# Alibaba Cloud ApsaraDB for MySQL

## User Guide

Issue: 20180912

# 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 instructio ns, 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 Connection management

## 1.1 Set the access mode

This function has been replaced by the database proxy function. For more information, see *Database proxy*.

## 1.2 Set network type

RDS supports two network types: classic network and Virtual Private Cloud (VPC). We recommend VPC because it provides higher security. This document describes the differences between the two network types and the method of switching between the network types.

> **Note:**
> To migrate an instance from a classic network to a VPC without service interrupptions, see *Hybrid access solution for the seamless migration from classic network to VPC*.

**Background information**

On the Alibaba Cloud platform, a classic network and a VPC differs in the following aspects:

- Classic network: Cloud services in a classic network are not isolated, and unauthorized access can be blocked only by the security group or whitelist policy of cloud services.
- VPC: It helps you build an isolated network environment in Alibaba Cloud. You can customize the routing table, IP address range and gateway on the VPC. In addition, you can combine your data center and cloud resources in the Alibaba Cloud VPC into a virtual data center through a leased line or VPN to smoothly migrate applications to the cloud.

**Precautions**

- After switching the network type, the original intranet IP address is changed and the Internet IP address remains unchanged. Update the connection address on your applications if necessary. For example, after an RDS instance is switched from a classic network to a VPC, the intranet IP address of the classic network is released and a VPC IP address is generated. Therefore, ECS instances in classic networks cannot access the RDS instance through the intranet any more.
- To switch MySQL 5.5, MySQL 5.6, or SQL Server 2008 R2 instances from a classic network to a VPC, the access mode must be set to safe connection mode. To switch the access mode, see *Set access mode*.

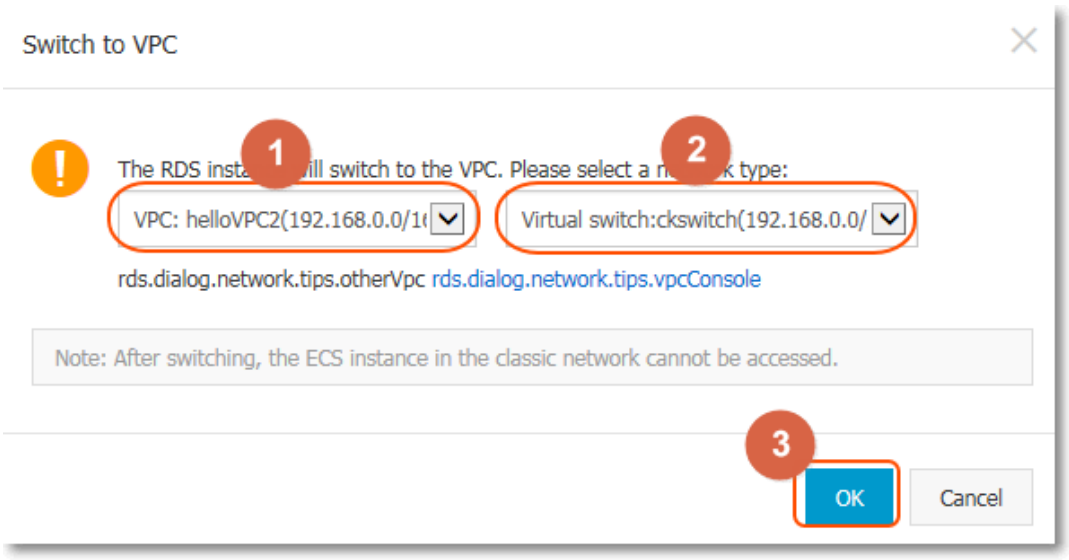
> **Note:**
> MySQL 5.5, MySQL 5.6, and SQL Server 2008 R2 instances in North China 1, North China 2, East China 1, and Hong Kong regions do not have this constraint.

- During network type switching, RDS services may be interrupted for about 30 seconds. Therefore, switch the network type during off-peak hours or make sure that your applications have the automatic reconnection mechanism.

**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 enter the **Basic Information** page.
4. Click **Connection Options** in the left-side navigation pane to open the **Connection Options** page.
5. Do as follows to switch the network type:
   - Switch from a classic network to a VPC
     1. Click **Switch to VPC**.
     2. Select a VPC and a virtual switch.

        > **Note:**
        > - If the drop-down lists do not display VPCs or virtual switches or if the VPCs and virtual switches are not what you need, create a VPC and virtual switch that are in the same region as the RDS instance. To create a VPC, see *Create a VPC*. To create a virtual switch, see *Create a switch*.
        > - For MySQL 5.5, MySQL 5.6, and SQL Server 2008 instances, their access mode must be safe connection mode if you want to switch from a classic network to a VPC. To switch the access mode, see *Set access mode*.




3. Click **OK**.

- Switch from a VPC to a classic network

  1. Click **Switch to Classic Network**.
  2. Click **OK**.

# 1.3 Hybrid access solution for smooth migration from classic networks to VPCs

*Virtual Private Cloud (VPC)* is a private network logically isolated from other virtual networks. A VPC allows you to build an isolated network environment with better security and performance than classic networks. With these benefits, VPCs have become a preferred networking choice for cloud users.

To meet the increasing network migration needs, RDS has added a new feature called hybrid access mode. This feature enables smooth migration from classic networks to VPCs with no intermittent service interruption or access interruption. The feature also offers the option to migrate a master instance and its read-only instances separately to a VPC without any interference with each other.

This document explains how to migrate from a classic network to a VPC on the RDS console using the hybrid access solution.

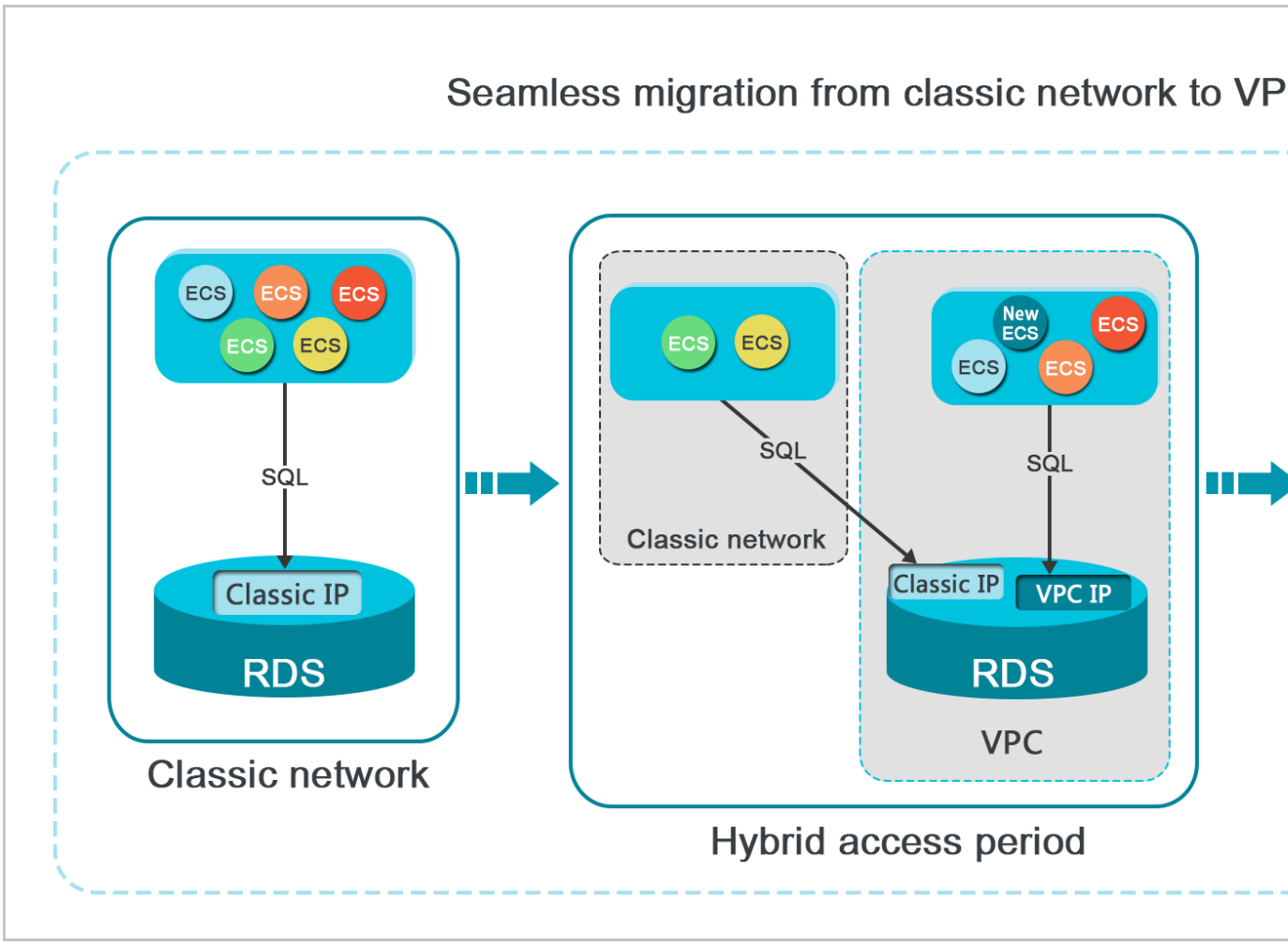
**Background information**

With a traditional solution, migrating an RDS instance from a classic network to a VPC causes immediate release of classic network IP address. As a result, an intermittent interruption for up to 30 seconds may be caused, and ECS on the classic network can no longer access the RDS

instance using the intranet IP address, which may have negative impact on your services. In many large companies, a database is usually designed for access by more than one application system . When they decide to migrate the database from a classic network to a VPC, it would be quite difficult to migrate the network of all the applications simultaneously, which may result in bigger impact on their services. Therefore, a transitional period is required. To accommodate the need for smooth migration, RDS has added the hybrid access feature, making it possible to have such a transitional period.

Hybrid access refers to the ability of an RDS instance to be accessed by ECSs on both a classic network and a VPC. During the hybrid access period, the RDS instance reserves the intranet IP address of the original classic network and adds an intranet IP address for a VPC, which prevents any intermittent interruption during migration. We recommend that you use a VPC only for purposes of security and performance. For this reason, hybrid access is available for a limited period of time. That means the intranet IP address of the original classic network is released when the hybrid access period expires. In this case, your applications cannot access the database using the intranet IP address of the classic network. You must configure the intranet IP address for a VPC in all your applications during the hybrid access period to guarantee smooth network migration and minimize the impact on your services.

For example, a company wants to migrate its database from a classic network to a VPC. The hybrid access solution can be used to provide a transitional period during which some of their applications can access the database through a VPC, and the others can continue to access the database through original classic network. When all the applications can access the database through the VPC, the intranet IP address of the original classic network can be released, as shown in the following figure.




**Functional Limits**

The following functional limits are proposed during the hybrid access period:

- Switch to classic networks is not supported.
- Zone migration is not supported.
- Switch between the High-availability Edition and Finance Edition is not supported.

**Prerequisites**

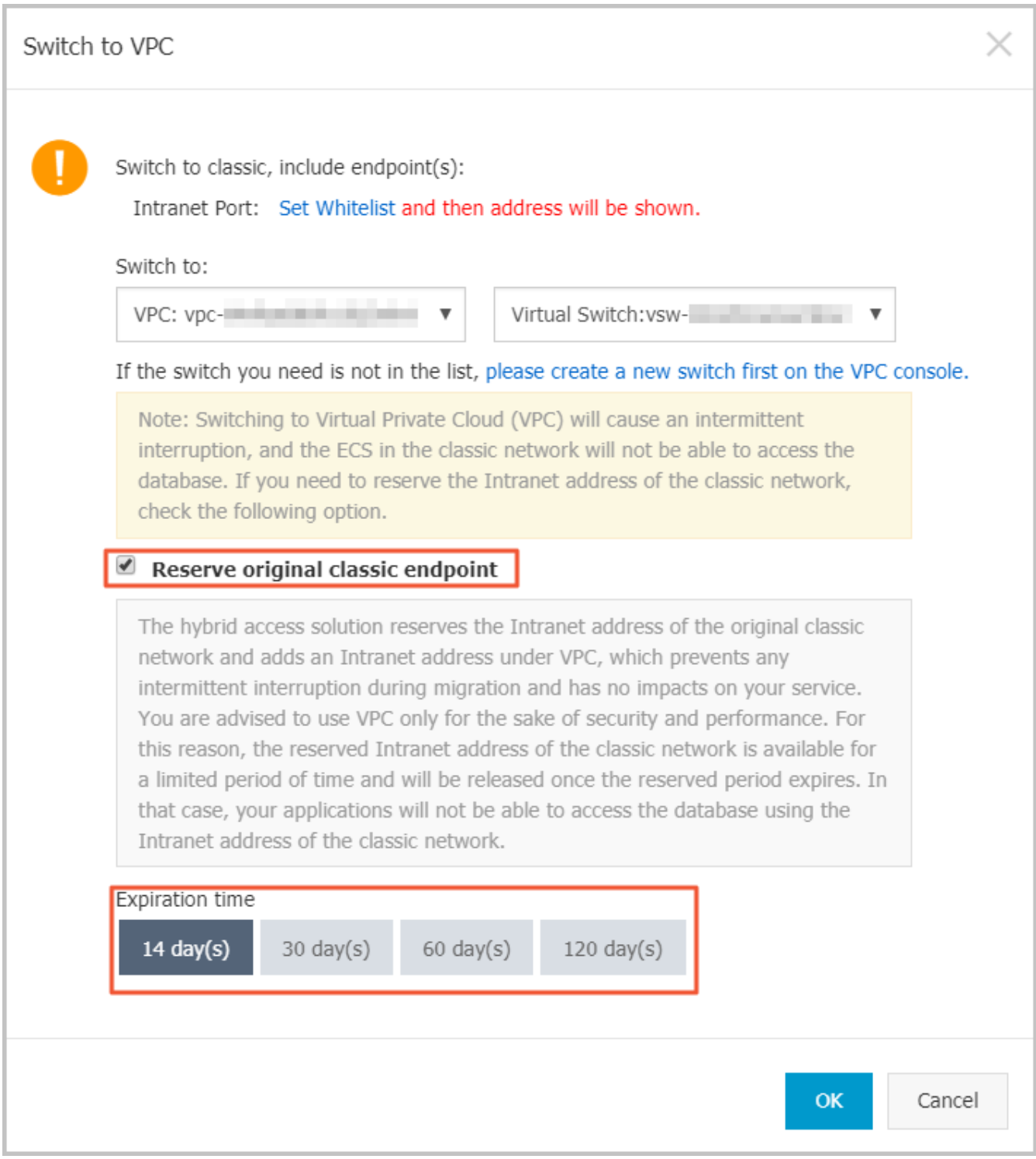
- The current access mode is safe connection mode. For more information on how to switch the access mode, see *Set access mode*. MySQL 5.7, SQL Server 2012, and SQL Server 2016 only support standard mode, but these instances also support hybrid access in this condition.
- The current network type is classic network.
- There are available VPC and VSwitch in the zone where the RDS instance is located. If not, create them by referring to *Create VPC* and *Create VSwitch*.

**Migration 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, click **Connection Options** to enter the **Connection Options** page.
5. On the **Instance Connection** tab page, click **Switch to VPC**.
6. On the **Switch to VPC** confirmation page, select the target VPC and Vswitch.
7. Check **Reserve original classic endpoint**, and select the **Expiration time** for the basic intranet IP address of the original network, as shown in the following figure.

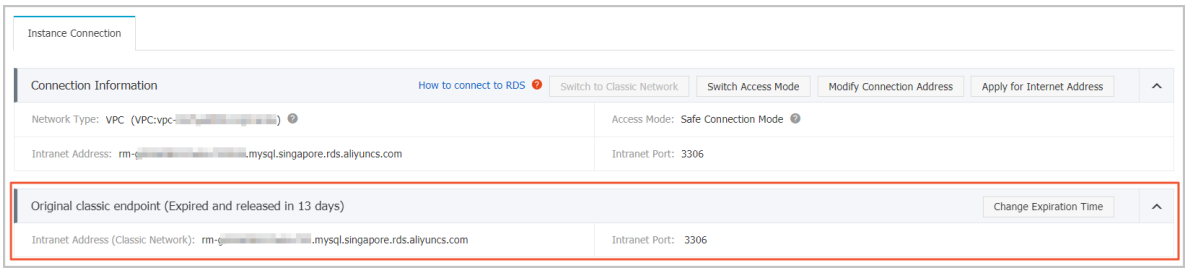
**Note:**

- From the seventh day before the date on which the intranet IP address of the original classic network is to be released, the system sends a text message of a notice to the mobile number bound to your account every day.
- When the reservation ages out, the intranet IP address of the classic network is automatically released and can no longer be used to access the database. To prevent service interruption, set a reservation period as necessary. After the hybrid access configuration is complete, you can change the expiration date.




8. Click **OK**.

   The **Original classic endpoint** area is displayed, as shown in the following figure.




### Change the expiration time of the original classic network

During the hybrid access period, you can change the reservation period of the intranet IP address of the original classic network at any time as needed, and the expiration date is recalculated from the new date. For example, if the intranet IP address of the original classic network is set to August 18, 2017, and you change the expiration time to 14 days later on August 15, 2017, the address is released on August 29, 2017.

Follow these steps to change the expiration time:

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, click **Connection Options** to enter the **Connection Options** page.
5. On the **Instance Connection** tab page, click **Change Expiration time**, as shown in the following figure.


6. On the **Change Expiration Time** confirmation page, select an expiration time and click **OK**.

## 1.4 Set intranet and Internet IP addresses

You can select the connection type (intranet or Internet) of the instance according to your business requirements. The system generates an intranet IP address by default, so this document mainly introduces how to apply for an Internet IP address, set the connection address of the Internet or intranet, and release an Internet IP address.

### Background information

RDS supports connections through the both intranet and Internet. The *series*, version, and *access mode* have the following effects on the selection of the connection address.

| Instance series | Instance version | Access mode | Connection address |
| --- | --- | --- | --- |
| Basic Edition | • MySQL 5.7<br>• SQL Server 2012 | Standard mode | • Intranet IP address<br>• Internet IP address<br>• intranet and Internet IP addresses |
| High-availability Edition | • MySQL 5.5/5.6<br>• SQL Server 2008 R2<br>• PostgreSQL 9.4<br>• PPAS 9.3 | Standard mode | • Intranet IP address<br>• Internet IP address |
| | | Safe connection mode | • Intranet IP address<br>• Internet IP address<br>• intranet and Internet IP addresses |
| Finance Edition | MySQL 5.6 | Standard mode | • Intranet IP address<br>• Internet IP address |
| | | Safe connection mode | • Intranet IP address<br>• Internet IP address<br>• intranet and Internet IP addresses |

The applicable scenarios of the connection addresses are as follows:

- Use the intranet IP address only:
  - The system provides an intranet IP 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 IP address only:
  - This scenario is applicable when your application is deployed on the ECS instance that is located in the different region from that of your RDS instance.
  - This scenario is applicable when your application is deployed on a platform other than Alibaba Cloud.
- Use both of the intranet and Internet IP addresses:

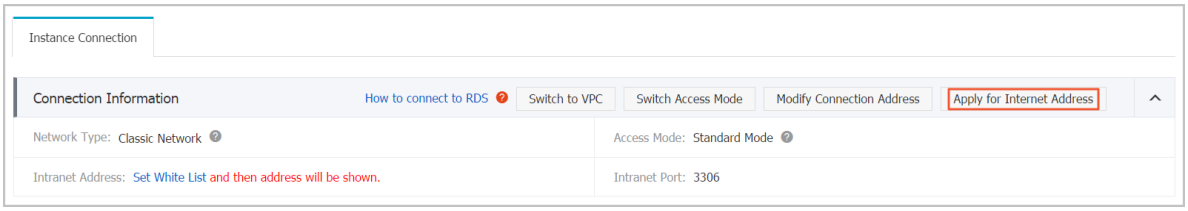
- This scenario is applicable when your application is deployed on the ECS instance that is located in the same region and has the same *network type* as your RDS instance, and application modules are deployed in an ECS where your RDS instance is not located.
- This scenario is applicable when your application 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 a platform other than Alibaba Cloud.

**Attentions**

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

**Apply for an Internet IP address**

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. Click **`Connection options`** in the left-side navigation pane.
5. Click **Apply for Internet Address**, as shown in the following picture.



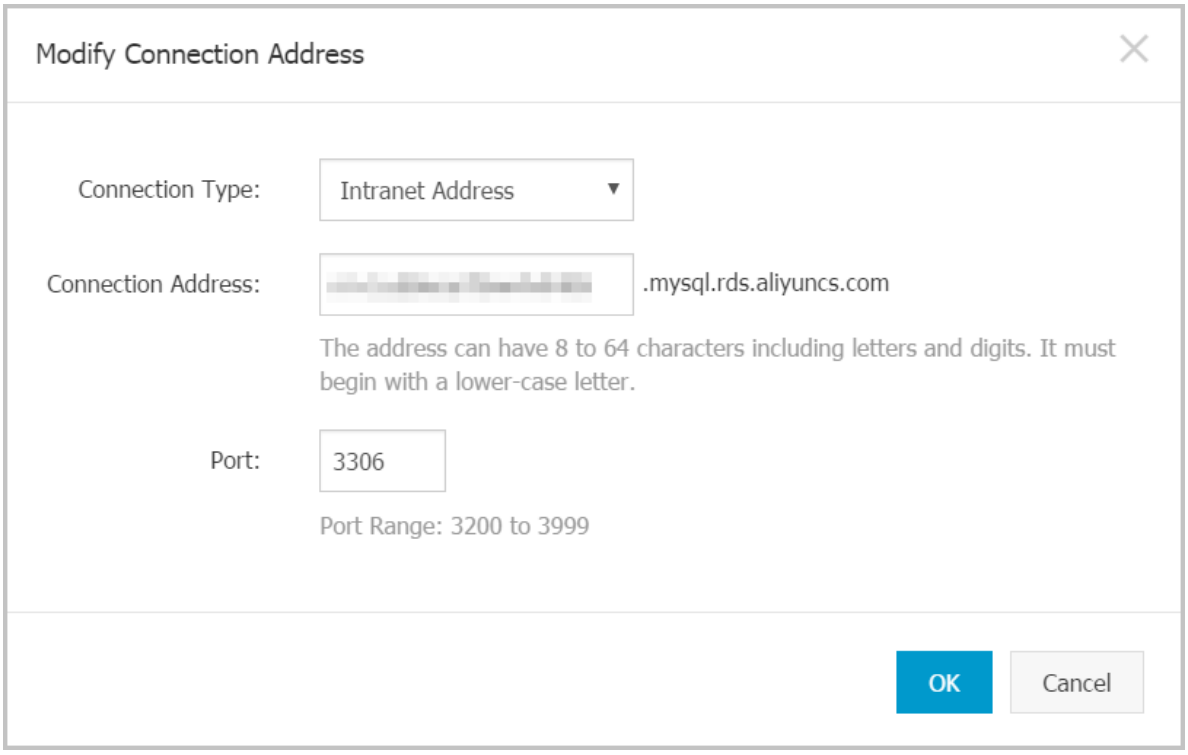

6. On the displayed confirmation window, click **OK** to generate an Internet IP address.

**Modify the connection address**

You can modify the Internet and intranet connection address based on your needs.

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. Click **Connection options** in the left-side navigation pane.
5. Click the **Instance Connection** tab.
6. In the **Connection Information** area, click **Modify Connection Address**.
7. Select the connection type and modify its connection addresses and port number, and then click **OK**, as shown in the following figure.




Parameters description:

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

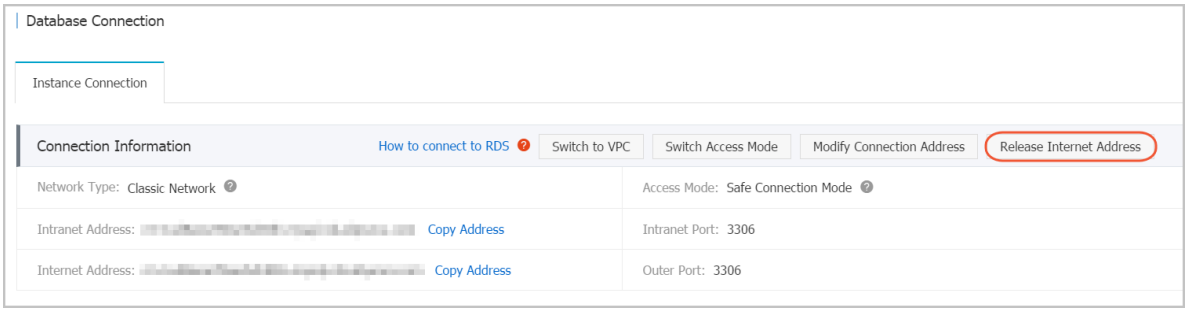
**Release an Internet IP address**

If you want to release an Internet IP address, do as follows:

**Note:**

The operation can be performed only in **safe connection mode**. For more information about the safe connection mode, see *Set access mode*.

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. Click **Connection options** in the left-side navigation pane.
5. Click the **Instance Connection** tab.
6. In the **Connection Information** area, click **Release Internet Address**.




7. Click **Confirm** on the displayed confirmation dialog box to release the Internet IP address.

# 2 Security

## 2.1 SQL audit

The SQL audit function allows you to view SQL details and periodically audit RDS instances.

**Attentions**

- Certain RDS instance types do not support the SQL audit function.
- The SQL audit function does not affect instance performance.
- SQL audit logs are kept for 30 days.
- Exported SQL audit files are kept for 2 days.
- The SQL audit function is disabled by default. Enabling this function incurs charges. For more information, see *Pricing*.

**Differences between SQL audit logs and binlog**

For MySQL instances, you can use SQL audit logs or binlog to view incremental data. Differences between them are as follows:

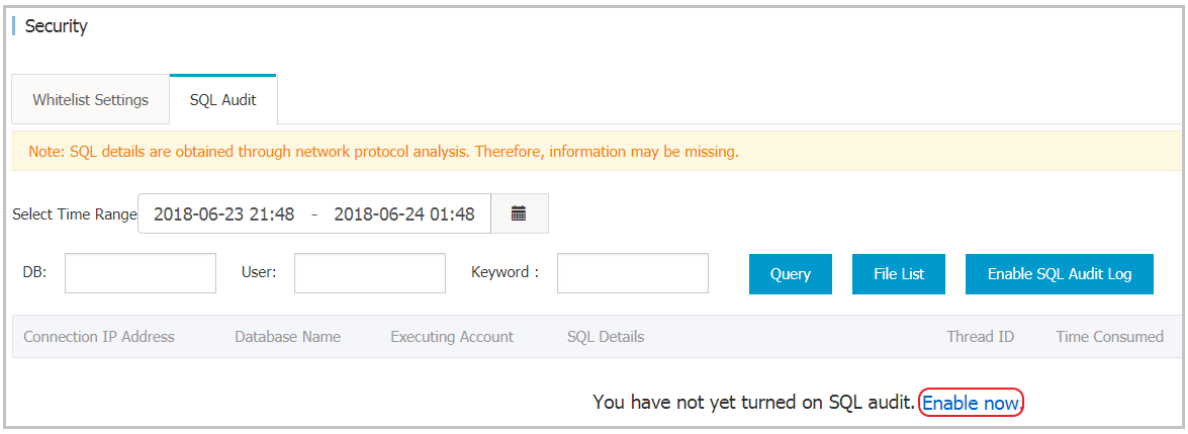
- SQL audit logs: Similar to MySQL audit logs, SQL audit logs collect information about all DML and DDL operations. The information is obtained through network protocol analysis. The SQL audit function does not parse actual parameter values, and a small number of records may be lost when the SQL query volume is large. Therefore, using SQL audit logs to collect incrementa l data may be inaccurate.
- Binlog: Binary logs accurately record all ADD, DELETE, and MODIFY operations and can accurately recover incremental data. Binary logs are stored in the instance temporarily. The system regularly transfers them to OSS and they are stored on OSS for 7 days. The system cannot save binlog files where data is being written, so certain binary logs are not uploaded when you click **Upload Binlog** on the RDS console.

  Therefore, binary logs accurately record incremental data, but you cannot obtain real-time binary logs.

**Enable SQL audit**

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 go to the **Basic Information** page.
4. In the left-side navigation pane, click **Security**.

5. Click the **SQL Audit** tab and click **Enable now**.



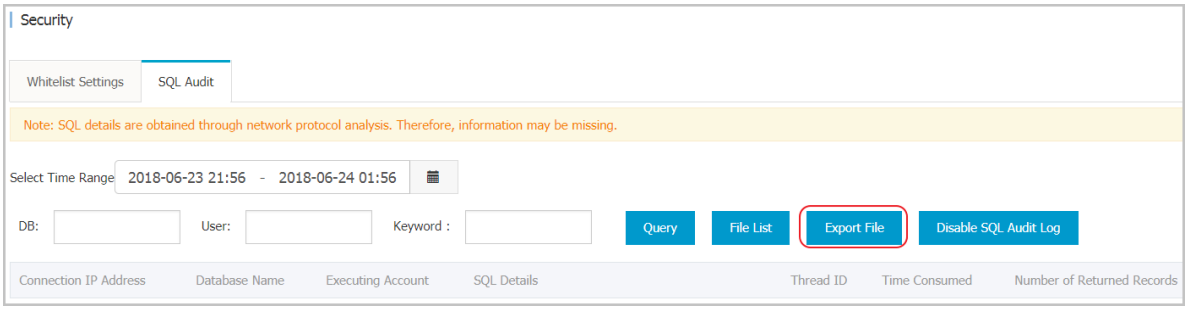

6. In the displayed dialog box, click **Confirm**.

## Disable SQL audit

To save costs, you can disable the SQL audit function when you do not need it.

> **Note:**
> Disabling the SQL audit function deletes all SQL audit logs. Export logs before disabling the function.

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 go to the **Basic Information** page.
4. In the left-side navigation pane, click **Security**.
5. Click the **SQL Audit** tab. Click **Export File** and then click **Confirm**.




6. Download the SQL audit file and put it in a local directory.
7. Click **Disable SQL Audit Log** and then click **Confirm**.

# 2.2 Set a whitelist

A whitelist contains specified IP addresses and IP address segments that are allowed to access RDS. By default, the RDS whitelist contains only the default IP address 127.0.0.1 and has no security group. This means that no server can access the RDS instance.

After you set a whitelist, only the following servers can access RDS:

- Servers whose IP addresses are in the whitelist
- ECS instances that are in the security group specified in the whitelist

A security group is a virtual firewall that is used to set network access control for one or more ECS instances. For more information about ECS security groups, see *Create a security group*.

We recommend that you periodically check and adjust your whitelists according to your requirements to maintain RDS security. The whitelist only controls access to the RDS instance but does not affect your instance. This document describes how to set a whitelist.

**Attentions**

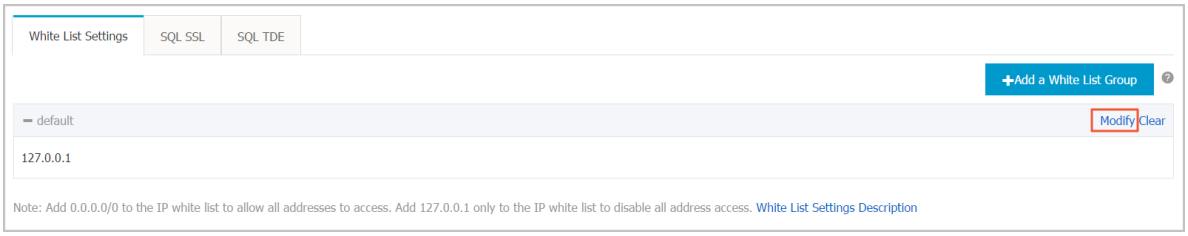
- The default whitelist group can only be modified or cleared, but cannot be deleted.
- % or 0.0.0.0/0 indicates any IP address is allowed to access the RDS instance. This configuration greatly reduces the security of the database and is not recommended.
- When a whitelist is set, the system automatically generates an intranet IP address for the RDS instance. If you need an Internet IP address, see *Set intranet and Internet addresses*.
- If you cannot connect to the RDS instance after adding the application service IP address to the whitelist, you can obtain the actual IP address of the application by referring to *How to locate the local IP address using ApsaraDB for MySQL*.

**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. Click **Security** in the left-side navigation pane to visit the **Security** page.
5. On the **Whitelist Settings** tab page, find the **default** whitelist group and click **Modify**.

**Note:**

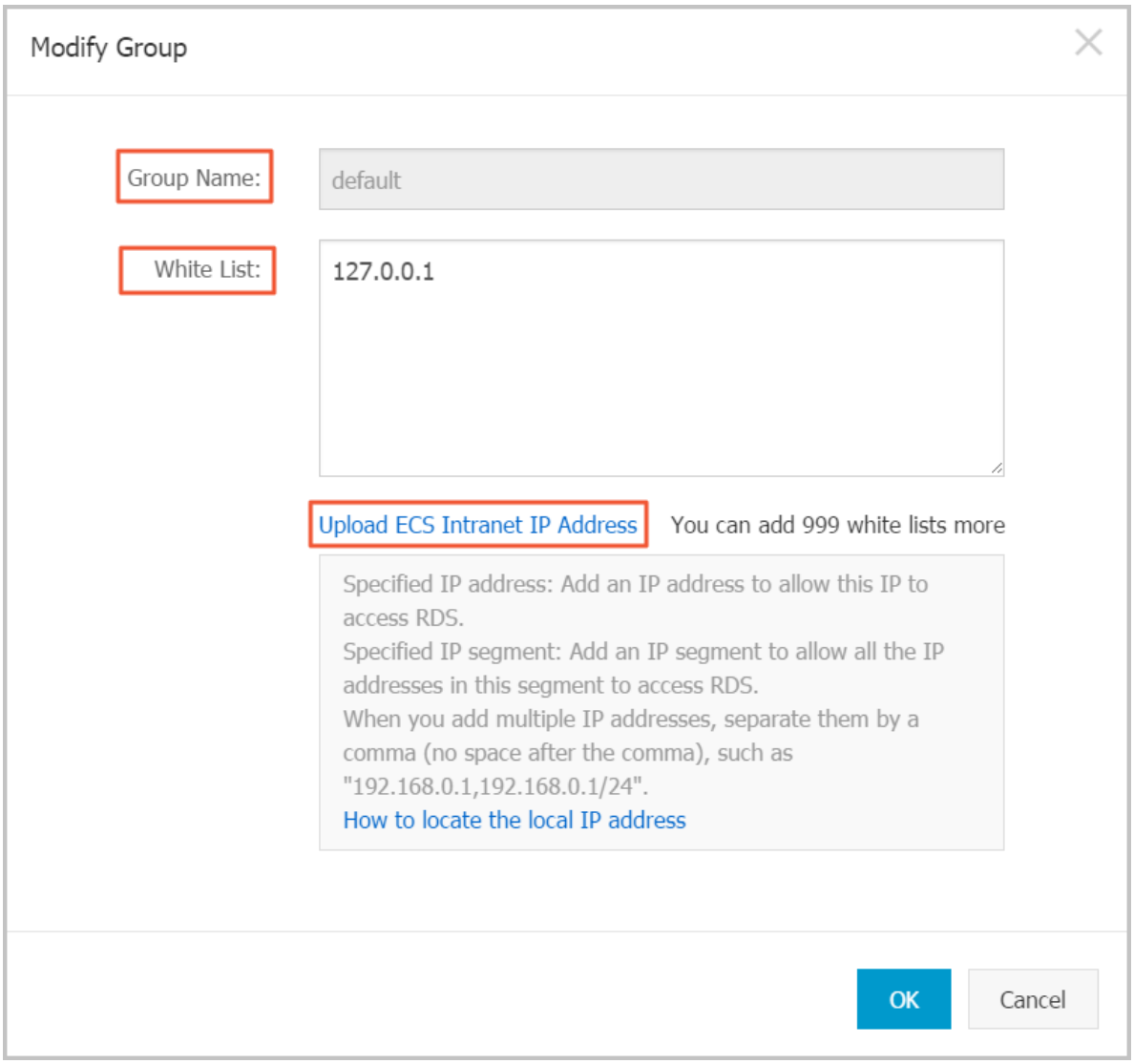
To add a customized whitelist group to the RDS instance, locate the **default** whitelist group and click **Clear** to delete the IP address 127.0.0.1, and then click **Add a whitelist Group**. The subsequent steps for customizing a whitelist are similar to the following steps.




6. On the **Modify Group** page, add the IP addresses or IP address segments that are allowed to access the RDS instance to the **`White List`** field. If you want to add the ECS intranet IP addresses, click **Upload ECS intranet IP Address**, select IP addresses, and click **OK**, as shown in the following figure.

**Note:**

If you add an IP address or IP address segment to the default group, the default IP address 127.0.0.1 is automatically deleted.




Parameter descriptions:

- **`Group Name`**: contains 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.
- **`White List`**: Enter the customized IP addresses or IP address segments that are allowed to access the RDS instance.
  - If you enter an IP address segment, such as 10.10.10.0/24, 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 address 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 address 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.

**Precautions for adding an ECS security group**

You can configure both the IP whitelist and ECS security group. Your RDS instance allows access from servers whose IP addresses are in the IP whitelist and ECS instances that are in the security group.

- Currently, only MySQL 5.6 and the Hangzhou, Qingdao, and Hong Kong regions support ECS security groups.
- One RDS instance supports one security group.
- Updates to the ECS security group are automatically applied to the whitelist.

**Add an ECS security group**

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 go to the **Basic Information** page.
4. Click **Security** in the left-side navigation pane to visit the **Security** page.
5. On the **Whitelist Settings** tab page, click **Add to Security Group**.

   **Note:**
   The security groups marked with "VPC" are in VPCs.
6. Select a security group and click **OK**.

# 2.3 Set SSL encryption

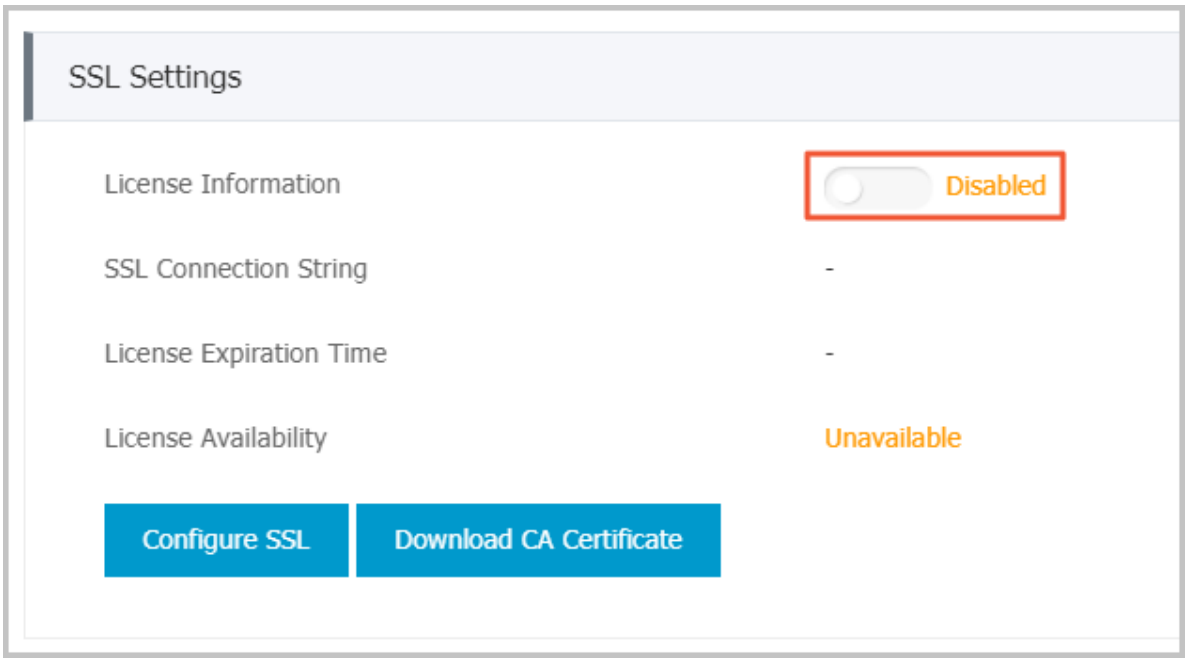
To increase link security, you can enable Secure Sockets Layer (SSL) encryption and install an SSL certificate for necessary application services. SSL is used on the transport layer to encrypt network connections. It increases security and integrity of communication data, but also increases the network connection time.

**Note:**

- Due to the inherent drawbacks of SSL encryption, activating this function significantly increases your CPU usage. We recommend that you only enable SSL encryption for Internet connections requiring encryption. Intranet connections are relatively secure, and generally do not require link encryption.
- In addition, SSL encryption cannot be disabled once it is enabled. Therefore, enable SSL encryption with caution.

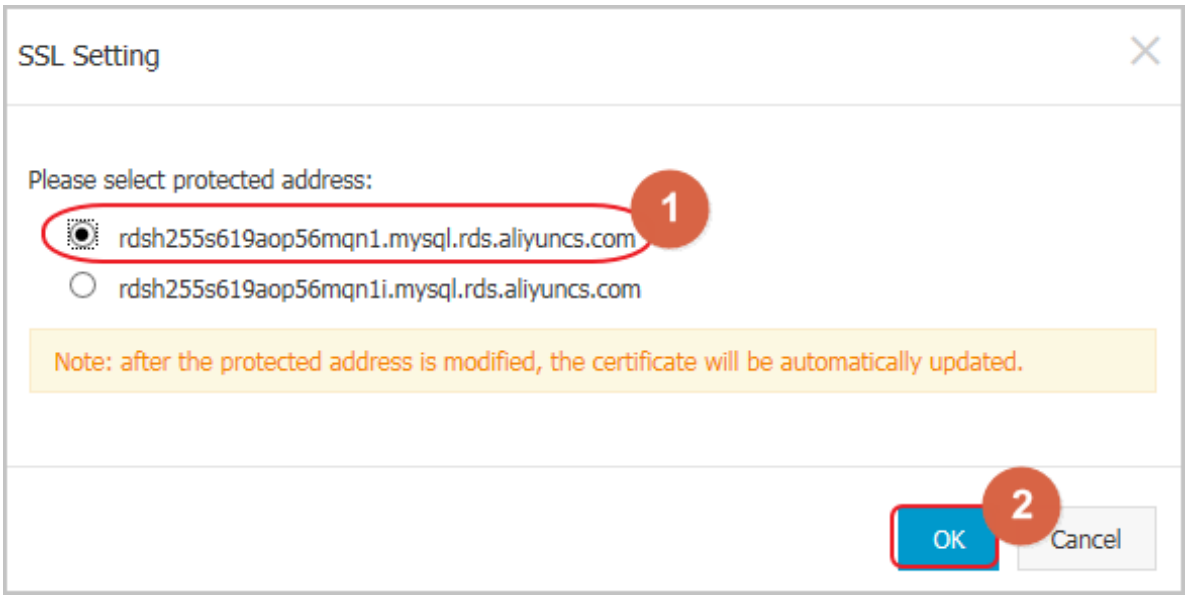
**Enable SSL encryption**

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 enter the **Basic Information** page.
4. In the left-side navigation pane, click **Security** to go to the **Security** page.
5. Click the **SSL** tab.
6. Click the button next to **Disabled**, as shown in the following figure.

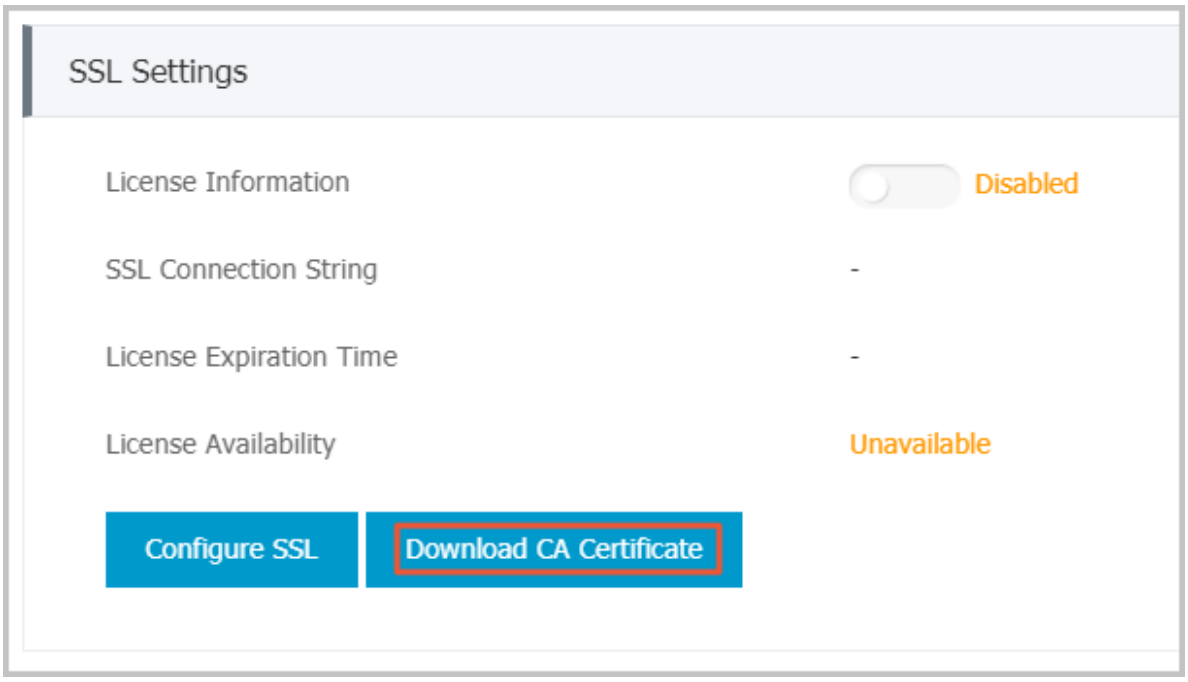



7. In the **SSL Setting** dialog box, select the link for which SSL encryption needs to be enabled and click **OK** to activate SSL encryption, as shown in the following figure.

**Note:**
You can choose to encrypt both Internet and intranet links as needed, but only one link can be encrypted.




8. Click **Download CA Certificate** to download an SSL certificate, as shown in the following figure.




The downloaded SSL certificate is a package including the following files:

- p7b file: is used to import the CA certificate on Windows OS.
- PEM file: is used to import the CA certificate on other systems or for other applications.
- JKS file: is a Java truststore certificate file used for importing CA certificate chains in Java programs. The password is apsaradb.

**Note:**

When using JKS certificate files in Java, modify default jdk security configurations of jdk7 and jdk8 as follows: In the `jre/lib/security/java.security` file of the machine that runs the database to be accessed through SSL, modify the following configurations:

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, DH keySize < 224
jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 1024
```

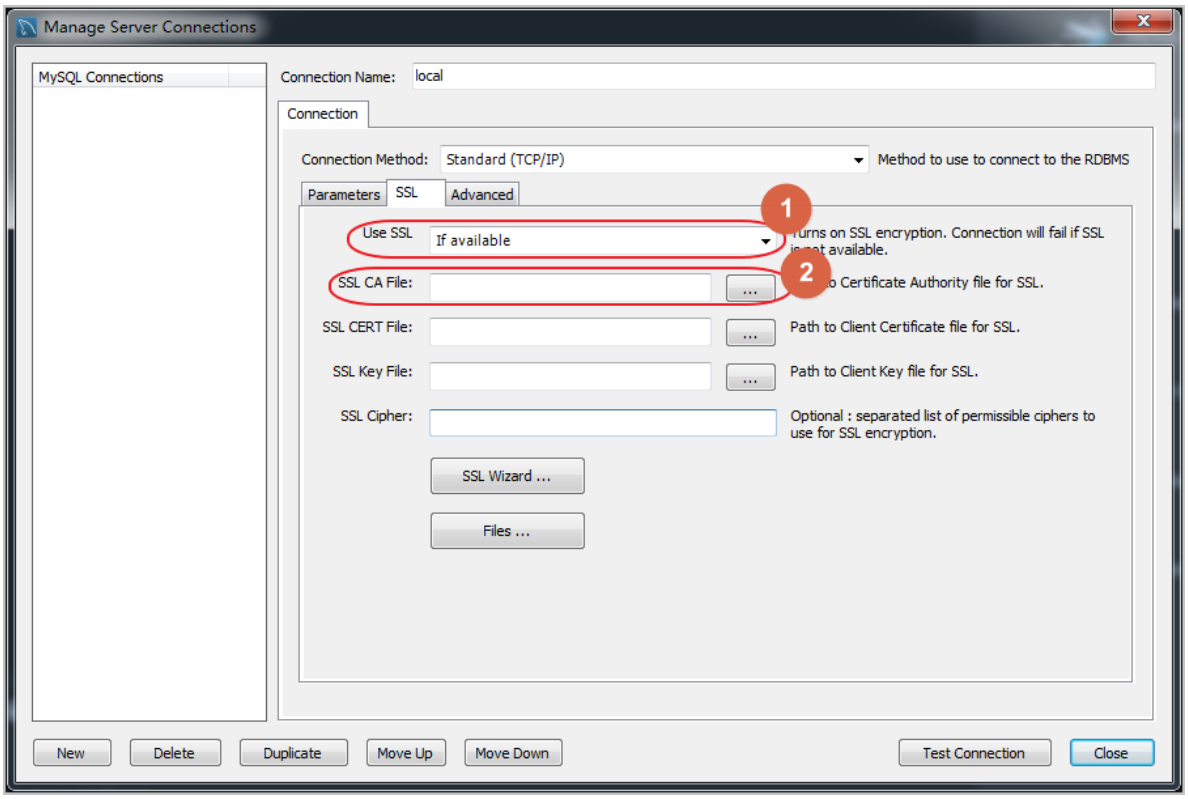
If you do not modify the JDK security configuration, the following error will be reported. Other similar errors are generally caused by Java security configurations.

```
javax.net.ssl.SSLHandshakeException: DHPublicKey does not comply
to algorithm
            constraints
```

### Configure the SSL CA certificate

After SSL encryption is enabled, you need to configure the SSL CA certificate for applications or clients that access RDS. The following uses MySQL Workbench as an example to describe how to install the SSL CA certificate. For other applications or clients, see their usage instructions.

1. Open MySQL Workbench.
2. Choose **Database** > **Manage Connections** .
3. Enable **Use SSL** and import the SSL CA certificate, as shown in the following figure.




## 2.4 Set TDE

Transparent Data Encryption (TDE) can be used to perform real-time I/O encryption and decryption on instance data files. To improve data security, you can enable TDE to encrypt instance data.

**Note:**

Currently, TDE is only applicable to databases of SQL Server 2008 R2 and MySQL 5.6. To view or modify TDE settings, you need to log on with an Alibaba Cloud account rather than a RAM account.

### Background information

TDE provides real-time I/O encryption and decryption on data files. The data is encrypted before being written to the disk and decrypted when being reading from the disk into the memory. TDE does not increase the size of data files. Developers do not have to modify any applications before using the TDE function.

### Considerations

- Once TDE is activated, it cannot be deactivated.

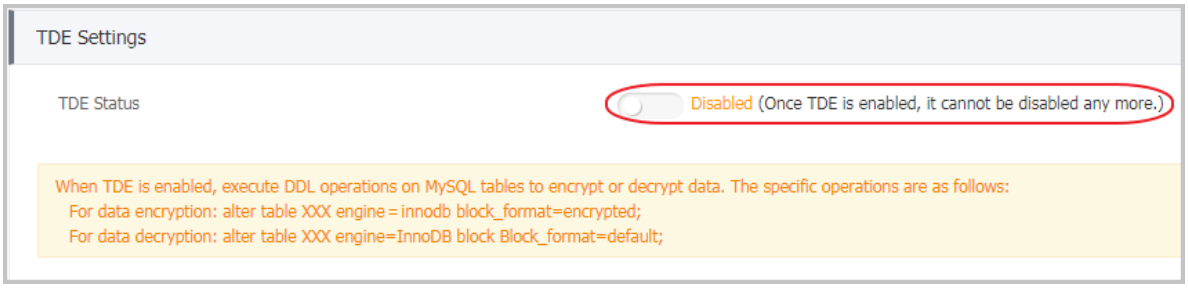
- Encryption uses keys produced and managed by the Key Management Service (KMS). RDS does not provide the keys and certificates required for encryption. After TDE is activated, if you want to restore data to your local device, use RDS to decrypt the data first.
- After TDE is activated, CPU usage significantly increases.

**Prerequisite**

KMS is activated.

**Procedure**

1. Log on to the *RDS console* and select the target instance.
2. Click **Data Security** in the left-side navigation pane.
3. On the **Data Security** page, click the **TDE** tab.
4. Click **Not Activated**, as shown in the following figure.




5. Click **OK** to activate TDE.

> **Note:**
> If you have not activated KMS, you are prompted to do so when activating TDE. After activating KMS, click **Not Activated** to activate TDE.

6. Log on to the database and run the following command to encrypt the relevant tables.

```
alter table <tablename> engine=innodb, block_format=encrypted;
```

**Subsequent operation**

If you want to decrypt a table encrypted by TDE, run the following command.

```
alter table <tablename> engine=innodb, block_format=default;
```

## 2.5 Switch the IP whitelist to enhanced security mode

**IP whitelist modes**

RDS instances provide two IP whitelist modes:

- **Standard mode**: IP addresses in the whitelist apply to both classic networks and VPCs. This has security risks, so you are recommended to switch to the enhanced security mode.
- **Enhanced security mode**: IP addresses in the whitelist are classfiied into two types: IP addresses for classic networks and those for VPCs. In this mode, you need to specify the network type when you create an IP whitelist group.

  Currently, RDS for MySQL, PostgreSQL, and PPAS instances support the enhanced security mode.

**Changes after switching to the enchanced security mode**

- If the instance network type is VPC, a new whitelist group is generated and contains all IP addresses in the original whitelist. The new IP whitelist group applies only to VPCs.
- If the instance network type is classic network, a new whitelist group is generated and contains all IP addresses in the original whitelist. The new IP whitelist group applies only to classic networks.
- If the instance is in *hybrid access mode* (namely, an instance uses both a classic network and a VPC), two new whitelist groups are generated and each contain all IP addresses in the original whitelist. One of the whitelist group applies to VPCs and the other applies to classic networks.

**Note:**

The switch does not affect the *ECS security group* in the instance whitelist.

**Attention**

An IP whitelist can be switched from the standard mode to the enhanced security mode, and the switch is irreversible.

**Procedure**

1. Log on to the *RDS console*.
2. Select the region where the instance is located.
3. Click the ID of instance.
4. In the left-side navigation pane, select **Security**.
5. On the **Whitelist Settings** tab page, click **Enable Enhanced Security Whitelist (Recommended)**.


6. In the displayed dialog box, click **Confirm**.

# 3 Monitoring and Alarming

## 3.1 Set the monitoring frequency

**Background information**

The RDS console provides abundant performance metrics for you to conveniently view and know the running status of instances. You can use the RDS console to set the monitoring frequency, view monitoring data of a specific instance, create monitoring views, and compare instances of the same type under the same account.

**Two monitoring frequencies provided before May 15, 2018**

- Once per 60 seconds (monitoring period: 30 days)
- Once per 300 seconds (monitoring period: 30 days)

**Second-level monitoring frequency introduced since May 15, 2018**

Minute-level monitoring frequencies cannot meet monitoring requirements of some users and maintenance personnel. Therefore, since May 15, 2018, RDS has introduced second-level monitoring frequencies. This facilitates problem locating and improves customer satisfaction.

- **Once per 5 seconds (monitoring period: 7 days), turning to once per minute since the eighth day**
- The detailed monitoring policies are described in the following table.

| Instance type | Once per 5 seconds | Once per minute (60 seconds) | Once per 5 minutes (300 seconds) |
|---|---|---|---|
| Basic Edition | Not supported | Supported for free | Default configuration |
| High-availability or Finance Edition: Memory < 8 GB | Not supported | Supported for free | Default configuration |
| High-availability or Finance Edition: Memory >= 8 GB | Supported (Not free) | Default configuration | Supported for free |

**Restrictions**

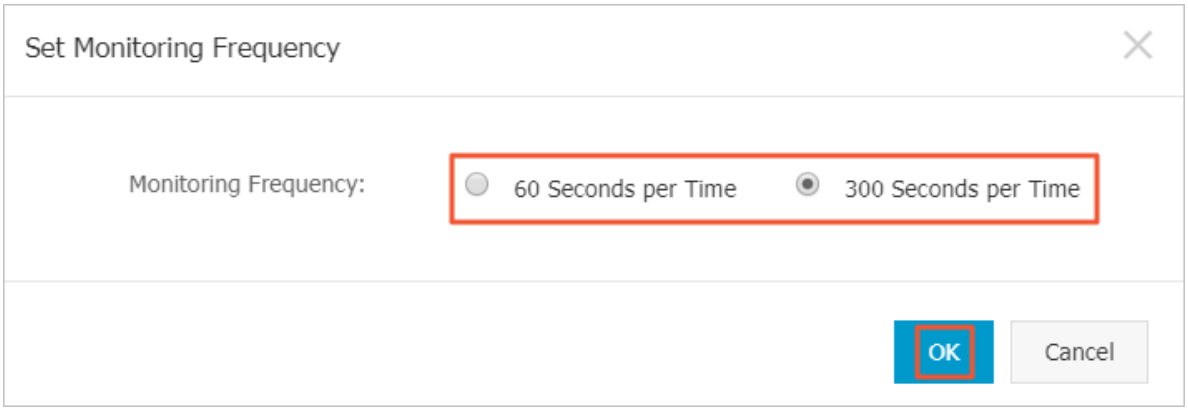
- You can configure second-level monitoring for instances that meet the following conditions:
  - The instance is located in these regions: China (Hangzhou), China (Shanghai), China ( Qingdao), China (Beijing), or China (Shenzhen)

  - The instance is an RDS for MySQL instance.
  - The instance storage type is local SSD.
  - The instance memory space is 8 GB or more.
- All engines (MySQL, SQL Server, ProstgraSQL, and PPAS) and database versions support the following monitoring frequencies:
  - Once per 60 seconds
  - Once per 300 seconds

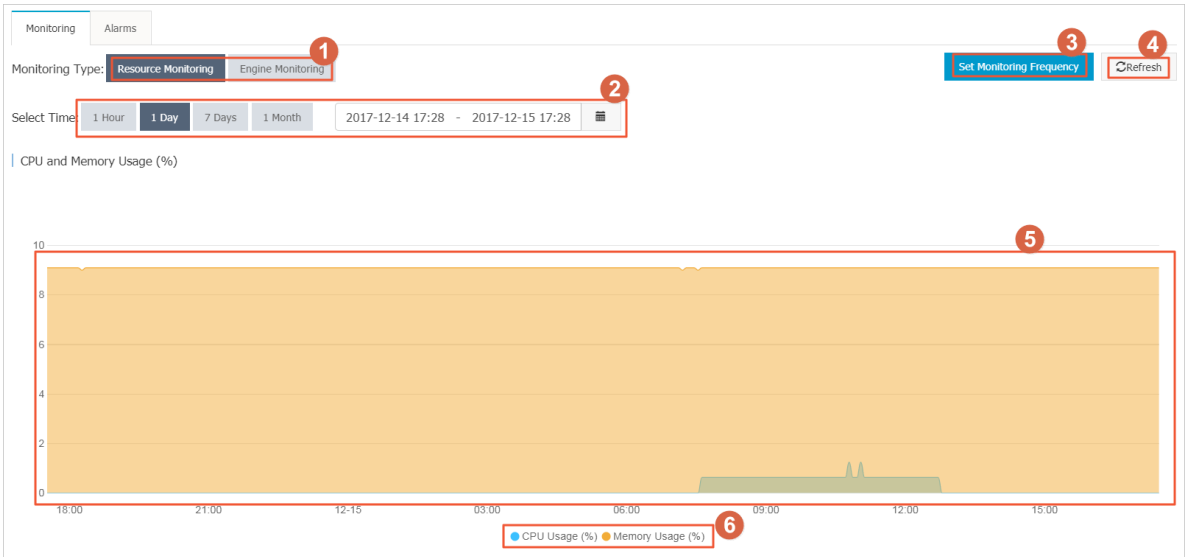
**Procedure**

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 enter the **Basic Information** page.
4. Click **Monitoring and Alarms** in the left-side navigation pane.

   **Note:**
   Different types of databases support different metrics. For more information, see **List of monitoring items** at the end of this document.
5. Click the **Monitoring** tab.
6. Click **Set Monitoring Frequency**.
7. Select the monitoring frequency in the **Set Monitoring Frequency** dialog box and click **OK**.




8. In the displayed **Confirm** dialog box, click **OK**.
9. On the **Monitoring** page, perform the following operations:




**Interface description:**

| No. | Description |
| --- | --- |
| 1 | Select the monitoring type. |
| 2 | Select the monitoring period. |
| 3 | Set the monitoring frequency. |
| 4 | Refresh monitoring results. |
| 5 | View monitoring results. |
| 6 | Select monitoring items. |

## List of monitoring items

### RDS for MySQL

| Monitoring items | Description |
| --- | --- |
| Disk Space | Disk space usage of the instance, including:<br>• Overall usage of the disk space<br>• Data space usage<br>• Log space usage<br>• Temporary file space usage<br>• System file space usage<br>Unit: MB |
| IOPS | Number of I/O request times of an instance per second. Unit: time/second |

| Monitoring items | Description |
| --- | --- |
| Total Connections | Total number of current connections, including the number of active connections and total connections |
| CPU and Memory Usage | CPU usage and memory usage of an instance (excluding the memory used by OS) |
| Network Traffic | Incoming/outgoing traffic of an instance per second. Unit: KB |
| QPS/TPS | Number of SQL statements executed and transactions processed per second |
| InnoDB Buffer Pool | InnoDB buffer pool read hit rate, utilization rate, and percentage of dirty data blocks |
| InnoDB Read/Write Volume | Average InnoDB data read and write times per second. Unit: KB |
| Number of InnoDB Read and Write Times Per Second | Number of read and write times per second of InnoDB |
| InnoDB Log | Number of InnoDB physical writes to a log file, log write requests, and FSYNC writes to a log file per second |
| Temporary Tables | Number of temporary tables created automatically on the hard disk when the database executes SQL statements |
| MyISAM Key Buffer | Average key buffer read hit rate, write hit rate, and usage per seconcd of MyISAM |
| MyISAM Read and Write Times | Number of MyISAM read and write times from/to the buffer pool and from/to the hard disk per second |
| COMDML | Number of statements executed on the database per second. The statements include:<br>• `Insert`<br>• `Delete`<br>• `Insert_Select`<br>• `Replace`<br>• `Replace_Select`<br>• `Select`<br>• `Update` |
| ROWDML | Number of operations performed on InnoDB, including:<br>• Number of physical writes to a log file per second<br>• Number of rows read in InnoDB tables per second<br>• Number of rows updated, deleted, and inserted in InnoDB tables per second |

**RDS for SQL Server**

| Monitoring items | Description |
| --- | --- |
| Disk Space | Disk space usage of the instance, including:<br>• Overall usage of the disk space<br>• Data space usage<br>• Log space usage<br>• Temporary file space usage<br>• System file space usage<br>Unit: MB |
| IOPS | Number of I/O request times of an instance per second. Unit: time/second |
| Connections | Total number of current connections, including the number of active connections and total connections |
| CPU usage | CPU usage (including CPU used by OS) of an instance |
| Network traffic | Incoming/outgoing traffic of an instance per second. Unit: KB |
| TPS | Number of transactions processed per second |
| QPS | Number of SQL statements executed per second |
| Cache hit rate | Read hit rate of the buffer pool |
| Average full table scans per second | Average number of full table scan times per second |
| SQL compilations per second | Number of compiled SQL statements per second |
| Page writes of the checking point per second | Number of page write times of the checking point in an instance per second |
| Logons per second | Number of logons per second |
| Lock timeouts per second | Number of lock expiration times per second |
| Deadlocks per second | Number of deadlocks in an instance per second |
| Lock waits per second | Number of lock waiting times per second |

**RDS for PostgreSQL**

| Monitoring item | Description |
| --- | --- |
| Disk Space | Usage of the instance disk space. Unit: MB |
| IOPS | Number of I/O request times of the data disk and log disk in an instance per second. Unit: time/second |

**RDS for PPAS**

| Monitoring item | Description |
| --- | --- |
| Disk Space | Usage of the instance disk space. Unit: MB |
| IOPS | Number of I/O request times of the data disk and log disk in an instance per second. Unit: time/second |

## 3.2 Set monitoring rules

RDS offers the instance monitoring function, and sends messages to you after detecting an exception in an instance. In addition, when the instance is locked due to the insufficient disk space , the system sends a message to you.

### Background information

Alibaba CloudMonitor offers monitoring and alarming. CloudMonitor helps you set alarm rules for metrics. You must add alarm contacts while set a contact group. The alarm contacts and the contact group are notified immediately when an alarm is triggered in the event of exceptions. You can create an alarm contact group using a related metric.

### 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. Click **Monitoring and Alarms** in the left-side navigation pane.
5. Click the **Alarms** tab.
6. Click **Set Alarm Rules** to open the CloudMonitor console.

   **Note:**
   You can click **Refresh** to manually refresh the current status of the alarm metric.
7. Select **Alarms** > **> Alarm Contacts** in the left-side navigation pane to open the **Alarm Contact Management** page.

   **Note:**
   When alarm rules are set for the first time, if the alarm notification object is not a contact of the Alibaba Cloud account of RDS, the alarm contact and alarm contact group must be created first. If you have already set the alarm contact and the alarm contact group, go to Step 10.

8. Click **Create Alarm Contact**.
9. Enter the alarm contact information in the **Set Alarm Contact** dialog box, click **Send verification code**, enter the verification code sent to your mailbox, and click **Save**.

> **Note:**
>
> - We recommend that you perform the next step to create the alarm contact group after you add all alarm notification objects.
> - Click **Edit** to modify a contact, or click **Delete** to delete a contact.

10. On the **Alarm Contact Management** page, click the **Alarm Contact Group** tab.
11. Click **Create Alarm Contact Group**.
12. Fill in **`Group Name`** and **`Description`**, select a contact from **Existing Contacts**, click  to add the contact to **`Selected Contacts`**, and click **OK**.

> **Note:**
>
> On the **Alarm Contact Group** page, you can click  to modify a contact group, click **X** to delete a contact group, or click **Delete** to delete a contact in the contact group.

13. After creating the alarm contact group, choose **Cloud Service Monitoring** > **ApsaraDB for RDS** from the left-side navigation pane.
14. Select the region of RDS for which the alarm rule is to be set.
15. Find the target instance and click **Alarm Rules** in the **Actions** column.

    The system displays the metrics of the current alarm.
16. Click **Create Alarm Rule** to add new alarm rules.

> **Note:**
>
> You can click **Modify**, **Disable**, or **Delete** for the metrics as needed.

# 4 Log management

All instance versions except MySQL 5.7 support log management. You can use the RDS console or SQL statements to query error logs and slow SQL log details for fault analysis. However, you can manage logs of instances in SQL Server 2012 and later versions only through SQL statements. This document describes how to manage logs through the RDS console and SQL statements.

### Use the RDS console to manage logs

You can use the RDS console to manage logs of MySQL 5.5/5.6, SQL Server 2008 R2, PostgreSQL, and PPAS instances. The actual interface may vary with engine types and versions.

### 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 enter the **Basic Information** page.
4. Click **Log Management** in the left-side navigation pane.
5. On the **Log Management** page, select **Error Log**, **Slow SQL Log Details**, **Slow SQL Log Summary**, or **Switch Logs**, select a time range, and click **Query**.

| Query item | Content |
| --- | --- |
| Error Log | Records the SQL statements that are failed to be executed in the past month. |
| Slow SQL Log Details | • Records the SQL statements that lasted for over one second (You can modify this time threshold by modifying the **long_query_time** parameter in **Parameters**) in the past month. Similar SQL statements are displayed once only.<br>• The list does not include slow SQL logs of the past two hours. To query these logs, check the **slow_log_view** table in the MySQL database. |
| Slow SQL Log Summary | Provides statistics and analysis reports for SQL statements that lasted for over one second (You can modify this time threshold by modifying the **long_query_time** parameter in **Parameters**) in the past month. |

**Use SQL statements to manage logs**

Instances in SQL Server 2012 and later versions read error logs only through the `sp_rds_read_error_logs` storage procedure. The method of using it is similar to that of using `sp_readerrorlog`.

Example 1:

```
EXEC sp_rds_read_error_logs
```

Example 2:

```
EXEC sp_rds_read_error_logs 0,1 ,'error'
```

# 5 Create a linked server for SQL Server instances

This document is applicable only to high-availability instances of RDS for SQL Server 2012 and later versions.

Currently, linked server creation has the following constraints:

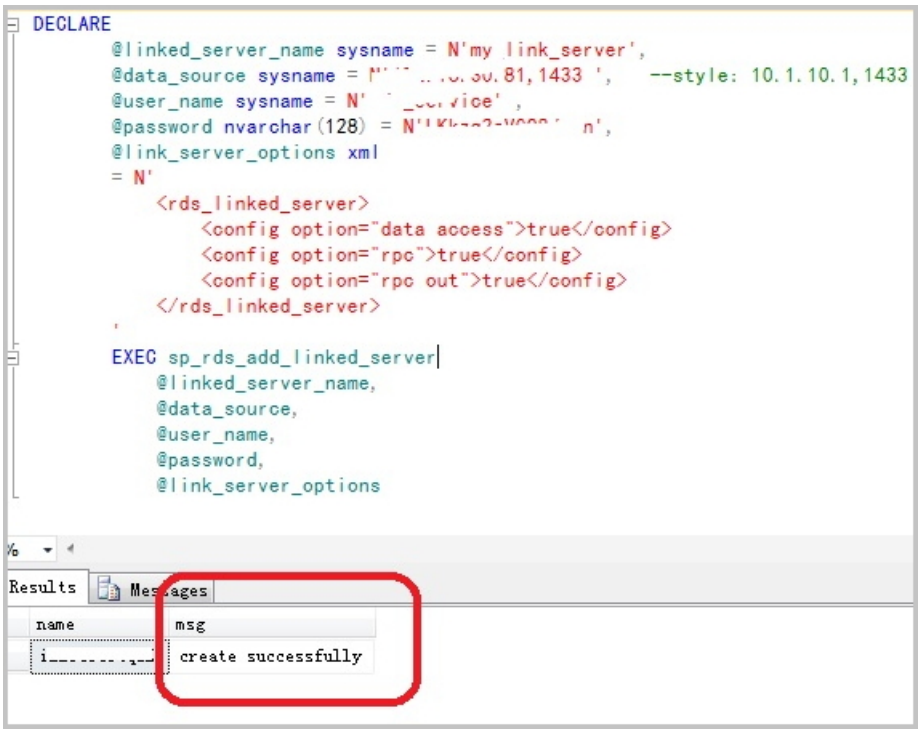
- You cannot create a linked server on the RDS console.
- Creating a linked server with a series of storage procedures is complex.
- You cannot create a linked server using DNS and the corresponding IP address.

Despite the constraints, this document provides a simple method of creating a linked server.

```
DECLARE
        @linked_server_name sysname = N'my_link_server',
        @data_source sysname = N'***********', --style: 10.1.10.1,1433
        @user_name sysname = N'****' ,
        @password nvarchar(128) = N'**********',
        @link_server_options xml
        = N'
            <rds_linked_server>
                <config option="data access">true</config>
                <config option="rpc">true</config>
                <config option="rpc out">true</config>
            </rds_linked_server>

        EXEC sp_rds_add_linked_server
            @linked_server_name,
            @data_source,
            @user_name,
            @password,
            @link_server_options
```

The following message `create successfully` is displayed after the linked server is successfully created.




Click the **Messages** tab shown in the preceding figure, and the following information is displayed.

```
The linked server 'my_link_server' has set option 'data access' to '
true'.
The linked server 'my_link_server' has set option 'rpc’ to 'true'.
The linked server 'my_link_server' has set option 'rpc out' to 'true'.
create link server 'my_link_server' successfully.
```

# 6 Preface

### Overview

ApsaraDB for Relational Database Service (RDS) is a stable and reliable online database service with auto-scaling capabilities. Based on Apsara distributed file system and high-performance SDD storage, RDS supports MySQL, SQL Server, PostgreSQL, and PPAS engines, and provides a complete set of solutions for disaster recovery, backup, recovery, monitoring, migration, and others. This helps you operate and manage your own database. For benefits of RDS, see *Benefits*.

This document describes RDS features and functions and further explains the procedure to configure RDS through the *RDS console* . You can also manage RDS through APIs and SDKs.

If you need technical assistance, you can open the *RDS console* and choose **Support** > **Open a new ticket** or *click here* to submit a ticket.

For more information about functions and pricing of RDS, log on to *official website of ApsaraDB for RDS*.

### Declaration

Some features or services described in this document may be unavailable for certain regions. See the relevant commercial contracts for specific terms and conditions.

This document serves as a user guide. No content in this document can constitute any express or implied warranty.

The content of this document is updated based on product upgrade and many other factors. You must first verify the document with your latest software version.

### Consideration

RDS supports multiple types of databases. This document takes MySQL as an example to describe the features and usage of RDS. Some types of databases may not support certain features. The actual interface may vary slightly.

### General terms

- Instance: A database service process that takes up physical memory independently. You can set different memory size, disk space, and database type, among which the memory specificat ion determines the performance of the instance. After the instance is created, you can change the configuration and delete the instance at any time.

- Database: A logical unit created in an instance. Multiple databases can be created in an instance, and the database name is unique within the instance.
- Region and zone: A region is a physical data center. A zone is a physical area that has independent power supply and networks within a region. For more information, see *Alibaba Cloud Global Infrastructure*.

**Common conventions**

| Term | Description |
| --- | --- |
| Local database/Source database | Refers to the database deployed in the local equipment room or the database not on the ApsaraDB. In most cases, it refers to the source database to be migrated to the ApsaraDB in this document. |
| RDS for XX (MySQL, SQL Server, PostgreSQL, PPAS) | It indicates the RDS of a specific database type, for example, RDS for MySQL means the instance enabled on the RDS with a database type of MySQL. |

# 7 Typical applications

## 7.1 Cached data persistence

RDS can be used together with ApsaraDB for Memcache and ApsaraDB for Redis to form storage solutions with high throughput and low delay. This document describes the cached data persistence solution based on the combined use of RDS and ApsaraDB for Memcache.

**Background information**

Compared with RDS, ApsaraDB for Memcache and the ApsaraDB for Redis have the following two features:

- High response speed: The request delay of the ApsaraDB for Memcache and the ApsaraDB for Redis is usually within several milliseconds.
- The cache area can support a higher Requests Per Second (QPS) than the RDS.

**System requirements**

- bmemcached (with support of SASL extension) has been installed in the local environment or ECS.

  bmemcached download address: Click *Here* to download.

  The bmemcached installation command is as follows:

  ```
  pip install python-binary-memcached
  ```

- Python is used as an example. Python and pip must be installed in the local environment or ECS.

**Sample code**

The following sample code realizes the combined use of RDS and ApsaraDB for Memcache:

```
/usr/bin/env python
import bmemcached
Memcache_client = bmemcached.Client((‘ip:port’), ‘user’, ‘passwd’)
#Search for a value in ApsaraDB for Memcache
res = os.client.get(‘test’)
if res is not None:
    return res #Return the searched value
else:
    #Query RDS if the value is not found
    res = mysql_client.fetchone(sql)
     Memcache_client.put(‘test’, res) #Write cached data to ApsaraDB
for Memcache
```

```
    return res
```

## 7.2 Multi-structure data storage

OSS is a cloud storage service provided by Alibaba Cloud, featuring massive capacity, security , low cost, and high reliability. RDS can work with OSS to form multiple types of data storage solutions.

For example, when the business application is a forum and RDS works with OSS, resources such as registered users' images and post content images can be stored in OSS to reduce the storage pressure of RDS.

**Sample code**

OSS works with the RDS.

1. Initialize OssAPI.

```
from oss.oss_api import *
endpoint=”oss-cn-hangzhou.aliyuncs.com”
accessKeyId, accessKeySecret=”your id”,”your secret”
oss = OssAPI(endpoint, accessKeyId, accessKeySecret)
```

2. Create a bucket.

```
#Set the bucket to private-read-write
res = oss.create_bucket(bucket,"private")
print "%s\n%s" % (res.status, res.read())
```

3. Upload an object.

```
res = oss.put_object_from_file(bucket, object, "test.txt")
print "%s\n%s" % (res.status, res.getheaders())
```

4. Obtain the corresponding object.

```
res = oss.get_object_to_file(bucket, object, "/filepath/test.txt")
print "%s\n%s" % (res.status, res.getheaders())
```

In the ECS application code, RDS stores the ID of each user, and OSS stores the avatar resource of the user. The Python code is as follows:

```
/usr/bin/env python
from oss.oss_api import *
endpoint=”oss-cn-hangzhou.aliyuncs.com”
accessKeyId, accessKeySecret=”your id”,”your secret”
oss = OssAPI(endpoint, accessKeyId, accessKeySecret)
User_id = mysql_client.fetch_one (SQL) # Search for user_id in RDS
#Obtain and download the user avatar to the corresponding path
oss.get_object_to_file(bucket, object, your_path/user_id+’.png’)
#Process the uploaded user avatar
```

```
oss.put_object_from_file(bucket, object, your_path/user_id+’.png’)
```

# 8 Quick start

If you use RDS for the first time, see the following *Cite LeftQuick StartCite Right* documents to get started with RDS.

- *Quick Start for MySQL*
- *Quick Start for SQL Server*
- *Quick Start for PostgreSQL*
- *Quick Start for PPAS*

If you have questions beyond *Cite LeftQuick StartCite Right*, see *Cite LeftUser GuideCite Right*.

**Database engines**

**ApsaraDB for MySQL**

MySQL is the world's most popular open source database. As an important part of LAMP and a combination of open source software (Linux + Apache + MySQL + Perl/PHP/Python), MySQL is widely used in a variety of applications.

In the Web 2.0 era, MySQL serves as the basis of the underlying architecture of the popular BBS software system Discuz! and blogging platform WordPress. In the Web 3.0 era, leading Internet companies including Alibaba, Facebook, and Google have built their large-scale mature database clusters by taking advantage of the advanced flexibility of MySQL.

Based on Alibaba's MySQL source code branch, ApsaraDB for MySQL proves to have excellent performance and throughput. It withstands the massive data traffic and a large number of concurrent users during many November 11 (Singles' Day) shopping festivals - the Chinese equivalent of Cyber Monday. ApsaraDB for MySQL also offers a range of advanced functions including optimized read/write splitting, data compression, and intelligent optimization.

RDS for MySQL currently supports versions 5.5, 5.6, and 5.7.

**ApsaraDB for SQL Server**

SQL Server is one of the first commercial databases and is an important part of the Windows platform (IIS + .NET + SQL Server), with support for a wide range of enterprise applications. The SQL Server Management Studio software comes with a rich set of built-in graphical tools and script editors. You can quickly get started with a variety of database operations through visual interfaces.

Powered by a high-availability architecture and the capability to recover data at any point in time, ApsaraDB for SQL Server provides strong support for a variety of enterprise applications. It also covers Microsoft's licensing fee.

RDS for SQL Server currently supports the following versions:

- SQL Server 2008 R2 Enterprise
- SQL Server 2012 Web, Standard, and Enterprise
- SQL Server 2016 Web, Standard, and Enterprise

**ApsaraDB for PostgreSQL**

PostgreSQL is the world's most advanced open source database. As an academic relational database management system, it provides full compliance with SQL specifications and robust support for a diverse range of data formats (including JSON, IP, and geometric data, which are not supported by most commercial databases).

ApsaraDB for PostgreSQL supports a range of features including transactions, subqueries, Multi-Version Concurrency Control (MVCC), and data integrity verification. It also integrates a number of important functions, including high availability, backup, and recovery, to help mitigate your O&M burden.

RDS for PostgreSQL currently supports version 9.4.

**ApsaraDB for PPAS**

Postgres Plus Advanced Server (PPAS) is a stable, secure, and scalable enterprise-level relational database. Based on PostgreSQL, PPAS delivers enhanced performance, application solutions, and compatibility, and provides the capability to run Oracle applications directly. It is a reliable and cost-effective option for running a variety of enterprise applications.

ApsaraDB for PPAS incorporates a number of advanced functions including account management , resource monitoring, backup, recovery, and security control, and it continues to be updated and improved regularly.

RDS for PPAS currently supports version 9.3.

# 9 Billing management

## 9.1 Change the billing method

You can change a Pay-As-You-Go instance to a Subscription instance.

**Attention**

- Think twice before such a conversion, because a Subscription instance cannot be converted back to a Pay-As-You-Go instance.
- Within the contract period of a Subscription instance, you can only upgrade it but cannot downgrade or release it.
- After the conversion is successful, the Subscription billing method is immediately applied. For more information, see *Pricing*.
- An order is generated when you change a Pay-As-You-Go instance to a Subscription instance. The conversion takes effect only after you pay for the order. If you leave the order unpaid, the order is displayed on the *Orders* page and you cannot purchase new instances or change billing methods of instances.

> **Note:**
>
> - If you upgrade an instance when its billing method change order is unpaid, you cannot pay for the order any more because the order amount is insufficient. Invalidate the order and change the billing method again.
> - If you do not want to pay for an order, invalidate it on the *Orders* page.

**Prerequisites**

- You are the owner of the instance.
- The instance type is not a history instance type. For more information, see *Instance type overview*.

> **Note:**
> A Pay-As-You-Go instance of a history type cannot be converted to a Subscription instance. To change the billing method for a Pay-As-You-Go instance of a history type, change the instance type to a new type first. For operation details, see *Change configurations*.

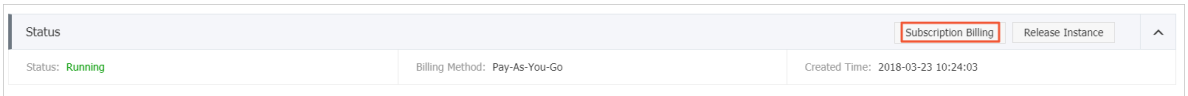
- The billing method of the instance is Pay-As-You-Go, and the instance status is Running.

> **Note:**
> After you submit the order, if the instance status changes (for example, to the **Locked** state), payment will fail. You can pay for the order only when the instance status restores to **Running** .

- There is no unfilled billing method change order (namely, new Subscription instance order) of an instance .

**Procedure**

1. Log on to the *RDS console*.
2. Select the region where the target instance is located.
3. Click the instance ID to enter the **Basic Information** page.
4. In the **Status** area, click **Subscription Billing**.




5. Select the subscription period.
6. Click **Pay Now** and pay for the order.

## 9.2 Manually renew a Subscription instance

A Subscription instance must be renewed within 15 days after expiration. Subscription instances are automatically released when the payment is overdue for 15 days. As a result, all data for the instance is deleted and cannot be recovered. For more information about renewal, see *Renewal*.

**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 go to the **Basic Information** page.
4. Click **Renew** in **Status** area, as shown in the following figure.


5. Select the renewal period on the **Renew** page.

> **Note:**
> You can change the configuration if needed.

6. Read and confirm the terms of service, then select **I agree to Product Terms of Service and Service Level Notice**.
7. Click **Pay** to complete the payment process.

**Related topic**

*Enable auto-renewal of the subscription instance*

# 9.3 Enable auto-renewal for a Subscription instance

Auto-renewal for a Subscription instance frees you from regular manual renewals. It also avoids service interruptions caused if the instance expires and is not renewed in time.

If you did not select auto-renewal when you purchased the Subscription instance, you can set it up on the Alibaba Cloud Billing Management console. When the setup is done, the subscription is automatically renewed based on the selected renewal cycle. For example, if you select a three-month renewal cycle, three months of subscription is automatically paid for each renewal. This document explains how to enable auto-renewal for your Subscription instance.

**Prerequisite**

You have logged on to Alibaba Cloud console with your master account.

**Attentions**

- The renewal cycle cannot be changed while enabling the auto-renewal function. For variable renewal cycles, renew the instance manually. For more information about how to handle manual renewal, see *Manually renew a Subscription instance*.
- If you select auto-renewal, you are charged three days before the instance expires. Credit cards and coupons are supported for each renewal payment.
- If you manually renew your instance before the charging date, auto-renewal takes place based on the new expiration date.
- The auto-renewal function takes effect the next day after it is enabled. If your instance expires on the next day, manually renew it to prevent service interruptions.

**Procedure**

1. Log on to the *Billing Management* console of Alibaba Cloud.
2. In the left-side navigation pane, select **Renewal**.
3. Select **ApsaraDB for RDS** in the **Product** drop-down list, and select the region where the target instance is located and its creation date. Alternatively, select the default search range.

4. Click **Search**.


5. In the **Auto-renewal** column for the target instance, move the slider to the right.
6. On the open automatic page, set automatic renewal hours.
7. Click **Open automatic**.