Alibaba Cloud
ApsaraDB for MySQL

Quick Start for PostgreSQL

Issue: 20190920

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 informatio n, 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 of RDS for PostgreSQL

This topic describes the limits of RDS for PostgreSQL. To guarantee stability and security, you must note the limits when using RDS for PostgreSQL instances.

The following table describes the limits of RDS for PostgreSQL.

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

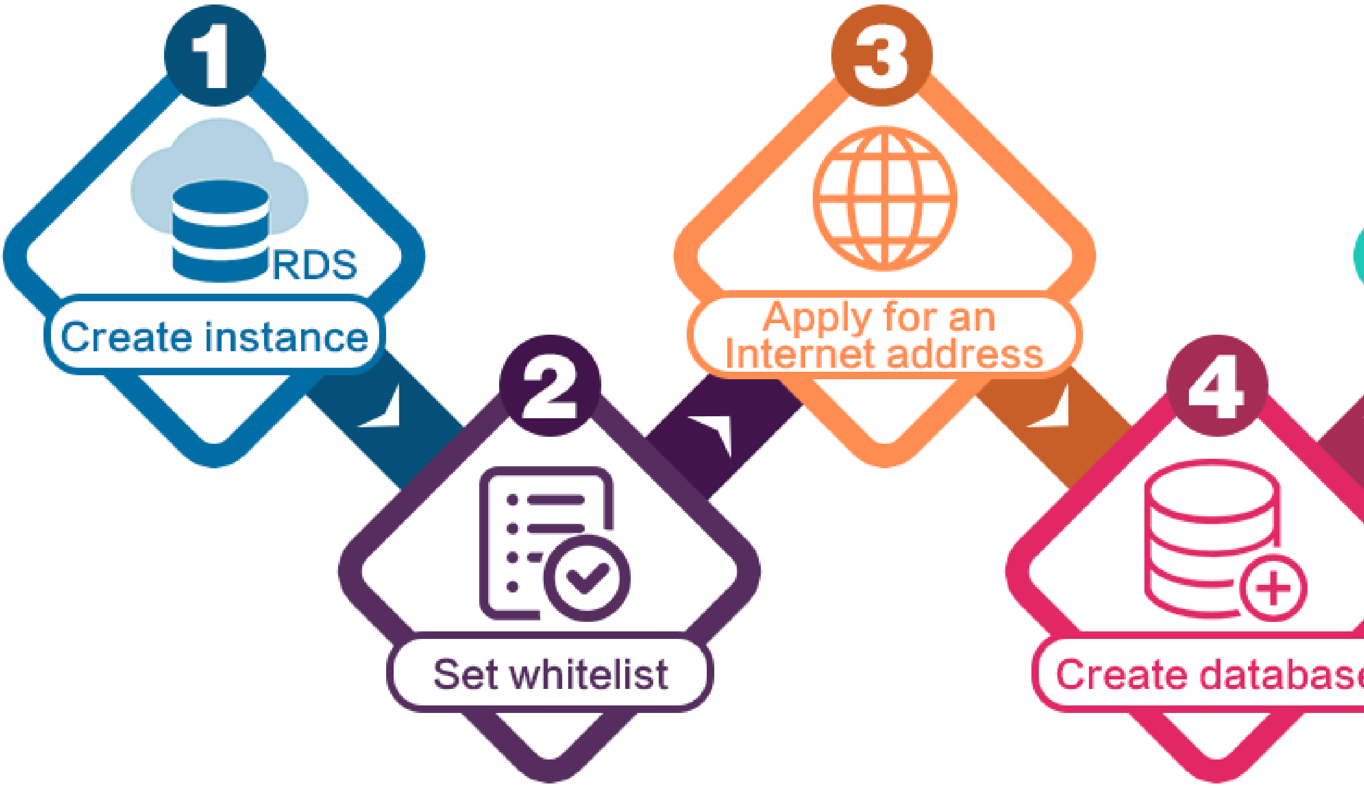
2 General process to use RDS for PostgreSQL

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

Quick start flowchart

If this is the first time that you use RDS for PostgreSQL, read #unique_6 before you purchase an RDS for PostgreSQL instance.

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



3 Create an RDS for PostgreSQL instance

This topic describes how to create an RDS for PostgreSQL instance by using the RDS console.

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

For information about the pricing of RDS for PostgreSQL instances, see #unique_9.

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_10.
- 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_9.

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_9.
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.

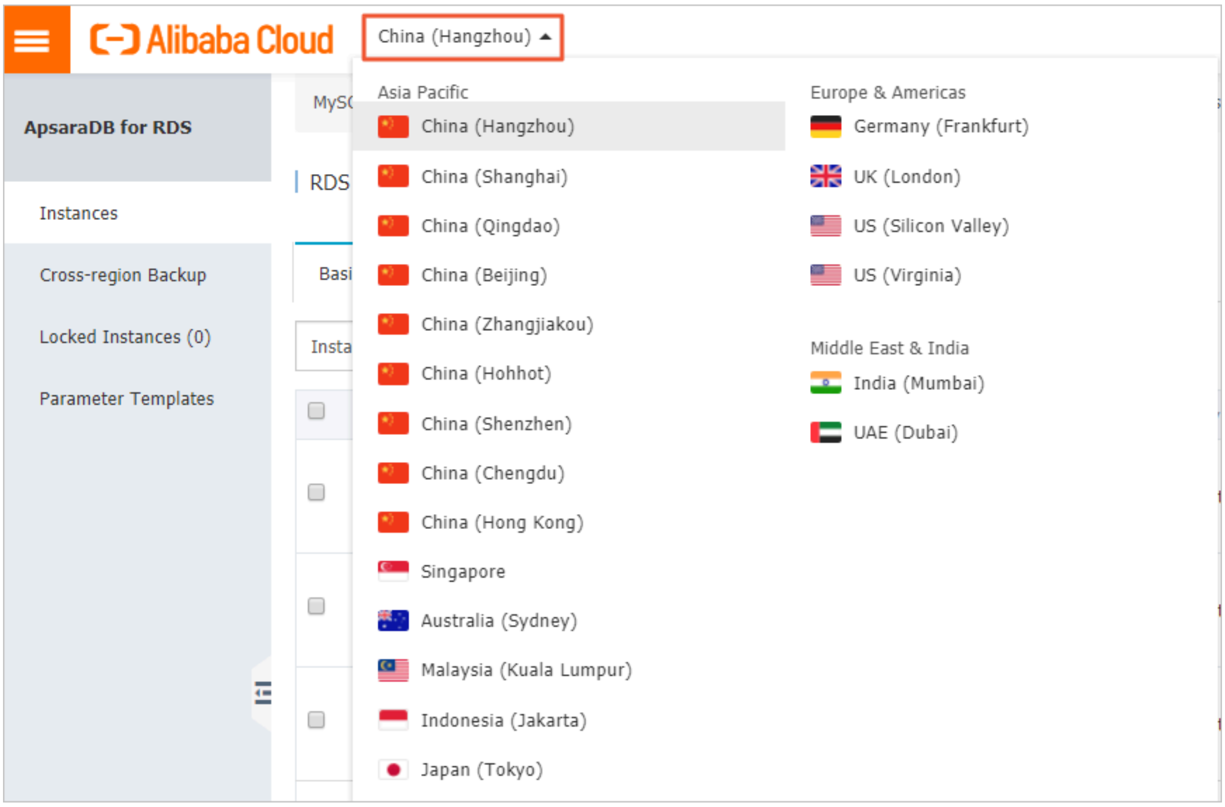
4. Set Quantity and Duration (the Duration parameter is available only when you are creating a subscription instance), then click Buy Now.

> 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 #unique_17.

APIs

API	Description
#unique_18	Used to create an RDS instance.

4 Initial configuration

4.1 Configure a whitelist for an RDS for PostgreSQL instance

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

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)

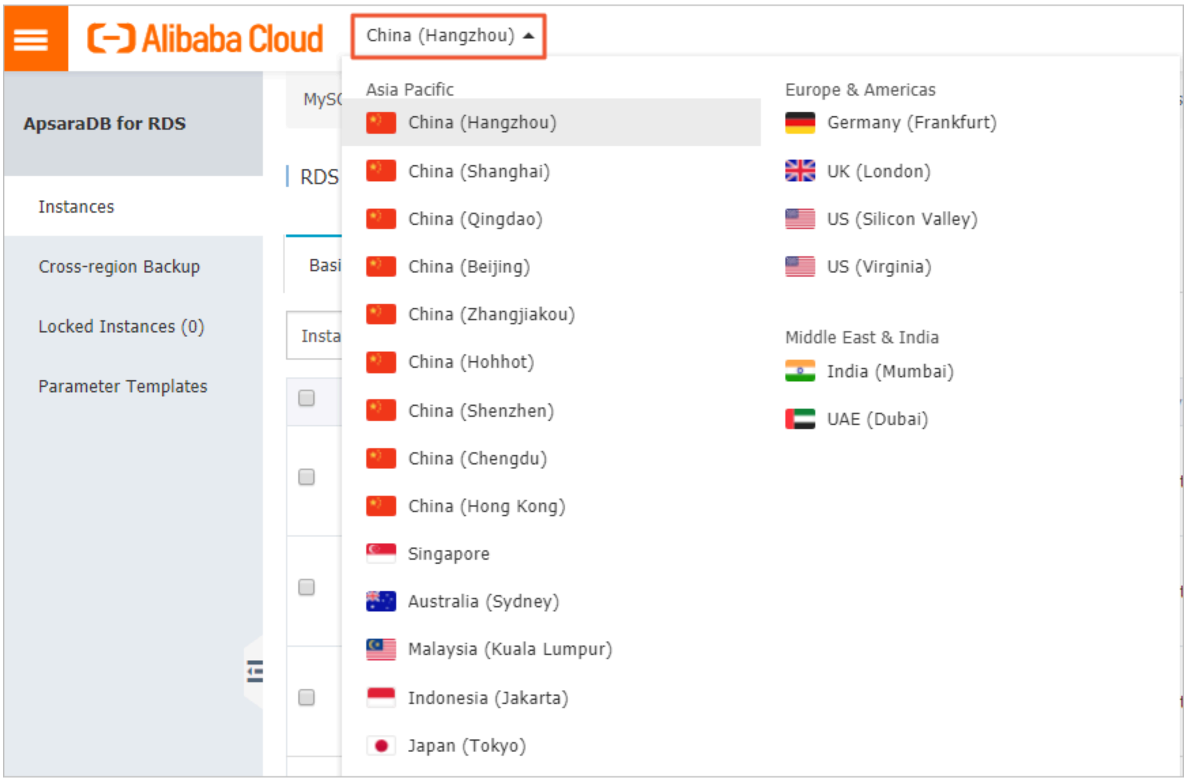
Precautions

- 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

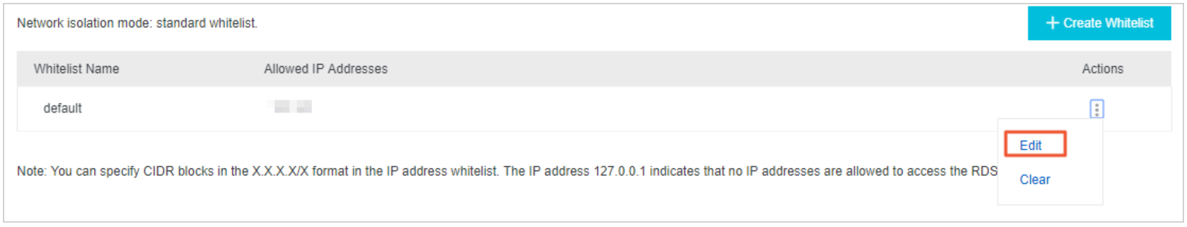
1. Log on to the PostgreSQL console.

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.



Network isolation mode: standard whitelist.

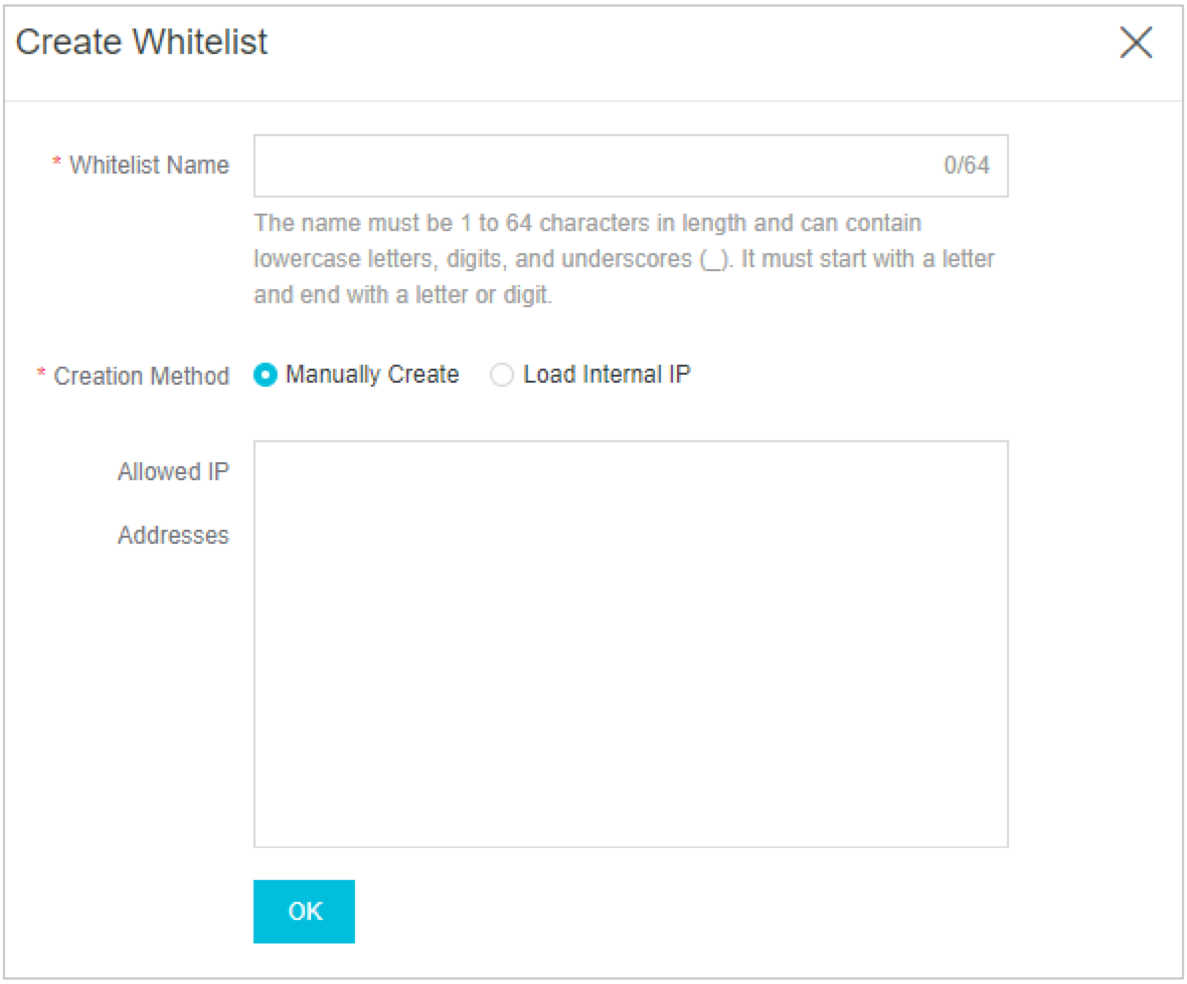
Whitelist Name	Allowed IP Addresses	Actions
default	[redacted]	⋮

Note: You can specify CIDR blocks in the X.X.X.X/X format in the IP address whitelist. The IP address 127.0.0.1 indicates that no IP addresses are allowed to access the RDS

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.



Create Whitelist

* Whitelist Name 0/64

The name must be 1 to 64 characters in length and can contain lowercase letters, digits, and underscores (_). It must start with a letter and end with a letter or digit.

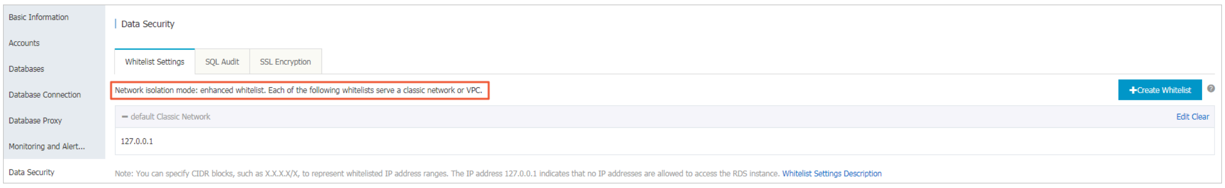
* Creation Method ● Manually Create ○ Load Internal IP

Allowed IP Addresses

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.

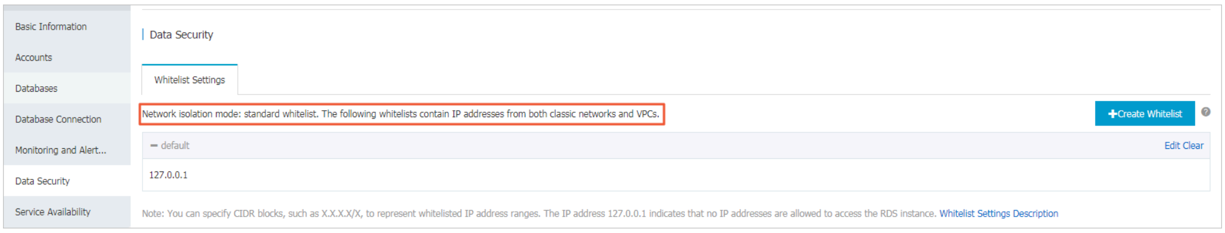


Network isolation mode: enhanced whitelist. Each of the following whitelists serve a classic network or VPC.

default Classic Network

127.0.0.1

Note: You can specify CIDR blocks, such as X.X.X.X/X, to represent whitelisted IP address ranges. The IP address 127.0.0.1 indicates that no IP addresses are allowed to access the RDS instance. Whitelist Settings Description



Network isolation mode: standard whitelist. The following whitelists contain IP addresses from both classic networks and VPCs.

default

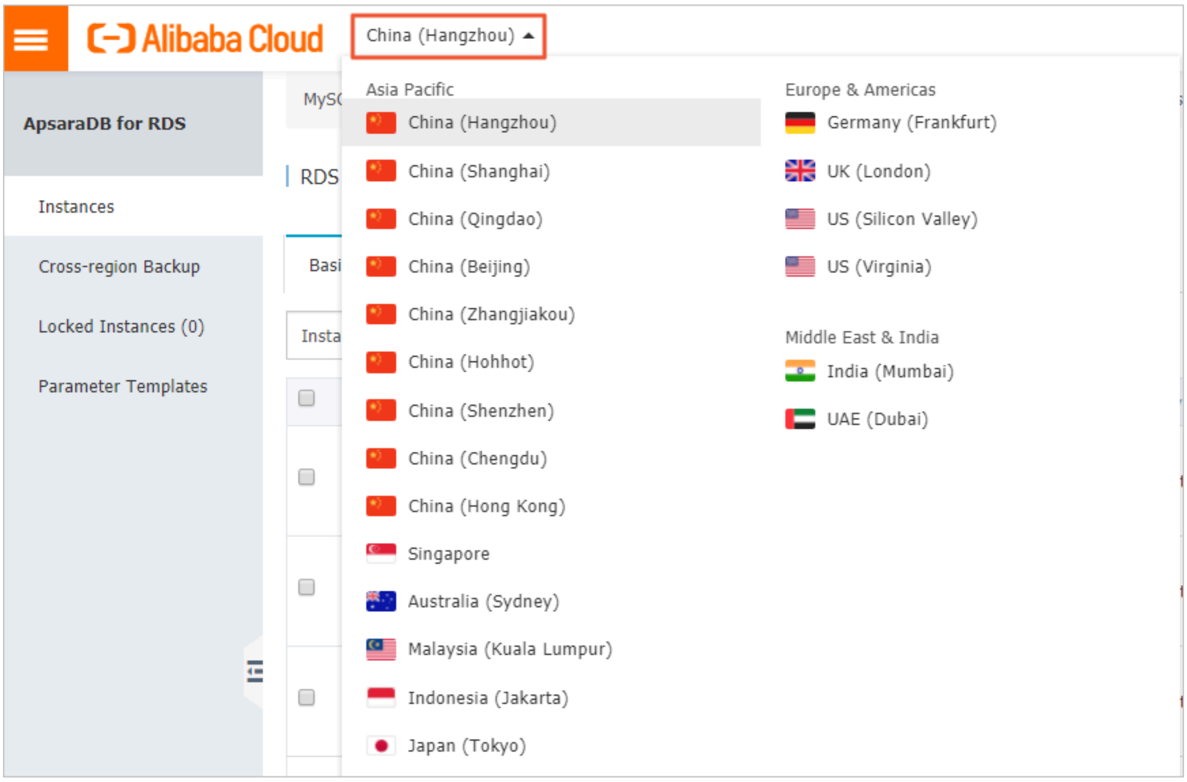
127.0.0.1

Note: You can specify CIDR blocks, such as X.X.X.X/X, to represent whitelisted IP address ranges. The IP address 127.0.0.1 indicates that no IP addresses are allowed to access the RDS instance. Whitelist Settings Description

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.

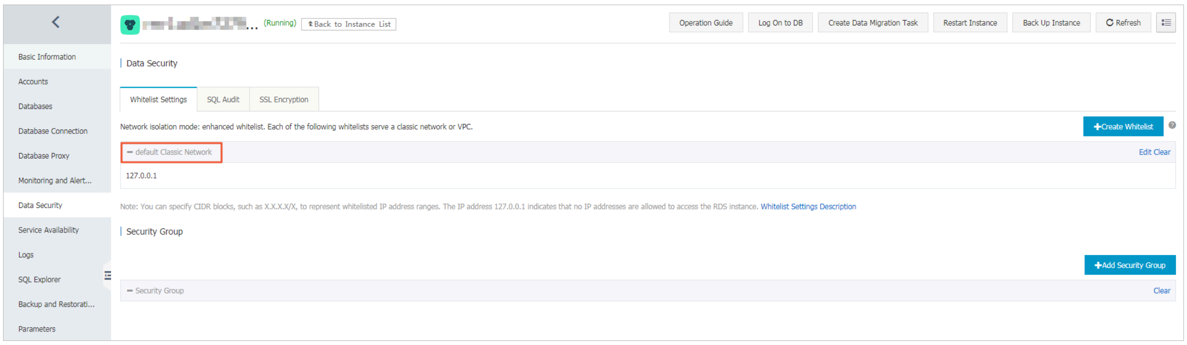


3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Data Security.
5. On the Whitelist Settings tab, select the whitelist you want to modify. Detailed steps are as follows:
   - If you want to connect the RDS instance to an ECS instance that is located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



Network isolation mode: enhanced whitelist. Each of the following whitelists serve a classic network or VPC.

127.0.0.1

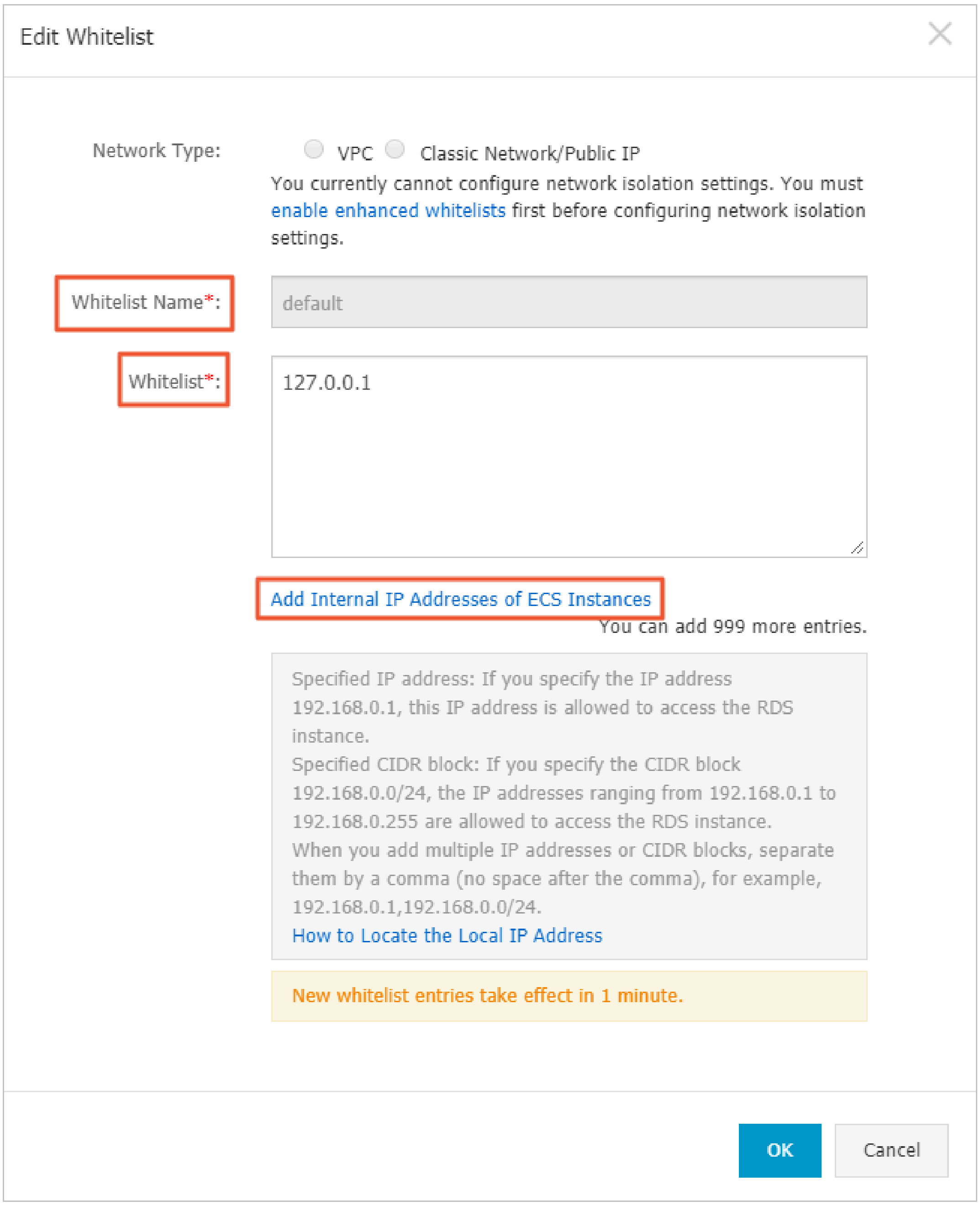
Note: You can specify CIDR blocks, such as X.X.X.X/X, to represent whitelisted IP address ranges. The IP address 127.0.0.1 indicates that no IP addresses are allowed to access the RDS instance. Whitelist Settings Description

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.



Edit Whitelist

Network Type: ○ VPC ○ Classic Network/Public IP

You currently cannot configure network isolation settings. You must enable enhanced whitelists first before configuring network isolation settings.

Whitelist Name*: default

Whitelist*: 127.0.0.1

Add Internal IP Addresses of ECS Instances

You can add 999 more entries.

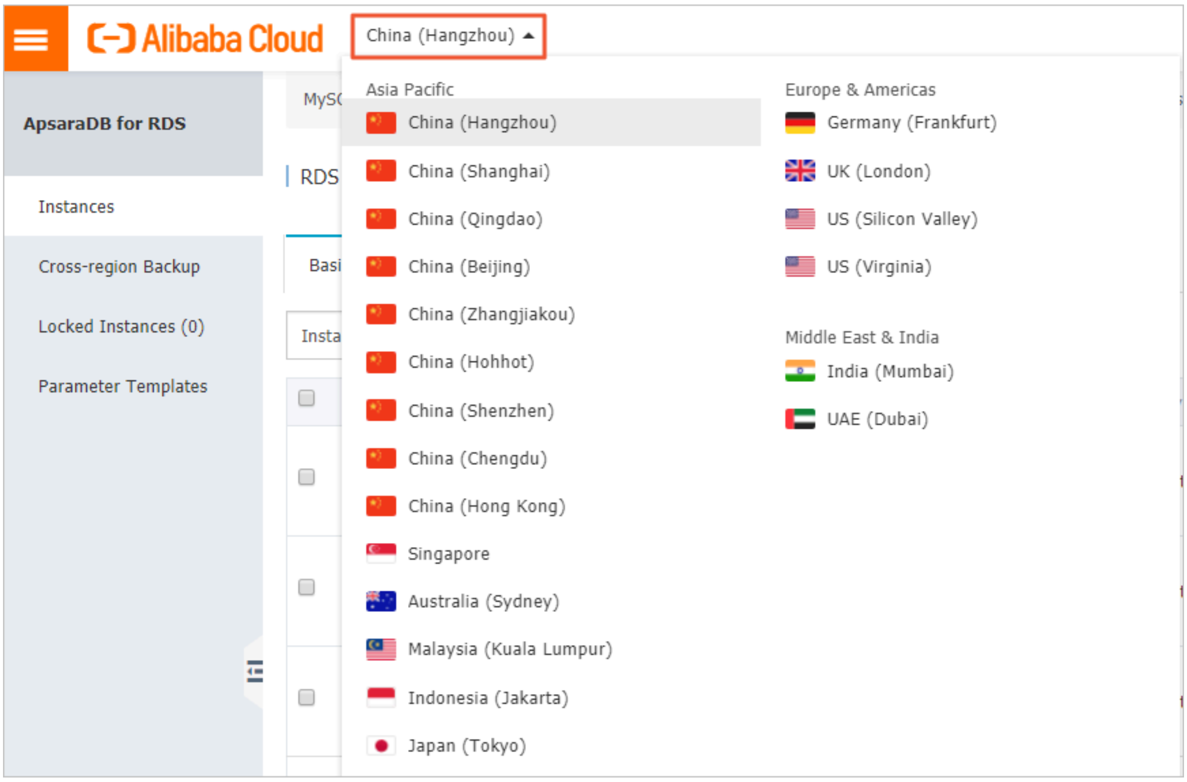
Specified IP address: If you specify the IP address 192.168.0.1, this IP address is allowed to access the RDS instance.
Specified CIDR block: If you specify the CIDR block 192.168.0.0/24, the IP addresses ranging from 192.168.0.1 to 192.168.0.255 are allowed to access the RDS instance.
When you add multiple IP addresses or CIDR blocks, separate them by a comma (no space after the comma), for example, 192.168.0.1,192.168.0.0/24.
How to Locate the Local IP Address

New whitelist entries take effect in 1 minute.

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.



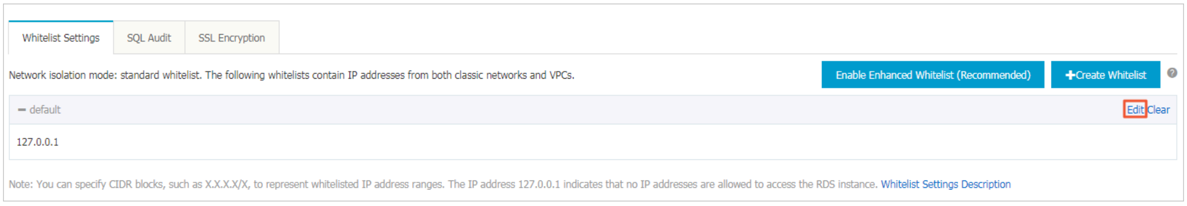
3. Find the target RDS instance and click the instance ID.

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.



Network isolation mode: standard whitelist. The following whitelists contain IP addresses from both classic networks and VPCs.

− default

127.0.0.1

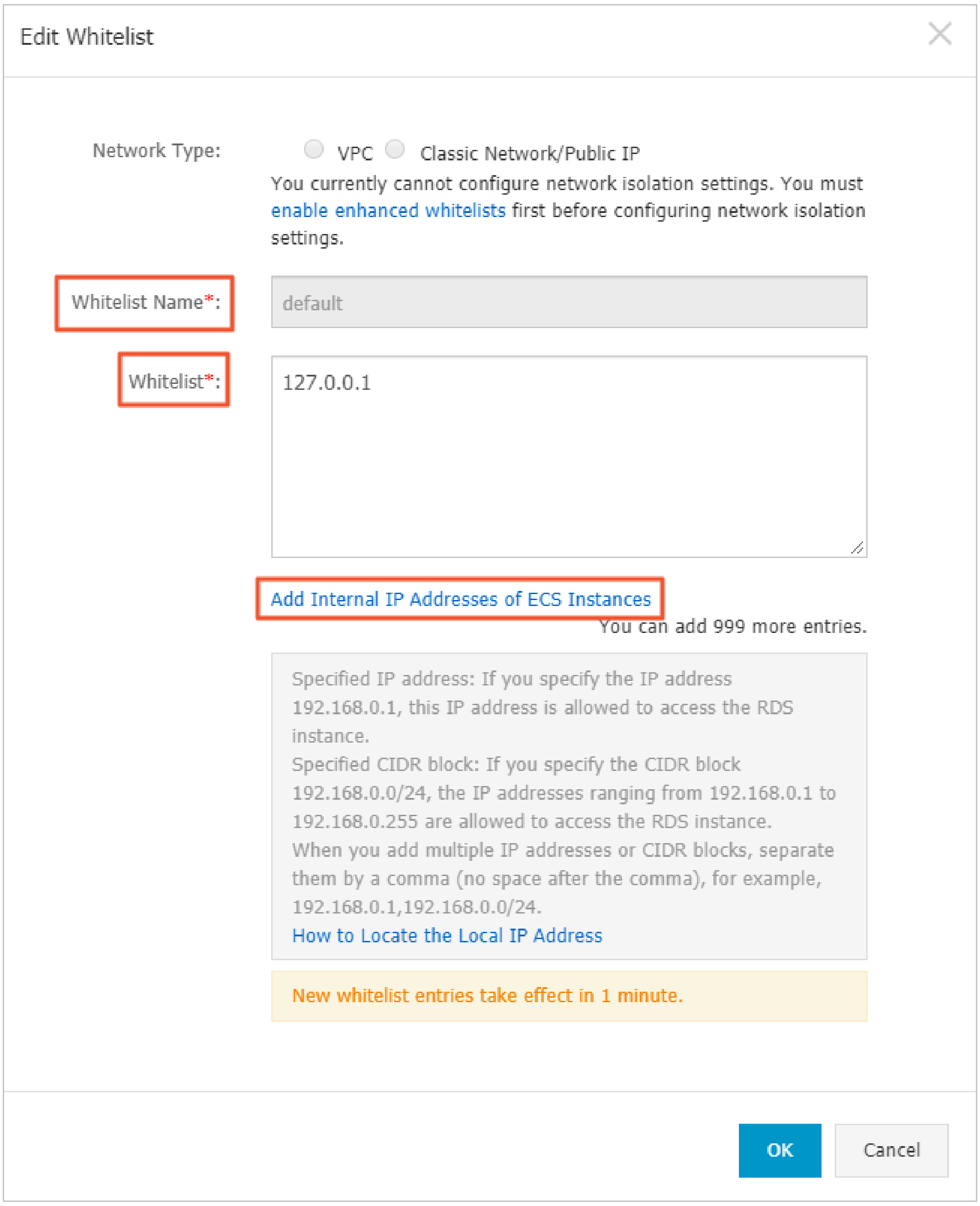
Note: You can specify CIDR blocks, such as X.X.X.X/X, to represent whitelisted IP address ranges. The IP address 127.0.0.1 indicates that no IP addresses are allowed to access the RDS instance. Whitelist Settings Description

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.



Edit Whitelist

Network Type: ○ VPC ○ Classic Network/Public IP

You currently cannot configure network isolation settings. You must enable enhanced whitelists first before configuring network isolation settings.

Whitelist Name*: default

Whitelist*: 127.0.0.1

Add Internal IP Addresses of ECS Instances

You can add 999 more entries.

Specified IP address: If you specify the IP address 192.168.0.1, this IP address is allowed to access the RDS instance.
Specified CIDR block: If you specify the CIDR block 192.168.0.0/24, the IP addresses ranging from 192.168.0.1 to 192.168.0.255 are allowed to access the RDS instance.
When you add multiple IP addresses or CIDR blocks, separate them by a comma (no space after the comma), for example, 192.168.0.1,192.168.0.0/24.
How to Locate the Local IP Address

New whitelist entries take effect in 1 minute.

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 .

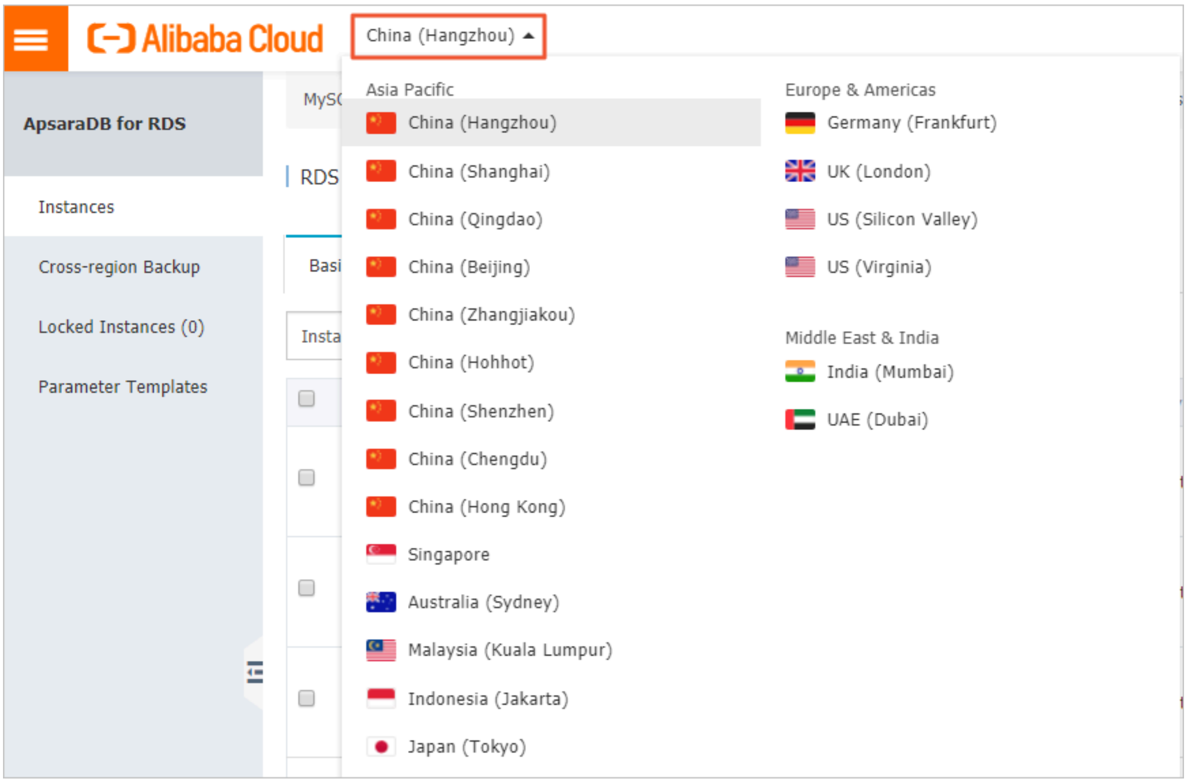
For more information, see Create a security group.

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 for an RDS for PostgreSQL instance

This topic describes how to apply for a public endpoint for an RDS for PostgreSQL instance. Apsara for RDS supports two types of endpoints: internal endpoints and public endpoints. By default, the system provides you with an internal endpoint for connecting to your RDS instance. If you want to connect to your RDS instance through the Internet, you must apply for a public endpoint.

Internal and public endpoints

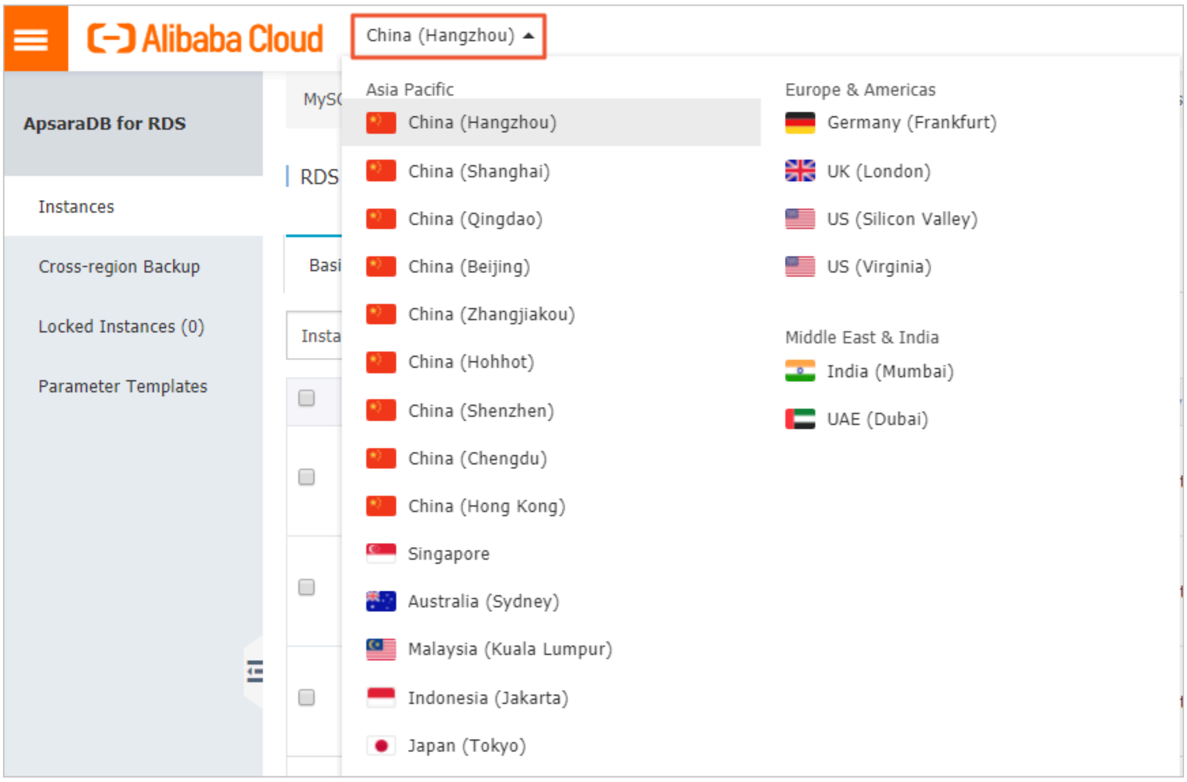
Endpoint type	Description
Internal endpoint	· An internal endpoint is generated by default. · If your application is deployed on an ECS instance that is located in the same region as your RDS instance and, at the same time, the ECS instance has the same network type as your RDS instance, your RDS instance 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)

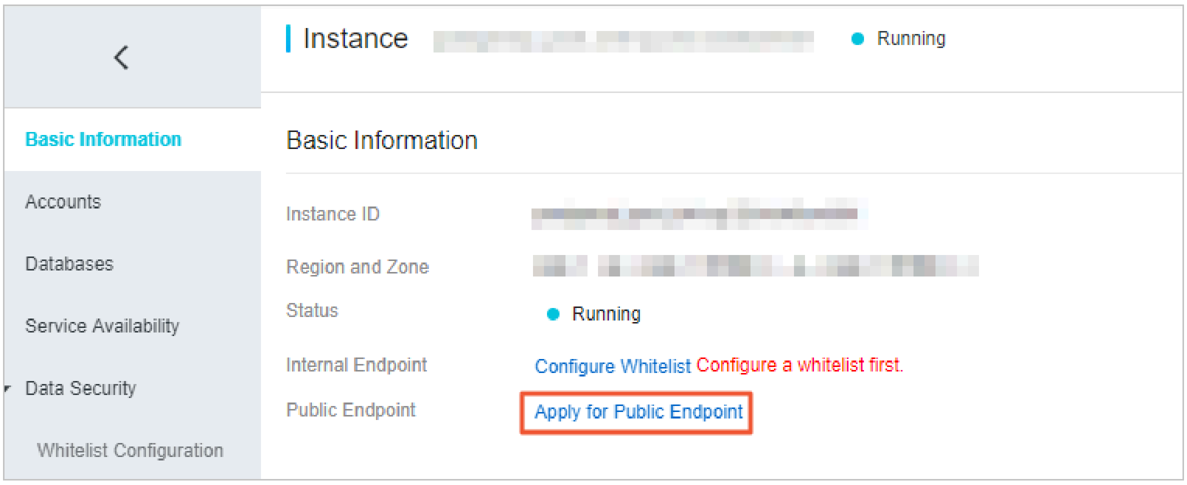
1. Log on to the PostgreSQL console.

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.



Basic Information

Instance ID

Region and Zone

Status: Running

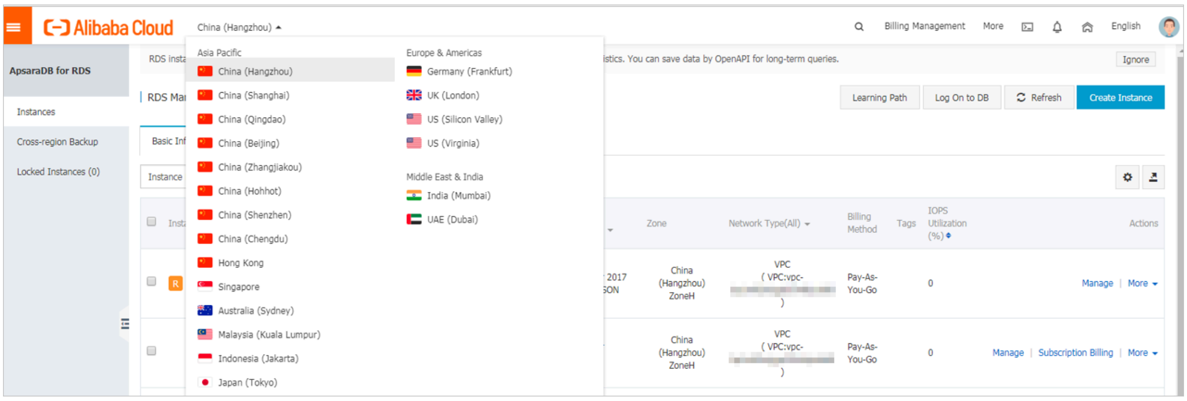
Internal Endpoint: Configure Whitelist Configure a whitelist first.

Public Endpoint: Apply for Public Endpoint

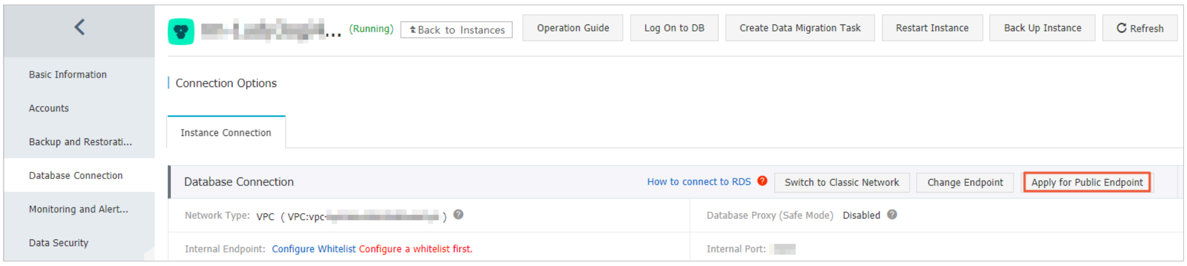
PostgreSQL 10 High-availability Edition (with local SSDs), PostgreSQL 10 Basic Edition, or PostgreSQL 9.4

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.



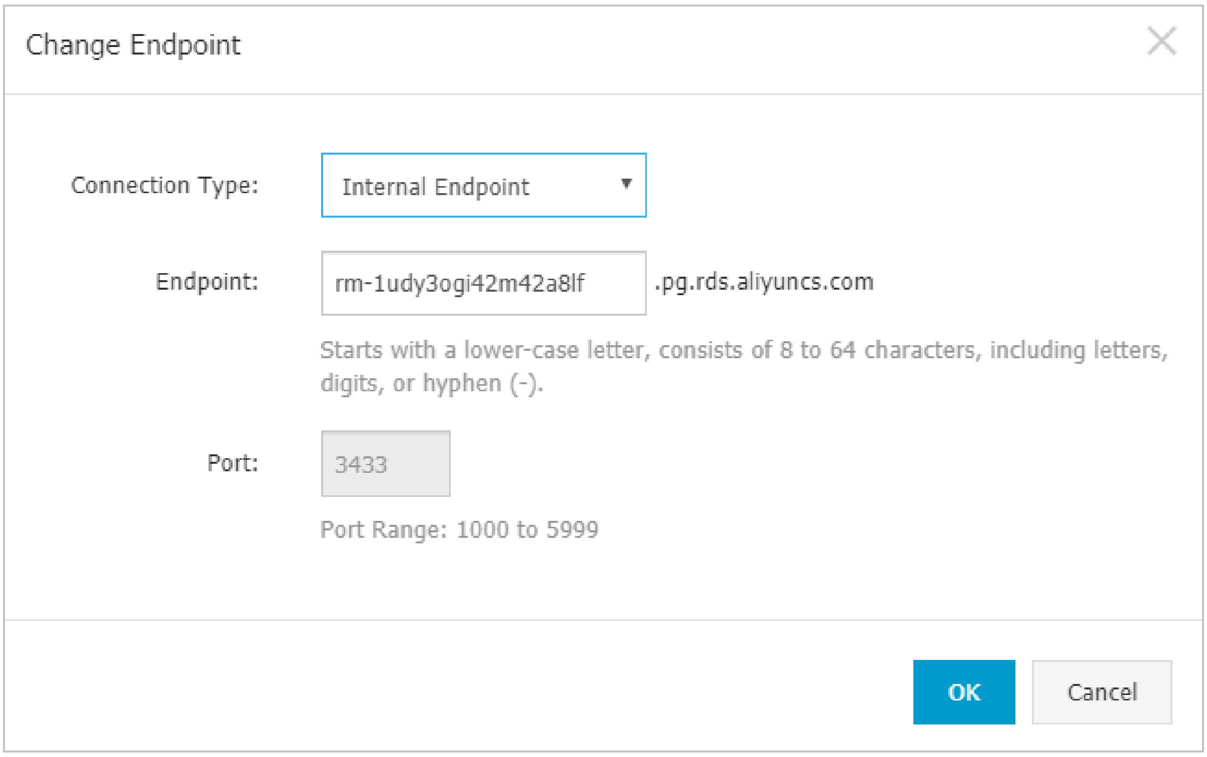
6. In the displayed dialog box, click OK.

   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.



Change Endpoint

Connection Type: Internal Endpoint

Endpoint: rm-1udy3ogi42m42a8lf .pg.rds.aliyuncs.com

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

Port: 3433

Port Range: 1000 to 5999

APIs

API	Description
#unique_28	Used to apply for an internal endpoint for an RDS instance.

4.3 Create databases and accounts for an PostgreSQL instance

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

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

- 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 premier account in the RDS console , and then create and manage databases by using the DMS console or a database client.

Account types

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

Account type	Description
Premier accounts	· You can create and manage premier accounts only in the console or through APIs. · In PostgreSQL 10 High-availability Edition (with local SSDs), PostgreSQL 10 Basic Edition, and PostgreSQL 9.4, you can create only one premier account for an RDS instance, and this premier account has the permissions to manage all standard accounts and databases in the RDS instance. · In PostgreSQL 11 High-availability Edition (with SSDs) and PostgreSQL 10 High-availability Edition (with SSDs), you can create one or more premier accounts for an RDS instance, and these premier account each have the permissions to manage all standard accounts and databases in the RDS instance. · More permissions are provided for premier accounts to manage permissions at finer levels based on individual needs. For example, you can grant the query permissions for tables by user. · A premier account has the permissions to disconnect the other accounts from the corresponding RDS instance.
Standard accounts	· You can create and manage standard accounts in the console, through APIs, or by running SQL statements. · You can create one or more standard accounts for an RDS instance. · You must manually grant the permissions for databases to standard accounts. · A standard account does not have the permissions to create, manage , or disconnect the other accounts from the corresponding RDS instance.

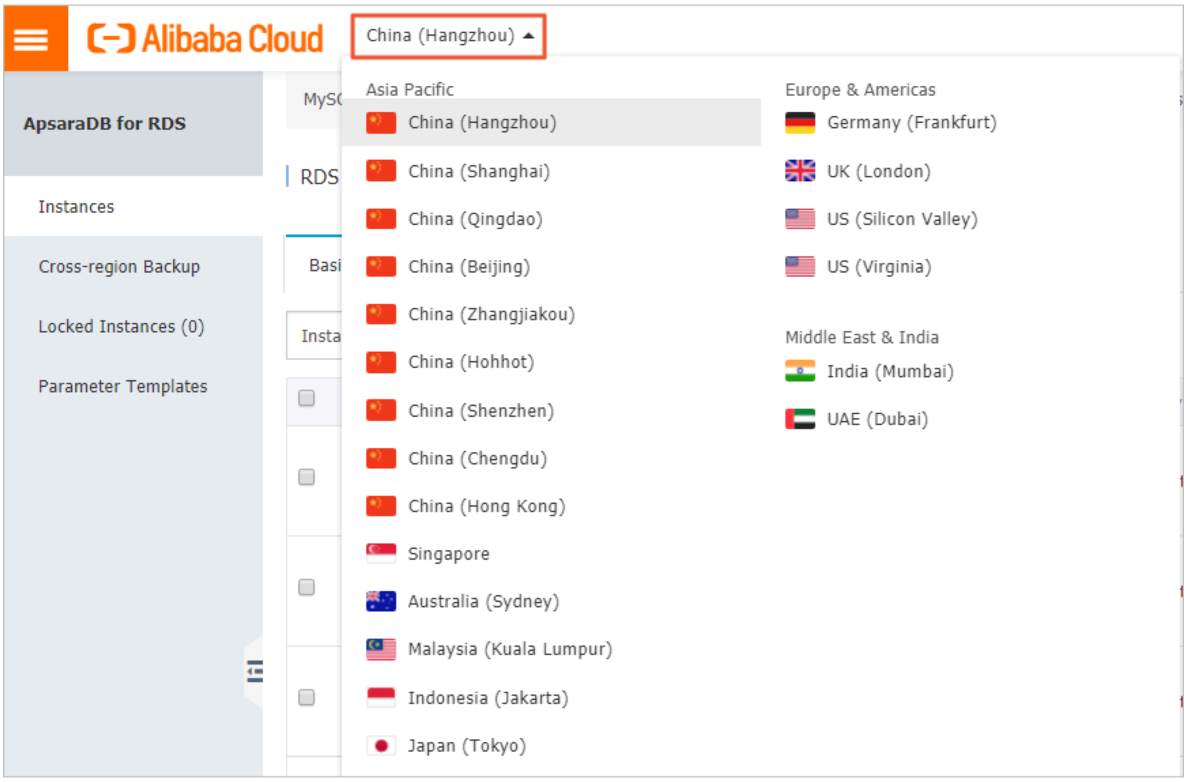
Precautions

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

- When assigning account permissions for each database, follow the minimum permission' principle and consider service roles to create accounts. 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.

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

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

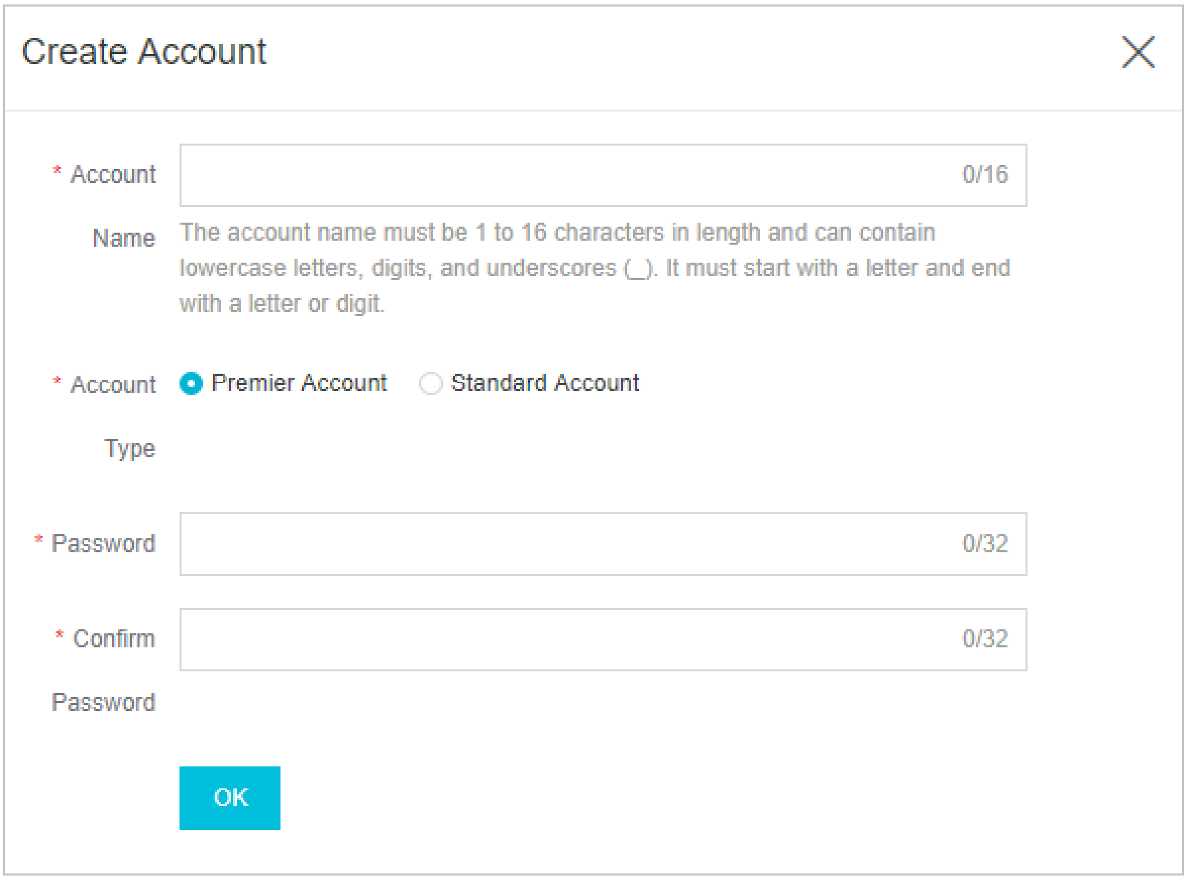


3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Accounts.
5. Click Create Account.

6. Set the following parameters.

Parameter	Description
Account Name	The name of the account. · The account name can contain up to 16 characters in length. · The account name can contain lowercase letters, digits, and underscores (_). · The account name must start with a lowercase letter and end with a lowercase letter or digit.
Account Type	Select Premier Account or Standard Account.
Password	The password of the account. · The account password must contain 8 to 32 characters in length. · The account password must contain at least three of the following types of characters: uppercase letters , lowercase letters, digits, and special characters. · The allowed special characters are as follows: ! @ # $ % ^ & * ( ) _ + - =

Parameter	Description
Confirm Password	Re-enter the password to confirm it.



Create Account

* Account Name 0/16

The account name must be 1 to 16 characters in length and can contain lowercase letters, digits, and underscores (_). It must start with a letter and end with a letter or digit.

* Account Type ● Premier Account ○ Standard Account

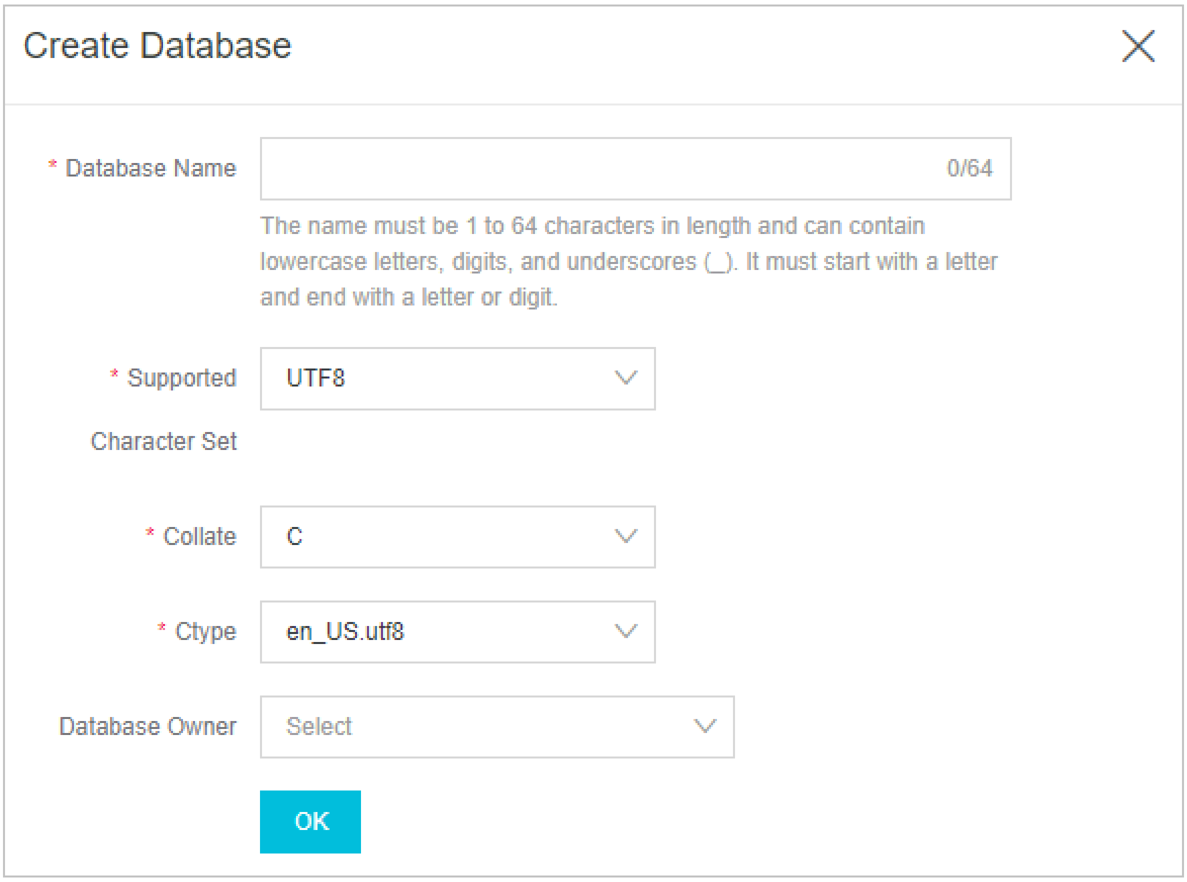
* Password 0/32

* Confirm Password 0/32

7. Click OK.
8. In the left-side navigation pane, click Databases.
9. Click Create Database.
10. Set the following parameters.

Parameter	Description
Database Name	The name of the database. · The database name can contain up to 64 characters in length. · The database name contain lowercase letters, digits, and underscores (_). · The database name must start with a lowercase letter and end with a lowercase letter or digit.
Supported Character Set	Select the character set supported by the database.
Collate	The rule for sorting strings.

Parameter	Description
Ctype	The type of character.
Database Owner	The owner of the database. This owner has all permissions for the database.



Create Database

* Database Name: 0/64

The name must be 1 to 64 characters in length and can contain lowercase letters, digits, and underscores (_). It must start with a letter and end with a letter or digit.

* Supported Character Set: UTF8

* Collate: C

* Ctype: en_US.utf8

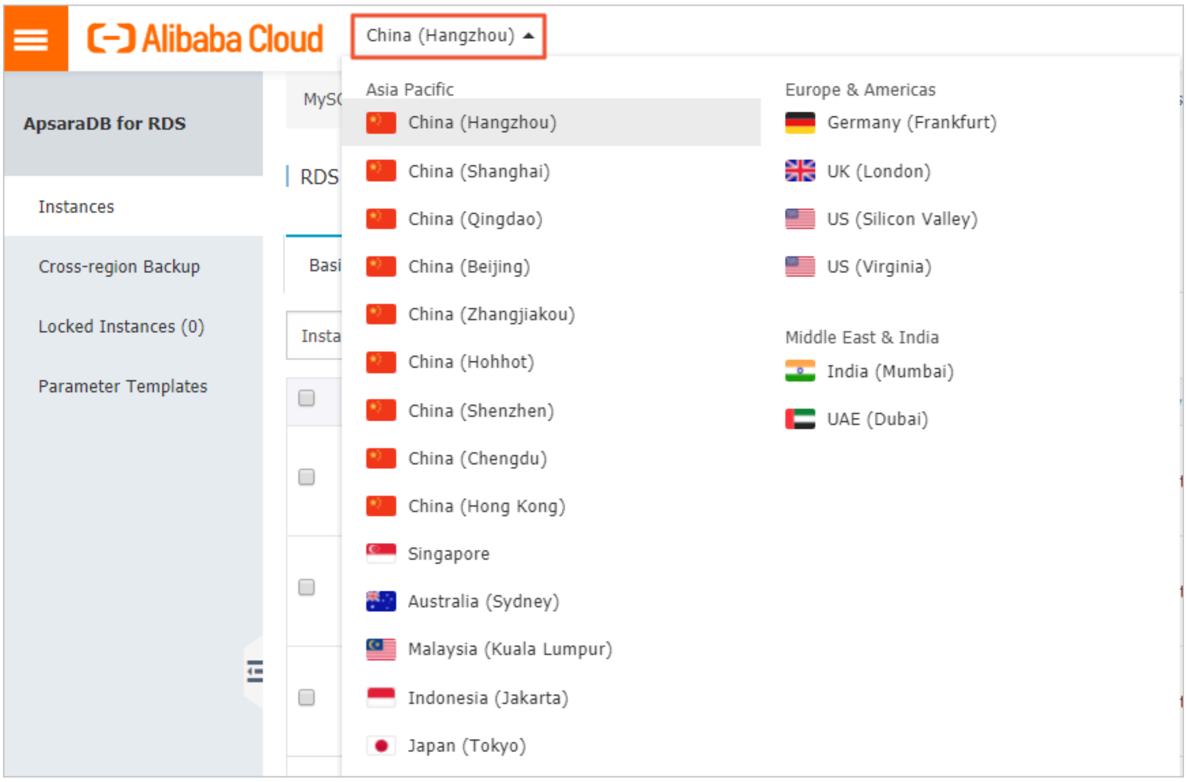
Database Owner: Select

11.Click OK.

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

1. Log on to the RDS console.

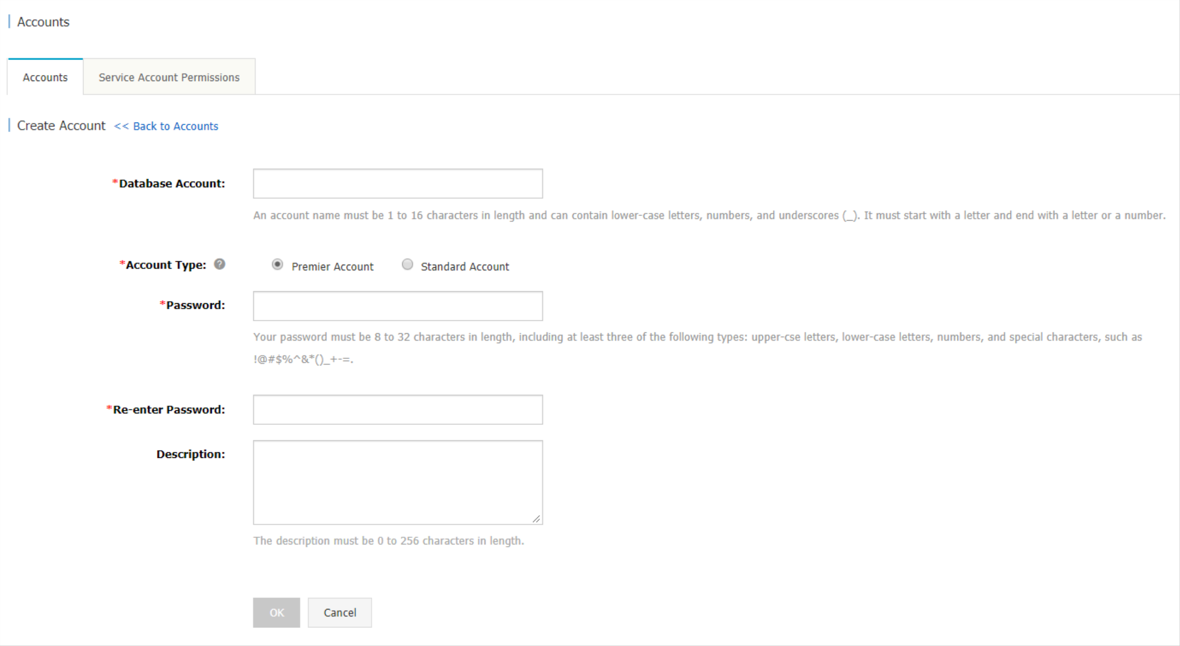
2. In the upper-left corner, select the region where the target RDS instance is located.



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

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

Parameter	Description
Re-enter Password	Re-enter the password to confirm it.



Accounts

Create Account << Back to Accounts

*Database Account:

An account name must be 1 to 16 characters in length and can contain lower-case letters, numbers, and underscores (_). It must start with a letter and end with a letter or a number.

*Account Type: ● Premier Account ○ Standard Account

*Password:

Your password must be 8 to 32 characters in length, including at least three of the following types: upper-cse letters, lower-case letters, numbers, and special characters, such as !@#$%^&*()_+-=.

*Re-enter Password:

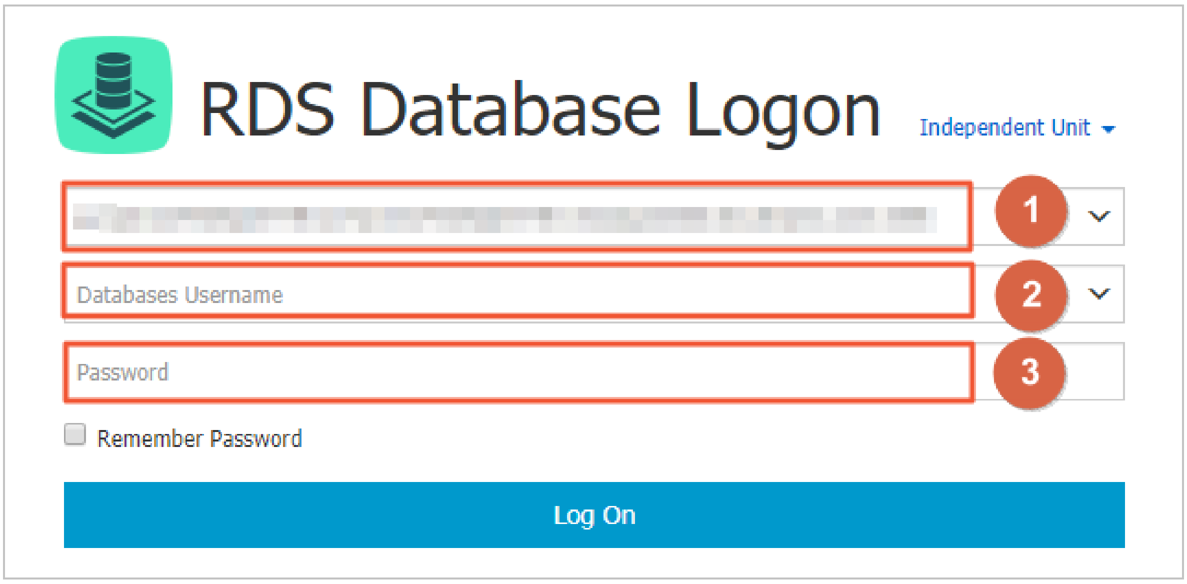
Description:

The description must be 0 to 256 characters in length.

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

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

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



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

10.Click Log On.

Note:

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

11.Optional. If the system prompts you to add the CIDR block where the DMS server is located to the whitelist of the RDS instance, see #unique_30.

12.Optional. After the whitelist is properly configured, click Log On.

13.After you log on to the RDS instance, choose SQL Operations > SQL Window from the main menu.

14.In the SQL window, enter the following command to create a database:

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

```
         [  CONNECTION   LIMIT  [=]  connlimit  ] ]
```

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

```
Create   database   test ;
```

15.Click execute to create the database.

16.In the SQL window, enter the following command to create a standard account:

```
CREATE   USER   name  [ [  WITH  ]  option  [ ... ] ]
where   option   can   be :
   SUPERUSER  |  NOSUPERUSE  R
|  CREATEDB  |  NOCREATEDB
|  CREATEROLE  |  NOCREATERO  LE
|  CREATEUSER  |  NOCREATEUS  ER
|  INHERIT  |  NOINHERIT
|  LOGIN  |  NOLOGIN
|  REPLICATIO  N  |  NOREPLICAT  ION
|  CONNECTION   LIMIT   connlimit
| [  ENCRYPTED  |  UNENCRYPTE  D  ]  PASSWORD  ' password '
|  VALID   UNTIL  ' timestamp '
|  IN   ROLE   role_name  [, ...]
|  IN   GROUP   role_name  [, ...]
|  ROLE   role_name  [, ...]
|  ADMIN   role_name  [, ...]
|  USER   role_name  [, ...]
|  SYSID   uid
```

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

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

17.Click execute to create the standard account.

FAQ

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

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

APIs

API	Description
#unique_31	Used to create an account.

5 Connect to an RDS for PostgreSQL instance

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

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

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

Background information

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

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

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

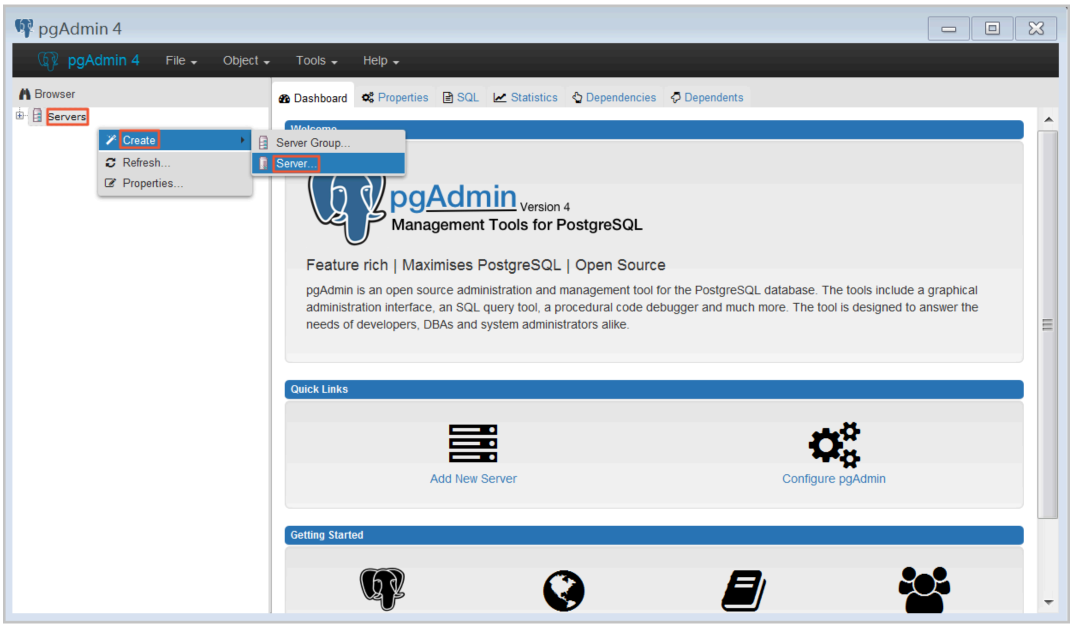
- Use the internal endpoint when your client is installed on an ECS instance that is located in the same region and the same network type as the RDS instance to be connected.
- Use the public endpoint for the other situations.

Connect to an RDS instance through DMS

For more information, see #unique_34.

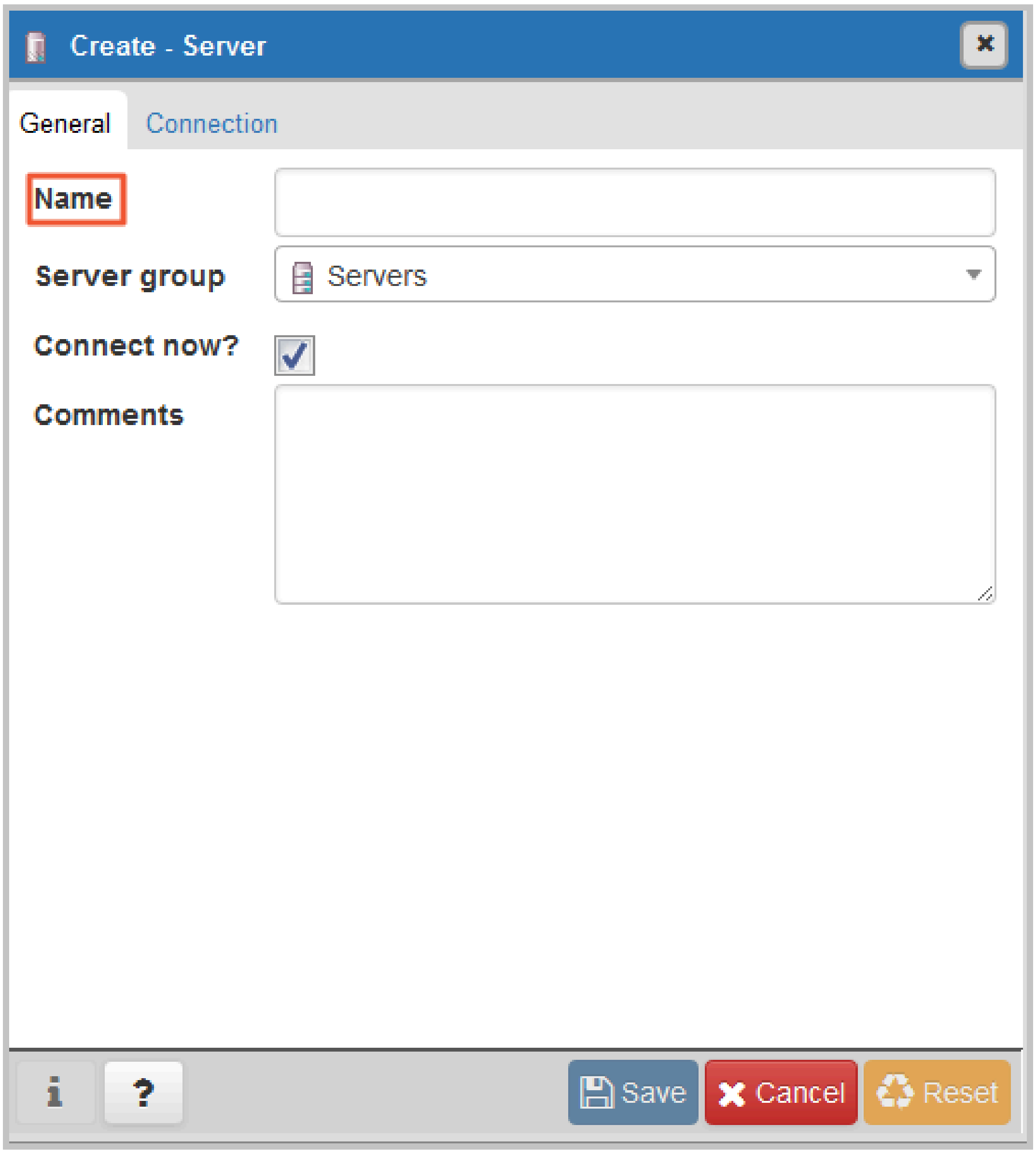
Connect to an RDS instance through a database client

1. Add the IP address of the device to access the RDS instance to a whitelist of the RDS instance. For more information, see #unique_30.
2. Start the pgAdmin 4 client.
3. Right-click Servers and choose Create > Server from the shortcut menu.



pgAdmin is an open source administration and management tool for the PostgreSQL database. The tools include a graphical administration interface, an SQL query tool, a procedural code debugger and much more. The tool is designed to answer the needs of developers, DBAs and system administrators alike.

4. On the General tab of the Create - Server dialog box, enter the server name.



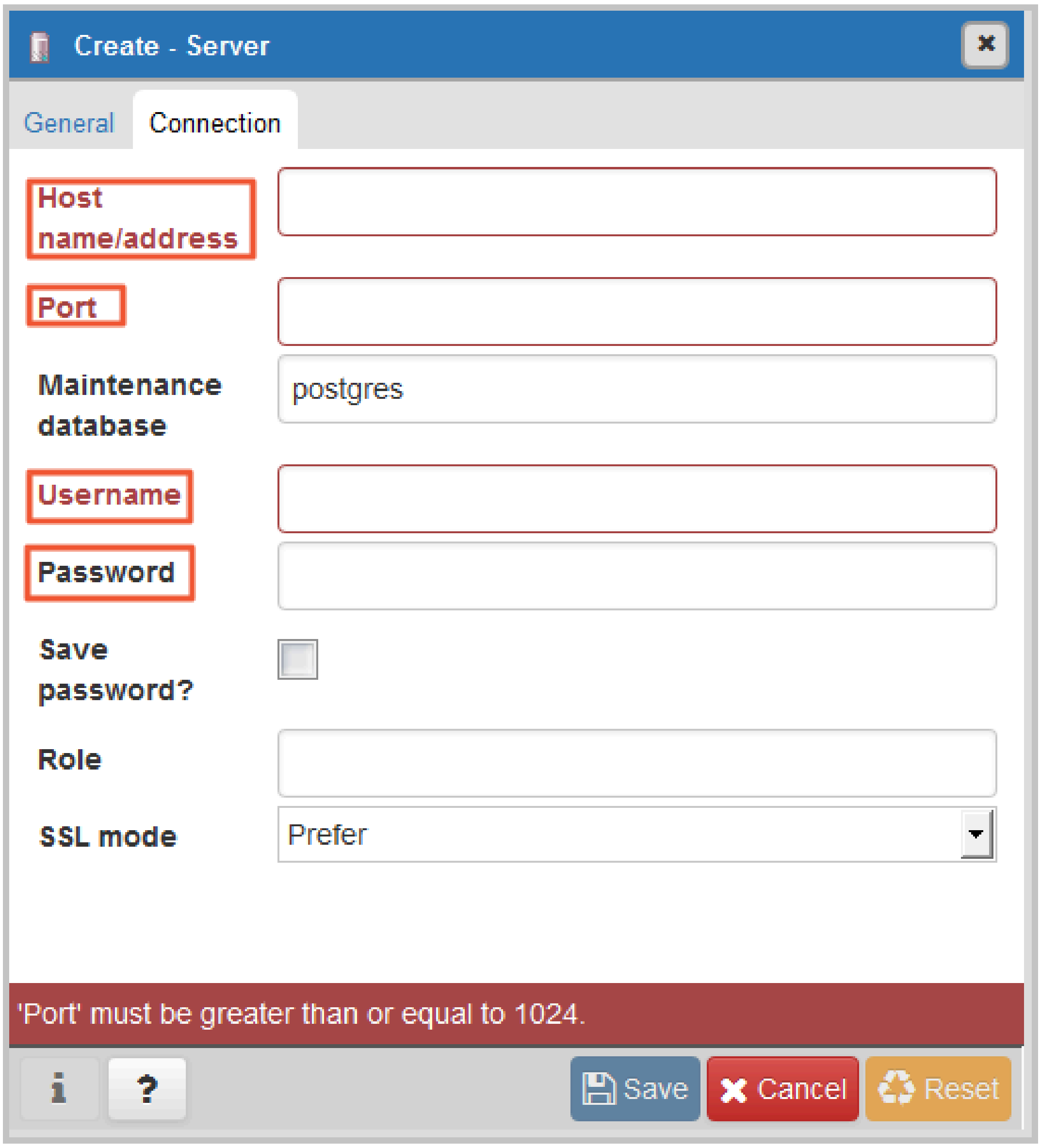
Name

Server group: Servers

Connect now? ☑

Comments

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



Host name/address:

Port:

Maintenance database: postgres

Username:

Password:

Save password? □

Role:

SSL mode: Prefer

'Port' must be greater than or equal to 1024.

Parameter description:

- `Host name / address` : to the endpoint of the RDS instance. If your application accesses the RDS instance through a private network, enter the internal endpoint of the RDS instance. If your application accesses the RDS instance through the Internet, enter the public endpoint of the RDS instance. To find the endpoints and ports of the RDS instance, follow these steps:

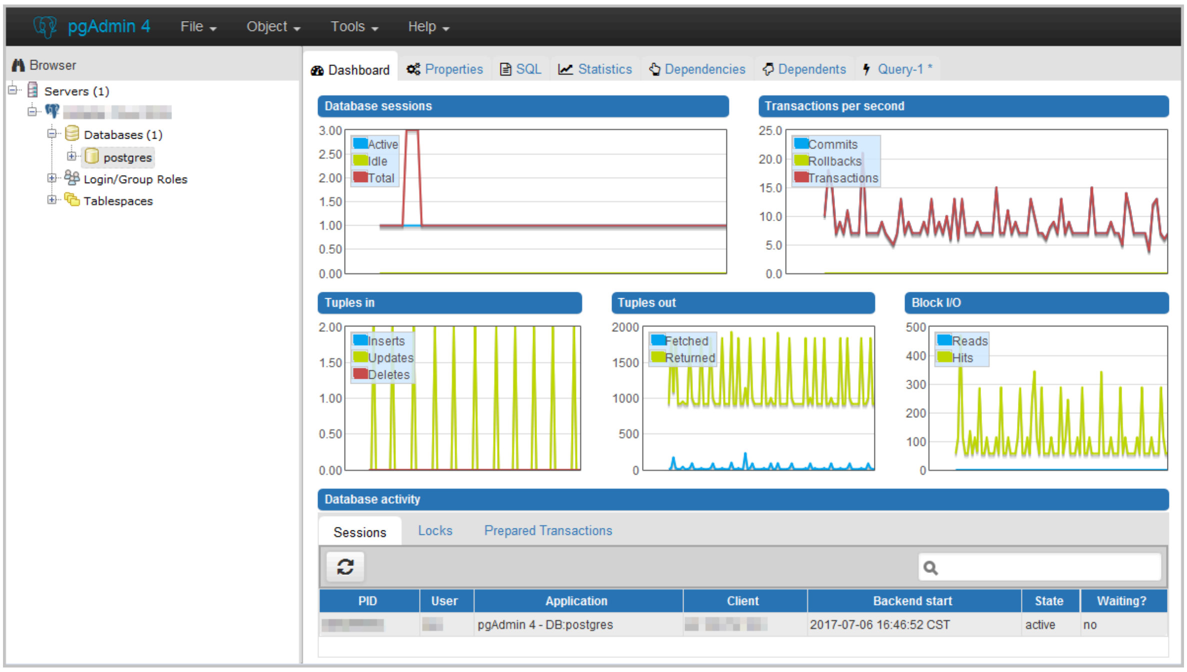
a. Log on to the RDS console.
b. Select the region where the target RDS instance is located.
c. Find the target RDS instance and click the instance ID.
d. In the Basic Information section of the Basic Information page, find the endpoints and ports of the RDS instance.

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

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

Note:

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



PID	User	Application	Client	Backend start	State	Waiting?
[redacted]	[redacted]	pgAdmin 4 - DB:postgres	[redacted]	2017-07-06 16:46:52 CST	active	no

6 RDS for PostgreSQL read-only instances

6.1 Introduction to RDS for PostgreSQL read-only instances

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

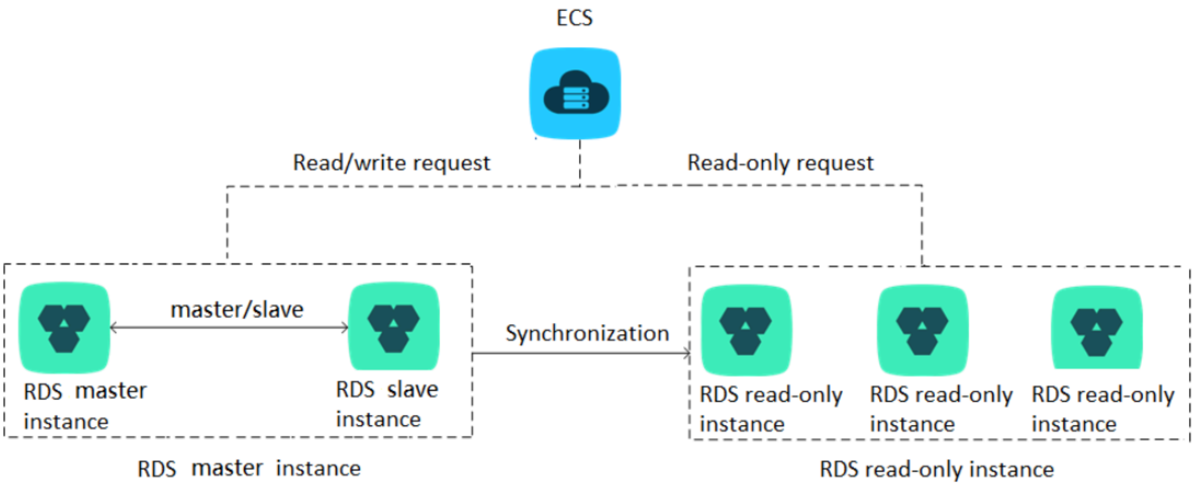
Overview

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

Note:

- Read-only instances must be PostgreSQL 10.0 High-Availability instances (with local SSDs).
- The configuration of the master instance must be at least 8-core 32 GB (dedicated or dedicated-host instance).
- Each read-only instance adopts a single-node architecture (without slave nodes).

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



Pricing

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

Features

Read-only instances offer the following features:

- Billing method: Pay-As-You-Go. This method is more flexible and cost-effective.
- Region and zone: A read-only instance must be in the same region as the master instance, but can be in a different zone from the master instance.
- Specifications and storage capacity: The specifications and storage capacity of a read-only instance cannot be lower than those of the master instance.
- Network type: The network type of a read-only instance can be different from that of the master instance.
- Account and database management: Users manage accounts and databases through the master instance rather than read-only instances.
- Whitelist: When a read-only instance is created, it automatically copies the whitelists of the master instance, but the whitelists of the read-only instance are independent of those of the master instance. You can modify the whitelists of a read-only instance according to #unique_37.
- Monitoring and alarming: You can monitor system performance metrics, including the disk capacity, IOPS, number of connections, and CPU usage.

Limits

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

FAQ

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

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

6.2 Create an RDS for PostgreSQL read-only instance

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

For more information, see #unique_39.

Prerequisites

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

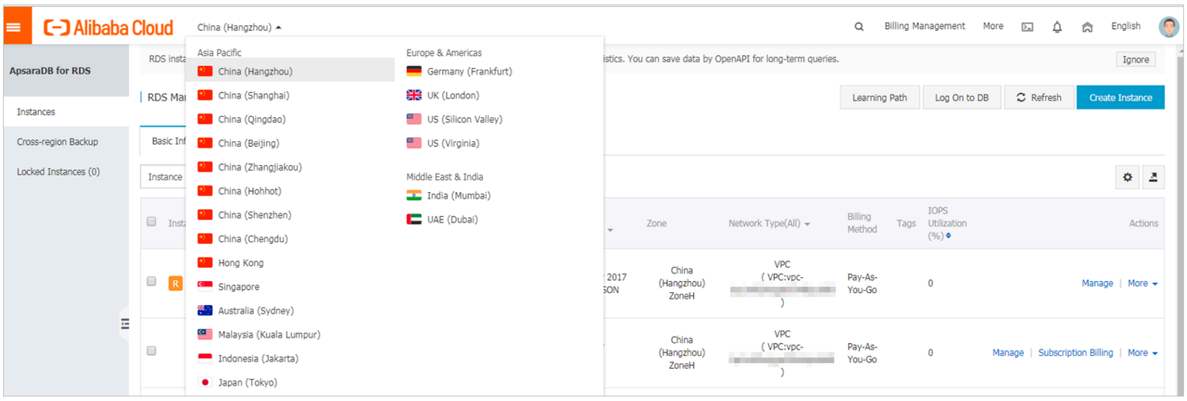
Precautions

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

Create a read-only instance

1. Log on to the RDS console.

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

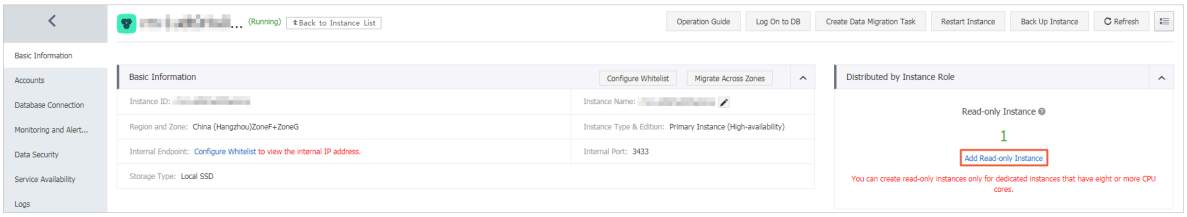


istics. You can save data by OpenAPI for long-term queries.

	Zone	Network Type(All)	Billing Method	Tags	IOPS Utilization (%)	Actions
2017 ON	China (Hangzhou) ZoneH	VPC (VPC:vpc-[redacted])	Pay-As-You-Go		0	Manage | More
	China (Hangzhou) ZoneH	VPC (VPC:vpc-[redacted])	Pay-As-You-Go		0	Manage | Subscription Billing | More

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

4. Click Add Read-only instance.



[redacted]... (Running)

Basic Information

Instance ID: [redacted]

Instance Name: [redacted]

Region and Zone: China (Hangzhou)ZoneF+ZoneG

Instance Type & Edition: Primary Instance (High-availability)

Internal Endpoint: Configure Whitelist to view the internal IP address.

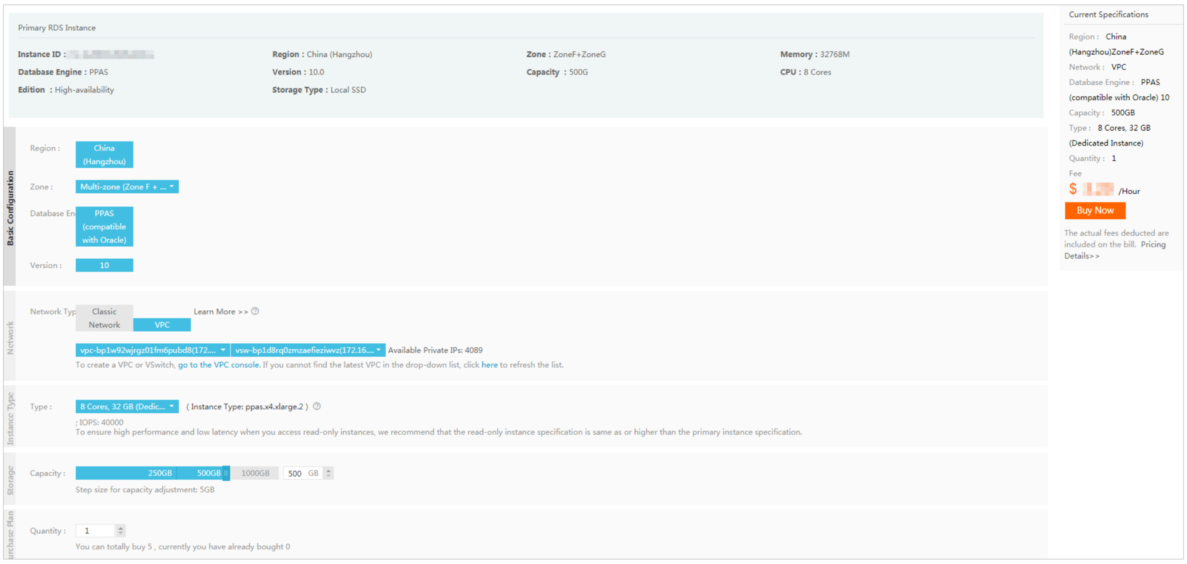
Internal Port: 3433

Storage Type: Local SSD

Read-only Instance 1

You can create read-only instances only for dedicated instances that have eight or more CPU cores.

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



Primary RDS Instance

Instance ID : [redacted]
Region : China (Hangzhou)
Zone : ZoneF+ZoneG
Memory : 32768M
Database Engine : PPAS
Version : 10.0
Capacity : 500G
CPU : 8 Cores
Edition : High-availability
Storage Type : Local SSD

Region : China (Hangzhou)

Zone : Multi-zone (Zone F + ...

Database En PPAS (compatible with Oracle)

Version : 10

Network Typ VPC

vpc-bp1w92wjrgz01fm6pubd8(172.... vsw-bp1d8rq0zmzaefieziwvz(172.16.... Available Private IPs: 4089

To create a VPC or VSwitch, go to the VPC console. If you cannot find the latest VPC in the drop-down list, click here to refresh the list.

Type : 8 Cores, 32 GB (Dedic... (Instance Type: ppas.x4.xlarge.2)

; IOPS: 40000

To ensure high performance and low latency when you access read-only instances, we recommend that the read-only instance specification is same as or higher than the primary instance specification.

Capacity : 250GB 500GB 1000GB 500 GB

Step size for capacity adjustment: 5GB

Quantity : 1

You can totally buy 5 , currently you have already bought 0

Current Specifications

Region : China (Hangzhou)ZoneF+ZoneG

Network : VPC

Database Engine : PPAS (compatible with Oracle) 10

Capacity : 500GB

Type : 8 Cores, 32 GB (Dedicated Instance)

Quantity : 1

Fee

$ [redacted] /Hour

The actual fees deducted are included on the bill.

Note:

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

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

The instance creation takes a few minutes.

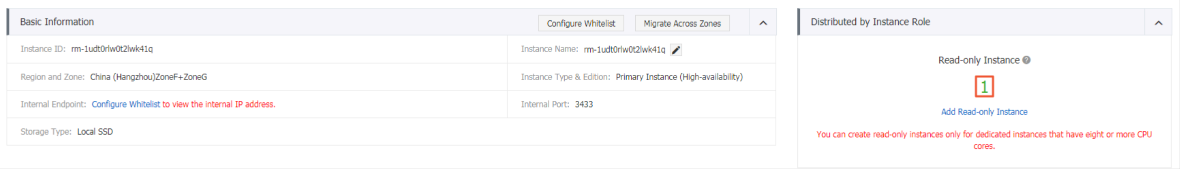
View a read-only instance

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

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

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

1. Log on to the RDS console.
2. Select the region where the master instance is located.
3. Find the master instance and click the instance ID.
4. On the Basic Information page, move the pointer over the number of read-only instances and click the ID of the read-only instance.



Instance ID: rm-1udt0rlw0t2lwk41q

Instance Name: rm-1udt0rlw0t2lwk41q

Region and Zone: China (Hangzhou)ZoneF+ZoneG

Instance Type & Edition: Primary Instance (High-availability)

Internal Endpoint: Configure Whitelist to view the internal IP address.

Internal Port: 3433

Storage Type: Local SSD

Read-only Instance

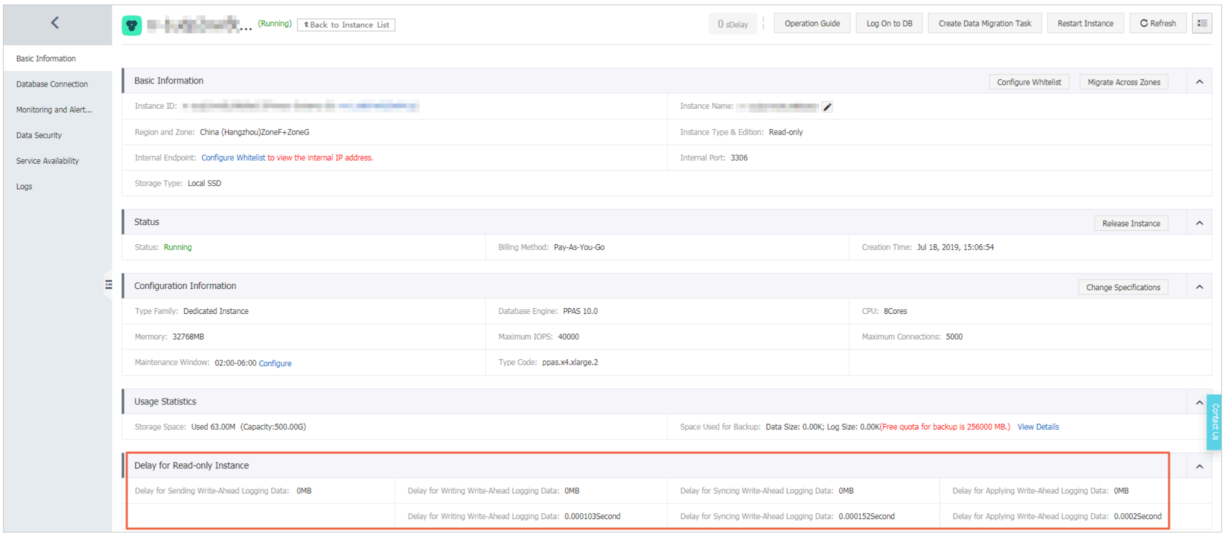
1

Add Read-only Instance

You can create read-only instances only for dedicated instances that have eight or more CPU cores.

View the delay of a read-only instance

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



[redacted]... (Running)

Basic Information

Instance ID: [redacted]

Instance Name: [redacted]

Region and Zone: China (Hangzhou)ZoneF+ZoneG

Instance Type & Edition: Read-only

Internal Endpoint: Configure Whitelist to view the internal IP address.

Internal Port: 3306

Storage Type: Local SSD

Status

Status: Running

Billing Method: Pay-As-You-Go

Creation Time: Jul 18, 2019, 15:06:54

Configuration Information

Type Family: Dedicated Instance

Database Engine: PPAS 10.0

CPU: 8Cores

Mermory: 32768MB

Maximum IOPS: 40000

Maximum Connections: 5000

Maintenance Window: 02:00-06:00 Configure

Type Code: ppas.x4.xlarge.2

Usage Statistics

Storage Space: Used 63.00M (Capacity:500.00G)

Space Used for Backup: Data Size: 0.00K; Log Size: 0.00K(Free quota for backup is 256000 MB.) View Details

Delay for Read-only Instance

Delay for Sending Write-Ahead Logging Data: 0MB

Delay for Writing Write-Ahead Logging Data: 0MB

Delay for Syncing Write-Ahead Logging Data: 0MB

Delay for Applying Write-Ahead Logging Data: 0MB

Delay for Writing Write-Ahead Logging Data: 0.000103Second

Delay for Syncing Write-Ahead Logging Data: 0.000152Second

Delay for Applying Write-Ahead Logging Data: 0.0002Second

APIs

API	Description
#unique_40	Used to create an RDS read-only instance.

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

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

oss_fdw parameters

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

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

CREATE SERVER parameters

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

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

- `oss_connect_timeout` : Connection expiration time, measured in seconds. Default value: 10s.
- `oss_dns_cache_timeout` : DNS expiration time, measured in seconds. Default value: 60s.

- `oss_speed_limit` : Minimum tolerable rate. Default value: 1,024 byte/s (1 Kbit/s).
- `oss_speed_time` : Maximum tolerable time. Default value: 15s.

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

CREATE FOREIGN TABLE parameters

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

    For example, if there are five files, *filepath* , *filepath . 1* , *filepath . 2* , *filepath . 3* , and *filepath . 5* , then the first four files are matched and imported, but the file named *filepath . 5* is not.
- `dir` : Virtual directory on OSS.
  - The value of this parameter must end with a slash (/).
  - All files (excluding subfolders and files in subfolders) in the virtual directory indicated by this parameter are matched and imported to a database.
- `prefix` : Prefix of the path in the data file. Regular expressions are not supported. You can set only one of the these parameters: `prefix` , `filepath` , and `dir` .
- `format` : File format, which can only be CSV currently.
- `encoding` : File data encoding format. It supports common PostgreSQL encoding formats, such as UTF-8.
- `parse_errors` : Parsing in error tolerance mode. The errors that occur during the file parsing process are ignored by row.
- `delimiter` : Delimiter specified for columns.
- `quote` : Quote character for a specified file.
- `escape` : Escape character for a specified file.

- `null` : Used to nullify the column matching a specified string. For example, `null 'test'` is used to set the column whose value is `test` to null.
- `force_not_null` : Used to un-nullify the value of one or more columns. For example, `force_not_null 'id'` is used to set the values of the `id` column to empty strings.
- `compressiontype` : Used to set whether the file read or written on OSS is compressed and set the compression format. Values:
  - `none` : Uncompressed (default value)
  - `gzip` : compressed gzip file
- `compressionlevel` : Used to set the compression level of the compression format written to OSS. Value range: `1` to `9` . Default value: `6` .

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

Export mode parameters for CREATE FOREIGN TABLE

- `oss_flush_block_size` : Buffer size for the data written to OSS at a time. Its default value is 32 MB, and the value range is 1 MB to 128 MB.
- `oss_file_max_size` : Maximum file size for the data written to OSS (subsequent data is written in another file when the maximum file size is exceeded). Its default value is 1,024 MB, and the value range is 8 MB to 4,000 MB.
- `num_parallel_worker` : The number of parallel compression threads in the compression mode in which the OSS data is written, ranging from 1 to 8. Its default value is 3.

Auxiliary function

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

- Used to obtain the name and size of the OSS file that an external table matches.

- The unit of file size is byte.

```
select  *  from   oss_fdw_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 Endpoints.
- If the error "oss endpoint userendpoint not in aliyun white list" is triggered during reading of SQL statements for external tables, use these regions and endpoints. If the problem persists, submit a trouble ticket.

Error handling

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

- `code` : HTTP status code of the erroneous request.
- `error_code` : Error code returned by OSS.
- `error_msg` : Error message provided by OSS.
- `req_id` : UUID that identifies the request. If you cannot solve the problem, you can seek help from OSS development engineers by providing the req_id.

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 IDs and keys

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

Encrypted information:

```
 postgres =#  select  *  from   pg_foreign  _server  ;
   srvname    |  srvowner  |  srvfdw  |  srvtype  |  srvversion  |
 srvacl  |
                    srvoptions

-----------+----------+--------+---------+------------+--------
+-----------------------------------------------------------------------------
----------------------------------
  ossserver  |        10  |   16390  |          |            |
    | { host = oss - cn - hangzhou - zmf . aliyuncs . com ,  id =
 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.

8 Appendixes

8.1 Appendix: User and schema management

Premier accounts are not generally available during use of RDS, so we recommend that you create a user separately and manage the user's private space through schema when using the database.

Note:

In this example, myuser is the premier account created together with the instance, and newuser is the account to be created.

Solution 1

1. Create a user with the logon permission by using the premier account myuser.

```
CREATE   USER   newuser   LOGIN   PASSWORD ’ password ’;
```

   Parameter description:

   - `USER` : The username of the account to be created, for example, newuser.
   - `password` : The password of the account to be created, for example, password.

2. Create a schema for the new user.

```
CREATE   SCHEMA   newuser ;
GRANT   newuser   to   myuser ;
ALTER   SCHEMA   newuser   OWNER   TO   newuser ;
REVOKE   newuser   FROM   myuser ;
```

   Note:

   - If newuser is not added to the myuser role before execution of `ALTER SCHEMA newuser OWNER TO newuser`, the following permission problem occurs:

```
    ERROR :  must   be   member   of   role   " newuser "
```

   - In consideration of security, remove newuser from the myuser role after authorization of OWNER.

3. Use newuser to log on to the database.

```
psql - U newuser - h intranet4e xample . pg . rds . aliyuncs
. com - p 3433 pg001Passw ord for user newuser : psql .
bin ( 9 . 4 . 4 , server 9 . 4 . 1 ) Type “ help ” for help
.
```

Solution 2

1. Use the premier account myuser to create a user who has the logon permission.

```
CREATE USER newuser CREATEDB LOGIN PASSWORD ’ password ’;
```

Parameter description:

- `USER` : The username of the account to be created, for example, newusernewuser.
- `password` : The password of the account to be created, for example, password.
- `CREATEDB` : The permission for the user to create databases.

2. Use newuser to log on to the database.

```
psql - U < Database instancec name > - p 3433 - U newuser
```

```
< Database name >
```

```
CREATE DATABASE
```

3. Create a schema for the new user.

```
CREATE SCHEMA newuser ;
GRANT myuser to newuser ;
ALTER SCHEMA myuser OWNER TO newuser ;
REVOKE newuser FROM myuser ;
```

Note:

- If newuser is not added to the myuser role before execution of `ALTER SCHEMA newuser OWNER TO newuser`, the following permission problem occurs:

```
ERROR : must be member of role " newuser "
```

- In consideration of security, remove newuser from the myuser role after authorization of OWNER.

4. Use newuser to log on to the database.

```
psql - U newuser - h intranet4e xample . pg . rds . aliyuncs
. com - p 3433 pg001
Password for user newuser :
```

```
psql . bin  ( 9 . 4 . 4 ,  server   9 . 4 . 1 )
Type  " help "  for   help .
```

8.2 Release notes

This topic provides the release notes of RDS for PostgreSQL versions.

Release notes 2016-08-01

PostGIS is upgraded from 2.1.7 to 2.2.2. The default version of the new PostGIS plugin is 2.2.2.

The following command can be used to upgrade the existing PostGIS 2.1.7 plugin.

Note:

We recommend that you perform application testing before the upgrade to avoid incompatibility between the new PostGIS version and applications.

```
--  Upgrade   PostGIS  ( includes   raster )
 ALTER   EXTENSION   postgis   UPDATE   TO  " 2 . 2 . 2 ";
--  Upgrade   Topology
 ALTER   EXTENSION   postgis_to  pology   UPDATE   TO   " 2 . 2 . 2 ";
--  Upgrade   US   Tiger   Geocoder
 ALTER   EXTENSION   postgis_ti  ger_geocod  er   UPDATE   TO   " 2 . 2
 . 2 ";
```

Release notes 2016-07-01

Syntax

- set supports multiple variables, including set par1=val1 and par2=val2.
- The rds discard all syntax is supported (including the proxy transparent connection pool, clearing virtual pid and virtual cancel key).
- A new syntax is added for rds_superuser creation: CREATE ROLE | ALTER ROLE | CEATE GROUP xxx [WITH] RDS_SUPERUSER

High availability

- HA transparent switchover does not require reconnection.
- Proxy transparency.

Stream replication

- The WAL Sender rate limiting function is introduced to solve the competition problem of synchronizing the xlog data of multiple instances to network cards.

- Logical incremental replication is supported through alidecode, enabling incremental replication from RDS to other databases or full replication from MySQL to RDS PG.

Management

- The maximum length of a row in logger printing is limited to 2 KB to reduce the performance impact caused by frequent and long SQL statements.
- RDS SUPERUSER is allowed to run CREATE EXTENSION for plugin creation.
- The max_connect soft switch is introduced to dynamically adjust the number of connections without restarting the database cluster.
- The OOM signal is added to asynchronously monitor the memory usage of PG instances. The terminating effect is enhanced to reduce memory overheads.
- Users with the rds_superuser permission are allowed to run REASSIGN OWNED BY and other commands.
- No error is returned when users without the rds_superuser permission specify tablespace as pg_default during database creation.
- The OOM probability is reduced.
- The storage full issue caused by logs is avoided.

Security

- The hash index is automatically changed to the b-tree index and the unlogged table is changed to a common table in the kernel to prevent data loss after HA switchover caused by the PostgreSQL replication policy.
- Common users run CREATE EXTENSION or ALTER EXTENSION without the rds_superuser permission if a trigger, rule, or function is triggered.
- Security definer traps (triggers and rules) are fixed.
- The unencrypted password and pg_hba.conf password is disabled, and the password complexity requirements are increased.
- The pg_authid MD5 code security vulnerability is fixed.

Performance

- Database optimization and data file pre-distribution are supported. Inode write operations and the I/O hang probability are reduced.

- The checkpoint is optimized. The amount of updated dirty pages is reduced during fsync. The probability of I/O hang caused by dirty page update is reduced when metadata is written due to data=ordered.
- The clog is optimized. The clog buffer is increased. fsync is implemented at the checkpoint.

Plugin

The extension list is supported.

- Plugins of the community version

```
  plpgsql ,
  pg_stat_st  atements ,
  btree_gin ,
  btree_gist ,
  chkpass ,
  citext ,
  cube ,
  dblink ,
  dict_int ,
  earthdista  nce ,
  hstore , intagg ,
  intarray ,
  isn ,
  ltree ,
  pgcrypto ,
  pgrowlocks ,
  pg_prewarm ,
  pg_trgm ,
  postgres_f  dw ,
  sslinfo ,
  tablefunc ,
  tsearch2 ,
  unaccent ,
  pgstattupl  e ,
 " uuid - ossp "  NOTE :  uuid - ossp   must   be   enclosed   by
 the   double   quotation   marks  (" ").
```

- New plugins

```
 postgis ,
  postgis_to  pology ,
  fuzzystrma  tch ,
  postgis_ti  ger_geocod  er ,
  plperl ,
  pltcl ,
  plv8 ,
  plls ,
  plcoffee ,
  zhparser ,  which   supports   custom   word   segmentati  on
  pgrouting ,
  rdkit ,
  pg_hint_pl  an ,
  jsonbx ,
  www_fdw ,
  oss_fdw ,
pg_rewind
```

Access to other databases of a instance through dblink and postgres_fdw

Monitoring

- Error: Database error log
- Space: Available space, data directory space, and XLOG directory space (archived and unarchived)
- Junk data
  - Table expansion
  - Index expansion
  - Deadtuple
  - Unreferenced large object
- Running condition
  - Database age
  - Long transaction and 2PC
  - Sequence depletion
  - Unlogged table
  - Hash index
- Performance view
  - Slave database delay
  - Stream replication SLOT delay
  - Cache hit rate
  - Transaction rollback percentage
  - Lock wait
  - Slow SQL
  - TOP SQL
  - Connections
  - Instance memory usage
  - Instance CPU usage
  - Instance IOPS usage

- Configuration
  - Password expiration time
  - Configuration inconsistency between master and slave databases
  - Configuration file inconsistency between master and slave databases