Alibaba Cloud ApsaraDB for MySQL

Quick Start for PPAS

Issue: 20190813

Legal disclaimer

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

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

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

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

Generic conventions

Table -1: Style conventions

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

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

Contents

1 Limits

To guarantee the instance stability and security, ApsaraDB for PPAS has the following restrictions.

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

2 General procedure to use RDS

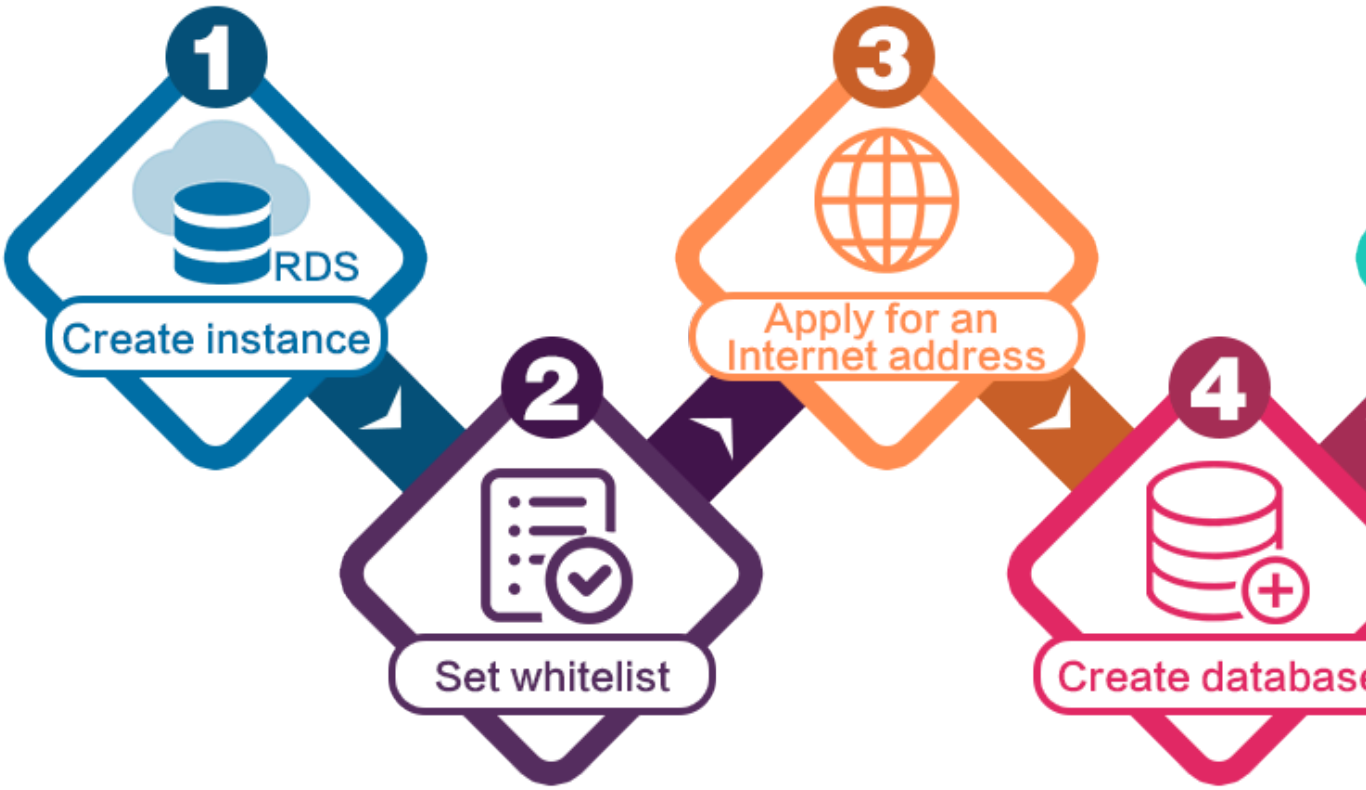
Purpose of the quick start

This document describes the procedure right from purchasing an RDS instance to using it. It also elaborates how to create an ApsaraDB for RDS instance, perform basic settings, and connect to the instance database.

Quick start flowchart

If you use Alibaba Cloud ApsaraDB for RDS for the first time, see Limits.

The following diagram explains the steps you must follow right from creating an instance to using it.



3 Create an RDS for PPAS instance

You can use the RDS console or APIs to create an RDS instance. For more information about instance pricing, see Pricing of ApsaraDB for RDS. This topic describes how to use the RDS console to create an instance. For more information about how to use the APIs to create an instance, see CreateDBInstance.

Prerequisites

- You have registered an Alibaba Cloud account.

Precautions

- Subscription instances cannot be converted to Pay-As-You-Go instances.
- Pay-As-You-Go instances can be converted to Subscription instances. For more information, see Change the billing method.
- An Alibaba Cloud account can create up to 30 Pay-As-You-Go RDS instances. You can open a ticket to apply for increasing the limit.

Procedure

1. Log on to the RDS console.
2. On the Instances page, click Create Instance.
3. Select Subscription or Pay-As-You-Go. For more information about the billing method, see Billing items and billing methods.
4. Set the following parameters.

Parameter	Description
Region	Indicates the location of the RDS instance you want to purchase. You cannot change the region once you confirm your order. - Select the region closest to your users to increase the access speed. - Select the region where your ECS instance is located so that the ECS instance can access the RDS instance through the intranet. If the ECS instance and RDS instance are located in different regions, they can communicate only through the Internet and hence performance is degraded.

Parameter	Description
Database Engine	The supported database engines are MySQL, Microsoft SQL Server, PostgreSQL, PPAS (compatible with Oracle), and MariaDB TX. In this example, select PPAS (compatible with Oracle). Note: The available database engines vary depending on the region you select.
Version	For RDS for PPAS, the supported versions are PPAS 9.3 and PPAS 10. Note: The available versions vary depending on the region you select.
Edition	Select High-availability. This edition adopts the high-availability architecture with one master node and one slave node. Note: The available product series vary depending on the region you select. For more information on the product series, see Product series overview.
Zone	A zone is a physical area within a region. Different zones in the same region are basically the same. You can deploy the master and slave nodes of your RDS instance in the same zone or in different zones.
Network Type	· Classic Network: indicates a traditional network. · VPC (recommended): short for Virtual Private Cloud. A VPC is an isolated network environment and therefore provides higher security and performance than a classic network. Note: Make sure the network type of the RDS instance is the same as that of your ECS instance so that the ECS instance can access the RDS instance through the intranet.

Parameter	Description
Type	Indicates the specifications of the RDS instance. Each instance type supports a specific number of CPU cores, memory size, maximum number of connections, and maximum IOPS. For more information, see Instance type list. RDS for PAAS supports the following instance type families: · General-purpose instance: owns dedicated memory and I/O resources, but shares CPU and storage resources with the other general-purpose instances on the same server. · Dedicated instance: owns dedicated CPU, memory, storage, and I/O resources. · Dedicated host: owns all the CPU, memory, storage, and I/O resources on the server where it is located. For example, 8 Cores 32 GB (Basic) indicates a general-purpose instance, and 8 Cores 32 GB (Dedicated) indicates a dedicated instance.
Capacity	Used for storing data, system files, binlog files, and transaction files.

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

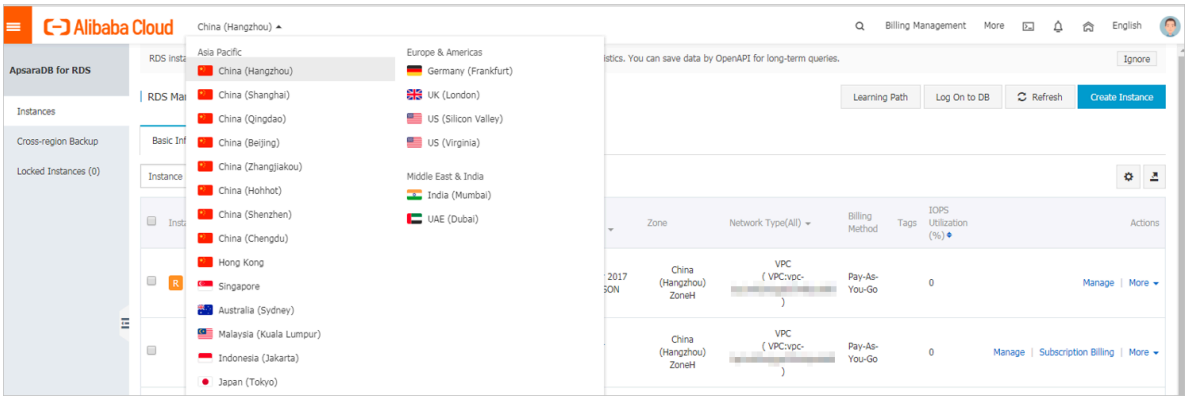
   Note:
   For a Subscription instance, you can:

   · Select Auto Renew in the Duration section. Then the system can automatically deduct fees to extend the validity period of your instance. For example, if you purchase a three-month Subscription instance with Auto Renew selected, the system automatically deducts 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, review the order information, select Terms of Service, Service Level Agreement, and Terms of Use, click Pay Now, and complete the payment.

What to do next

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



2. Configure a whitelist.
3. Create accounts.
4. Apply for an Internet address (if you want to access the RDS instance through the Internet).
5. Connect to the RDS instance.

APIs

API	Description
CreateDBInstance	Used to create an RDS instance.

4 Initial configuration

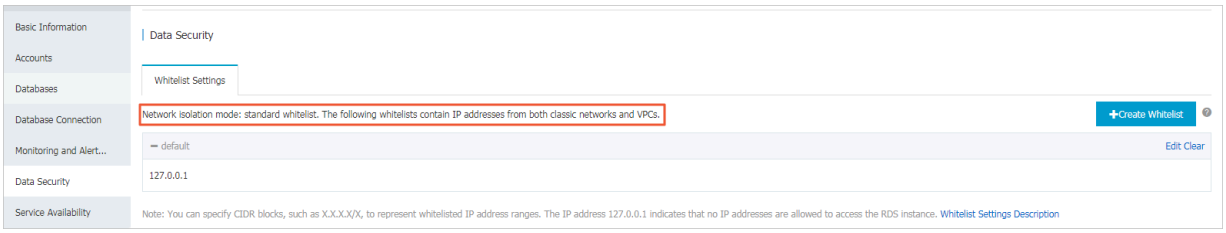
4.1 Configure a whitelist

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

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

Precautions

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



Note:

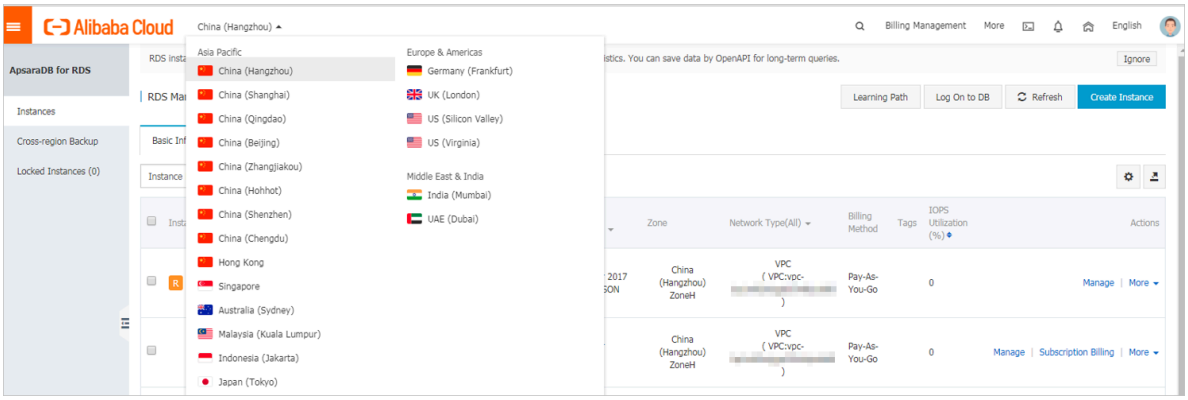
The internal networks to which RDS instances belong are divided into two types: classic network and VPC.

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

Procedure

Enhanced whitelist

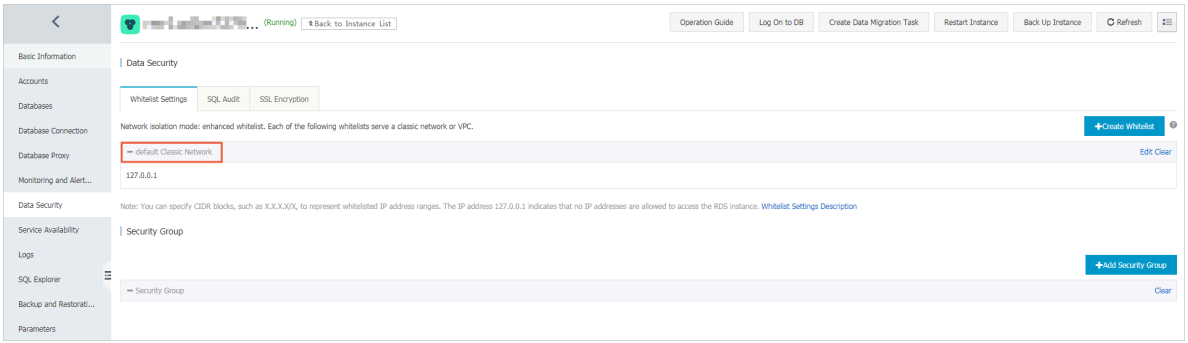
1. Log on to the RDS console.
2. In the upper-left corner, select the region where the target instance is located.



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

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

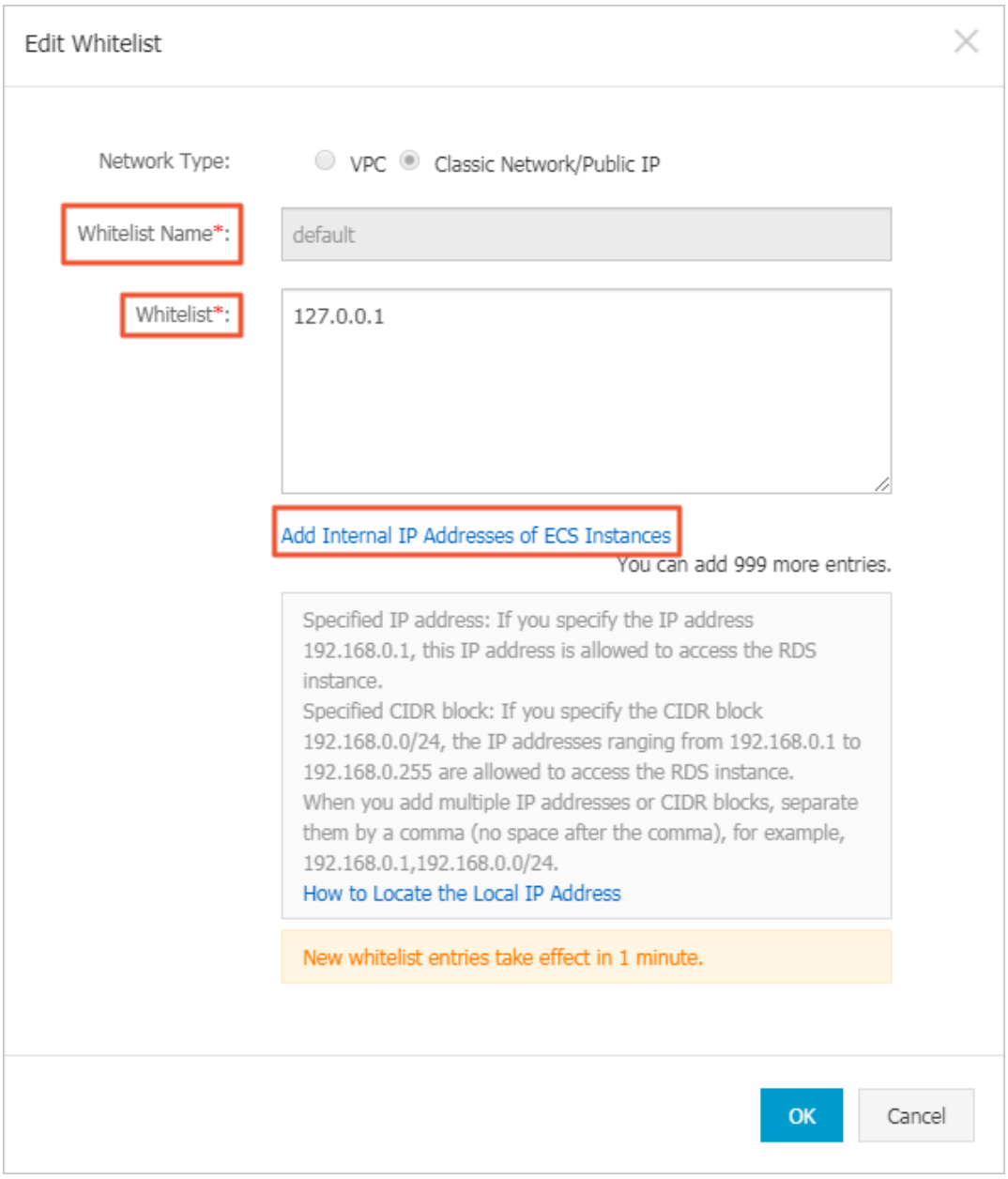
- You can also click Create Whitelist. In the displayed Create Whitelist dialog box, select VPC or Classic Network/Public IP.



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

 **Note:**

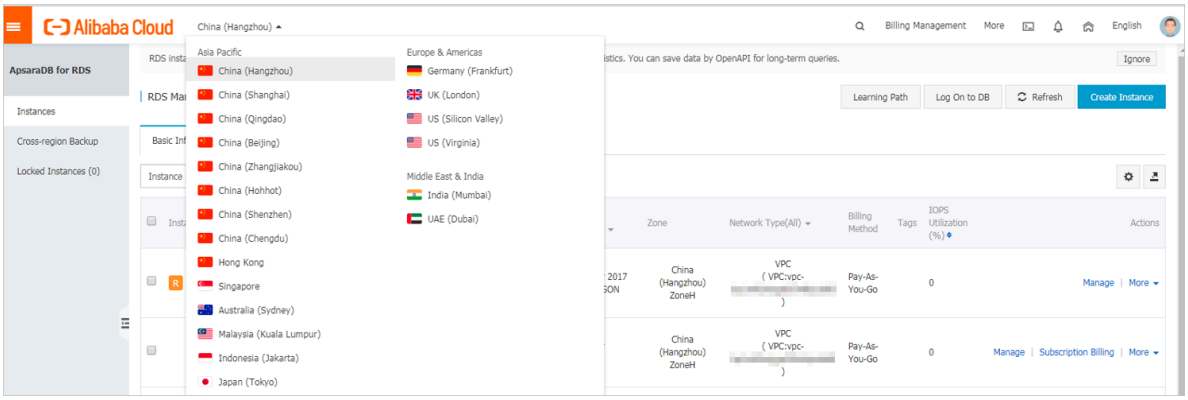
After you add an IP address or CIDR block to the default whitelist, the default address 127.0.0.1 is automatically deleted.



Standard whitelist

1. Log on to the RDS console.

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



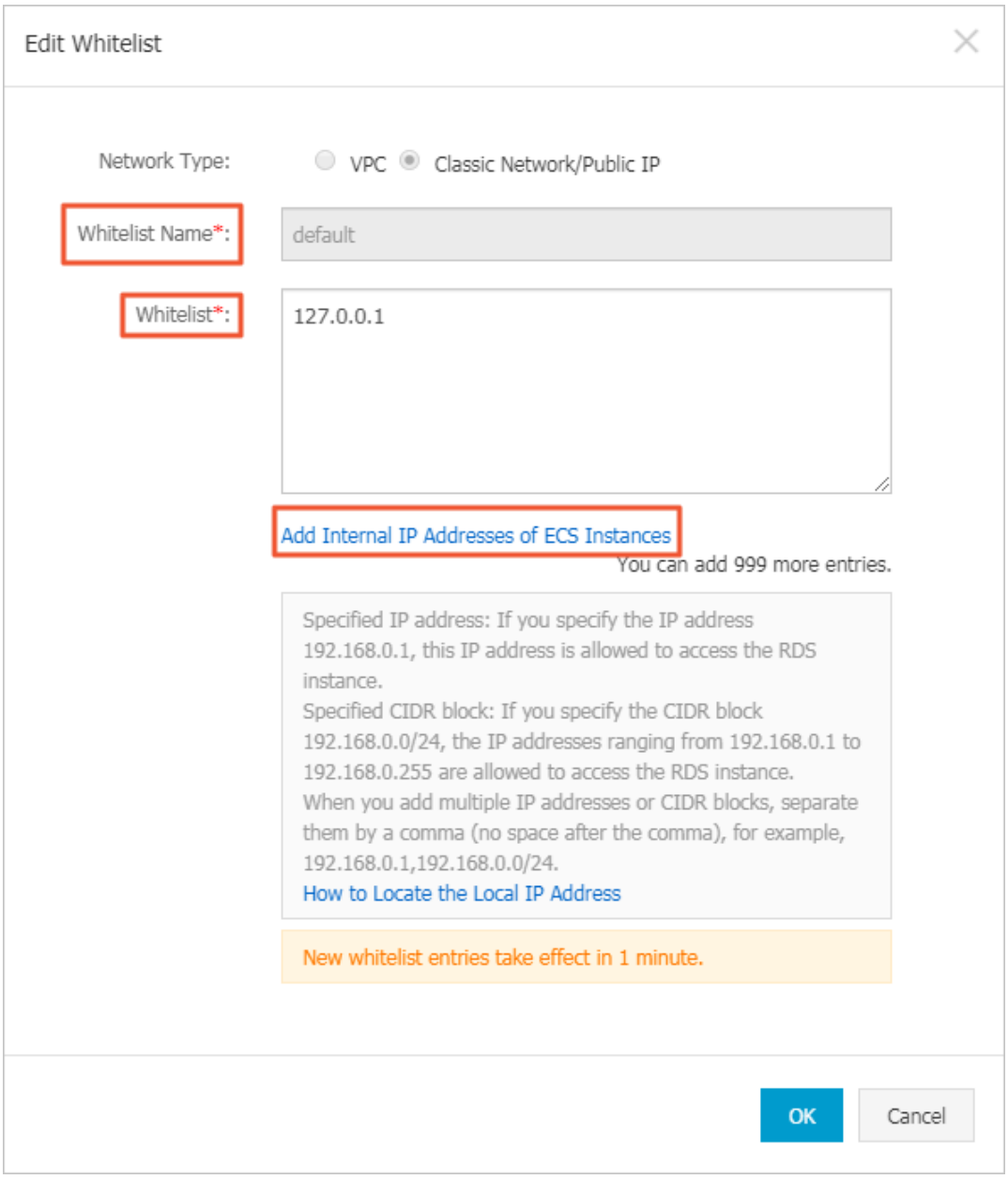
3. Find the target instance and click its ID.
4. In the left-side navigation pane, click Data Security.
5. On the Whitelist Settings tab page, click Edit corresponding to the default whitelist.

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

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

> **Note:**

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



Common errors

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

Note:

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

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

  For more information, see How do I find the public IP address of my computer that needs to connect to RDS for MySQL or MariaDB TX?.

APIs

API	Description
DescribeDBInstanceIPArrayList	Used to view the IP address whitelist of an RDS instance.
ModifySecurityIps	Used to modify the IP address whitelist of an RDS instance.

4.2 Apply for an Internet address

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

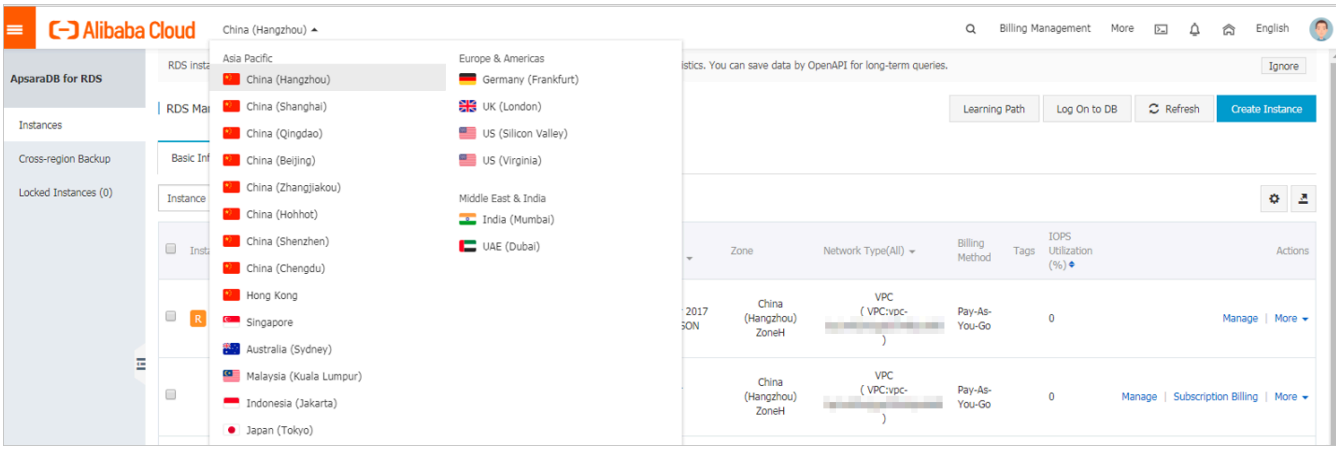
Intranet and Internet addresses

Address Type	Description
Intranet address	The intranet address is generated by default. Use the intranet address if all of the following conditions are met: · Your application is deployed on an ECS instance. · The ECS instance is located in the same region as your RDS instance. · The ECS instance has the same network type as your RDS instance. We recommend that you use the intranet address to access your RDS instance because this is more secure and delivers optimal performance.
Internet address	You need to manually apply for the Internet address. You can also release it anytime. Use the Internet address if you cannot access RDS through the intranet. Specific scenarios are as follows: · An ECS instance accesses your RDS instance but the ECS instance is located in a different region or has a network type different from your RDS instance. · A server or computer outside Alibaba Cloud accesses your RDS instance. Note: · The Internet address and traffic are currently free of charge. · Using the Internet address reduces security. Please exercise caution . · To ensure high security and performance, we recommend that you migrate your application to an ECS instance that is in the same region and has the same network type as your RDS instance and then use the intranet address.

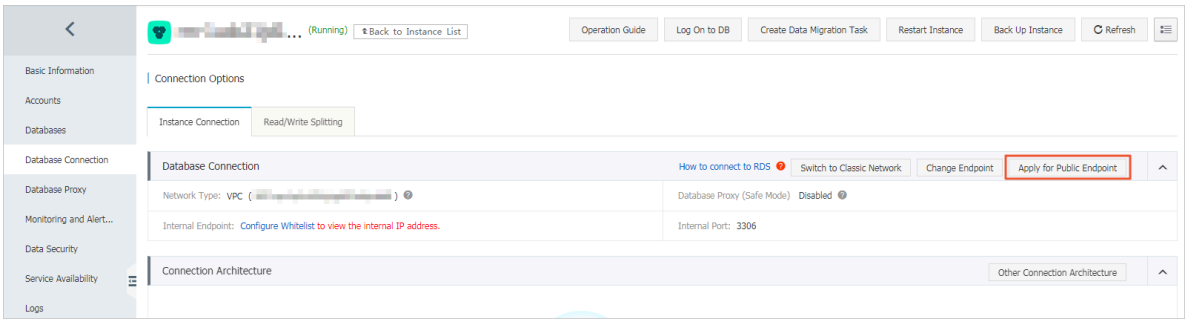
Procedure

1. Log on to the RDS console.

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



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



6. In the displayed dialog box, click OK.

   The Internet address is generated.

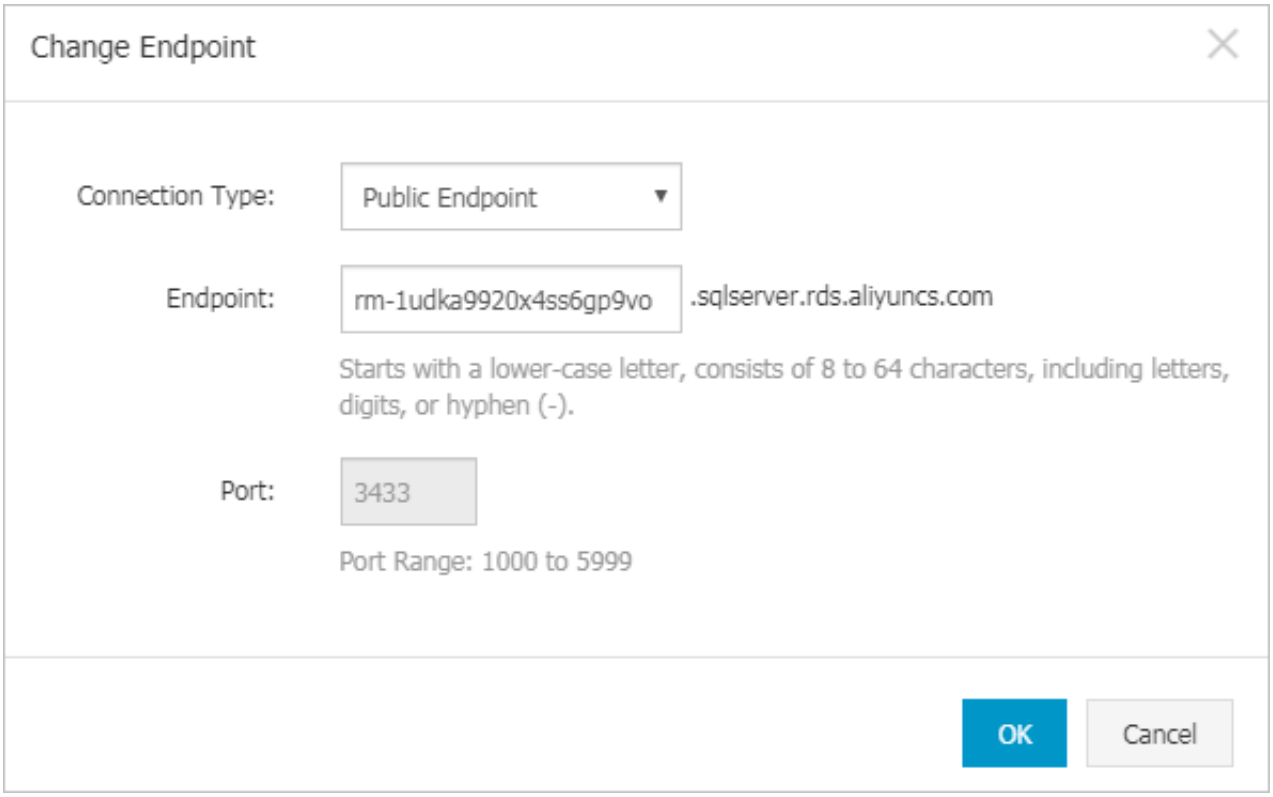
7. Optional. If you want to change the Internet address or port number, click Change Endpoint. In the displayed dialog box, set the Internet address and port number and click OK.

   - Connection Type: Select Public Endpoint.

   Note:

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

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



APIs

API	Description
AllocateInstancePublicConnection	Used to apply for an Internet address for an RDS instance.

4.3 Create databases and accounts

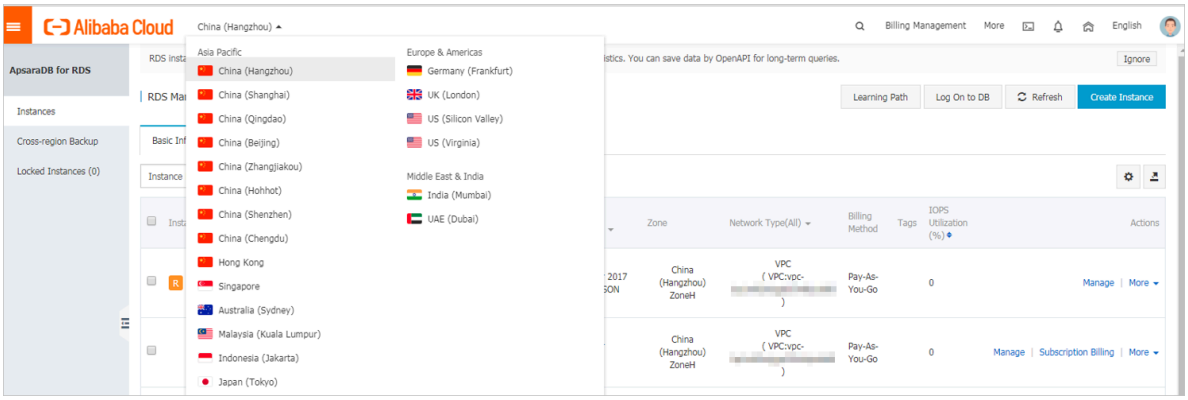
Before using RDS, you must create databases and accounts for your RDS instance. For PPAS instances, you must create an initial account on the RDS console. And then you can create and manage databases through a client. This topic takes the pgAdmin 4 client as an example to introduce how to create databases and accounts for PPAS instances.

Precautions

- Databases under a single instance share all the resources of this instance. Each PPAS instance supports one initial account, countless general accounts, and countless databases. You must create and manage common accounts and databases through SQL statements.
- To migrate your local database to an RDS instance, you must create the same databases and accounts for the RDS instance as your local database.
- When assigning account permissions for each database, follow the minimum permission' principle and consider service roles to create accounts. Alternatively , 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.

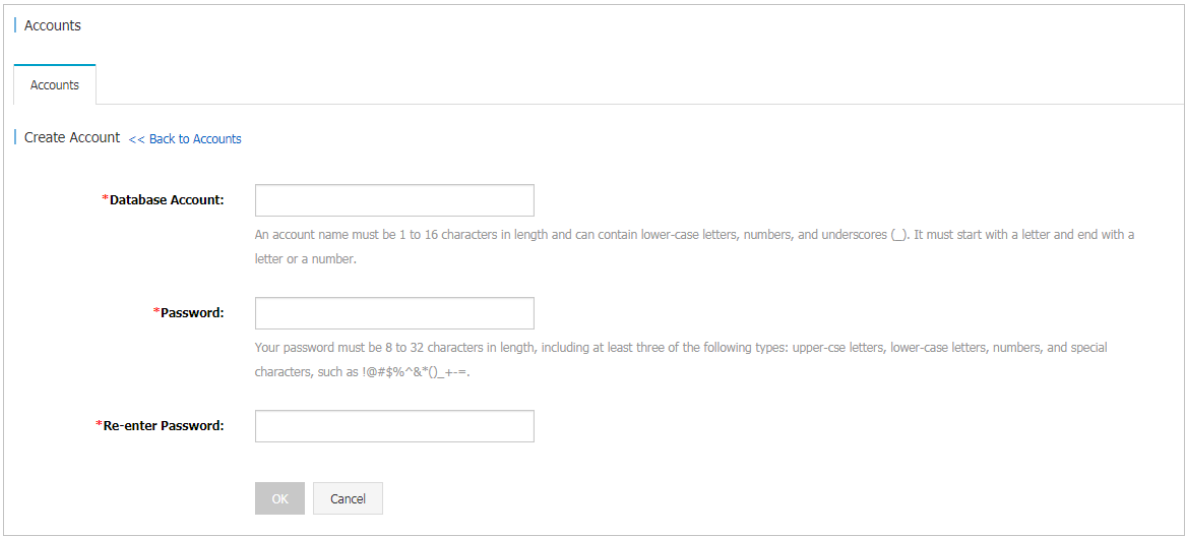
Procedure

1. Log on to the RDS console.
2. Select the region where the target instance is located.



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

6. Enter the account information.



Parameter description:

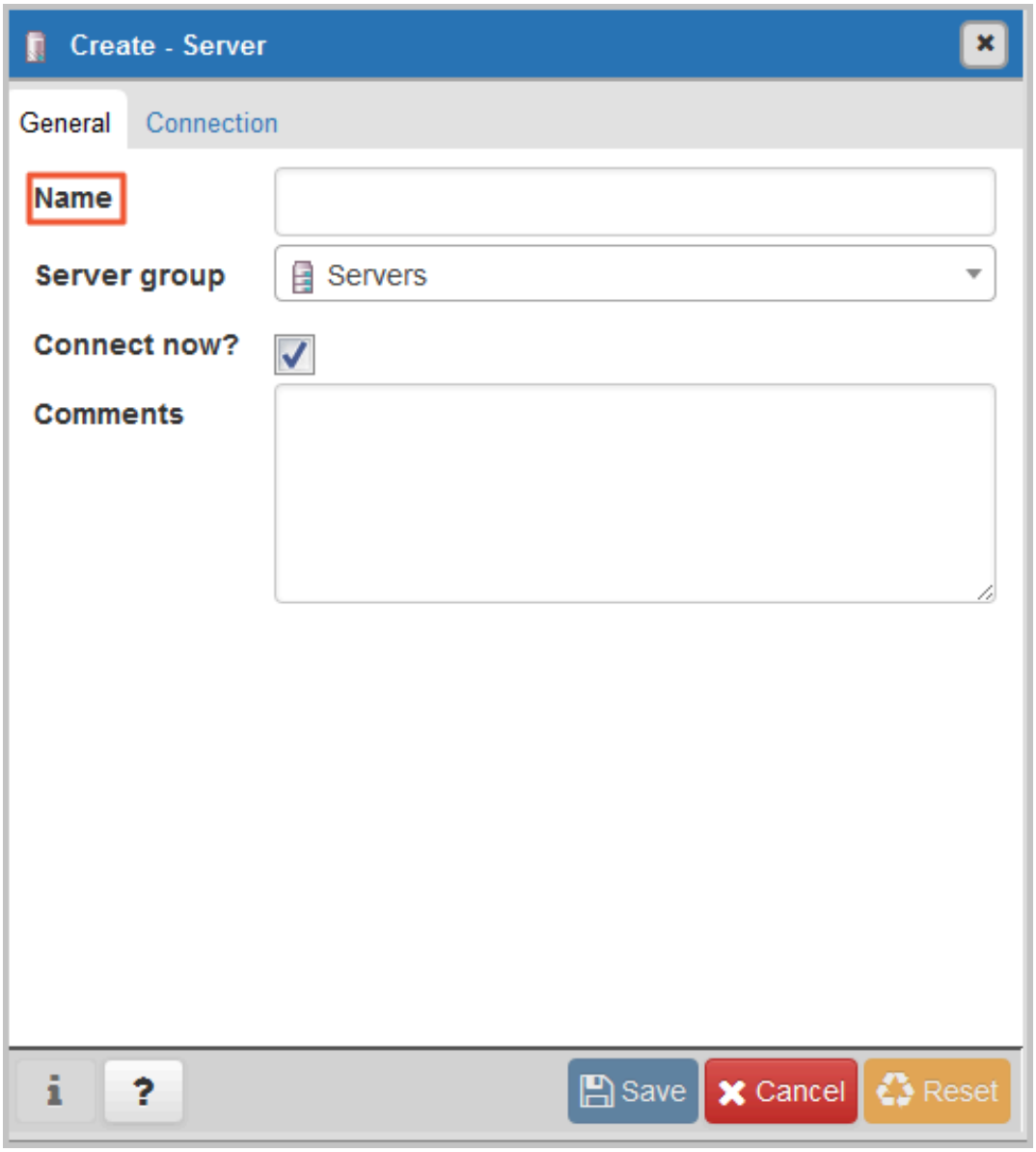
- Database Account: the name of the initial account. It contains 2 to 16 characters including the lowercase letters, digits, or underscores (_). It must begin with a letter and end with a letter or digit.
- Password: the password of the initial account. It contains 8 to 32 characters including at least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

  ! @ # $ % ^ & * ( ) _ + - =
- Re-enter Password: Re-enter the password to make sure that the password is entered correctly.

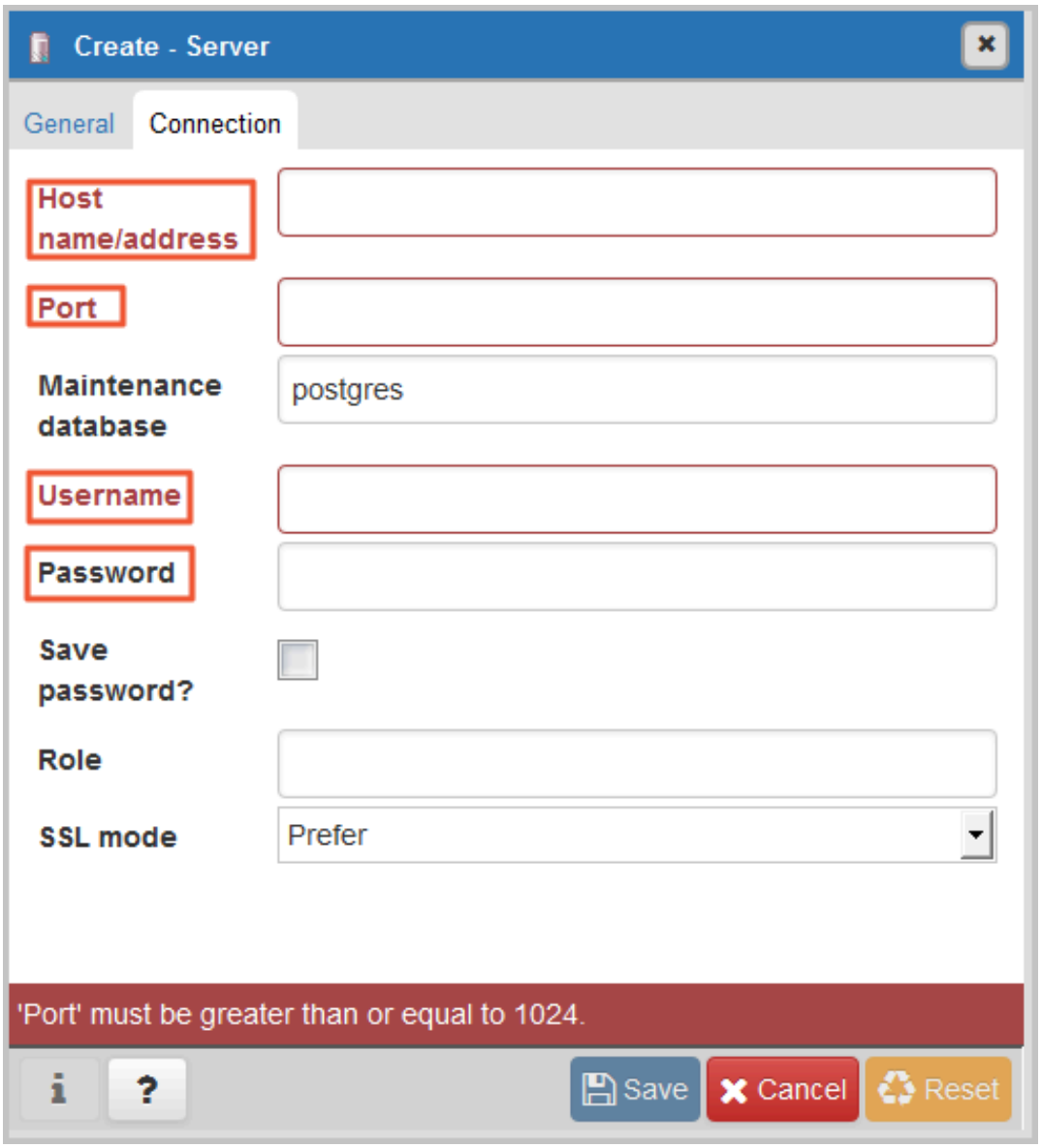
7. Click OK.
8. Add the IP address that is allowed to access the RDS instance to the RDS whitelist. For more information about how to configure a whitelist, see Configure a whitelist.
9. Start the pgAdmin 4 client.

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

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



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

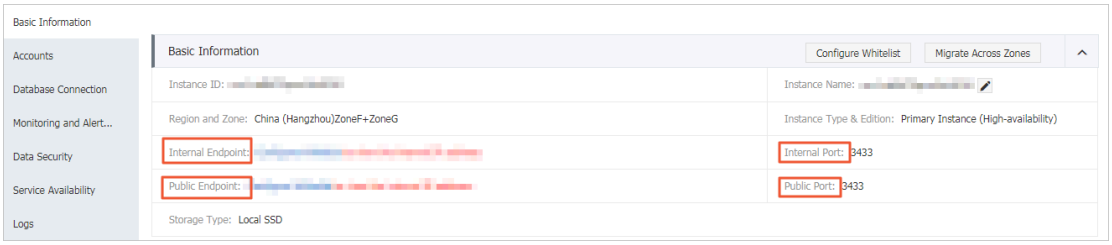


Parameter description:

- Host name/address: the connection address of the RDS instance. If your application accesses the RDS instance through the intranet, enter the intranet IP address of the RDS instance. If your application accesses the RDS instance through the Internet, enter the Internet IP address of the RDS instance. The

following procedure shows how to find the connection address and port number of the RDS instance:

a. Log on to the RDS console.
b. Select the region where the target instance is located.
c. Find the target instance and click its ID.
d. On the Basic Information page, find the Internet/intranet IP address and Internet/intranet port number of the instance.

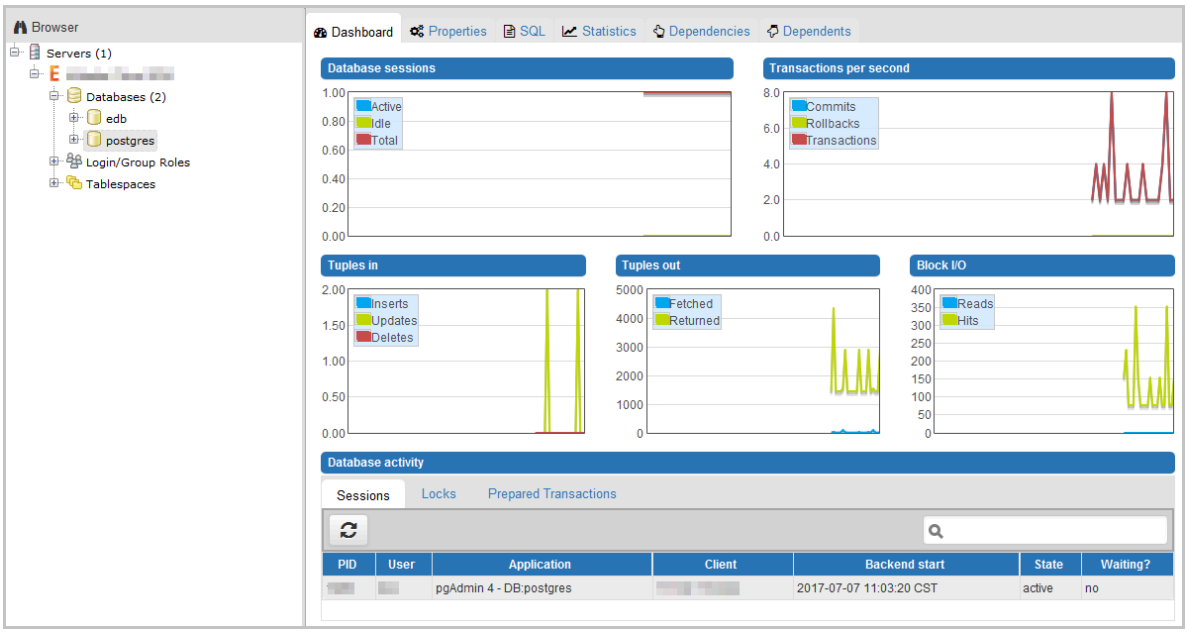


- Port: the port number of the RDS instance. If your application accesses the RDS instance through the intranet, enter the intranet port number of the RDS instance. If your application accesses the RDS instance through the Internet, enter the Internet port number of the RDS instance.
- Username: the name of the initial account name for the RDS instance.
- Password: the password of the initial account for the RDS instance.

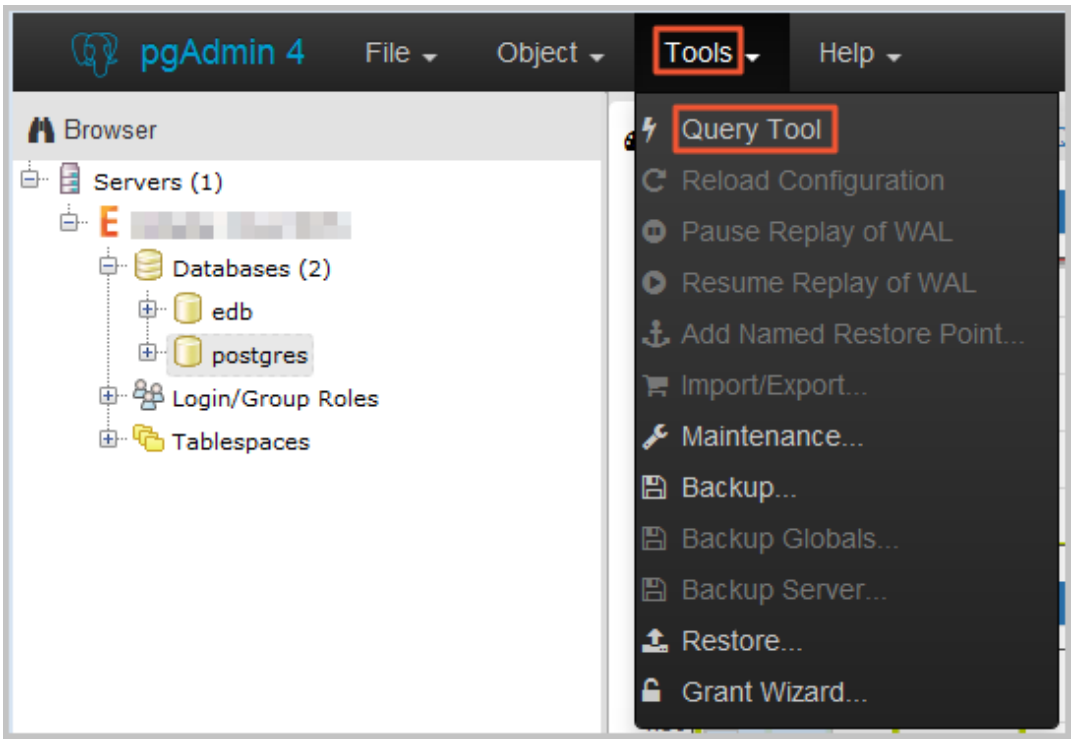
13. Click Save.
14. If the connection information is correct, choose Servers > server name > Databases > edb or postgres. The following page is displayed, which indicates that the connection to the RDS instance is successful.

Note:

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

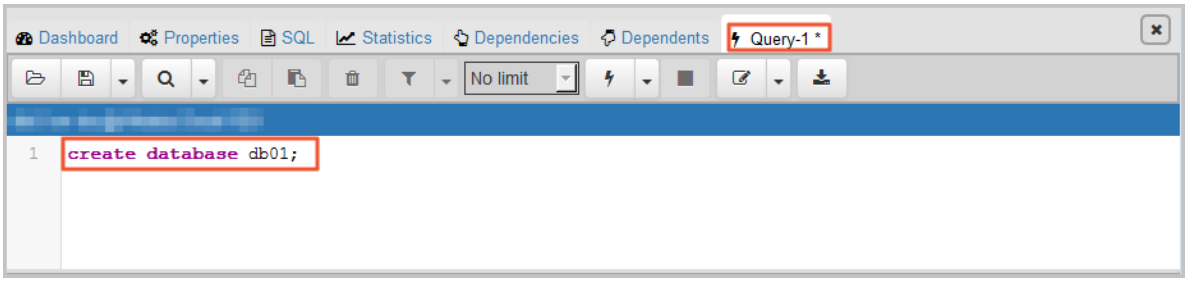


15.Double-click postgres and choose Tools > Query Tool.

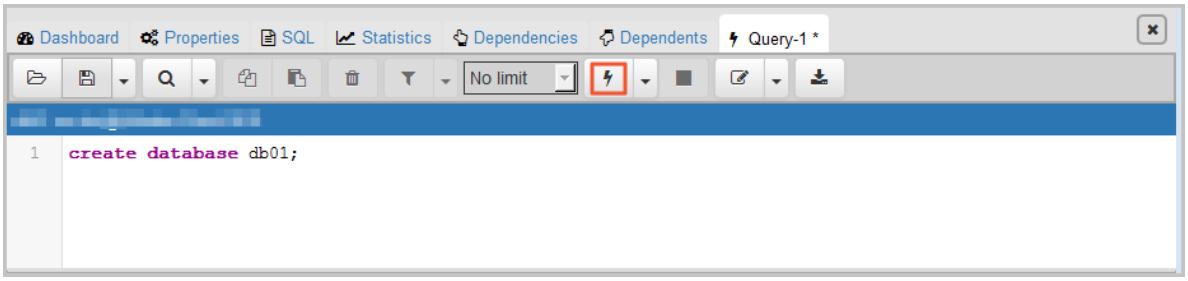


16. Enter the following command on the Query-1 tab page to create a database:

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

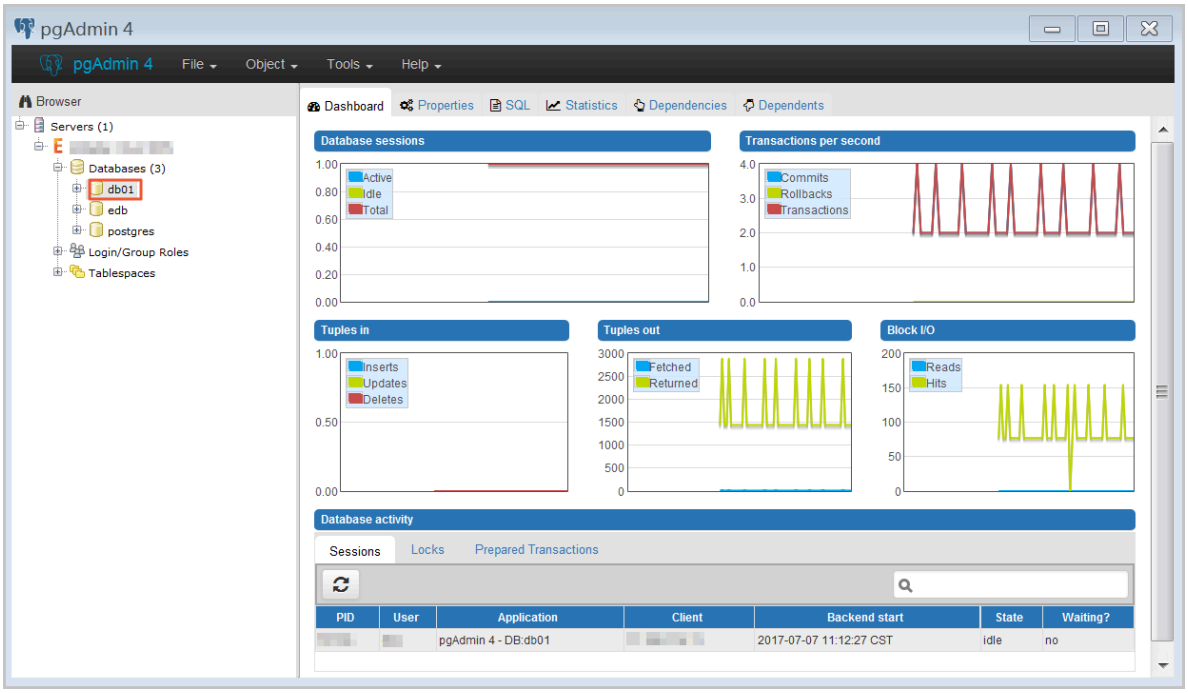


17. Click Execute/Refresh, as shown in the following figure.



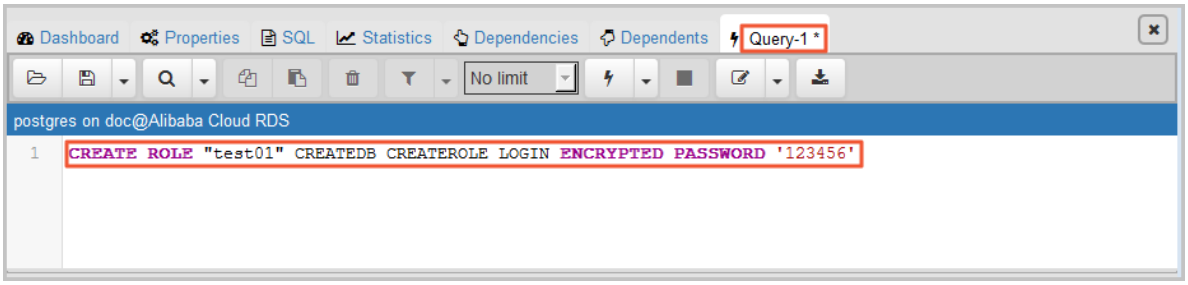
If the execution is successful, the new database is created.

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

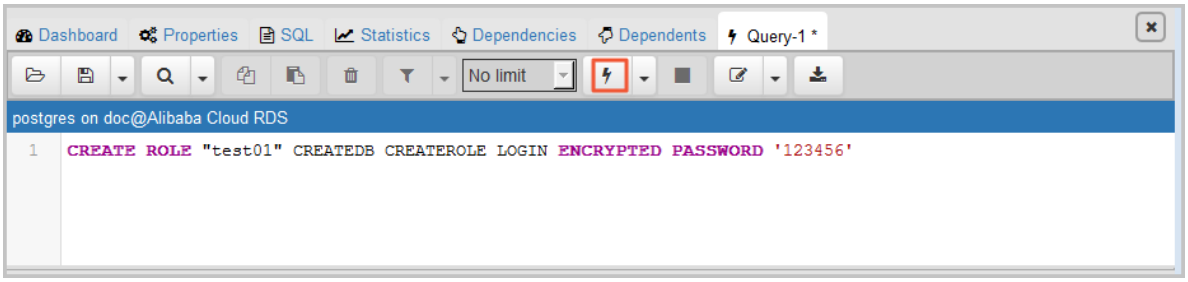


19. Enter the following command on the Query-1 tab page to create an account:

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

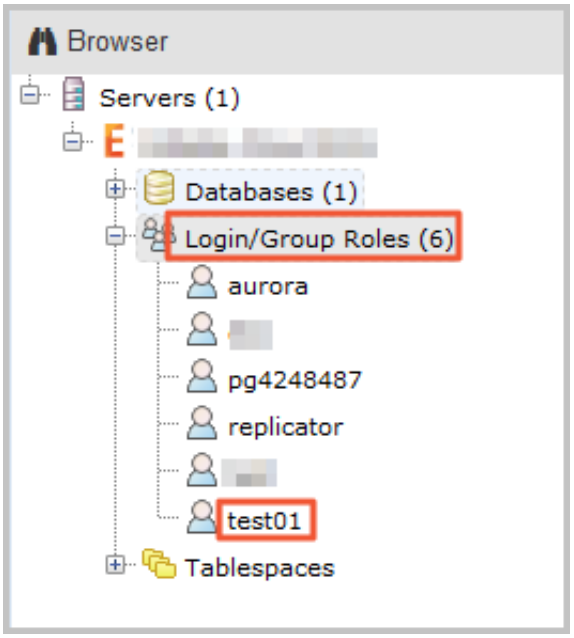


20. Click Execute/Refresh, as shown in the following figure.



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

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



FAQ

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

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

APIs

API	Description
CreateAccount	Used to create an account.

5 Connect to an instance

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

Background information

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

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

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

Use DMS to connect to an RDS instance

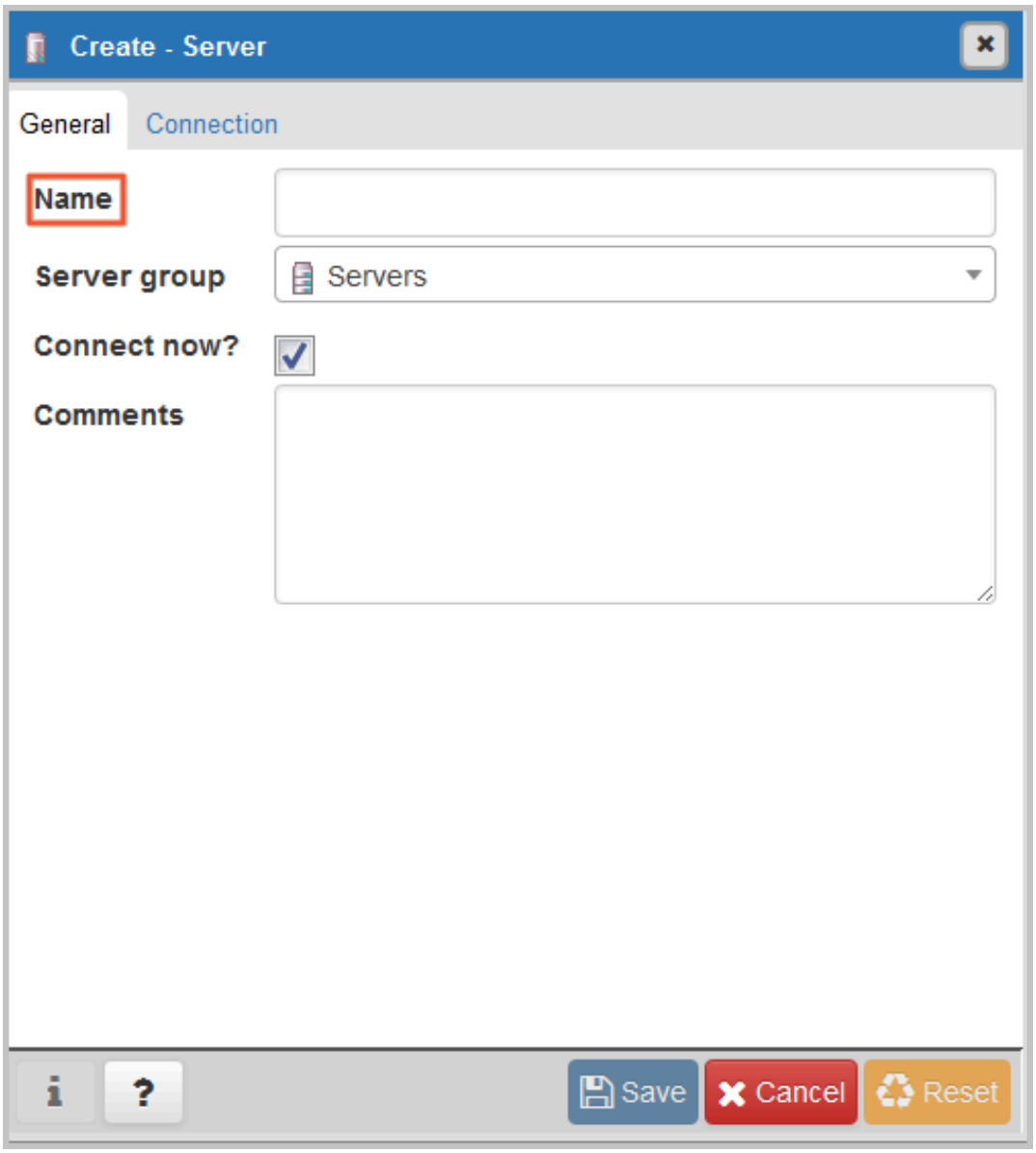
For more information about how to connect to an RDS instance through DMS, see Log on to the RDS database through DMS.

Use a client to connect to an RDS instance

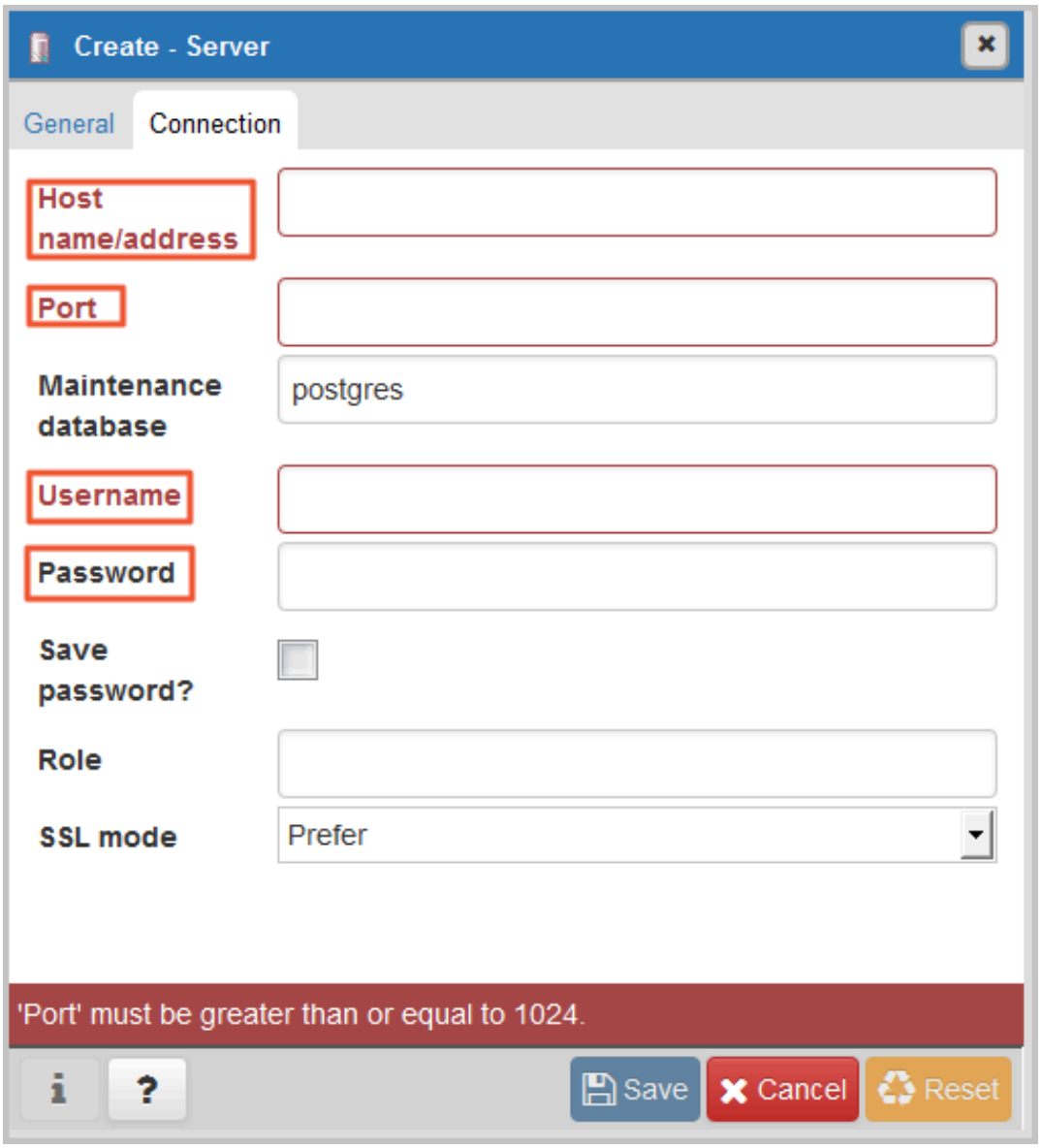
1. Add the IP address that is used to access the RDS instance to the RDS whitelist. For more information about how to configure a whitelist, see Configure a whitelist.
2. Start the pgAdmin 4 client.

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

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



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

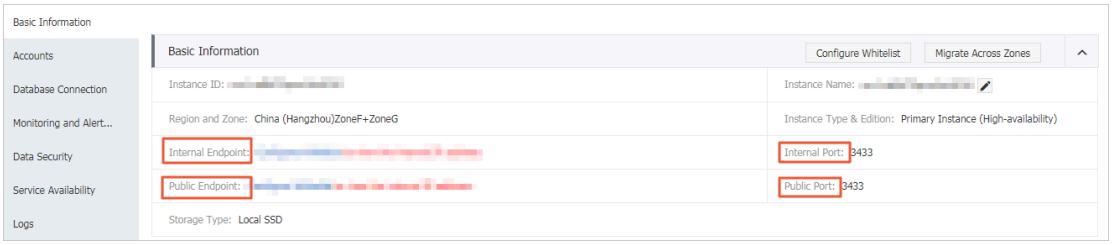


Parameter description:

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

the connection address and the port information of the RDS instance, take these steps:

a. Log on to the RDS console.
b. In the upper-left corner, select the region where the target instance is located .
c. Find the target instance and click its ID.
d. On the Basic Information page, find the Internet/intranet IP address and Internet/intranet port number of the instance.

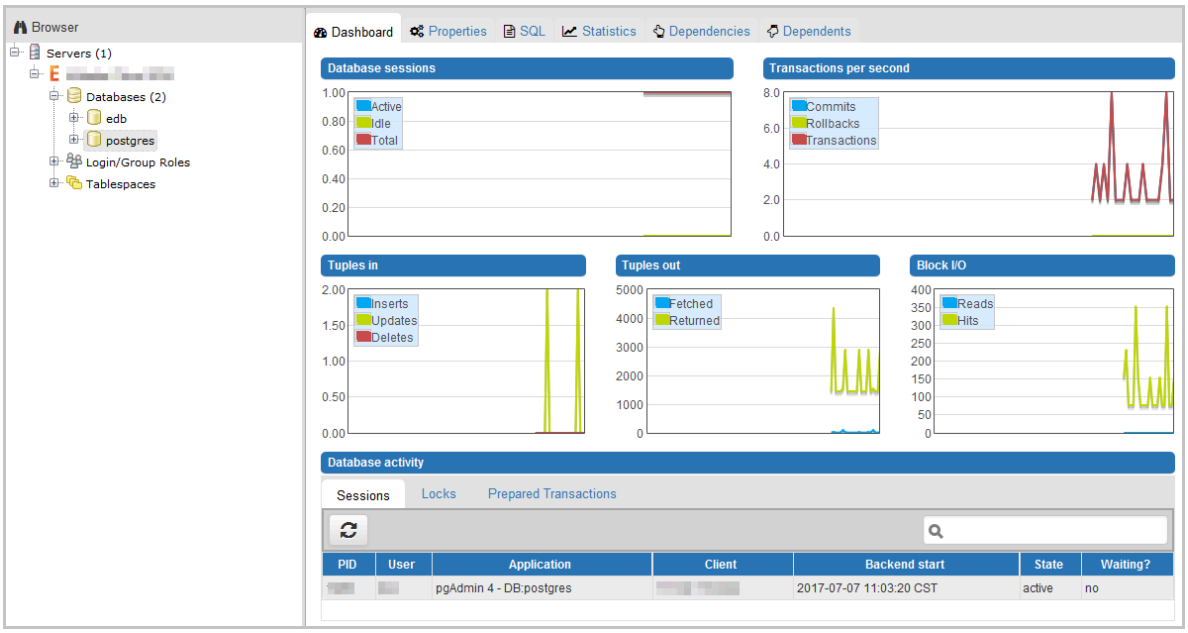


- Port: the port number of the RDS instance. If it is an internal connection, enter the port number for internal connections. If it is an external connection, enter the port number for external connections.
- Username: the name of the initial account name for the RDS instance.
- Password: the password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

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

Note:

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



6 Read/write external data files using oss_fdw

In Alibaba Cloud, you can use oss_fdw plugin to load data on OSS to PostgreSQL and PPAS databases, and you can also write data in a database 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 the intranet
- 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 adjust 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 parameter values are used, a timeout error occurs when the transmissi on 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, filepath, filepath.1, filepath.2, filepath.3, and filepath.5.

    The first four files are matched and imported, but the file named filepath.5 is not .
- dir: Virtual directory on OSS.
  - dir must end with a slash (/).
  - All files (excluding subfolders and files in subfolders) in the virtual directory indicated by dir 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. Value range:
  - none: Uncompressed (default value)
  - gzip: compressed gzip file

- compressionlevel: Used to set the compression level of the compression format written to OSS, ranging from 1 to 9. The default value is 6.

 Note:

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

Export mode parameters for CREATE FOREIGN TABLE

oss_flush_block_size and oss_file_max_size are added for the export mode.

- 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.

 Note:
oss_flush_block_size and oss_flush_block_size are invalid for the import mode.

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_li  st_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_o  ne_file  = ' oss_test / test . gz .  2 ';
 select  *  from   oss_fdw_li  st_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_ERRO  RS  ' 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 the reference links at the end of this document.
- If the error "oss endpoint userendpoint not in aliyun white list" is triggered during reading of SQL statements for external tables, use these 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.

For more information about error types, see the reference links at the end of this document. Timeout errors can be handled using oss_ext parameters.

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

Hide ID and key

If ID and key parameters for CREATE SERVER are not encrypted, plaintext information is displayed 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 =
MD5xxxxxxx x , key = MD5xxxxxxx x , 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.

7 Apply for an Internet address

If your application is deployed on the ECS instance that is located in the same region and has the same network type as your RDS instance, you do not need an Internet address. If your application is deployed on the ECS that is located in the different region or has the different network type from those of your RDS instance, or on a platform other than Alibaba Cloud, an Internet address is necessary to access an RDS instance.

Note:

When instances are in the same region (their zones can be different), they can access each other through the intranet.

Background information

RDS supports connections through the intranet and Internet. The access mode and instance type of the instance determine available connection types.

Instance series	Instance version	Access mode	Connection address
Basic Edition	· MySQL 5.7 · SQL Server 2016 Web Basic Edition/2012 Web Basic Edition/2012 Enterprise Basic Edition · PostgreSQL 10	Standard whitelist mode	· Intranet address · Internet address · Intranet and Internet addresses

Instance series	Instance version	Access mode	Connection address
High-availability Edition	· MySQL 5.5/5.6/5.7 · SQL Server 2008 R2/2016 Standard High-availability Edition/2012 Standard High-availability Edition/2016 Enterprise High-availability Edition/2012 Enterprise High-availability Edition · PostgreSQL 9.4 · PPAS 10	Standard whitelist mode	· Intranet address · Internet address
		Enhanced whitelist mode	· Intranet address · Internet address · Intranet and Internet addresses
Finance Edition	MySQL 5.6	Standard whitelist mode	· Intranet address · Internet address
		Enhanced whitelist mode	· Intranet address · Internet address · Intranet and Internet addresses

The applicable scenarios of the connection addresses are as follows:

· Use the intranet address only:

  - The system provides an intranet address by default and you can directly modify the connection address.
  - This condition is applicable when your application is deployed on an ECS instance that is located in the same region and has the same network type as your RDS instance.

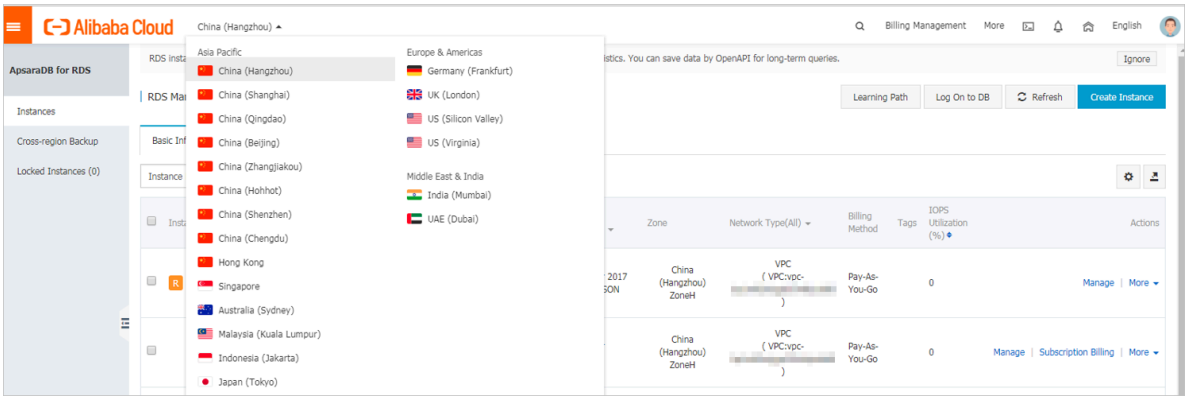
- Use the Internet address only:
  - This condition is applicable when your application is deployed on an ECS instance that is located in the different region from that of your RDS instance.
  - This condition is applicable when your application is deployed on a platform other than Alibaba Cloud.
- Use both intranet and Internet addresses:
  - This scenario is applicable when your application is deployed on an ECS instance that is located in the same region and has the same network type as your RDS instance, and application modules are deployed in an ECS where your RDS instance is not located.
  - This scenario is applicable when your application is deployed on an ECS instance that is located in the same region and has the same network type as your RDS instance, and on a platform other than Alibaba Cloud.

Precautions

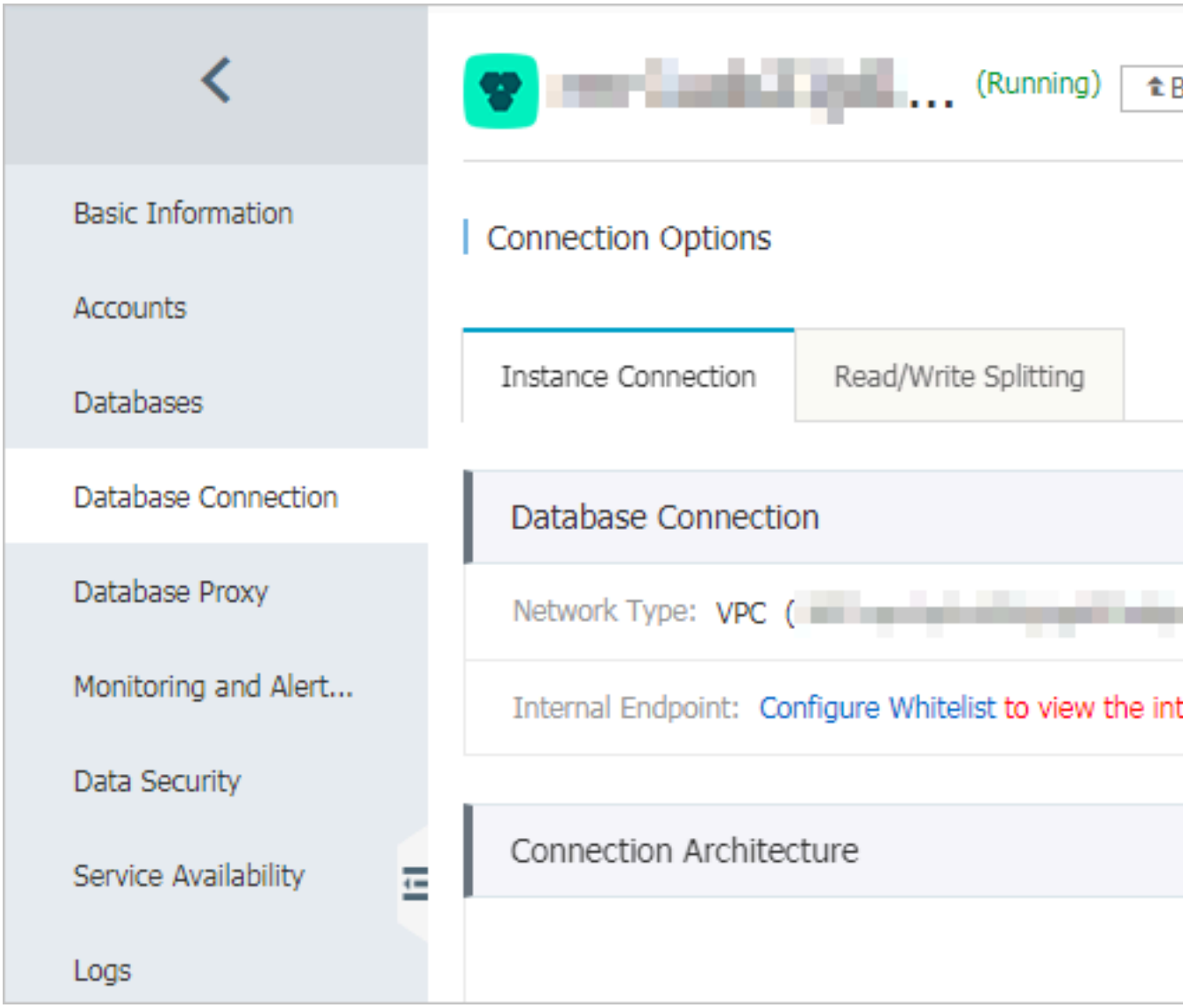
- Before accessing the database, you must add the addresses or CIDR blocks to a whitelist. For more information, see Set the whitelist.
- Traffic fees are charged for connections through Internet. For more information about pricing and fees charging, see RDS Pricing.
- Connecting the RDS instance through an Internet address may reduce the instance security. Proceed with caution. To get a higher transmission rate and a higher security level, we recommend that you migrate your applications to an ECS instance that is in the same region as your RDS instance.

Procedure

1. Log on to the RDS console.
2. Select the region where the target instance is located.

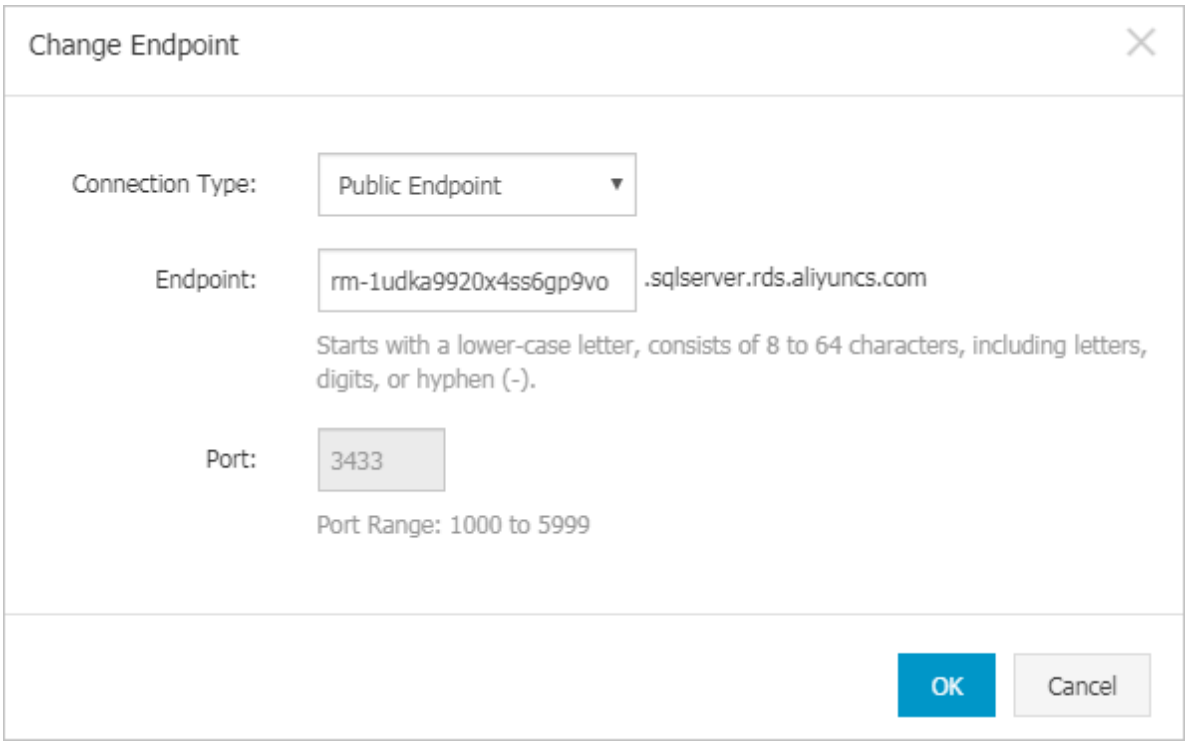


3. Find the target instance and click its ID.
4. In the left-side navigation pane, click Database Connection.
5. Click Apply for Public Endpoint.



6. In the displayed dialog box, click OK.

7. Click Change Endpoint, and in the displayed dialog box change the address and port number of the instance.



Parameter description:

- Connection Type: Select Internet Endpoint or Intranet Endpoint.
- Endpoint: The address format is `xxx . mysql . rds . aliyuncs . com`, where *xxx* is a user-defined field. The address contains 8 to 64 characters including letters and digits. It must begin with a lowercase letter.
- Port: The number of the port through which RDS provides external services. The port number can be an integer within the range [3200, 3999].

8. Click OK.