ApsaraDB for RDS

Quick Start (SQL Server)

Quick Start (SQL Server)

Getting started with ApsaraDB

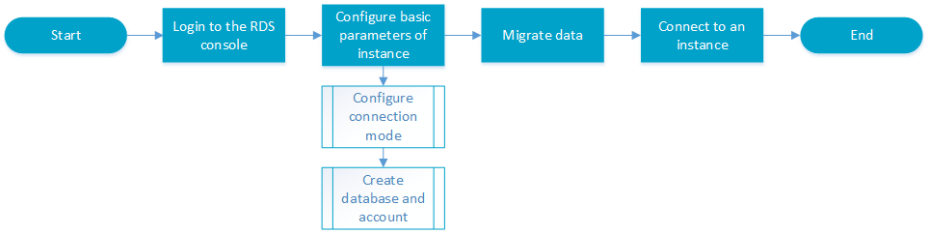
The ApsaraDB Relational Database Service (RDS) is a stable, reliable, and auto-scaling online database service. Based on the Apsara distributed file system and high-performance storage, the RDS supports MySQL, SQL Server, PostgreSQL, and PPAS (highly compatible with Oracle) engines. It provides a complete set of solutions for backup & restore, monitoring, migration, and other features, to save your time by relieving operational work for databases so that you can keep focusing on your business and development.

The ApsaraDB RDS Console provides web interface to access and manage your RDS resources. You can create a new database instance, make some changes on database configurations, set up scalability in process, memory resources and storages. This document shows step-by-step guide how to do some of these tasks.

ApsaraDB RDS API provides same level of controls to RDS resources over Rest APIs. For the list of RDS APIs, please see RDS API Reference.

Document overview

This document describes the following entry level task.



For more information about functions and pricing of the ApsaraDB, please log in to the Official Website of ApsaraDB.

General description convention

Description	Note
Local database/Source database	Refers to the database deployed to local servers running at customer data center 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 (XX is MySQL, SQL Server, PostgreSQL, or PPAS)	RDS for XX indicates the RDS of a specific database type, for example, RDS for MySQL means the instance enabled on the RDS and whose database type is MySQL.

Instructions before use

Functional limitations

To ensure instance stability and security, RDS for SQL Server has the following limitations on use:

- A single instance supports up to 50 databases.
- The maximum number of database accounts is 500.
- There is no permission for creating databases and accounts from command lines or GRANT permission.
- For security reasons, some SQL Server functions are not allowed to use, for example, distributed transaction, Windows domain account login, email, BI analysis, report, database-level DDL trigger (which contains Alter Table, Create Table, Add/Delete Index and other DDL statements), assembly, Service Broker, SQL Server Profiler, copy, policy management, and proxy start/stop.

SQL server license

Currently, RDS for SQL Server provides only instances with accompanying licenses. That is, after an instance is created, it is granted with a license of the Microsoft SQL Server Enterprise Edition and does not support to replace licenses by users.

Login to the RDS console

Management operations on the instances on the RDS need to be performed through the RDS console. This section describes how to log in to the RDS console and enter the page for subsequent instance management and control operations.

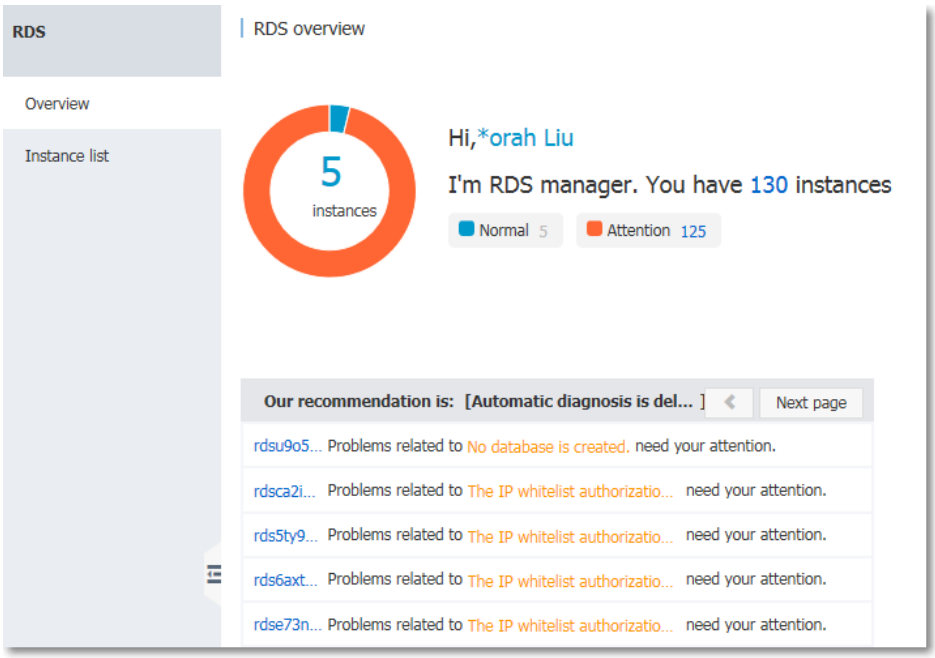
Prerequisites

Before logging in to the RDS Console, you need to buy the RDS instance. Please refer to Purchase for buying RDS instances. For detailed charging standards, please refer to RDS Price.

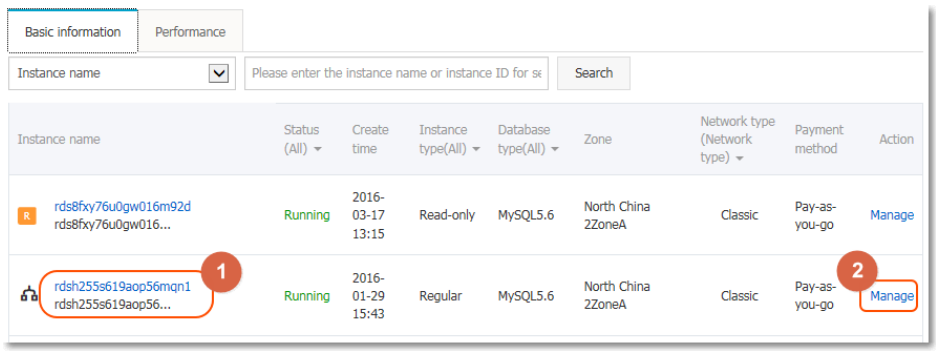
Operation procedure

Use the account for purchasing the RDS to log in to the RDS Console.

The system displays the **RDS Overview** interface, as shown in the figure below.



Select **Instance List** in the menu, and click **Instance Name** of the database or the corresponding **Manage** button to access the instance management interface, as shown in the figure below.



Subsequent operations

After accessing the specific instance management console, you can manage the instance account and database, set instance parameters, etc.

Setting the basic configuration

Setting a white list

For the security and stability of the database, you need to add IP addresses or IP segments used to access the database to a white list. This section describes how to set a white list.**Before using the target instance, you need to modify the white list.**

Context

You can access the database in three scenarios:

Access the ApsaraDB through the Internet

Refer to Set Intranet and Internet addresses to apply for an Internet IP address.

Refer to this section to add the application service IP address to the white list.

If you cannot connect to the ApsaraDB after adding the application service IP address to the white list, refer to How to locate the local IP address using ApsaraDB for MySQL to obtain the actual IP address of the application service.

Access the ApsaraDB through the Intranet:

Ensure that the network type is the same for ApsaraDB and ECS. For details about how to set the network type, refer to Set network type.

Refer to Set Intranet and Internet addresses to apply for an Intranet IP address.

Refer to this section to add the ECS IP address to the white list.

Access the ApsaraDB through the Internet and Intranet simultaneously:

Ensure that the network type is the same for ApsaraDB and ECS, and set the access mode to **High Security Mode**. For details about how to set the network type, refer to Set network type.

Refer to Set Intranet and Internet addresses to apply for Internet and Intranet IP addresses.

Refer to this section to add the application service IP address and ECS IP address to the white list.

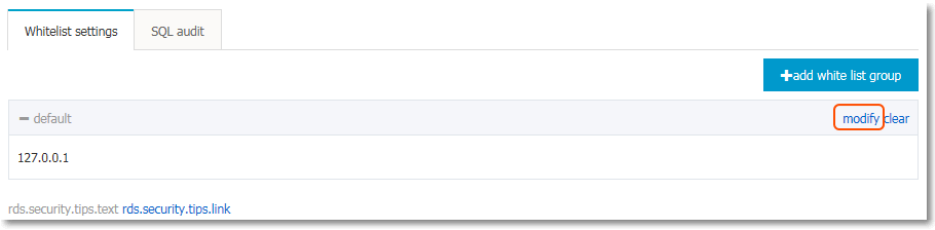
Operation procedure

Log in to the RDS Console and select the target instance.

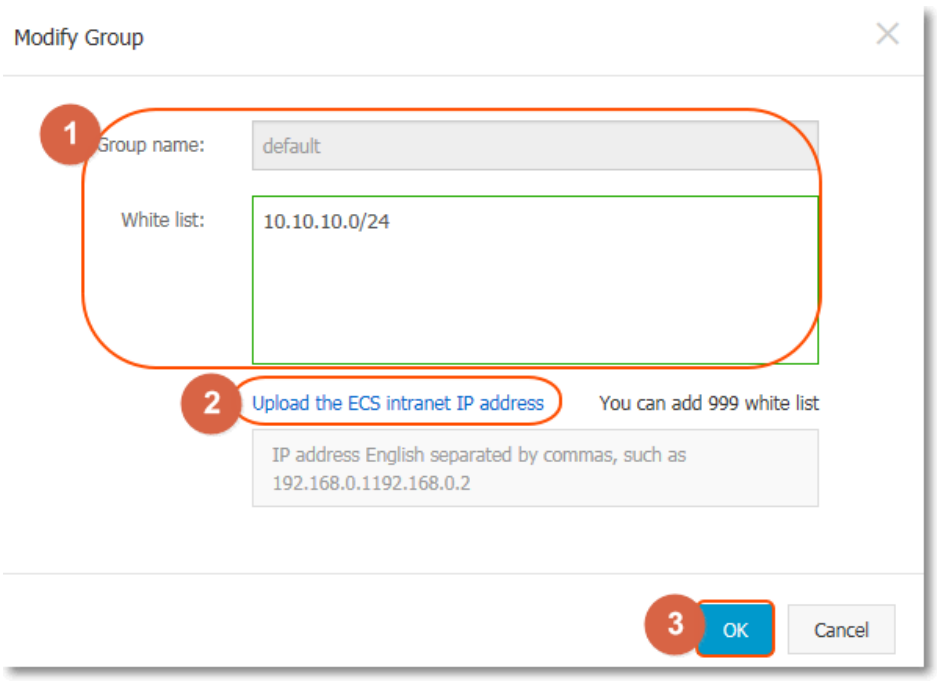
Select **Data Security** in the instance menu.

On the *Data Security* page, click **Modify** after the default group, as shown in the figure below.

You can also click **Clear** after the default group to delete the white list from the default group, and click **Add White List Group** to create a custom group.



On the *Add White List Group* page, delete the default white list *127.0.0.1*, enter a custom white list and then click **OK**, as shown in the figure below.



Parameters are described as follows:

- Group name: The group name contains 2 to 32 characters which consist of lowercase letters, digits or underscores. The group name must start with a lowercase letter and end with a letter or digit. The default group cannot be modified or deleted.
- Intra-group white list: Enter IP addresses or IP segments which can access the database. IP addresses or IP segments are separated by commas.
    - 1,000 white lists can be set for MySQL, PostgreSQL and PPAS, and 800 white lists can be set for SQL Server.
    - The white list can contain IP addresses (for example, 10.10.10.1) or IP segments (for example, 10.10.10.0/24, which indicates any IP address in the format of 10.10.10.X can access the database).
    - *%* or *0.0.0.0/0* indicates any IP address is allowed to access the database. **This configuration greatly reduces security of the database, and thus is not recommended unless necessary.**
    - After an instance is created, the local loopback IP address *127.0.0.1* is set as the default white list, and thus external IP addresses are prohibited to access this instance.
- Load Intranet IP address of ECS: Click the IP address, and ECS of the same account is displayed. You can add the ECS to the white list.

Subsequent operations

Correct use of the white list can provide improved access security protection for RDS, and thus it is recommended to periodically maintain the white list.

During future operations, you can click **Modify** after the group name to modify an existing group, or click **Delete** to delete an existing group.

Configuring the connection mode

If your applications are deployed on the ECS in the same region, you do not need an Internet address. In this case, skip this step. If your applications are deployed on the ECS in other region or a system other than Alibaba Cloud, you need to apply for an Internet address in order to access remotely from the application running out side of the region (running at another region or out side of Alibaba Cloud).

Background information

The RDS provides two kinds of connection addresses: Intranet address and Internet address.

- The Intranet address or the Internet address can be used only when **Access Mode** is set to **Standard Mode**.
  - If your applications are deployed on the ECS in the same region, you can use the Intranet address. The system provides an Intranet address by default, and you can directly modify the connection address.
  - If your applications are deployed on the ECS in the other region or a system other than Alibaba Cloud, you need to use an Internet address. You can click the **Apply for an Internet Address** to release an Intranet address and generate an Internet address.
- The Intranet address and the Internet address can be used at the same time only when *Access Mode* is *High Security Mode*. If your applications are deployed on the ECS in the same region and a system other than Alibaba Cloud at the same time, you must use both Intranet and Internet addresses.

Note

- The RDS will charge a fee for traffic over the internet address. For detailed charges, refer to RDS Price.
- To get a higher transmission rate and a higher security level, you are recommended to migrate the applications to an Alibaba ECS in the same region where you RDS is running.

Operation procedure

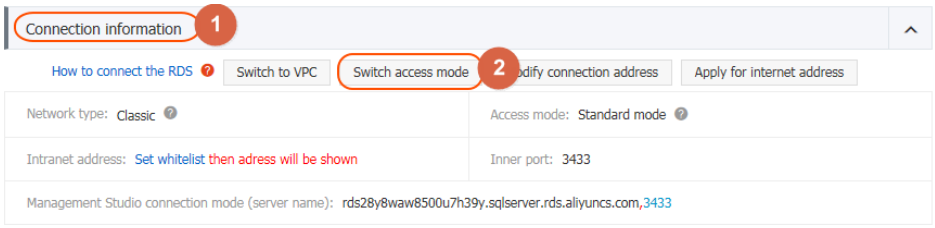
Both the Intranet address and the Internet address are used in this example. When using the RDS, configure the connection mode based on the system plan.

1. Log in to the RDS console and select the target instance.
2. Select **Database Connection** in the menu.

Click **Switch Access Mode** in **Database Connection**, click **OK** on the displayed confirmation interface, and switch the access mode to **High Security Mode**, as shown in the figure below.

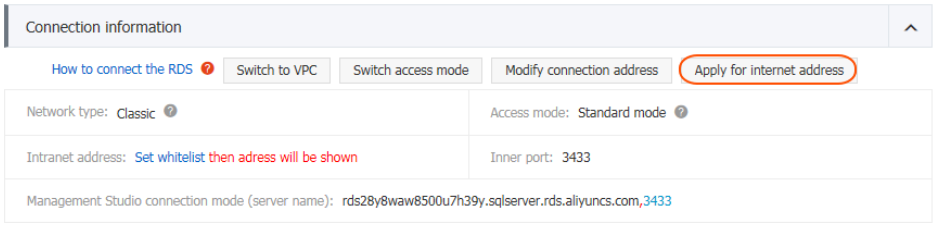
If **Access Mode** is **High Security Mode** already, no switch is needed.

> Standard mode: The RDS uses Server Load Balancer to eliminate the impact of database engine HA switching on the application layer and shorten the response time, but that may slightly increase the probability of transient disconnections and disable the RDS from intercepting SQLs.
>
> This mode supports only one connection address. When the instance has both the Intranet address and the Internet address, it is required to first release the Intranet address or the Internet address, and then switch to **Standard Mode**.
>
> High security mode: This mode can prevent 90% of transient disconnections and SQL hijacking (the SQL injection attack is prevented based on SQL semantic analysis), but the response time will be increased by 20% or more. This mode supports coexistence of the Intranet address and the Internet address.



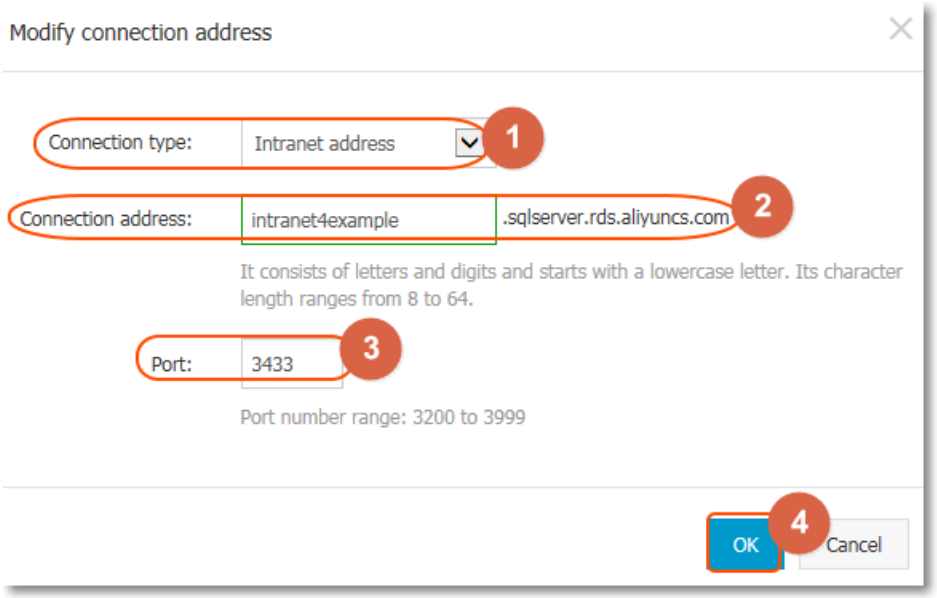
Click **Apply for an Internet Address**, and click **OK** on the displayed confirmation interface to generate an Internet address, as shown in the figure below.

Traffic at the Internet address may cause charges and reduce the instance security. Be cautious about your selection.



Click **Modify the Connection Address**, set the Intranet and the Internet connection

addresses and port numbers in the displayed window, and click **OK**, as shown in the figure below.



- 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. **xxx** is a user-defined field consisting of 8 to 64 characters (only supporting letters and digits). It must start with a lowercase letter, for example, **extranet4example**.
- Port: indicates the number of the port through which the RDS provides external services, which can be an integer within the range of 3,200 to 3,999.

Creating a database and an account (SQL Server 2008 R2)

Before using a database, you need to create the database and an account in the RDS instance; before database migration, you need to create the same database in the local database and the RDS instance and create the same account in the RDS instance and the local database.

Background information

- The section describes a sample operation procedure for SQL Server 2008 R2.
- If you use SQL Server 2012, refer to Creating a database and an account (SQL Server 2012).
- To migrate the local database to the RDS, use the consistent migration account and database in the RDS database with the local database.

- Databases under a single instance share all the resources of this instance. SQL Server instances support creating up to 50 databases and 500 accounts.

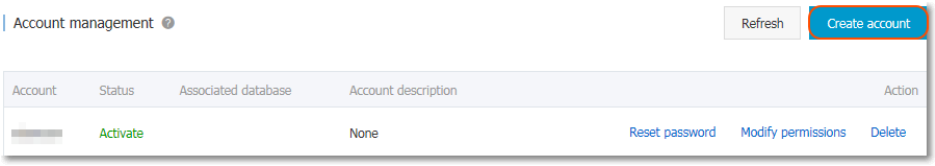
Note:

- When assigning database account permissions, follow the minimum permission principle and service roles to create accounts and rationally assign Read-Only and Read/Write permissions. When necessary, you may split database accounts and databases into smaller units so that each database account can only access data for its own services. If you do not need to write data to a database, assign Read-Only permission.
- Use strong passwords for database accounts and change the passwords on a regular basis.

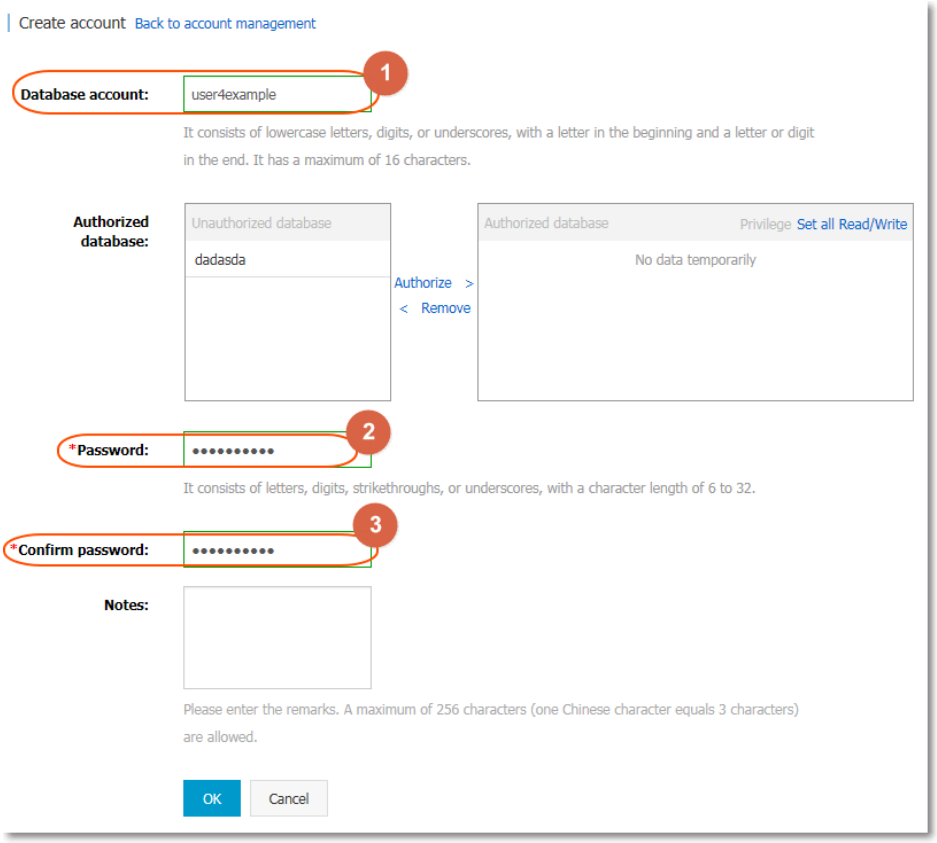
Operation procedure

1. Log in to the RDS console and select the target instance.

   Select **Account Management** in the menu, and click **Create an Account**, as shown in the figure below.



   Enter the information of the account to create, and click **OK**, as shown in the figure below.

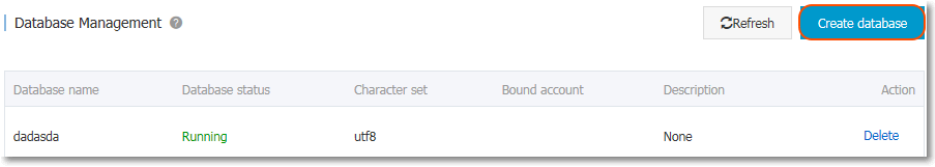


- Database account: It consists of 2 to 16 characters (which can be lowercase letters, digits or underscores). It must begin with a letter and end with a letter or digit, for example, user4example*.
- Authorized database: It refers to the authorized database of this account. Select **Unauthorized Database** on the left, and click **Authorize** to add the database to **Authorized Database**. This field can be blank if no database has been created.

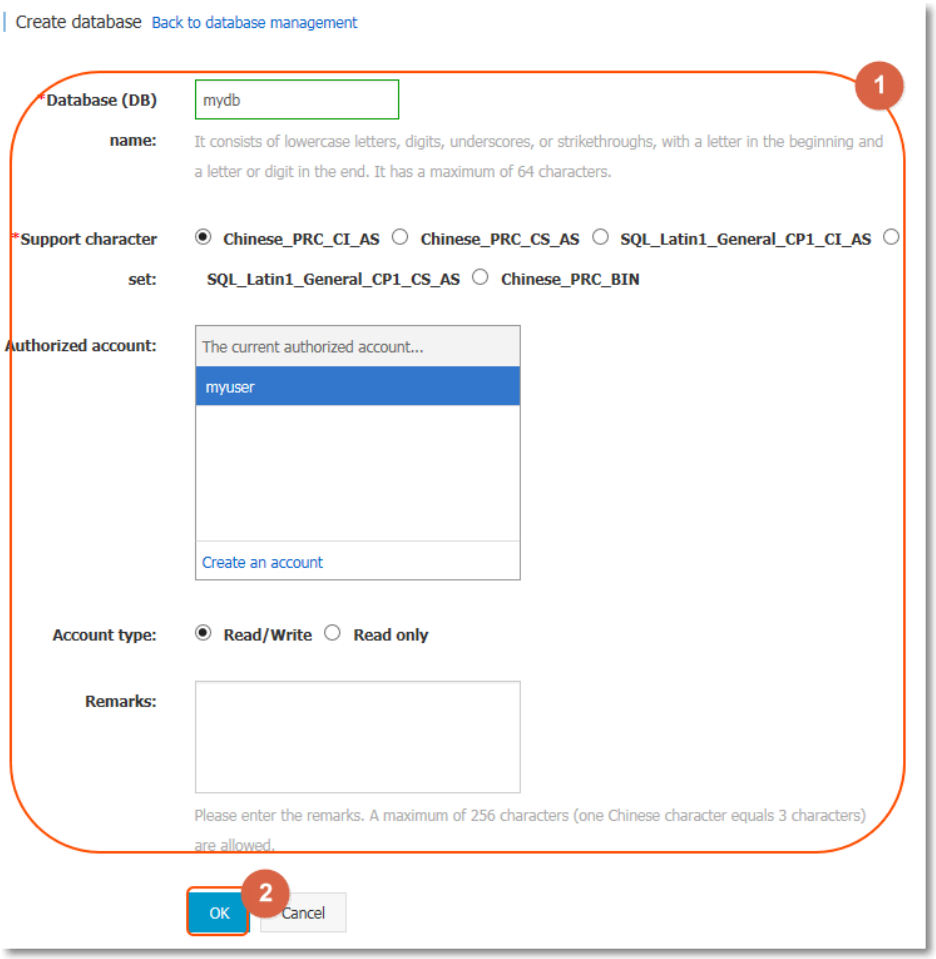
You can click the permission setting button on the upper-right corner of *Authorized Database* to batch set the permissions of the databases under this account to **All to Read and Write** or **All to Read Only**.

- Password: It refers to the password corresponding to this account. The password consists of 6 to 32 characters which may be letters, digits, hyphens or underscores, for example, *password4example*.
- Confirm the password: Enter the password again, for example, *password4example* to ensure that a correct password is entered.
- Remarks: Related information of this account can be added to the remarks to facilitate subsequent account management. A maximum of 256 characters can be entered (one Chinese character is equal to three characters).

Select **Database Management** in the menu, and click **Create a Database**, as shown in the figure below.



Enter the information of the database you want to create, and click **OK**, as shown in the figure below.



- Database (DB) name: The database name contains 2 to 64 characters which consist of lowercase letters, digits, underscores, or strikethroughs. It must start with a letter and end with a letter or digit, for example, *dbname4example*.
- Supported character sets: Five character sets are supported: Chinese_PRC_CI_AS, Chinese_PRC_CS_AS, SQL_Latin1_General_CP1_CI_AS, SQL_Latin1_General_CP1_CS_AS, and Chinese_PRC_BIN.
- Authorized account: Select an account authorized by this database. This field can be blank if no account has been created.
- Account type: This option is visible after **Authorized Account** is selected. Set the permission authorized by this database to **Authorized Account**, which can be set to **Read and Write** or **Read Only**.

- Remarks: Related information of this database can be added to the remarks to facilitate later database management. A maximum of 256 characters can be entered (one Chinese character is equivalent to three characters).

Create a database and an account (SQL Server 2012)

Before using a database, you need to create a database and an account in the RDS instance. Before database migration, you need to create a database consistent with the local database in the RDS instance and create a consistent account in the RDS instance and the local database.

Background information

This section describes the sample operation procedure for SQL Server 2012. Compared with SQL Server 2008 R2, the permission system of SQL Server 2012 is more open, allowing you to manage instances only using an initial account.

If you use SQL Server 2008 R2, refer to Create a database and an account (SQL Server 2008 R2).

To migrate the local database to RDS, you need to create a consistent migration account and database respectively in the RDS database and local database.

The databases under an instance share all the resources of this instance.

Note:

When granting permissions to the database account, create an account according to the minimum permission principle and the role, and grant reasonable permissions to this account. When necessary, you may split database accounts and databases into smaller units so that each database account only has access to its own service data.

Use strong passwords for database accounts and change the passwords on a regular basis.

Operation procedures

Log on to the RDS Console.

Select the region where the target instance is located.

Click the name of the target instance to go to the “Basic information” page.

Select **Account management** in the left menu and click **Create Account**.

Note: You can create only one initial account for each instance.

Enter the information of the account you want to create, and click **OK**. The parameters are described as follows:

Database account: The database account consists of 2 to 16 characters including lower-case letters, numbers or underscores. It must start with a letter and end with a letter or number.

Password: Indicates the password of the account. The password consists of 8 to 32 characters including uppercase letters, lower-case letters, numbers or special characters. The password must be a combination of no less than three types of the above-mentioned characters. Special characters include !, @, #, $, %, ^, &, *, (,), _, +, -, and =.

Password confirmation: Re-enter the password to verify that it is correct.

Use the account to connect to RDS for SQL Server.

For details about how to connect to RDS for SQL Server, refer to Connect to an instance. This section uses SQL Server Management Studio as an example.

Right-click **Database**, choose **Create a Database**, enter **Database Name**, and click **OK**.

Right-click **Security > Login Name**, select **Create a Login Name**, enter the account information, and select **Default Database**.

Note: For identity authentication, select **SQL Server Authentication**, and customize the password policy as required.

Connecting to an instance

An RDS instance can be connected via common methods or Alibaba Cloud DMS.This chapter describes the methods of connecting to an RDS instance.

Prerequisites

If you want to use DMS or a client to access an RDS instance, you must add the corresponding intranet and Internet IP addresses to the RDS white list. For detail, see Setting a White List.

Login via client

This section uses Microsoft SQL Server Management Studio as an example to describe the method of connecting to an RDS for SQL Server instance. You can refer to this method when using other clients.

1. Click **Connect** in Microsoft SQL Server Management Studio.
2. In the **Connect to Server** dialog box that is displayed, enter the login information and click **Connect**, as shown in the figure below.
   - Server name: intranet/Internet address and port ID of an RDS instance
   - Login name: database account
   - Password: password of a database account

Appendix: function differences between SQL Server 2008 R2/2012

There are some differences in features and Open API between SQL Server 2008 R2 and SQL Server 2012:

List of Feature Differences between SQL Server 2008 R2 and SQL Server 2012

List of Open API Feature Differences

List of Feature Differences between SQL Server 2008 R2 and SQL Server 2012

Feature	SQL Server 2008 R2	SQL Server 2012
Database backup and recovery	Available	Available

Anti-DDoS	Available	Available
IP white list	Available	Available
Blocking SQL injection and brute force cracking	Available	Available
Master/backup architecture	Available	Not available
Local disaster tolerance	Available	Not available
Remote disaster tolerance	Available	Not available
Auto scaling	Available	Available
SSIS	Not available	Not available
SSAS	Not available	Not available
SSRS	Not available	Not available
Broker service	Not available	Not available
Distributed Transaction Controller (DTC)	Not available	Not available
Linking to server	Not available	Available

List of Open API Feature Differences

Open API	Interface name	SQL Server 2008 R2	SQL Server 2012
Migrate to a zone	MigrateToOtherZone	Available	Not available
Request for Intranet address	SwitchDBInstanceNetType	Available	Not available
Modify the instance access mode	ModifyDBInstanceConnectionMode	Available	Not available
Create an account	CreateAccount	Available	Not available
Create a database	CreateDatabase	Available	Not available
Grant privileges to an account	GrantAccountPrivilege	Available	Not available
Revoke privileges from an account	RevokeAccountPrivilege	Available	Not available
Get a file upload address	CreateUploadPathForSQLServer	Available	Not available
Import data	ImportDataForSQLServer	Available	Not available
Migrate other instances	ImportDatabaseBetweenInstances	Available	Not available
Cancel migration	CancelImport	Available	Not available