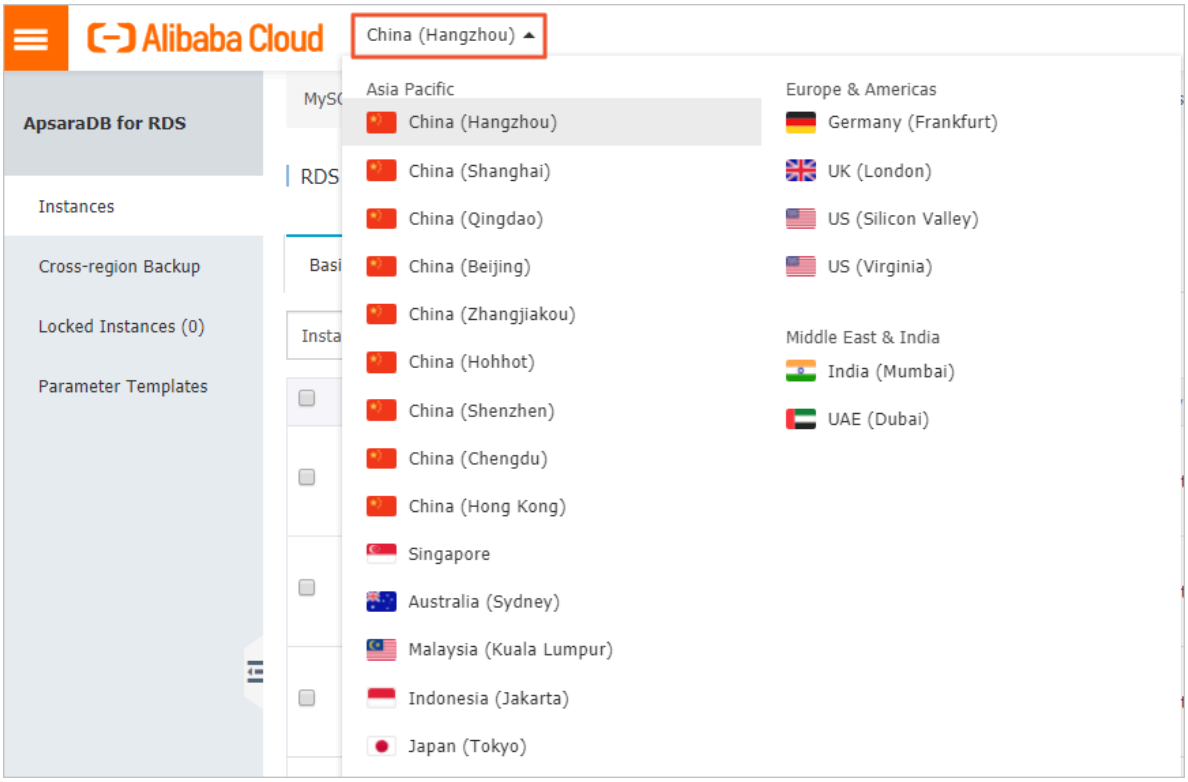
**Notes**

- **The default whitelist can only be edited or cleared, but cannot be deleted.**
- **If you log on to DMS without adding your IP address to the whitelist, DMS will prompt you to add the address. By default, DMS will also create a whitelist that contains your IP address.**
- **You must check your instance to verify its network isolation mode before configuring whitelists. Refer to the corresponding procedures based on the network isolation mode.**




### Configure a whitelist in the enhanced whitelist mode

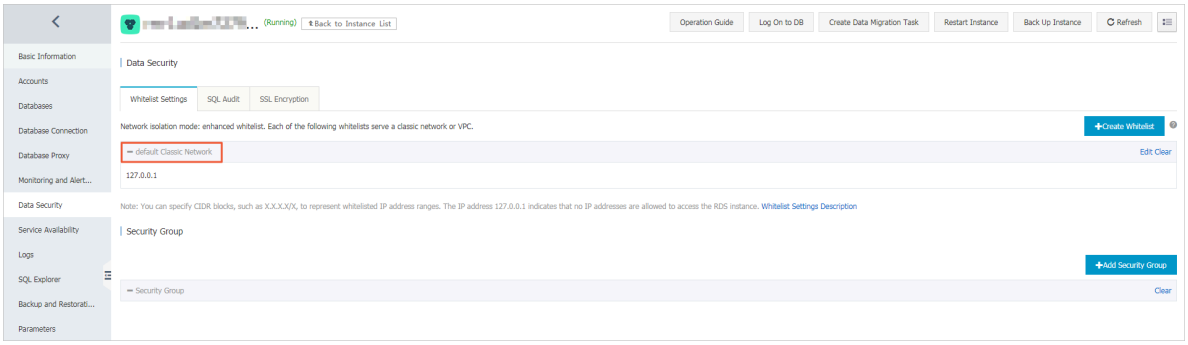
1. **Log on to the *ApsaraDB for RDS console*.**
2. **In the upper-left corner of the page, select the region where the instance is located.**




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

5. On the Whitelist Settings tab, select the whitelist group to be modified as required. The following section describes the detailed steps:
   - If you want to access an RDS instance from an ECS instance located in the same VPC, click Edit corresponding to the default `VPC whitelist group`.
   - If you want to access an RDS instance from an ECS instance located in the classic network, click Edit corresponding to the default `classic-network whitelist group`.
   - If you want to access an RDS instance from an instance or host located in a public network, click Edit corresponding to the default `classic-network whitelist group`.

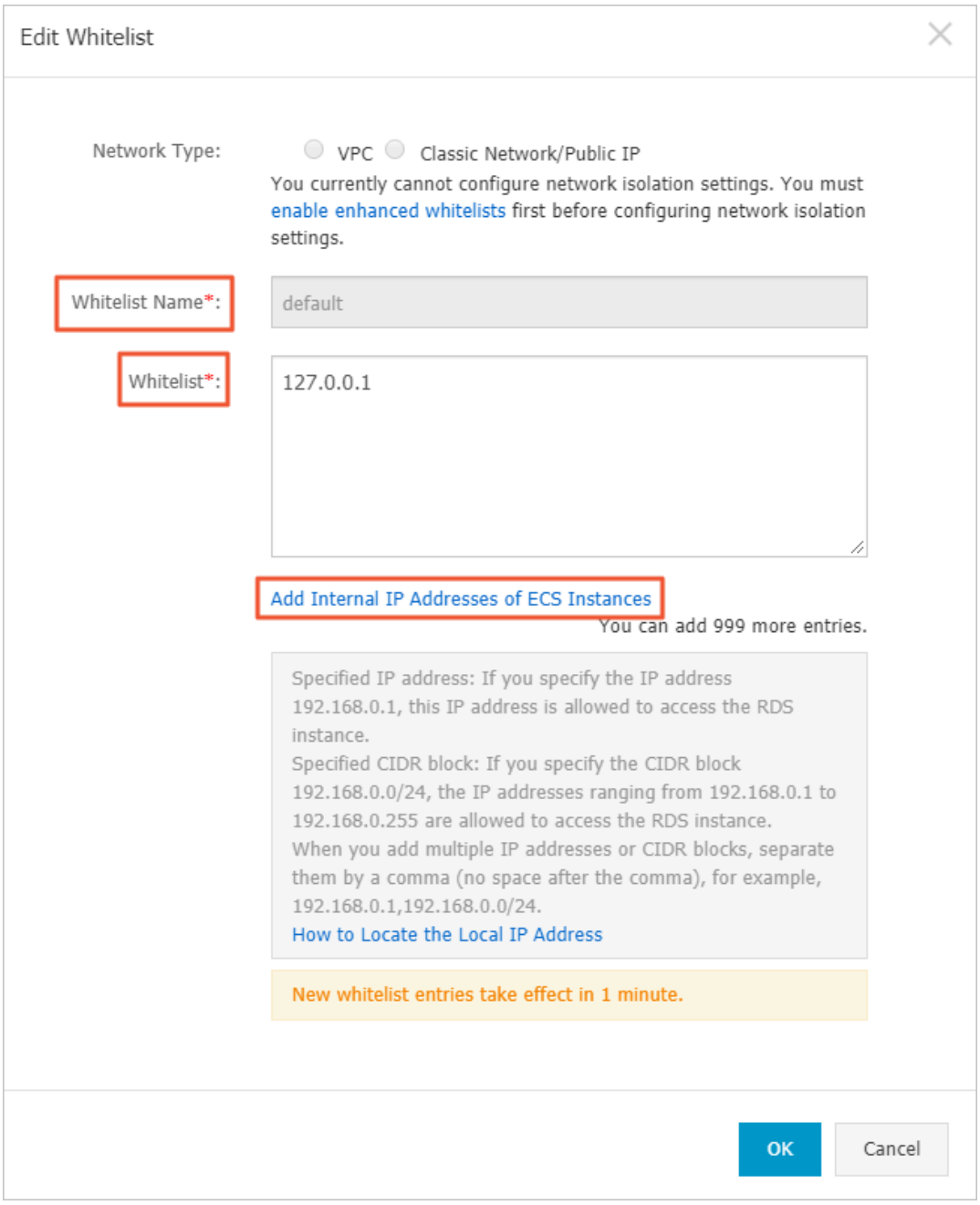
> **Note:**
>
> - If an ECS instance connects to an RDS instance by using the internal endpoint of a VPC or classic network, you must make sure that the two instances are in the same region. The two instances must also have the same *network type*. Otherwise, the connection fails.
> - You can also click Create Whitelist to create a new whitelist. In the Create Whitelist dialog box that appears, select VPC or Classic Network/Public IP.



6. **In the dialog box that appears, specify the IP addresses or CIDR blocks used to access the instance, and then click OK. The following section describes the rules:**
   - **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.**
   - **If you want 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 select Load Internal IP, the IP addresses of all the ECS instances under your Alibaba Cloud account are displayed. You can select the required IP addresses to add into the whitelist.**

**Note:**

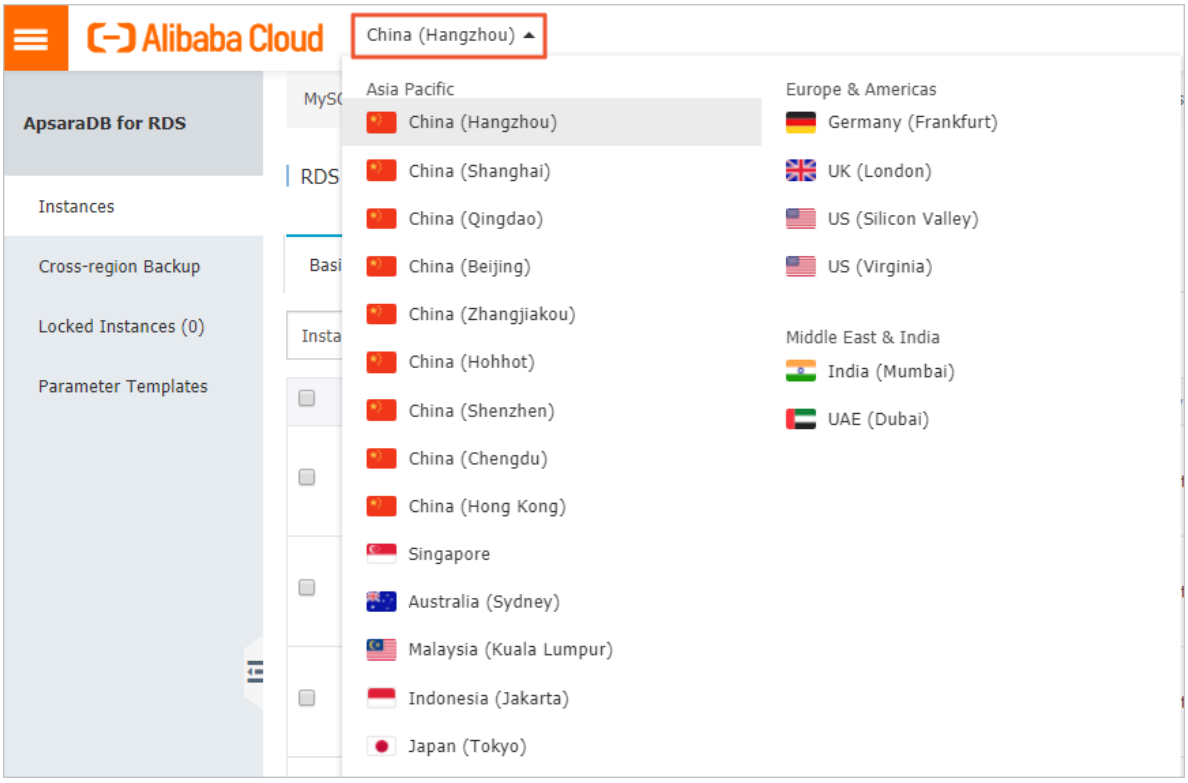
**If you add a new IP address or CIDR block to the default whitelist, the IP address 127.0.0.1 is deleted by default.**




### Configure a whitelist in the standard whitelist mode

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 Data Security.
5. On the Whitelist Settings tab, click Edit corresponding to the default whitelist, as shown in the following figure.

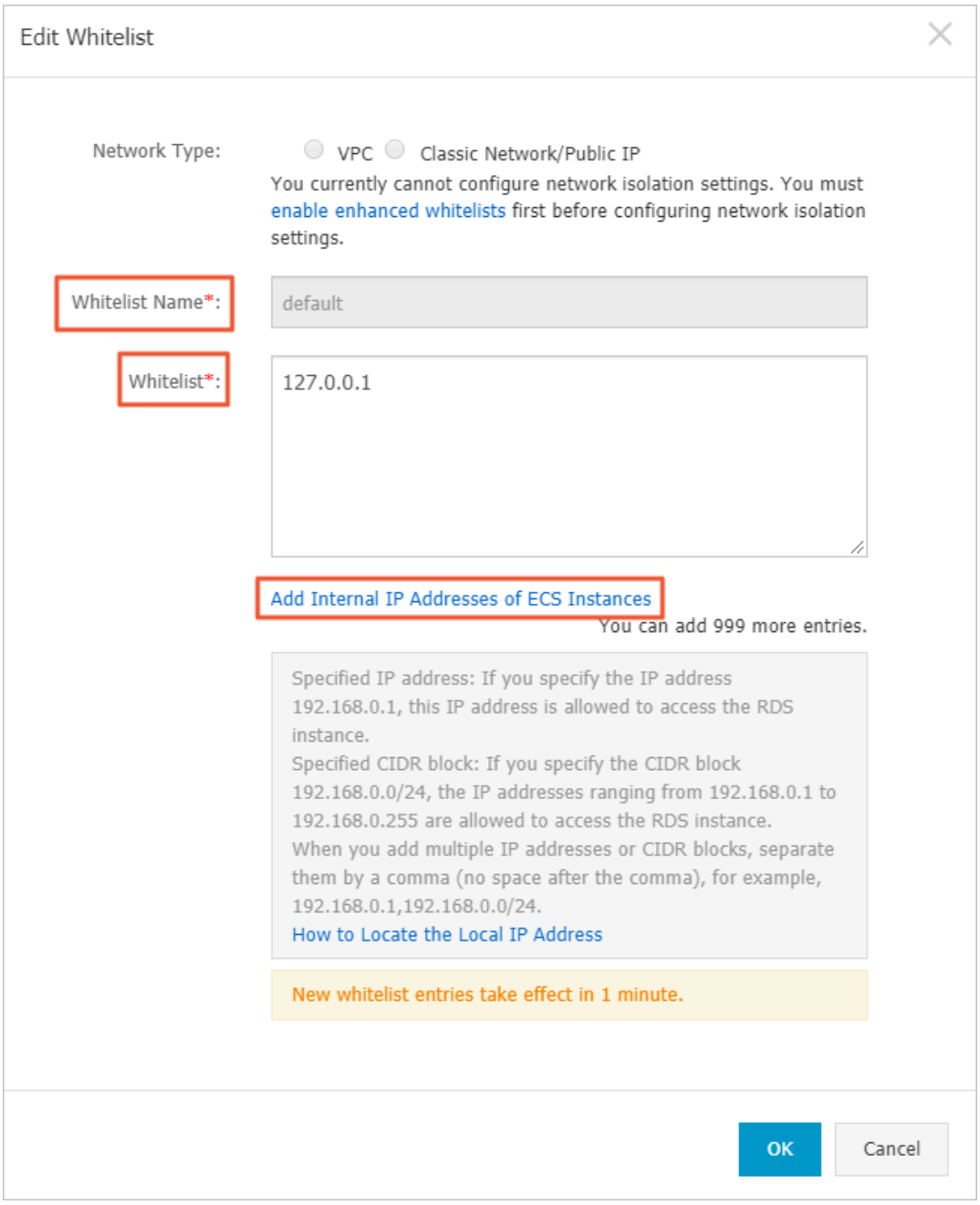
**Note:**

You can also click Create Whitelist to create a new whitelist.

6. **In the Edit Whitelist dialog box that appears, enter the IP addresses or CIDR blocks used to access the instance, and then click OK. The following section describes the rules:**
   - **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.**
   - **If you want 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 select Load Internal IP, the IP addresses of all the ECS instances under your Alibaba Cloud account are displayed. You can select the required IP addresses to add into the whitelist.**

**Note:**

**If you add a new IP address or CIDR block to the default whitelist, the default address 127.0.0.1 is deleted by default.**




Common whitelist configuration errors

- **The default whitelist contains only the IP address 127.0.0.1, which indicates that no other IP addresses are allowed to access the RDS instance. Therefore, you must add the IP addresses of the instances, hosts, or applications into the whitelist to access the RDS instance.**

- **The IP address in the whitelist is set to 0.0.0.0, while the correct setting is 0.0.0.0/0.**

  **Note:**
  **0.0.0.0/0 indicates that all IP addresses are allowed to access the RDS instance. Use caution when adding this IP CIDR block.**

- **The instance has enabled the *enhanced whitelist mode*, but the IP addresses are added into the incorrect group. To avoid this issue, check the IP addresses as follows:**
  - **If the network type is VPC, the internal IP address of the ECS instance is added to the default VPC whitelist group.**
  - **If the network type is a classic network, the internal IP address of the ECS instance is added to the default classic-network whitelist group.**
  - **If you connect to an RDS internal endpoint through *ClassicLink*, make sure that the internal IP address of the ECS instance is added to the default VPC whitelist group.**
  - **If you connect to an RDS instance through a public network, the public IP address of the instance or host must be added to the default classic-network whitelist group.**
- **The public IP address of the specified instance, host, or application is invalid. The IP address you entered may not be the actual public IP address of the instance, host, or application. The reasons are as follows:**
  - **The public IP address may be a dynamic IP address.**
  - **The tools or websites used to query the public IP addresses provide the incorrect IP addresses.**

  **For more information about how to fix this issue, see *Locate the public IP address for ApsaraDB RDS for PostgreSQL and ApsaraDB RDS for PPAS instances*.**

Configure a security group

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

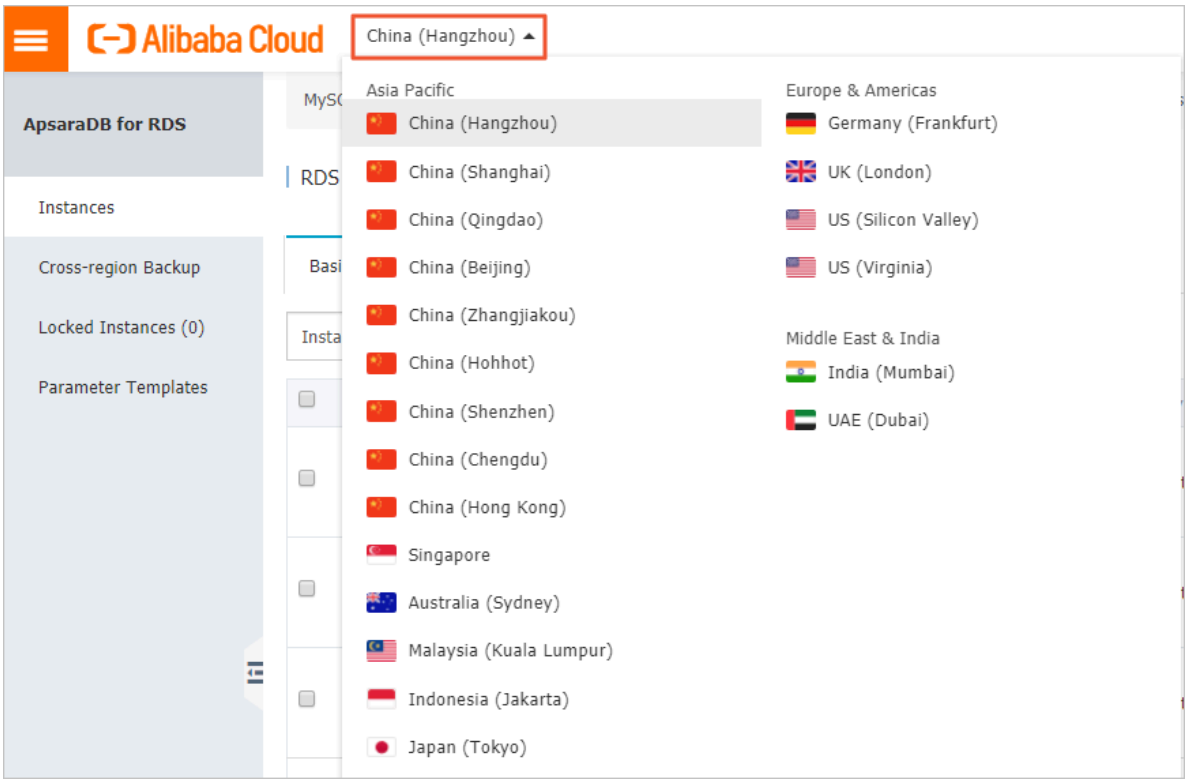
**For more information about security groups, see *Create a security group*.**

### Notes

- Security groups are available in the following three editions: PostgreSQL 10 Cluster Edition (Local SSD), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4.
- Security groups are available in the following regions: China (Hangzhou), China ( Qingdao), and Hong Kong.
- You can configure both the IP whitelist and the ECS security group. Both the IP addresses in the whitelists and the ECS instances in the security group can all access the RDS instance.
- You can only add one security group to an RDS instance.
- Changes to the security group are automatically synchronized to the whitelist.

### 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 Data Security.
5. On the Whitelist Settings tab, click Add Security Group.

**Note:**

**Security groups with a VPC tag are security groups that contain ECS instances within VPCs.**

6. **Select the security group to be added and click OK.**

API reference

| Operation | Description |
| --- | --- |
| *#unique_25* | You can call this operation to query the IP whitelist of an RDS instance. |
| *#unique_26* | You can call this operation to modify the IP whitelist of an RDS instance. |

# 13 SQL audit and event history

## 13.1 SQL audit (database engine)

**This topic describes the SQL audit function. You can use this function to audit SQL executions and check the details. Enabling SQL audit does not affect the instance performance.**

> **Note:**
> **You cannot view the records that are generated before enabling SQL audit.**

Precautions

- **Enabling SQL audit does not affect the instance performance.**
- **SQL audit records are retained for 30 days.**
- **Files exported from SQL audit can be retained for two days. The system will clean the files that are older than two days.**
- **The SQL audit is disabled by default. When this feature is enabled, the instance will incur additional fees. For more information, see *ApsaraDB for RDS pricing*.**

Prerequisites

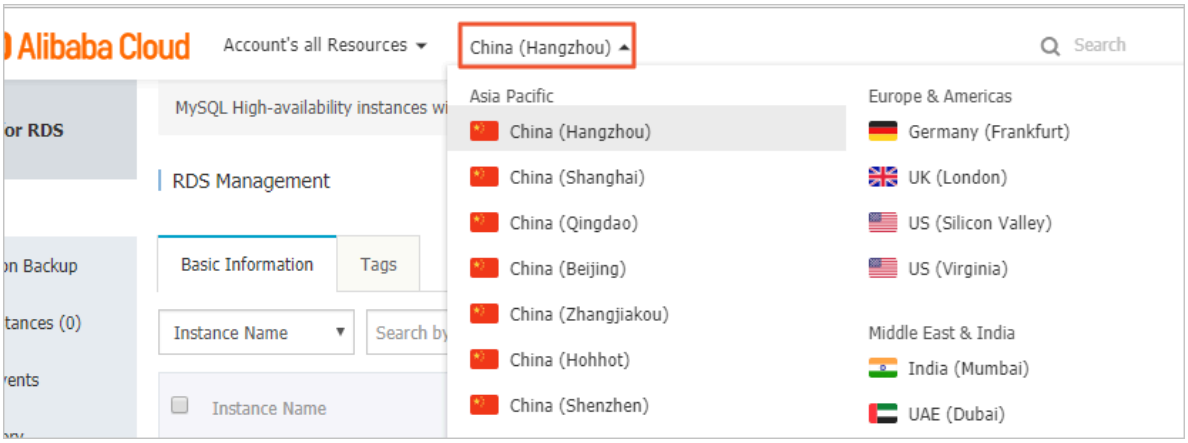
**The instance edition must be either of the following editions:**

- **PostgreSQL 10 Cluster Edition (Local SSD)**
- **PostgreSQL 9.4**

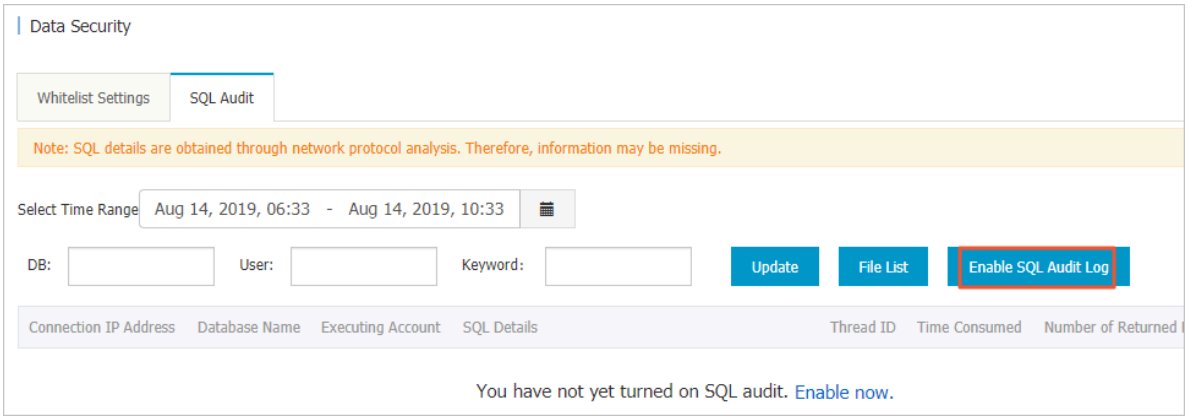
Enable SQL audit

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 Data Security.
5. Select the SQL Audit tab, and click Enable SQL Audit Log.




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

   After enabling SQL audit, you can query SQL information based on criteria such as time, database, user, and other key words.

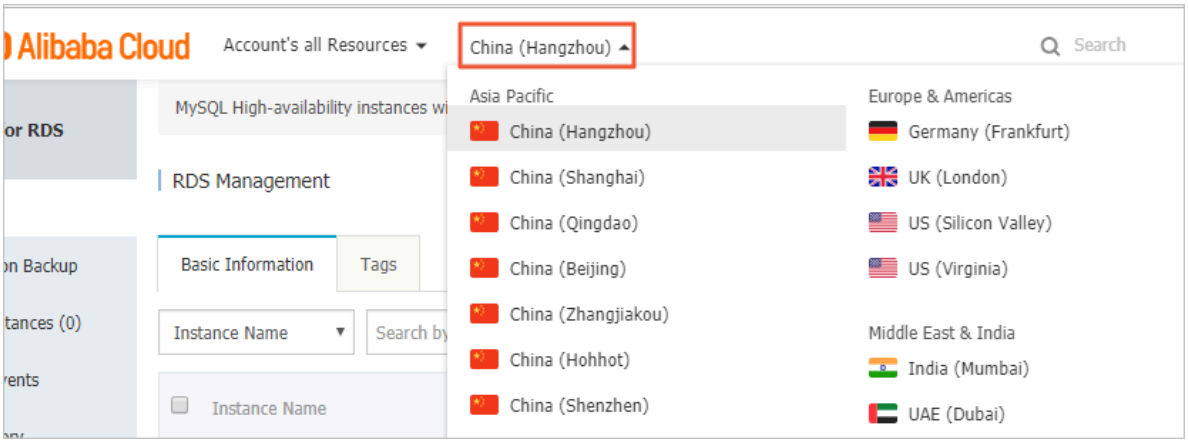
## Disable SQL audit

You can disable the SQL audit feature when you do not need to audit SQL to save costs. To disable SQL audit, follow these steps:

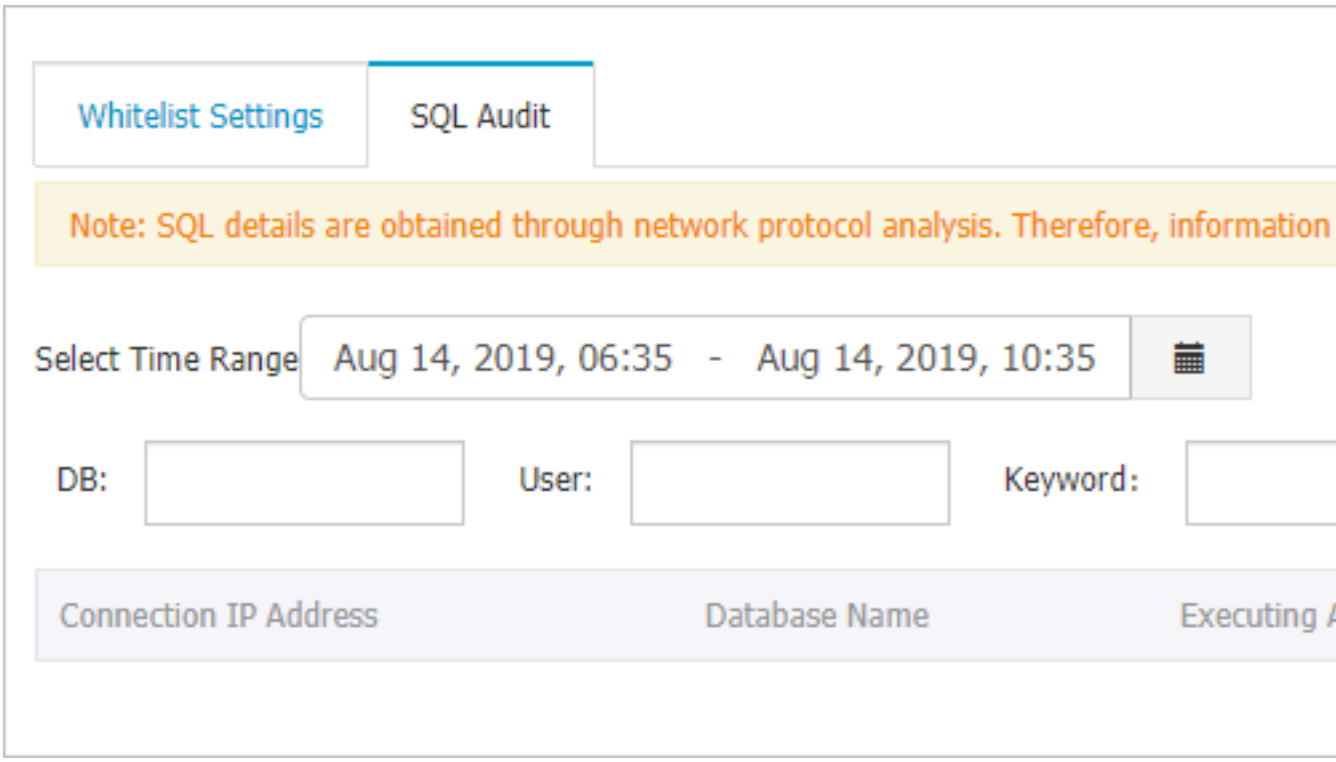
> **Note:**
> When the SQL audit feature is disabled, all the SQL audit records are cleared. We recommend that you export and store the audit records locally before disabling SQL audit.

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 Data Security.
5. Select the SQL Audit tab, click Export, and then store the exported file locally.
6. After the file is exported, click Disable SQL Audit Log.




7. In the message box that appears, click OK.

# 14 Data backup

## 14.1 Back up the data of an RDS for PostgreSQL instance

**RDS automatically backs up data based on the default backup policy. You can also modify the automatic backup settings or manually back up RDS data.**

Precautions

- **Instance backup files occupy backup space. You are allocated a free quota of backup space, and backups that exceed the free quota incur charges. We recommend that you design a backup cycle that meets your requirements and the limits of the free quota. For more information about the free quota of the backup space, see** *View the free quota of the backup space for an RDS for PostgreSQL instance*.
- **For more information about the billing methods and billing items, see** *#unique_13*.
- **For more information about the billing standard for backup space usage, see** *Pricing*.
- **Do not perform DDL operations during backup because the backup may fail due to table locks.**
- **Back up data during off-peak hours.**
- **Backing up a large volume of data may take a long time.**
- **The backup files are only retained for a certain period of time. Download the backup files you need in time.**

Backup description

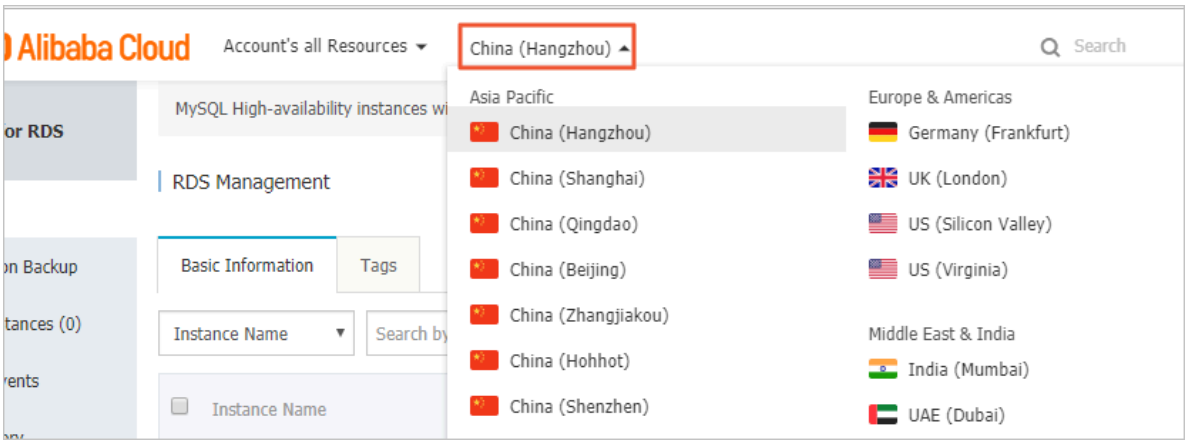
| Database engine | Data backup | Log backup |
| --- | --- | --- |
| PostgreSQL | Supports full physical backup. | Write-ahead logs (WALs) (16 MB per log) are compressed and uploaded immediately after they are generated. Local files are deleted within 24 hours. |

Modify the automatic backup settings

**After you configure a backup policy, ApsaraDB for RDS automatically backs up databases based on the policy.**

**If the PostgreSQL version and edition are PostgreSQL 11 High-availability Edition ( with standard SSDs) or PostgreSQL 10 High-availability Edition (with standard SSDs ), follow these steps to modify the automatic backup settings:**

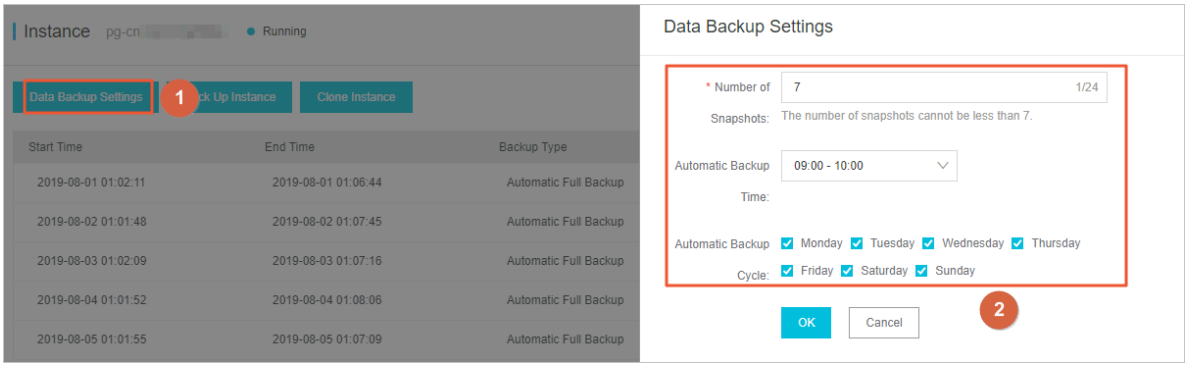
1. **Log on to the *ApsaraDB RDS for PostgreSQL console*.**
2. **Select the target region.**




3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, choose Backup and Restoration > Data Backup.**
5. **In the upper-left corner of the page, click Data Backup Settings.**
6. **Configure the following parameters.**

| Parameter | Description |
| --- | --- |
| Number of Snapshots | You can retain 7 to 60 data snapshots. The default value is 7. |
| Automatic Backup Time | You can specify any period of time in a day. Unit: hour. |

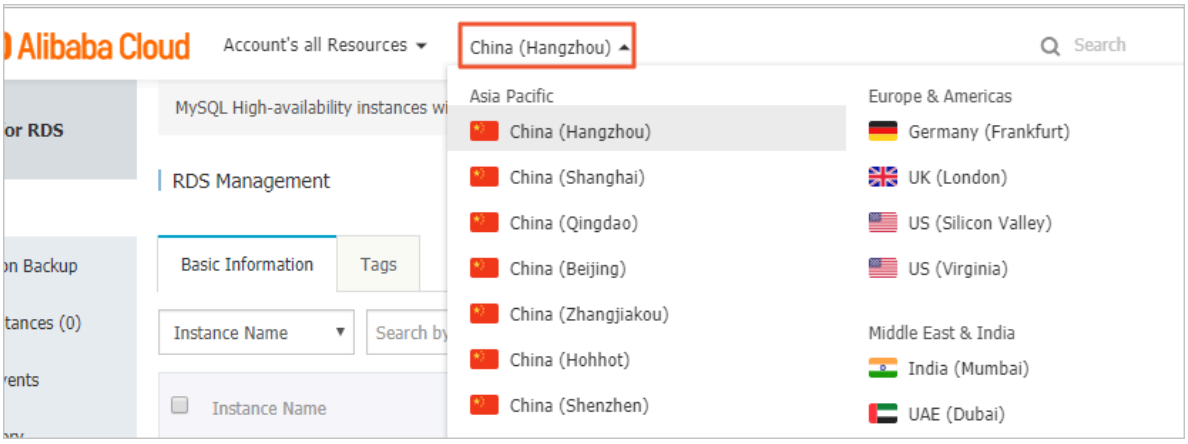
| Parameter | Description |
| --- | --- |
| Automatic Backup Cycle | You can specify more than one day in a week. Data must be backed up at least twice a week. |




7. Click OK.

To configure a default log backup policy, follow these steps:

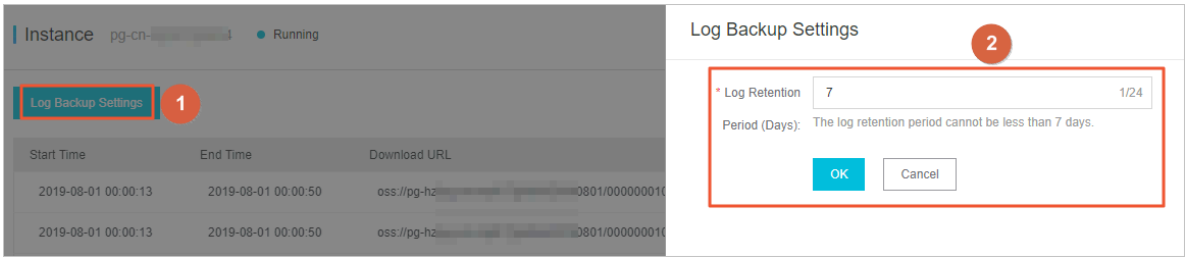
1. Log on to the *ApsaraDB RDS for PostgreSQL console*.
2. Select the target region.




3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, choose Backup and Restoration > Log Backup.
5. In the upper-left corner of the page, click Log Backup Settings.
6. Set Log Retention Period (Days).

**Note:**

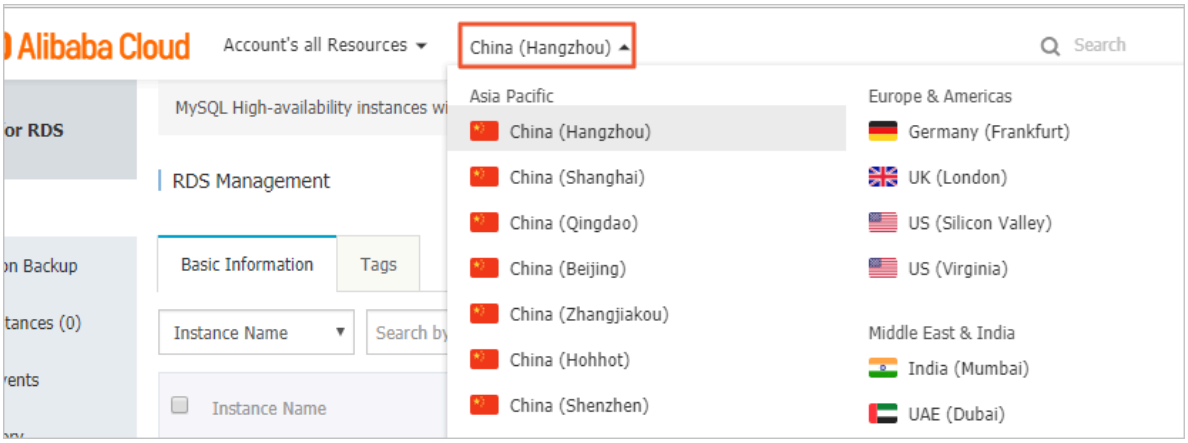
Log backup files can be retained for 7 to 365 days. The default value is 7 days.




7. Click OK.

If the PostgreSQL version and edition are PostgreSQL 10 High-availability Edition ( with local SSDs), PostgreSQL 10 Basic Edition, or PostgreSQL 9.4, follow these steps to modify the automatic backup settings:

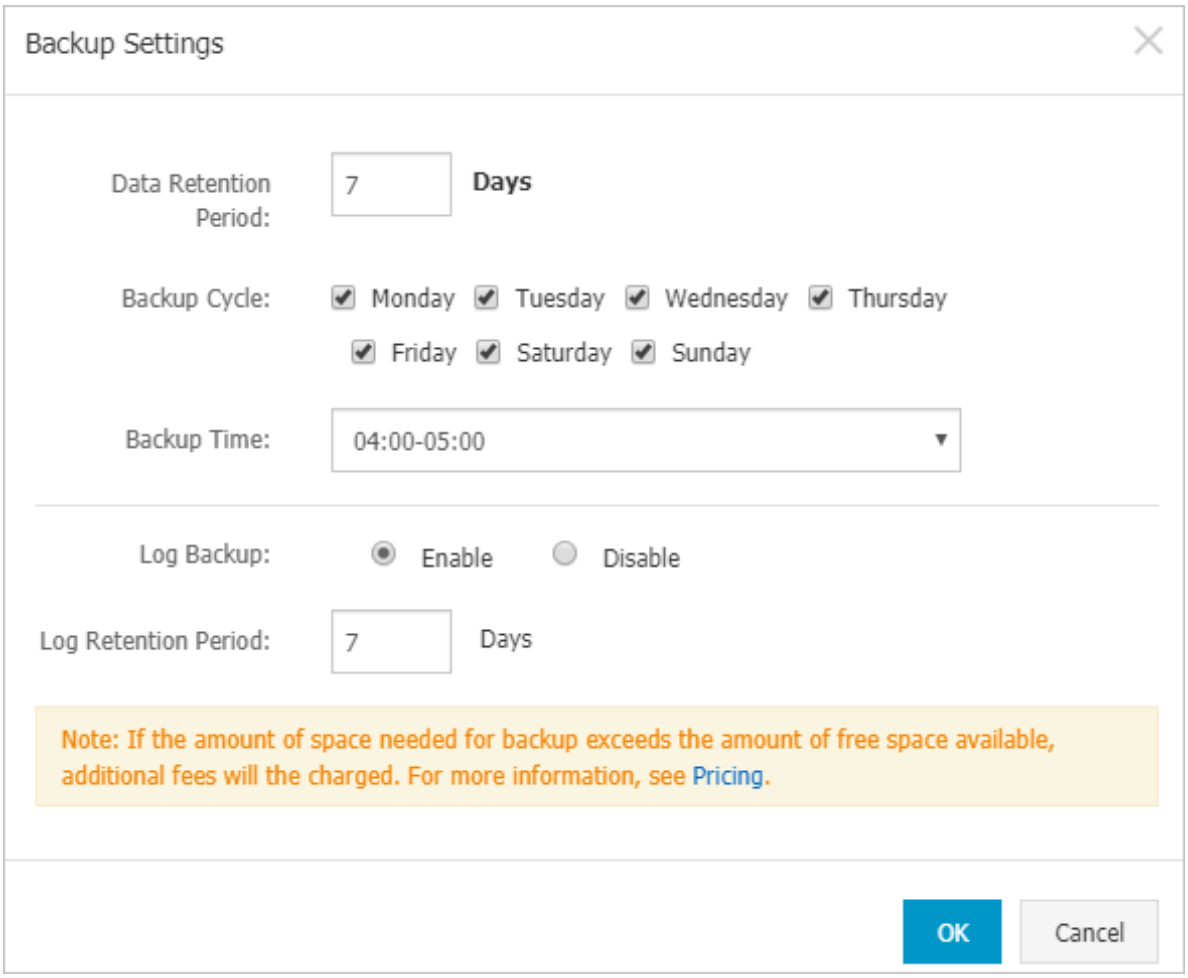
1. Log on to the *RDS console*.
2. Select the target region.




3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Backup and Restoration.
5. On the Backup and Restoration page that appears, click the Backup Settings tab and click Edit.
6. Configure the following parameters.

| Parameter | Description |
| --- | --- |
| Data Retention Period | You can specify the number of days when data backup files are retained. The default value is 7 days. The value range is 7 to 730 days.<br><br>**Note:**<br>Backup files of PostgreSQL 10 Basic Edition can only be retained for seven days. This parameter cannot be modified. |

| Parameter | Description |
| --- | --- |
| Backup Cycle | You can specify more than one day in a week. |
| Backup Time | You can specify any period of time in a day. Unit: hours. |
| Log Backup | You can enable or disable the log backup function.<br>**Notice:**<br>If you disable log backup, all the log backup files are deleted, and you cannot restore data by time point. |
| Log Retention Period | · You can specify the number of days when the log backup files are retained. The default value is 7 days.<br>· The value range is 7 to 730 days and it must be less than or equal to the value of the data retention period.<br>**Note:**<br>PostgreSQL 10 Basic Edition does not allow you to back up log files. |

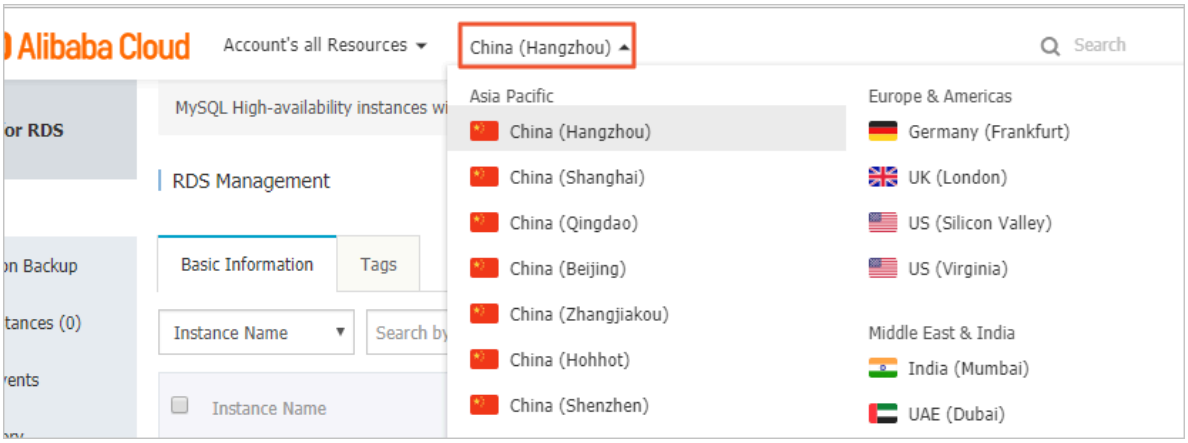


7. Click OK.

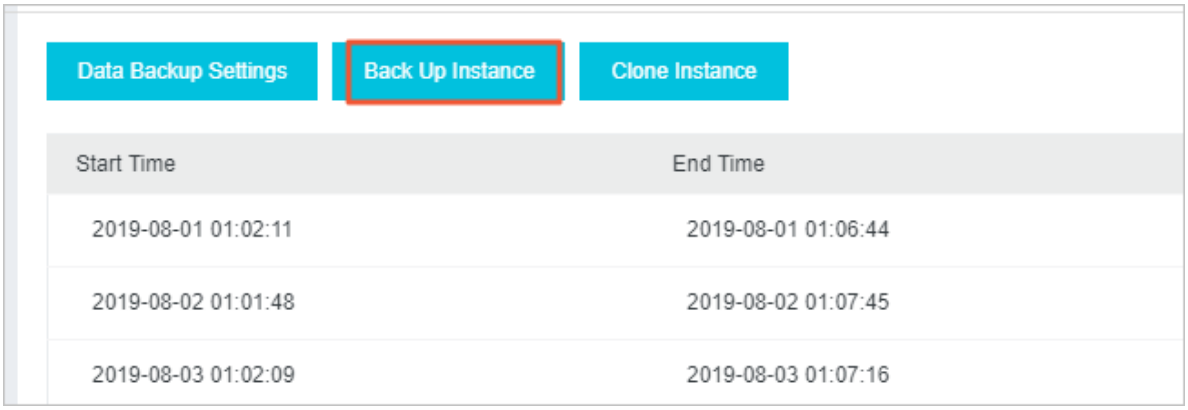
Manually back up an RDS for PostgreSQL instance

**If the PostgreSQL version and edition are PostgreSQL 11 High-availability Edition ( with standard SSDs) or PostgreSQL 10 High-availability Edition (with standard SSDs ), follow these steps:**

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




3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, choose Backup and Restoration > Data Backup.
5. In the upper-left corner of the page, click Instance Backup.

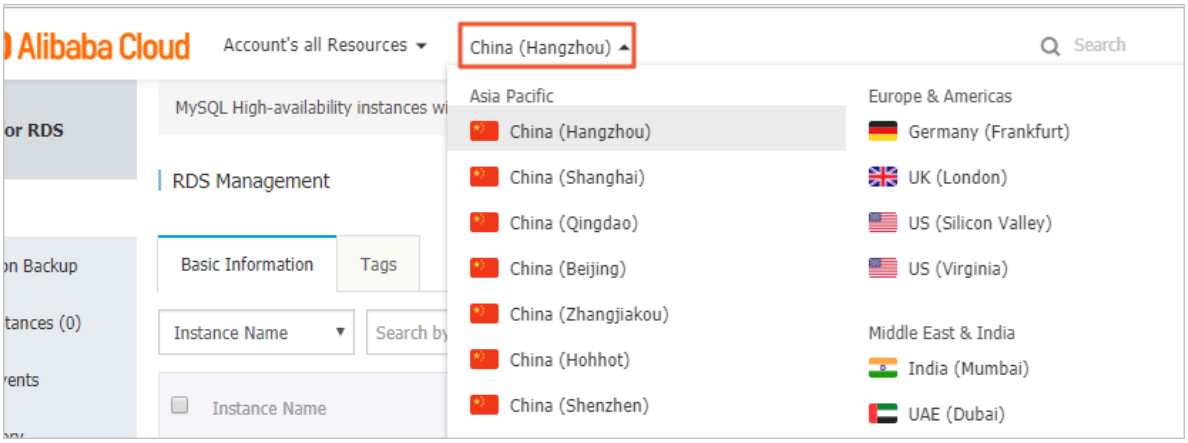



6. In the message that appears, click OK.

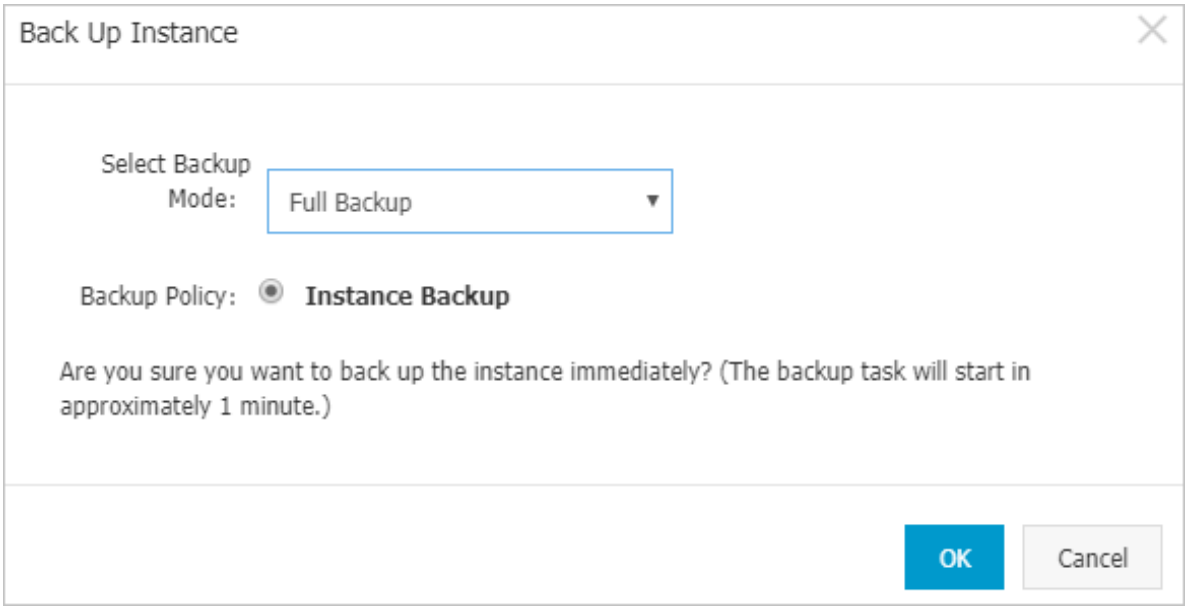
**If the PostgreSQL version and edition are PostgreSQL 10 High-availability Edition ( with local SSDs), PostgreSQL 10 Basic Edition, or PostgreSQL 9.4, follow these steps:**

1. Log on to the *RDS console*.

2. **Select the target region.**




3. **Find the target RDS instance and click the instance ID.**
4. **In the upper-right corner of the Basic Information page, click Back Up Instance.**




5. **Click OK.**

FAQ

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

   **No, but you can decrease the backup frequency, but to no less than twice a week.**
2. **Can I disable the log backup function for an RDS for PostgreSQL instance?**

   **Yes, you can log on to the RDS console and navigate to the Backup Settings tab to disable the log backup function for an instance in the PostgreSQL 10 High-availability Edition (with local SSDs) or PostgreSQL 9.4.**

APIs

| API | Description |
| --- | --- |
| *CreateBackup* | Creates a backup for an RDS instance. |
| *DescribeBackups* | Queries the list of backups for an RDS instance. |
| *DescribeBackupPolicy* | Queries a backup policy for an RDS instance. |
| *ModifyBackupPolicy* | Modifies a backup policy for an RDS instance. |

## 14.2 View the free quota of the backup space for an RDS for PostgreSQL instance

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

**Free quota of backup space = 50% × Purchased storage space of the instance (Unit: GB, rounded up).**

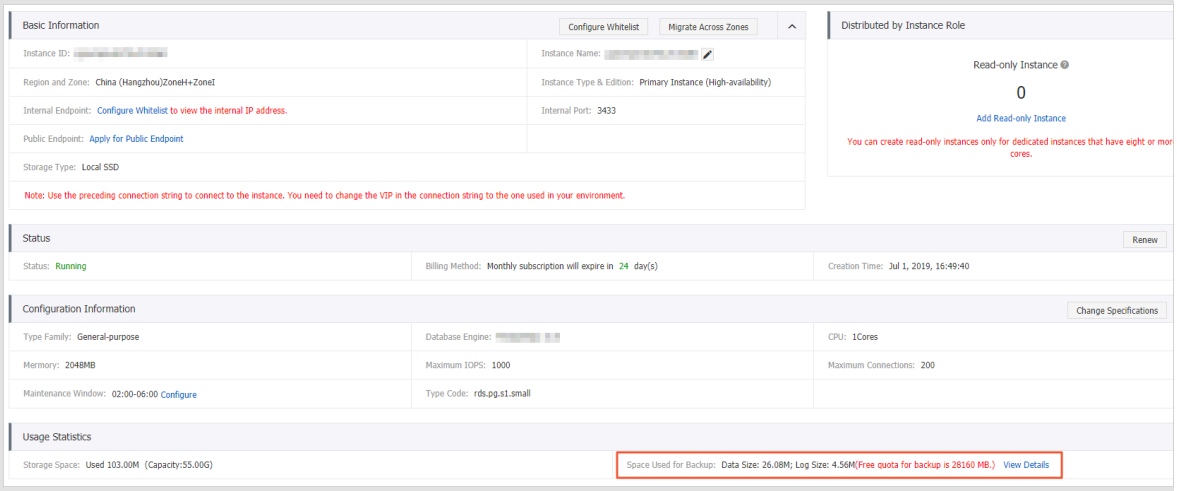
**Backup space exceeding the free quota = data backup volume + log backup volume - 50% × storage space purchased of the instance (Unit: GB, rounded up).**

**For example, if the data backup volume is 30 GB, the log backup volume is 10 GB, and the storage space is 60 GB, the `volume charged per hour = 30 + 10 - 50% × 60 = 10 (GB)`. An additional 10 GB space is charged per hour.**

**Note:**

- **For the hourly cost of backup space that exceeds the free quota, see *Pricing of ApsaraDB for RDS*.**

- **Basic Edition instances of some engines save the backup files of the last seven days for free. For more information, refer to the console.**




View the free quota of the backup space in the ApsaraDB for RDS console

### Prerequisites

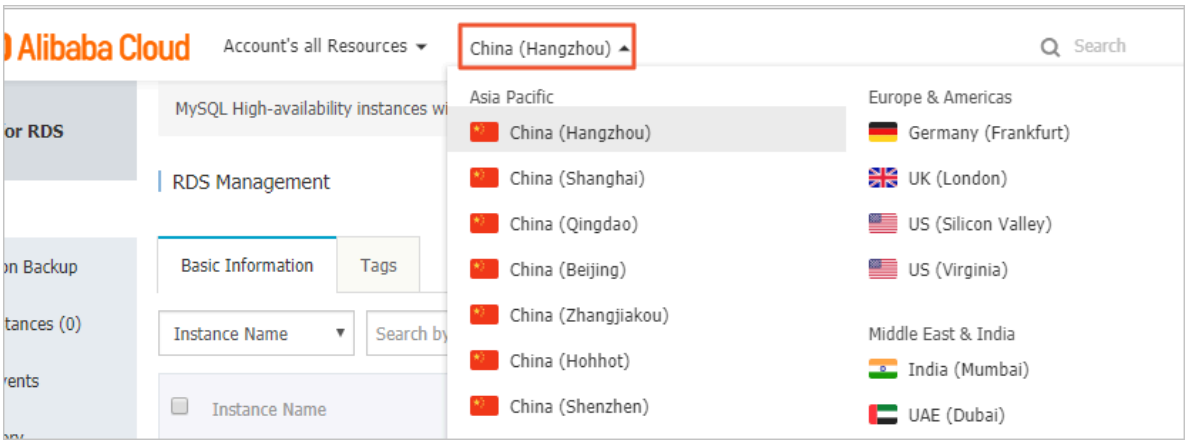
**The instance must be of the following versions:**

- **PostgreSQL 10 High-availability Edition (local disk)**
- **PostgreSQL 9.4**

> **Note:**
> **You cannot view the free quota of the PostgreSQL 11 High-availability Edition (cloud disk) or PostgreSQL 10 High-availability Edition (cloud disk) in the console.**

### 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. Click the ID of the instance to go to the Basic Information page.
4. In the `Usage Statistics` section at the lower part of the page, check the free quota following `Space Used for Backup`, as shown in the following figure.

> **Note:**
> Instances of different types support different amounts of free quotas. The following figure is only an example. Refer to the console for the exact information.


## 14.3 Download data and log backup files

You can download unencrypted data and log backup files from the RDS console to archive and restore data to an on-premises database.

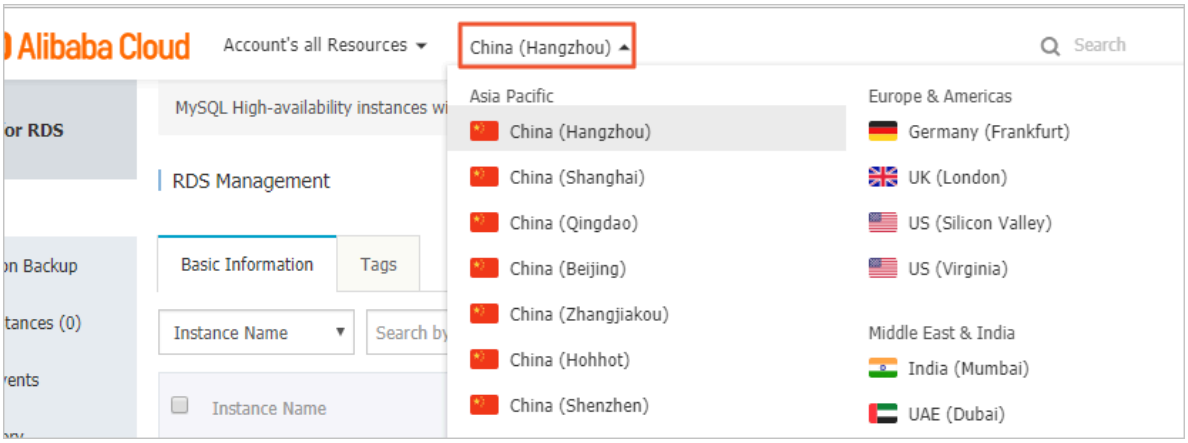
### Precautions

- PostgreSQL 11 High-availability Edition (cloud disk) and PostgreSQL 10 High-availability Edition (cloud disk) do not allow you to download backup files.
- PostgreSQL 10 Basic Edition does not allow you to download backup files.
- You cannot download backup files by using a read-only RAM user account. You can assign permissions to the RAM user in the RAM console. For more information, see *#unique_114*.

### Procedure

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

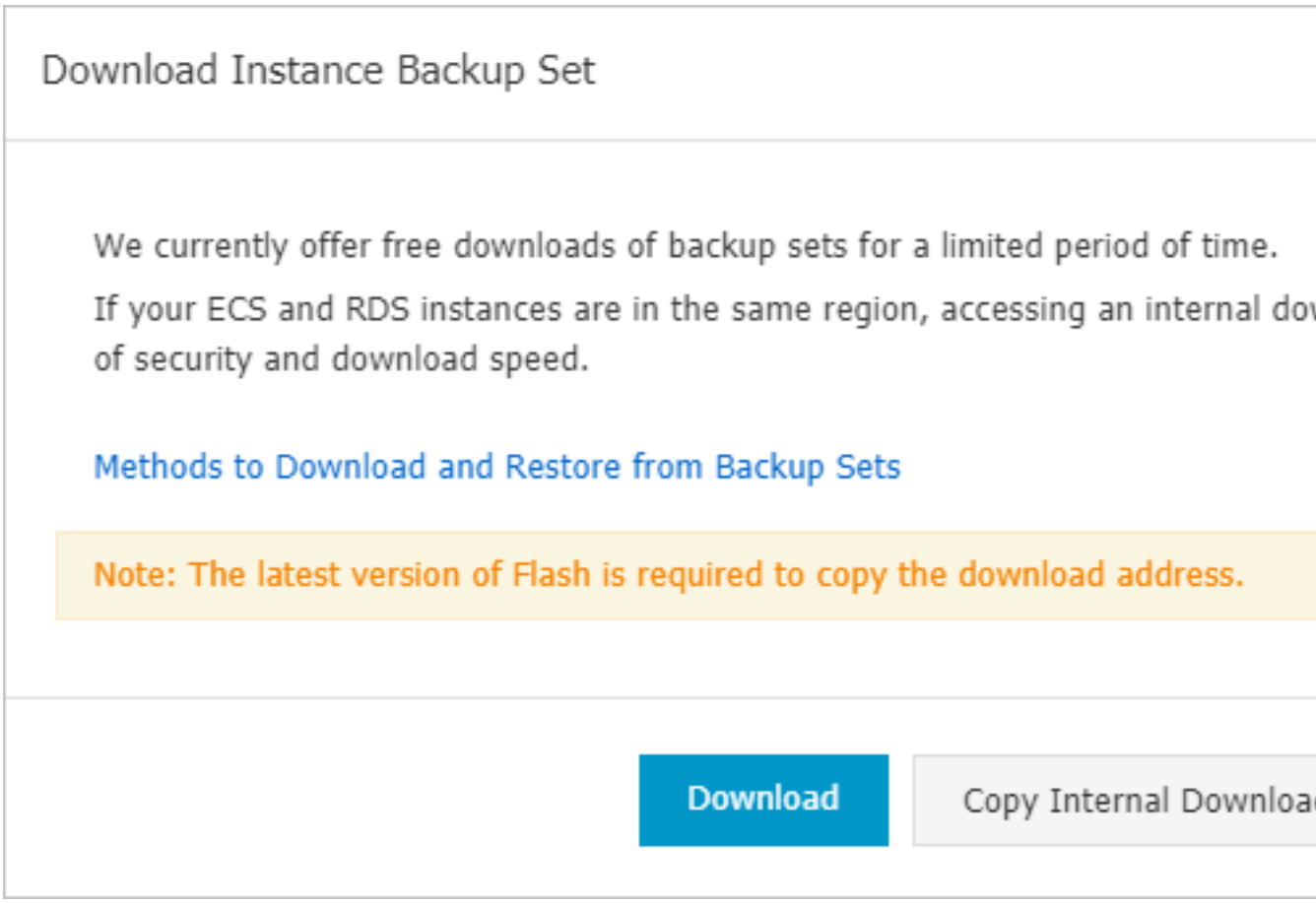
2. In the upper-left corner of the page, select the region where the instance is located.




3. Click the ID of the instance to go to the Basic Information page.
4. In the left-side navigation pane, select Backup and Restoration to go to the Backup and Restoration page.
5. Click the corresponding tab based on the type of backup that you want to download.
   - Data backup: Click the Backup Sets tab.
   - Log backup: Click the Archive List tab.
6. Specify a time range to query the backups created in that period.
7. Find the data backup or binlog file that you want to download, and click Download in the Actions column.

> **Note:**
>
> - If you need to restore data by using data backup files, select the backup file that is closest to the time for restoration.
> - If you use the binlog file to restore data to an on-premises database, note that:
>   - The Instance ID of the binlog file on the Archive List tab must be the same as the Instance No. of the data backup file on the Backup Sets tab.
>   - The start time of the binlog file must be later than the data backup time and earlier than the time when you need to restore data.

8. **In the Download Instance Backup Set or Download Binary Log dialog box that appears, select a download method.**




| Download method | Description |
| --- | --- |
| Download | Download the backup file by using an Internet address. |
| Copy Internal Download URL | Copy the internal download URL. If the ECS and RDS instances are in the same region, you can log on to the ECS console and use the internal address to download the backup file. This method is faster and more secure. |
| Copy External Download URL | Copy the external download URL and use other tools to download the backup file. |

**Note:**

**If you download a file in Linux, run the following command:**

```
wget -c '<download address>' -O <customized file name>.tar.gz
```

- **-c: specifies to resume from the breakpoint.**
- **-O: specifies a name for the download file (use the file name suffix .tar.gz or .xb.gz as contained in the URL).**
- **If the download URL has multiple parameters, we recommend that you add single quotation marks to the download URL to avoid download failure.**

# 15 Data restoration

## 15.1 Restore PostgreSQL data

**The topic describes how use backups to restore data to ApsaraDB RDS for PostgreSQL instances.**

**You can restore ApsaraDB RDS for PostgreSQL data by backup set or by time. The procedure is as follows:**

1. **Restore data to a new instance (formerly known as cloning an instance).**
2. **Log on to the new instance to verify the data.**
3. **Migrate the data to the original instance.**

Precautions

- **The new instance must have the same whitelist, backup, and parameter settings as the original instance.**
- **The new instance must have the same data and account information as the backup set or instance at the time point.**

Pricing

**It is the same as purchasing a new instance. For more information, see** *Pricing*.

Prerequisites

**The original instance must meet the following conditions:**

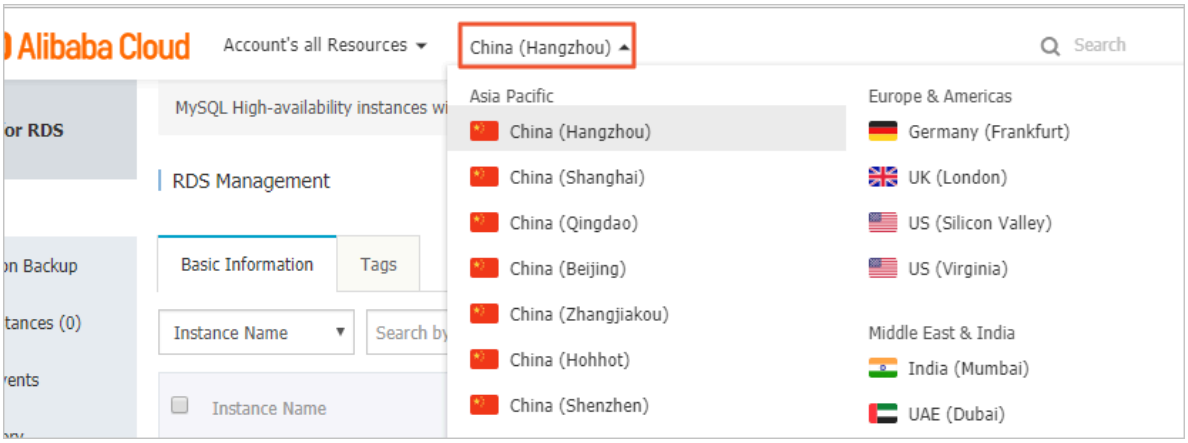
- **It is running and is not locked.**
- **It is not undergoing any migration tasks.**
- **To restore data by time, you must make sure that the log backup function is enabled.**
- **To restore data by backup set, you must make sure that the original instance has at least one backup set.**

Restore data to a new instance

**PostgreSQL 11 High-availability Edition (cloud disk) and PostgreSQL 10 High-availability Edition (cloud disk)**

1. **Log on to the new** *ApsaraDB RDS for PostgreSQL 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, choose Backup and Restoration > Data Backup.
5. In the upper-left corner of the page, click Clone Instance.
6. On the page that appears, select a billing method for the new instance.
   - Subscription You are charged when you create an instance. For long-term usage, subscription instances can be more cost-effective than pay-as-you-go instances. The longer the subscription period, the greater the discount.
   - Pay-As-You-Go: You are charged by hour. Pay-as-you-go instances can be more cost-effective over a short-term period. You can release the instance if you no longer need it.

> **Note:**
> Pay-as-you-go instances can be changed to subscription instances. Subscription instances cannot be changed to pay-as-you-go instances.

7. Configure parameters for the new instance.

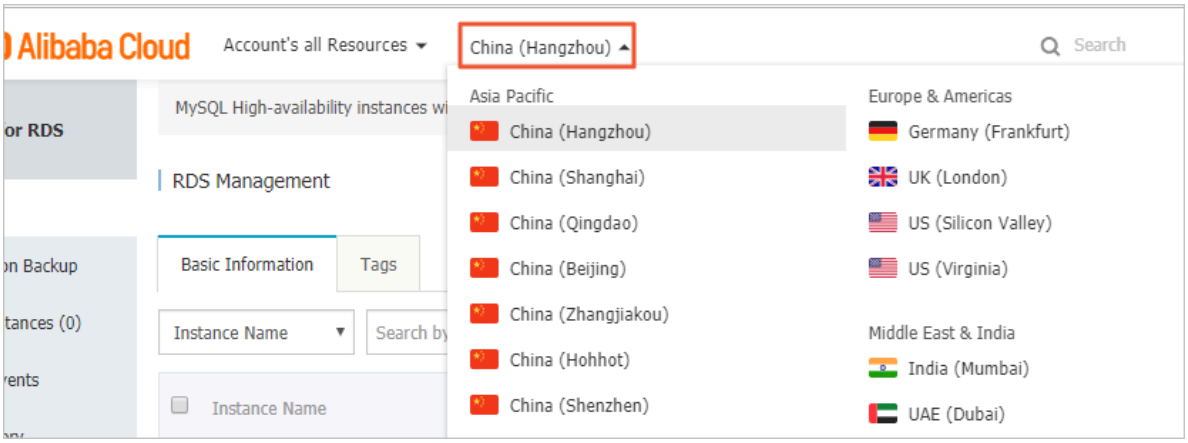
| Parameter | Description |
| --- | --- |
| Restore Mode | · By Time: You can restore data to any point in time within the retention period of log backup. To view or modify the retention period of log backup, see *Back up the data of an RDS for PostgreSQL instance*.<br>· By Backup Set<br>**Note:**<br>By Time is displayed only if the log backup function is enabled. |

| Parameter | Description |
| --- | --- |
| Primary Zone | The ID of the primary zone to which the RDS instance belongs.<br>· A zone is an independent physical area located within a region. There are no substantive differences between the zones.<br>· You can deploy RDS and ECS instances in the same zone or in different zones.<br>· You only need to select a primary zone. The system automatically selects a secondary zone. |
| Instance Type | Each instance type provides a specific number of CPU cores, memory, maximum number of connections, and maximum IOPS. For more information, see #unique_16.<br>RDS provides the following instance families:<br>· General-purpose (including test and entry-level instances): A general-purpose instance uses dedicated allocations of memory and I/O resources while sharing CPU and storage resources with other general-purpose instances on the same server.<br>· Dedicated: A dedicated instance uses dedicated allocations of CPU, memory, storage, and I/O resources.<br>· Dedicated host: A dedicated instance type with maximum specifications. Instances of this type occupy the CPU, memory, storage, and I/O resources of the entire server.<br>For example, an instance with 4 cores and 16 GB memory indicates a general-purpose instance. An instance with 8 cores and 32 GB of dedicated memory indicates a dedicated instance. An instance with 30 cores and 220 GB of dedicated memory indicates a dedicated host instance. |
| Virtual Private Cloud (VPC)<br>VSwitch | · Select the VPC and VSwitch if you have created a VPC that meets your network plan.<br>· Otherwise, use the default VPC and VSwitch. |
| Storage Type | Standard SSD or Enhanced SSD. For more information, see *Storage types*. |
| Capacity | The storage space of the instance, including the space for data, system files, binlog files, and transaction files. |

8. Configure the duration for subscription instances only, select the check box of ApsaraDB RDS for PostgreSQL Agreement of Service, and click Pay.

**PostgreSQL 10 High-availability Edition (local disk), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4**

1. Log on to the *ApsaraDB for RDS console*.
2. Select the region where the instance is located.




3. Click the ID of the instance.
4. In the left-side navigation pane, select Backup and Restoration.
5. In the upper-right corner of the page, click Restore Database (Previously Clone Database).
6. On the page that appears, select a billing method for the new instance.
   - Pay-As-You-Go: You are charged by hour. Pay-as-you-go instances can be more cost-effective over a short-term period. You can release the instance if you no longer need it.
   - Subscription: You are charged when you create the instance. For long-term usage, subscription instances can be more cost-effective than pay-as-you-go instances. The longer the subscription period, the greater the discount.

> **Note:**
> Pay-as-you-go instances can be changed to subscription instances. Subscription instances cannot be changed to pay-as-you-go instances.

7. Configure parameters for the new instance.

| Parameter | Description |
| --- | --- |
| Restore Mode | · By Time: You can restore data to any point in time within the retention period of log backup. To view or modify the retention period of log backup, see *Back up the data of an RDS for PostgreSQL instance*.<br>· By Backup Set<br>**Note:**<br>By Time is displayed only if the log backup function is enabled. |
| Edition | · RDS for PostgreSQL 10 Basic Edition. The Basic Edition is of a single-node structure that separates computing from storage. This edition is cost-effective, but is not recommended for production environments.<br>· RDS for PostgreSQL 9.4 High-availability Edition and PostgreSQL 10 High-availability Edition. A high-availability instance includes one primary node and one secondary node, which is a classic high-availability architecture.<br>For more information, see *Product series overview*. |
| Zone | The zone of the instance. A zone is an independent physical area located within a region. There are no substantive differences between the zones.<br>You can choose to create RDS and ECS instances in the same zone or in different zones.<br>High-availability instances in some regions can be deployed in multiple zones, for example, Zone F + Zone G. In this case, the high-availability instance is deployed across different zones, which provides a higher disaster recovery capability at no additional charge.<br>**Note:**<br>The new instance is in the same region as the original instance and the region cannot be modified. |

| Parameter | Description |
| --- | --- |
| Type | The instance type. We recommend that you select a type and storage space that are larger than those of the primary instance. Otherwise, the data restoration may take a long time due to performance limitations.<br><br>Each instance type provides a specific number of CPU cores, memory, maximum number of connections, and maximum IOPS. For more information, see *Instance type list*.<br><br>RDS provides the following instance families:<br><br>· General-purpose: A general-purpose instance uses dedicated allocations of memory and I/O resources while sharing CPU and storage resources with other general-purpose instances on the same server.<br>· Dedicated: A dedicated instance uses dedicated allocations of CPU, memory, storage, and I/O resources.<br>· Dedicated host: A dedicated instance type with maximum specifications. Instances of this type occupy the CPU, memory, storage, and I/O resources of the entire server.<br><br>For example, an instance with 8 cores and 32 GB memory indicates a general-purpose instance. An instance with 8 cores and 32 GB of dedicated memory indicates a dedicated instance. An instance with 30 cores and 220 GB of dedicated memory indicates a dedicated host instance. |
| Capacity | The storage space of the instance, including the space for data and system files. |
| Network Type | · Classic Network<br>· VPC (recommended): Virtual Private Cloud. A VPC is an isolated virtual network with higher security and performance than a classic network.<br><br>Note:<br>- Select the VPC and VSwitch if you have created a VPC that meets your network plan.<br>- Otherwise, use the default VPC and VSwitch. |

8. Configure the number of instances and their duration.

9. Click Buy Now.
10. Select and Product Terms of Service and Service Level Notice and Terms of Use, and click Pay Now.

Log on to the new instance and verify the data

For more information about logging on to an instance, see *Connect to an instance*.

Migrate data to the original instance

After you verify the data in the new instance, you can migrate the data that you require from the new instance to the original instance.

**Precautions**

You cannot perform DDL operations during data migration. Otherwise, the migration may fail.

**Procedure**

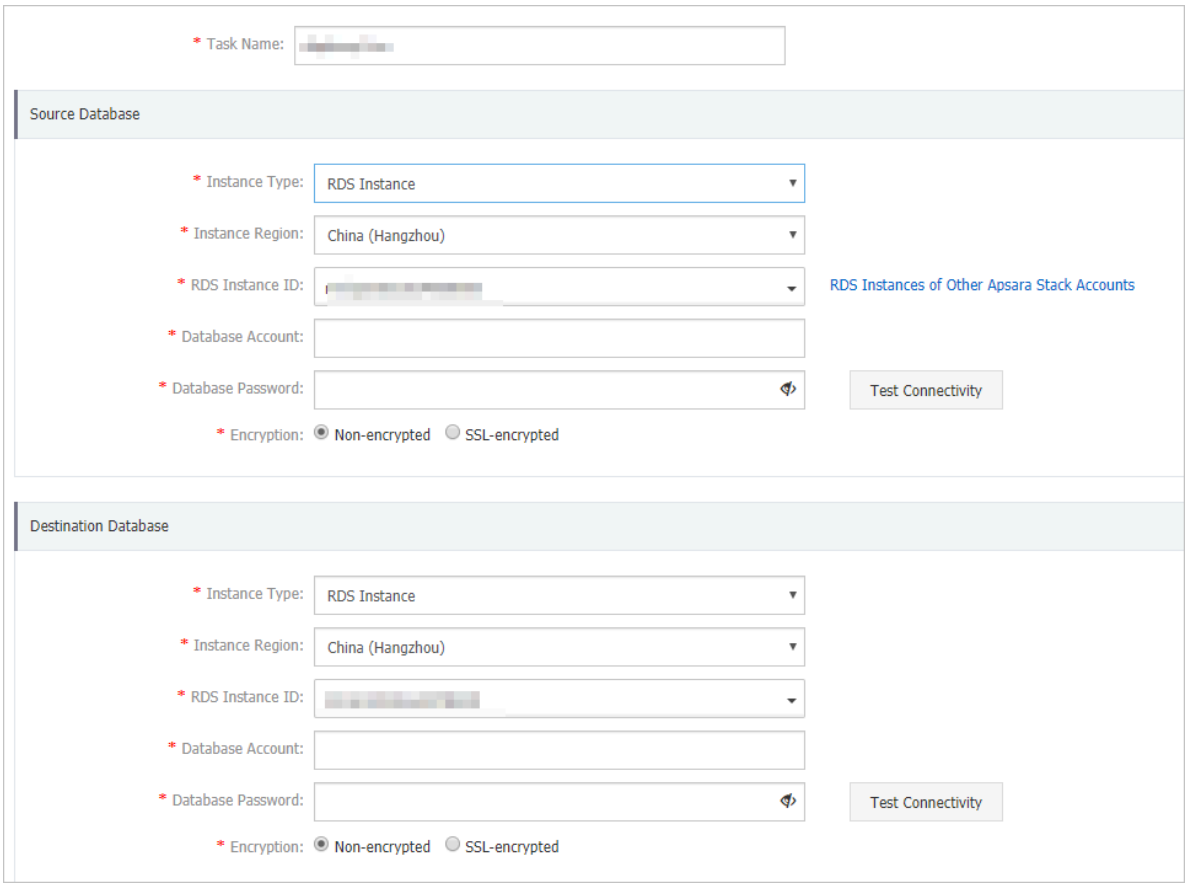
1. Log on to the *DTS console*.
2. In the left-side navigation pane, select Data Migration.
3. In the upper-right corner of the page, click Create Migration Task.
4. Enter the task name and the information of source and destination databases. The following table describes the parameters.

| Section | Parameter | Description |
| --- | --- | --- |
| - | Task Name | DTS automatically generates a name for each task. We recommend that you change it to a descriptive name to help identify the task. |
| Source Database | Instance Type | Select RDS Instance. |
| | Instance Region | Select the region where the new instance is located. |
| | RDS Instance ID | Select the ID of the new instance. |
| | Database Name | Enter the name of the database that you need to migrate in the new instance.<br>Note:<br>If you need to migrate multiple databases, you must create a migration task for each database. |

| Section | Parameter | Description |
| --- | --- | --- |
| | Database Account | Enter the premier account of the new instance. |
| | Database Password | Enter the password of the premier account. |
| Destination Database | Instance Type | Select RDS Instance. |
| | Instance Region | Select the region where the original instance is located. |
| | RDS Instance ID | Select the ID of the original instance. |
| | Database Name | Enter the database to be migrated in the original instance. |
| | Database Account | Enter the premier account of the original instance. |
| | Database Password | Enter the password of the premier account. |

 **Note:**

**The values of Instance Type and RDS Instance ID determine which parameters you need to specify.**




5. **In the lower-right corner of the page, click Set Whitelist and Next.**
6. **Select Migrate object structure and Migrate existing data.**
7. **In the left-side Migration objects section, select the objects that you need to migrate, and click > to add them to the right-side Selected objects section.**

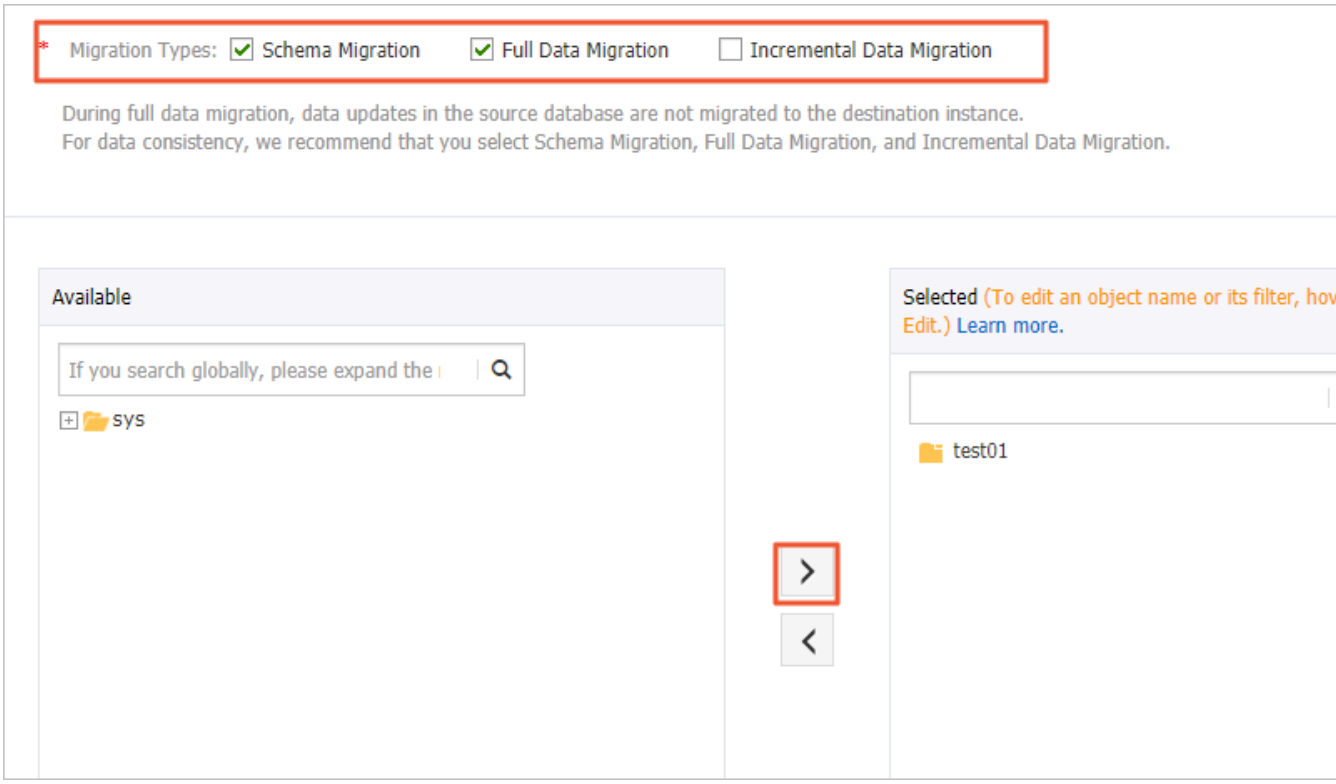
**Note:**

**DTS will perform object name conflict check. If an object in the destination RDS instance has the same name as the object to be migrated, the migration fails.**

**Solution:**

- **In the Selected objects section, move the pointer over the object and click Edit to modify the object name.**

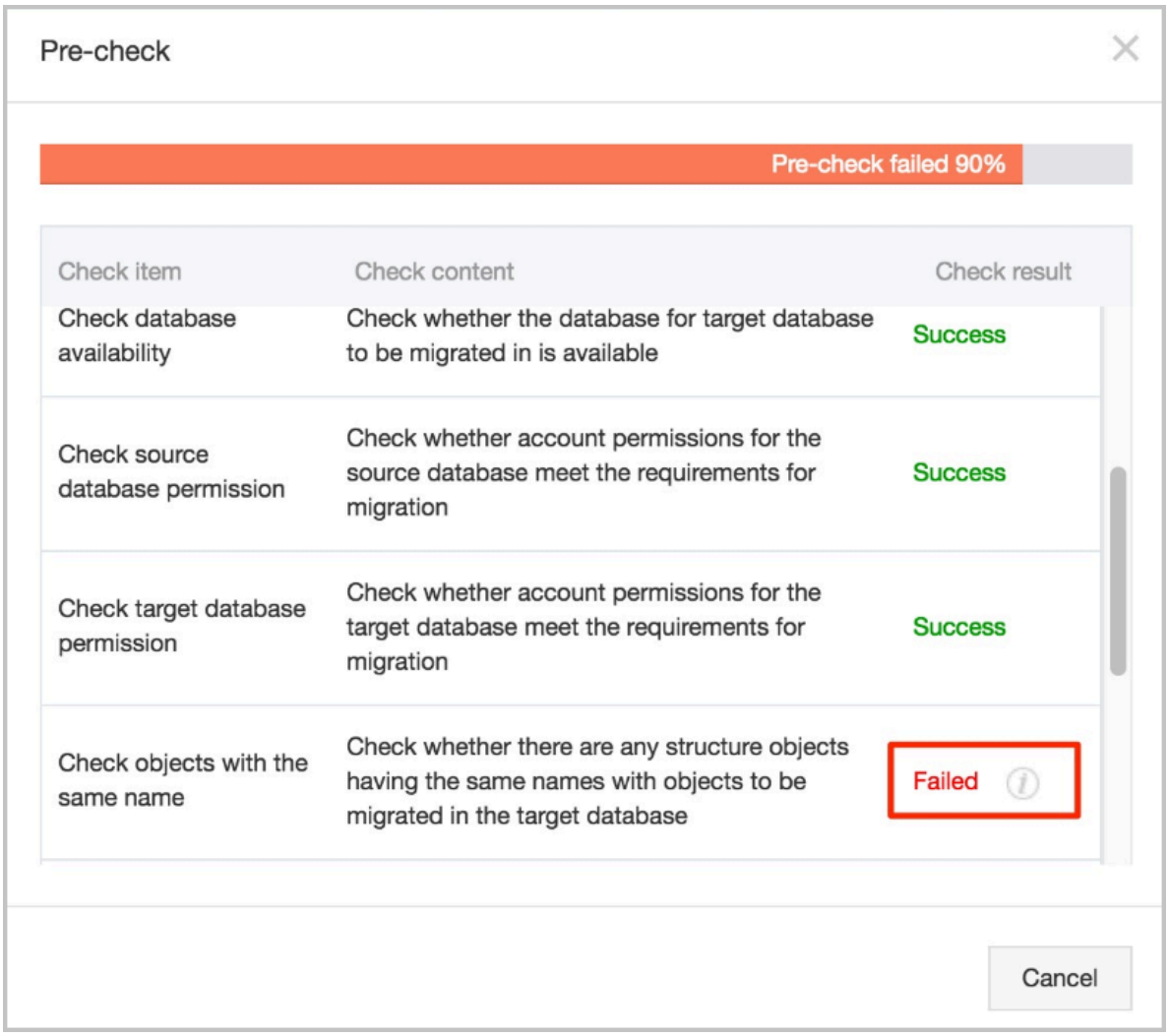
- **Rename the object in the destination database.**



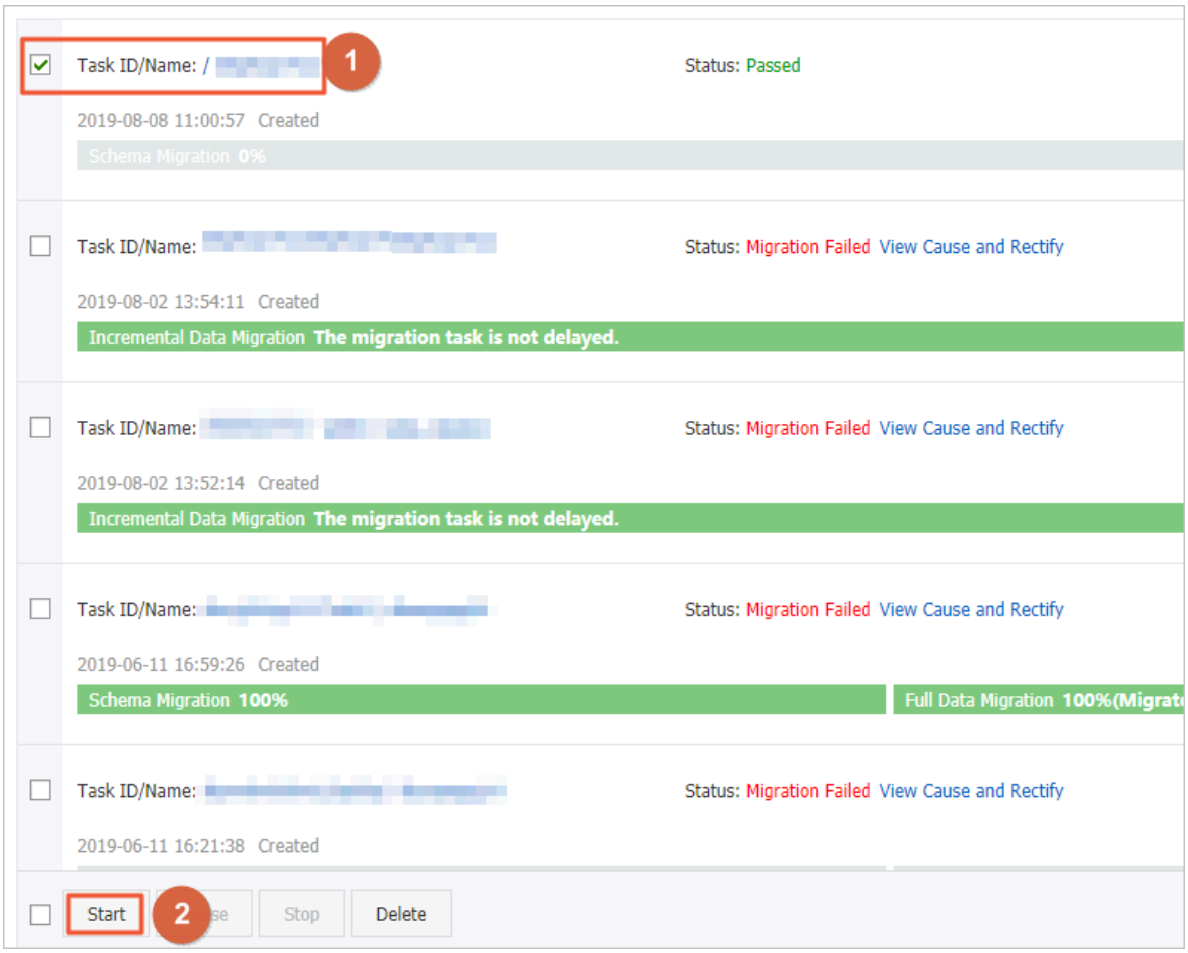

8. **Click Precheck and Start.**
9. **If the precheck fails, perform this step. If the precheck succeeds, go to step 11.**

   **If the precheck fails, click the icon next to the check item with check result as Failed to check the failure details as shown in the following figure. After**

**troubleshooting, select the current migration task on the Migration task list page and perform a precheck again.**



10. After all the errors are fixed, on the Migration task list page, select the newly created migration task and click Start.




11. After the precheck succeeds, click OK.
12. On the Confirm Purchase Configuration page, confirm configuration information and select Service Terms of Data Transmission (Pay-As-You-Go), and click Buy and Start Now.

# 16 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:**
> **If network links are not upgraded in a timely manner, some unintended service disruptions may occur in the database proxy mode. For example, network jitter may occur when you attempt to access resources. You must upgrade your RDS network link in time to ensure that your service is running smoothly. For more information, see** *Upgrade the RDS network link*.

Precautions

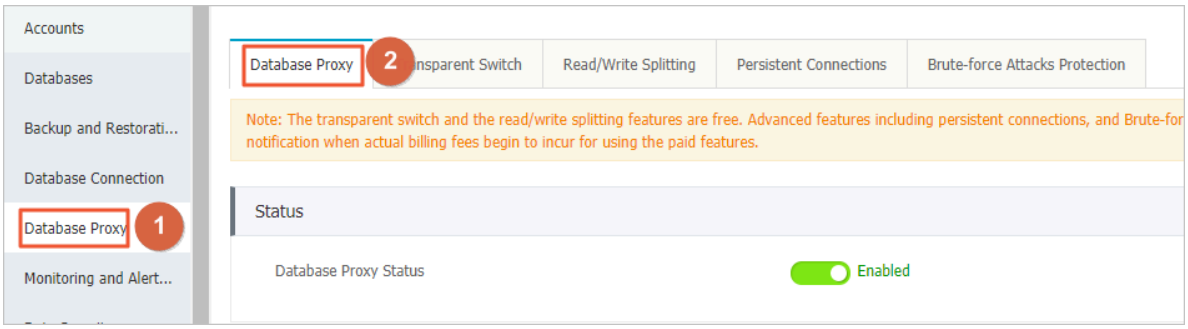
- **You can only disable the database proxy mode (that is, switch from the database proxy mode to the standard mode). You cannot enable the database proxy mode ( that is, switch from the standard mode to the database proxy mode).**
- **Switching the access mode may cause a 30-second transient disconnection. 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

- **You have enabled the database proxy mode.**

  > **Note:**
  > - **If the Database Proxy tab is displayed, the database proxy mode has been enabled. Follow the subsequent steps to disable the database proxy mode.**

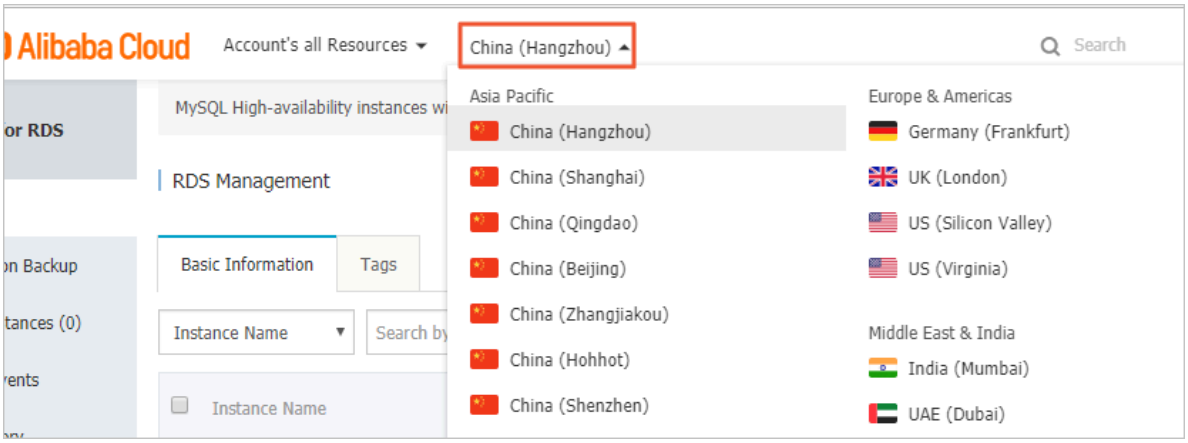
- If this tab is not displayed, the database proxy mode has been disabled. You do not need to perform this operation.




- The instance edition must be one of the following editions:
  - PostgreSQL 10 Cluster Edition (Local SSD)
  - PostgreSQL 10 Basic Edition
  - PostgreSQL 9.4

Procedure

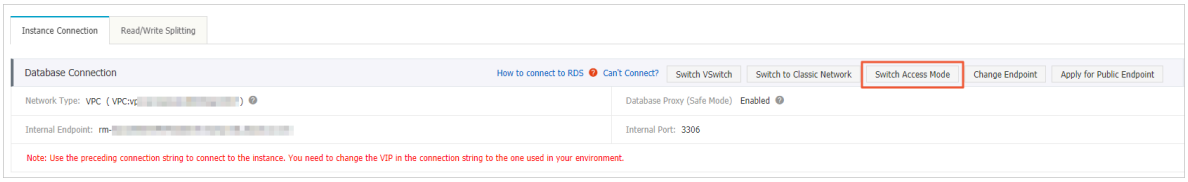
1. Log on to the *ApsaraDB for RDS console*.
2. In the upper-left corner of the page, select the region where the instance is located.




3. Find the instance and click the instance ID.
4. In the left-side navigation pane, select Database Connections.
5. On the Instance Connection tab, click Switch Access Mode in the upper-right corner. In the message box that appears, click OK.

**Note:**

**Only the instances that are in the database proxy mode shows the Switch Access Mode button.**



# 17 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.**

**You can query error logs, slow query logs, and primary/secondary instance switching logs of an instance through the console or by running SQL commands . These logs help you troubleshoot database issues. This topic describes how to manage logs through the console.**

- **For more information about the log backup settings, see** *Back up the data of an RDS for PostgreSQL instance***.**
- **For more information about how to download log backup files, see** *Download data and log backup files***.**
- **For more information about how to recover from a log backup file, see** *Restore PostgreSQL data***.**

**Note:**

- **PostgreSQL 10 Basic Edition does not support logs about switching between the primary database and secondary database.**
- **PostgreSQL 11 Cluster Edition (Standard SSD) and PostgreSQL 10 Cluster Edition (Standard SSD) do not support manage logs through the console. However, you can use SQL commands to query and manage logs.**

Prerequisites

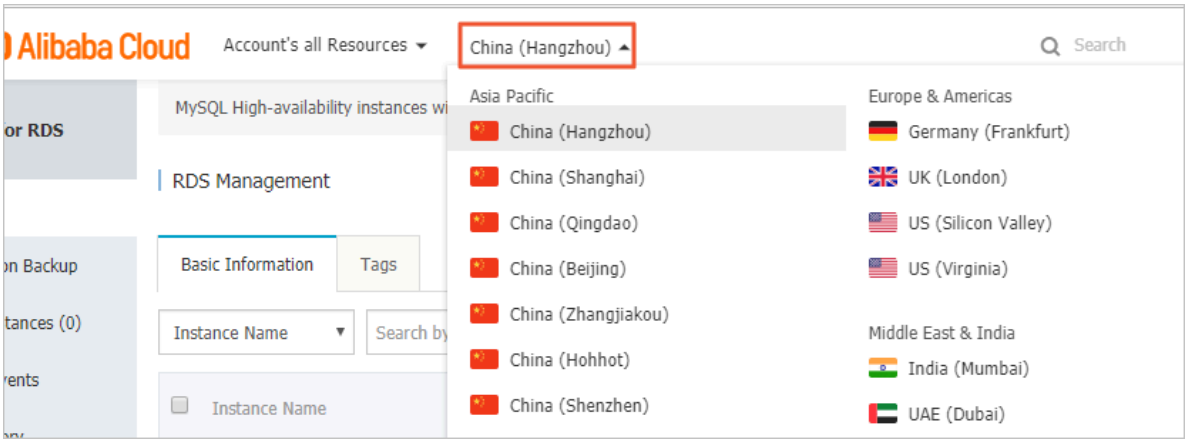
**The instance edition must be one of the following editions:**

- **PostgreSQL 10 Cluster Edition (Local SSD)**
- **PostgreSQL 10 Basic Edition**
- **PostgreSQL 9.4**

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 Logs.
5. On the Logs page, select the Error Log, Slow Query Log or Primary/Secondary Instance Switching Log tab, select a time range, and click Update.

| Log type | Description |
| --- | --- |
| Error log | Records the logs of database errors within one month. |
| Slow query log | Records the logs of SQL statements whose execution period exceeds one second in the database within a month and removes the duplicates in the logs. |
| Primary/ secondary instance switching log | Records the logs of switching between the primary and secondary databases within one month. |

**Note:**
Instances in China (Zhangjiakou-Beijing Winter Olympics) only retain the error logs and slow query logs within nine days.

API reference

| Operation | Description |
| --- | --- |
| *DescribeSlowLogs* | You can call this operation to query the list of slow query logs. |
| *DescribeSlowLogRecords* | You can call this operation to query the details of slow query logs. |

| Operation | Description |
| --- | --- |
| *DescribeErrorLogs* | You can call this operation to query error logs. |
| *DescribeBinlogFiles* | You can call this operation to query binlogs. |
| *DescribeSQLLogRecords* | You can call this operation to query audit logs. |
| *DescribeSQLLogFiles* | You can call this operation to query the list of audit log files. |

# 18 Tag management

## 18.1 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.**

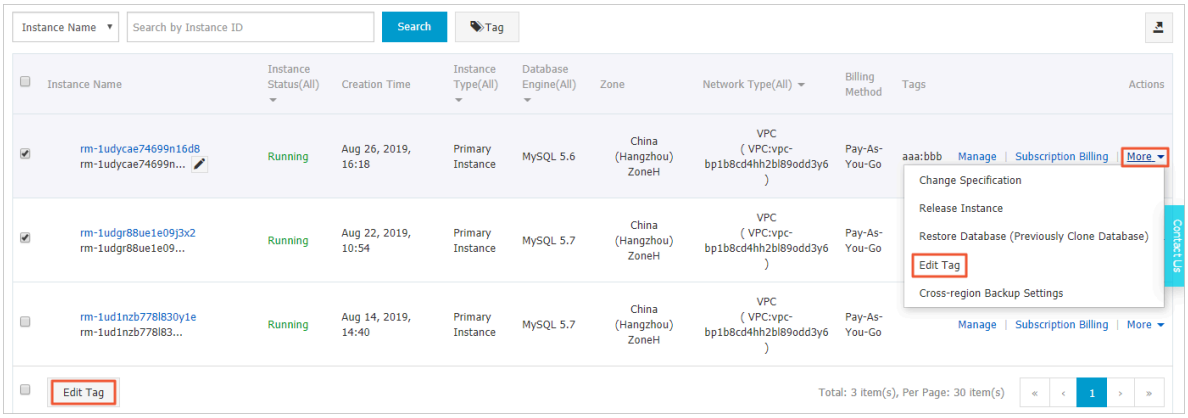
Limits

- **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

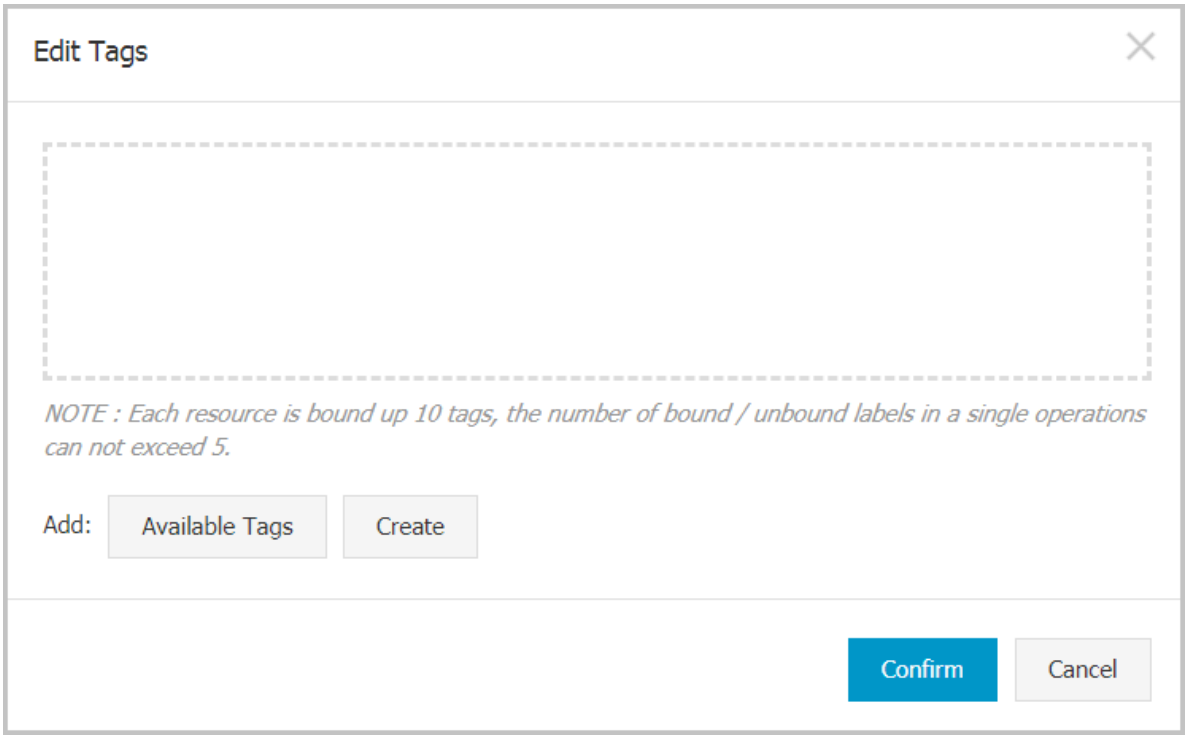
1. **Log on to the *RDS console* and in the left-side navigation pane, click Instances.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**

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. |

## 18.2 Delete tags

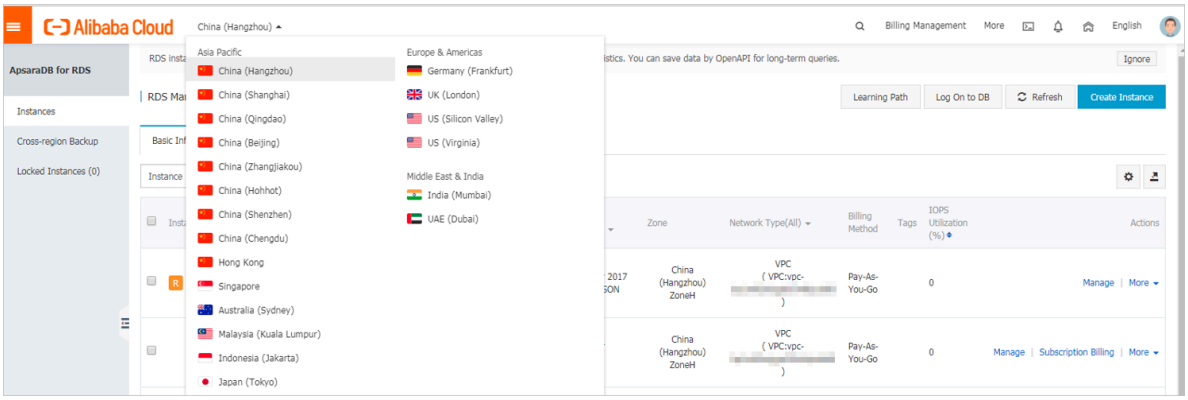
**This topic describes how to delete tags from an RDS instance when you no longer need the tags or due to adjustments to the instance.**

Limits

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

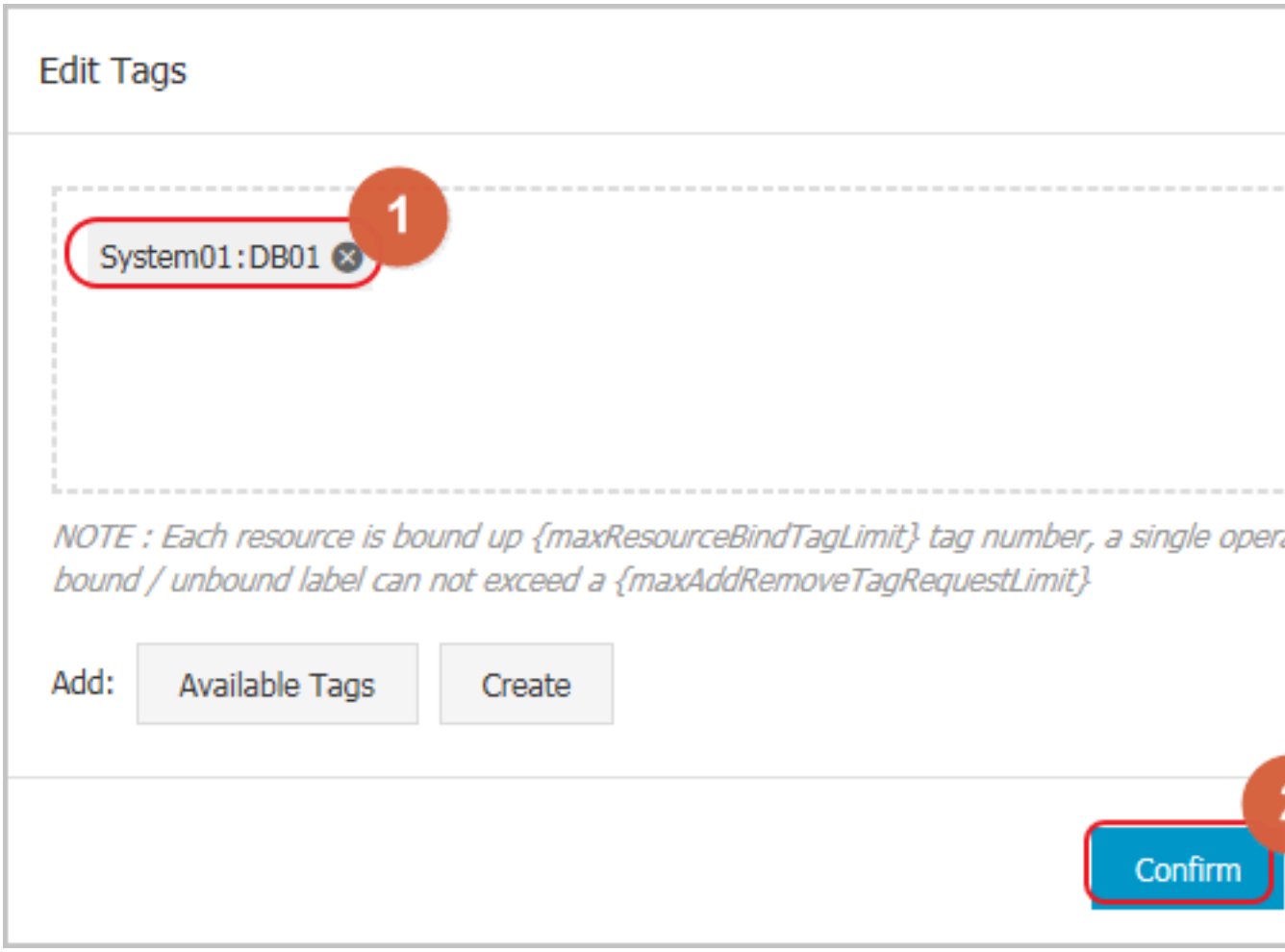
Procedure

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

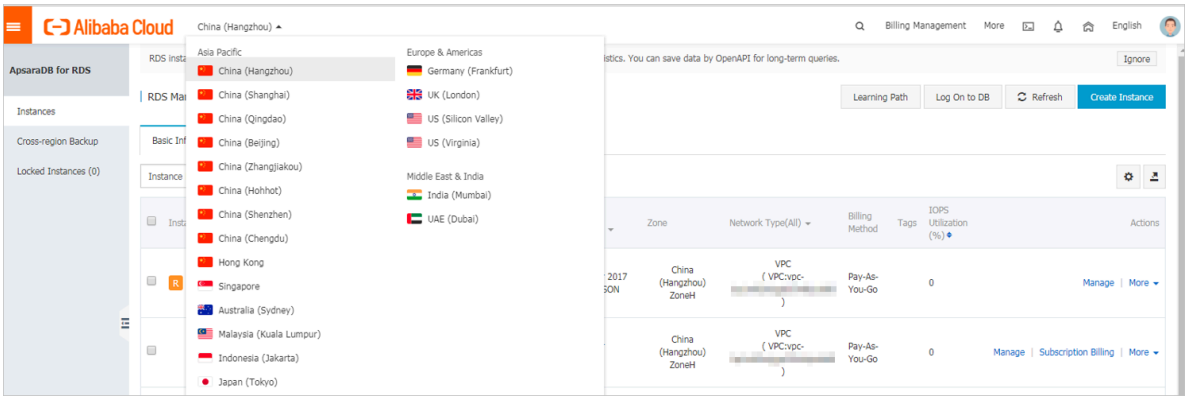
| API | Description |
| --- | --- |
| *#unique_133* | **Used to unbind a tag from an RDS instance.** |

## 18.3 Filter RDS instances by tag

**This topic describes how to filter RDS instances by tag.**

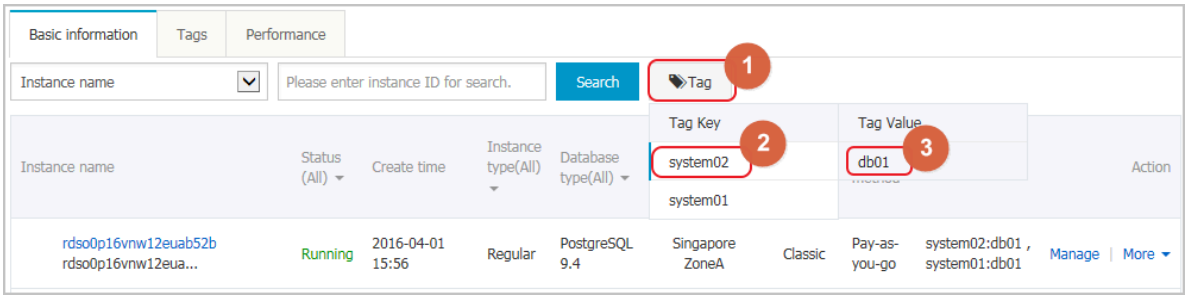
1. **Log on to the** *RDS console*.

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. |

# 19 Use the TimescaleDB plug-in

**The ApsaraDB RDS for PostgreSQL Basic Edition and ApsaraDB RDS for PostgreSQL Cluster Edition instances introduce the TimescaleDB 1.3.0 plug-in. The plug-in supports automatic sharding, efficient writing, retrieval, and near real-time aggregation of time-series data.**

**Currently, the TimescaleDB plug-in supported by ApsaraDB RDS for PostgreSQL 10 is an open-source edition and may not support some advanced features. For more information, see *TimescaleDB*.**

## Prerequisites

**You can directly use the TimescaleDB 1.3.0 plug-in in instances that are created after May 20, 2019. To use the TimescaleDB 1.3.0 plug-in in the instances that are created before May 20, 2019, you can restart these instances.**

**Note:**

**If you receive the following error message after restarting an instance:**

```
ERROR: could not access file "$libdir/timescaledb-0.8.0": No such
file or directory.
```

**Run the following SQL statement in the corresponding database to update the plug-in:**

```
alter extension timescaledb update;
```

## Add the TimescaleDB plug-in

**Use the pgAdmin client to *connect to an instance*. Run the following command to add the TimescaleDB plug-in:**

```
CREATE EXTENSION IF NOT EXISTS timescaledb CASCADE;
```

## Create a time-series table

1. **Create a standard table conditions, for example:**

```
CREATE TABLE conditions (
  time        TIMESTAMPTZ       NOT NULL,
  location    TEXT              NOT NULL,
  temperature DOUBLE PRECISION  NULL,
  humidity    DOUBLE PRECISION  NULL
```

```
);
```

2. **Create a time-series table, for example:**

```
SELECT create_hypertable('conditions', 'time');
```

**Note:**

**For more information about the statement, see** *Create a hypertable*.

Insert data into hypertables

**You can run standard SQL commands to insert data into hypertables, for example:**

```
INSERT INTO conditions(time, location, temperature, humidity)
  VALUES (NOW(), 'office', 70.0, 50.0);
```

**You can also insert multiple rows of data into a hypertable at a time, for example:**

```
INSERT INTO conditions
  VALUES
    (NOW(), 'office', 70.0, 50.0),
    (NOW(), 'basement', 66.5, 60.0),
    (NOW(), 'garage', 77.0, 65.2);
```

Retrieve data

**You can use advanced SQL queries to retrieve data, for example:**

```
-- Data is collected every 15 minutes in the past three hours and
sorted by time and temperature.
SELECT time_bucket('15 minutes', time) AS fifteen_min,
    location, COUNT(*),
    MAX(temperature) AS max_temp,
    MAX(humidity) AS max_hum
  FROM conditions
  WHERE time> NOW ()-interval '3 hours'
  GROUP BY fifteen_min, location
  ORDER BY fifteen_min DESC, max_temp DESC;
```

**You can also use built-in functions for analysis and query, for example:**

```
-- Query the median
SELECT percentile_cont(0.5)
  WITHIN GROUP (ORDER BY temperature)
  FROM conditions;
```

```
-- Query the moving average
SELECT time, AVG(temperature) OVER(ORDER BY time
      ROWS BETWEEN 9 PRECEDING AND CURRENT ROW)
    AS smooth_temp
  FROM conditions
  WHERE location = 'garage' and time > NOW() - interval '1 day'
  ORDER BY time DESC;
```

# 20 Logical subscriptions

**RDS for PostgreSQL provides a logical subscription function that supports one-way real-time synchronization at the table level between multiple RDS for PostgreSQL instances. This function can be used for data sharing, data aggregation, data splitting, and other business scenarios.**

**If you deploy your business in multiple regions across the country, you can use logical subscriptions to share data in different regions. For example, you can share the data in the data center to other regions, or aggregate data from other regions to the center for real-time analysis and query.**

**This topic describes how to use the logical subscription function. The following example describes the whole procedure:**

**Create a publication in the src database of the source instance, publish the public .t1 table, create a subscription named sub1_from_pub1 in the dst database of the destination instance, and subscribe to the public.t1 table that is in the source database.**

**For more information, see** *Logical subscriptions*.

Note

**You can implement logical subscriptions between two tables of a single instance or between two instances in the same VPC. For the logical subscriptions between two instances in the same VPC, you must use the internal endpoint.**

Prerequisites

- **Currently, only ApsaraDB RDS for PostgreSQL 10 Basic Edition supports logical subscriptions because of the network connectivity.**
- **The wal_level parameter of the instance must be set to logical for logical subscriptions. You can modify it on the Parameter Settings page. After you modify the parameter, you must restart the instance to make the changes take effect. A restart will disconnect the instance. Use caution when performing the instance restart and make sure that the restart does not affect your services.**
- **To implement logical subscriptions between two instances in the same VPC, you must add the IP CIDR block of the VPC to the whitelist of each instance.**

**For example, the IP CIDR block of the VPC is 172.16.0.0/16, you must add 172.16.0.0/16 to the whitelist. For more information, see** *Configure a whitelist*.

- **The account used to implement logical subscriptions must have the rds_superuser permission, such as a privileged account and accounts created by running the command:** `create role xxx with superuser`.

Procedures

**Create a new publication in the source database**

1. *Connect to the ApsaraDB RDS for PostgreSQL instance*.
2. **Run the following command to create a new publication in the source database:**

```
CREATE PUBLICATION <publication name> FOR TABLE <table name>;
```

**Examples**

```
create publication pub1 for table public.t1;
```

**Note:**

- **Only persistent base tables can be part of a publication. For more information, see** *CREATE PUBLICATION*.
- **You can query the publications of the current database by running the command:** `select * from pg_publication`.

**Create a subscription in the destination database**

1. *Connect to the ApsaraDB RDS for PostgreSQL instance*.
2. **This step takes the source database and the destination database in the same instance as an example. If you want to implement logical subscriptions between two instances, skip to step 3.**

   **Run the following command:**

```
select * from pg_create_logical_replication_slot('<subscription name
>','pgoutput');
```

3. **To create a new subscription in the destination database, run the following command:**

```
CREATE SUBSCRIPTION <subscription name>
    CONNECTION '<The connection string of the source instance>'
```

```
    PUBLICATION <The publication name of the source database>;
```

### Examples

```
create subscription sub1_from_pub1
connection 'host=pgm-xxxxx.pgsql.singapore.rds.aliyuncs.com port=
3433 user=test password=xxxxx dbname=src'
publication pub1 with (enabled, create_slot, slot_name='sub1_from_
pub1');
```

**Note:**

- **The connection string of the source database is in the following format:** `host = <VPC name of the source instance> port = <internal port of the source instance> user = <account that has the permission to publish tables in the source database> password = <account password to access the source instance > dbname = <source database name> .`
- **If the source database and destination database are in the same instance, you need to specify** `host = localhost`, `create_slot = false`**. The port number can be queried by running the** `show port` **command. By default, the port number is 3002.**
- **You can run** `select * from pg_sub` **to query all the subscriptions of the database cluster.**
- **You can add relevant subscription parameters after the publication name of the source database by using with statements. For more information, see** *Create subscription*.