Alibaba Cloud ApsaraDB for MySQL

FAQs

Issue: 20190830

Legal disclaimer

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

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

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

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

Generic conventions

Table -1: Style conventions

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

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

Contents

1 How to connect/cannot connect

1.1 What do I do if I cannot connect an ECS instance to an ApsaraDB for RDS instance?

This topic describes what you can do if you cannot connect an ECS instance to an RDS instance in various situations.

If you fail to connect ECS to RDS, one common reason is that the network type of the ECS instance differs from that of the RDS instance. Another common reason is that the IP address whitelist for the RDS instance does not contain the required IP addresses. The most common reasons and corresponding solutions are as follows:

ECS and RDS belong to different network types

The ECS instance runs in a VPC while the RDS instance runs in a classic network.

- Solution 1 (recommended): Switch the RDS instance from its classic network to the VPC where the ECS instance resides. For detailed steps, see #unique_5.

  Note:
  The RDS instance must run in the same VPC as the ECS instance after the switching so that they can communicate with each other through the intranet.
- Solution 2: Purchase another ECS instance that runs in the classic network because ECS instances cannot be switched from a VPC to the classic network. A VPC is safer than the classic network. Therefore, we recommend that you use a VPC.
- Solution 3: Connect the ECS instance to the RDS instance through the Internet by using the public address of the RDS instance. This solution is inferior to solutions 1 and 2 in terms of performance, security, and stability.

The ECS instance runs in the classic network while the RDS instance runs in a VPC.

- Solution 1 (recommended): Switch the ECS instance from the classic network to the VPC where the RDS instance resides.

  Note:
  The ECS instance must run in the same VPC as the RDS instance after the switching so that they can communicate with each other through the intranet.

- Solution 2: Switch the RDS instance from its VPC to the classic network. However, a VPC is safer than the classic network. Therefore, we recommend that you use a VPC.
- Solution 3: Use the ClassicLink function. This function allows the ECS instances in the classic network to communicate with the resources in a VPC through the intranet.
- Solution 4: Connect the ECS instance to the RDS instance through the Internet by using the public address of the RDS instance. This solution is inferior to solutions 1 , 2, and 3 in terms of performance, security, and stability.

ECS and RDS are in different VPCs

Each VPC is a logically isolated network on Alibaba Cloud. If the ECS instance and RDS instance both run in VPCs, they must be in the same VPC so that they can communicate with each other through the intranet.

- Solution 1 (recommended): Switch the RDS instance to the VPC where the ECS instance is located.

  Specifically, switch the RDS instance from its VPC to the classic network and then switch from the classic network to the VPC where the ECS instance resides. For detailed steps, see #unique_5.
- Solution 2: Establish an Express Connect channel between the two VPCs. For detailed steps, see Interconnect two VPCs under the same account.
- Solution 3: Connect the ECS instance to the RDS instance through the Internet. This solution is inferior to solutions 1 and 2 in terms of performance, security, and stability.

ECS and RDS are in different regions

If the ECS instance is located in a region different from the RDS instance, they cannot communicate with each other through the intranet.

- Solution 1: Release the ECS or RDS instance and purchase instances again.
- Solution 2: Set the network types of the ECS instance and RDS instance to VPCs, and establish an Express Connect channel between the two VPCs. For detailed steps, see #unique_5 and #unique_6.
- Solution 3: Connect the ECS instance to the RDS instance through the Internet. This solution is inferior to solutions 1 and 2 in terms of performance, security, and stability.

Incorrect IP address whitelist settings

- The whitelist contains only the default IP address 127.0.0.1, which indicates that no devices are allowed to access the RDS instance. You need to add the IP address of the ECS instance to the whitelist. For detailed steps, see #unique_7.
- The IP address in the whitelist is 0.0.0.0. However, the correct format is 0.0.0.0/0.

  > Note:
  > 0.0.0.0/0 indicates that all devices are allowed to access the RDS instance. Please use it with caution.

- The whitelist is set to the enhanced security mode. In this case, you need to check the following:
  - If you want the ECS instance to connect to the RDS instance through the VPC address, ensure that the private IP address of the ECS instance is added to the VPC whitelist of the RDS instance.
  - If you want the ECS instance to connect to the RDS instance through the classic network address, ensure that the private IP address of the ECS instance is added to the classic network whitelist of the RDS instance.
  - If you want the ECS instance to connect to the RDS instance through the Internet address, ensure that the public IP address of the ECS instance is added to the classic network whitelist of the RDS instance. The VPC whitelist does not restrict access from the Internet.
- The public IP address that you add to the whitelist is not the real outbound IP address of the ECS instance. Possible reasons are as follows:
  - The public IP address is not fixed and may change.
  - The IP address query tool or website may provide inaccurate IP addresses.

  To find out the real IP address, see Locate the real IP address.

Domain name resolution failures

If your Domain Name Server (DNS) fails or its network interface card (NIC) configuration is changed, domain name resolution may fail. You can run the `ping` and `telnet` commands to check whether you can properly connect to the RDS instance.

```
ping  < domain   name >
```

```
telnet < domain name >< port number >
```

Example:

If the communication is abnormal, you can modify the NIC configuration file of your DNS to resolve the problem by completing the following steps:

1. Modify the NIC configuration file.

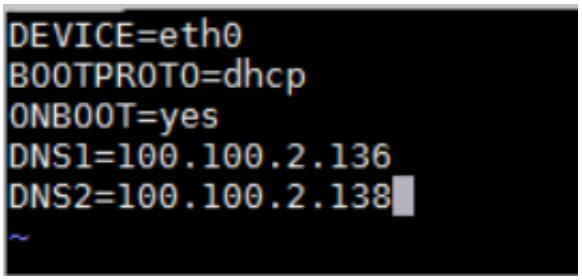
```
vi / etc / sysconfig / network - scripts /< name of the NIC
  configurat ion file >
```

> Note:
> Fill the name of the NIC used by the ECS server in the <name of the NIC configuration file> field. You can run the `ifconfig` command to check the suffix. The default suffix is ifcfg-eth0.

2. Add the following information to the end of the NIC configuration file:

```
DNS1 = 100 . 100 . 2 . 136
DNS2 = 100 . 100 . 2 . 138
```

> Note:
> If the `DNS1` and `DNS2` parameters are set, you need to change their settings to the IP addresses shown above.



3. Run the following command to restart your network service:

```
systemctl restart network
```

4. Run the following command to check whether the modification is successful:

```
cat / etc / resolv . conf
```

Common connection failures and solutions

Database type	Error message	Cause	Solution
MySQL or MariaDB TX	· ERROR 2003 (HY000): Can’t connect to MySQL server on ‘XXX’ (10038, 10060, or 110) · Cannot connect to the database: XXX	The network connection is abnormal.	Click here.
	· ERROR 1045 (HY000): #28000ip not in whitelist · ERROR 2801 (HY000): #RDS00ip not in whitelist, client ip is XXX	The IP address whitelist is set improperly.	Click here.
	· ERROR 1045 (28000): Access denied for user ‘XXX’@’XXX’ (using password: YES or NO)	The user name or password is incorrect.	Click here.
	· ERROR 2005 (HY000): Unknown MySQL server host ‘xxxxxxx’ (110 or 11004) · SQLSTATE[HY000] [2002] php_network_getaddresses: getaddrinfo failed: Name or service not known · Name or service not known	The DNS cannot parse IP addresses properly.	Click here.
SQL Server	Cannot connect to XXX. A network-related or instance-specific error occurs when a connection is being established with SQL Server. The server cannot be found or accessed. Check whether the instance name is correct. Also check whether the SQL Server is configured and allows remote access. (provider: TCP Provider, error: 0 - The receiver fails to respond correctly within the specified period or the host to be connected does not respond.) (Microsoft SQL Server, error: 10060 or 258)	The network connection is abnormal.	Click here.

Database type	Error message	Cause	Solution
	Cannot connect to XXX. A connection is established with the server, but an error occurs during the login. provider: TCP Provider, error: 0 - The specified network name is no longer available.)(Microsoft SQL Server, error: 64)	The IP address whitelist is set improperly.	Click here.
PostgreSQL /PPAS	Unable to connect to server: could not connect to server: Connection timed out (0x0000274C/10060)Is the server running on host “XXX.rds.aliyuncs.com” and acceptingTCP/IP connections on port XXX?	The network connection is abnormal.	Click here.
	· server closed the connection unexpectedly This probably means the server terminated abnormally before or while processing the request. · Error connecting to the server: FATAL: no pg_hba.conf entry	The IP address whitelist is set improperly.	Click here.

1.2 How do I locate the public IP address of my computer that needs to connect to RDS for MySQL or MariaDB TX?

Problem

- You have added the public IP address of your computer to the IP address whitelist of the RDS instance. However, your computer cannot access the instance while other devices can.
- You have added the public IP address of your computer to the IP address whitelist of the RDS instance, but your computer cannot access the instance unless you set the IP address whitelist to 0.0.0.0/0 or your company's address range.

If either of the preceding problems occurs, the public IP address you add to the whitelist of the RDS instance may be incorrect. You need to find the real public IP address of your computer.

> **Note:**
> This topic applies only when you access the RDS instance from a device other than an ECS instance. If you access the RDS instance from an ECS instance, you can find the public and private IP addresses of the ECS instance on the ECS console.

Precautions

If the public IP address of your computer is not fixed and your RDS instance is used in a production environment, we recommend that you use a private connection instead or configure an appropriate IP address range in the whitelist. This is to ensure that the connection remains available even if the public IP address of your computer changes.

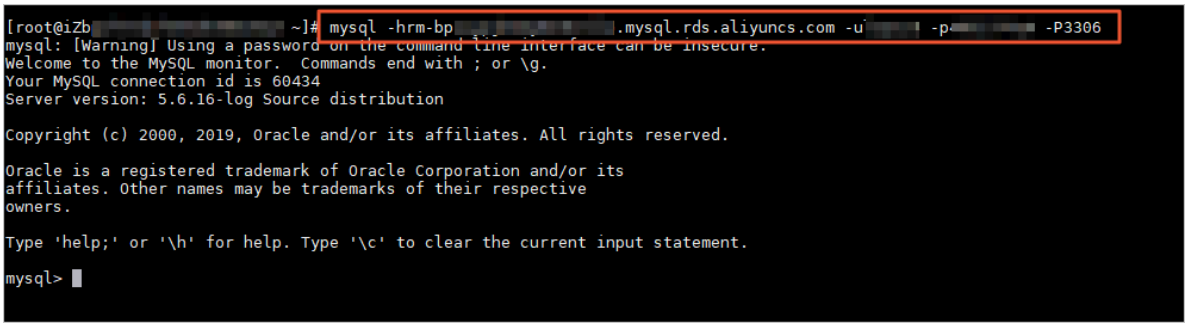
Procedure

1. Add your company's public IP address range or 0.0.0.0/0 to the IP address whitelist of the RDS instance. For more information, see #unique_10.

   > **Note:**
   > 0.0.0.0/0 indicates that all devices are allowed to access the RDS instance. Use the address with caution. If you add 0.0.0.0/0 to the whitelist, we recommend that you remote it from the whitelist immediately once you no longer need it.

2. Connect your computer to the RDS instance by using a client or the command line interface (CLI).

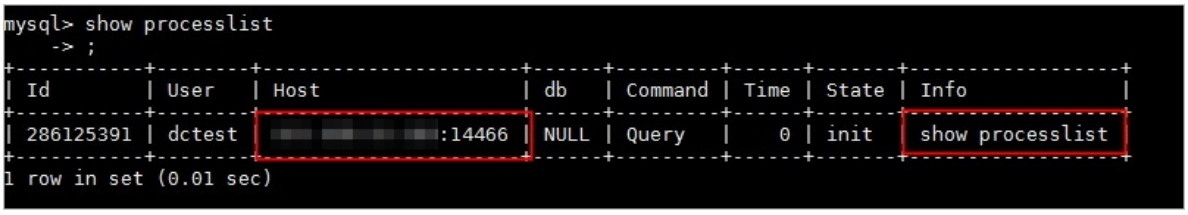
   ```
   mysql -h< RDS Connection address > -u< Username > -p< Password >
    -P3306
   ```



3. Check the process information.

```
show   processlis  t
```

As shown in the following figure, the value of Host for the show processlist record is the real public IP address of your computer.



4. Remove 0.0.0.0/0 from the whitelist and add the real public IP address of your computer to the whitelist.

1.3 How do I locate the IP address connected to an RDS for SQL Server instance?

Obtain the IP address of your computer connected to an RDS instance

Problem description

The public IP address of your computer dynamically changes, therefore the IP address you obtain by using a local IP address query tool may be incorrect. As a result , RDS reports connection errors even after you add the obtained public IP address to the IP address whitelist of the RDS instance. You can access the RDS instance only after you obtain the correct IP address of your computer.

Precautions

If the public IP address of your computer changes and the established connection to the RDS instance is used in a production environment, we recommend that you use a private network connection instead or add an appropriate CIDR block to the IP address whitelist of the RDS instance. This helps to guarantee a stable connection despite changes to the public IP address of your computer.

Procedure

1. Add the IP address `0 . 0 . 0 . 0 / 0` to the IP address whitelist of the RDS instance. For more information, see #unique_12.

Note:

> The IP address `0.0.0.0/0` indicates that all IP addresses are allowed to access the RDS instance.

2. Use a client to connect your computer to the RDS instance. For more information, see #unique_13.
3. Run the following commands to query the IP address of your computer:

```
SELECT    CONNECTION  PROPERTY (' PROTOCOL_T  YPE ')  AS
PROTOCOL_T  YPE ,
        CONNECTION  PROPERTY (' CLIENT_NET  _ADDRESS ')  AS
CLIENT_NET  _ADDRESS
```

4. Delete the IP address `0.0.0.0/0` that you added to the IP address whitelist in Step 1, and add the real outbound IP address of your computer to the IP address whitelist.

Obtain all IP addresses connected to an RDS instance

Problem description

You want to obtain all IP addresses that are connected to the RDS instance, or you want to locate security issues such as link leakage.

Procedure

1. Add the IP address `0.0.0.0/0` to the IP address whitelist of the RDS instance. For more information, see#unique_12.
2. Use a client to connect your computer to the RDS instance.
3. Run the following commands to query all IP addresses that are connected to the RDS instance.

```
SELECT
SP . SPID ,
SP . LOGINAME ,
SP . LOGIN_TIME ,
SP . HOSTNAME ,
SP . PROGRAM_NA  ME ,
DC . CLIENT_TCP  _PORT ,
DC . CLIENT_NET  _ADDRESS
FROM   SYS . SYSPROCESS  ES   AS   SP
INNER   JOIN   SYS . DM_EXEC_CO  NNECTIONS   AS   DC
ON   SP . SPID  =  DC . SESSION_ID
WHERE   SP . SPID  >  50
AND   DC . AUTH_SCHEM  E =' SQL '
```

4. Delete the IP address `0.0.0.0/0` or the CIDR block containing your company's IP address segment that you added to the IP address whitelist in Step 1.

View the parameter settings of a connection

After you obtain all IP addresses that are connected to the RDS instance, you can run the following command to view the parameter settings of a specific connection:

```
SELECT * FROM SYS . DM_EXEC_SE SSIONS WHERE SESSION_ID =<
The obtained SPID >
```

1.4 How do I locate the IP address connected to an RDS for PostgreSQL or RDS for PPAS instance?

Problem description

- You have added the public IP address of your computer to the IP address whitelist of the RDS instance. However, your computer cannot access the instance while the other devices can.
- You have added the public IP address of your computer to the IP address whitelist of the RDS instance, but your computer cannot access the instance. However, after you set the IP address whitelist to your company's CIDR block or 0.0.0.0/0, your computer can access the instance.

If either of the preceding problems occurs, the public IP address you add for your computer to the IP address whitelist of the RDS instance may be incorrect. In such case, you must find the real outbound IP address of your computer.

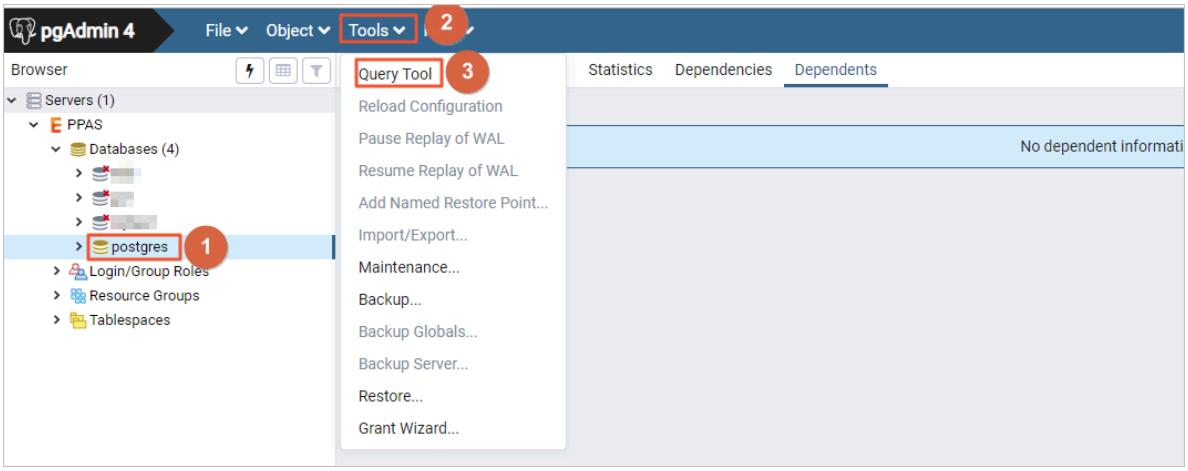
 Note:
This topic applies only when you access the RDS instance from a device other than ECS. If you access the RDS instance from an ECS instance, you can find the public and private IP addresses of the ECS instance in the ECS console.

Precautions

If the public IP address of your computer dynamically changes and the establishe d connection is used in a production environment, we recommend that you use a private connection instead or add an appropriate CIDR block to the IP address whitelist of the RDS instance. This helps to guarantee a stable connection despite changes to the public IP address of your computer.

Procedure

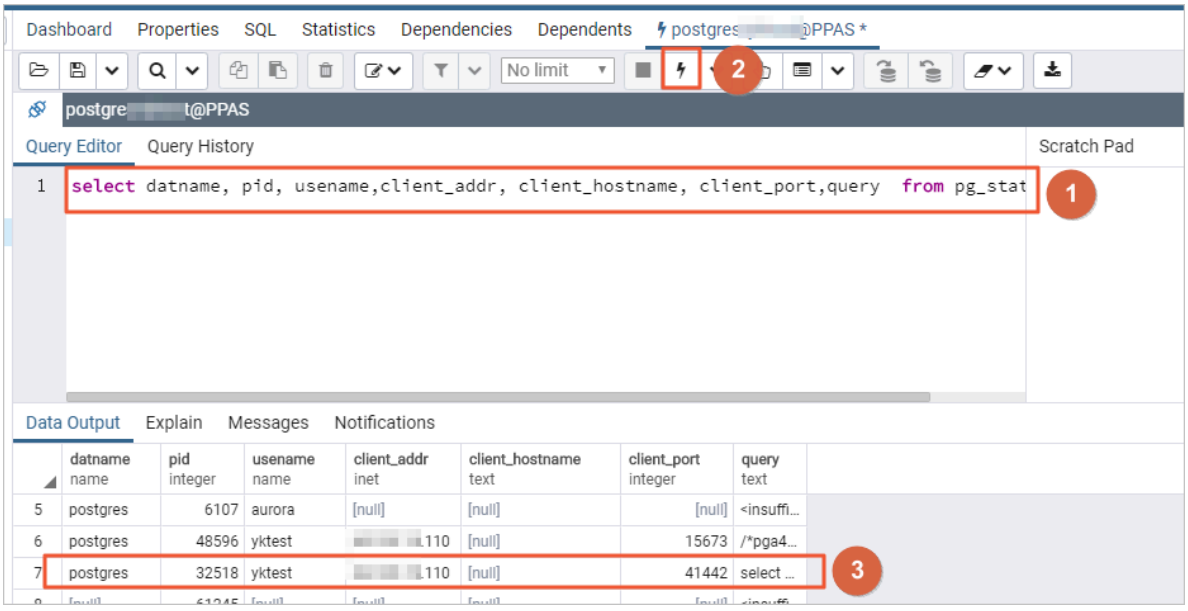
1. Add the IP address 0.0.0.0/0 to the IP address whitelist of the RDS for PostgreSQL or RDS for PPAS instance. For more information, see #unique_17.
2. Use a pgAdmind 4 client to connect your computer to the RDS instance.
3. In the left-side navigation pane, chooseDatabases > postgres. Then in the main menu choose Tools > Query Tool.



4. Run the following command:

```
select   datname ,  pid ,  usename , client_add  r ,  client_hos
tname ,  client_por  t , query    from   pg_stat_ac  tivity ;
```

5. On the Data Output tab in the lower area, find the record whose query value is SELECT. The value in the client_addr column for this record is the real outbound IP address of your computer.



6. **Delete the IP address 0.0.0.0/0 you added to the IP address whitelist in Step 1, and add the obtained real outbound IP address to the IP address whitelist.**

2 Data backup/recovery

2.1 Restore data from physical backup files of ApsaraDB for MySQL to an on-premises user-created database

The open source software Percona XtraBackup can be used to back up and restore databases. This topic describes how to use this software to restore data from physical backup files of ApsaraDB for MySQL to a user-created database.

> Note:
>
> - For more information about how to back up ApsaraDB for MySQL data, see #unique_20.
> - Percona XtraBackup does not support Windows. For more information about how to back up and restore data in Windows, see #unique_21.

Precautions

This topic describes how to restore data from physical backup files of MySQL 5.7 in Linux 7.

- Make sure that Percona XtraBackup has been installed. You can download from the Percona XtraBackup official website.

  To restore data of MySQL 5.6 and earlier versions, you must install Percona XtraBackup 2.3. For more information, see Installing Percona XtraBackup 2.3.

  To restore data of MySQL 5.7, you must install Percona XtraBackup 2.4. For more information, see Installing Percona XtraBackup 2.4.
- If your ApsaraDB for MySQL instances use the database engine MySQL 5.6 and are created after February 20, 2019, the backup files of such instances are in xbstream format with the suffix of _qp.xb.
- The on-premises MySQL database is installed in a 64-bit Linux system. The version of the database is the same as that of ApsaraDB for MySQL.

  > Note:
  > You can only restore data from backup files of ApsaraDB for MySQL to an on-premises MySQL database in Linux.

Prerequisites

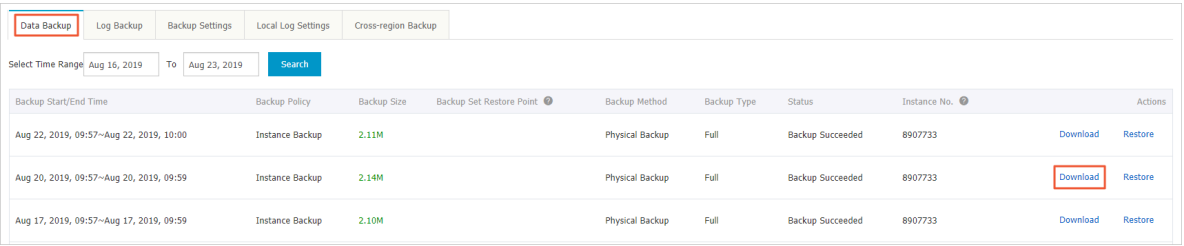
The database engine of the ApsaraDB for MySQL instance must be in one of the following editions:

- MySQL 5.7 High-availability Edition (with local SSDs)
- MySQL 5.6
- MySQL 5.5

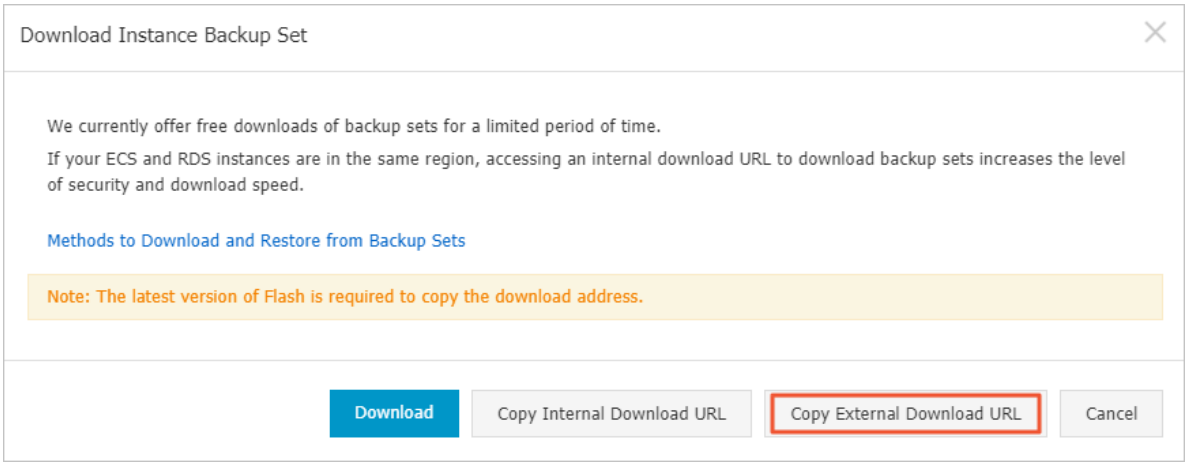
Procedure

1. Log on to the ApsaraDB for RDS console.
2. In the upper-left corner of the page, select the region where the instance is located.
3. Find the instance and click the instance ID.
4. In the left-side navigation pane, click Backup and Restoration.
5. Click the Data Backup tab.
6. Select a time range that you need to query, then click Search.
7. In the backup list, find the backup file and click Download.

> **Note:**
> If Download does not appear, make sure that the version of your instance supports downloading physical backup files.



8. In the Download Instance Backup Set dialog box that appears, click Copy External Download URL.



9. Log on to the ECS instance.
10. Run the following command to download the backup file:

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

Note:

- `-c`: specifies to resume from the breakpoint.
- `-O`: specifies a name for the download file (use the file name suffix .tar.gz, .xb.gz or _qp.xb as contained in the URL).

11. Run the following command to decompress the downloaded backup file:

Note:
This topic uses the custom path */home/mysql/data* as an example. You can replace it with the path of your backup file.

There are three formats for physical backup files:

- tar compressed package (.tar.gz)
- xbstream compressed package (.xb.gz)
- xbstream file package (_qp.xb)

Note:

If your ApsaraDB for MySQL instances use the database engine MySQL 5.6 and are created after February 20, 2019, the backup files of such instances are in xbstream format with the suffix of _qp.xb.

For tar compressed packages (.tar.gz), run the following command:

```
tar -izxvf <backup file name>.tar.gz -C /home/mysql/data
```

For xbstream compressed packages (.xb.gz), run the following command:

```
gzip -d -c <backup file name>.xb.gz | xbstream -x -v -C /home/mysql/data
```

For xbstream file packages (_qp.xb), run the following command:

```
## Unpack
cat <backup file name> _qp.xb | xbstream -x -v -C /home/mysql/data
## Decompress
innobackup ex --decompress --remove-original /home/mysql/data
```

Note:

`-C` specifies the directory to decompress the file to. Optional. If you do not specify this parameter, the file is decompressed to the current directory.

12. Run the following command to query the information of the files after decompression:

```
ls -l /home/mysql/data
```

After the command is executed, the following result is displayed. The information in blue indicates the databases contained in the RDS instance when the backup file was generated.

```
[root@testcentos ~]# ls -l /home/mysql/data
total 204844
-rw-r--r-- 1 root root       297 Apr 28 21:13 backup-my.cnf
-rw-rw---- 1 root root 209715200 Apr 28 21:04 ibdata1
drwxr-xr-x 2 root root      4096 Apr 28 22:01 mysql
drwxr-xr-x 2 root root      4096 Apr 28 22:01 performance_schema
drwxr-xr-x 2 root root      4096 Apr 28 22:01 test
drwxr-xr-x 2 root root      4096 Apr 28 22:01 xiangluo
```

13. Run the following command to restore the backup file to the on-premises database:

```
innobackup  ex  -- defaults - file =/ home / mysql / data / backup
- my . cnf  -- apply - log  / home / mysql / data
```

If the following result is displayed, the backup file is restored to the on-premises database.

```
InnoDB: Shutdown completed; log sequence number 1635350
150428 22:08:40  innobackupex: completed OK!
[root@testcentos ~]#
```

Note:
Make sure that you have installed the proper version of Percona XtraBackup. Install Percona XtraBackup 2.3 for MySQL 5.6 and earlier versions, Percona XtraBackup 2.4 for MySQL 5.7, and Percona XtraBackup 8.0 for MySQL 8.0.

14. To avoid compatibility problems, follow these steps to reconfigure the `backup - my . cnf` parameter:

a. Run the following command to edit the *backup - my . cnf* file in text:

```
vi  / home / mysql / data / backup - my . cnf
```

b. Comment out the following parameters that are not supported in user-created databases:

```
# innodb_log  _checksum_  algorithm
# innodb_fas  t_checksum
# innodb_log  _block_siz  e
# innodb_dou  blewrite_f  ile
# rds_encryp  t_data
# innodb_enc  rypt_algor  ithm
# redo_log_v  ersion
# master_key  _id
```

Note:

- If your on-premises database uses the MyISAM engine, which is incompatible with the InnoDB engine in ApsaraDB for RDS, you must comment out the following parameters and add the skip-grant-tables parameter:

```
# innodb_log  _checksum_  algorithm = strict_crc  32
# redo_log_v  ersion = 1
```

```
skip - grant - tables
```

- If your on-premises database uses the MyISAM engine, and error messages related to the storage engine are displayed when you manage system tables, run the following command to switch the storage engine:

```
alter  engine  < table  name >  engine = myisam ;
```

c. Press the EscEsc key, enter `: wq` , and press the Enter key to save.

15. Run the following command to change the owner of the file to the on-premises MySQL user:

```
chown  - R  mysql : mysql  / home / mysql / data
```

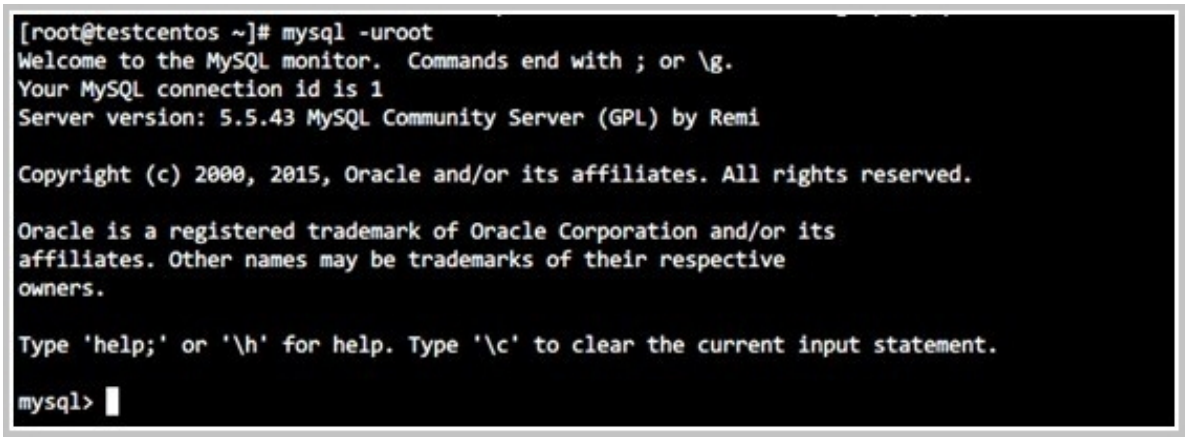
16. Run the following command to start the on-premises MySQL process:

```
mysqld_saf  e  -- defaults - file =/ home / mysql / data / backup -
my . cnf  -- user = mysql  -- datadir =/ home / mysql / data  &
```

17. Run the following command to log on to the on-premises MySQL database to verify that the process has been started:

```
mysql  - uroot  - p < database  password >
```

If the following result is displayed, the parameters are commented out and the owner of the file is changed.



2.2 FAQ on binlogs

1. Q: Two binlog files have a similar start time and end time. Why has this occurred? Is the start time of one file consecutive with that of another?

   A: The two files contain binlogs that were generated during the backup of the primary and secondary nodes. As a result, the two files have a similar start time and end time. The start time of each file is not the same.

2. Q: Are binlog files compressed?

   A: Binlog files are not compressed.

3. Q: How are the generation, upload, and clearing of binlogs triggered?

   A: When more than 500 MB of log data is written to a binlog file, a new binlog file is generated. Backup logs are uploaded to OSS based on local backup settings, and then local logs are cleared.

2.3 How do I use the mysqlbinlog command to view the binary logs of an RDS for MySQL instance?

You can run the mysqlbinlog command to view specific SQL statements in the binary logs of an RDS for MySQL instance.

Prerequisites

MySQL has been installed on your Linux-based on-premises host that runs a Linux operating system.

Procedure

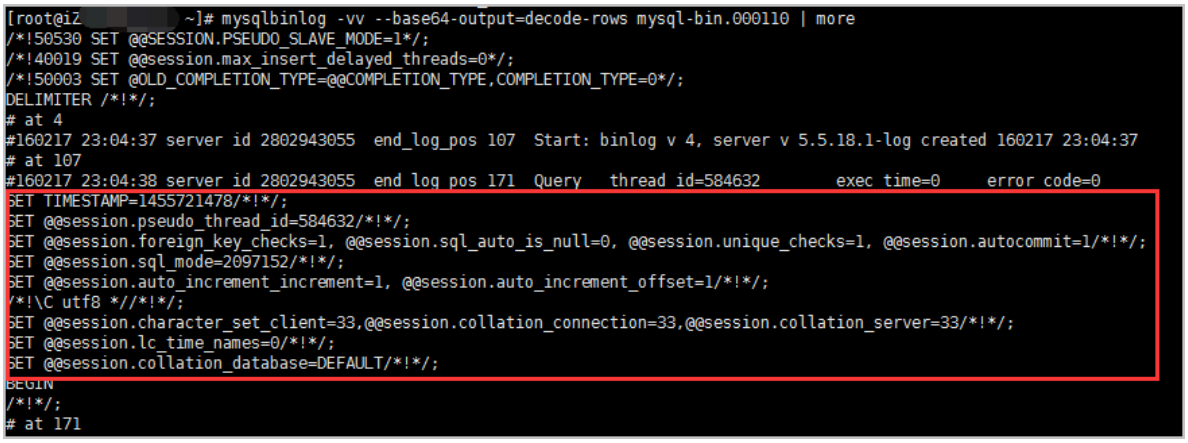
1. #unique_22 on your Linux-based on-premises host that runs MySQL.
2. Run the following command in the CLI:

```
mysqlbinlo  g  - vv  -- base64 - output = decode - rows  < Save
path  of  binary  files >
```

Note:

- `- vv` : to view SQL statements and remarks.

- `--base64-output=decode-rows`: to decode the content.



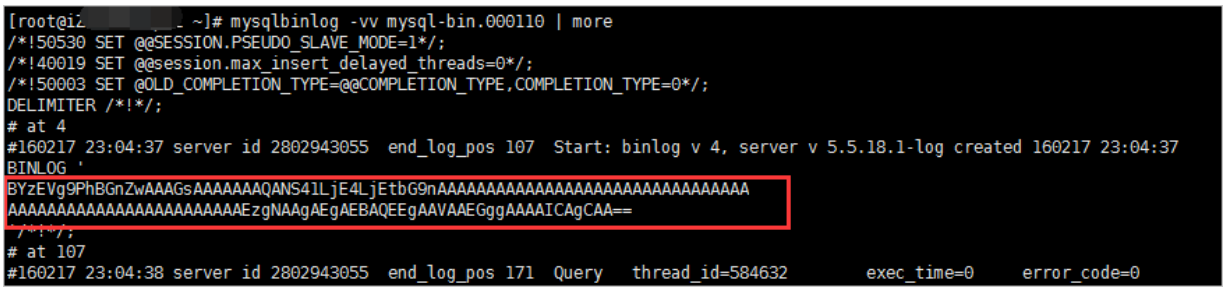
System errors

```
ERROR : Error in Log_event :: read_log_e vent (): ' Sanity
check failed ', data_len : 151 , event_type : 35
ERROR : Could not read entry at offset 120 : Error in
  log format or read error .
```

If either of the preceding errors occurs, check the version of the used `mysqlbinlog` command. For example, if you use Version 3.3, these errors may occur. In such case, you can upgrade the command version.

Content errors

If you forget to enter `--base64-output=decode-rows`, the displayed content is not decoded, as shown in the following figure.



3 Functions and billing methods

3.1 Why does RDS for MySQL not support the MyISAM engine?

The following lists the major reasons why RDS for MySQL does not support the MyISAM engine:

- **MyISAM has defects in data integrity protection, and these defects may cause corruption or even loss of database data. Additionally, many of these defects are design issues and cannot be fixed without compromising compatibility.**
- **Most data corruption issues of MyISAM can only be manually fixed, and therefore MyISAM cannot be used for product services.**
- **For RDS storage, MyISAM is not the best solution for I/O operations. Therefore, MyISAM does not necessarily surpass InnoDB in terms of performance.**
- **It is easy to migrate from MyISAM to InnoDB because most applications simply need to modify the table creation code.**
- **MyISAM is developing towards InnoDB. MySQL 5.7 can be completely different from MyISAM and the system's data control is also switched to InnoDB.**

4 Space/Memory

4.1 What occupies the capacity of new RDS for MySQL instances?

In RDS for MySQL instances, system files ib_logfile0 and ib_logfile1 occupy certain storage capacity.

After creating an RDS for MySQL instance, you can see that a few GB of storage space has been used. This is because of the system files ib_logfile0 and ib_logfile1.

The two log files are used to store the transaction log of the InnoDB engine table. Their size is always approximately 2 GB and cannot be changed. Due to the large size of the two files, the transaction log files do not need to be switched frequently when there are highly concurrent transactions. Therefore, the instance performance is improved.