Alibaba Cloud ApsaraDB for MySQL

Quick Start for PostgreSQL

Issue: 20190828

Legal disclaimer

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

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

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

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

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `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 instance stability and security, ApsaraDB for PostgreSQL has the following restrictions.

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. 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 Open APIs.
Network setting	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

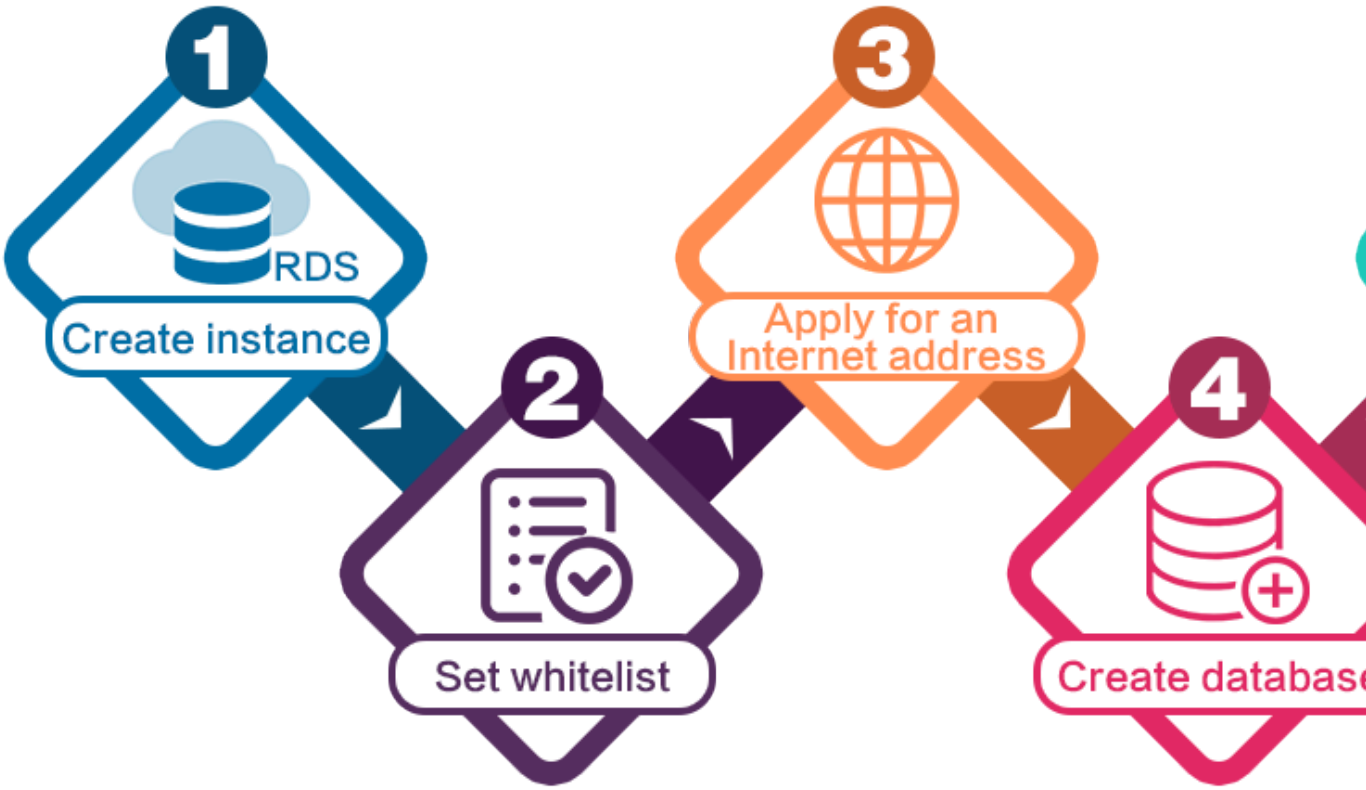
Purpose of the quick start

This document describes the procedure right from purchasing an RDS instance to using it. It also elaborates on 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 PostgreSQL instance

This topic describes how to use the RDS console to create an RDS for PostgreSQL instance. For more information about how to use APIs to create an instance, see CreateDBInstance. 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.

Prerequisites

- You have registered an Alibaba Cloud account.
- If you are creating a Pay-As-You-Go instance, make sure that your account balance is sufficient.

Precautions

- Subscription instances cannot be converted to Pay-As-You-Go instances.
- Pay-As-You-Go instances can be converted to Subscription instances. For more information, see #unique_9.
- 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.
- If you want to create an RDS instance in the PostgreSQL 10 High-availability Edition with local SSDs, PostgreSQL 10 Basic Edition, or PostgreSQL 9.4, you must log on to the RDS console.
- If you want to create an RDS instance in the PostgreSQL 10 or 11 High-availability Edition with SSDs, you must log on to the new PostgreSQL console.

Create an RDS instance in PostgreSQL 10 or 11 High-availability Edition with SSDs

1. Log on to the new PostgreSQL console.
2. Click the Subscription or Pay-As-You-Go tab.

> Note:
> For more information about the billing method, see #unique_10.

3. Set the following parameters.

Parameter	Description
Region	The region where the RDS instance is located. You cannot change the region after the instance is purchased. · Select the region where your target users are located to increase access speeds. · Make sure that the RDS instance is located in the same region as the ECS instance to be connected. Otherwise, the RDS and ECS instances cannot communicate through a private network and consequently cannot achieve their optimal performance.
Edition	High-availability. In the HA architecture, the RDS instance consists of two nodes: one master node and one slave node. For more information, see #unique_11.
Primary Zone	The primary zone of the RDS instance. · A zone is an independent physical zone in a region. Zones in the same region are basically the same. · You can create the RDS instance in the same or different zone from the ECS instance to be connected. · You only need to select a primary zone. The system automatically assigns a secondary zone.
Database Engine	The type of the DB engine. Only one option is available: PostgreSQL.
Version	The version of PostgreSQL. The new PostgreSQL console supports PostgreSQL 11 and PostgreSQL 10.

Parameter	Description
Instance Type	The type of the RDS instance. Each instance type provides a specific number of CPU cores, memory size, maximum number of connections, and maximum IOPS. For more information, see #unique_12. RDS instances fall into the following types: · General-purpose instances (including entry-level instances and test instances) : Each instance owns the memory and I/O resources allocated to it and shares CPU and storage resources with the other general-purpose instances on the same server. · Dedicated instances: Each instance owns the CPU, memory, storage, and I/O resources allocated to it. · Dedicated-host instances: Each instance owns all the CPU, memory, storage, and I/O resources on the server where it is deployed. For example, 4 Cores, 16 GB is a general-purpose instance, 8 Cores, 32 GB (Dedicated Instance) is a dedicated instance, and 30 Cores, 220 GB (Dedicated Host) is a dedicated-host instance.
Network Type	VPC. A Virtual Private Cloud (VPC) is an isolated network that is superior to a classic network in terms of security and performance. Note: Make sure that the network type of the RDS instance is the same as that of the ECS instance to be connected. If their network types are different, they cannot communicate through a private network.
VPC VSwitch	· If you have created a VPC that meets your network planning requirements, you can select the VPC and a VSwitch on the VPC. · If you have not created a VPC that meets your network planning requirements, you can select the default VPC and VSwitch.
Storage Type	Standard SSD or Enhanced SSD. For more information, see #unique_13.
Capacity	Used to store data, system files, binary log files, and transaction files.

Parameter	Description
Data Encryption	Available only to the China (Hong Kong) region. Two options are provided: No Encryption and KMS Encryption. For more information, see Manage CMKs.

4. Set Quantity and Duration, then click Buy Now.

> Note:
> You must set Duration only when you are creating a Subscription instance.

5. On the Confirm Order page, select the terms of service, and click Pay to complete the payment.

Create an RDS instance in PostgreSQL 10 High-availability Edition (with local SSDs), PostgreSQL 10 Basic Edition, or PostgreSQL 9.4 (through the old RDS console)

1. Log on to the old RDS console.
2. Click the Subscription or Pay-As-You-Go tab. For more information about pricing, see #unique_10.
3. Set the following parameters.

Parameter	Description
Region	The physical location where the RDS instance is located. You cannot change the region after the instance is purchased. · Select the region where your target users are located to increase access speeds. · Make sure that the RDS instance is located in the same region as the ECS instance to be connected. Otherwise, the RDS and ECS instances cannot communicate through a private network and consequently cannot achieve their optimal performance.
Resource Group	The resource group to which the RDS instance belongs.
Database Engine	The type of the DB engine. Select PostgreSQL. Note: The available DB engines vary depending on the region you select.

Parameter	Description
Version	The version of PostgreSQL. The old RDS console supports PostgreSQL 9.4 and PostgreSQL 10. Note: The available versions vary depending on the region you select.
Edition	· Basic: The RDS instance consists of only one node. Compute is decoupled from storage to reduce costs. · High-availability: The RDS instance consists of a master node and a slave node. For more information, see #unique_11. The available editions vary depending on the version you select.
Storage Type	· Local SSD: A local SSD is located on the same node as the DB engine. Data is stored on the local SSD to reduce I/O latency. · SSD: An SSD is a scalable block storage device designed based on the distributed architecture. Data is stored on the SSD to decouple compute and storage. For more information, see #unique_13.
Zone	A zone is an independent physical zone in a region. Zones in the same region are basically the same. You can create the master and slave nodes of the RDS instance in the same or different zones. Multi-zone deployment provides a higher level of disaster tolerance than single-zone deployment.
Network Type	· Classic Network: a classic network. · VPC (recommended): A Virtual Private Cloud (VPC) is an isolated network that is superior to a classic network in terms of security and performance. Note: Make sure that the network type of the RDS instance is the same as that of the ECS instance to be connected. If their network types are different, they cannot communicate through a private network.

Parameter	Description
CPU and Memory	The type of the RDS instance. Each instance type provides a specific number of CPU cores, memory size, maximum number of connections, and maximum IOPS. For more information, see #unique_12. RDS instances fall into the following types: · General-purpose instances (including entry-level instances and test instances) : Each instance owns the memory and I/O resources allocated to it and shares CPU and storage resources with the other general-purpose instances on the same server. · Dedicated instances: Each instance owns the CPU, memory, storage, and I/O resources allocated to it. · Dedicated-host instances: Each instance owns all the CPU, memory, storage, and I/O resources on the server where it is deployed. For example, 4 Cores, 16 GB is a general-purpose instance, 8 Cores, 32 GB (Dedicated Instance) is a dedicated instance, and 30 Cores, 220 GB (Dedicated Host) is a dedicated-host instance.
Capacity	Used to store data, system files, binary log files, and transaction files.

4. Set Quantity and Duration (the Duration parameter is available only when you are creating a Subscription instance), then click Buy Now.

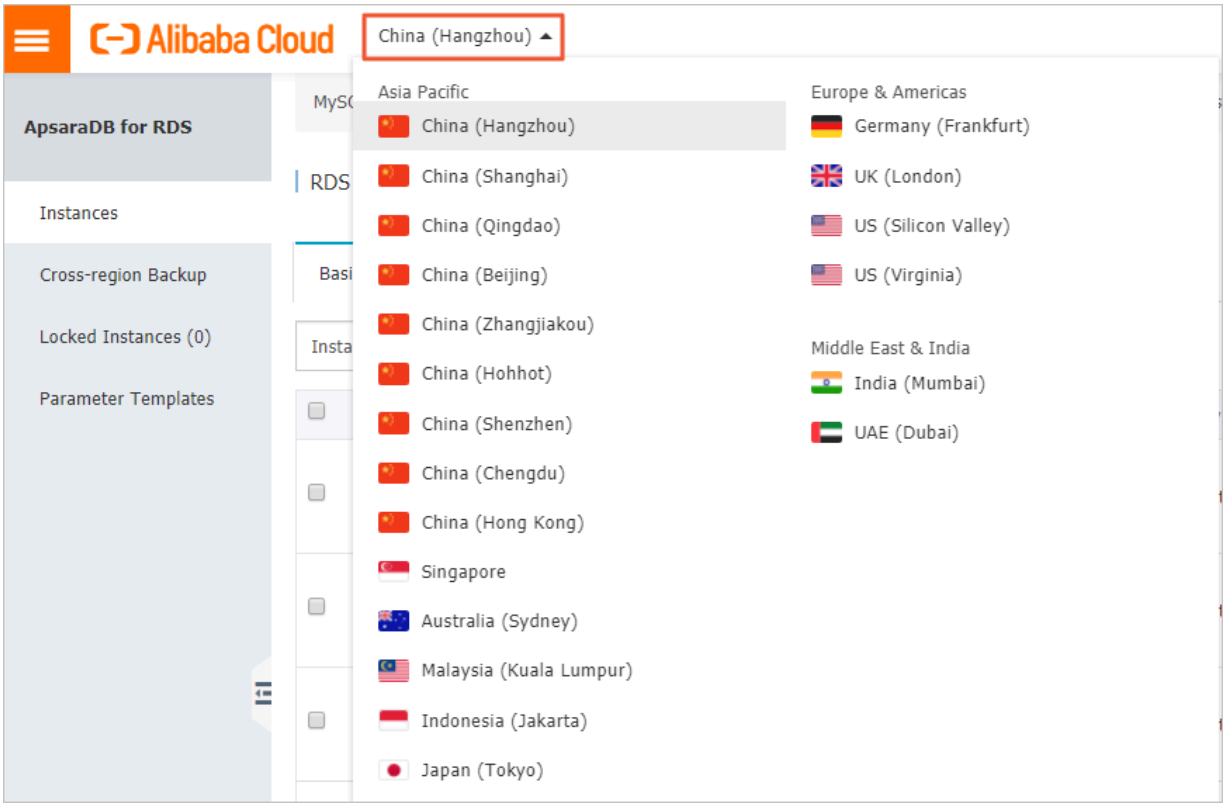
   Note:

   · If you are creating a Subscription instance, you can select Auto-renewal. Then the system automatically deducts fees based on the specified duration. For example, if you select a duration of three months, the system automatically deducts fees of three months in each automatic renewal.
   · If you are creating a Subscription instance, you can click Add to Cart to add the RDS instance to the cart, and click Cart later to pay for the instance.

5. On the Order Confirmation page, select the terms of service, and click Pay Now to complete the payment.

What to do next

In the upper-left corner, select the region where the new RDS instance is located. Then you can view the new RDS instance.



After you create the RDS instance, you must configure a whitelist and create databases and accounts for it. If you connect the RDS instance through the Internet, you must also apply for a public connection address. For more information about how to connect to an RDS instance, see Connect to an instance.

APIs

API	Description
#unique_18	Used to create an RDS instance.

4 Initial configuration

4.1 Configure a whitelist

After an RDS instance is created, you must configure a whitelist so that external devices can access the RDS instance. 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.

To configure a whitelist, follow these steps:

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

> Note:
> You can configure VPC security groups only in PostgreSQL 10 High-availability Edition (with local SSDs), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4

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.

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

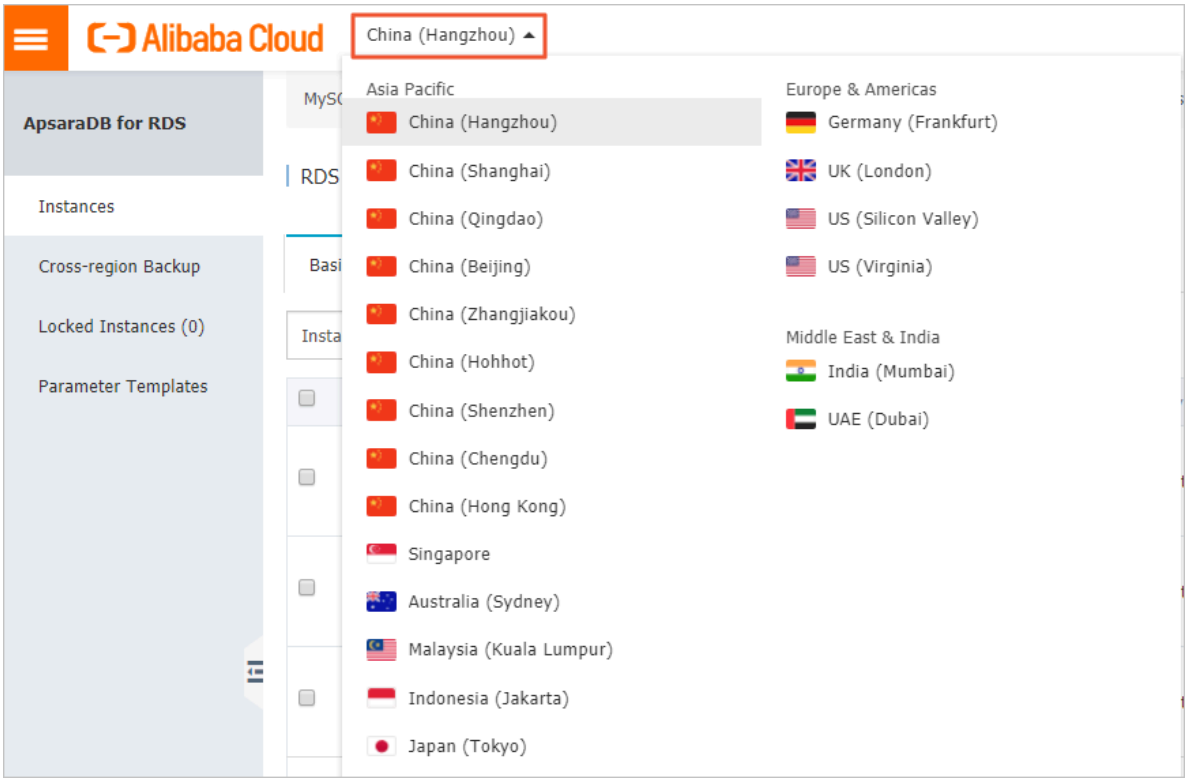
Precautions

- 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.

Procedure

1. Log on to the PostgreSQL console.

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

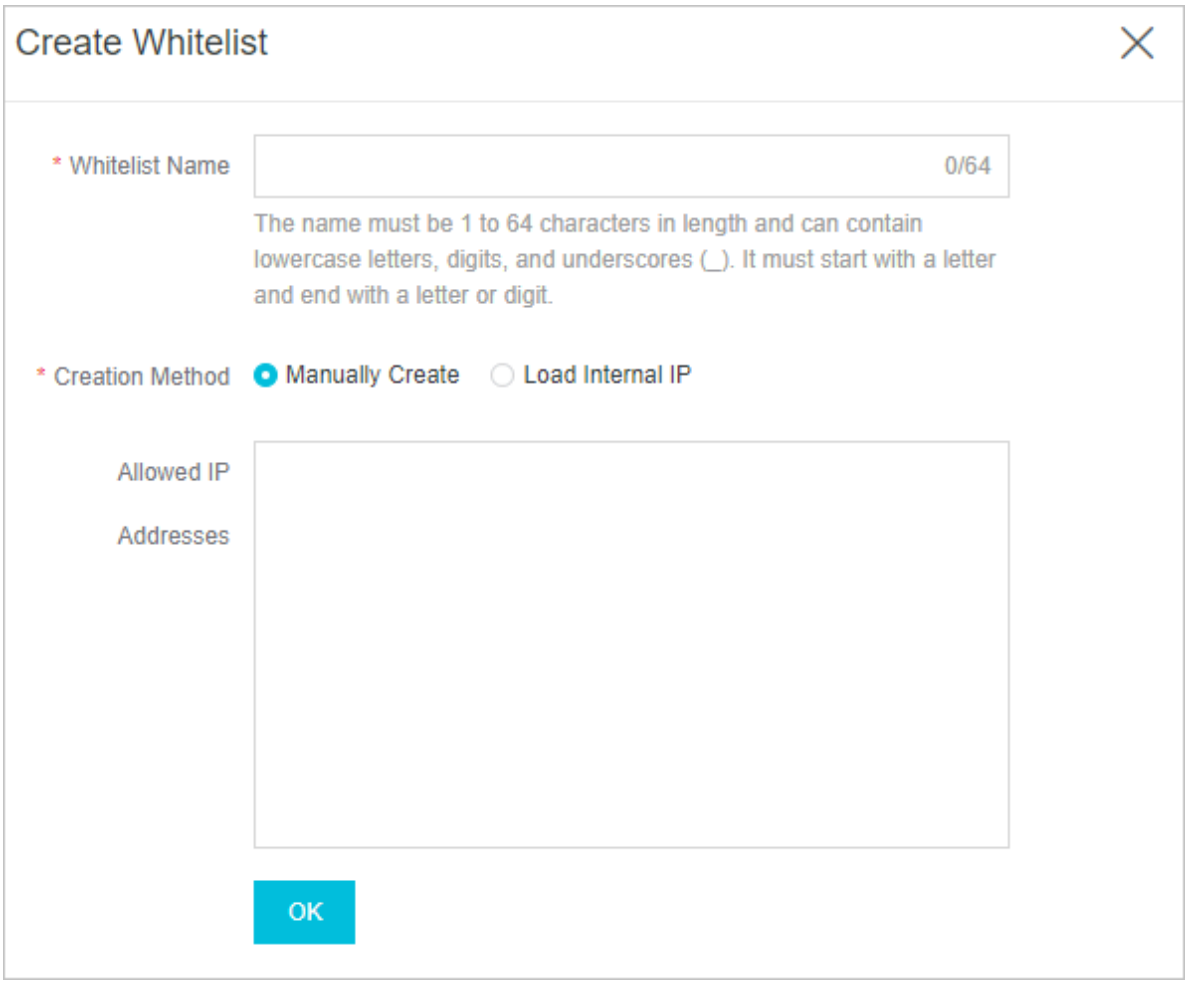


3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, choose Data Security > Whitelist Configuration.
5. On the displayed page, find the whitelist named default and in the Actions column choose # > Edit.

> **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 select Load Internal IP for Creation Method, then you can select an IP address from the Load Internal IP drop-down list.

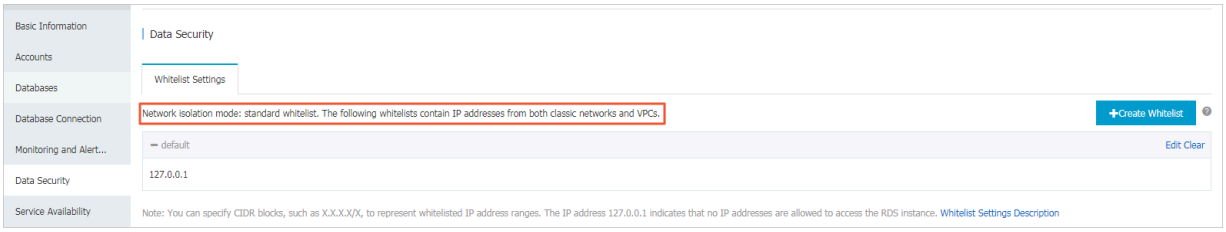
   Note:
   After you add IP addresses or CIDR blocks to the default whitelist, the system automatically deletes the default IP address 127.0.0.1.



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

Precautions

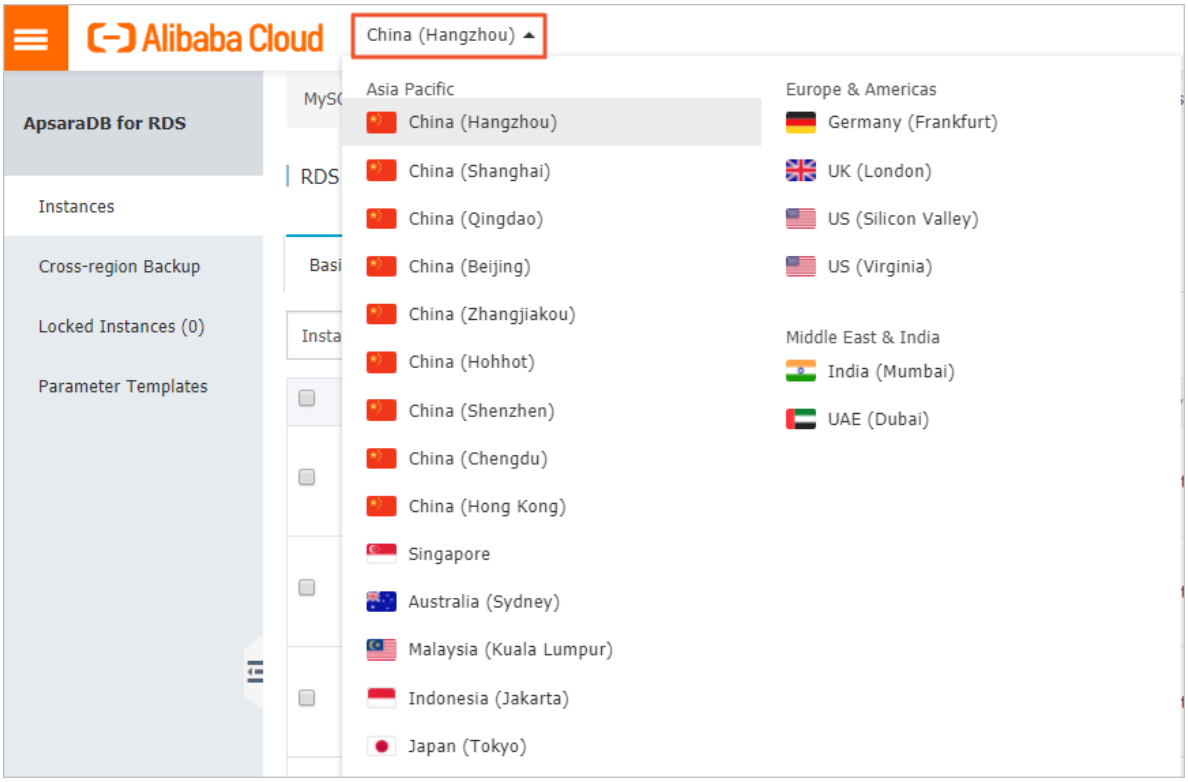
- The default IP address whitelist can be modified or cleared but cannot be deleted.
- Up to 1,000 IP addresses or CIDR blocks can be added to each IP address whitelist. If you want to add a large number of IP addresses, we recommend that you merge them into CIDR blocks, for example, 192.168.1.0/24.
- 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.



Configure an enhanced whitelist

1. Log on to the RDS console.

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

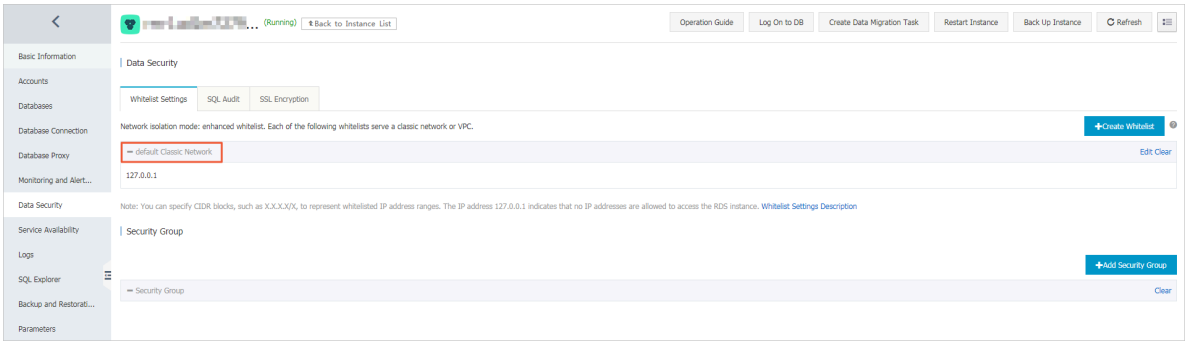


3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Data Security.
5. On the Whitelist Settings tab, select the whitelist you want to modify. Detailed steps are as follows:

   - 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_21.

- 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.

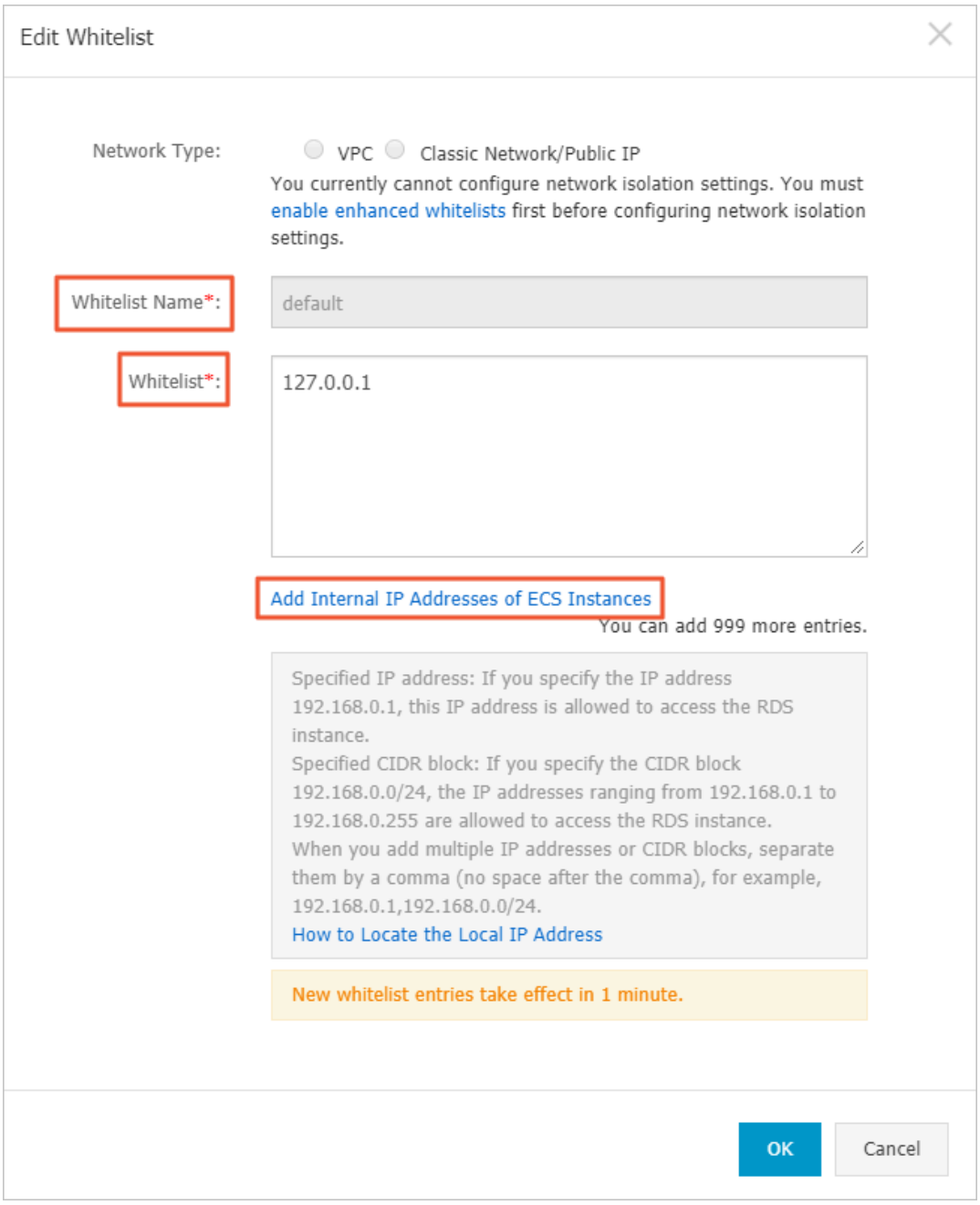


6. In the displayed dialog box, enter IP addresses or CIDR blocks and click OK. Detailed rules are as follows,

   - 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:

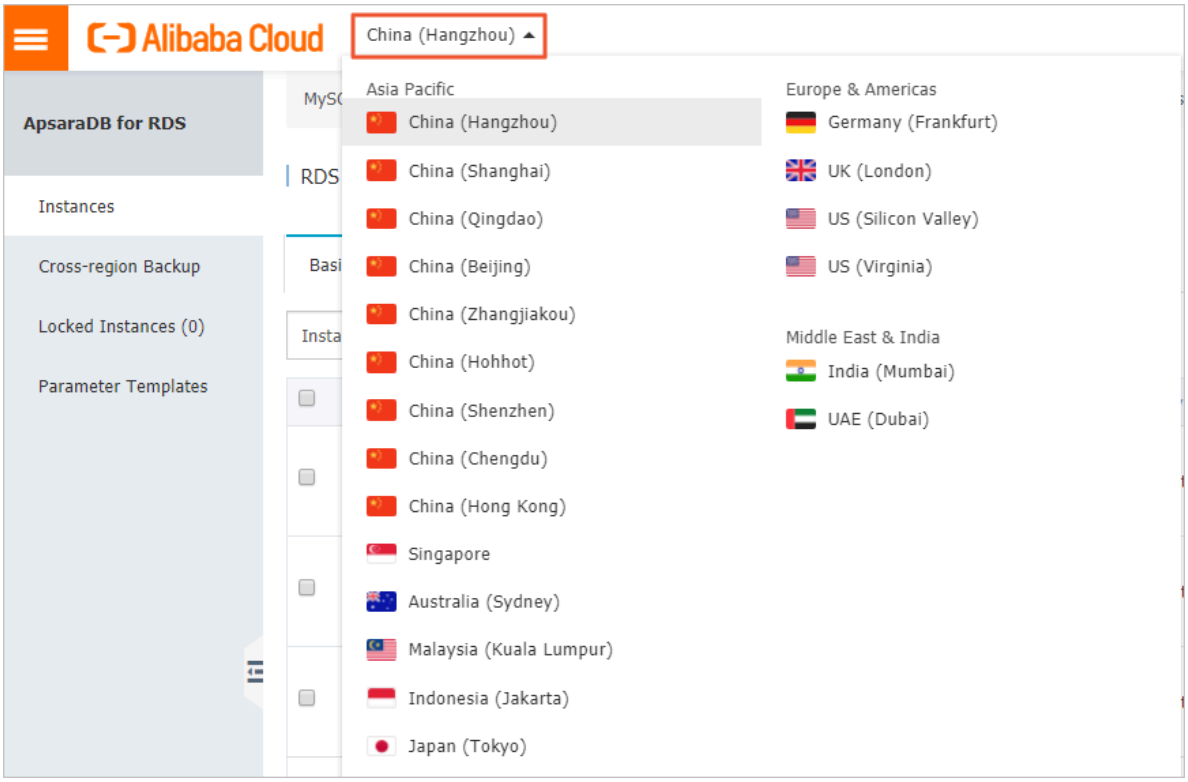
After you add IP addresses or CIDR blocks to the default whitelist, the system automatically deletes the default IP address 127.0.0.1.



Configure a standard whitelist

1. Log on to the RDS console.

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



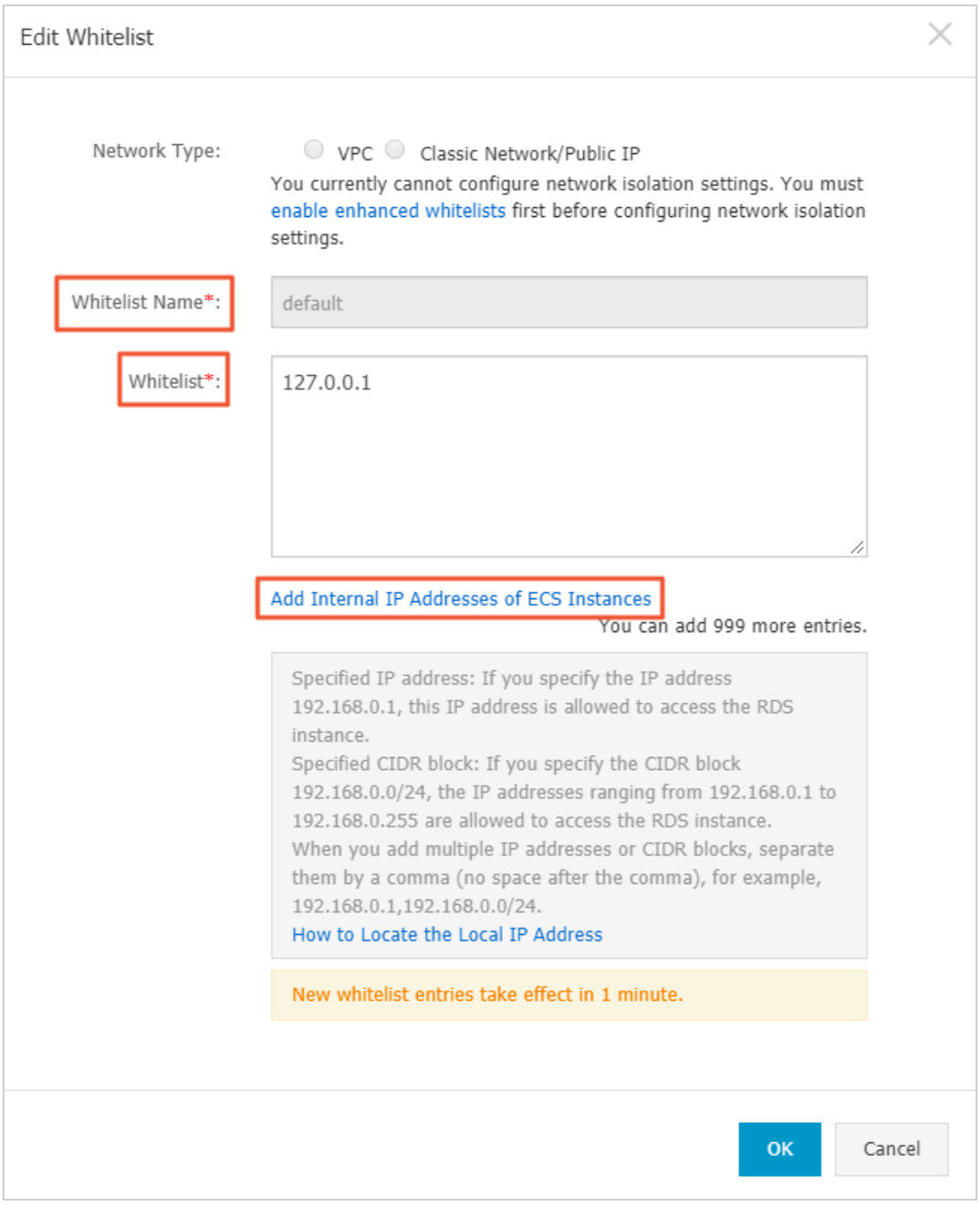
3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Data Security.
5. On the Whitelist Settings tab, click Edit in the default whitelist.

> **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_23.

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 .

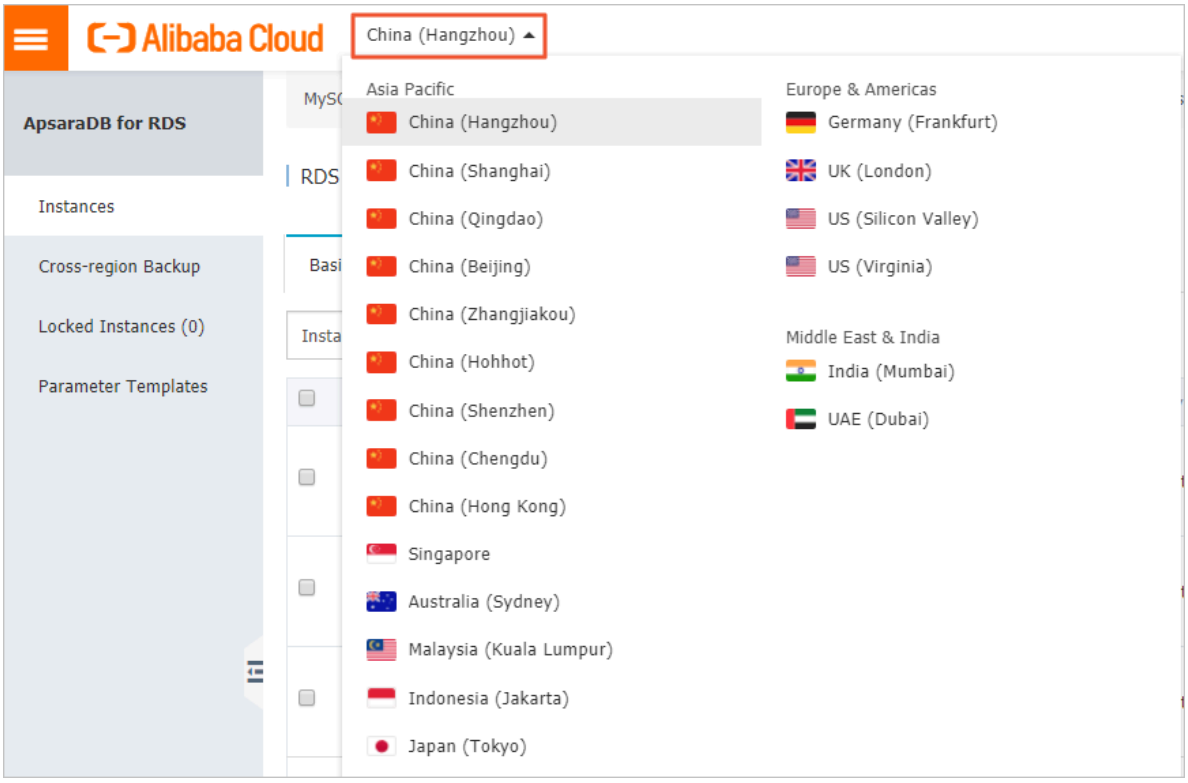
For more information, see Create a security group.

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. 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 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_24	Used to view the IP address whitelists of an RDS instance.
#unique_25	Used to modify the IP address whitelists of an RDS instance.

4.2 Apply for a public endpoint

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

Internal and public endpoints

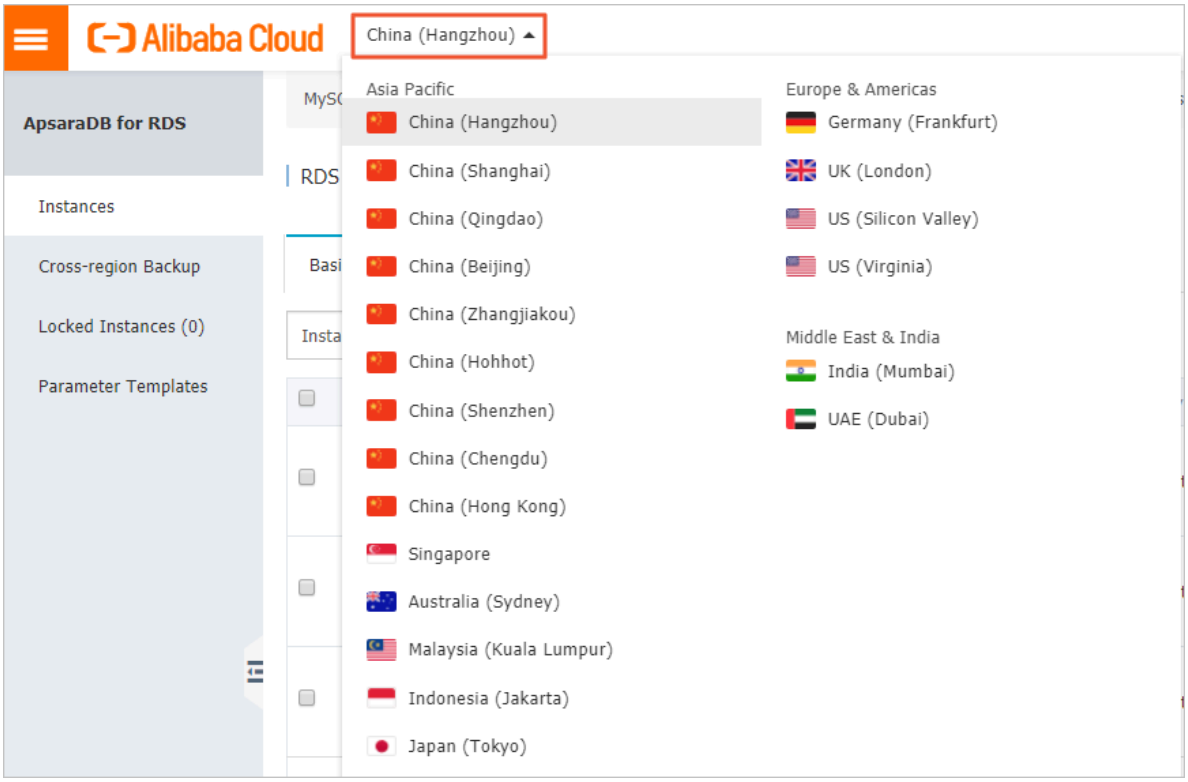
Endpoint type	Description
Internal endpoint	· An internal endpoint is generated by default. · If your application is deployed on an ECS instance that is located in the same region as your RDS instance and, at the same time, the ECS instance has the same network type as your RDS instance, your RDS instance can communicate with the ECS instance through a private network. In such case, you do not need to apply for a public endpoint. · 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. · If you cannot access your RDS instance through a private network in one of the following scenarios, you must apply for a public endpoint: - 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. · You access your RDS instance from a device outside the Alibaba Cloud. Note: · The public endpoint and traffic are currently free of charge. · Using the public endpoint reduces security. Please exercise caution. · To guarantee high security and performance, we recommend that you migrate your application to an ECS instance that is located in the same region and has the same network type as your RDS instance and then use the internal endpoint.

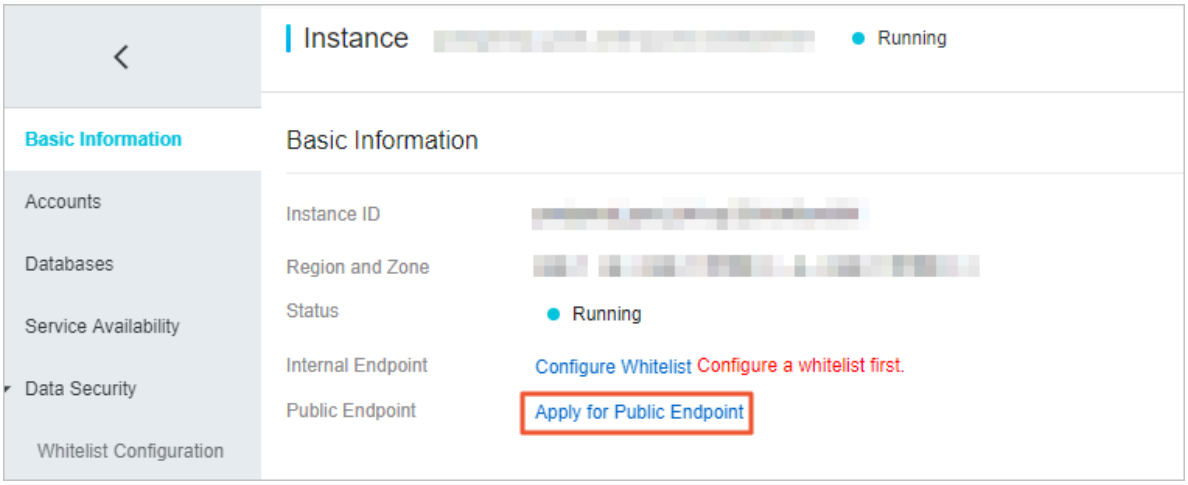
PostgreSQL 11 High-availability Edition (with SSDs) or PostgreSQL 10 High-availability Edition (with SSDs)

1. Log on to the PostgreSQL console.

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



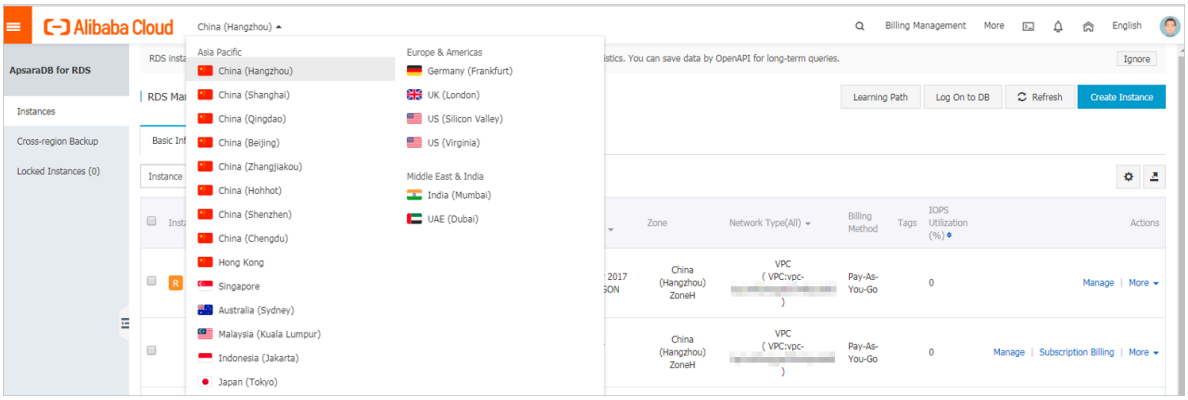
3. Find the RDS instance and click the instance ID.
4. In the Basic Information section of the Basic Information page, click Apply for Public Endpoint and in the displayed dialog box click OK.



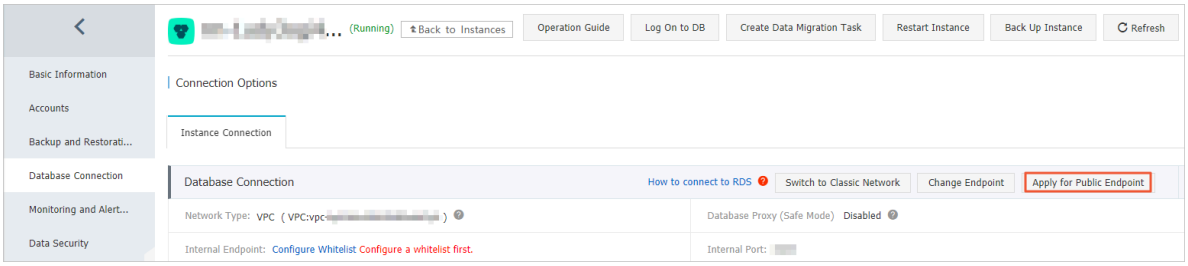
PostgreSQL 10 High-availability Edition (with local SSDs), PostgreSQL 10 Basic Edition, or PostgreSQL 9.4

1. Log on to the RDS console.

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



3. Find the 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.

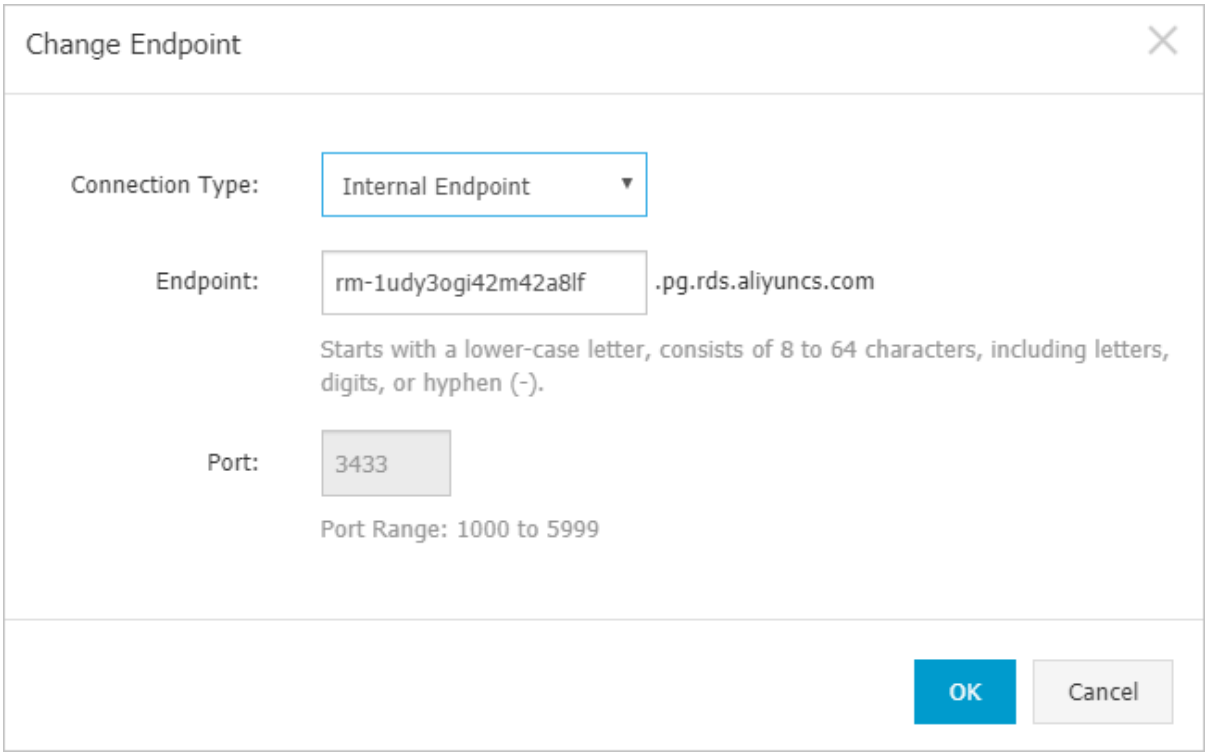
   A public endpoint is generated.

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_27	Used to apply for an internal endpoint for an RDS instance.

4.3 Create databases and accounts

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

- For PostgreSQL 11 High-availability Edition (with SSDs) and PostgreSQL 10 High-availability Edition (with SSDs), you can create and manage databases and accounts in the RDS console.
- For PostgreSQL 10 High-availability Edition (with local SSDs), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4, you must create a superuser account in the RDS console, and then create and manage databases by using the DMS console or a client.

Background information

- Databases under a single instance share all the resources of this instance. Each PostgreSQL instance supports one initial account, countless general accounts,

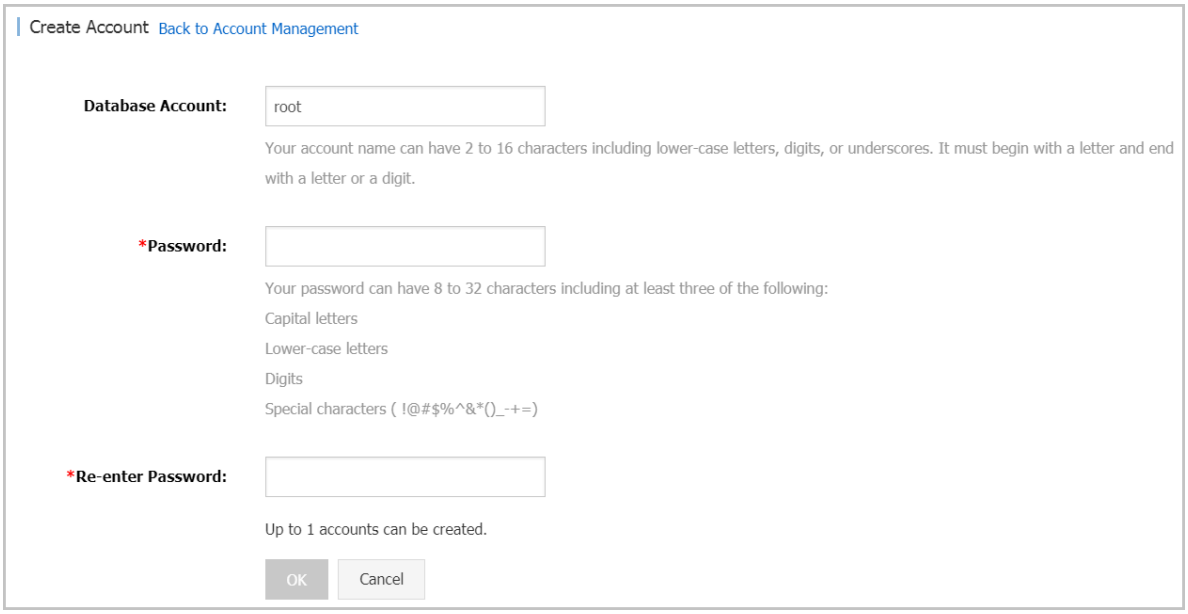
and countless databases. You must create and manage the general accounts and databases through SQL statements.

- To migrate your local database to the RDS instance, you must create the same databases and accounts for the RDS instance as your local database.
- When assigning account permissions for each database, follow the minimum permission' principle and consider service roles to create accounts. Alternativ ely, rationally assign read-only and read/write permissions. When necessary, you can split accounts and databases into smaller units so that each account can only access data for its own services. If the account does not need to write data to a database, assign the read-only permission for the account.
- For database security, 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. Click the ID of the instance to visit the Basic Information page.
4. In the left-side navigation pane, select Accounts.
5. Click Create Initial Account.

6. To create an account, set the related fields.



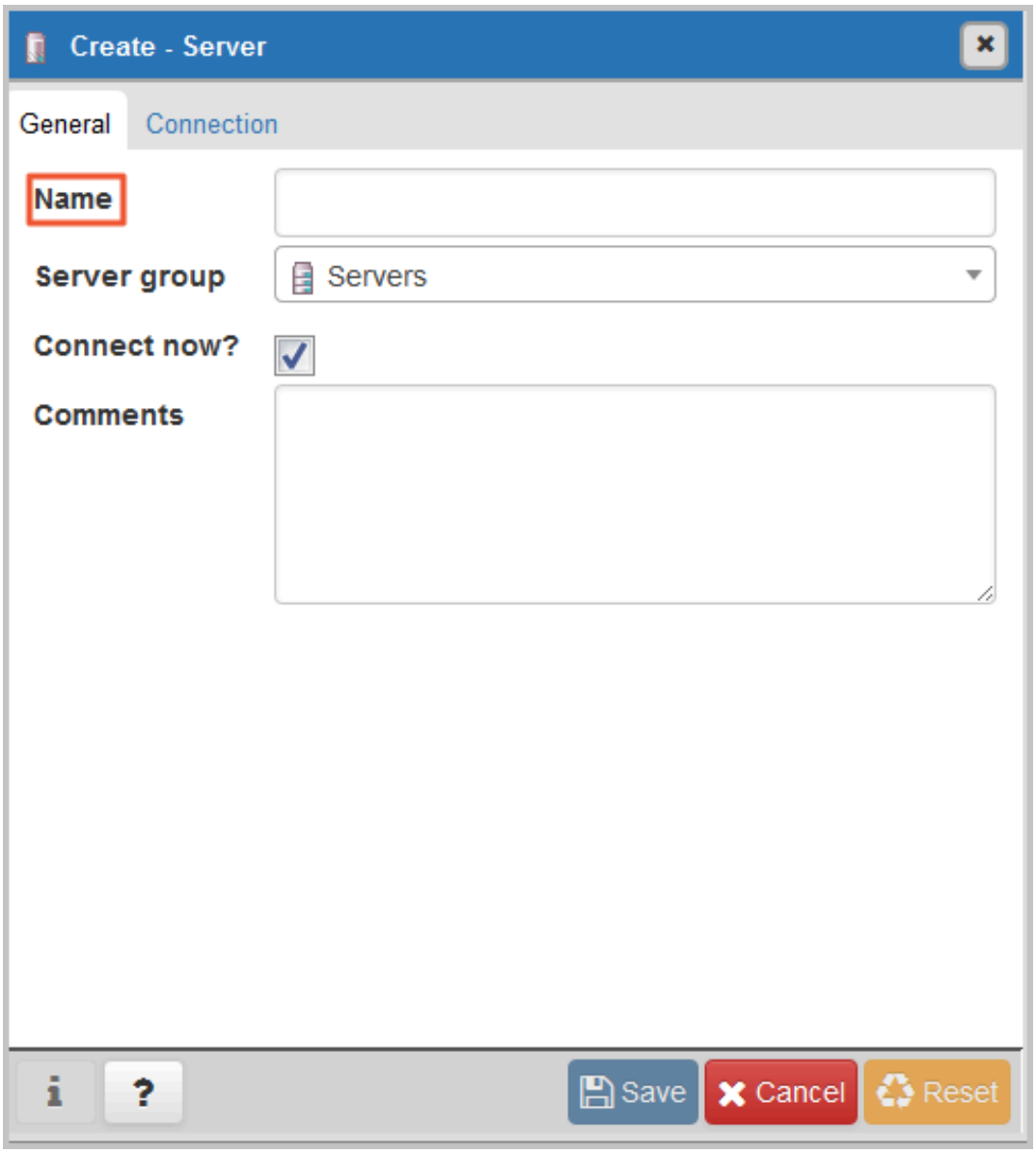
Parameters description:

- `Database Account` : refers to the name of the initial account. It contains 2 to 16 characters including the lower-case letters, digits, or underscores (_). It must begin with a letter and end with a letter or digit.
- `Password` : refers to the password of the initial account. It contains 8 to 32 characters including at least three of the following: capital letters , lower-case letters, digits, and special characters (!@#$%^&*()_-+=)
- `Re - enter Password` : Re-enter the password to make sure the password is entered correctly.

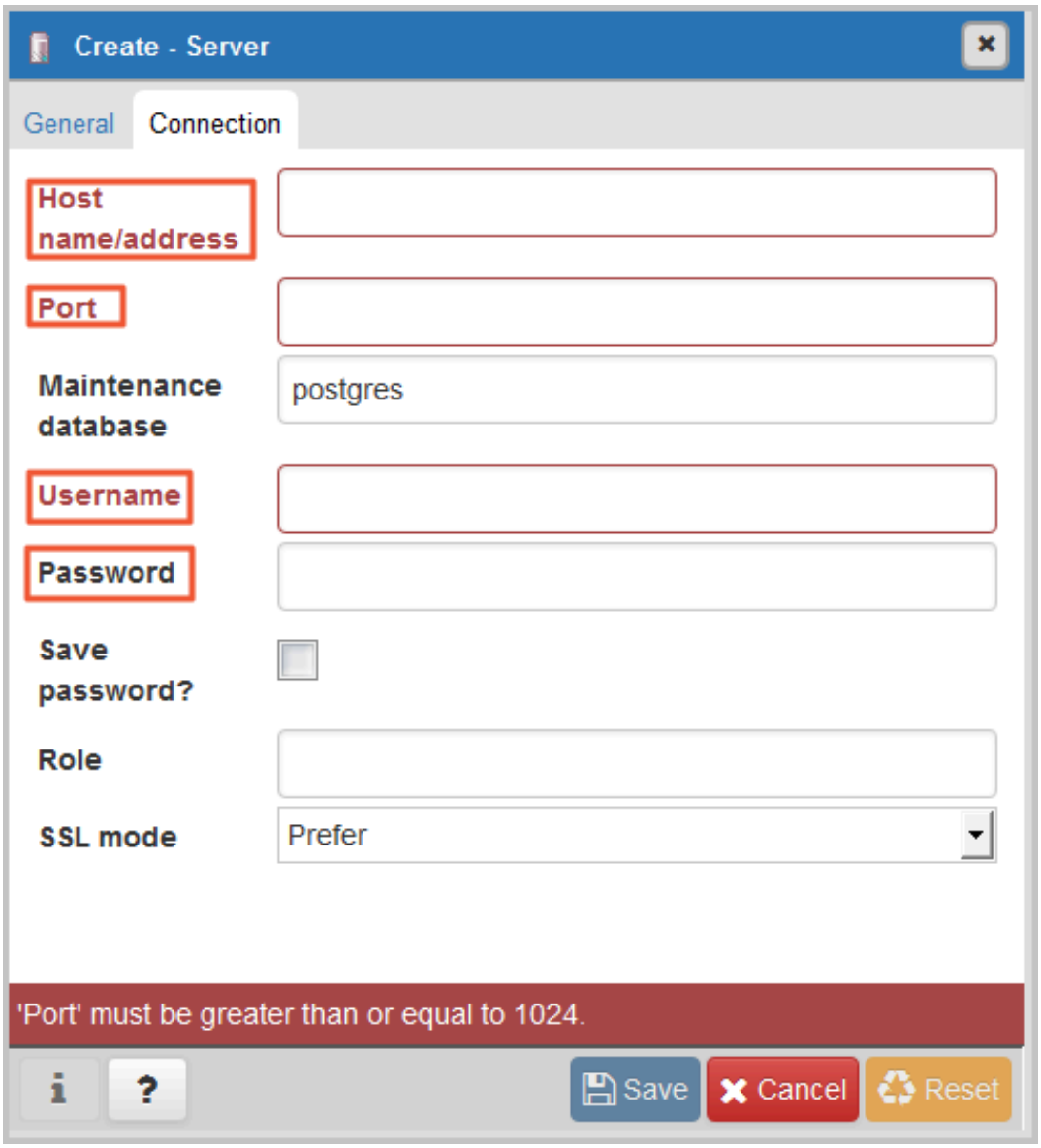
7. Click OK.
8. Add the IP address that is allowed to access the RDS instance to the RDS whitelist. For more information about how to set the whitelist, see #unique_28.
9. Start the pgAdmin 4 client.

10. Right-click Servers, and then select Create > Server, as shown in the following figure.

11. On the General tab of Create - Server window, enter server name, as shown in the following figure.



12. Click the Connection tab, and enter the information of the instance to be connected, as shown in the following figure.



Parameters description:

- `Host name / address` : refers to 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. You can view the connection address and port number as follows:

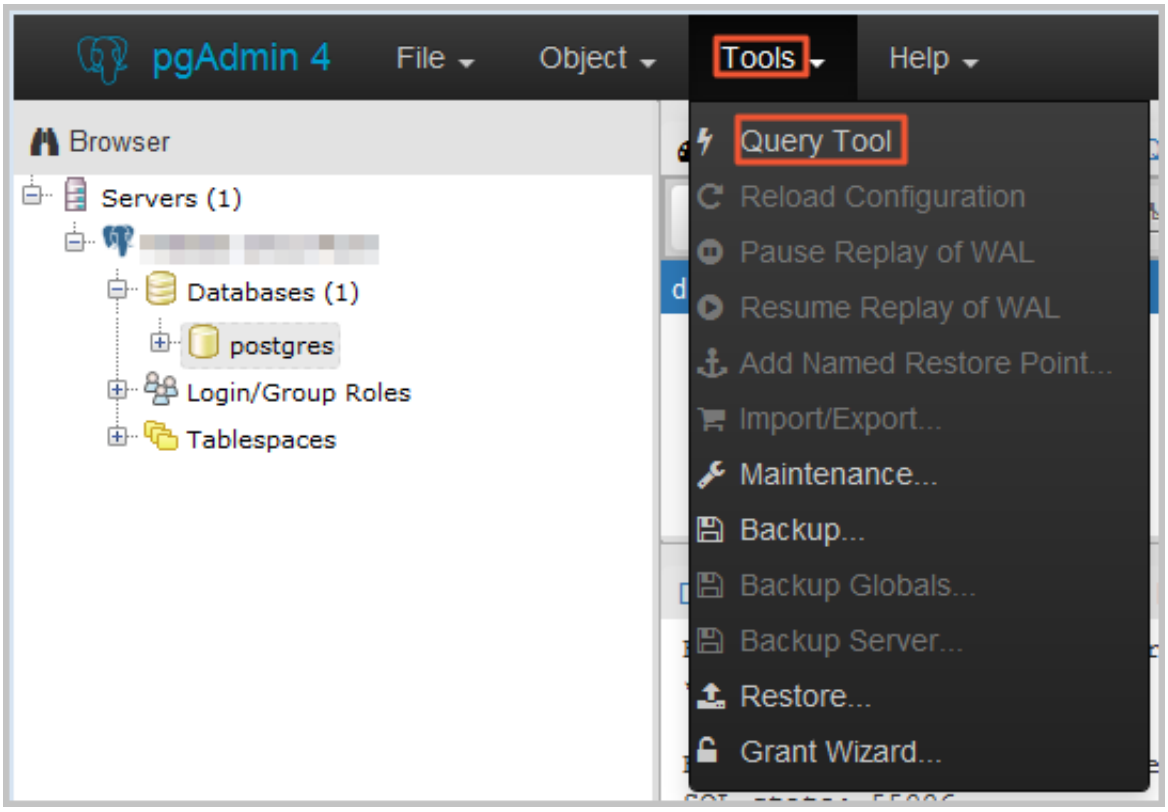
a. Log on to the RDS console.
b. Select the region where the target instance is located.
c. Click the ID of the instance to visit the Basic Information page.
d. View the intranet and Internet IP addresses and ports in the Basic Information area.

- `Port` : refers to the port number of the 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` : refers to the initial account name of the RDS instance.
- `Password` : refers to the password of the initial account of the RDS instance.

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

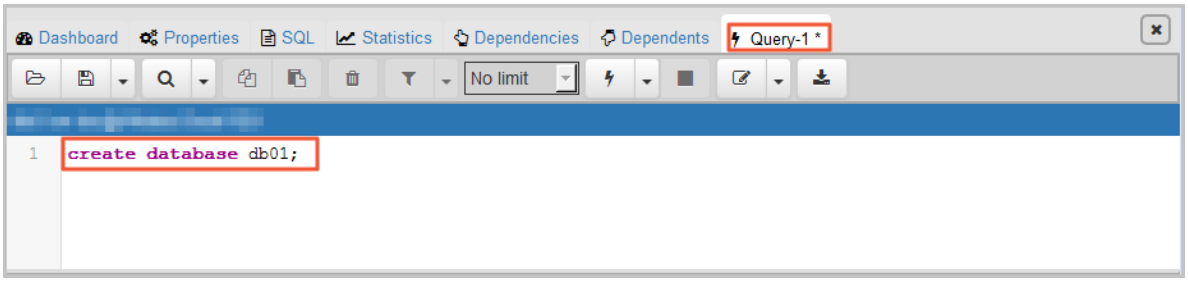
> **Note:**
> postgres is the default system database of the RDS instance. Do not do any operation in this database.

15. Click postgres, and then select Tools > Query Tool, as shown in the following figure.

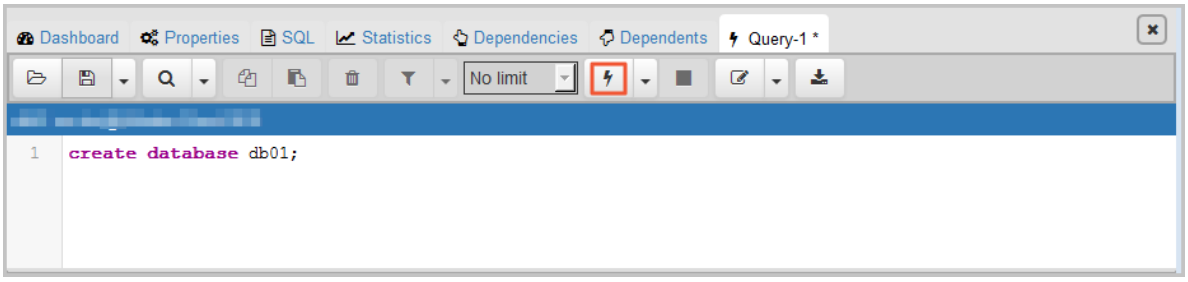


16. Enter the following command on the Query-1 tab page to create a database, as shown in the following figure.

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

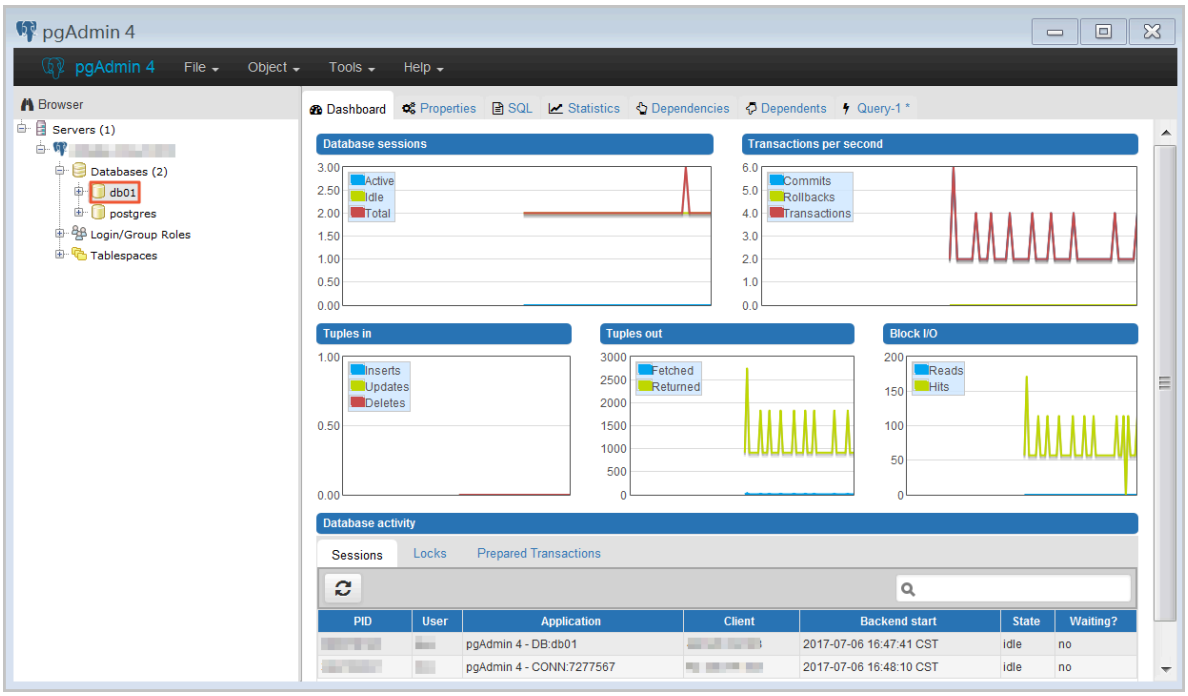


17. Click Execute/Refresh, as shown in the following figure.



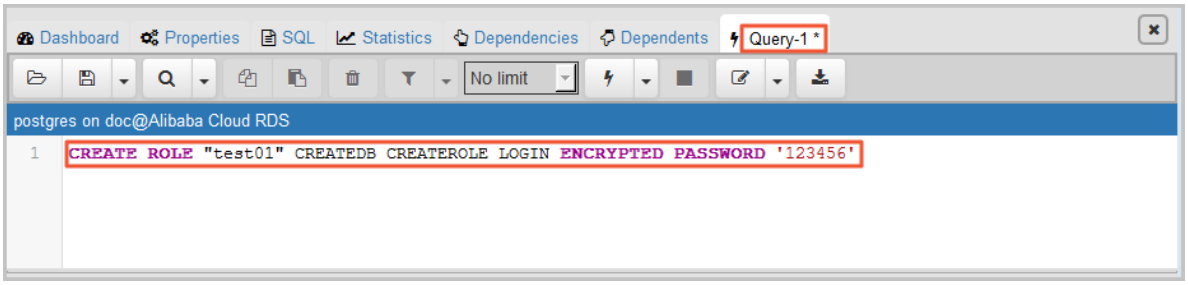
If the execution is successful, the new database is created successfully.

18. Right-click Databases and click Refresh, and then you can find the newly created database, as shown in the following figure.

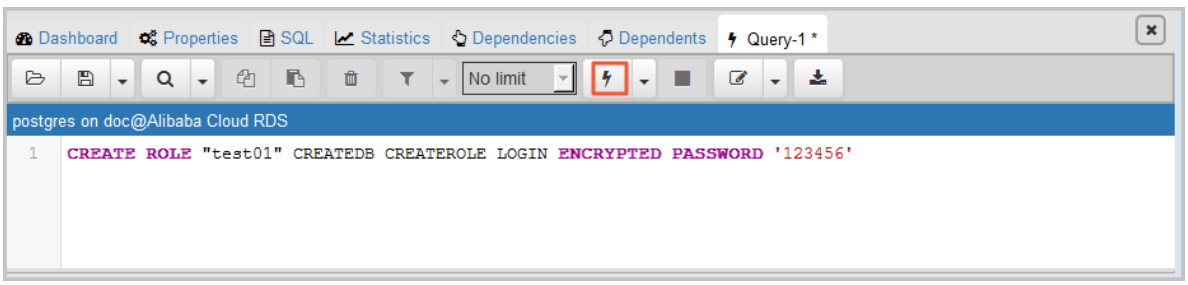


19. Enter the following command on the Query-1 tab page to create an account, as shown in the following figure.

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

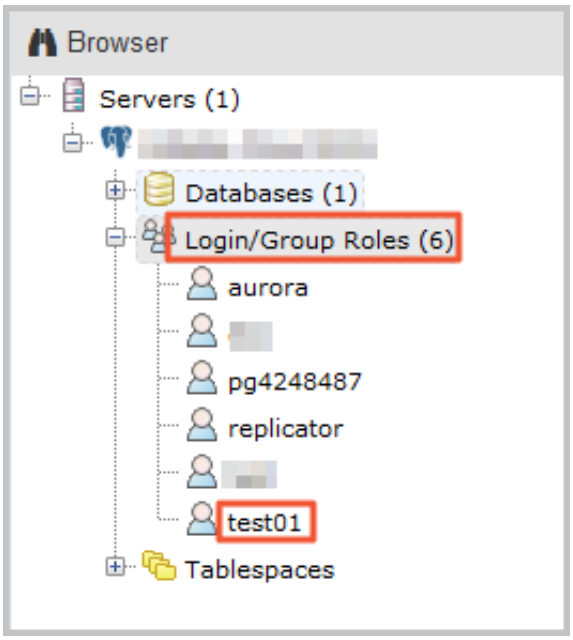


20. Click Execute/Refresh, as shown in the following figure.



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

21. Right-click Login/Group Roles and click Refresh, and then you can find the newly created account, as shown in the following figure.



5 Connect to an instance

You can connect to an RDS instance through the PostgreSQL client. This document introduces the connection procedure by taking the pgAdmin 4 client as an example.

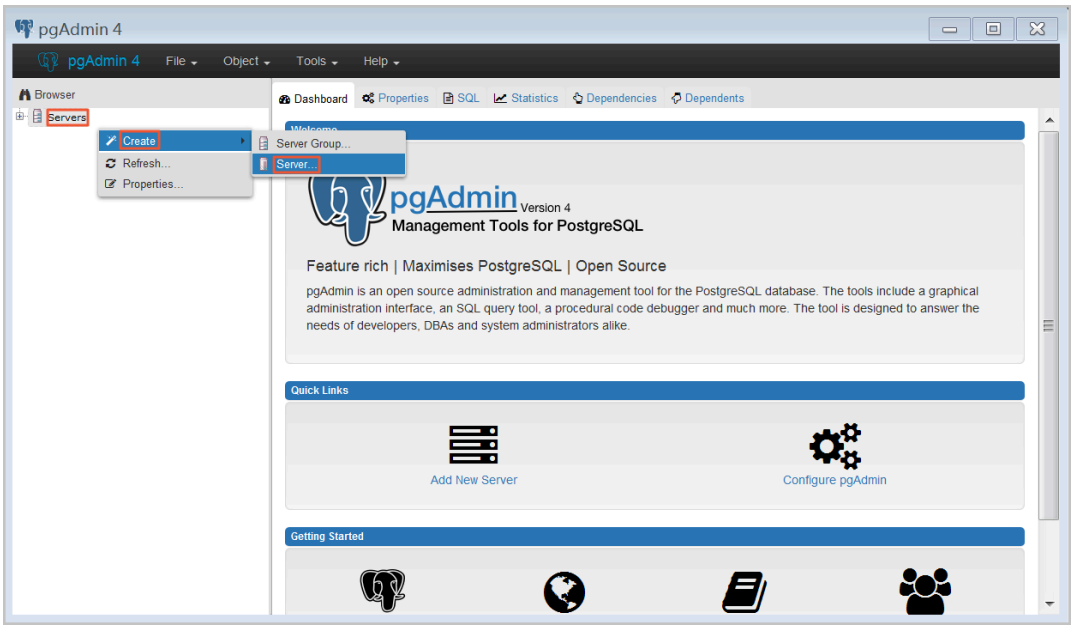
Background information

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 document 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 intranet or Internet address as follows:

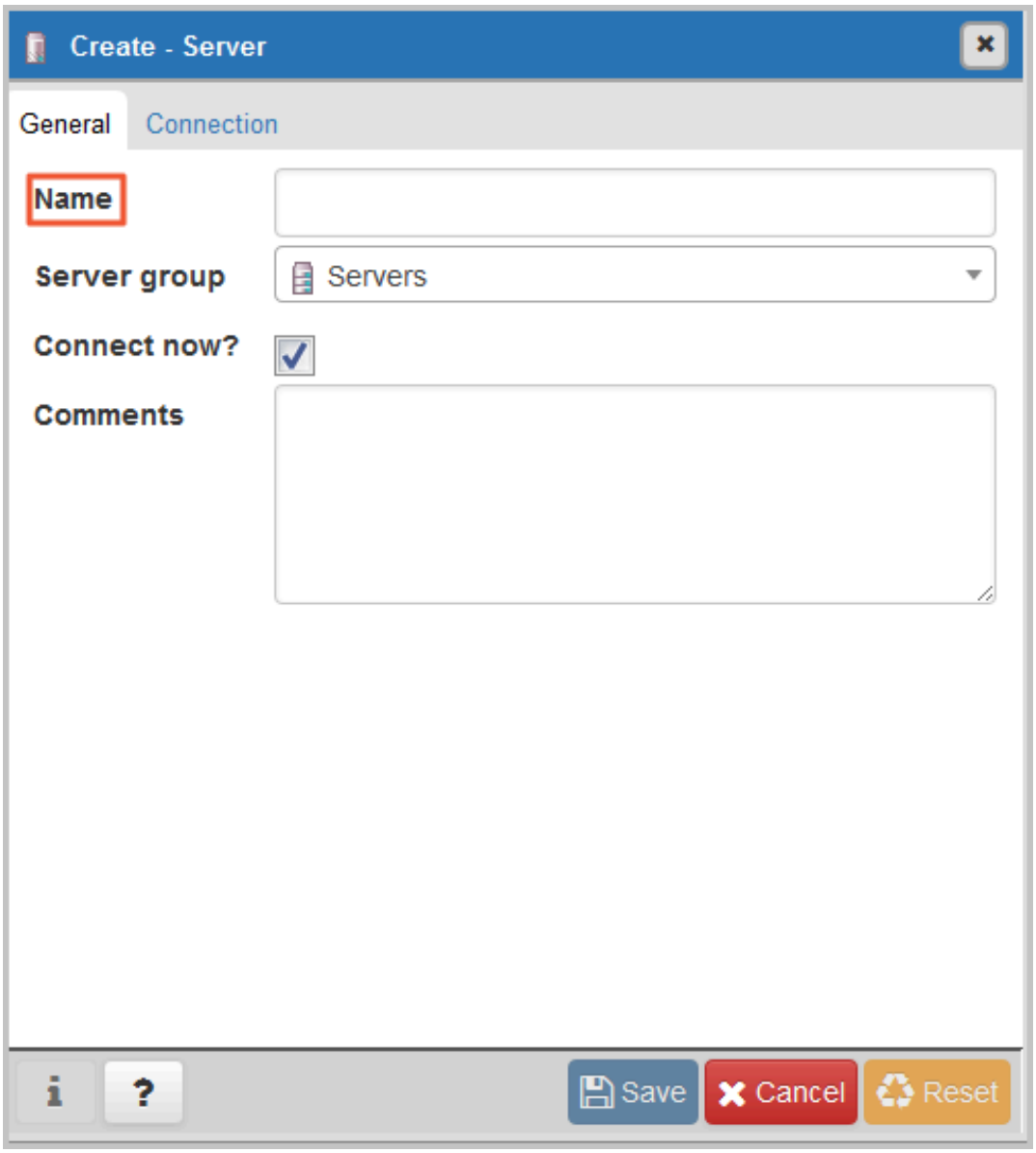
- Use the intranet IP address when your client is installed on the ECS that is located in the same region and the same network type as the RDS instance to be connected.
- Use the Internet IP address for the other situations.

Log on through a client

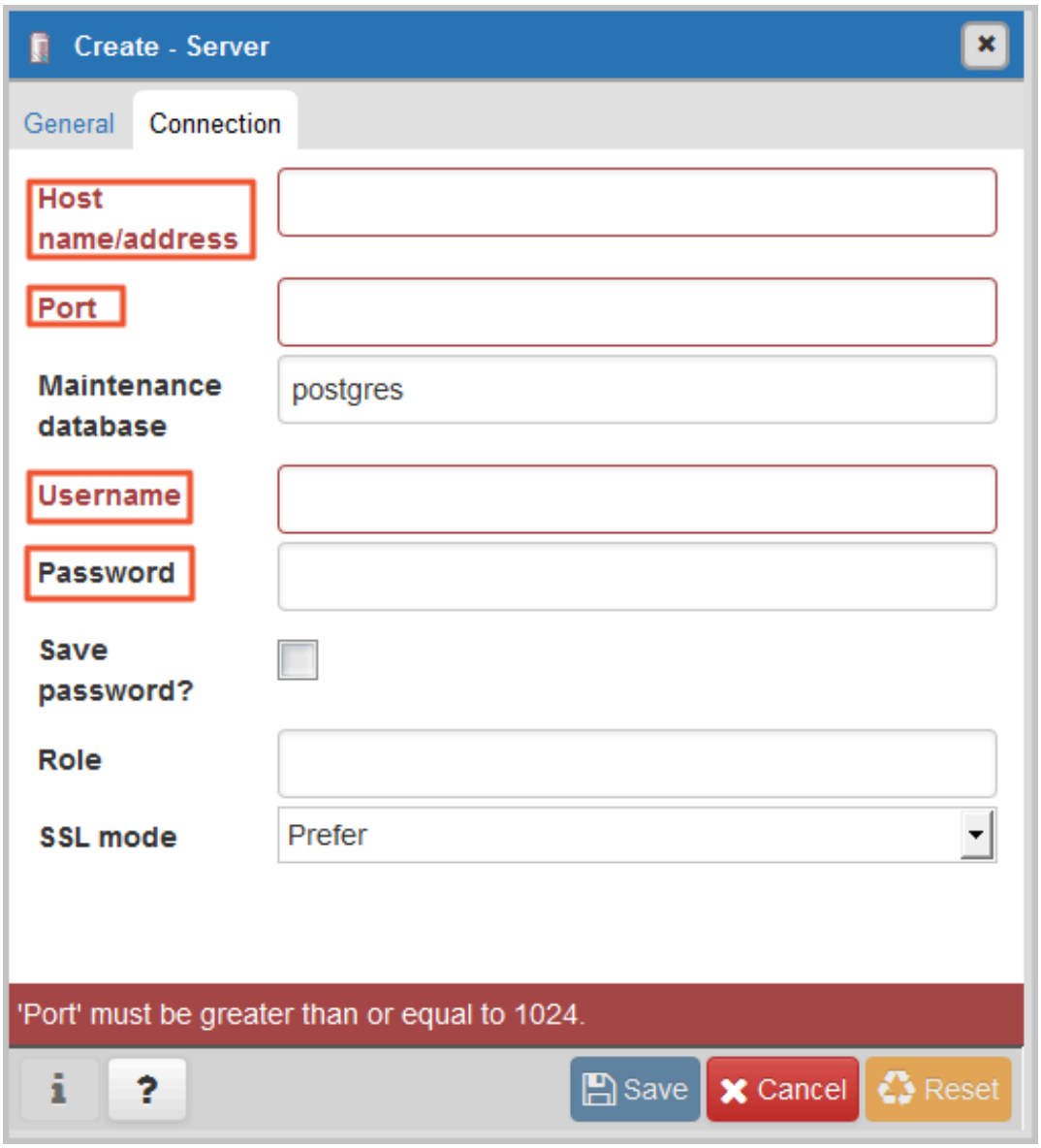
1. Add the IP address that is allowed to access the RDS instance to the RDS whitelist. For more information, see #unique_28.
2. Start the pgAdmin 4 client.
3. Right click Servers, and then select Create > Server, as shown in the following figure.



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



5. Click the Connection tab, enter the information of the instance to be connected, as shown in the following figure.



Parameters description:

- `Host name / address` : refers to 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. Perform the following steps to find the connection address and port number of the RDS instance.

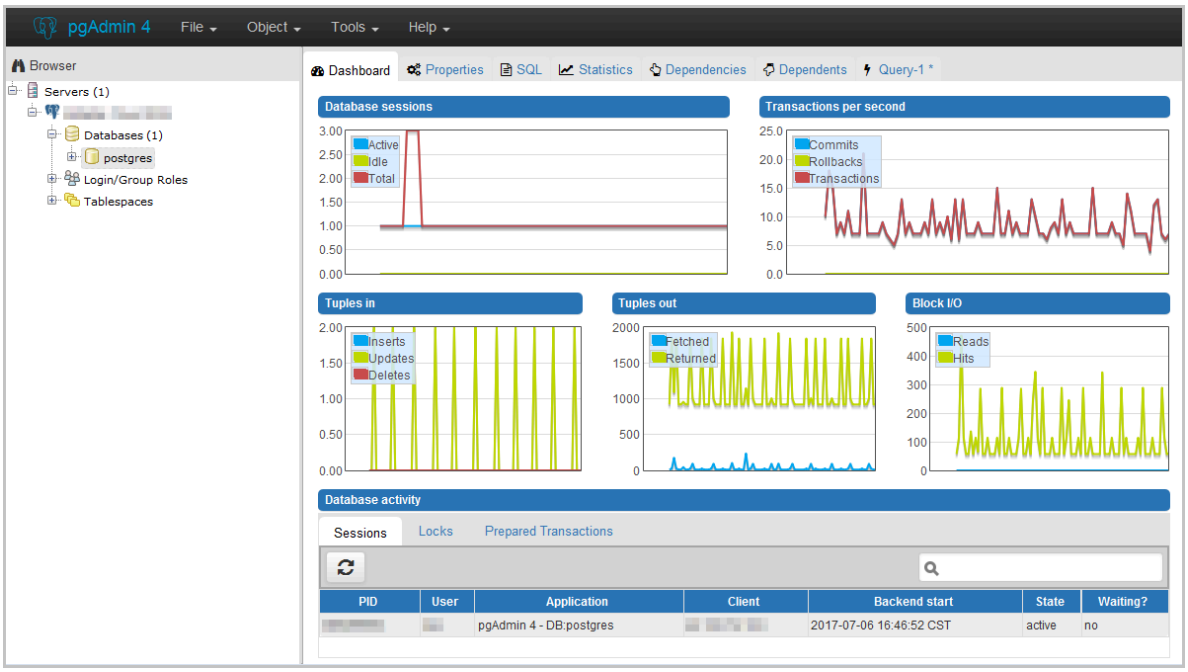
a. Log on to the RDS console.
b. Select the region where the target instance is located.
c. Click the ID of the instance to visit the Basic Information page.
d. In the Basic Information area, you can find the connection addresses and port numbers of the RDS instance.

- `Port` : refers to 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` : refers to the initial account name of the RDS instance.
- `Password` : refers to the password of the initial account name of the RDS instance.

6. Click Save.
7. If the connection information is correct, select 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.



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.