Alibaba Cloud ApsaraDB for MySQL

Quick Start for PostgreSQL

Issue: 20180807

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.	 **Note:** 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]*
{} 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 by 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 API.
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 e purchasing an RDS instance to its usage. It also elaborates on how to create an ApsaraDB for RDS instance, perform basic settings, and connect to the instance database.

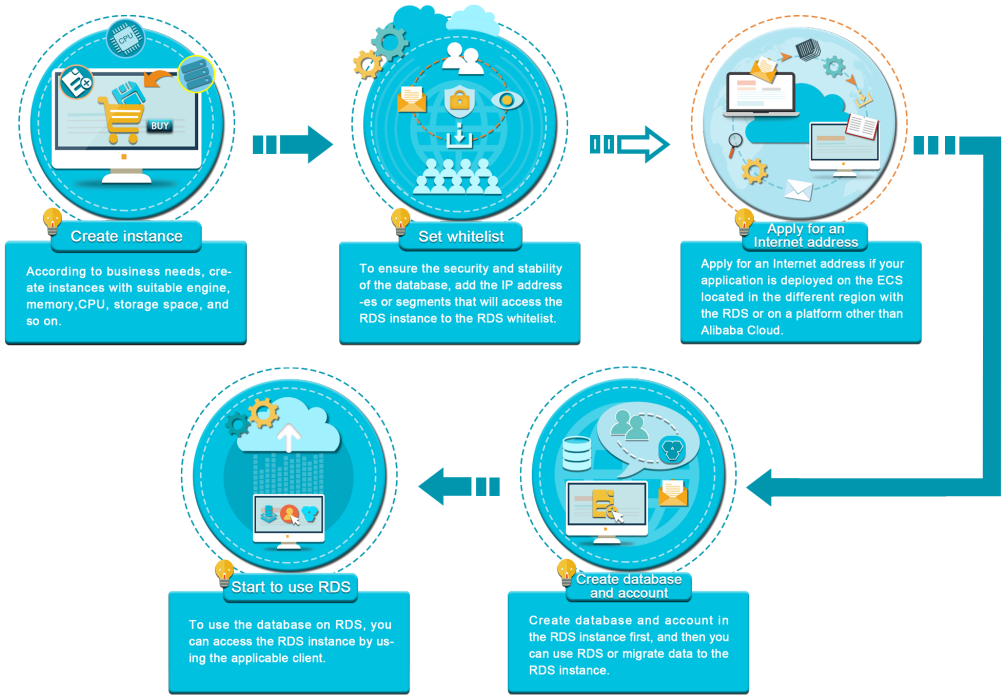
Target reader

- Users who buy an ApsaraDB for RDS instance for the first time.
- Users who need to perform basic settings for the instance they created.
- Users who want to know how to connect to an ApsaraDB for RDS instance.

Quick start flowchart

If you use Alibaba Cloud ApsaraDB for RDS for the first time, see *Limits* and *The instance management interface for PostgreSQL*.

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



3 Create an instance

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

Prerequisites

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

Procedure

1. Log on to the *RDS console*.
2. On the **Instances** page, click **Create Instance**.
3. Select **Subscription** or **Pay-As-You-Go**. For more information about the billing method, see *Billing items and billing methods*.
4. Select the instance configuration. The parameters are described as follows:
   - Basic configuration
     - Region and zone: Select the region and zone in which the instance is located. Some regions support a single zone or multi-zone, while some regions support only a single zone. For more information about regions and zones, see *Regions and zones*.

       Note:
       Products in different regions cannot intercommunicate through the intranet, and you cannot change the instance region after buying an instance. Therefore, be careful when selecting the region.
     - Database engine: RDS supports MySQL, SQL Server, PostgreSQL, and PPAS. Different database types are supported in different regions. Verify with the actual interface while using this document.
     - Version: The database version. Currently, RDS supports MySQL 5.5/5.6/5.7, SQL Server 2008 R2/2012, PostgreSQL 9.4, and PPAS 9.3. Different database versions are supported in different regions. Verify with the actual interface while using this document.

- Series: RDS instances support the Basic Edition, High-availability Edition, and Finance Edition. Different database versions support different series. Verify with the actual interface while using this document.

- Network type: RDS supports the classic network and virtual private cloud (VPC). You can change the network type after creating instances. For more information, see *Set network type*.
- Type: The CPU and memory occupied by the instance. The number of connections and maximum IOPS (measured respectively for read and write, up to double of the benchmark with mixed read/write) vary depending on different types. For more information, see *Instance type list*.
- Storage: The storage space contains space for data, system files, binlog files, and transaction files.
- Subscription time: Set the duration of the subscription instance.
- Quantity: The number of instances with the same configurations to be purchased.

5. Click **Buy Now** to enter the **Confirm Order** page.

> **Note:**
> To buy multiple instances of different configurations, you can click **Add To List** for each instance type and click **Batch Purchase**.

6. Select **Product Terms of Service and Service Level Notice and Terms of Use**, and then:

- Click **Pay**, if the billing method of the instance is subscription.
- Click **Activate**, if the billing method of the instance is Pay-As-You-Go.

4 Initial configuration

4.1 Set a whitelist

To ensure database security and stability, before you start using RDS instances, you must whitelist the IP addresses or IP address segments that need to access the database. We recommend that you periodically check and adjust your whitelists according to your requirements to maintain RDS security. This document provides the necessary information and procedure to set the whitelist.

Background information

You can access the RDS instances through the intranet, the Internet, or both of the intranet and Internet. For more information on the applicable scenarios of each connection type (intranet and Internet), see the **Background information** of *Set intranet and Internet addresses*.

- Access the RDS instances through the intranet.
- Access the RDS instances through the Internet.
- Access the RDS instances through both the intranet and Internet.

Before setting the connection type, you must add the IP addresses or IP segments of your application service or the ECS instance to the whitelist of RDS instance. When the whitelist is set, the system automatically generates the intranet address for the RDS instance. If you need an Internet address, see *Apply for an Internet address*.

Note:
If you cannot connect to the RDS instance after adding the application service IP address to the whitelist, you must obtain the actual IP address of the application service.

Attentions

- The system automatically creates a **default** whitelist group for each newly created RDS instance. This default whitelist group can only be modified or cleared, but cannot be deleted.
- For each newly created RDS instance, the local loopback IP address 127.0.0.1 is added to the **default** whitelist group by default. This means that all the IP addresses or IP segments are prohibited to access this RDS instance. Therefore, you must delete 127.0.0.1 from the default whitelist group first, before you add other IP addresses or IP segments to the RDS whitelist.
- % or 0.0.0.0/0 indicates any IP address is allowed to access the RDS instance. This configurat ion greatly reduces the security of the database and is not recommended.

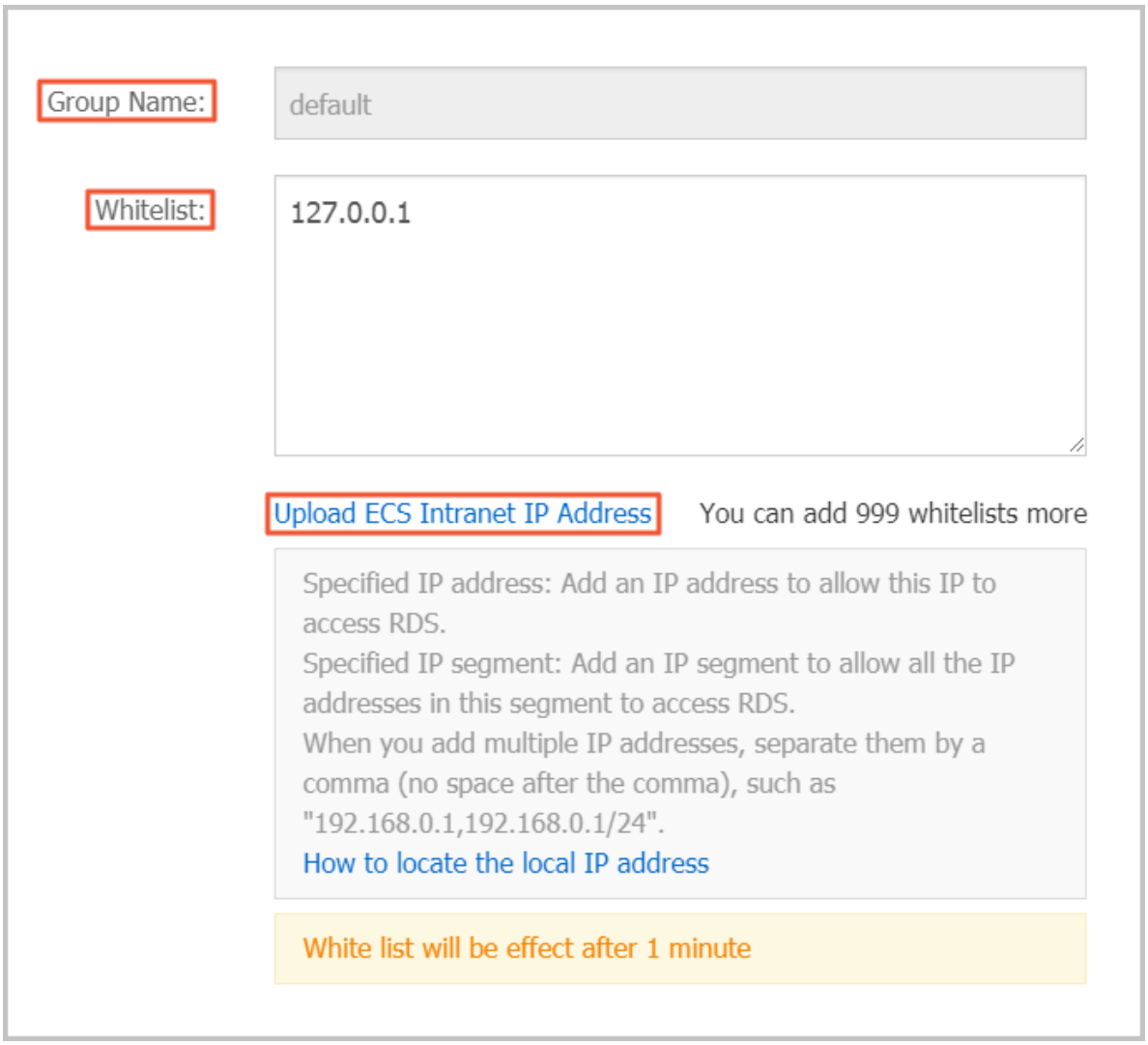
Procedure

1. Log on to the *RDS console*.
2. Select the region where the target instance is located.
3. Click the name of the target instance to go to the **Basic Information** page.
4. Select **Security Controls** in the left-side navigation pane to visit the **Security Controls** page.
5. On the **Whitelist Settings** tab page, click **Modify** of the **default** whitelist group, as shown in the following figure.

> **Note:**
> If you want to add a custom whitelist group to the RDS instance, you can click **Clear** of the **default** whitelist group to delete the IP address 127.0.0.1 first, and then click **Add a Whitelist Group**. The setting steps for a custom whitelist are similar to the following steps.

6. On the **Modify Group** page, add the IP addresses or IP segments to access the RDS instance to **Whitelist** field. If you want to add the ECS intranet IP addresses, click **Upload ECS Intranet IP Address** and select the IP addresses according to the prompt window, as shown in the following figure.

> **Note:**
> After you add a new IP address or IP address segment to the **default** group, the loopback address 127.0.0.1 is automatically deleted.



Parameters description:

- Group Name: it can contain 2 to 32 characters including lowercase letters, digits, or underscores (_). The group name must start with a lowercase letter and end with a letter or digit. This name cannot be modified once the whitelist group is successfully created.
- Whitelist: enter the custom IP addresses or IP segments that can access the RDS instance.
  - If you enter an IP segment, such as 10.10.10.0/24, it indicates that any IP address in the format of 10.10.10.X can access the RDS instance.
  - If you want to enter multiple IP addresses or IP segments, separate them by commas (,) (do not add blank spaces), such as 192.168.0.1,172.16.213.9.
  - For each whitelist group, up to 1,000 IP addresses or IP segments can be set for MySQL , PostgreSQL, and PPAS instances; and up to 800 can be set for SQL Server instances.

- Upload ECS intranet IP Address: by clicking this button, you can select the intranet IP addresses of the ECS instances under the same account with the RDS instance, which is a quick method to add ECS intranet IP addresses.

7. Click **OK**.

Modify or delete the whitelist group

You can modify or delete the whitelist group according your business requirements. The detailed procedure is as follows:

1. Log on to the *RDS console*.
2. Select the region where the target instance is located.
3. Click the name of the target instance to go to the **Basic Information** page.
4. Select **Security** in the left-side navigation pane.
5. On the **Whitelist Settings** tab page, click **Modify** or **Delete** button of the target whitelist group.
6. Click **OK** after you modify the IP addresses or IP segments. Or click **Confirm** if you are sure that it is the whitelist group to be deleted.

4.2 Apply for an Internet address

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

Note:

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

Background information

RDS supports connections through the intranet addresses and Internet addresses. The *access mode* and *instance type* have the following effects on the selection of the connection address.

Instance series	Instance version	Access mode	Connection address
Basic Edition	• MySQL 5.7 • SQL Server 2012	Standard mode	• Intranet address • Internet address

Instance series	Instance version	Access mode	Connection address
			• Intranet and Internet addresses
High-availability Edition	• MySQL 5.5/5.6 • SQL Server 2008 R2 • PostgreSQL 9.4 • PPAS 9.3	Standard mode	• Intranet address • Internet address
		Safe connection mode	• Intranet address • Internet address • Intranet and Internet addresses
Finance Edition	MySQL 5.6	Standard mode	• Intranet address • Internet address
		Safe connection mode	• Intranet address • Internet address • Intranet and Internet addresses

The applicable scenarios of the connection addresses are as follows:

- Use the intranet address only:
  - The system provides an intranet address by default and you can directly modify the connection address.
  - This scenario is applicable when your application is deployed on the ECS instance that is located in the same region and has the same *network type* as your RDS instance.
- Use the Internet address only:
  - This scenario is applicable when your application is deployed on the ECS instance that is located in the different region with that of your RDS instance.
  - This scenario is applicable when your application is deployed on the platform other than Alibaba Cloud.
- Use both of the intranet and Internet addresses:
  - This scenario is applicable when your application is deployed on the ECS instance that is located in the same region and has the same *network type* as your RDS instance, and on the ECS instances of different regions at the same time.

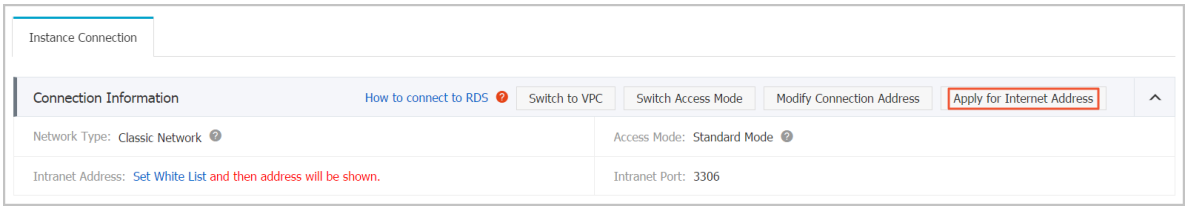
— This scenario is applicable when your application is deployed on the ECS instance that is located in the same region and has the same *network type* as your RDS instance, and on the platform other than Alibaba Cloud at the same time.

Attention

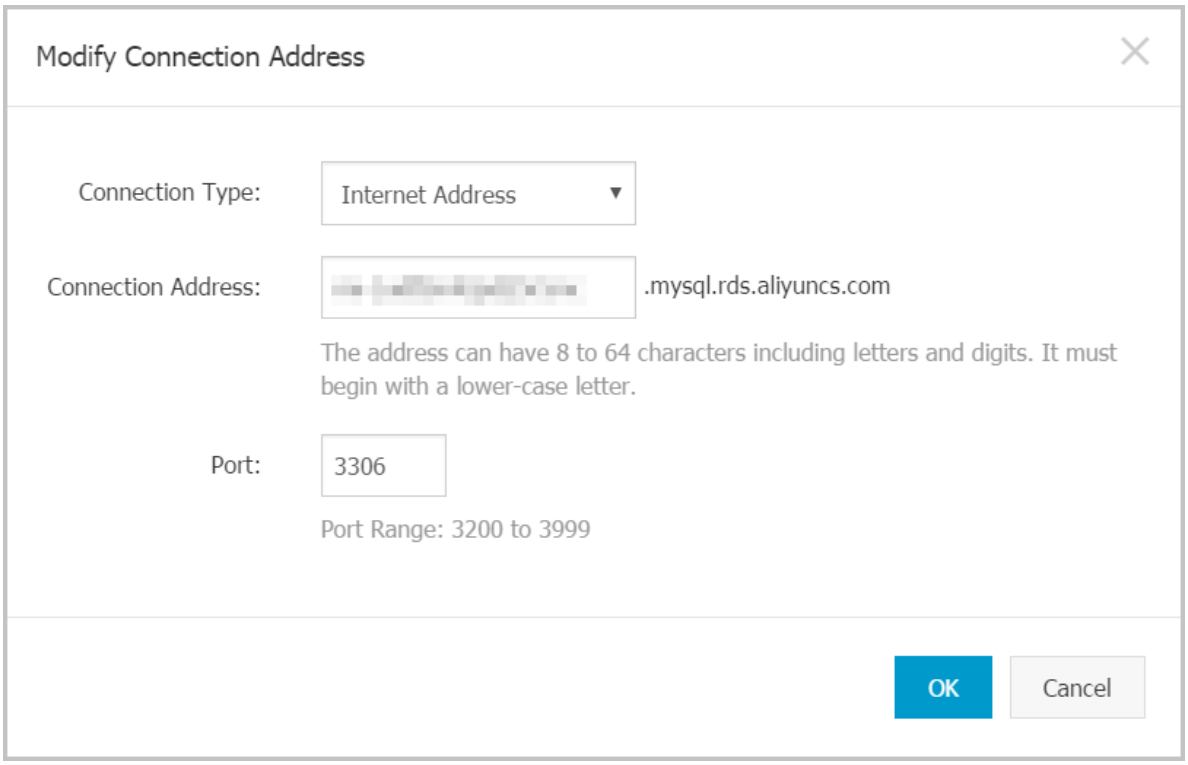
- Before accessing the database, you must add the IP addresses or IP segments used to access the database to a whitelist. For more information, see *Set whitelist*.
- A traffic fee is charged for connections using an Internet address. For more information about pricing and fees charges, see *RDS Pricing*.
- Connecting the RDS instance with an Internet address may reduce the instance security . Proceed with caution. To get a higher transmission rate and a higher security level, we recommend that you migrate your applications to the ECS instances in the same region with that of your RDS.

Procedure

1. Log on to the *RDS console*.
2. Select the region where the target instance is located.
3. Click the ID of the target instance to visit to the **Basic Information** page.
4. Select **Database Connection** in the left-side navigation pane to visit the **Database Connection** page.
5. Click **Apply for Internet Address**, as shown in the following picture.



6. On the displayed confirmation window, click **OK** to generate an Internet address.
7. Click **Modify Connection Address** and modify the connection address and port of the Internet or intranet, as shown in the following picture.



Parameter description:

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

8. Click **OK**.

4.3 Create database and account

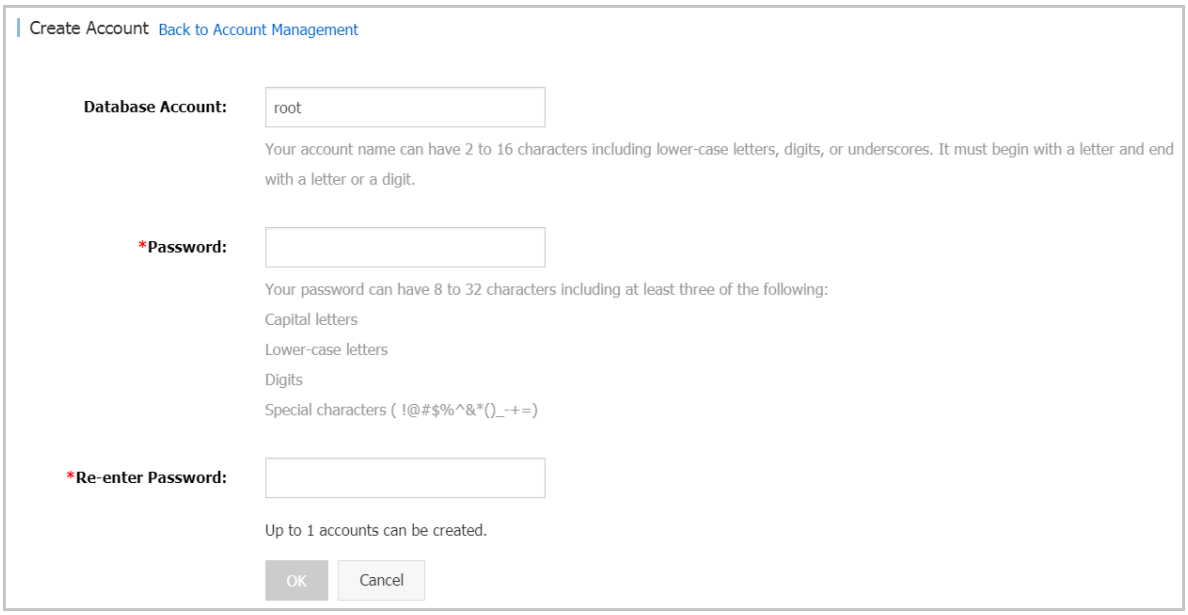
Before RDS can be used, a database and an account must be created for the RDS instance. For PostgreSQL instance, you must create an initial account on the RDS console. And then you can create and manage the databases through a client. This document takes the client pgAdmin 4 as an example to introduce how to create databases and accounts for PostgreSQL instance.

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 the local database to RDS, you must create the same database and account in RDS instance as those of the local database.
- When assigning account permissions for each database, follow the minimum permission principle and service roles to create accounts and 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 Read-only permission.
- 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, enter the relevant details in the required fields.

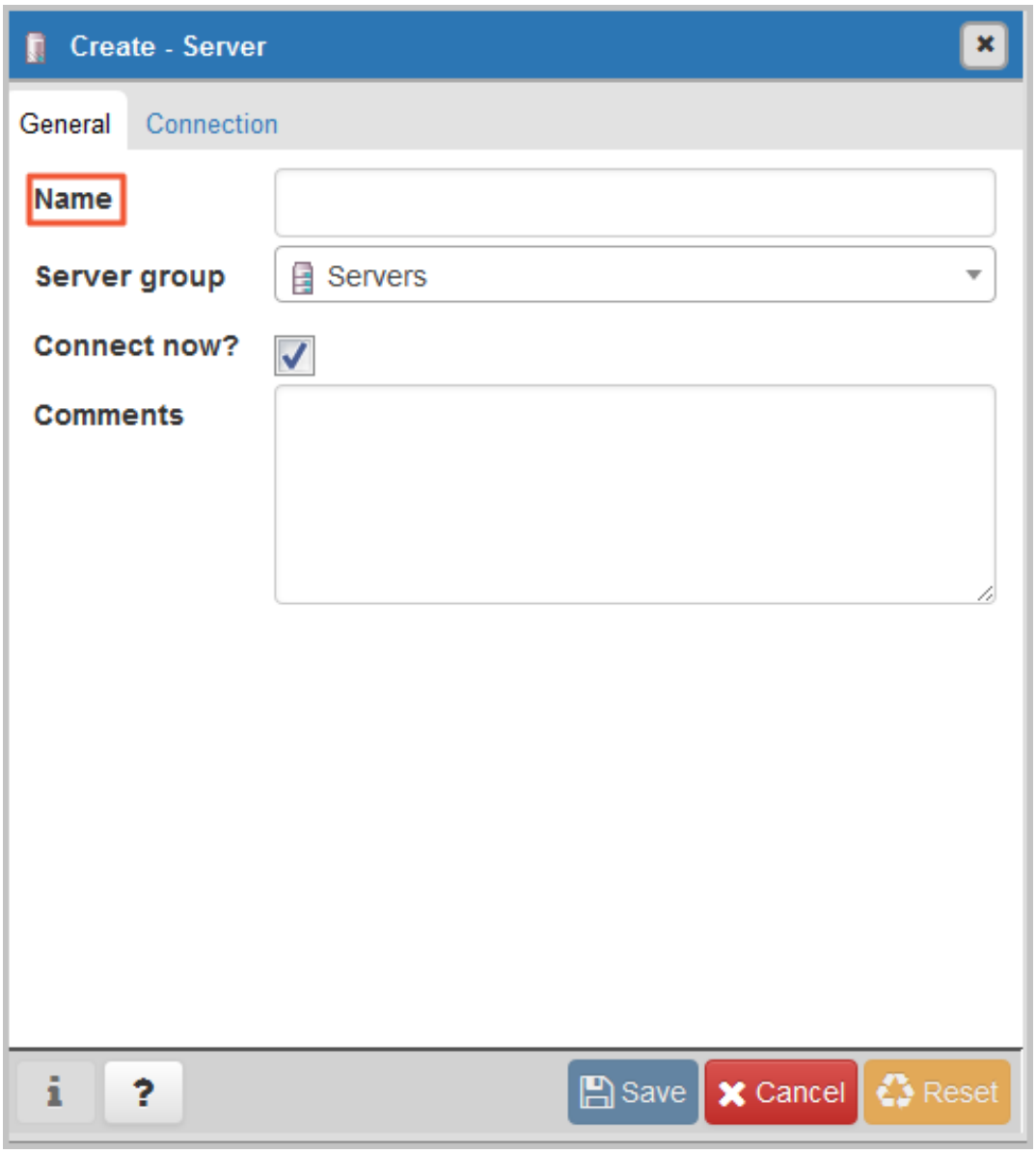


Parameters description:

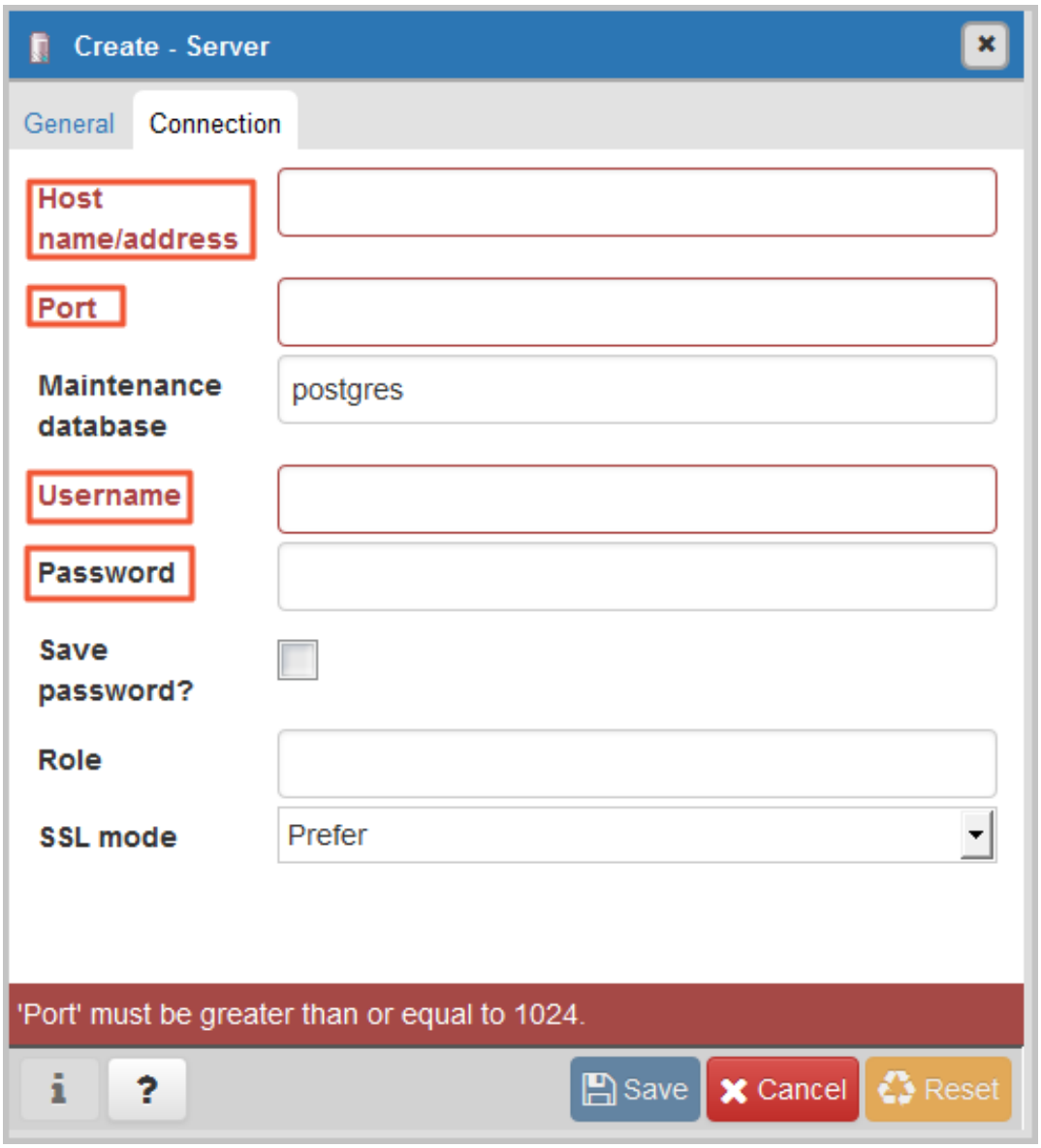
- Database Account: refers to the name of the initial account. It can have 2 to 16 characters including the lower-case letters, digits, or underscores (_). It must begin with a letter and end with a letter or digit.
- Password: refers to the password corresponding to the initial account. It can have 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 accessing the RDS instance to RDS whitelist. For more information on how to set whitelist, see *Set whitelist*.
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. Select 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 by using the intranet, enter the intranet address of the RDS instance. If your application accesses the RDS instance by using the Internet, enter the Internet address of the RDS instance. You can view the connection address and port number as follows:

  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. View the intranet and Internet IP addresses and ports in the **Basic Information** area.

- Port: refers to the port number of the RDS instance. If your application accesses the RDS instance by using the intranet, enter the intranet port number of the RDS instance. If your application accesses the RDS instance by using 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 corresponding to the initial account of the RDS instance.

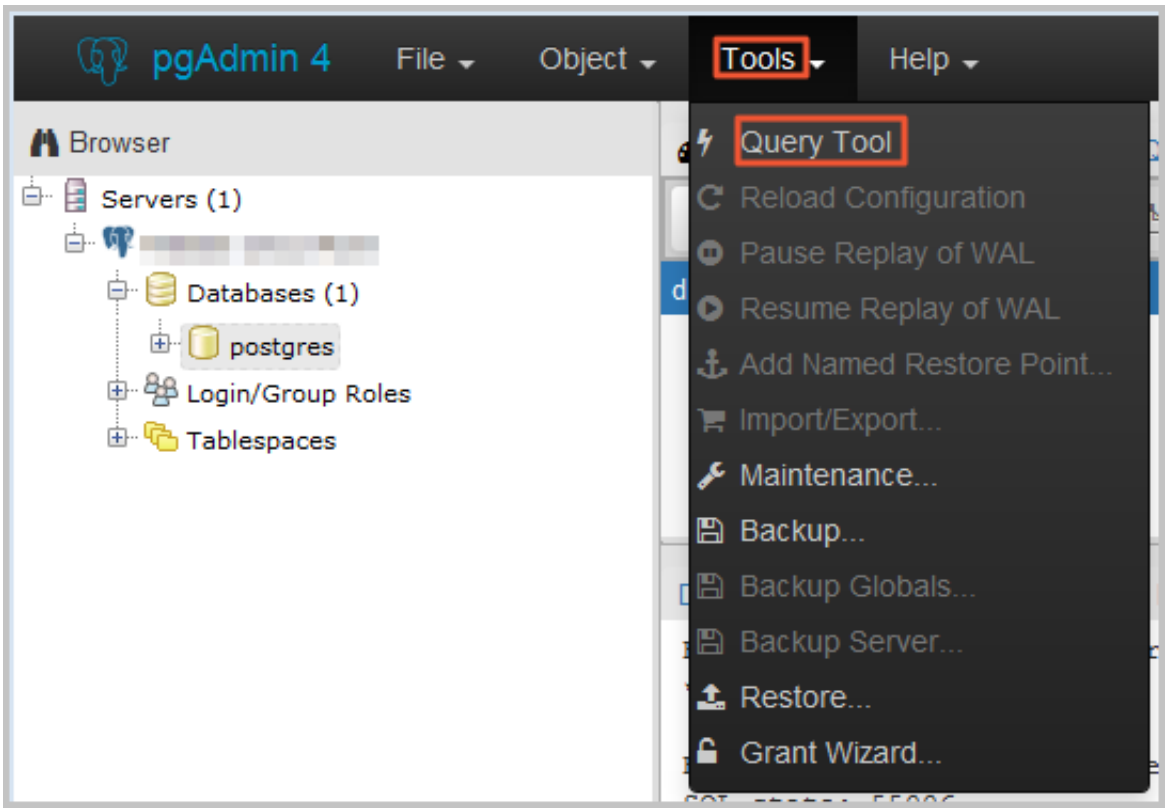
13. Click **Save**.

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

Note:

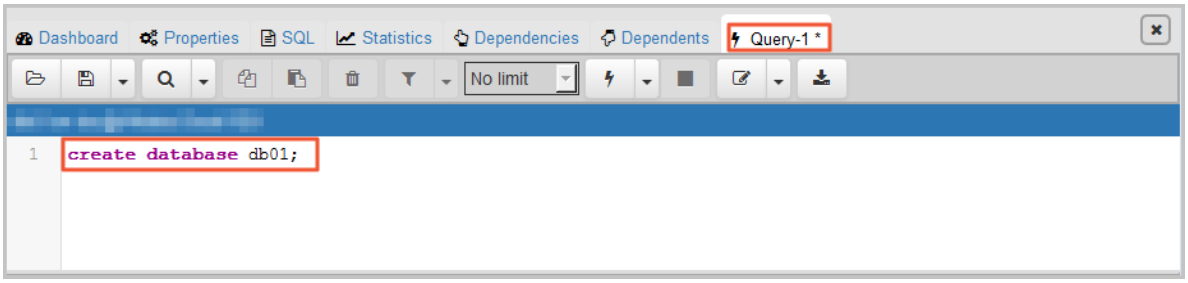
postgres is the defaul system database of the RDS instance. Do not do any operation in this database.

15. Select postgres, and then select **Tools** > **> Query Tool**, as shown in the following picture.

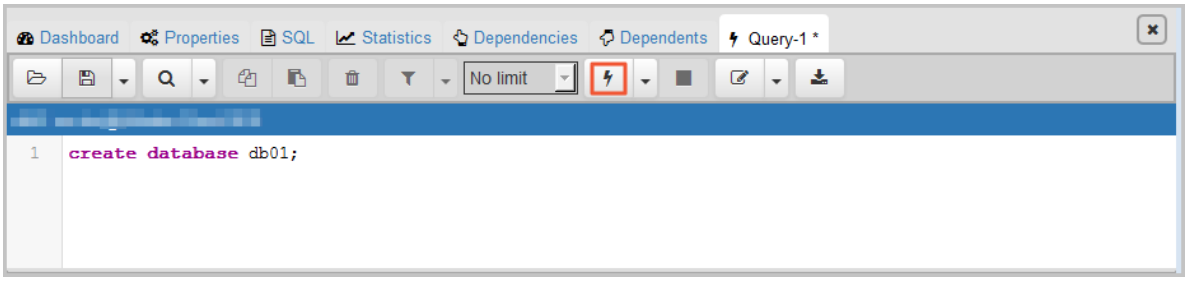


16. Enter the following command on the **Query-1** tab page to create a database, as shown in the following figure.

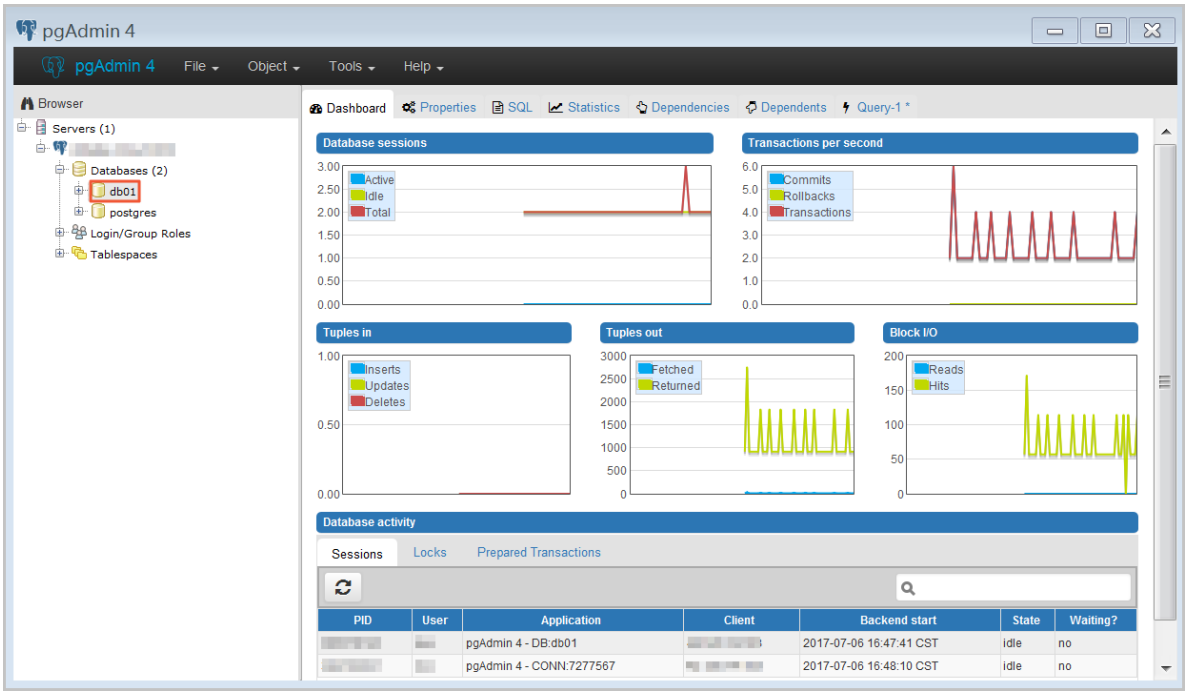
```
create database <database name>;
```



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

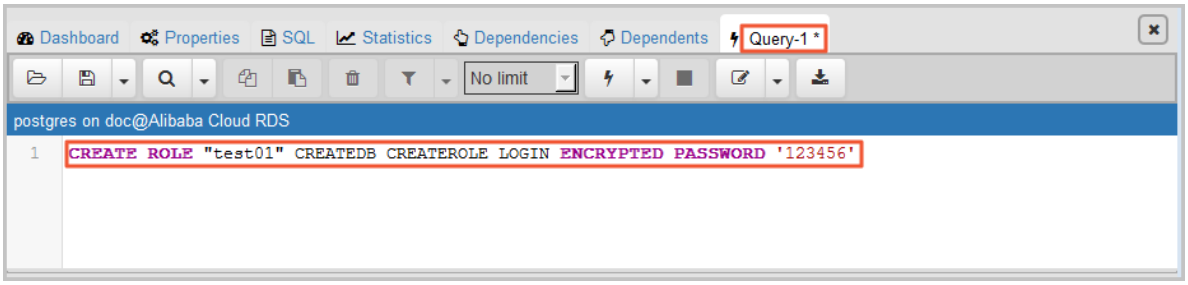


18. If the execution is successful, it indicates that the new database is created successfully. Right click **Databases** and click **Refresh**, and then you can find the newly created database, as shown in the following figure.

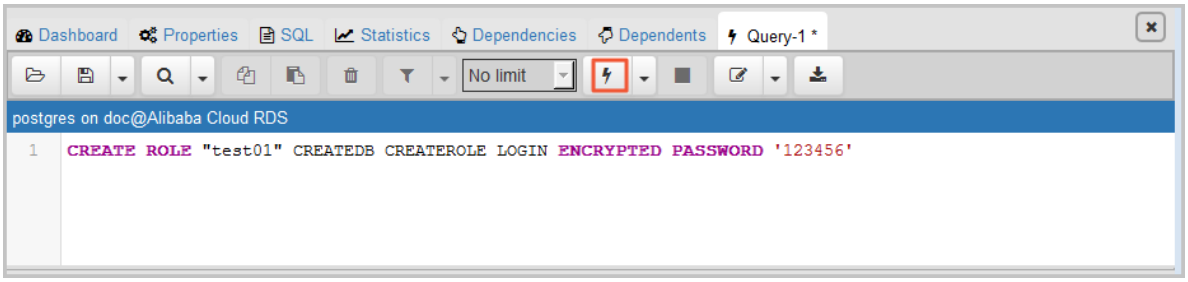


19. Enter the following command on the **Query-1** tab page to create account, as shown in the following figure.

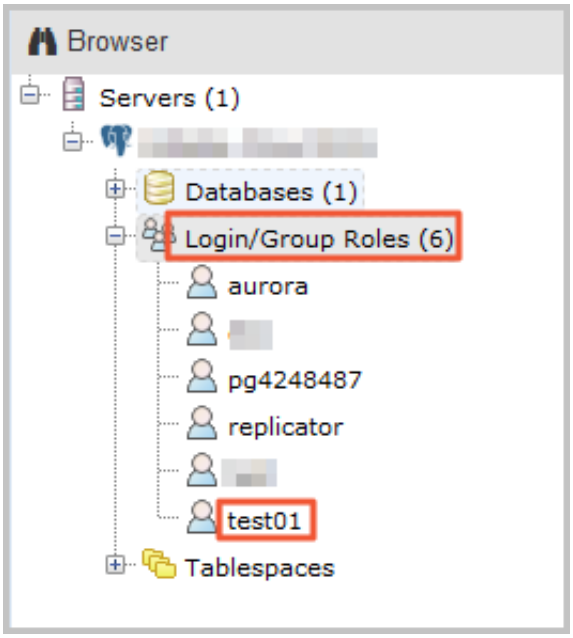
```
CREATE ROLE "username" CREATEDB CREATEROLE LOGIN ENCRYPTED PASSWORD
 'password';
```



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



21. If the execution is successful, it indicates that the new account is created successfully. 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

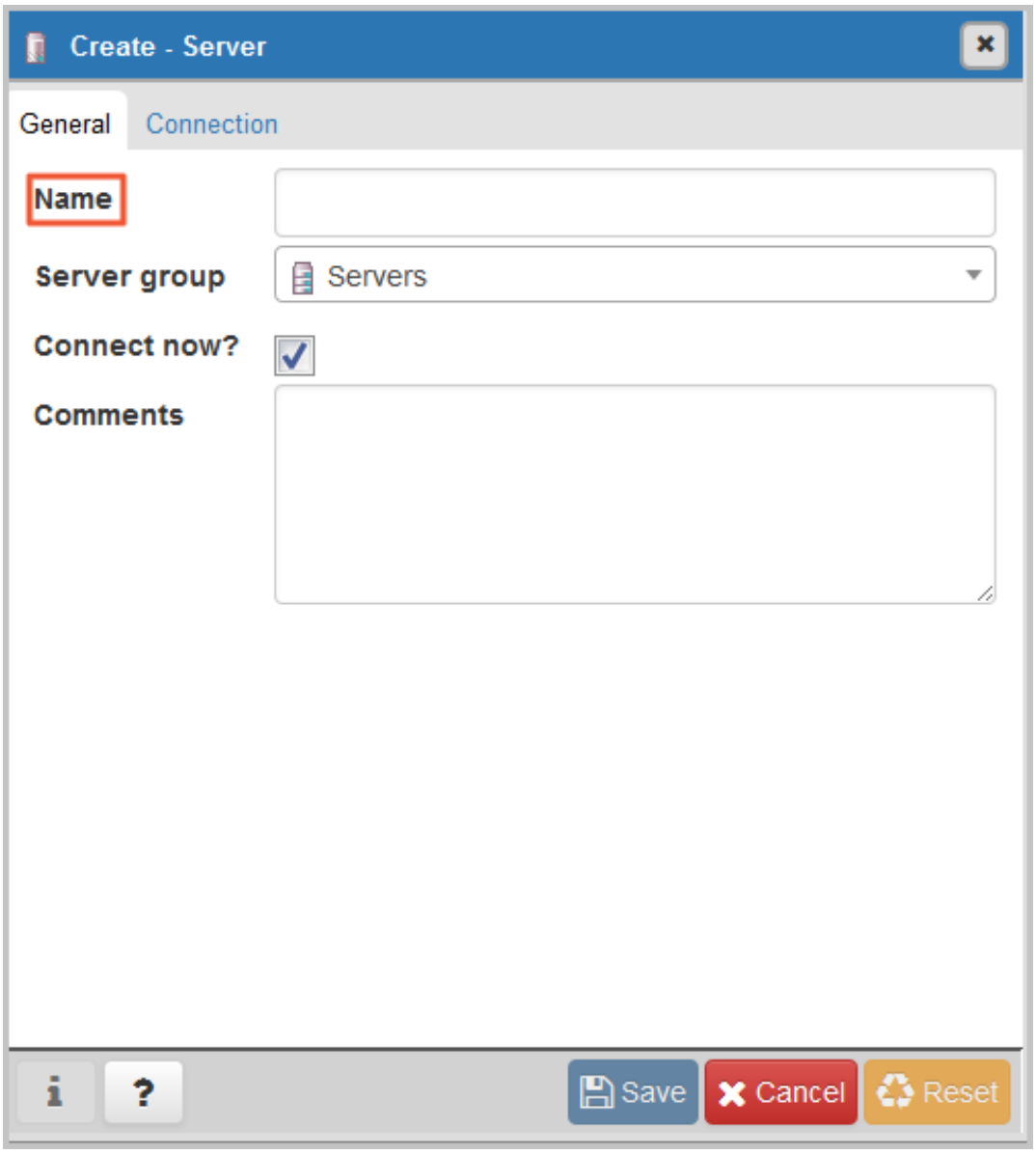
Because RDS for PostgreSQL is fully compatible with PostgreSQL, the same method can be used to connect to the database. This document takes the pgAdmin 4 client as an example to connect to an RDS instance. You can see this method when using other clients. When you connect to an RDS instance through a client, choose to use an *intranet or Internet address* as follows:

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

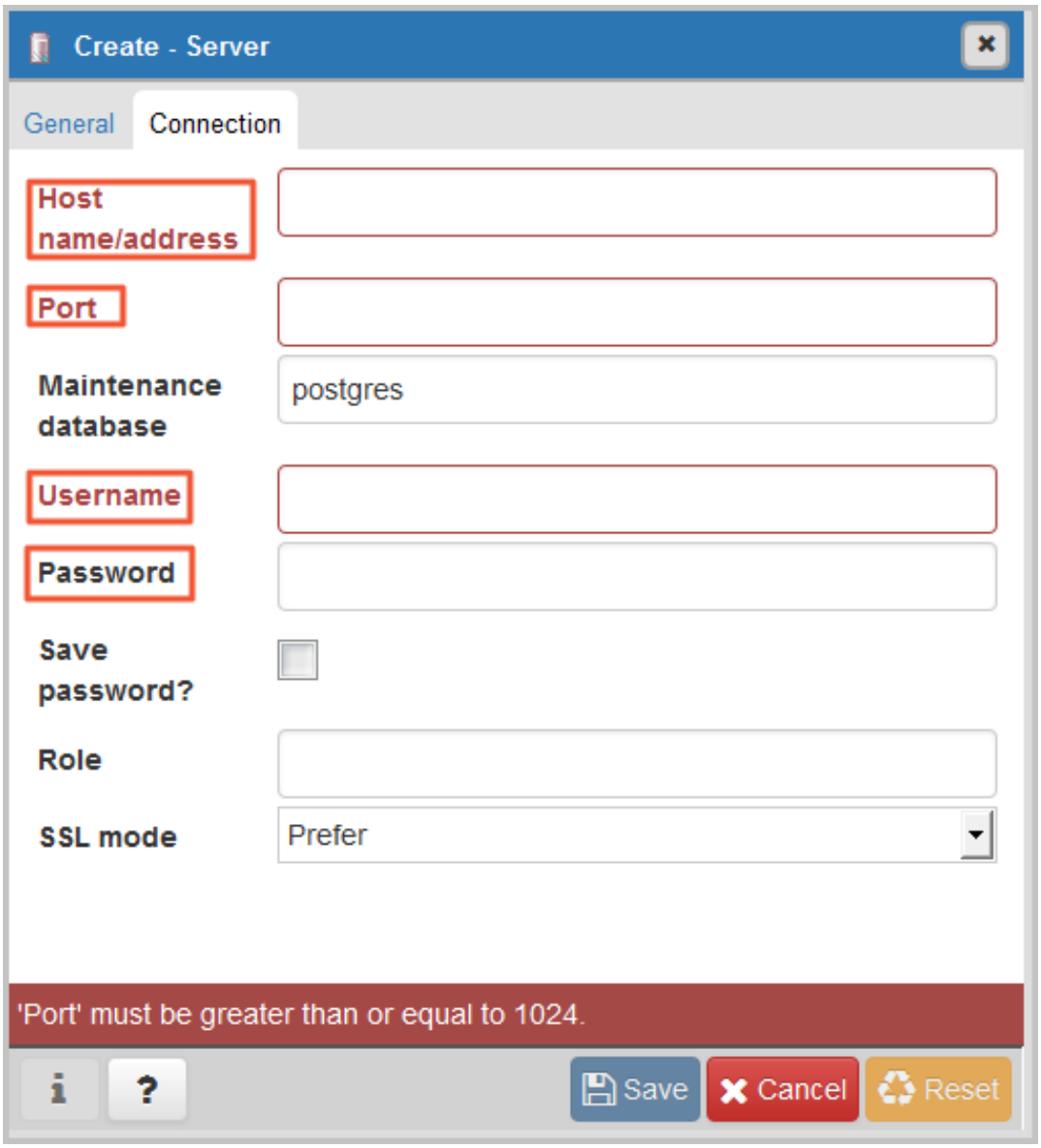
Log on via client

1. Add the IP address accessing the RDS instance to RDS whitelist. For more information, see *Set whitelist*.
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. Select 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 applicatio n accesses the RDS instance by using the intranet, enter the intranet address of the RDS instance. If your application accesses the RDS instance by using the Internet, enter the Internet address of the RDS instance. Do the following steps to find the connection address and port number of the RDS instance.

  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 **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 by using the intranet, enter the intranet port number of the RDS instance. If your application accesses the RDS instance by using 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 corresponding to 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 appears, 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 the external data files using oss_fdw

In Alibaba Cloud, you can use the 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 source), allowing you to read files on OSS, like reading data from a table. oss_fdw provides unique parameters used to connect to and parse 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 does not 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 bad, you can adjust these parameters to make the import and export successful.

- oss_connect_timeout: Connection timeout time, measured in seconds. Default value: 10s.
- oss_dns_cache_timeout: DNS timeout time, measured in seconds. Default value: 60s.
- oss_speed_limit: Minimum tolerable rate. Default value: 1,024 Bytes/s (1 Kbps).
- oss_speed_time: Maximum tolerable time. Default value: 15s.

If the default parameter values are used, a timeout error occurs when the transmission rate is smaller than 1 Kbps for 15 consecutive seconds.

CREATE FOREIGN TABLE parameters

- filepath: File name indicating 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 instance, 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 of 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. Support the 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: The delimiter specified for columns.
- quote: The 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 the 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, not filepath.

Export mode parameters for CREATE FOREIGN TABLE

oss_flush_block_size and oss_file_max_size are added to export mode.

- oss_flush_block_size: Buffer size for the data written to OSS at a time; default value: 32 MB; value range: 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); default value: 1,024 MB; value range: 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. Default value: 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 get the name and size of the OSS file that an external table matches.
- The unit of file size is byte.

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

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

Auxiliary feature

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

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

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

  oss_test/test.gz. 2 | 739413041
```

```
(1 rows)
```

oss_fdw example

```
# Create the plugin
create extension oss_fdw;
# Create a server instance
CREATE SERVER ossserver FOREIGN DATA WRAPPER oss_fdw OPTIONS
     (host 'oss-cn-hangzhou.aliyuncs.com' , id 'xxx', key 'xxx',
bucket 'mybucket');
# Create an OSS external table
CREATE FOREIGN TABLE ossexample
    (date text, time text, open float,
     high float, low float, volume int)
     SERVER ossserver
     OPTIONS ( filepath 'osstest/example.csv', delimiter ',' ,
         format 'csv', encoding 'utf8', PARSE_ERRORS '100');
# Create a table, to which data is loaded
create table example
        (date text, time text, open float,
         high float, low float, volume int);
# Load data from ossexample to example.
insert into example select * from ossexample;
# As you can see
# oss_fdw estimates the file size on OSS and formulates a query plan
correctly.
explain insert into example select * from ossexample;
                             QUERY PLAN

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

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

oss_fdw usage tips

- oss_fdw is an external table plugin developed based on the PostgreSQL FOREIGN TABLE framework.
- The data import performance is related to the PostgreSQL cluster resources (CPU I/O MEM MET) and OSS.
- For expected data import performance, ossendpoint in ossprotocol must match the region where PostgreSQL is located in Alibaba Cloud. For more information, see the reference links at the end of this article.

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

Encrypted information:

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

  srvoptions

-----------+----------+--------+---------+------------+--------
+-------------------------------------------------------------------------------
--------------------------------
```

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

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

7 Appendix

7.1 Appendix: User and schema management

Superuser is not generally available during use of the 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 management account created together with the instance, and newuser is the account to be created now.

Solution 1

1. Create a user with the logon permission.

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

Parameters are described as follows:

- USER: The user name to be created, for example, **newuser**
- password: The password corresponding to the user name, 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 `ALTER SCHEMA newuser OWNER TO newuser`, the following permission problem occurs:
>
> ```
> ERROR: must be member of role "newuser"
> ```
>
> - In consideration of security, please remove newuser from the myuser role to improve security after the authorization of OWNER is handled.

3. Use newuser to log on to the database.

```
psql -U newuser -h intranet4example.pg.rds.aliyuncs.com -p 3433
pg001Password for user newuser:psql.bin (9.4.4, server 9.4.1)Type “
help” for help.
```

Solution 2

1. Use the initial account myuser to create a user that has the logon permission.

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

Parameters are described as follows:

- USER: The user name to be created, for example, **newuser**
- password: The password corresponding to the user name, for example, **password**
- CREATEDB: The permission for the user to create databases.

2. Use newuser to log on to the database.

```
psql -U <数据实例域名> -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 `ALTER SCHEMA newuser OWNER TO newuser`, the following permission problem occurs:

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

- In consideration of security, please remove newuser from the myuser role to improve security after the authorization of OWNER is handled.

4. Use newuser to log on to the database.

```
psql -U newuser -h intranet4example.pg.rds.aliyuncs.com -p 3433
pg001
Password for user newuser:
psql.bin (9.4.4, server 9.4.1)
```

```
Type "help" for help.
```

7.2 Release notes

Release notes 20160801

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 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_topology UPDATE TO "2.2.2";
-- Upgrade US Tiger Geocoder
ALTER EXTENSION postgis_tiger_geocoder UPDATE TO "2.2.2";
```

Release notes 20160701

Syntax

- set supports multiple variables, including set par1=val1 and par2=val2.
- The rds discard all syntax is supported (support of the proxy transparent connection pool, and clearance of virtual pid and virtual cancel key).
- New syntax is added for rds_superuser creation.

  CREATE ROLE | ALTER ROLE | CEATE GROUP xxx [WITH] RDS_SUPERUSER

High availability

- HA transparent switch. No reconnection is required.
- 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 plug-in 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 overhead.
- 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 switch 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 use of 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 writes and I/O hang times 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 updating 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_statements,
 btree_gin,
 btree_gist,
 chkpass,
 citext,
 cube,
 dblink,
 dict_int,
 earthdistance,
 hstore,intagg,
 intarray,
 isn,
 ltree,
 pgcrypto,
 pgrowlocks,
 pg_prewarm,
 pg_trgm,
 postgres_fdw,
 sslinfo,
 tablefunc,
 tsearch2,
 unaccent,
 pgstattuple,
 "uuid-ossp" NOTE: uuid-ossp must be enclosed by the double
quotation marks (" ").
```

- **New plugins**

```
postgis,
 postgis_topology,
 fuzzystrmatch,
 postgis_tiger_geocoder,
 plperl,
 pltcl,
 plv8,
 plls,
 plcoffee,
 zhparser, which supports custom word segmentation
 pgrouting,
 rdkit,
 pg_hint_plan,
 jsonbx,
 www_fdw,
 oss_fdw,
 pg_rewind
```

Access to other databases of this 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
  - Standby 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
  - Master configuration and backup configuration inconsistent
  - Master configuration file and backup configuration file inconsistent