

# 阿里云 云数据库RDS 快速入门MySQL版

文档版本：20180907

# 法律声明

---

阿里云提醒您 在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

## 通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 <b>禁止：</b> 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 <b>警告：</b> 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 <b>说明：</b> 您也可以通过按 <b>Ctrl + A</b> 选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
<b>粗体</b>	表示按键、菜单、页面名称等UI元素。	单击 <b>确定</b> 。
<code>courier</code> 字体	命令。	执行 <code>cd /d C:/windows</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
[ ]或者[a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ }或者{a b}	表示必选项，至多选择一个。	<code>swich {stand   slave}</code>

# 目录

---

法律声明.....	I
通用约定.....	I
<b>1 Limits.....</b>	<b>1</b>
<b>2 General process to use RDS.....</b>	<b>3</b>
<b>3 Create an instance.....</b>	<b>4</b>
<b>4 Initial configuration.....</b>	<b>6</b>
4.1 Set the whitelist.....	6
4.2 建立帳號和資料庫.....	9
4.3 Apply for an Internet IP address.....	13
<b>5 Connect to an instance.....</b>	<b>18</b>
<b>6 Scale instances.....</b>	<b>22</b>
6.1 Read-only instance.....	22
6.1.1 Introduction to read-only instances.....	22
6.1.2 Create a read-only instance.....	24
6.2 Disaster recovery instances.....	26
<b>7 隱藏目錄.....</b>	<b>30</b>
7.1 Create databases and accounts.....	30
7.1.1 Create accounts and databases for MySQL 5.7 High-availability Edition/5.5/5.6 instances.....	30
7.1.2 Create accounts and databases for MySQL 5.7 Basic Edition.....	33
7.1.3 Create a master account.....	35
7.2 Manage read-only instances.....	40

# 1 Limits

To guarantee the stability and security of ApsaraDB for MySQL, certain limits are propose.

Items	Restrictions
Parameter modification	The <a href="#">RDS console</a> or APIs must be used to modify database parameters. But some parameters cannot be modified. For more information, see <a href="#">Set parameters through the RDS console</a> .
Root permission	The root or sa permission is not provided.
Backup	<ul style="list-style-type: none"><li>Command lines or graphical interfaces can be used for logical backup.</li><li>For physical backup, the <a href="#">RDS console</a> or APIs must be used.</li></ul>
Restoration	<ul style="list-style-type: none"><li>Command lines or graphical interfaces can be used for logical restoration.</li><li>For physical restoration, the <a href="#">RDS console</a> or APIs must be used.</li></ul>
Migration	<ul style="list-style-type: none"><li>Command lines or graphical interfaces can be used for logical import.</li><li>You can use the MySQL command line tool or Data Transmission Service (DTS) to migrate data.</li></ul>
MySQL storage engine	<ul style="list-style-type: none"><li>Currently only InnoDB and TokuDB are supported. The MyISAM engine has defects and may cause data loss. If you create MyISAM engine tables, they are automatically converted to InnoDB engine tables. For more information, see <a href="#">Why does RDS for MySQL not support the MyISAM engine?</a></li><li>The InnoDB storage engine is recommended for performance and security requirements.</li><li>The Memory engine is not supported. If you create Memory engine tables, they are automatically converted to InnoDB engine tables.</li></ul>
Replication	MySQL provides a dual-node cluster based on the master/slave replication architecture, so you manual deployment is not required. The slave instance in the architecture is invisible to you, and your application cannot access to the slave instance directly.
Restarting RDS instances	Instances must be restarted through the <a href="#">RDS console</a> or APIs.
User, password, and database management	By default, is used to manage users, passwords, and databases, including operations such as instance creation, instance deletion, permission modification, and password modification. MySQL also allows you to create a master account for finer-grained management.
Common account	<ul style="list-style-type: none"><li>Does not support customized authorization.</li></ul>

Items	Restrictions
	<ul style="list-style-type: none"><li>• The account management and database management interfaces are provided on the RDS console.</li><li>• Instances that support common accounts also support master accounts.</li></ul>
Master account	<ul style="list-style-type: none"><li>• Support customized authorization.</li><li>• SQL statements can be used for management.</li></ul>
Network settings	If a MySQL 5.5/5.6 instance is in a classic network and its <i>access mode</i> is safe connection mode, do not enable net.ipv4.tcp_timestamps in SNAT mode.

## 2 General process to use RDS

### Purpose of the Quick Start

This document describes the procedure right from purchasing an RDS instance to using it. This document also elaborates on how to create an ApsaraDB for RDS instance, perform basic settings, and connect to the instance database.

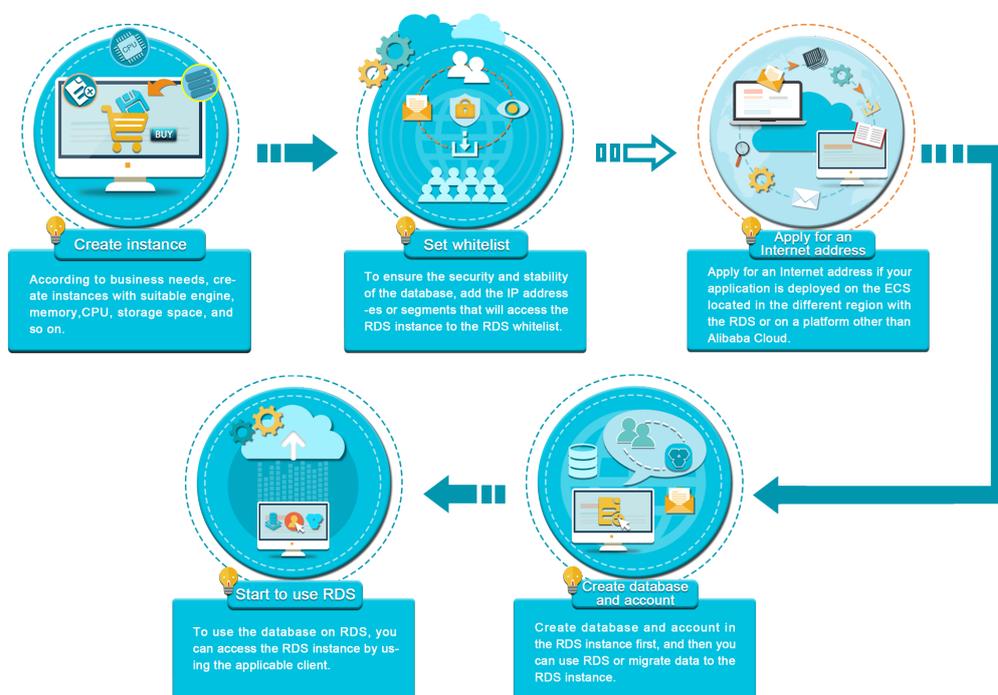
### Target reader

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

### Quick Start flowchart

If you use Alibaba Cloud ApsaraDB for RDS for the first time, see [Limits](#) and [Instance management interface for MySQL](#).

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



## 3 Create an instance

---

You can use the RDS console or APIs to create an RDS instance. For more information about instance pricing, see . This document describes how to use the RDS console to create an instance. For more information about how to use APIs to create an instance, see [CreateDBInstance](#).

### Prerequisites

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

### Procedure

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

For more information about regions and zones, see [Regions and zones](#).



#### Note:

Products in different regions cannot intercommunicate through the intranet, and you cannot change the instance region after creating an instance. Therefore, special attention is required when you select the region.

- Database engine: RDS supports MySQL, SQL Server, PostgreSQL, and PPAS. Different database types are supported in different regions. Choose the database type according to the instructions on the RDS console.
- Version: indicates the database version. Currently, RDS supports MySQL 5.5/5.6/5.7, SQL Server 2008 R2/2012, PostgreSQL 9.4, and PPAS 9.3. Different database versions

are supported in different regions. Choose the database version according to the instructions on the RDS console.

For the MySQL database, we recommend that you use MySQL 5.6 because it supports the TokuDB storage engine, which can save the storage cost by greatly reducing the space occupied by data files.

- **Series:** RDS instances support the Basic Edition, High-availability Edition, and Finance Edition. Different database versions support different series. Choose the instance series according to the instructions on the RDS console.
- **Network type:** RDS supports the classic network and virtual private cloud (VPC). A VPC needs to be created beforehand. Alternatively, you can change the network type after creating an instance. For more information, see [Set network type](#).
- **Specifications:** indicate the CPU and memory occupied by the instance, the number of connections, and the maximum IOPS. For more information about instance specifications, see [Instance type list](#).
- **Storage:** indicates space used by data, system files, binlog files, and transaction files.
- **Subscription time:** indicates the duration of a Subscription instance.
- **Quantity:** indicates the number of instances with the same configurations to be purchased.

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



**Note:**

To buy multiple instances with different configurations, click **Add To List** for each instance type and click **Batch Purchase**.

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

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

## 4 Initial configuration

---

### 4.1 Set the whitelist

To ensure database security and stability, before you start using an RDS instance, you must whitelist the IP addresses or IP address segments that need to access the database. We recommend that you periodically check and adjust your whitelist according to your requirements to maintain RDS security. This document provides information about and the procedure of setting a whitelist.

#### Background information

You can access the RDS instance through the intranet, the Internet, or both the intranet and Internet. For more information about the applicable scenarios of each connection type (intranet and Internet), see Background information of [Set intranet and Internet addresses](#).

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



#### Note:

If you cannot connect to the RDS instance after adding the application service IP address to the whitelist, refer to [How to locate the local IP address using ApsaraDB for MySQL](#) to obtain the actual IP address of the application service.

#### Attentions

- The system automatically creates a **default** whitelist group for each newly created RDS instance. This default whitelist group can only be modified or cleared, but cannot be deleted.
- For each newly created RDS instance, the local loopback IP address 127.0.0.1 is added to the **default** whitelist group by default. This means that all the IP addresses or IP address segments are prohibited to access this RDS instance. Therefore, you must delete 127.0.0.1 from the default whitelist group before you add other IP addresses or IP address segments to the whitelist.
- % 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.

## Procedure

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



### Note:

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



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



### Note:

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

**Group Name:** default

**Whitelist:** 127.0.0.1

[Upload ECS Intranet IP Address](#) You can add 999 whitelists more

Specified IP address: Add an IP address to allow this IP to access RDS.  
Specified IP segment: Add an IP segment to allow all the IP addresses in this segment to access RDS.  
When you add multiple IP addresses, separate them by a comma (no space after the comma), such as "192.168.0.1,192.168.0.1/24".  
[How to locate the local IP address](#)

White list will be effect after 1 minute

Parameters description:

- **Group Name:** It can contain 2 to 32 characters including lowercase letters, digits, or underscores (\_). The group name must start with a lowercase letter and end with a letter or digit. This name cannot be modified once the whitelist group is successfully created.
- **Whitelist:** Enter the 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, it indicates that any IP address in the format of 10.10.10.X can access the RDS instance.
  - If you want to enter multiple IP addresses or IP 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 address of the ECS instance under the same account as the RDS instance. This is a quick method to add ECS intranet IP address.
7. Click **OK**.

### Modify or delete the whitelist group

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

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

## 4.2 建立帳號和資料庫

本文介紹如何為RDS for MySQL執行個體建立帳號和資料庫。

### 檢查執行個體的帳號管理機制

部分RDS for MySQL執行個體的帳號管理機制已升級。使用本文前，請先檢查您的執行個體是否已升級，檢查方式如下：

1. 登入[RDS控制台](#)。
2. 選擇目標執行個體所在地域。
3. 單擊目標執行個體的ID，進入基本資料頁面。
4. 在左側導覽列中選擇帳號管理。
  - 如果只顯示一個建立帳號按鈕，表示已升級。具體請參見本文。
  - 如果顯示建立高許可權帳號或建立初始帳號按鈕，或不顯示任何建立帳號的按鈕，表示未升級。

- MySQL 5.7基礎版：請參見[建立資料庫和帳號](#)
- MySQL 5.7高可用版/MySQL 5.5/MySQL 5.6：請參見[建立高許可權帳號](#)以及[建立資料庫和帳號](#)。

### 帳號管理機制升級說明

- 執行個體升級前，如果不建立高許可權帳號，那麼只能用普通帳號，許可權有限。如果建立高許可權帳號，那麼該執行個體的資料庫管理頁面將消失，以及帳號管理頁面上建立帳號的按鈕也會消失。之後需要登入資料庫，使用SQL語句進行帳號管理和資料庫管理。
- 執行個體升級後，您可以按需建立高許可權帳號，而控制台始終提供資料庫管理頁面和建立帳號按鈕，您可以在控制台管理所有帳號和資料庫。
- 阿里雲將在9月底之前完成所有RDS for MySQL執行個體的帳號管理機制升級。

### 帳號類型

RDS for MySQL執行個體支援兩種資料庫帳號：高許可權帳號和普通帳號。

帳號類型	說明
高許可權帳號	<ul style="list-style-type: none"> <li>• 只能在控制台建立和管理。</li> <li>• 一個執行個體中只能建立一個高許可權帳號，用於管理普通帳號和資料庫。</li> <li>• 開放了更多許可權，可滿足個人化和精細化的許可權管理需求，比如可按使用者指派不同表的查詢許可權。</li> <li>• 擁有執行個體下所有資料庫的所有許可權。</li> <li>• 可以斷開任意帳號的串連。</li> </ul>
普通帳號	<ul style="list-style-type: none"> <li>• 可以通過控制台或者 SQL語句建立和管理。</li> <li>• 一個執行個體可以建立多個普通帳號，具體的數量與執行個體核心有關。</li> <li>• 只能斷開自己的串連。</li> </ul>

### 建立高許可權帳號

1. 登入[RDS控制台](#)。
2. 選擇目標執行個體所在地域。
3. 單擊目標執行個體的ID，進入基本資料頁面。
4. 在左側導覽列中選擇帳號管理。
5. 單擊建立帳號。

## 6. 設定以下參數：

參數	說明
資料庫帳號	填寫帳號名稱。要求如下： <ul style="list-style-type: none"> <li>以字母開頭，以字母或數字結尾；</li> <li>由小寫字母、數字或底線組成；</li> <li>長度為2~16個字元。</li> </ul> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  说明：              如果建立的高許可權帳號的帳號名與已有的普通帳號的帳號名相同，則原來的普通帳號會被替換為該高許可權帳號。           </div>
帳號類型	此處選擇高許可權帳號。
密碼	設定帳號密碼。要求如下： <ul style="list-style-type: none"> <li>由大寫字母、小寫字母、數字、特殊字元中的任意三種組成；</li> </ul> 特殊字元為!@#%\$^&*()_+ -= ; <ul style="list-style-type: none"> <li>長度為8~32個字元。</li> </ul>
確認密碼	再次輸入密碼。
備忘說明	備忘該帳號的相關資訊，便於後續帳號管理。最多支援256個字元。

## 7. 單擊確定。

## 建立普通帳號

1. 登入[RDS控制台](#)。
2. 選擇目標執行個體所在地域。
3. 單擊目標執行個體的ID，進入基本資料頁面。
4. 在左側導覽列中選擇帳號管理。
5. 單擊建立帳號。
6. 設定以下參數：

參數	說明
資料庫帳號	填寫帳號名稱。要求如下： <ul style="list-style-type: none"> <li>以字母開頭，以字母或數字結尾；</li> </ul>

參數	說明
	<ul style="list-style-type: none"> <li>由小寫字母、數字或底線組成；</li> <li>長度為2~16個字元。</li> </ul>
帳號類型	此處選擇普通帳號。
授權資料庫	<p>為該帳號授予一個或多個資料庫的許可權。本參數可以留空，在建立帳號後再給帳號授權。</p> <ol style="list-style-type: none"> <li>從左側選中一個或多個資料庫，單擊授權添加到右側。</li> <li>在右側框中，為某個資料庫選擇讀寫、只讀、僅DDL或僅DML。</li> </ol> <p>如果要為多個資料庫批量設定相同的許可權，則單擊右側框裡右上方的按鈕，如全部設讀寫。</p> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> <p> 说明：</p> <p>右上方的按鈕會隨著點擊而變化。例如，單擊全部設讀寫後，該按鈕會變成全部設只讀。</p> </div>
密碼	<p>設定帳號密碼。要求如下：</p> <ul style="list-style-type: none"> <li>由大寫字母、小寫字母、數字、特殊字元中的任意三種組成；</li> </ul> <p>特殊字元為!@#%\$^&amp;*()_+ -= ；</p> <ul style="list-style-type: none"> <li>長度為8~32個字元。</li> </ul>
確認密碼	再次輸入密碼。
備忘說明	非必填。備忘該帳號的相關資訊，便於後續帳號管理。最多支援256個字元。

#### 7. 單擊確定。

### 建立資料庫

1. 登入[RDS控制台](#)。
2. 選擇目標執行個體所在地域。
3. 單擊目標執行個體的ID，進入基本資料頁面。
4. 在左側導覽列中選擇資料庫管理。
5. 單擊建立資料庫。
6. 設定以下參數。

參數	說明
資料庫 ( DB ) 名稱	<ul style="list-style-type: none"> <li>以字母開頭，以字母或數字結尾；</li> <li>由小寫字母、數字、底線或中劃線組成；</li> <li>長度為2~64個字元。</li> </ul>
支援字元集	選擇utf8、gbk、latin1或utf8mb4。 如果需要其他字元集，請選擇全部，然後從列表中選擇需要的字元集。
授權帳號	選中需要訪問本資料庫的帳號。本參數可以留空，在建立資料庫後再綁定帳號。  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px;">  <b>说明：</b>              此處只會顯示普通帳號，因為高許可權帳號擁有所有資料庫的所有許可權，不需要授權。           </div>
帳號類型	選擇要授予帳號的許可權：讀寫、只讀、僅DDL或僅DML。
備忘說明	非必填。用於備忘該資料庫的相關資訊，便於後續資料庫管理，最多支援256個字元。

7. 單擊確定。

### 4.3 Apply for an Internet IP address

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



#### Note:

Instances in the same region (can be in different zones) can access each other through the intranet.

#### Background information

RDS supports connections through the intranet and Internet. The *series*, version, and *access mode* of the instance determine available connection types.

Series	Version	Access mode	Connection address
Basic Edition	<ul style="list-style-type: none"> <li>MySQL 5.7</li> <li>SQL Server 2012</li> </ul>	Standard mode	<ul style="list-style-type: none"> <li>Intranet IP address</li> <li>Internet IP address</li> <li>Both intranet and Internet IP addresses</li> </ul>
High-availability Edition	<ul style="list-style-type: none"> <li>MySQL 5.5/5.6</li> <li>SQL Server 2008 R2</li> <li>PostgreSQL 9.4</li> <li>PPAS 9.3</li> </ul>	Standard mode	<ul style="list-style-type: none"> <li>Intranet IP address</li> <li>Internet IP address</li> </ul>
		Safe connection mode	<ul style="list-style-type: none"> <li>Intranet IP address</li> <li>Internet IP address</li> <li>Both intranet and Internet IP addresses</li> </ul>

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 an 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 an ECS instance that is located in a region different from that of your RDS instance.
  - This scenario is applicable when your application is deployed on a platform other than Alibaba Cloud.
- Use both the intranet and Internet IP addresses:
  - This scenario is applicable when your application is deployed on both: (1) An ECS instance that is in the same region and has the same *network type* as your RDS instance; (2) An ECS instance that is in a region different from your RDS instance.
  - This scenario is applicable when your application is deployed on both: (1) An ECS instance that is in the same region and has the same *network type* as your RDS instance; (2) A platform other than Alibaba Cloud.

## Attentions

- Before accessing an RDS instance, add IP addresses or IP address segments to the whitelist. Otherwise, they cannot access the RDS instance. For more information, see [Set a 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.

## Procedure

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



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

### Modify Connection Address

Connection Type:

Connection Address:  .mysql.rds

The address can have 8 to 64 characters and must begin with a lower-case letter.

Port:

Port Range: 3200 to 3999

Parameter description:

- **Connection Type:** Select **intranet address** or **Internet address** according to the connection type to be modified.
- **Connection Address:** The address format is `xxx.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].

**8. Click OK.**

## 5 Connect to an instance

---

If you want to use cloud database RDS, you can manage DMS (Data Management) through the client or Ali cloud data. Service) connects an RDS instance. This chapter describes how to connect an RDS instance with a DMS and a MySQL-front client.

### Background information

You can log in to the DMS first through the RDS Management Console, reconnect to the RDS instance that needs to be accessed. ( DMS offers an integrated solution for data management, structure management, access security, BI charts, data trends, data tracking, performance and optimization, and server management. Support for MySQL, SQL Server, PostgreSQL, MongoDB, redis, and other relational databases, as well as the database management of neosql, linux server administration is also supported.

You can also use the client to connect to an RDS instance. RDS for MySQL is fully compatible with MySQL, so you can connect to RDS in the way you connect to an on-premise MySQL server . This document introduces the connection procedure by taking the MySQL-Front client as an example. When connecting an RDS instance with a client, be aware to select the inside and out network address:

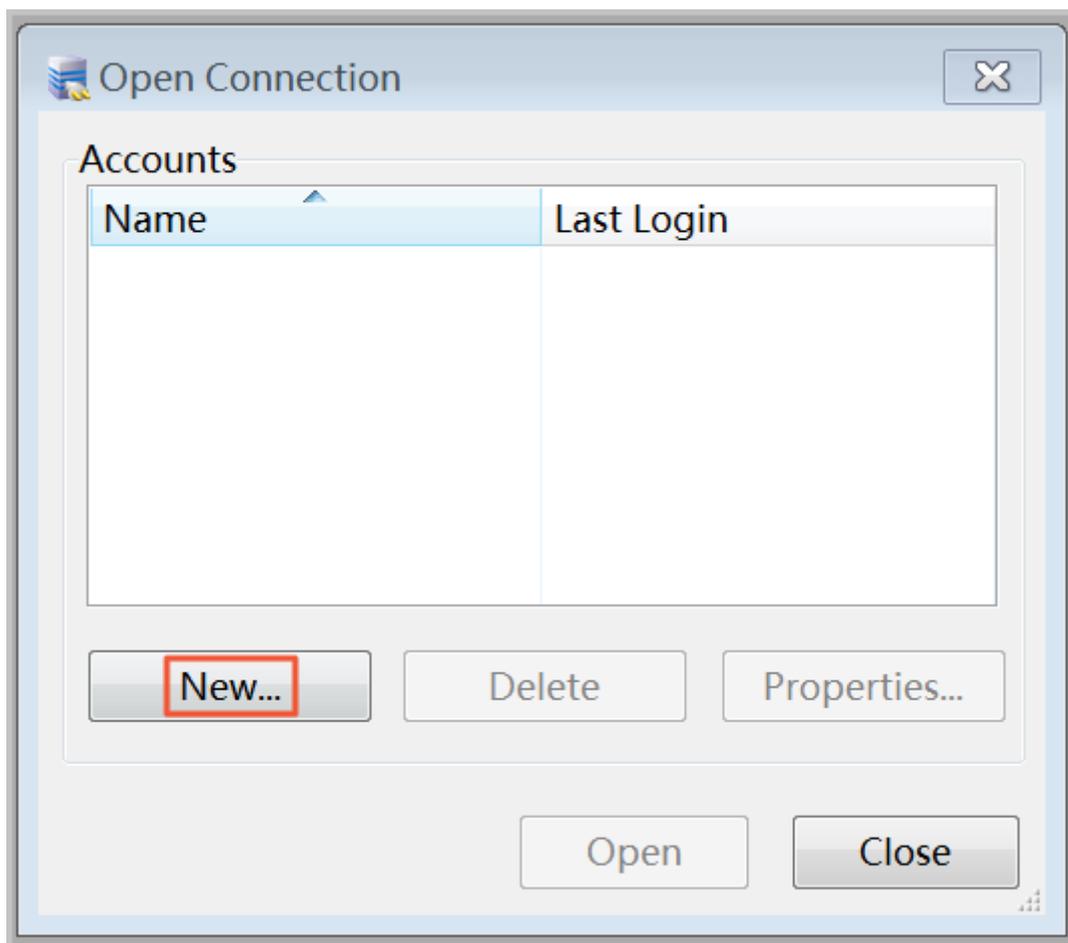
- If your client is deployed on an ECS instance that is in the same region and has the same network type as your RDS instance, use the intranet IP address.
- In other cases, use the Internet IP address.

### Connecting to an RDS instance using DMS

For methods about how to connect an RDS instance with a DMS, see.

### Log on with a client

1. In the RDS whitelist, add the IP address of the computer that runs the client. For information about how to set the whitelist, see [Set a whitelist](#).
2. Start the MySQL-Front client.
3. In the **Open Connection** window, click **New**, as shown in the following figure.



4. Enter the RDS connection information.

The image shows a screenshot of a software dialog box titled "Add Account". The dialog is organized into three main sections:

- Description:** Contains a text input field labeled "Description Name:". This field is highlighted with a red rectangular box.
- Connection:** Contains three controls:
  - A text input field labeled "Host:" highlighted with a red rectangular box.
  - A spin box labeled "Port:" with the value "3306" displayed, also highlighted with a red rectangular box.
  - A dropdown menu labeled "Connection Type:" currently showing "Built-in".
- Login Information:** Contains three text input fields:
  - A field labeled "User:" highlighted with a red rectangular box.
  - A field labeled "Password:" highlighted with a red rectangular box.
  - A field labeled "Database:" with a small "..." button to its right.

At the bottom of the dialog, there are three buttons: "Help", "Ok", and "Cancel". The "Ok" button is highlighted with a blue border.

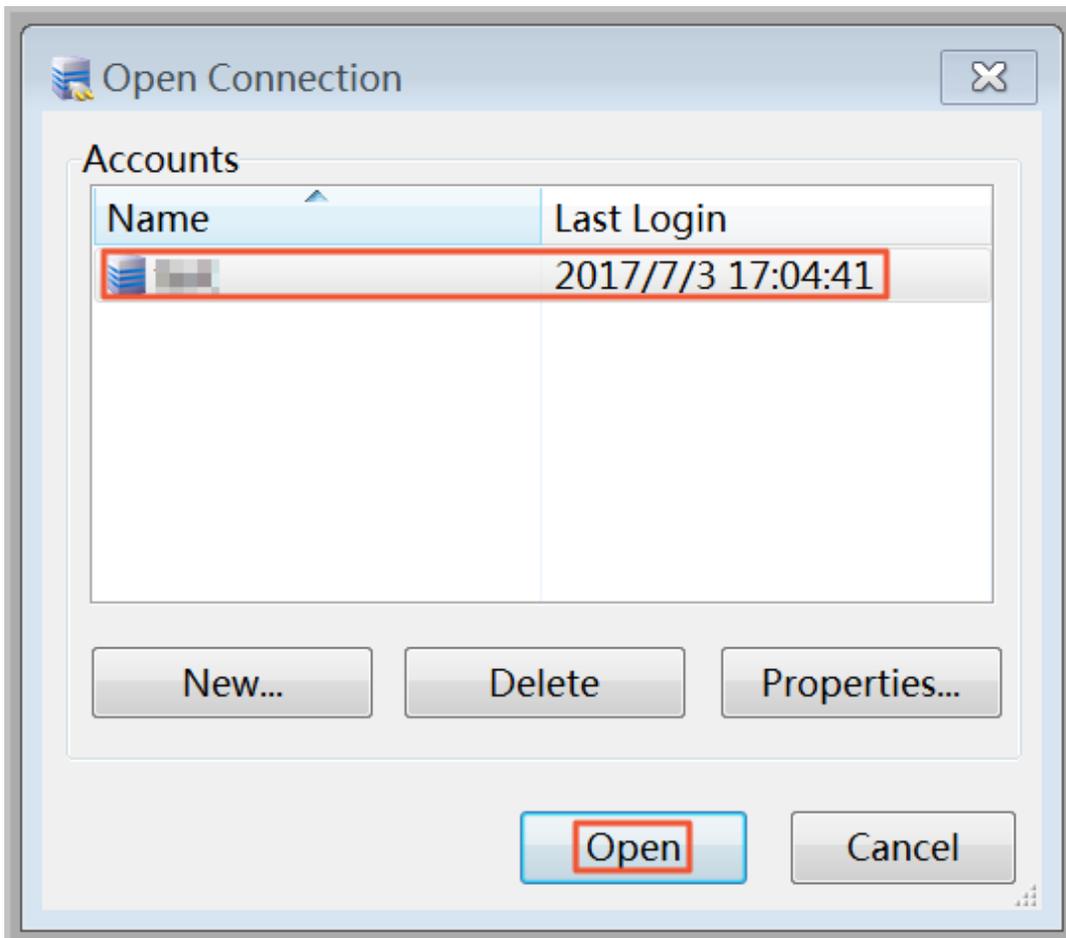
Parameter description:

- **Description Name:** Enter the connection task name. It is the same as the `Host` field by default.
- **Host:** Enter the intranet or Internet IP address allowed to access the RDS instance by referring to **Background information** of this document. You can view the address and port information as follows:
  1. Log on to the [RDS console](#).
  2. Select the region where the target instance is located.

3. Click the ID of the instance to visit the **Basic Information** page.
4. In the **Basic Information** area, you can find the Internet and intranet IP addresses and port numbers.



- **Port:** Enter the intranet port number if you use an intranet connection. Enter the Internet port number if you use an Internet connection.
  - **User:** Enter an account name of the RDS instance.
  - **Password:** Enter the account password of the RDS instance.
5. Click **OK**.
  6. In the **Open Connection** window, select the connection task that you created and click **Open**.  
If the connection information is correct, the RDS instance gets connected successfully.



## 6 Scale instances

### 6.1 Read-only instance

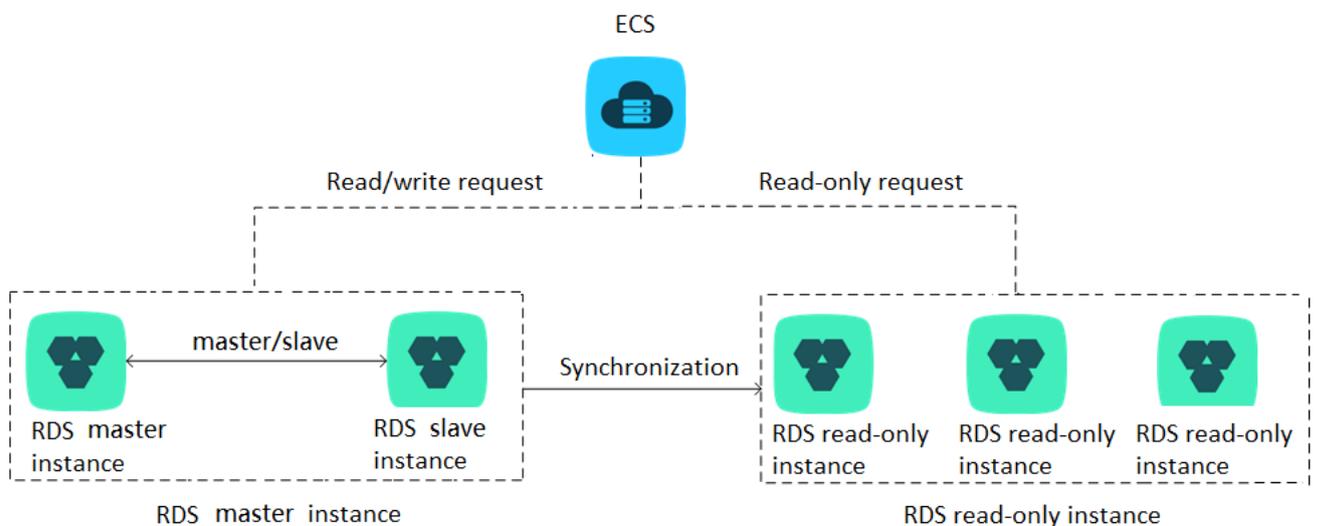
#### 6.1.1 Introduction to read-only instances

##### Scenario

For a business that needs a small number of write requests but a great number of read requests, a single instance might not resist the read pressure. As a result, business operations may be affected. To achieve the elastic expansion of the read ability and share the pressure of the database, you can create one or more read-only instances in a region. The read-only instances can handle massive read requests sent to the database and increase the application throughput.

##### Overview

A read-only instance is a read-only copy of the master instance. Changes to the master instance are also automatically synchronized to all relevant read-only instances through the native replication capability of MySQL. The synchronization works even if the master and read-only instances have different network types. Read-only instances and the master instance must be in the same region, but they can be in the different zones. The following topology shows the positioning of the read-only instance.



##### Note

- Currently, only the following ApsaraDB for RDS versions support read-only instances: MySQL 5.6 and MySQL 5.7 (excluding MySQL 5.7 Basic Edition)

- A read-only instance is in a single-node architecture with no slave node.

## Pricing

The billing method of read-only instances is Pay-As-You-Go. For more information, see [Pricing](#).



### Note:

For information about data retention policies for read-only instances, see [Expiration and overdue payment](#).

## Features

Read-only instances offer the following features:

- The specifications of a read-only instance differ from those of the master instance, and can be changed at any time, to facilitate easy elastic upgrade and downgrade.
- Read-only instances support billing measured per hour, which is user-friendly and cost-efficient.
- No account or database maintenance is required for a read-only instance. Both the account and database are synchronized through the master instance.
- Read-only instances support independent whitelist configuration.
- Read-only instances support system performance monitoring.

Up to 20 system performance monitoring views can be used, which includes disk capacity, IOPS, connections, CPU utilization, and network traffic. Users can view the load of instances at ease.

- Read-only instances provide optimization suggestions.

Optimization tools support storage engine check, primary key check, large table check, and excessive indexing and missing indexing checks.

## Restrictions

Read-only instances have the following usage restrictions:

- One master instance can only have five read-only instances.
- Read-only instances do not support backup settings or temporary backup.
- Instance recovery:

- Read-only instances do not support the creation of temporary instances through backup files or backups at any point in time. Read-only instances do not support the overwriting of instances using backup sets.
- After creating a read-only instance, the master instance does not support data recovery through the direct overwriting of instances using backup sets.
- You cannot migrate data to read-only instances.
- You cannot create or delete databases for read-only instances.
- You cannot create or delete accounts for read-only instances.
- You cannot authorize accounts or modify account passwords for read-only instances.

## 6.1.2 Create a read-only instance

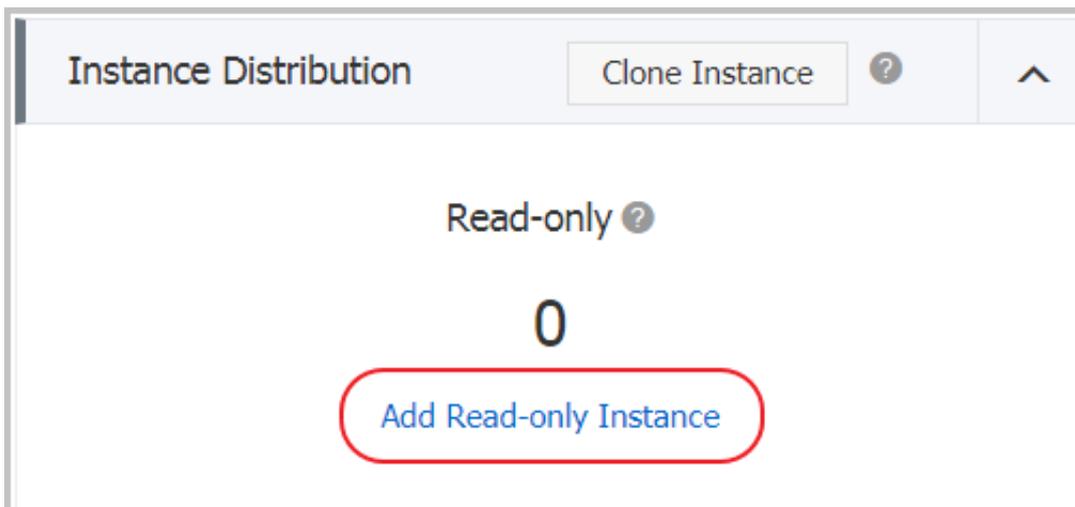
You can create read-only instances to process massive read requests sent to the database and increase the application throughput. A read-only instance is a read-only copy of the master instance. Changes to the master instance are also automatically synchronized to all relevant read-only instances through the native replication capability of MySQL.

### Attentions

- Currently, only the following ApsaraDB for RDS versions support read-only instances: MySQL 5.6 and MySQL 5.7 (excluding MySQL 5.7 Basic Edition)
- One master instance can have five read-only instances at most.
- Read-only instance is subject to an additional charge and its billing method is Pay-As-You-Go. For more information, see [Pricing](#) for read-only instances.
- The read-only instance automatically copies the whitelist its master instance, but the whitelist of the read-only instance and that of the master instance are independent. To modify the whitelist of the read-only instance, see [Set a whitelist](#).

### Procedure

1. Log on to the [RDS console](#).
2. Select the region where the target instance is located.
3. Click the ID of the target instance to visit the **Basic Information** page.
4. In the **Instance Distribution** area, click **Add Read-only Instance**, as shown in the following figure.



5. On the purchasing page, choose the configuration of the read-only instance, and then click **Buy Now**.

**Note:**

- We recommend that the read-only instance and the master instance be in the same VPC.
- To guarantee sufficient I/O for data synchronization, we recommend that the configuration of the read-only instance (the memory) is not less than that of the master instance.
- We recommend that you purchase multiple read-only instances to improve availability.

6. Select **Product Terms of Service and Service Level Notice and Terms of Use**, and then click **Pay Now**.
7. After creating the read-only instance, you can view it on the **Instances** page, as shown in the following figure.

<input type="checkbox"/>	Instance Name	Status(All) ▼	Creation Time	Instance Type(All) ▼
<input type="checkbox"/>		Running	2017-07-26 16:24	Read-only
<input type="checkbox"/>		Running	2017-07-18 15:03	Regular

## 6.2 Disaster recovery instances

For services that require high data reliability or financial services that require regulation, the RDS provides remote disaster recovery instances to improve data reliability.

### Background introduction

RDS achieves real-time synchronization between the master instance and the remote disaster recovery instance through Data Transmission Service (DTS). Both instances are deployed in the master/slave high-availability architecture. If the master node and slave node cannot be connected due to any abrupt event such as natural disasters in the region of the master instance, you can switch over the remote disaster recovery instance to the master instance. After the database link address is modified on the application, service access to the application can be quickly recovered.

Through the DTS console, disaster recovery instances can enable synchronization links to support original features such as synchronization object changing, synchronization rate setting, and delay alarming. For details, see DTS product documentation.

Disaster recovery instances have the following features:

- Provide independent database connection addresses so that the connections can be independently controlled by user applications.
- Use the master/slave high-availability architecture.
- Support hourly billing and can be enabled and disabled out-of-the-box.
- Support independent whitelist configuration and account management.

### Billing

The configuration of an RDS disaster recovery instance is exactly the same as its master instance configuration, data transmission realizes real-time synchronization between the master instance and the remote disaster recovery instance. As a result, creating disaster recovery instances will result in fees of both RDS and DTS. For price details, refer to RDS pricing information and data transmission pricing information.

### Prerequisites

- Currently, disaster recovery instances support RDS for MySQL instances only.
- When a disaster recovery instance is to be created, the master instance version must be MySQL 5.6 or later. Make a compatibility test before upgrading the master instance version. Alternatively, create a new MySQL 5.6 to copy the data from the master instance to the new instance, then create a disaster recovery instance on the new instance.

- The master instance that creates the disaster recovery instance must have an internal network address.

### Functional restrictions

Disaster recovery instances have the following functional limitations:

- Support creating accounts with the read-only permission, to ensure stability of synchronization links.
- Backup settings, backup recovery, data migration, database management, Internet IP address application, and connection address modification are not supported.

### Operation steps

1. Log on to the [RDS Management Console](#).
2. Select the target instance.
3. On the **Basic Information** page, click **Add Disaster Recovery Instance**.
4. On the **Create Synchronization Task** page, click **Purchase Instance Right Now** to purchase a disaster recovery instance.

Parameter description:

- **Synchronization Task Name**: indicates the name of a synchronization task. The default name can be retained.
  - **Instance ID** (local instance information): indicates the ID of the local instance. The system automatically associates the current instance ID, or you can click an RDS instance under a different Alibaba Cloud account. Fill in an RDS instance ID, database, account number, and the corresponding password.
  - **Instance ID** (target instance information): indicates the ID of the target instance. Click **Buy Now** to purchase the disaster recovery instance.
5. In the target RDS instance purchase window, select the region where the instance is located, and click **Buy Now**.

During the purchase of a disaster recovery instance, you can only select a region, and other configuration information is consistent with that of the master instance by default. If there are any disaster recovery instance upgrade requirements, you can create them successfully in [RDS Management Console](#) to change configuration of the disaster recovery instance.



#### Note:

It takes minutes to create a disaster recovery instance. Do not close the dialog box during creation. Otherwise, the disaster recovery instance may fail to be created.

6. After the disaster recovery instance is purchased, the instance ID is automatically added to the target instance ID. Then, click **Authorize White List and Next**.
7. The system automatically creates a migration account. After the creation is complete, click **Next**.

**Note:**

The name is automatically generated for the disaster recovery instance. For DTS synchronization, do not modify or delete the account. Otherwise, a synchronization exception may occur.

8. Select the objects to be migrated from the source database objects, click > to add the selected objects, and then click **Next**.
9. Select the synchronization initialization type and set the synchronization rate, and click **Pre-check** to start the synchronization.

Parameter description:

- **Synchronization Initialization:** Migrate the structure and data of the synchronization objects from the local instance to the disaster recovery instance, which will be used as the basis for subsequent incremental data synchronization. This parameter has two options: **Structure Initialization** and **Full Data Initialization**. Both options must be selected for your first data synchronization.
- **Synchronization Rate:** Set the rate of synchronization between the master instance and the disaster recovery instance to protect services on the master instance. The unit is TPS. If this default value of the parameter is retained, the synchronization rate is the upper limit of the DTS performance.

**Note:**

Pre-check failure is described below. If pre-check is passed, go to Step 12.

10. The system displays the pre-check results.
11. Click the detection item after the test results is failed. View the failure details to complete the error troubleshooting.
12. After troubleshooting, select the current synchronization task from **Synchronization Task List** and click **Start**.

13. After the pre-check is passed, click **OK**. The synchronization task is automatically started.
14. On the data synchronization list page of DTS, you can query created synchronization tasks and operate such tasks by changing the synchronization object, setting the monitoring alarm, and modifying the synchronization rate. For details, see DTS product documentation.

**Note:**

In order to ensure the real-time performance of disaster backup instance data, do not pause the synchronization task of the disaster recovery instance.

## 7 隐藏目录

---

### 7.1 Create databases and accounts

#### 7.1.1 Create accounts and databases for MySQL 5.7 High-availability Edition/5.5/5.6 instances

This document is applicable only to MySQL 5.7 High-availability Edition, MySQL 5.5, and MySQL 5.6 instances. For more information about how to create a database and an account for MySQL 5.7, see [Create account and database for MySQL 5.7 Basic Edition](#).

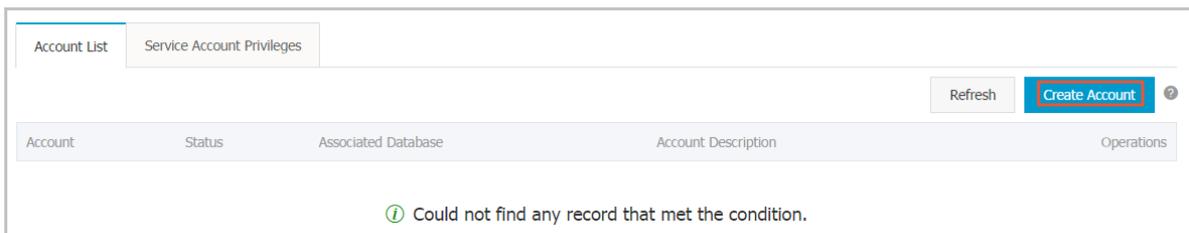
Before using RDS, you must create databases and accounts for the RDS instance. For MySQL 5.7 High-availability Edition, MySQL 5.5, and MySQL 5.6 instances, this document provides detailed procedure to create and manage databases and accounts directly on the RDS console.

#### Attentions

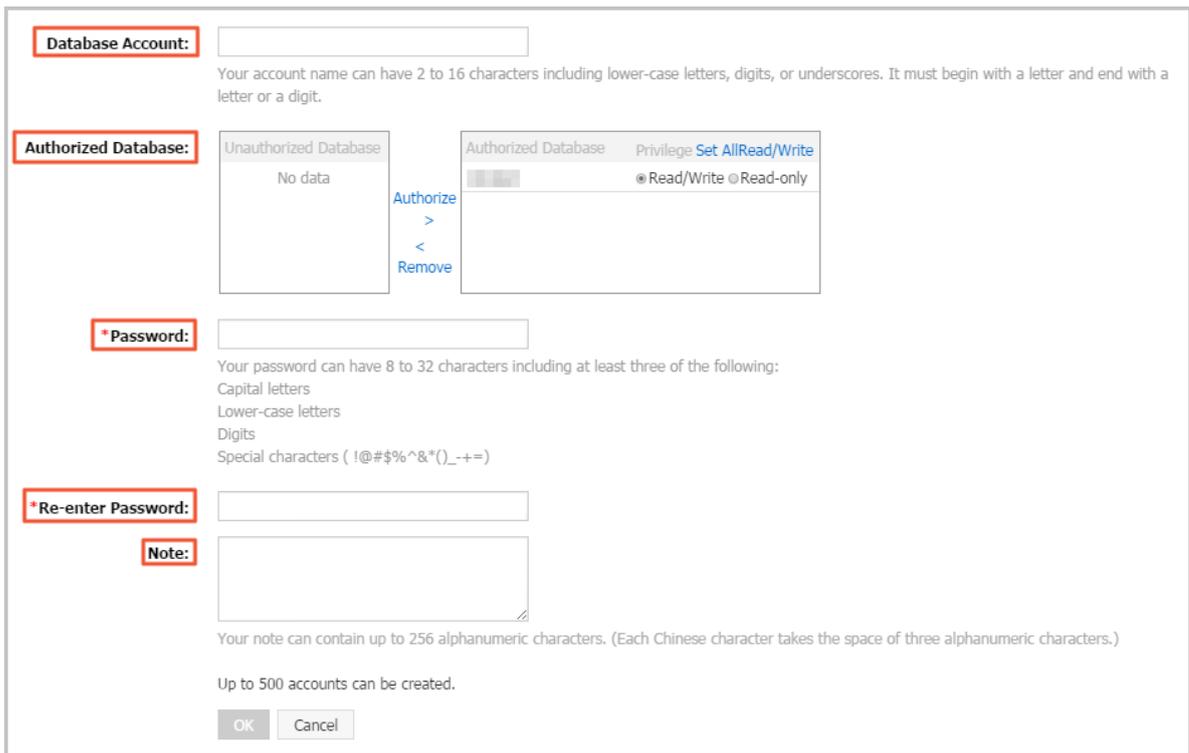
- Databases under a single instance share all the resources of this instance. Each instance supports up to 500 databases and 500 accounts.
- To migrate your local database to the RDS instance, you must create the same databases and accounts as those of on the local database.
- When assigning account permissions for each database, follow the minimum permissions' principle and consider service roles to create accounts. Additionally, rationally assign read-only and read/write permissions. When necessary, you can split accounts and databases into smaller units so that each account can only access data for its own services. If the account does not need to write data to a database, assign the read-only permission for the account.
- For database security, set strong passwords for the accounts and change the passwords regularly.

#### Procedure

1. Log on to the [RDS console](#).
2. Select the region where the target instance is located.
3. Click the ID of the instance to visit the **Basic Information** page.
4. Select **Account Management** in the left-side navigation pane to visit the **Account Management** page.
5. Click **Create Account**, as shown in the following figure.



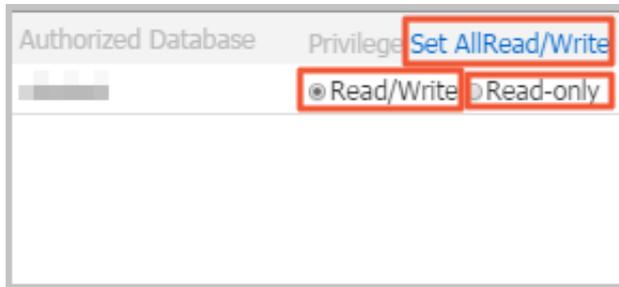
6. To create an account, set the related fields, as shown in the following figure.



Parameters description:

- **Database Account:** refers to the account name. It contains 2 to 16 characters including lower-case letters, digits, or underscores (\_). It must begin with a letter and end with a letter or a digit.
- **Authorized Database:** refers to the database that this account is authorized to access. If there is no database, you do not need set this field. Do as follows to authorize an account to access multiple databases:
  1. In the **Unauthorized Database** box, select the target database.
  2. Click **Authorize** to add the selected database to the **Authorized Database** box.
  3. You can authorize the **Read-only** or **Read/Write** permission to the account for each authorized database. If you want to authorize the same permissions to the account for

accessing all the authorized databases, click **Set All Read/Write** or **Set All Read-only**, as shown in the following figure.



- **Password:** refers to the password of this account. It contains 8 to 32 characters including at least three of the following: capital letters, lower-case letters, digits, and special characters ( !@#\$\$%^&\*()\_-= )
- **Re-enter Password:** re-enter the password to make sure the password is entered correctly.
- **Note:** You can add additional information about this account for the convenience of follow-up account management. A maximum of 256 English characters can be entered (one Chinese character equals to three English characters).

7. Click **OK**. An account is created.

8. Select **Database Management** in the left-side navigation pane to visit the **Database Management** page.

9. Click **Create Database**, as shown in the following figure.



10. Enter the information about the database, as shown in the following figure.

**\*Database Name:**   
Your database name can have 2 to 64 characters including the lowercase letters, digits, underscores, or hyphens. It must begin with a letter and end with a letter or a digit.

**\*Supported Character Set:**  Chinese\_PRC\_CI\_AS  Chinese\_PRC\_CS\_AS  SQL\_Latin1\_General\_CP1\_CI\_AS  SQL\_Latin1\_General\_CP1\_CS\_AS  
 Chinese\_PRC\_BIN  all

**Authorized Account:** The current authorized account...  
  
[Create an Account](#)

**Account Type:**  Read/Write  Read-only

**Remarks:**   
Your note can contain up to 256 alphanumeric characters. (Each Chinese character takes the space of three alphanumeric characters.)

Parameters description:

- **Database (DB) Name:** contains 2 to 64 characters including the lowercase letters, digits, underscores (\_), or hyphens (-). It must begin with a letter and end with a letter or a digit.
- **Supported Character set:** refers to the supported character set of the database. You can select utf8, gbk, latin1, or utf8mb4.
- **Authorized Account:** You can select an account authorized to access this database. Set this field only if the account is created.
- **Account Type:** This option is visible after **Authorized Account** is set. You can authorize the **Read/Write** or **Read-only** permission to the authorized account.
- **Remarks:** Enter additional information about this database for subsequent database management. A maximum of 256 English characters can be entered (one Chinese character equals to three English characters).

11. Click **OK**. A database is created.

## 7.1.2 Create accounts and databases for MySQL 5.7 Basic Edition



### Note:

This document is applicable only to MySQL 5.7 Basic Edition instances. For more information about how to create databases and accounts for MySQL 5.7 High-availability Edition and MySQL 5.6 instances, see [Create account and database for MySQL 5.7 High-availability Edition/5.5/5.6 instances](#).

To use the cloud database RDS, you must create a database and an account in the instance. For MySQL An instance of the basic version of 5.7 that you want to create an initial account in the RDS console, then create regular accounts and databases through the data management (DMS) console, detailed steps are described in this article.

## Background information

- Databases under a single instance share all the resources of this instance. Each instance supports one initial account, countless general accounts, and countless databases. You must create and manage general accounts and databases using SQL statements. For more information, see [Commonly used SQL commands \(MySQL\)](#).
- To migrate your local database to the RDS instance, you must create the same databases and accounts for the RDS instance as your local database.
- When assigning account permissions for each database, follow the minimum permission' principle and consider service roles to create accounts. Alternatively, rationally assign read-only and read/write permissions. When necessary, you can split accounts and databases into smaller units so that each account can only access data for its own services. If the account does not need to write data to a database, assign the read-only permission for the account.
- For database security, set strong passwords for the accounts and change the passwords regularly.

## Procedure

1. Create an initial account.
  - a. Log on to the [RDS console](#).
  - b. Select the region where the target instance is located.
  - c. Click the ID of the instance to visit the **Basic Information** page.
  - d. Select **Accounts** in the left-side navigation pane.
  - e. Click **Create Initial Account**.

Create Account [Back to Account Management](#)

**Database Account:**

Your account name can have 2 to 16 characters including lower-case letters, digits, or underscores. It must begin with a letter and end with a letter or a digit.

**\*Password:**

Your password can have 8 to 32 characters including at least three of the following:

- Capital letters
- Lower-case letters
- Digits
- Special characters ( !@#\$\$%^&\*()\_-= )

**\*Re-enter Password:**

Up to 1 accounts can be created.

#### Parameter description:

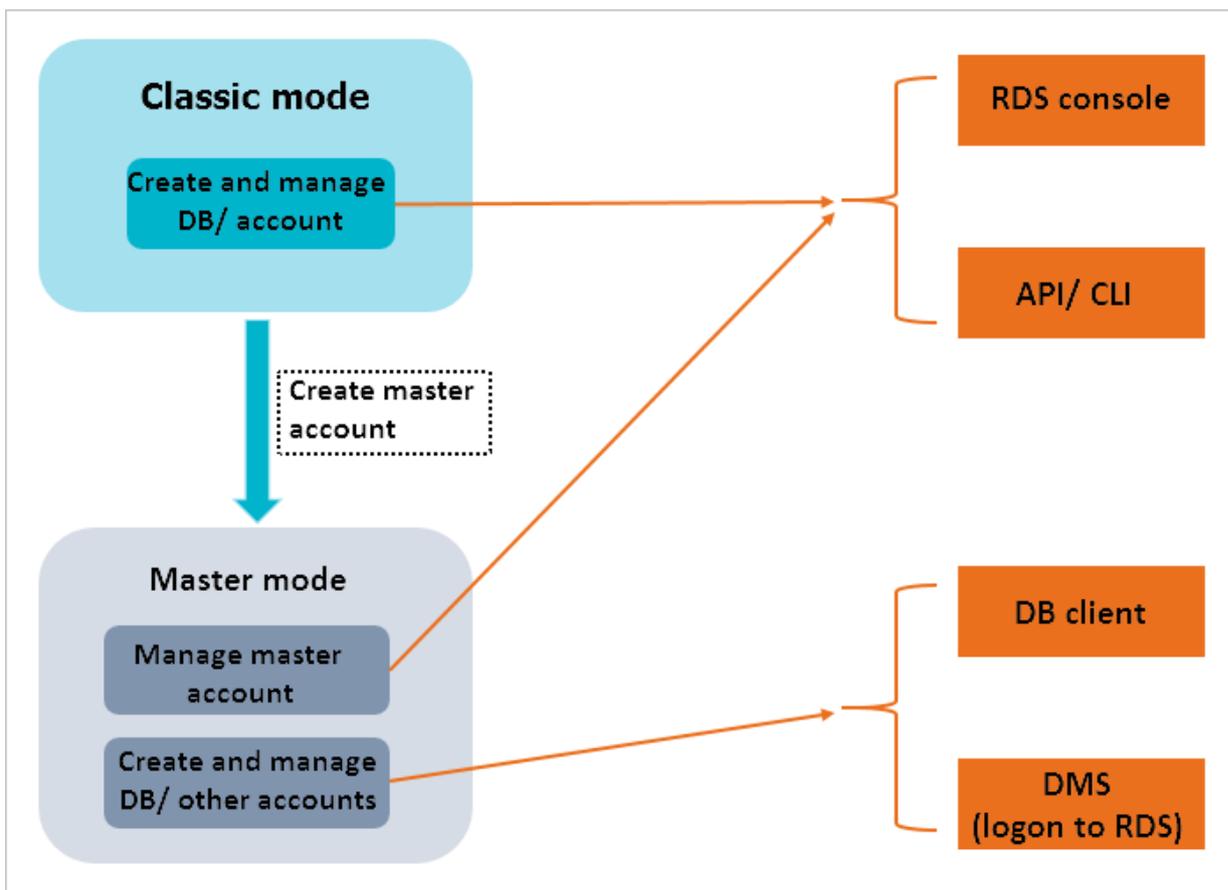
Parameters	Description
<b>Database Account</b>	Refers to the name of the initial account. It contains 2 to 16 characters including the lower-case letters, digits, or underscores. It must begin with a letter and end with a letter or digit.
<b>Password</b>	Refers to the password of the initial account . It contains 8 to 32 characters including at least three of the following: capital letters , lower-case letters, digits, and special characters (!@#\$\$%^&*()_-=)
<b>Re-enter Password</b>	Enter the password again to make sure that a correct password is entered.

- f. Click **OK**.

## 7.1.3 Create a master account

### Background information

RDS supports the classic mode and the master mode. For instances of MySQL 5.7 High-availability Edition, MySQL 5.6, and MySQL 5.5, you can create a master account to upgrade the account management mode from classic to master. The following figure shows how to switch from the classic mode to the master mode, and their differences in creating and managing databases and accounts.



Compared with the classic mode, the master mode enables more permissions to meet the personalized and sophisticated permission management needs. You can also use SQL statements to directly manage databases and accounts. Therefore, we recommend that you use the master mode.

This document describes how to upgrade the account management mode, namely to create a master account, for MySQL 5.7 High-availability Edition, MySQL 5.6, and MySQL 5.5 instances. For details about the usage, supported engines, functions, and permissions of accounts in the classic mode and master mode, see [Create an account](#).

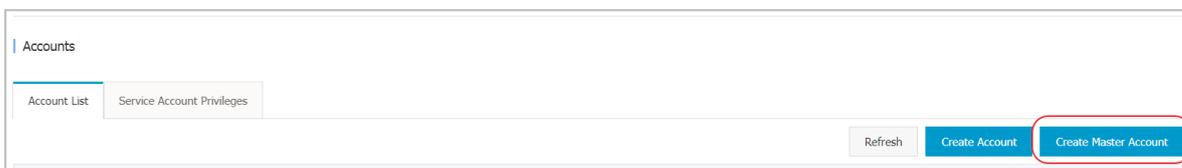
### Attentions

- After a master account is created for a master instance, the account is synchronized to the read-only instances and disaster tolerance instances.
- In the master mode:
  - You can manage databases and common accounts only by using [Commonly used SQL commands for MySQL](#).
  - However, you can reset the permissions and password of the master account on the RDS console or through APIs, without affecting other accounts in the instance.

- The following changes occur after an instance switches to the master account mode: After the master account is created, the **Databases** page and **Create Account** on the **Accounts** page disappear. However, this change only affects the single instance and has nothing to do with other instances.
- For MySQL 5.5/5.6 instances:
  - You can only upgrade from the classic mode to the master mode and cannot roll back.
  - You cannot directly access the mysql.user and mysql.db tables, but you can view the existing account and permissions through mysql.user\_view and mysql.db\_view.
  - You cannot use the master account to modify passwords of other common accounts. To modify passwords of other common accounts, you must delete the master account and create a new account.
- MySQL 5.7 instances support only the master mode.
- When the master account is created, an instance restart cause a transient network disconnection of 30s. Make sure that you create an account at proper time and the application supports auto-reconnection to prevent disconnections.

## 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. Select **Accounts** in the left-side navigation pane to visit the **Accounts** page.
5. Click **Create Master Account**, as shown in the following figure.



6. Select **I understand the above warnings and want to proceed with creating a master account** and click **Next**.

### Create Master Account ✕

*[Blurred text]*

**Note:**

I understand the above warnings and want to proceed with creating a master account.

Next Cancel

7. Set the related fields.

### Create Master Account ✕

**Database Account:**

Your account name can have 2 to 16 characters including lower-case letters, digits, or underscores. It must begin with a letter and end with a letter or a digit.

**\*Password:**

Your password can have 8 to 32 characters including at least three of the following:

- Capital letters
- Lower-case letters
- Digits
- Special characters ( !@#\$%^&\*()\_-= )

**\*Re-enter Password:**

[Previous](#) [Create](#) [Cancel](#)

#### Parameter descriptions:

- **Database Account:** The account is a string of 2 to 16 characters. It must contain lowercase letters, numbers, and underscores (\_). The account must start with a letter and end with a letter or a number.
- **Password:** refers to the password of the account. The password is a string of 8 to 32 characters. It must contain any three of letters, numbers, hyphens (-), and underscores (\_).
- **Re-enter Password:** Re-enter the password to verify that the password is entered correctly.

## 8. Click **Create**.



### Note:

After a master account is created, the account name cannot be modified, but the password can be modified later on the RDS console.

## 7.2 Manage read-only instances

You can manage read-only instances through the RDS console. Read-only instances are managed similarly to common instances. Executable management operations can be performed on the RDS console. This document describes how to enter the management interface for read-only instances and how to view the synchronization delay of read-only instances.

### Enter the management interface directly through the read-only instance

1. Log on to the [RDS console](#).
2. Select the region where the target read-only instance is located.
3. Click the ID of the target read-only instance to enter its management interface.



### Note:

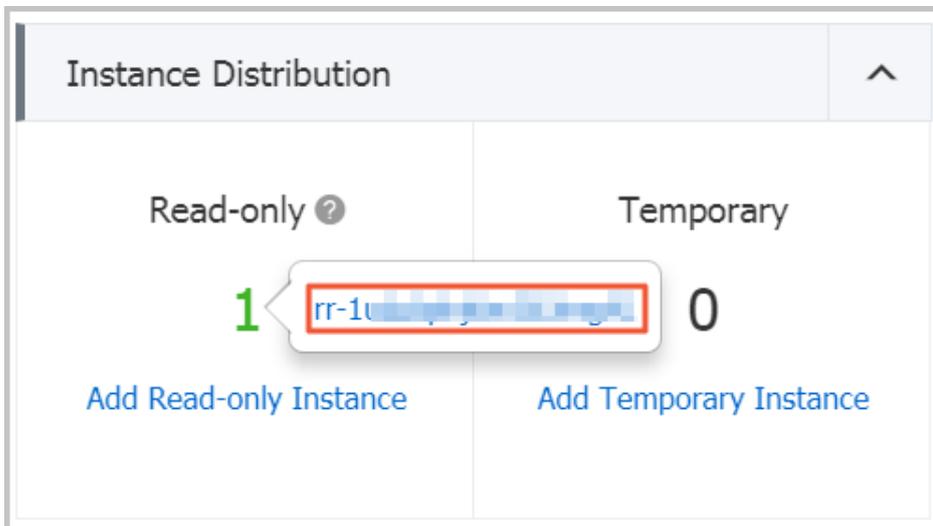
On the **Instances** page, the instance ID marked with an R indicates a read-only instance, as shown in the following figure.

<input type="checkbox"/>	Instance Name	Status(All) ▼	Creation Time	Instance Type(All) ▼
<input type="checkbox"/>		Running	2017-07-26 16:24	Read-only
<input type="checkbox"/>		Running	2017-07-18 15:03	Regular

### Enter the management interface through the master instance

1. Log on to the [RDS console](#).
2. Select the region where the target master instance is located.
3. Click the ID of the target master instance to enter the **Basic Information** page.

- 4. In the **Instance Distribution** area, put the mouse over the number of the read-only instance, and then the instance IDs are displayed, as shown in the following figure:



- 5. Click the ID of the target read-only instance to enter its management interface.

### View the data synchronization delay of read-only instance

When synchronizing data from the master instance, the read-only instance may delay for some time. You can view the delay on the **Basic Information** page of the read-only instance, as shown in the following figure:

