Alibaba Cloud ApsaraDB for RDS

RDS for SQL Server Database

Issue: 20191127

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, consequent**

ial, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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.**

Document conventions

Style	Description	Example
	A danger notice 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.
	A warning notice 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 restart an instance.
	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 **Notice:** If the weight is set to 0, the server no longer receives new requests.
	A note indicates supplemental instructions, best practices, tips, and other content.	 **Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type.
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands.	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *`Instance_ID`*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`

Style	Description	Example
{} or {a|b}	**This format is used for a required value, where only one item can be selected.**	`switch {active|stand}`

Contents

1 Preface

This topic provides an overview of RDS for MySQL, including a disclaimer, terms, and concepts.

Overview

ApsaraDB for RDS offers stable, reliable, and scalable cloud database services. Based on Apsara Distributed File System and high-performance storage (SSD), ApsaraDB for RDS supports the following database engines: MySQL, SQL Server, PostgreSQL, and PPAS (high compatibility with Oracle). ApsaraDB for RDS also provides solutions for disaster recovery, backup, database restoration, monitoring, and migration to simplify the database operations and maintenance. For more information about the benefits of ApsaraDB for RDS, see *Benefits*.

This document describes how to configure ApsaraDB for RDS through the *ApsaraDB for RDS console* to help you know more about its features and functions. You can also manage ApsaraDB for RDS through APIs and SDKs.

For further assistance, you can contact a customer service representative at +86 95187. You can also log on to the *ApsaraDB for RDS console*, click More in the top navigation bar, and choose Support > Open a new ticket. If your business is complex, you can purchase a *support plan* to obtain support from IM enterprise groups, technical account managers (TAMs), and service managers.

For more information about ApsaraDB for RDS, see *Product Details*.

Disclaimer

Some product features or services described in this document may be unavailable in certain regions. See the actual commercial contracts for specific Terms and Conditions. This document serves as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby states that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly.

Terms

- **Instance: A database service process that takes up physical memory independently. You can set different memory size, disk space, and database type, where the memory size determines the performance of the instance. After the instance is created, you can change the configuration or delete the instance at any time.**
- **Database: A database is a logical unit created in an instance. The name of each database under the same instance must be unique.**
- **Region and zone: Each region is a separate geographic area. Each region has many isolated locations known as zones. The power supply and network of each zone are independent. For more information, see *Alibaba Cloud Global Infrastructure*.**

General terms

Term	Description
On-premise database	Refers to the database deployed in the local server room or the database not on the ApsaraDB for RDS.
ApsaraDB RDS for XX (XX represents one of the following database engines: MySQL, SQL Server, PostgreSQL, and PPAS.)	Indicates the ApsaraDB for RDS of a specific database engine. For example, ApsaraDB RDS for MySQL means the database engine of the instance enabled on the RDS is MySQL.

2 Limits of RDS for SQL Server

This topic describes the limits of RDS for SQL Server. To guarantee instance stability and security, you must understand the limits.

An RDS for SQL Server instance provides a Microsoft SQL Server license. You cannot use your own license. The other limits are described in the following table.

Function	Cluster (AlawayOn) Edition	High-Availibility Edition		Basic Edition
	2017 Enterprise	2017 Standard 2016 Standard/ Enterprise 2012 Standard / Enterprise	2008 R2 Enterprise	2016 Web 2012 Web/ Enterprise
Maximum number of(Note) databases	300	300	50	400
Maximum number of database accounts	Unlimited	Unlimited	500	Unlimited
Create user , LOGIN, or database	Supported	Supported	Supported	Supported
Database-level DDL trigger	Supported	Supported	Not supported	Supported
Database permission authorization	Supported	Supported	Not supported	Supported
KILL permission	Supported	Supported	Supported	Supported
LinkServer	Supported	Supported	Not supported	Not supported
Distributed transaction	Supported	Supported	Not supported	Not supported

Function	Cluster (AlawayOn) Edition	High-Availibility Edition		Basic Edition
	2017 Enterprise	2017 Standard 2016 Standard/ Enterprise 2012 Standard / Enterprise	2008 R2 Enterprise	2016 Web 2012 Web/ Enterprise
SQL Profiler	Supported	Supported	Supported	Supported
Tuning Advisor	Supported	Supported	Not supported	Supported
Change Data Capture (CDC)	Supported	Supported	Not supported	Supported
Chage Tracking	Supported	Supported	Supported	Supported
Windows domain account login	Not supported	Not supported	Not supported	Not supported
Email				
SQL Server Integration Services (SSIS)				
SQL Server Analysis Services (SSAS)				
SQL Server Reporting Services (SSRS)				
R Services				
Common Language Runtime (CLR)				
Asynchronous communication				

Function	Cluster (AlawayOn) Edition	High-Availibility Edition		Basic Edition
	2017 Enterprise	2017 Standard 2016 Standard/ Enterprise 2012 Standard / Enterprise	2008 R2 Enterprise	2016 Web 2012 Web/ Enterprise
Replication				
Policy management				

Note:

- **RDS for SQL Server instances already have Microsoft SQL Server licenses and do not support your own licenses.**
- **For SQL Server 2012/2016/2017, you can *submit a ticket* to apply for increasing the higher maximum number of databases.**

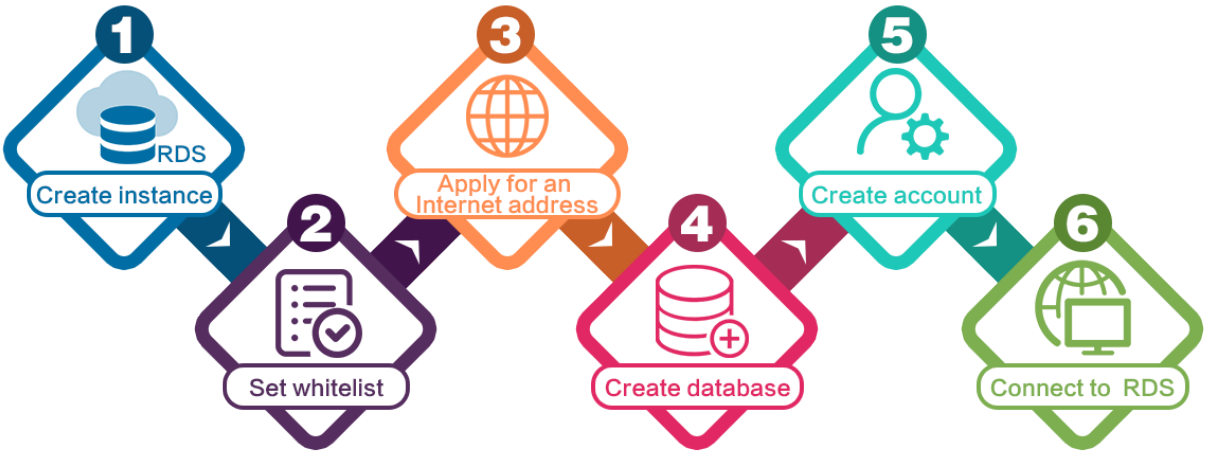
3 Quick start

3.1 General workflow to use RDS for SQL Server

This topic describes the general workflow for how to create and use an RDS for SQL Server instance.

If this is the first time that you use RDS for SQL Server, read *Limits of RDS for SQL Server* **before you purchase an RDS for SQL Server instance.**

The following flowchart shows the general workflow.



1. *Create an RDS for SQL Server instance.*
2. *Configure a whitelist for the RDS for SQL Server instance.*
3. *Apply for a public endpoint for an RDS for SQL Server instance.*
4. **Create databases and accounts for the RDS for SQL Server instance. For more information, see the following resources:**
   - *Create databases and accounts for an RDS instance in SQL Server 2017 EE*
   - *Create databases and accounts for an RDS instance in SQL Server 2017 SE, 2016, or 2012*
   - *Create databases and accounts for an RDS instance in SQL Server 2008 R2*
5. *Connect to the RDS for SQL Server instance.*

3.2 Create an RDS for SQL Server instance

This topic describes how to create an RDS for SQL Server instance through the RDS console.

For information about how to create an RDS for MySQL instance by calling an API action, see *CreateDBInstance*.

For information about the pricing of RDS for MySQL instances, see *#unique_16*.

Prerequisites

You have registered an Alibaba Cloud account.

For more information, see *Sign up with Alibaba Cloud*.

By

Precautions

- **Subscription instances cannot be converted to pay-as-you-go instances.**
- **Pay-as-you-go instances can be converted to subscription instances. For operation instructions, see** *Switch from pay-as-you-go billing to subscription billing*.
- **By default, each Alibaba Cloud account can create up to 30 pay-as-you-go RDS instances. You can** *open a ticket* **to apply for an increase to the limit.**

Procedure

1. **Log on to the** *RDS console*.
2. **On the Instances page, click Create Instance.**
3. **Select a billing method:**
   - **Pay-As-You-Go: indicates post payment (billed by hour). For short-term requirements, create pay-as-you-go instances because they can be released at any time to save costs.**
   - **Subscription: indicates prepayment. You must pay when creating an instance. For long-term requirements, create subscription instances because they are more cost-effective. Furthermore, the longer the subscription, the higher the discount.**

4. Set the following parameters.

Parameter	Description
Region	Select the region in which the RDS instance to be purchased will be located. The region cannot be changed after the instance is created. We recommend that you: · Select the same region as the corresponding ECS instance to avoid incurring charges for Internet traffic usage and guarantee fast access. · Check whether the selected region supports your required MySQL version and whether multi-zone support is available.
Database Engine	Select a DB engine. In this example, select MySQL. Note: The available DB engines vary depending on the region you select.
Version	Select a version of MySQL. You can select MySQL 5.5, 5.6, 5.7, or 8.0. Note: The available versions vary depending on the region you select.

Parameter	Description
Edition	Select an RDS edition. Valid values: · Basic: The DB system has only one instance. In this edition, computation is separated from storage, which is cost-effective. However, we recommend that you do not use this edition in production environments. · High-availability: The DB system has two instances: one master instance and one slave instance. The two instances work in a classic high-availability architecture. · Enterprise Edition: The DB system has three instances: one master instance and two slave instances. The three instances are located in three different zones in the same region to guarantee service availability. This edition is available to the China (Hangzhou), China (Shanghai), China (Shenzhen), and China (Beijing) regions.  Note: The available editions vary depending on the DB engine version you select. For information about the RDS editions, see #unique_18.
Storage Type	Select a storage type. Valid values: · Local SSD: An SSD that is located on the same node as the DB engine. Storing data to local SSDs reduces I/O latency. · Standard SSD: An elastic block storage device that is designed based on a distributed storage architecture. Storing data to cloud SSDs makes separation between computation and storage possible. · Enhanced SSD: An SSD that is designed based on the new-generation distributed block storage architecture and the 25 GB and RDMA technologies to reduce single-link latency. Each enhanced SSD can process up to 1,000,000 random read and write requests. For more information, see #unique_19.

Parameter	Description
Zone	Select a zone. A zone is a physical area within a region. Different zones in the same region are basically the same. You can deploy the master and slave instances in the same zone or in different zones. Multi-zone deployment is more secure because it provides zone-level disaster tolerance.
Network Type	Select a network type. Valid values: · Classic Network: indicates a traditional network. · VPC (recommended): short for Virtual Private Cloud. A VPC is an isolated network environment and therefore provides higher security and performance than a classic network. Note: Make sure the network type of the RDS instance is the same as that of your ECS instance so that the ECS instance can access the RDS instance through the intranet.
Type	Select an RDS instance type. The RDS instance type specifies the specifications of the RDS instance. Each type supports a specific number of CPU cores, memory size, maximum number of connections, and maximum IOPS. For more information, see *#unique_20*. Valid values: · General-purpose instance: provides dedicated memory and I/O resources, but shares the CPU and storage resources with the other general-purpose instances on the same server. · Dedicated instance: provides dedicated CPU, memory, storage, and I/O resources. · Dedicated host: provides all the CPU, memory, storage, and I/O resources on the server where it is located. For example, 8 Cores 32 GB (Basic) indicates a general-purpose instance, and 8 Cores 32 GB (Dedicated) indicates a dedicated instance.

Parameter	Description
Capacity	The capacity is used for storing data, system files, binlog files, and transaction files.

5. Optional. Set the duration of the billing method for a subscription instance and specify the number of instances to be created. Then, click Buy Now.

> **Note:**
> For a subscription instance, you can:
>
> - Select Auto Renew in the Duration section. Then the system can automatically deduct fees to extend the validity period of the instance. For example, if you purchase a three-month subscription instance with Auto Renew selected, the system automatically deducts frees of three months when the instance is about to expire.
> - Click Add to Cart and then click the cart to place the order.

6. On the Order Confirmation page, read and confirm you agree to Terms of Service, Service Level Agreement, and Terms of Use by selecting the checkbox, confirm the order details, and click Pay Now.

What to do next

Log on to the *RDS console*, select the target region, and view the instance details.

After the RDS instance is created, you must *configure whitelists* and *create accounts* for it. If you want to connect to the RDS instance through the Internet, you must also *apply for a public endpoint* for it. After all is done, you can *connect to the RDS instance*.

APIs

API	Description
#unique_21	**Used to create an RDS instance.**

3.3 Connect to an RDS for SQL Server instance

This topic describes how to connect to an RDS for SQL Server instance. After the initial configuration is complete, you can connect to your RDS instance from an ECS instance or your computer.

After you *create an instance*, *configure a whitelist*, **and create a database and an account, you can use Data Management Sevice (DMS) or a database client to connect to the RDS instance.**

Use DMS to connect to an instance

DMS is a graphical data management service provided by Alibaba Cloud. It can be used to manage non-relational databases and relational databases, and supports data and schema management, user authorization, security audit, data trends, data tracking, BI charts, and performance and optimization.

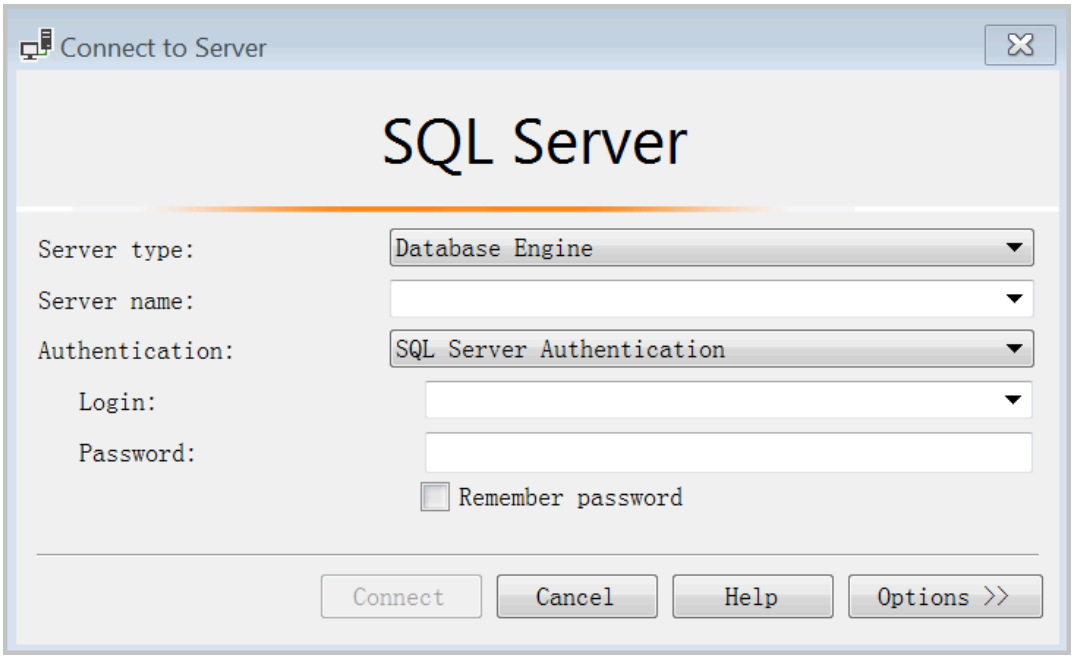
For more information, see *#unique_22*.

Use a client to connect to an instance

This topic describes how to use the Microsoft SQL Server Management Studio (SSMS) client to connect to an RDS instance.

1. **Start the SSMS client in an ECS instance or your computer.**
2. **Choose Connect > Database Engine.**

3. In the displayed Connect to Server dialog box, enter the logon information.



Parameter	Description
Server type	Select Database Engine.
Server name	Enter the connection address and the port number of the RDS instance. Separate the address and the port number with a comma (,), such as `rm-bptest.sqlserver.rds.aliyuncs.com,3433`. The following procedure shows how to view the internal and public addresses and the port number of the RDS instance: a. Log on to the *ApsaraDB for RDS console*. b. In the upper-left corner of the page, select the region where the instance is located. c. Click the ID of the instance. d. Find the internal IP address and port number, or the public IP address and port number of the instance in the Basic Information section, as shown in the following figure. 
Authentication	Select SQL Server Authentication.
Login	Enter the account name of the RDS instance.

Parameter	Description
Password	Enter the password of the account of the RDS instance.

4. Click Connect.

3.4 Configure a whitelist for an RDS for SQL Server instance

This topic describes how to configure a whitelist for an RDS for MySQL instance. After you create an RDS instance, you must configure a whitelist for it to allow external devices to access the instance.

Configuring a whitelist does not affect the normal running of your RDS instance, but only makes your RDS instance more secure. We recommend that you update the whitelists for your RDS instance on a regular basis.

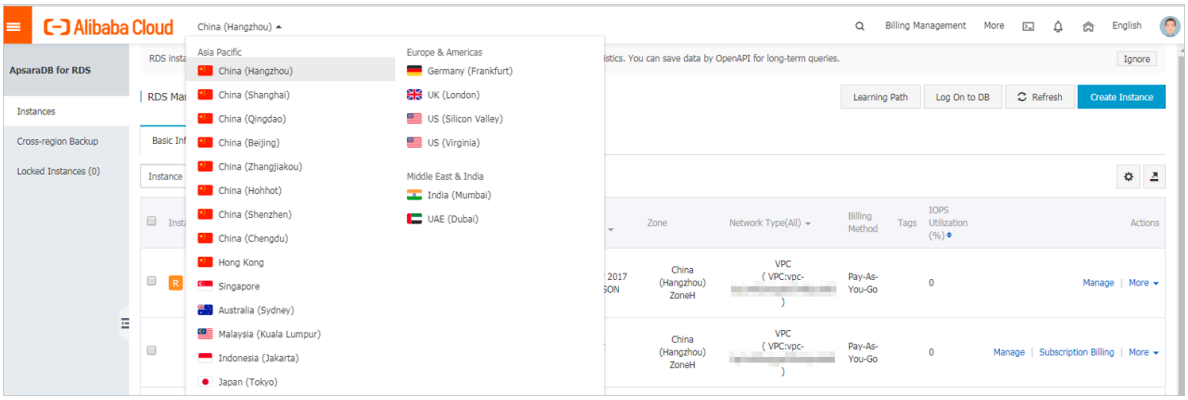
Note:
The default whitelist contains only the default IP address 127.0.0.1. Before you add new IP addresses to the whitelist, no devices can access the RDS instance.

Precautions

- The default whitelist can only be edited or cleared. It cannot be deleted.
- If you log on to DMS but your IP address has not been added to the whitelist, DMS prompts you to add the IP address and automatically generates a whitelist containing your IP address.

Procedure

1. Log on to the *RDS console*.
2. In the upper-left corner of the page, select the region where the instance is located.



3. Find the instance and click its ID.

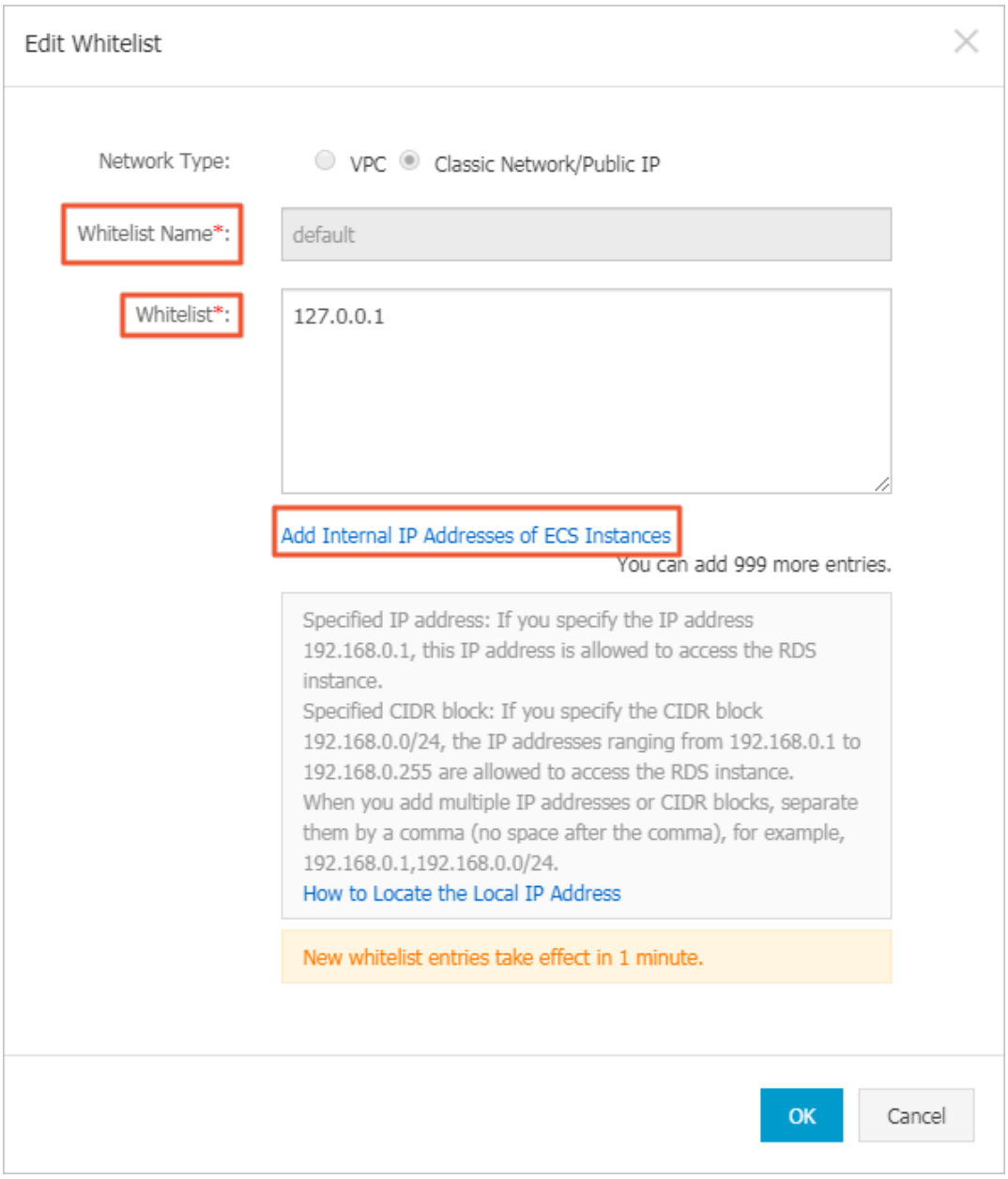
4. In the left-side navigation pane, click Data Security.
5. On the Whitelist Settings tab page, click Edit corresponding to the default whitelist.

> **Note:**
> You can click Create Whitelist to create a whitelist.

6. In the displayed Edit Whitelist dialog box, specify the IP addresses or CIDR blocks used to access the instance, and then click OK.
   - If you specify the CIDR block 10.10.10.0/24, any IP addresses in the 10.10.10.*X* format are allowed to access the RDS instance.
   - To add multiple IP addresses or CIDR blocks, separate each entry with a comma (without spaces), for example, `192.168.0.1,172.16.213.9`.
   - After you click Add Internal IP Addresses of ECS Instances, the IP addresses of all the ECS instances under your Alibaba Cloud account are displayed. You can quickly add internal IP addresses to the whitelist.

> **Note:**

After you add an IP address or CIDR block to the default whitelist, the default address 127.0.0.1 is automatically deleted.



Common errors

- **The default address 127.0.0.1 in Data Security > Whitelist Settings indicates that no device is allowed to access the RDS instance. Therefore, you must add IP addresses of devices to the whitelist to allow access to the instance.**
- **The IP address in the whitelist is set to 0.0.0.0, but the correct format is 0.0.0.0/0.**

Note:

0.0.0.0/0 indicates that all devices are allowed to access the RDS instance. Exercise caution when using this IP address.

- **The public IP address that you add to the whitelist may not be the real egress IP address. The reasons are as follows:**
  - **The public IP address is not fixed and may dynamically change.**
  - **The tools or websites used to query the public IP addresses provide wrong IP addresses.**

APIs

API	Description
#unique_23	**Used to view the IP address whitelist of an RDS instance.**
#unique_24	**Used to modify the IP address whitelist of an RDS instance.**

3.5 Creating accounts and databases

3.5.1 Create databases and accounts for an RDS instance in SQL Server 2017 EE

This topic describes how to create databases and accounts for an RDS instance in SQL Server 2017 EE. You must create a premier account through the RDS console, and then use a database client or DMS to create and manage databases.

Note:
For information about how to create accounts and databases in other SQL Server versions, see the following resources:

- *Create databases and accounts for an RDS instance in SQL Server 2017 SE, 2016, or 2012*
- *Create databases and accounts for an RDS instance in SQL Server 2008 R2*

Prerequisites

The SQL Server version is 2017 EE.

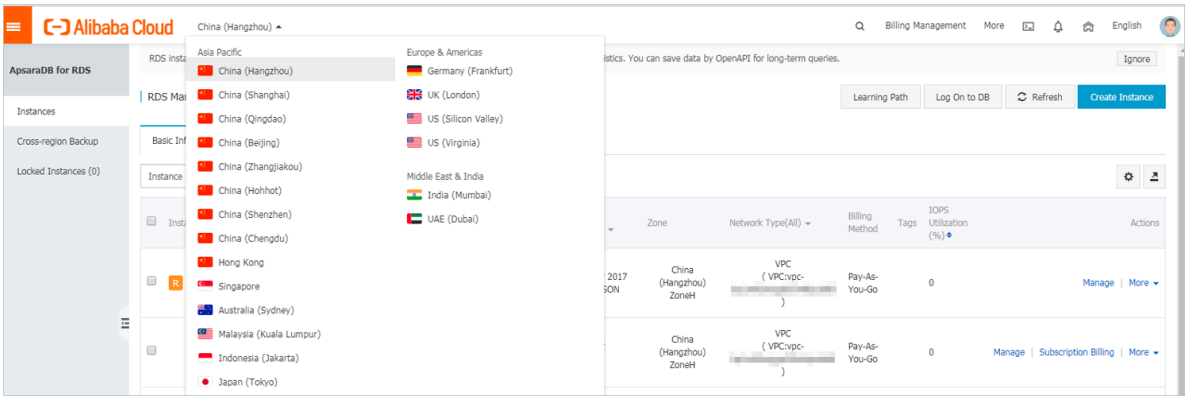
Precautions

- **Databases within the same instance share all the resources of the instance. You can manage standard accounts and databases by using SQL statements.**

- When assigning permissions to database accounts, follow the principle of least privilege and create accounts based on the roles required. Assign the appropriate level of permissions to the accounts. When necessary, you can create multiple database accounts and allow each of them to access data relevant to their own business tasks. If an account does not need to write data to a database, assign read-only permissions to the account.
- For database security, you must set strong account passwords and change the passwords regularly.

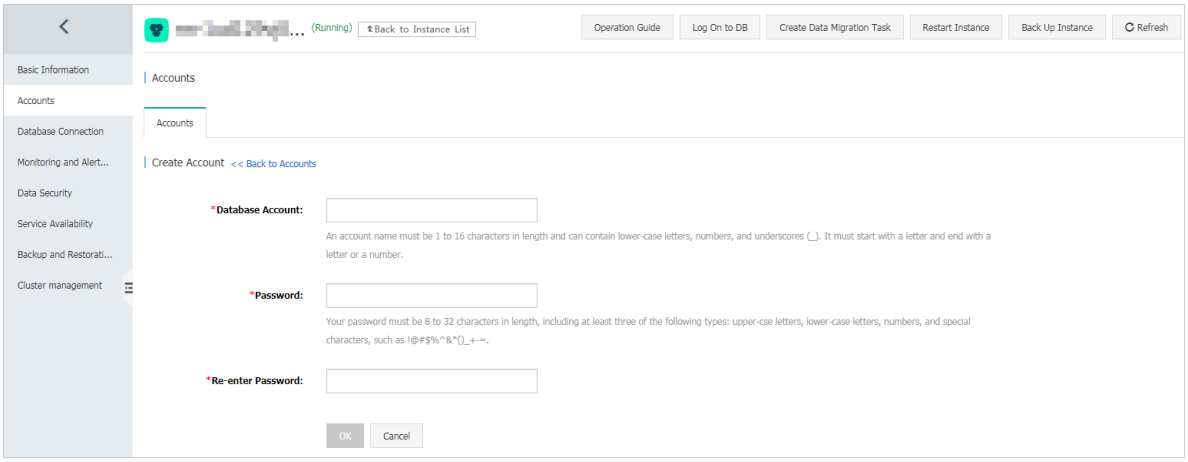
Procedure

1. Log on to the *RDS console*.
2. Select the target region.



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Accounts.
5. Click Create Initial Account.

6. Enter the account information.



Parameter description:

- Database Account: The name of the premier account. The account name must be 2 to 16 characters in length and can contain lowercase letters, numbers, and underscores (_). It must start with a letter and end with a letter or number.

  Note:
  Reserved keywords such as *test* and *root* cannot be set as account names.

- Password: The password of the premier account.
  - The password must be 8 to 32 characters in length.
  - The password must contain at least three of the following types of characters: uppercase letters, lowercase letters, numbers, and special characters.
  - The allowed special characters are as follows:

    ! @ # $ % ^ & * ( ) _ + - =

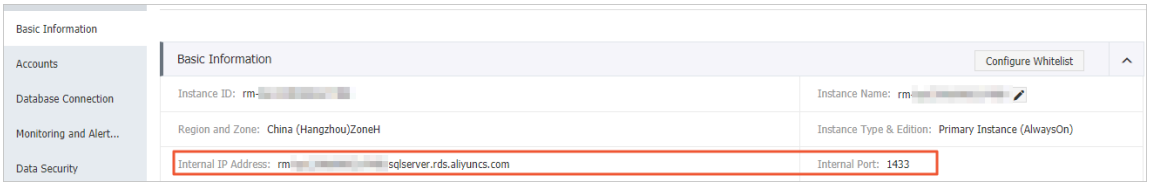
- Re-enter Password: Enter the password again.

7. Click OK.
8. Click Log On to DB in the upper-right corner to go to the RDS Database Logon page of the *Data Management Service console*.

9. Enter the correct IP address, port number, database username, and password.

   Parameter description:

   - 1: The IP address and port information of the RDS instance. You can view the IP address and port information on the Basic Information page or Database Connection page.



   - 2: The name of the account to access the database.
   - 3: The password of the account to access the database.

10. Click Log On.

> **Note:**
> If you want your browser to remember your account and password, you can select Remember Password before you click Log On.

11. If the system displays a message, asking you to add the CIDR block of the DMS server to the IP address whitelist of the RDS instance, click Set a Whitelist. For more information, see *Configure a whitelist for an RDS for SQL Server instance*.
12. After the whitelist is configured, click Log On.
13. After you have logged on to the RDS instance, choose SQL Operations > SQL Window in the top navigation bar.
14. In the SQL window, run the following statement to create a database:

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

15. Click execute.
16. In the SQL window, run the following statement to create a standard account:

```
CREATE LOGIN <login name> WITH PASSWORD = '<password>';
```

17. Click execute.

> **Note:**
> Standard accounts that are created in DMS by using T-SQL do not appear in the account list in the console. However, you can use a standard account to log on to the database.

18. In the SQL window, run the following statements to create a database user and associate the user to the standard account that you have created.

```
USE <database name>;
CREATE USER <user name> FOR LOGIN <login name>;
```

19. Click execute. The standard account can access the corresponding database.

FAQ

Can I manage the created account in the read-only instances?

The account created in the master instance is synchronized to the read-only instances. You cannot manage the account in the read-only instances. The account can only read data from the read-only instances.

APIs

API	Description
#unique_26	**Used to create an account for an RDS instance.**
#unique_27	**Used to create a database an RDS instance.**

3.5.2 Create databases and accounts for an RDS instance in SQL Server 2017 SE, 2016, or 2012

This topic describes how to create databases and accounts for an RDS instance in SQL Server 2017 SE, 2016, or 2012 through the RDS console.

Note:

For more information on how to create databases and accounts in other SQL Server versions, see the following resources:

- *Create databases and accounts for an RDS instance in SQL Server 2017 EE*
- *Create databases and accounts for an RDS instance in SQL Server 2008 R2*

Prerequisites

The SQL Server version is one of the following:

- **SQL Server 2012**
- **SQL Server 2016**
- **SQL Server 2017 SE**

Create an account

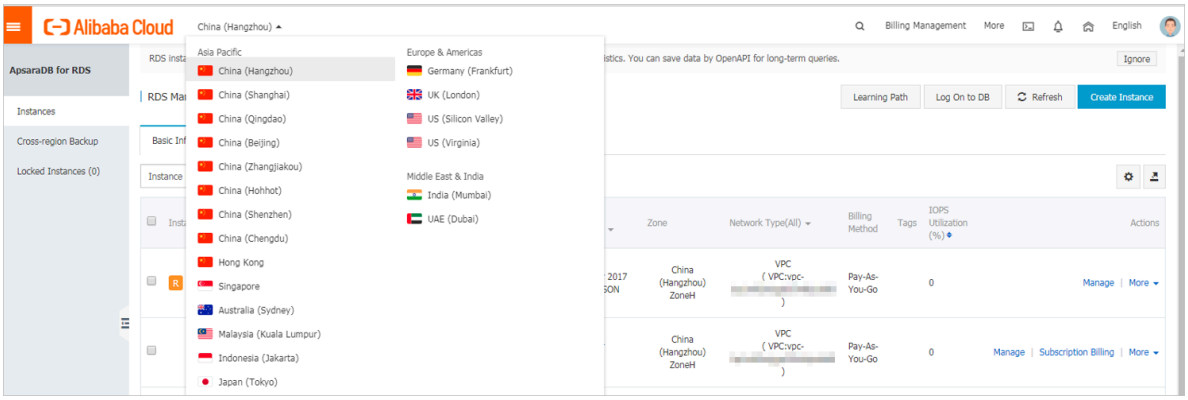
You can create a premier account and standard accounts through the RDS console. The premier account can be created only through the RDS console.

Precautions

- **When assigning permissions to database accounts, follow the principle of least privilege and create accounts based on the roles required. Assign the appropriate level of permissions to the accounts. When necessary, you can create multiple database accounts and allow each of them to access data relevant to their own business tasks. If an account does not need to write data to a database, assign read-only permissions to the account.**
- **For database security, you must set strong account passwords and change the passwords regularly.**

Procedure

1. **Log on to the *RDS console*.**
2. **Select the target region.**



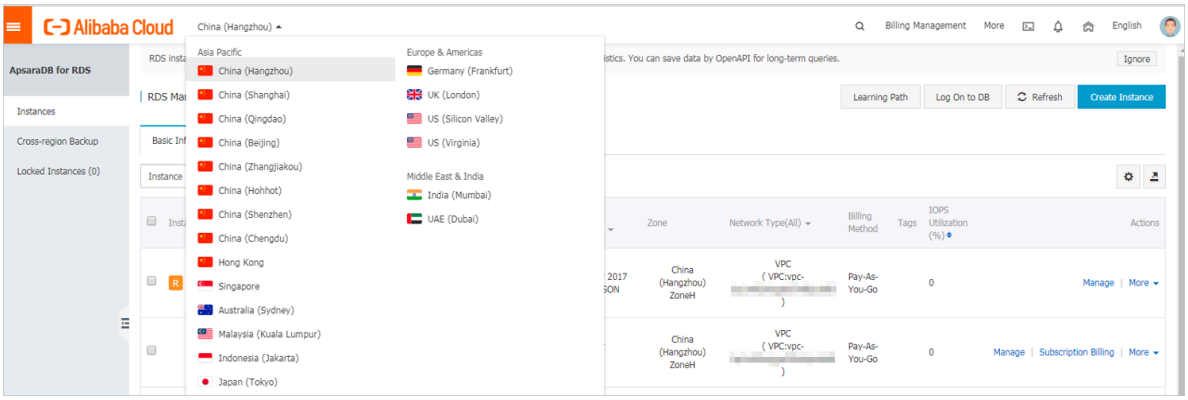
3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Accounts.**
5. **Click Create Account.**
6. **Enter the account information and click OK.**

Parameter	Description
Database Account	The account name must be 2 to 16 characters in length and can contain lowercase letters, numbers, and underscores (_). It must start with a letter and end with a letter or number.

Parameter	Description
Account Type	· Superuser Account: This option is available only when you create an account for the first time. You can create standard accounts only after you create a premier account. Each instance has only one premier account and this premier account cannot be deleted. · Standard Account: This option is available only after you create a premier account. One instance can have multiple standard accounts. You must assign database permissions to standard accounts manually.
Password	The account password must be 8 to 32 characters in length and contain at least three of the following types of characters: uppercase letters, lowercase letters, numbers, and special characters. The allowed special characters are as follows: ! @ # $ % ^ & * ( ) _ + - =
Re-enter password	Enter the password again.
Description	Optional. Enter details about the database to better identify it. You can enter up to 256 characters.

Create a database

1. Log on to the *RDS console*.
2. Select the target region.



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Databases.
5. Click Create Database.

6. Set the following parameters and click OK.

Parameter	Description
Database Name	The database name must be 2 to 64 characters in length and can contain lowercase letters, numbers, underscores (_), and hyphens (-). It must start with a letter and end with a letter or number.
Supported Character Set	Select a character set. If the character set you need is not listed, click All and select it from the drop-down list.
Authorized Account	Select the account to which you want to assign permissions. After you select an account, the Account Type parameter is displayed and you can set it to Read/Write, Read-only, or Owner. If no accounts have been created, you can leave the Authorized Account parameter blank.
Remarks	Optional. Enter details about the database to better identify it. You can enter up to 256 characters.

APIs

API	Description
#unique_26	Used to create an account for an RDS instance.
#unique_27	Used to create a database for an RDS instance.

3.5.3 Create databases and accounts for an RDS instance in SQL Server 2008 R2

This topic describes how to create databases and accounts for an RDS instance in SQL Server 2008 R2 through the RDS console.

Note:
For more information on how to create databases and accounts in other SQL Server versions, see the following resources:

- *Create databases and accounts for an RDS instance in SQL Server 2017 EE*
- *Create databases and accounts for an RDS instance in SQL Server 2017 SE, 2016, or 2012*

Prerequisites

The SQL Server version is 2008 R2.

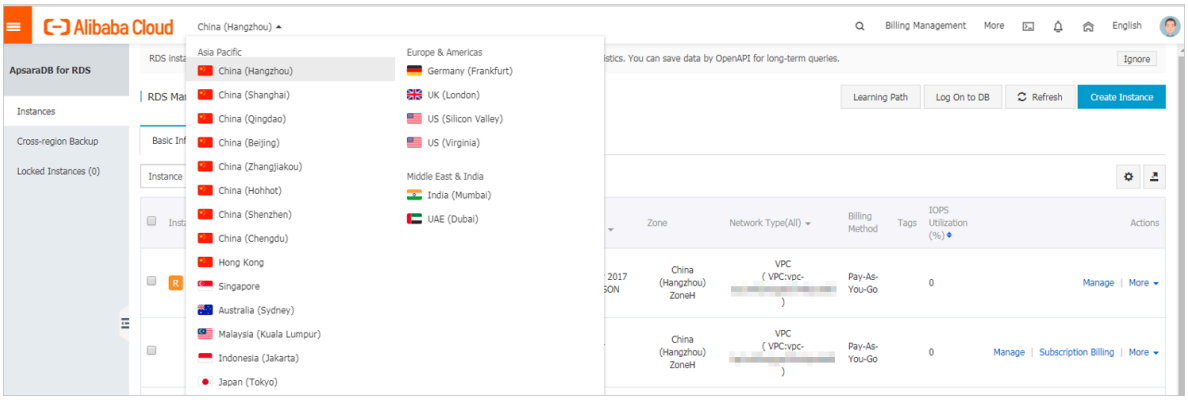
Create an account

Precautions

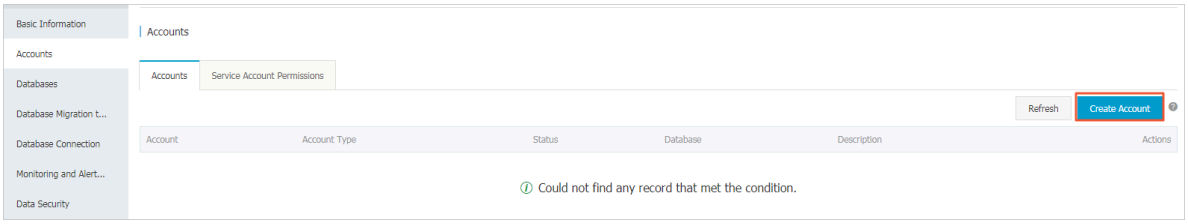
- To migrate data from an on-premises database to RDS, you must create databases and accounts that are the same as those of the on-premises database.
- When assigning permissions to database accounts, follow the principle of least privilege and create accounts based on the roles required. Assign the appropriate level of permissions to the accounts. When necessary, you can create multiple database accounts and allow each of them to access data relevant to their own business tasks. If an account does not need to write data to a database, assign read-only permissions to the account.
- For database security purposes, set strong passwords for the accounts and change the passwords regularly.

Procedure

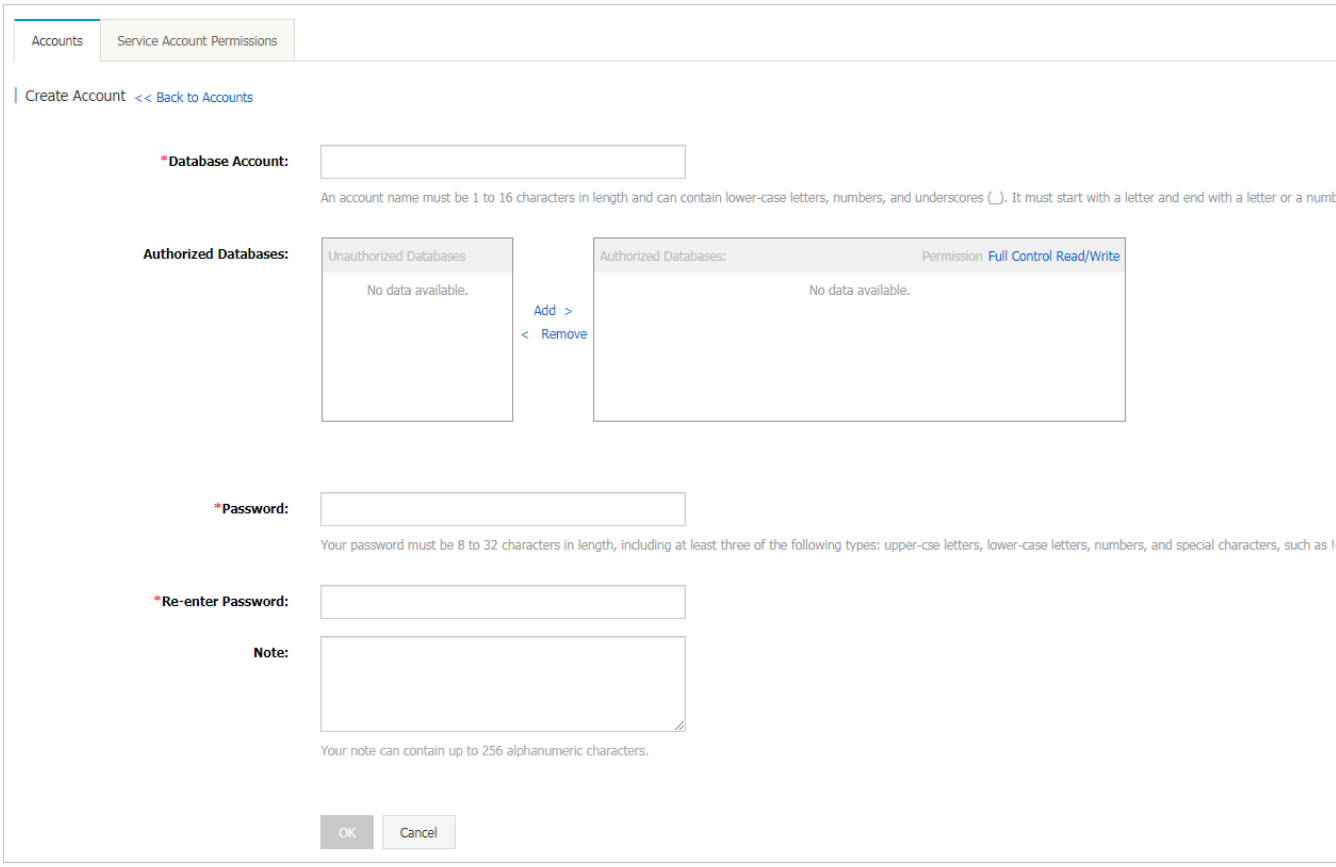
1. Log on to the *RDS console*.
2. Select the target region.



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Accounts.
5. Click Create Account.



6. Enter the account information.



Parameter	Description
Database Account	The account name must be 2 to 16 characters in length and can contain lowercase letters, numbers, and underscores (_). It must start with a letter and end with a letter or number.

Parameter	Description
Authorized Databases	Select the databases for which the account has permissions. If no databases have been created, you can leave this parameter blank. An account can be authorized with multiple databases. To authorize an account to databases, follow these steps: a. In the left area, select the target databases. b. Click Add to add the selected databases to the right area. c. Set the account's permission on each database, which can be Read/Write or Read-only. You can also click the button (for example, Full Control Read-only) in the upper-right corner to set the permissions for the databases in batches. 
Password	The account password must be 8 to 32 characters in length and contain at least three of the following types of characters : uppercase letters, lowercase letters, numbers, and special characters. The allowed special characters are as follows: ! @ # $ % ^ & * ( ) _ + - =
Re-enter Password	Enter the password again.
Remarks	Optional. Enter details about the account to better identify it. You can enter up to 256 characters.

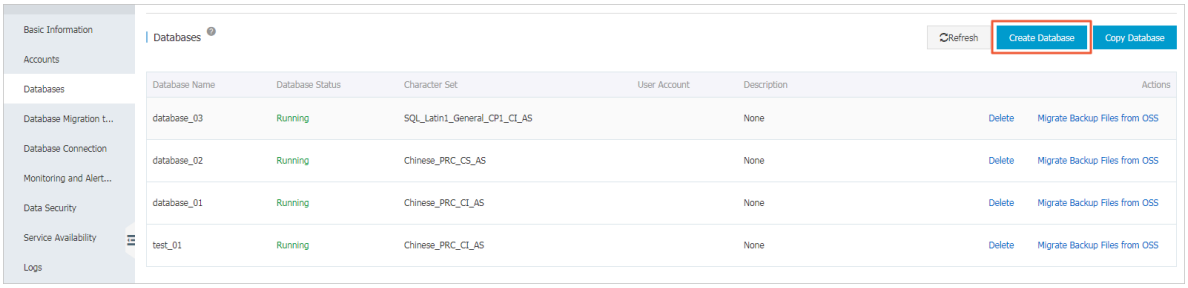
7. Click OK.

Create a database

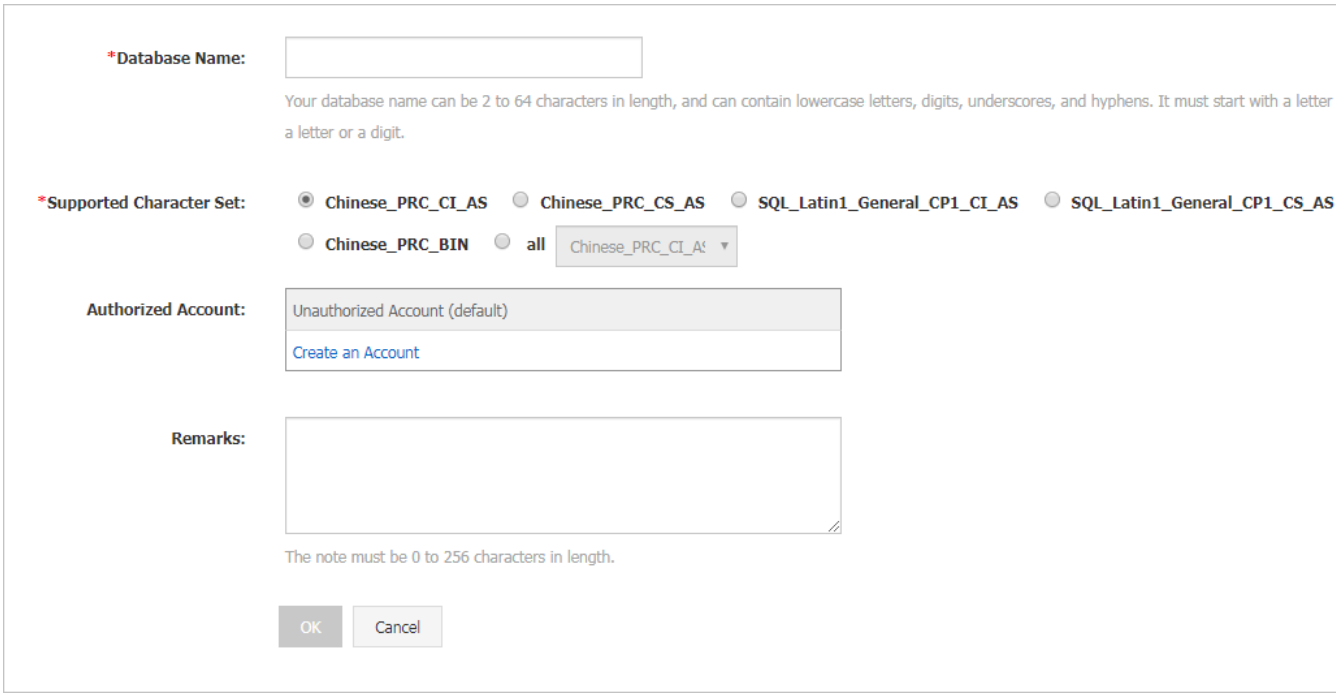
You can create up to 300 databases for an RDS for SQL Server 2008 R2 instance.

1. Log on to the *RDS console*.
2. Select the target region.
3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Databases.

5. Click Create Database.



6. Enter the database information.



Parameter	Description
Database Name	The database name must be 2 to 64 characters in length and can contain lowercase letters, numbers, underscores (_), and hyphens (-). It must start with a letter and end with a letter or number.
Supported Character Set	Select a character set. If the character set you need is not listed, click All and select it from the drop-down list.
Authorized Account	Select the account to which you want to assign permissions. If no accounts have been created, you can leave this parameter blank.
Account Type	This parameter is displayed after you select an authorized account. You can set this parameter to Read/Write or Read-only.
Remarks	Optional. Enter details about the database to better identify it. You can enter up to 256 characters.

7. Click OK.

Resources

#unique_28

APIs

API	Description
#unique_26	Used to create an account for an RDS instance.
#unique_27	Used to create a database for an RDS instance.

3.6 Read-only instances

3.6.1 Introduction to SQL Server read-only instances

This topic introduces SQL Server read-only instances. If your application initiates a small number of write requests but a large number of read requests, a single instance may not be able to resist the read pressure. As a result, services 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 and increase the application throughput.

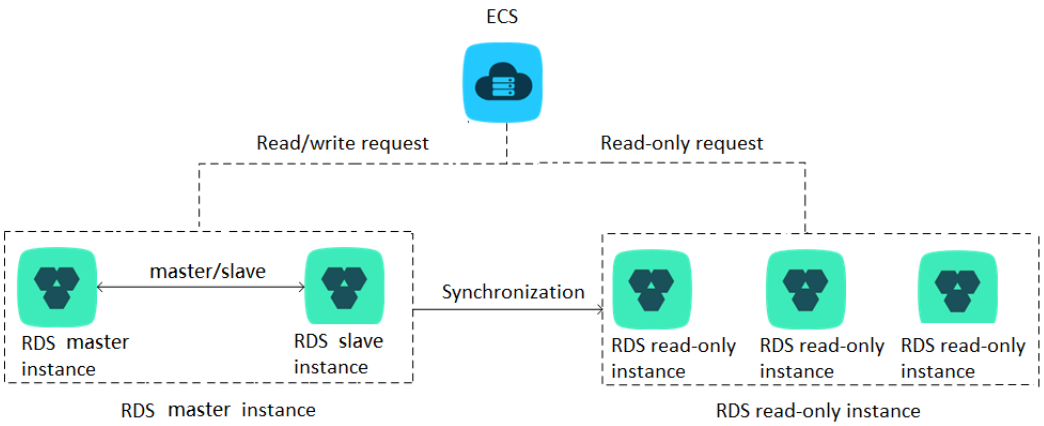
Overview

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.

Note:

- **For RDS SQL Server, only the SQL Server 2017 Cluster (AlwaysOn) Edition supports read-only instances.**
- **Each read-only instance adopts a single-node architecture (without slave nodes).**

The following topology shows the positioning of the read-only instance.



Pricing

The billing method of read-only instances is Pay-As-You-Go. The following table lists the prices of common instances.

Hourly prices of specifications and storage

Region	rds.mssql.s2.large 2-core 4 GB	rds.mssql.s2.xlarge 2-core 8 GB	rds.mssql.s3.large 4-core 8 GB	rds.mssql.m1.medium 4-core 16 GB	rds.mssql.c1.large 8-core 16 GB	rds.mssql.c1.xlarge 8-core 32 GB	rds.mssql.c2.xlarge 16-core 64 GB	Storage
China mainland's regions	$0.225	$0.447	$0.459	$0.851	$0.888	$1.732	$3.389	$0.0003/GB
China (Hong Kong)	$0.264	$0.522	$0.537	$0.993	$1.035	$2.02	$3.954	$0.0004/GB
US (Virginia)	$0.273	$0.542	$0.556	$1.028	$1.072	$2.093	$4.096	$0.0003/GB
US (Sillicon Vally)	$0.292	$0.579	$0.595	$1.099	$1.146	$2.237	$4.378	$0.0003/GB
Singapore	$0.311	$0.616	$0.632	$1.170	$1.220	$2.381	$4.661	$0.0004/GB

Region	rds.mssql.s2.large 2-core 4 GB	rds.mssql.s2.xlarge 2-core 8 GB	rds.mssql.s3.large 4-core 8 GB	rds.mssql.m1.medium 4-core 16 GB	rds.mssql.c1.large 8-core 16 GB	rds.mssql.c1.xlarge 8-core 32 GB	rds.mssql.c2.xlarge 16-core 64 GB	Storage
Australia	$0.315	$0.622	$0.646	$1.209	$1.259	$2.415	$4.829	$0.0005/GB
Malaysia	$0.296	$0.586	$0.601	$1.112	$1.159	$2.262	$4.428	$0.0004/GB
Indonesia	$0.311	$0.616	$0.632	$1.170	$1.220	$2.381	$4.661	$0.0004/GB
Japan	$0.311	$0.615	$0.632	$1.171	$1.221	$2.381	$4.660	$0.0005/GB
Germany (Frankfurt)	$0.311	$0.615	$0.632	$1.171	$1.221	$2.381	$4.660	$0.0005/GB
UK (London)	$0.311	$0.615	$0.632	$1.171	$1.221	$2.381	$4.660	$0.0005/GB
UAE (Dubai)	$0.327	$0.646	$0.665	$1.230	$1.283	$2.500	$4.895	$0.0007/GB
India (Mumbai)	$0.296	$0.586	$0.601	$1.112	$1.159	$2.262	$4.428	$0.0004/GB

Features

Read-only instances offer the following features:

- **Account and database management: No account or database maintenance is required for a read-only instance. Both the account and database are synchronized through the master instance.**
- **Billing: Read-only instances support billing measured per hour, which is user-friendly and cost-efficient.**
- **Specifications: The specifications of a read-only instance can differ from those of the master instance, and can be changed at any time. We recommend that**

the specifications of the read-only instance be equal to or higher than those of the master instance; otherwise the read-only instance may have high latency or workloads.

- **Network type: can differ from that of the master instance.**
- **Whitelist: When a read-only instance is created, it automatically copies the whitelist of the master instance. However, the whitelist of the read-only instance is independent from that of the master instance. You can modify the whitelist of the read-only instance by referring to** *Configure a whitelist for an RDS for SQL Server instance***.**
- **Monitoring and alarms: 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.**

Limits

- **Quantity of read-only instances:**

Database	Quantity
SQL Server	Up to 7 read-only instances can be created for each master instance.

- **Read-only instances do not support backup settings or manual backup.**
- **Instance recovery:**
  - **Read-only instances do not support the creation of temporary instances through backup files or a 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.**

FAQ

Can the accounts on the master instance be used on the read-only instances?

Accounts on the master instance are synchronized to the read-only instances. You can use the accounts to read data from the read-only instances but cannot write data into the read-only instances.

3.6.2 Create an RDS for SQL Server read-only instance

This topic describes how to create read-only instances for an RDS for SQL Server master instance to handle a large number of read requests and increase the application throughput. A read-only instance is a read-only replica of the master instance. Changes to the master instance are automatically synchronized to all read-only instances attached to the master instance.

For more information, see *Introduction to SQL Server read-only instances*.

Prerequisites

The master instance adopts the Cluster Edition and runs the SQL Server 2017 engine.

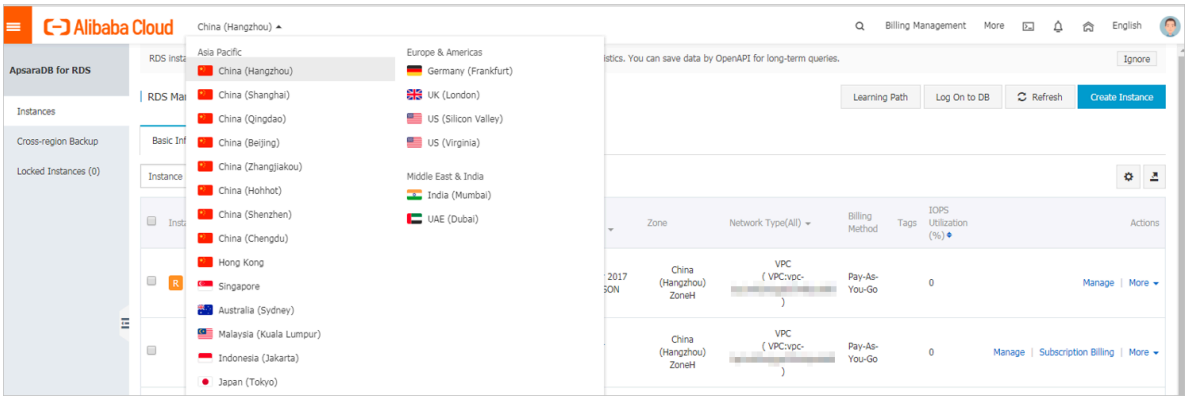
Precautions

- **You can only create read-only instances under the master instance but cannot switch an existing instance to a read-only instance.**
- **Creating a read-only instance does not affect the master instance because the read-only instance copies data from the slave instance.**
- **You can create up to seven read-only instances for the master instance.**
- **A read-only instance is charged according to the Pay-As-You-Go billing method. That is, fees are deducted once per hour, and the deducted fees vary depending on the specifications of the read-only instance at the time of fee deduction. For more information, see the "Pricing" section in** *Introduction to SQL Server read-only instances*.

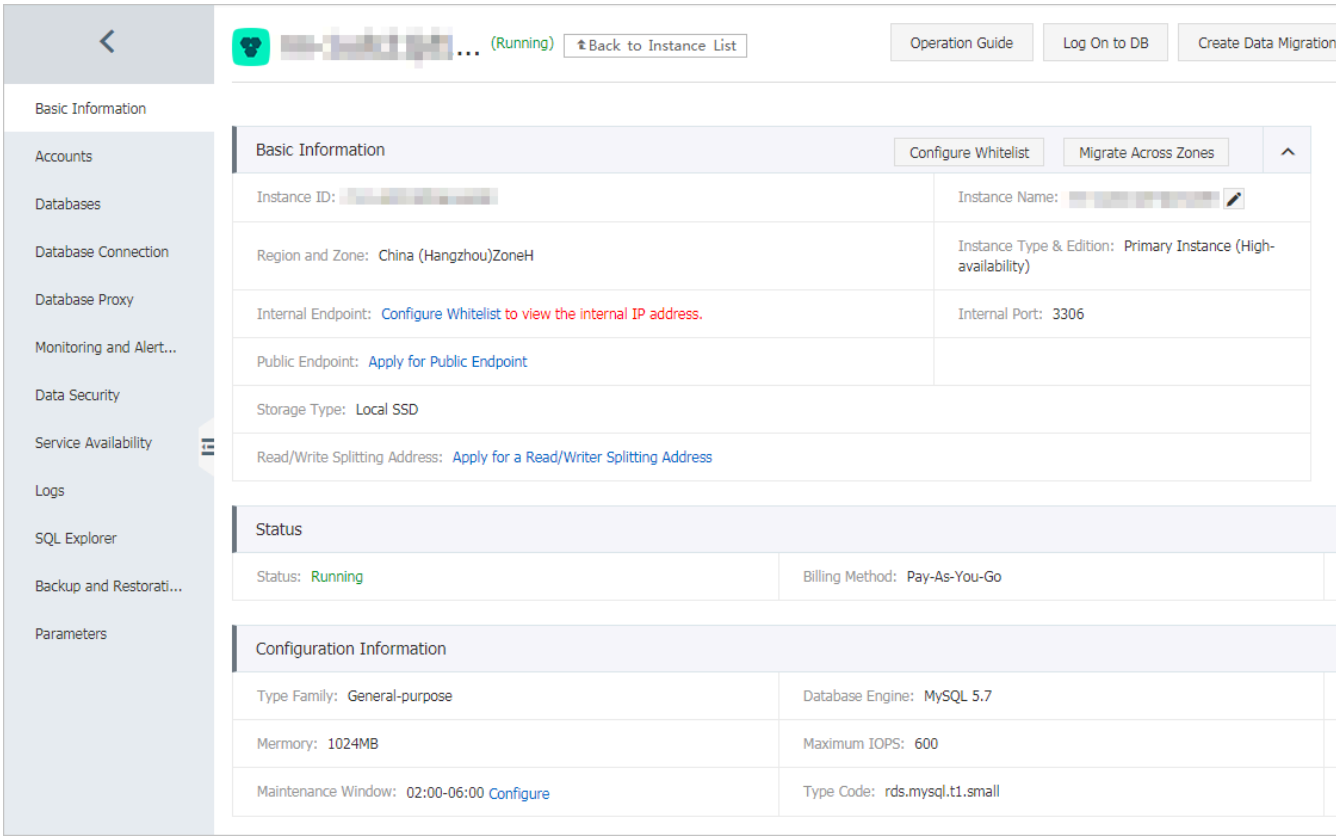
Create a read-only instance

1. **Log on to the** *RDS console*.

2. In the upper-left corner, select the region where the target instance is located.



3. Find the target instance and click the instance ID.
4. Click Add Read-only Instance.



5. On the purchase 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 greater than or equal to that of the master instance.
- We recommend that you purchase multiple read-only instances based on your business needs to improve availability.

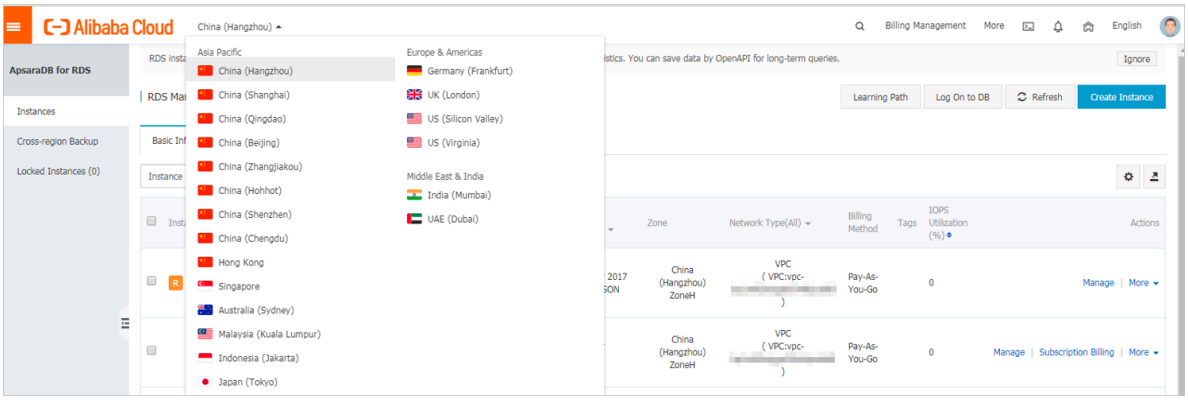
6. On the Order Confirmation page, review the order information, select the terms and agreements as prompted, click Pay Now, and complete the payment.

   The instance creation takes a few minutes.

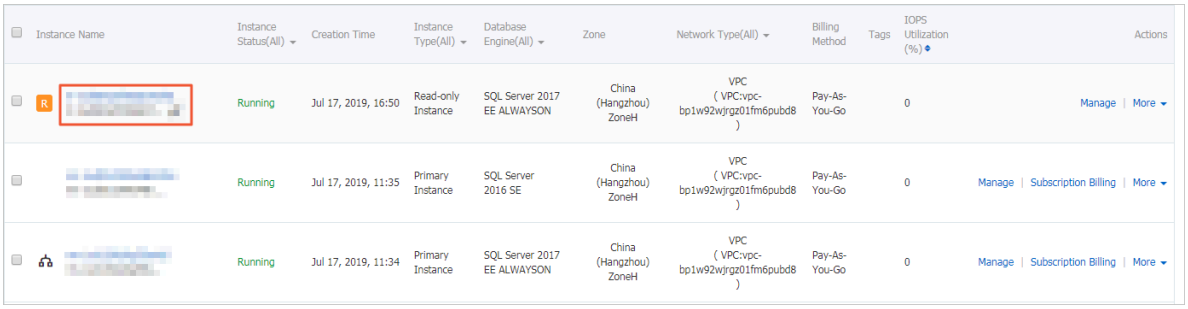
View a read-only instance

View a read-only instance in the instance list

1. Log on to the *RDS console*.
2. Select the region where the read-only instance is located.



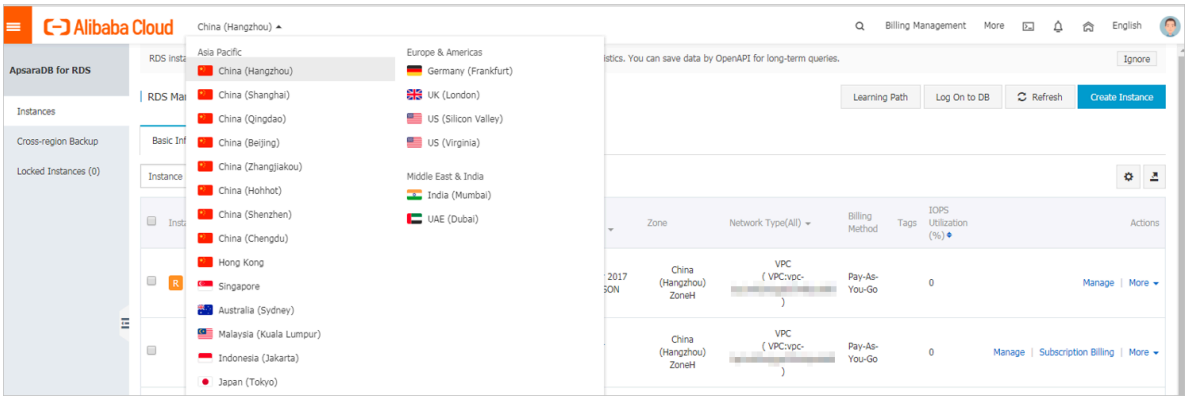
3. In the instance list, find the read-only instance and click its ID.



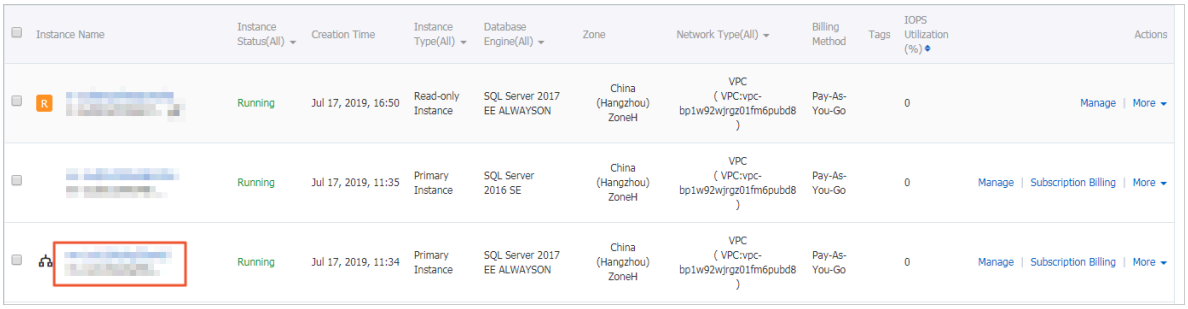
View a read-only instance on the Basic Information page for the master instance

1. Log on to the *RDS console*.

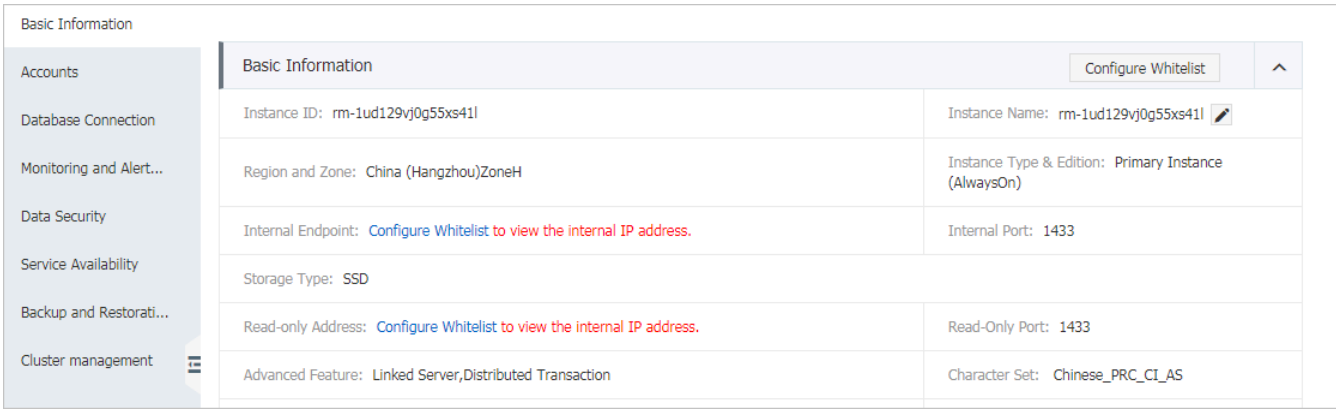
2. **Select the region where the master instance is located.**



3. **In the instance list, find the master instance and click its ID.**



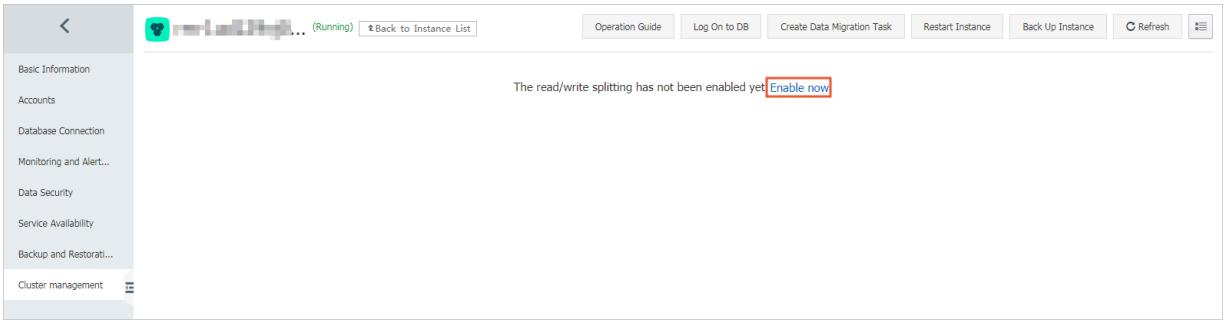
4. **On the Basic Information page of the master instance, move the pointer over the number below Read-only Instance and click the ID of the read-only instance.**



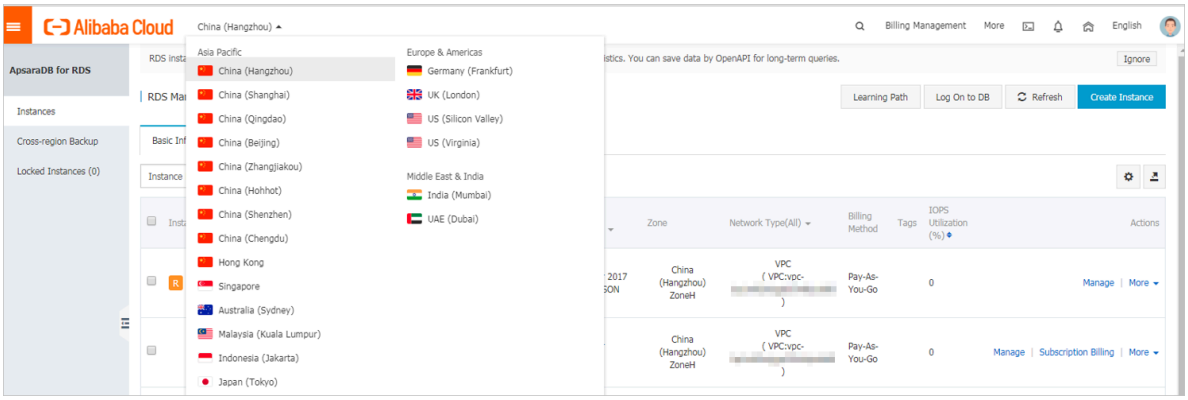
View a read-only instance on the Cluster management page

Prerequisites

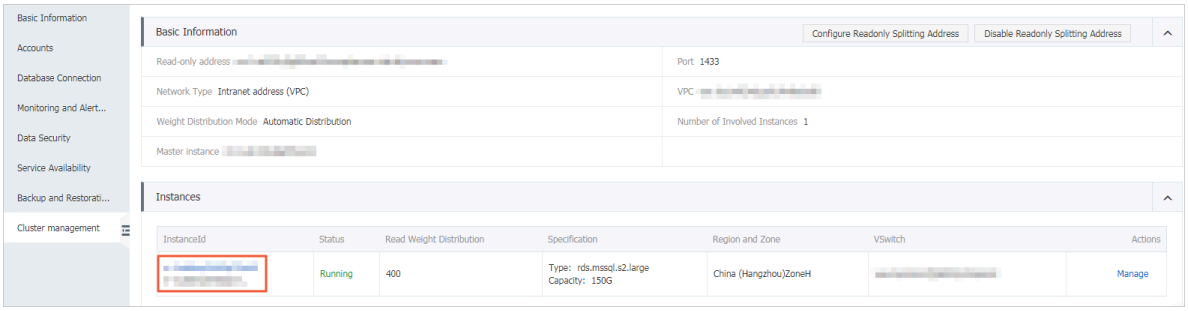
You have enabled read/write splitting on the Cluster management page. For more information, see *#unique_32*.



1. **Log on to the *RDS console*.**
2. **Select the region where the master instance is located.**

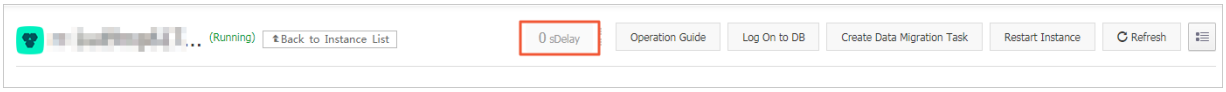


3. **In the instance list, find the master instance and click its ID.**
4. **In the left-side navigation pane, click Cluster management.**
5. **Find the read-only instance and click its ID.**



View the delay time of a read-only instance

When a read-only instance synchronizes data from the master instance, the read-only instance may lag behind the master instance by a small amount of time. You can view the delay on the Basic Information page of the read-only instance.



APIs

API	Description
#unique_33	Used to create an RDS read-only instance.

3.7 Functions supported by different versions and editions of SQL Server

This topic describes the functions supported by different versions and editions of SQL Server.

Basic functions

Module	Function	High-availability editions		Basic editions
		2017 Standard 2016 Standard/ Enterprise 2012 Standard/ Enterprise	2008 R2 Enterprise	2016 Web 2012 Web 2012 Enterprise
Life cycle	Create an instance	Supported	Supported	Supported
	Restart an instance			
	Automatic renewal			
	Change the billing method			
	Change specifications			
	Release an instance			
	Create a temporary instance	Not supported	Supported	Supported

Module	Function	High-availability editions		Basic editions
		2017 Standard 2016 Standard/ Enterprise 2012 Standard/ Enterprise	2008 R2 Enterprise	2016 Web 2012 Web 2012 Enterprise
	Upgrade the engine version	Coming soon	Supported	Coming soon
	Clone an instance	Supported	Not supported	Supported
	Create a read-only instance	Not supported	Not supported	Not supported
Instance properties	View a list of instances	Supported	Supported	Supported
	View instance details			
	Edit instance description			
	Set the maintenance time period			
	Manage instance labels			
	Migrate to another zone	Not supported	Supported	Not supported
Database connection	VPC address	Supported	Supported	Supported
	Public network address			
	Read/write splitting address	Not supported	Not supported	Not supported

Module	Function	High-availability editions		Basic editions
		2017 Standard 2016 Standard/ Enterprise 2012 Standard/ Enterprise	2008 R2 Enterprise	2016 Web 2012 Web 2012 Enterprise
Service availability	Disaster recovery in a zone	Supported	Supported	Supported
	Cross-zone disaster recovery	Supported	Supported	Not supported
	Cross-region disaster recovery	Not supported	Not supported	Not supported
	Disaster recovery drill			
Backup and restore	Full backup	Supported	Supported	Supported
	Incremental backup			
	Log backup			
	Customize backup policies			
	Restore from a backup set			
	Restore to time			
	Restore from external backup files	Supported (full backup, differential backup, or log backup)	Supported (full backup)	Supported (full backup, differential backup, or log backup)
	Restore to a clone instance	Supported	Not supported	Coming soon

Module	Function	High-availability editions		Basic editions
		2017 Standard 2016 Standard/ Enterprise 2012 Standard/ Enterprise	2008 R2 Enterprise	2016 Web 2012 Web 2012 Enterprise
	Partial backup	Supported	Not supported	Not supported
	Partial restore			
Monitoring and alarms	Resource monitoring	Supported	Supported	Supported
	Engine monitoring			
	Customize monitoring policies			
	Aggregate monitoring items			
Parameter management	Parameter update	Supported (T-SQL)	Supported	Supported (T-SQL)
	Parameter template			
Log management	Error logs	Supported (T-SQL)	Supported	Supported (T-SQL)
	Running logs			

Data management functions

Module	Function	High-availability editions		Basic editions
		2017 Standard 2016 Standard/ Enterprise 2012 Standard/ Enterprise	2008 R2 Enterprise	2016 Web 2012 Web 2012 Enterprise
Data management	User management	Supported (T-SQL)	Supported	Supported (T-SQL)
	Databases and table management		Supported (T-SQL)	
	Table operations			
	Task scheduling			
Data tunnel	Homogeneous data migration	Supported (DTS)	Supported (DTS)	Supported (DTS)
	Heterogeneous data migration			
	Data synchronization			
	Data subscription	Not supported	Not supported	Not supported
	Database replication between instances	Supported	Not supported	Supported
Data security	IP address whitelist	Supported	Supported	Supported

Module	Function	High-availability editions		Basic editions
		2017 Standard 2016 Standard/ Enterprise 2012 Standard/ Enterprise	2008 R2 Enterprise	2016 Web 2012 Web 2012 Enterprise
	Management and operation audit			
	Firewall	Supported (IP address whitelist)	Supported (IP address whitelist)	Supported (IP address whitelist)
	Database audit	Supported	Supported	Supported
	Storage encryption	Not supported	Supported	Not supported
	Network encryption	Not supported	Supported	Not supported
	Security group management	Not supported	Not supported	Not supported
Performance optimization	Professional service	Supported	Supported	Supported
	Resource analysis	Not supported	Not supported	Not supported
	Engine analysis			
	Engine/code optimization			

Functions supported by official editions

The following table describes the functions supported by SQL Server Web, Standard, and Enterprise editions.

Function	Web Edition	Standard Edition	Enterprise Edition
Specifications	16-core 64 GB	24-core 128 GB	None
High availability	Single host	Mirror HA	Always On availability
Data compression	Not supported	Supported	Supported
SQL Profiler			
Column-based index			
Table/index partitioning		Supported by SQL Server 2016 but not by SQL Server 2012	
CDC			
Online DDL		Not supported	
Parallel queries			
Adjust parallelism of partitioned tables			
TDE			
Advanced R integration			

- For more information about functional differences between SQL Server 2016 editions (Web, Standard, or Enterprise), see *Editions and supported features of SQL Server 2016*.
- For more information about functional differences between SQL Server 2012 editions (Web, Standard, or Enterprise), see *Features Supported by the Editions of SQL Server 2012*.
- For more information about functional differences between SQL Server editions, written by Alibaba Cloud engineers, see *Addressing Key Business Needs Efficiently and Cost -Effectively with Different Editions of ApsaraDB For SQL Server*.

3.8 Stored procedures

This topic describes the stored procedures supported by the following SQL Server versions: SQL Server 2012, SQL Server 2016, and SQL Server 2017.

- *Copy a database in an instance*
- *Bring a database online*

- *Set global database privileges*
- *Delete a database*
- *Set change tracking*
- *Enable change data capture*
- *Disable change data capture*
- *Configure instance parameters*
- *Add a linked server*
- *Set a trace flag*
- *Rename a database*

Copy a database in the instance

T-SQL:

sp_rds_copy_database

Supported editions:

- **High-Availability Edition**
- **Basic Edition**

Description:

Copies a database in an instance.

Note:
The remaining storage capacity of the instance must be at least 1.3 times the database size.

Method:

```
EXEC sp_rds_copy_database 'testdb','testdb_copy'
```

- **The first parameter represents the source database.**
- **The second parameter represents the target database.**

Bring a database online

T-SQL:

sp_rds_set_db_online

Supported editions:

- **High-availability Edition**
- **Basic Edition**

Description:

After you bring a database offline, you cannot directly bring it online by running the ALTER DATABASE statement. Use this stored procedure to bring a database online.

Method:

```
EXEC sp_rds_set_db_online 'db'
```

The parameter represents the database to be brought online.

Set global database privileges

T-SQL:

sp_rds_set_all_db_privileges

Supported editions:

- **High-Availability Edition**
- **Basic Edition**

Description:

Grants the privileges of all or multiple databases to a user.

Note:
Your current database privileges must be higher or equal to the privileges you want to grant.

Method:

```
sp_rds_set_all_db_privileges 'user','db_owner','db1,db2...'
```

- **The first parameter represents the user to whom you want to grant privileges.**
- **The second parameter represents the database role to be granted to the user.**
- **The third parameter represents the databases. You can specify one or more databases, and separate multiple database databases with commas (,). (If the parameter is left blank, it indicates all user databases.)**

Delete a database

T-SQL:

sp_rds_drop_database

Supported editions:

High-Availability Edition

Note:
The Basic Edition currently does not support this stored procedure. For the Basic Edition, you can delete a database by running `DROP DATABASE db` .

Description:

Delete a database from the instance. Dependent objects will be deleted when a database is deleted. The High-Availability Edition automatically deletes the mirror and terminates the database connection.

Method:

```
EXEC sp_rds_drop_database 'db'
```

The parameter represents the database to be deleted.

Set change tracking

T-SQL:

sp_rds_change_tracking

Supported editions:

High-Availability Edition

Description:

Sets change tracking for the database.

Method:

```
EXEC sp_rds_change_tracking 'db',1
```

- **The first parameter represents the database name.**
- **The second parameter indicates whether change tracking is enabled.**
  - **1: Enable.**
  - **0: Disable.**

Enable change data capture (CDC)

T-SQL:

sp_rds_cdc_enable_db

Supported editions:

High-Availability Edition

Note:
If mirroring exists, this stored procedure also removes the availability group. In this case, this stored procedure is not recommended.

Description:

Enables change data capture.

Method:

```
USE db
GO
sp_rds_cdc_disable_db
```

Disables change data capture

T-SQL:

sp_rds_cdc_disable_db

Supported editions:

High-Availability Edition

Note:
If mirroring exists, this stored procedure also removes the availability group. In this case, this stored procedure is not recommended.

Description:

Disables change data capture.

Method:

```
USE db
```

```
GO
sp_rds_cdc_disable_db
```

Configure instance parameters

T-SQL:

sp_rds_configure

Supported editions:

- **High-availability Edition**
- **Basic Edition**

Description:

Sets instance parameters. If your instance has primary and secondary nodes, the configuration is automatically synchronized from the primary node to the secondary node.

Parameters currently supported:

- **fill factor (%)**
- **maximum worker threads**
- **cost threshold for parallelism**
- **max degree of parallelism**
- **min server memory (MB)**
- **max server memory (MB)**
- **blocked process threshold (s)**

Method:

```


EXEC sp_rds_configure 'max degree of parallelism',4
```

- **The first parameter represents the instance parameters to be set.**
- **The second parameter represents the instance parameter value.**

Add a linked server

T-SQL:

sp_rds_add_linked_server

Supported editions:

- **SQL Server 2012/2016 Standard Edition High-Availability series**
- **SQL Server 2012/2016 Enterprise Edition High-Availability series**

Description:

Adds a linked server to the instance. Supports distributed transactions. The linked server created for both the primary and secondary nodes. If a switchover occurs, you do not need to add the link server again.

Method:

```
DECLARE
@linked_server_name sysname = N'yangzhao_slb',
@data_source sysname = N'****.sqlserver.rds.aliyuncs.com,3888', --
style: 10.1.10.1,1433
@user_name sysname = N'ay15' ,
@password nvarchar(128) = N'******',
@source_user_name sysname = N'test',
@source_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,
@source_user_name,
@source_password,
@link_server_options
```

Set a trace flag

T-SQL:

sp_rds_dbcc_trace

Supported editions:

- **High-availability Edition**
- **Basic Edition**

Description:

Sets trace flags for the instance. Only partial trace flags are currently supported. If your instance has primary and secondary nodes, the trace flags are automatically synchronized from the primary node to the secondary node.

Method:

```
EXEC sp_rds_dbcc_trace '1222',1/0
```

- **The first parameter represents the trace flag.**
- **The second parameter indicates whether the trace flag is enabled or disabled.**
  - **1: Enable.**
  - **0: Disable.**

Rename a database

T-SQL:

sp_rds_rename_database

Supported editions:

Basic Edition

Description:

Renames a database.

Note:
This stored proceudre does not rename the physical database file.

Method:

```
EXEC sp_rds_rename_database 'db','new_db'
```

- **The first parameter represents the database to be renamed.**
- **The second parameter represents the new name of the database.**

4 Data migration

4.1 Integrate data

You can integrate data by using Data Integration. *Data Integration* **is a reliable, secure, cost-effective, and scalable data synchronization platform provided by Alibaba Group to integrate data across heterogeneous data storage systems. It provides offline (full/incremental) data access channels in different network environments for more than 20 data sources. You can use Data Integration to import data from and export data to ApsaraDB for RDS. For more information, see** *Supported data sources*.

5 Billing

5.1 Switch from pay-as-you-go billing to subscription billing

This topic describes how to change the billing method of an RDS for PPAS instance from pay-as-you-go to (monthly or annual) subscription.

Impacts

Changing the billing method does not interrupt the running of your RDS instance.

Precautions

- **You cannot change the billing method of an RDS instance from subscription to pay-as-you-go. To optimize your cost plan, you must evaluate your usage model thoroughly before you change the billing method of your RDS instance.**
- **If an RDS instance has an unpaid subscription order, the subscription order becomes invalid after you upgrade the instance type. In such case, you must first go to the *Orders* page in the RDS console to cancel the subscription order, and then change the billing method to subscription again.**

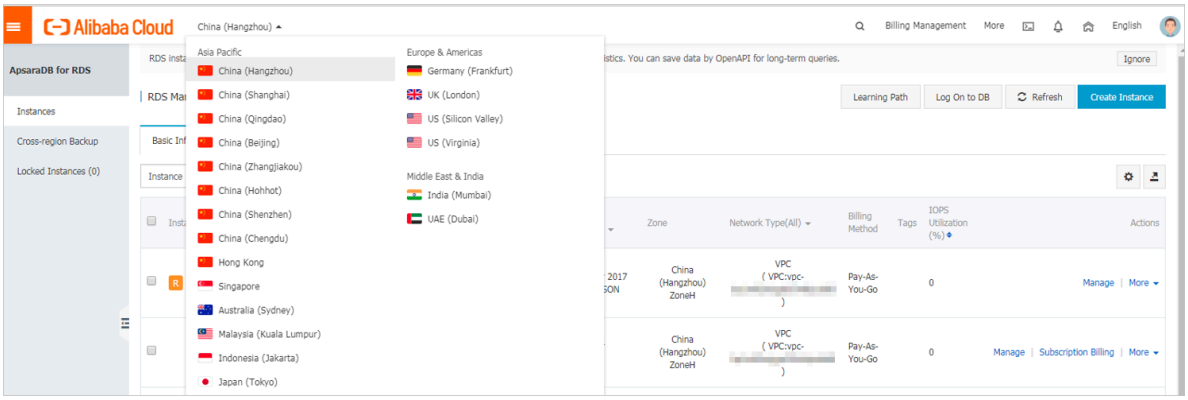
Prerequisites

- **The instance type cannot be a historical one, which means that the instance type must be available for sale. For more information about historical instance types, see *#unique_20*. Before you change the billing method of a historical-type RDS instance to subscription, you must change the instance type to one that is available for sale. For detailed steps, see *Change the configuration of an RDS for SQL Server instance*.**
- **The RDS instance uses the pay-as-you-go billing method.**
- **The RDS instance is in the Running state.**
- **The RDS instance does not have an unpaid subscription order.**

Procedure

1. **Log on to the *RDS console*.**

2. In the upper-left corner, select the region where the target RDS instance is located.



3. Find the target RDS instance and use one of the following two methods to open the Switch to Subscription Billing page.

   - In the Actions column, click Subscription Billing.
   - Click the instance ID. Then in the Status section of the Basic Information page, click Subscription Billing.

4. Select a duration of purchase.
5. Select Terms of Service, Service Level Agreement, and Terms of Use. Then click Pay Now.

> **Note:**
> The system generates a subscription order. If this order is not paid or canceled, you cannot change the billing method of this RDS instance from pay-as-you-go to subscription or purchase a new RDS instance. You can go to the *Orders* page to pay for or cancel this order.

6. Complete the payment.

5.2 Manually renew an RDS for SQL Server instance

This topic describes how to manually renew an RDS for SQL Server instance that is charged by using subscription billing. If a subscription RDS instance expires and is not renewed in time, services will be stopped and data may be permanently deleted.

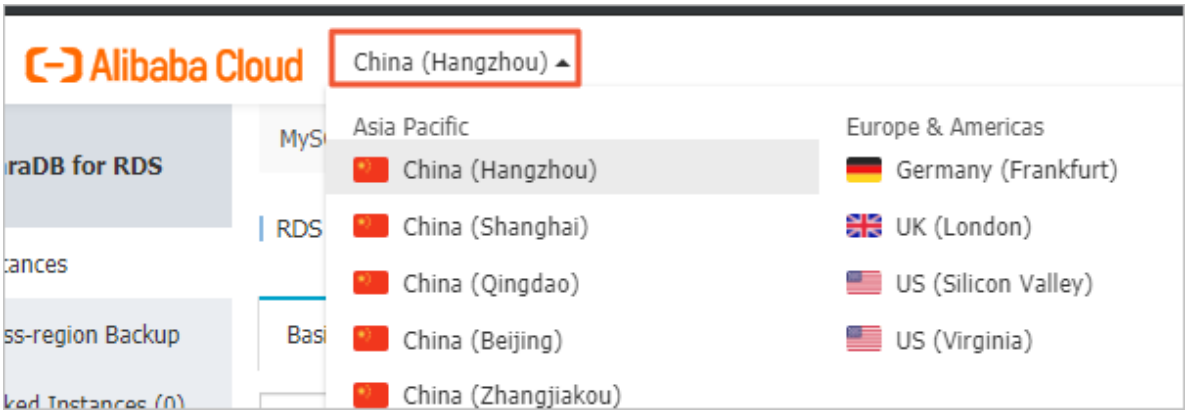
For more information about the impacts, see *Expiration and overdue policy*.

Note:
A pay-as-you-go-based instance does not have an expiration date and no renewal is required.

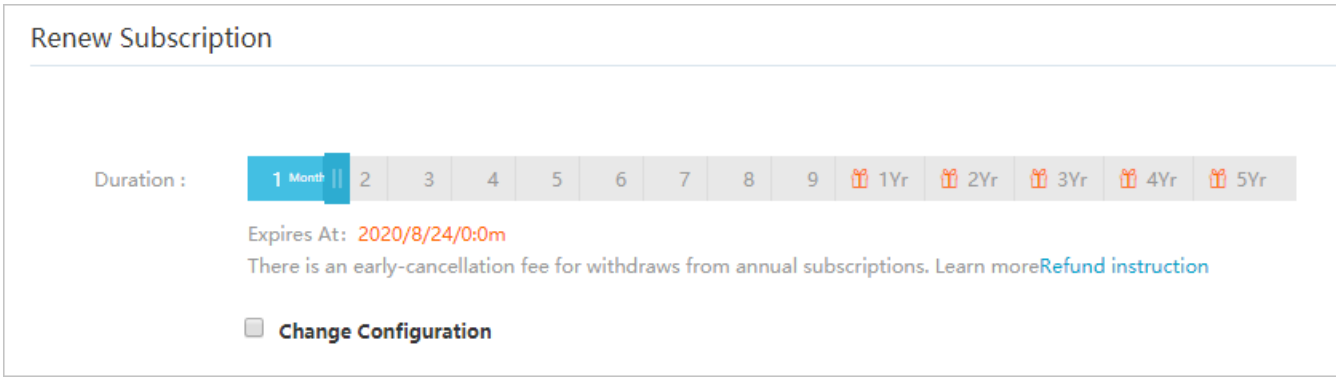
You can manually renew a subscription-based instance before it expires or within 15 days after it expires.

Method 1: Renew an RDS instance in the RDS console

1. **Log on to the *RDS console*.**
2. **Select the target region.**



3. **Find the target RDS instance and in the Actions column click Renew.**
4. **On the Renew Subscription page, select a duration. The longer the duration, the bigger discount you have.**

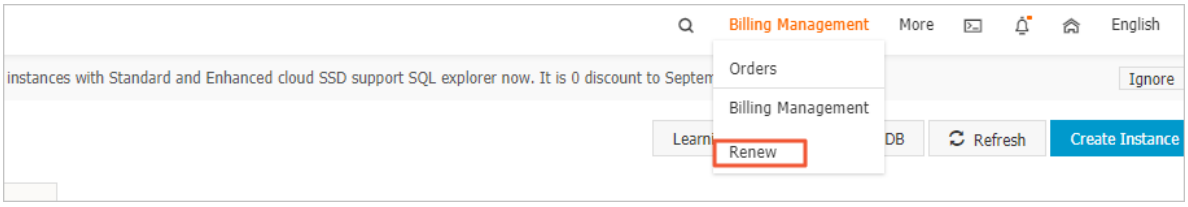


5. **Read and confirm you agree to Terms of Service, Service Level Agreement, and Terms of Useby selecting the checkbox, confirm the order details, and click Pay Now**

Renew an RDS instance in the Renew console

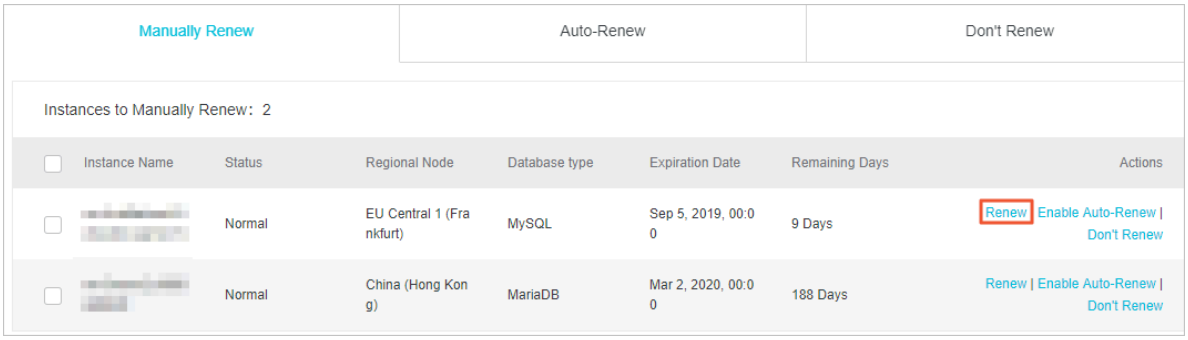
1. **Log on to the *RDS console*.**

2. In the upper-right corner of the page, choose Billing Management > Renew.



3. In the left-side navigation pane, click ApsaraDB for RDS.
4. On the Manually Renew tab, find the target RDS instance and in the Actions column click Renew

> **Note:**
>
> - If the target RDS instance is on the Don't Renew tab, you can click Enable Manual Renew in the Actions column to restore the instance to manual renewal.
> - If the target RDS instance is on the Auto-Renew tab, you can click Modify Auto-Renew in the Actions column, and then in the displayed dialog box select Disable Auto-Renew and click OK to restore the instance to manual renewal.



5. Select a duration, read and confirm you agree to Terms of Service, Service Level Agreement, and Terms of Use by selecting the checkbox, confirm the order details, and click Pay Now.

Auto-renewal

Enabling auto-renewal guarantees that your business runs smoothly without the need of manual renewal when your instance expires. For more information, see *Automatically renew an RDS for SQL Server instance*.

5.3 Automatically renew an RDS for SQL Server instance

This topic describes how to automatically renew an RDS for SQL Server instance. With the automatic renewal function enabled, you do not need to manually renew your RDS instance on a regular basis, and your database services will not become unavailable in case that you forget to renew the instance.

Each subscription-based instance has an expiration date. If an instance is not renewed in time when the instance expires, a service interruption or even data loss may occur. For more information about the impacts, see *Expiration and overdue policy*. Enabling auto-renewal guarantees that your business runs smoothly without the need of manual renewal when your instance expires.

Note:
A pay-as-you-go-based instance does not have an expiration date and no renewal is required.

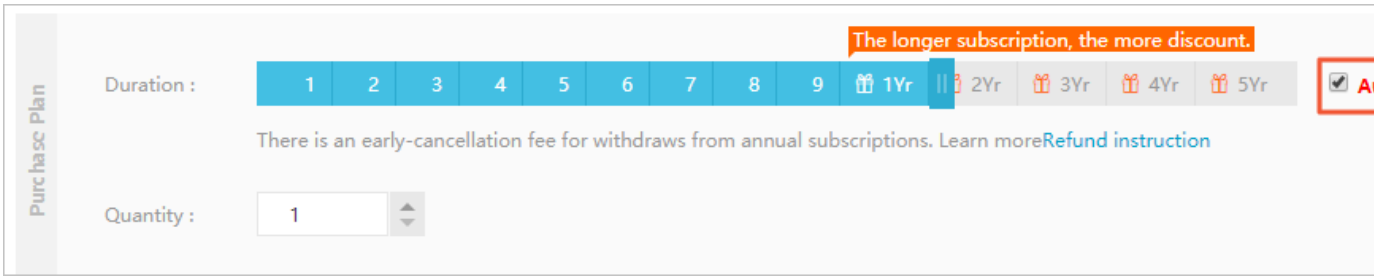
Precautions

- **If you have enabled automatic renewal for your subscription-based instance, a payment will be deducted three days before the expiration date. You can pay the fees by credit cards or coupons. Make sure that your credit card has sufficient balance.**
- **If you manually renew an instance before the automatic deduction date, the system will automatically renew the instance before the next expiration date.**
- **The automatic renewal function takes effect the next day after you enable it. If your instance expires the next day, renew it manually to prevent service interruption. For more information, see *Manually renew an RDS for SQL Server instance*.**

Enable automatic renewal when you purchase an RDS instance

Note:
After you enable automatic renewal, the system automatically renews your instance based on the specified Duration when the instance expires. For example, if you have purchased a three-month subscription-based instance and selected Auto-renewal, the fees are automatically paid every three months for each renewal.

When you *purchase a subscription-based instance*, you can select Auto Renewal on the purchase page.

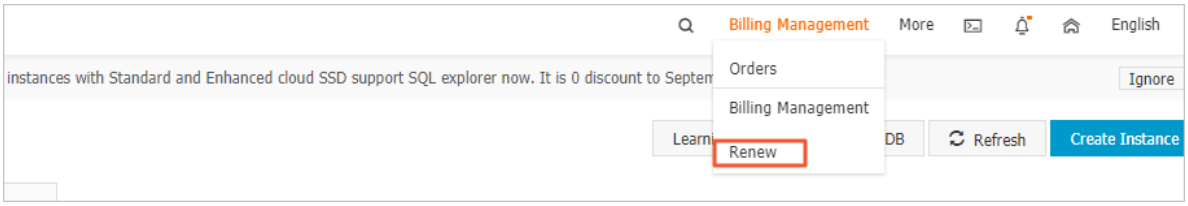


Enable automatic renewal after you purchase an RDS instance

Note:

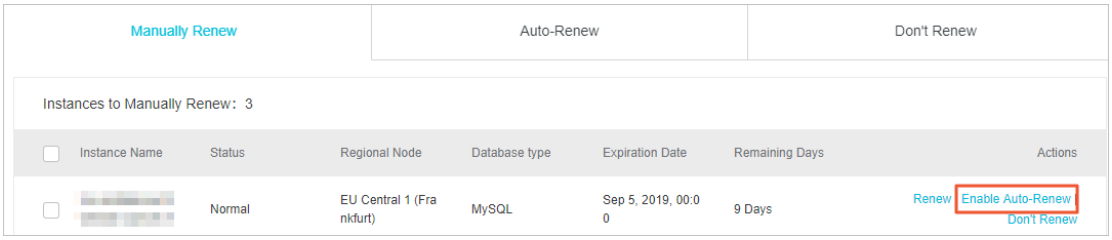
After you enable automatic renewal, the system automatically renews your instance based on the selected renewal duration. For example, if you select a three-month renewal duration, the fees are automatically paid every three months for each renewal.

1. **Log on to the *RDS console*.**
2. **In the upper-right corner, choose Billing Management > Renew.**



3. **In the left-side navigation pane, click ApsaraDB for RDS.**

4. On the Manually Renew or Auto-Renew tab, find the target RDS instance. You can enable automatic renewal for one or more RDS instances at a time.
   - Follow these steps to enable automatic renewal for one RDS instance:
     a. Find the target RDS instance and in the Actions column click Enable Auto-Renew.

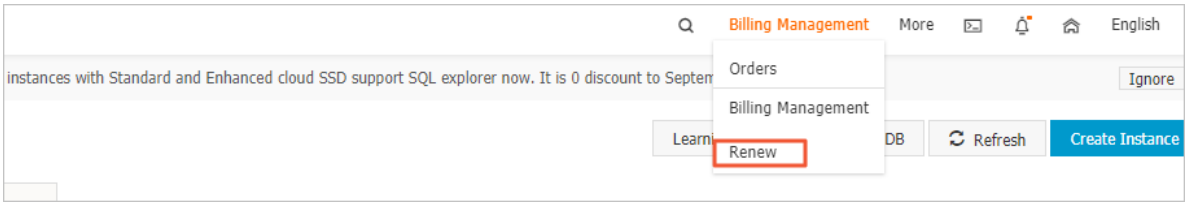


     b. In the displayed dialog box, set Auto-Renew Cycle and click Enable Auto-Renew.
   - Follow these steps to enable auto-renewal for more than one RDS instance:

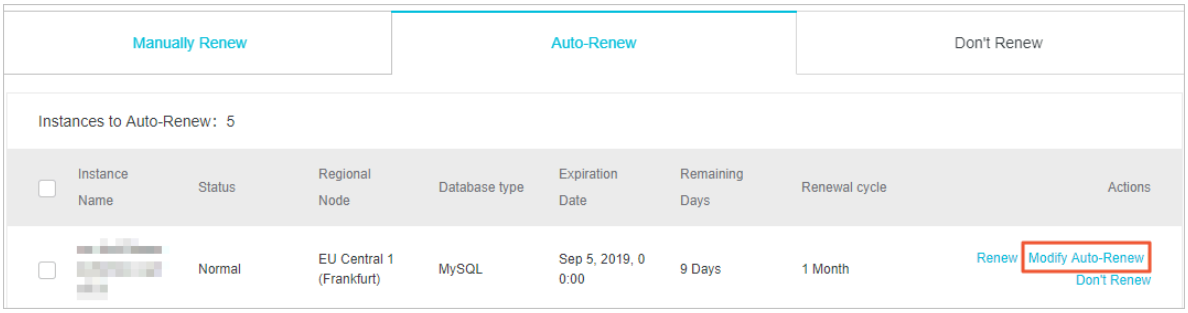
     Select the target RDS instances, and click Enable Auto-Renew below the instance list.
   - In the displayed dialog box, set Auto-Renew Cycle and click Enable Auto-Renew.

Change the auto-renew cycle of an RDS instance

1. Log on to the *RDS console*.
2. In the upper-right corner, choose Billing Management > Renew.



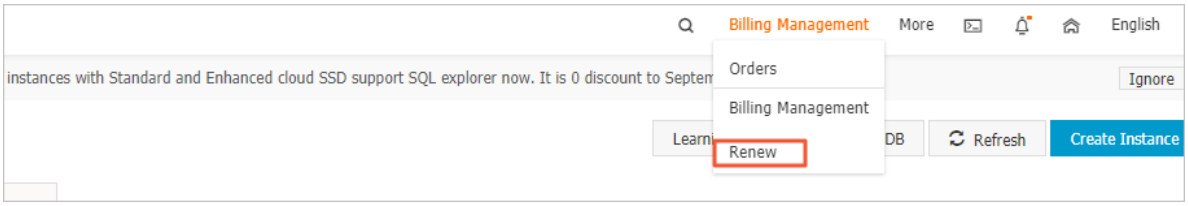
3. In the left-side navigation pane, click ApsaraDB for RDS.
4. On the Auto-Renew tab, find the target RDS instance and in the Actions column click Modify Auto-Renew.



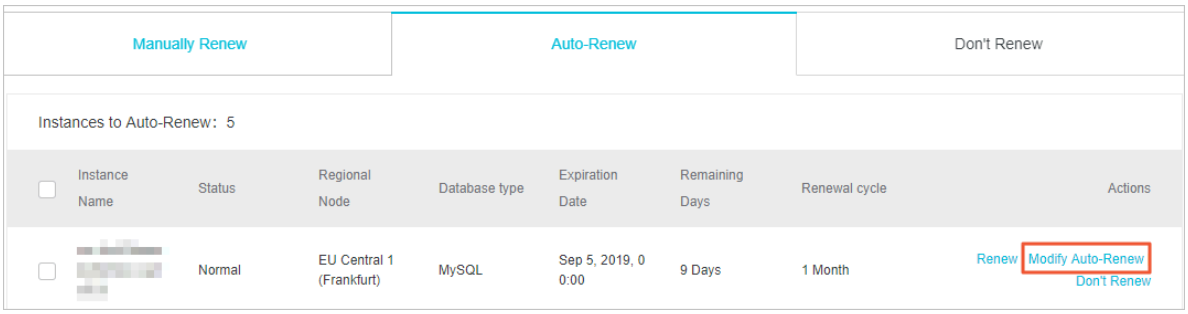
5. In the displayed dialog box, select Modify Auto-Renew Cycle, select an auto-renew cycle, and click OK.

Disable automatic renewal for an RDS instance

1. Log on to the *RDS console*.
2. In the upper-right corner, choose Billing Management > Renew.



3. In the left-side navigation pane, click ApsaraDB for RDS.
4. On the Auto-Renew tab, find the target RDS instance and in the Actions column click Modify Auto-Renew.



5. In the displayed dialog box, select Disable Auto-Renew and click OK.

APIs

Operation	Description
#unique_21	Used to create an RDS instance. **Note:** Automatic renewal is enabled when you create the instance.
#unique_54	Used to renew a subscription-based RDS instance. **Note:** Automatic renewal is enabled after you create the instance.

6 Version upgrade

6.1 Upgrade from Basic Edition to High-availability Edition

This topic describes how to upgrade an ApsaraDB RDS for SQL Server instance from Basic Edition to High-availability Edition. During the upgrade, you can also upgrade the SQL Server version.

#unique_57 **instances do not have secondary instances for hot backup. Therefore, an instance may remain unavailable for an extended period of time if it fails, changes specifications, or undergoes a version upgrade.**

#unique_58 **instances each have a secondary instance. Data between the primary and secondary instances is synchronized in real time. If the primary instance cannot be accessed, your business is automatically switched to the secondary instance. In addition, High-availability Edition instances provide complete product features, including auto scaling, backup and recovery, performance optimization, and read/write splitting.**

For information about the functional differences between different versions and editions, see *Functions supported by different versions and editions of SQL Server*.

Billing description

For information about the billing for version upgrade, see *#unique_59*.

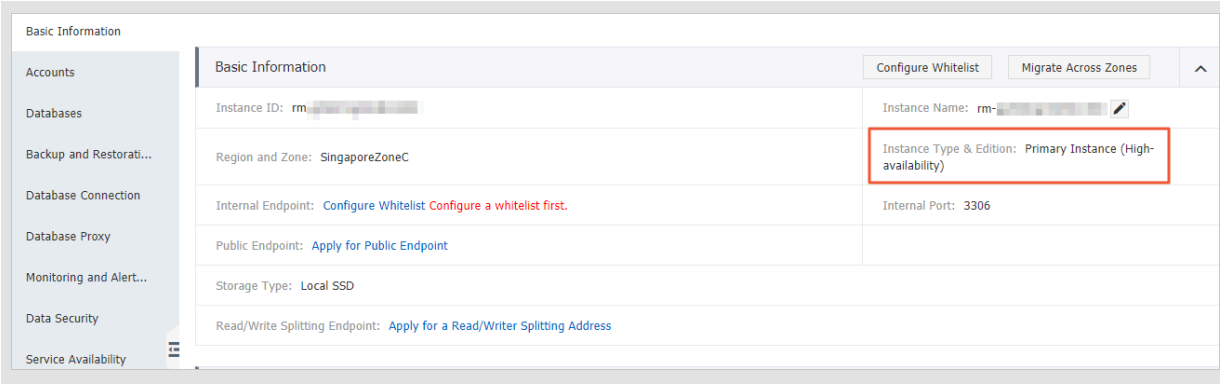
Impact

After the upgrade is complete, you must switch over services. The downtime caused by the switchover varies depending on the instance size. In most cases, the switchover can be completed within 20 minutes. We recommend that you switch over services during system maintenance. Make sure each application can be reconnected in the event of disconnection.

Prerequisites

An SQL Server Basic Edition instance is available.

Note:
You can view the edition of the instance on the Basic Information page.



Precautions

- **Your instance cannot be rolled back to earlier versions or editions after the upgrade is complete.**

  Warning:
  We recommend that you *create a pay-as-you-go instance* to test the version or edition compatibility before the upgrade.

- **The following table lists the upgrade rules.**

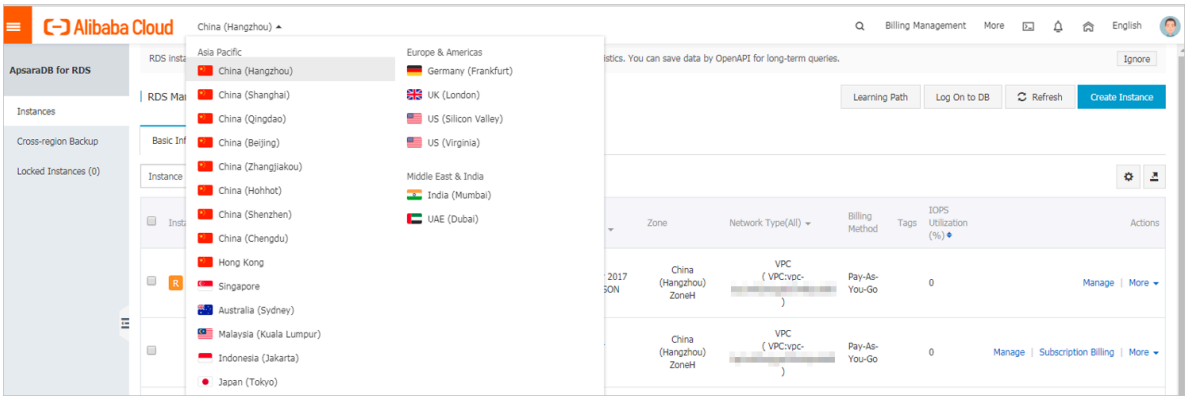
  Table 6-1: Upgrade rules

Original version or edition	Higher available version or edition
2016 Enterprise Edition (Basic Edition)	2016 Enterprise Edition (High-availability Edition)
2012 Enterprise Edition (Basic Edition)	2016 Enterprise Edition (High-availability Edition)
	2012 Enterprise Edition (High-availability Edition)
2016 Standard Edition (Basic Edition)	2016 Standard Edition (High-availability Edition)
	2016 Enterprise Edition (High-availability Edition)
2012 Standard Edition (Basic Edition)	2016 Enterprise Edition (High-availability Edition)
	2016 Standard Edition (High-availability Edition)
	2012 Enterprise Edition (High-availability Edition)

Original version or edition	Higher available version or edition
	2012 Standard Edition (High-availability Edition)
2016 Web Basic Edition	2016 Enterprise Edition (High-availability Edition)
	2016 Standard Edition (High-availability Edition)
2012 Web Basic Edition	2016 Enterprise Edition (High-availability Edition)
	2016 Standard Edition (High-availability Edition)
	2012 Enterprise Edition (High-availability Edition)
	2012 Standard Edition (High-availability Edition)

Procedure

1. Log on to the *ApsaraDB for RDS console*.
2. Select the target region.

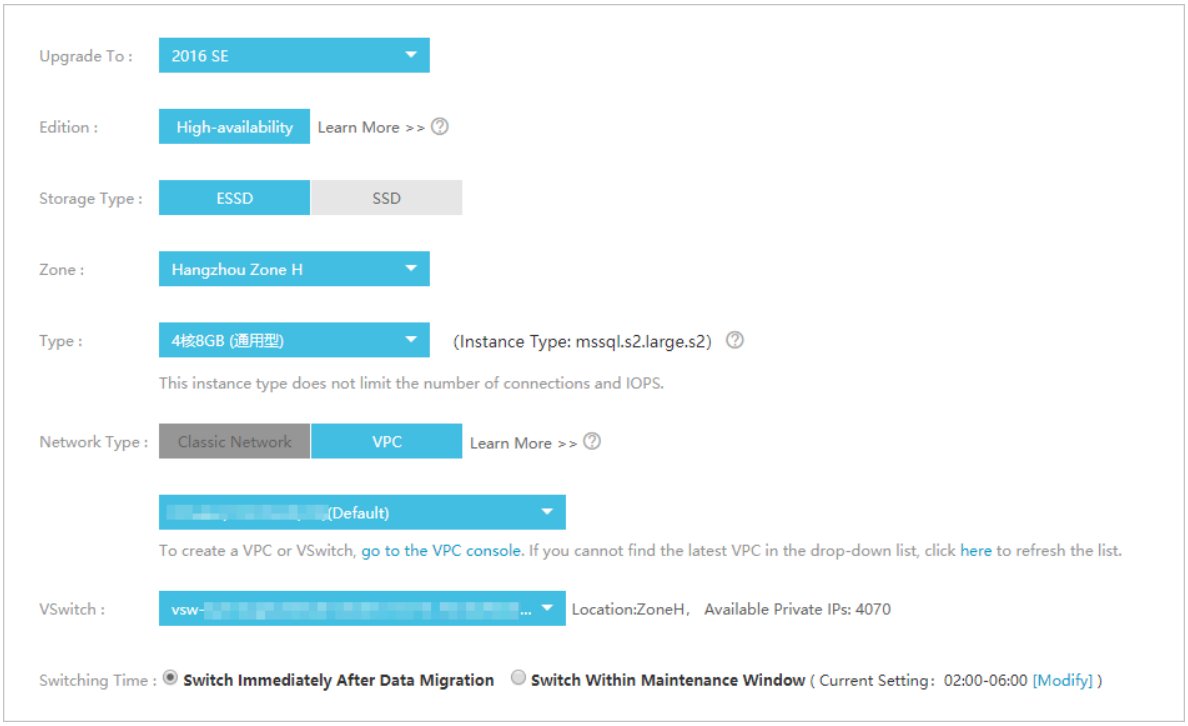


3. Find the target RDS instance and click the instance ID.
4. On the Basic Information page, click Upgrade Version. In the message that appears, click Confirm.

5. On the Upgrade Engine Version page, modify your instance configurations as follows.

Parameter	Description
Upgrade To	Select the target version. The Edition, Storage Type, and Instance Type settings vary depending on the selected target version.
Edition	Select High-availability: The classic high-availability architecture allows your instance to work in primary/ secondary mode to achieve balanced performance in all aspects.
Storage Type	· Standard SSD: an elastic block storage device based on the distributed storage architecture. You can separate computing and storage from each other by storing data in a standard SSD. · Enhanced SSD: an ultra-high performance cloud disk provided by Alibaba Cloud. Enhanced SSDs are based on the next-generation distributed block storage architecture, a 25 GE network, and remote direct memory access (RDMA) technology. They can deliver up to 1 million random IOPS per disk and have low latency.
Zone	Select the zone to which you want to migrate your instance. Multi-zone migration is supported.
CPU and Memory	Each instance type supports a specific number of CPU cores, memory, maximum number of connections, and maximum IOPS. For more information, see *#unique_20*.
Network Type	Classic Network is unavailable. You must specify the VPC information. · If your instance is accessed through a classic network before the upgrade, you can change its network type to VPC and configure a VSwitch. · If your instance is accessed through a VPC or through both a classic network and a VPC before the upgrade, you are not allowed to change its VPC. However, you can change its VSwitch.

Parameter	Description
VSwitch	Select the target VSwitch. If you select multiple zones for your instance, you must select multiple target VSwitches. **Note:** · If your instance is accessed through a VPC or through both a classic network and a VPC before the upgrade, you are not allowed to change its VPC. However, you can change its VSwitch. The available VSwitches vary depending on the specified zone and VPC. · If you select the default VPC, the target VSwitch can be either the default VSwitch or a non-default VSwitch. · Otherwise, the target VSwitch can only be a non-default VSwitch.
Switching Time	· Switch Immediately After Data Migration: Data is migrated and services are switched over immediately. · Switch Within Maintenance Window: Data is migrated, and services are switched over later during a maintenance period.



6. Select the terms of service and click Confirm.

Change the database connection address

After the upgrade, the instance can only be accessed through a VPC. The following table describes how to change the database connection address for the instance after the upgrade based on the original network type of the instance.

Original network type	Change rule
Classic network	The instance after the upgrade is accessed through both a classic network and a VPC: · The original connection address of the classic network still applies to the instance after the upgrade. This address does not expire. · A VPC connection address is generated for the instance after the upgrade based on the VPC that is specified during the upgrade.
VPC	The instance after the upgrade is accessed still through a VPC. The original VPC connection address still applies to the instance after the upgrade, but the virtual IP address (VIP) may change.
Classic network and VPC	The instance after the upgrade is accessed still through both a classic network and a VPC. The original classic network and VPC connection addresses still apply to the instance after the upgrade. The expiration time of the classic network connection address remains unchanged.

6.2 Upgrade SQL Server 2008 R2 to SQL Server 2012/2016

This topic describes how to upgrade an RDS for SQL Server instance from the 2008 R2 version to the 2012 or 2016 version. During the upgrade, you can also migrate the instance to other zones.

From July 9, 2019 onwards, Alibaba Cloud has stopped providing patch updates for new RDS instances in the SQL Server 2008 R2 version. For more information, see *#unique_61*. **We recommend that you upgrade the version of your RDS instance as soon as possible.**

For function differences between SQL Server versions, see *Functions supported by different versions and editions of SQL Server*.

Prerequisites

- The storage capacity of your SQL Server 2008 R2 instance is at least 20 GB.
- The *TDE* feature of your SQL Server 2008 R2 instance has not been enabled.

> **Note:**
> If TDE is enabled, you must disable TDE for all databases and then open a ticket to disable TDE for the entire instance.

Precautions

- Your instance cannot be rolled back to SQL Server 2008 R2 after the upgrade is completed.

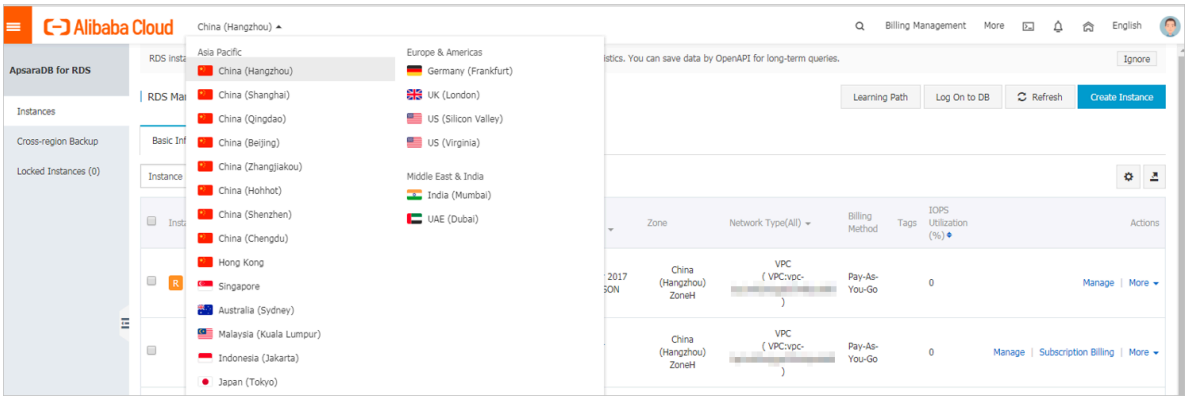
> **Warning:**
> We recommend that you use *a temporary instance of the target version* to test the version compatibility before the upgrade.

- You can upgrade from SQL Server 2008 R2 to SQL Server 2012/2016 Enterprise Edition or SQL Server 2016 Standard Edition only.
- If SSL is enabled for your instance, you can still upgrade your instance version directly. After the upgrade is completed, the instance connection address remains unchanged, but SSL is disabled by default. You can enable it again by referring to *#unique_64*.
- The TDE feature remains if you upgrade your instance from SQL Server 2008 R2 to SQL Server 2012/2016 Enterprise Edition, but does not exist if you upgrade your instance to SQL Server 2016 Standard Edition.
- After the upgrade is completed, the downtime caused by the backend switchover depends on the instance size. The switchover is usually completed within 20 minutes. We recommend that you choose the maintenance window as the swithover time and make sure that your applications can automatically reconnect to the instance.

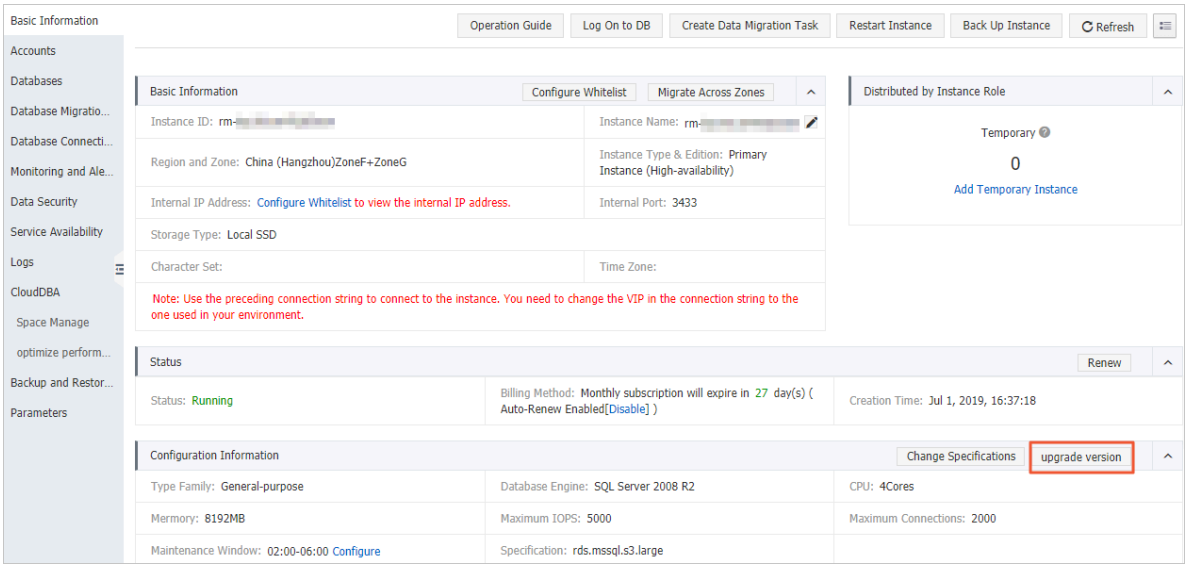
Procedure

1. Log on to the *RDS console*.

2. Select the region where your instance is located.



3. Click the ID of your instance.
4. On the Basic Information page, click Upgrade Version. In the displayed dialog box, click Confirm.



5. On the Upgrade Engine Version page, modify your instance configurations as follows.

Parameter	Description
Upgrade To	Select the target version. The Edition, Storage Type, and Type settings vary depending on the selected target version.
Edition	Select High-availability: The classic HA architecture allows your instance to work in master/slave mode with balanced performance in all aspects.
Storage Type	Select SSD or ESSD.
Zone	Select the zone to which you want to migrate your instance. You can choose a multi-zone combination if available.

Parameter	Description
Type	Each instance type provides a specific number of CPU cores, memory, maximum number of connections, and maximum IOPS. For more information, see *#unique_20*.
Network Type	Classic Network is unavailable. You must specify the VPC information. · If the original network type is the classic network, you can select any VPC and vSwitch. · If the original network type is a VPC or the hybrid mode (both classic network and a VPC), you cannot change the VPC but you can change the VSwitch. The available VSwitches vary depending on the specified Zone and VPC.
VSwitch	Select the VSwitch. If you select multiple zones for your instance, you must select multiple VSwitches.
Switching Time	· Switch Immediately After Data Migration: After the data migration, the switchover occurs immediately. · Switch Within Maintenance Window: After the data migration, the switchover does not occur until the maintenance period.

6. Select the terms of service and click Confirm.

Instance connection address after the upgrade

After the upgrade, the instance connection address is changed as follows.

If the original network type is	Then after the upgrade
Classic network	Two connection addresses are available: · The original connection address of the classic network still can be used and will not expire. · A VPC connection address is generated for the instance based on the VPC that is specified during the upgrade.
VPC	A new VPC connection address is generated based on the VPC that is specified during the upgrade. This address replaces the original VPC connection address of the instance.
Hybrid mode (Classic network and VPC)	The instance remains in hybrid mode. The original classic network and VPC connection addresses remain unchanged. The expiration time of the classic network connection address also remains unchanged.

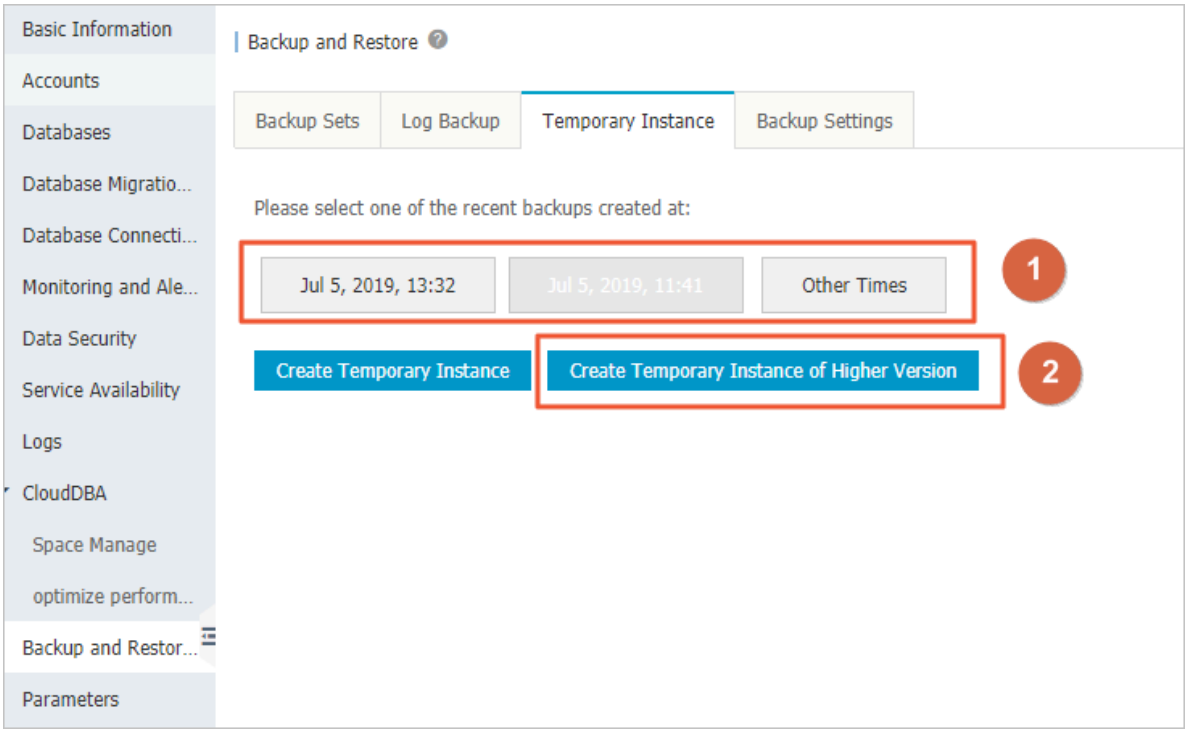
Create a temporary instance of the target version

Before the upgrade, we recommend that you create a temporary instance of the target version to test the version compatibility.

Note:
You can create a temporary instance of the target version only for an SQL Server 2008 R2 instance whose TDE and SSL are disabled.

1. **Log on to the *RDS console*.**
2. **Select the region where your instance is located.**
3. **Click the ID of your instance.**
4. **In the left-side navigation pane, click Backup and Restoration.**

5. Click the Temporary Instance tab, specify the time from which you want to clone data, and click Create Temporary Instance of Higher Version.

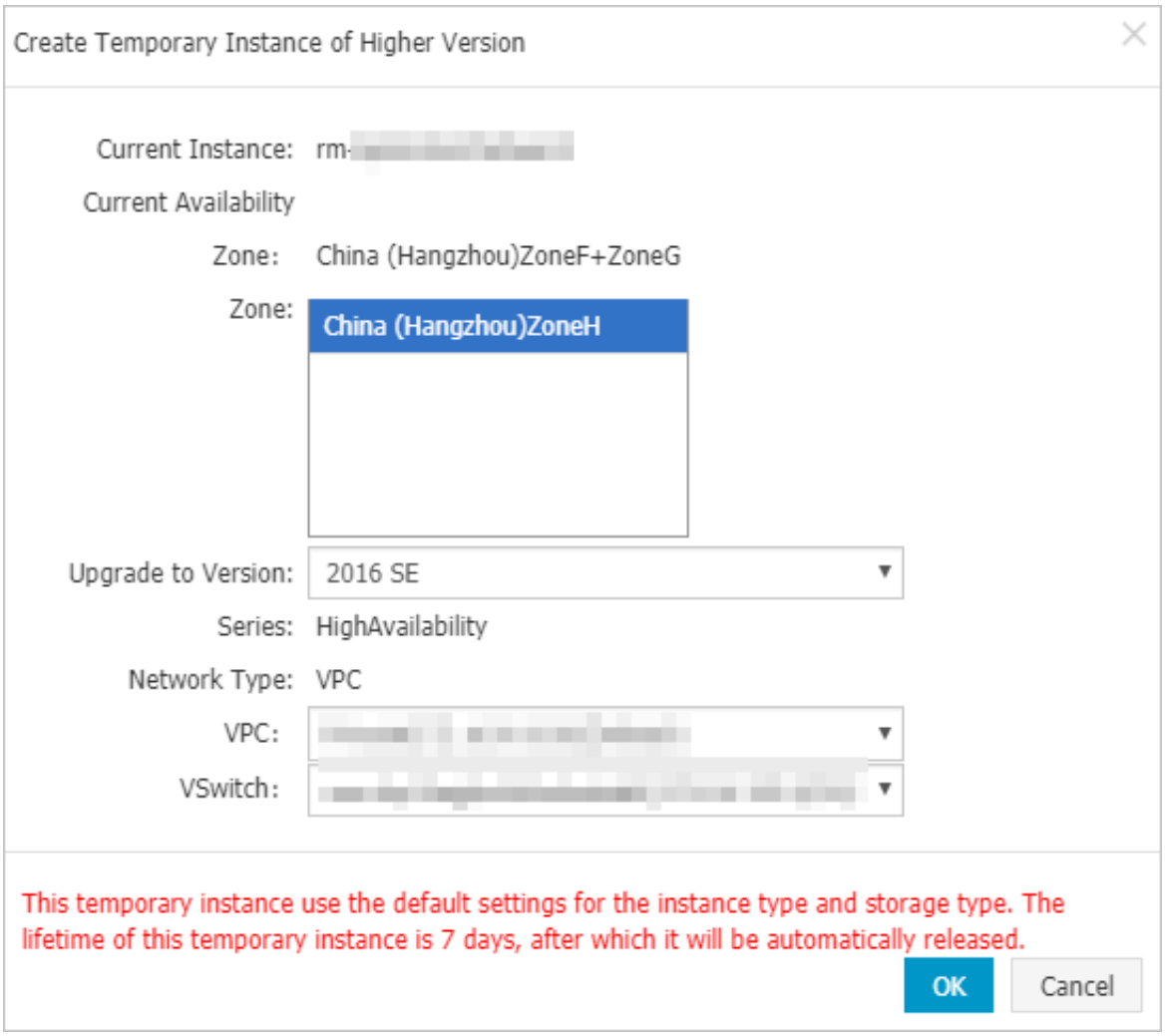


6. In the displayed dialog box, set the following parameters.

Parameter	Description
Zone	Select the zone where you can create a temporary instance.
Upgrade To Version	Select the target version. The available target versions are as follows: · 2016 SE · 2016 EE · 2012 EE
VPC	Select the VPC where the ECS instance to be connected is located. Otherwise, the temporary instance cannot communicate with the ECS instance through the intranet.
VSwitch	Select a VSwitch under the specified VPC.

Note:

The temporary instance adopts a default instance type and a default storage type.



7. **Click OK.**

Note:

The temporary instance will be automatically released after seven days.

Related API

API	Description
UpgradeDBInstanceEngineVersion	**Upgrades the database version of an instance.**

6.3 Upgrade an instance from SQL Server 2012 to SQL Server 2016

You can upgrade an instance from SQL Server 2012 Basic Edition to SQL Server 2016 High-availability Edition.

For details about the functional differences between different versions and editions, see *Functions supported by different versions and editions of SQL Server*.

Billing description

For details about the billing for version upgrade, see *#unique_59*.

Impact

After the upgrade is completed, you must switch over services. The downtime caused by the switchover varies depending on the instance size. In most cases, switchover can be completed within 20 minutes. We recommend that you switch over services during system maintenance. Make sure each application can be reconnected in the event of disconnection.

Prerequisites

The SQL Server version and RDS edition are as follows:

- **SQL Server 2012 Enterprise Edition**
- **SQL Server 2012 Web**
- **SQL Server 2012 Standard Edition (Basic Edition)**

Precautions

Your instance cannot be rolled back to SQL Server 2012 Basic Edition after the upgrade is completed.

Warning:

We recommend that you *create a pay-as-you-go instance* **to test the version compatibility before the upgrade.**

Procedure

For more information, see *Upgrade from Basic Edition to High-availability Edition*.

7 Instance

7.1 Restart an RDS for SQL Server instance

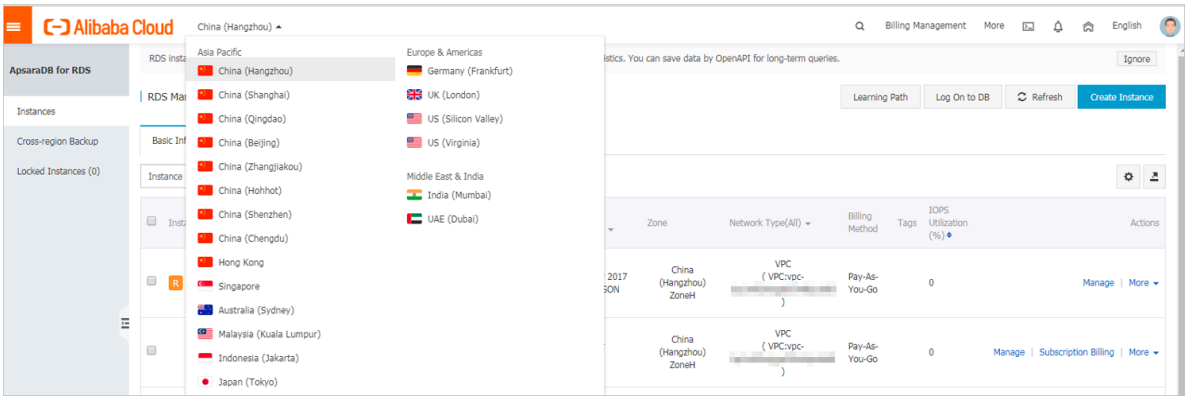
This topic describes how to restart an RDS for SQL Server instance in the RDS console if the number of connections exceeds its upper limit or any performance issue occurs for the instance.

Impact

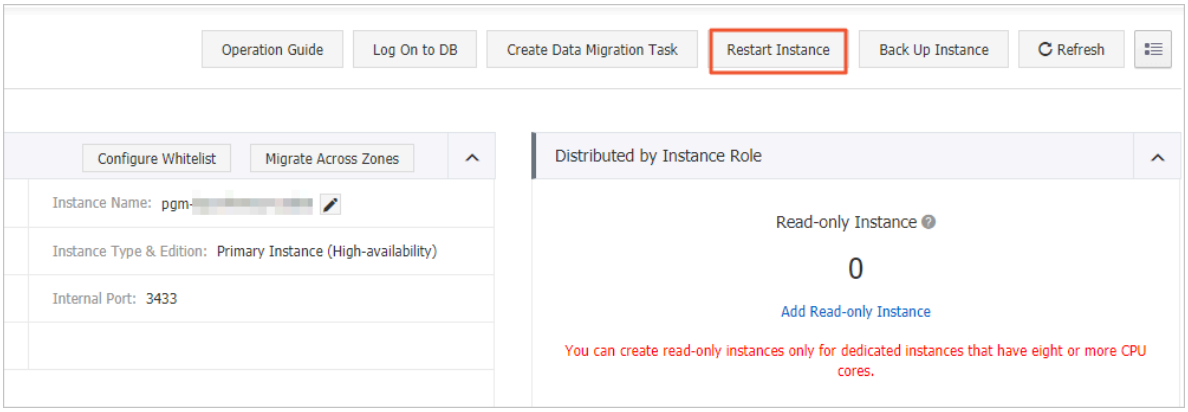
Restarting an RDS instance may interrupt its connections and impact your services. Exercise caution when performing this action.

Procedure

1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance. Then, click the instance ID or in the Actions column click Manage.**
4. **In the upper-right corner of the Basic Information page, clickRestart Instance.**



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

APIs

API	Description
#unique_69	**Used to restart an RDS instance.**

7.2 Set the maintenance window of an RDS for SQL Server instance

This topic describes how to set the maintenance window of an RDS for SQL Server instance so that RDS for SQL Server can perform regular maintenance operations as needed according to a defined schedule. The default maintenance window is from 02:00 to 06:00. You can set the maintenance window to the off-peak period of your business to avoid impacts on business.

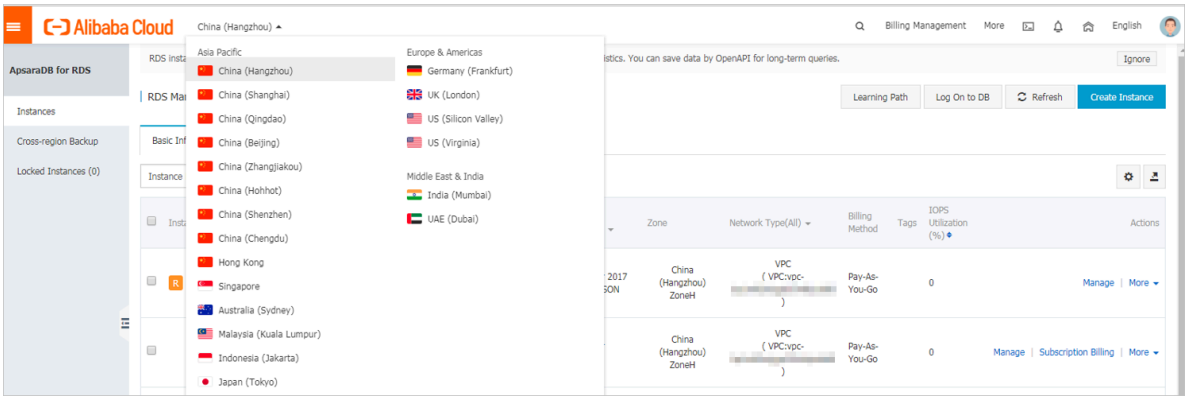
Precautions

- **Before maintenance is performed, ApsaraDB for RDS sends SMS messages and emails to the contacts listed in your Alibaba Cloud accounts.**
- **To guarantee service stability during the maintenance process, the instance enters the Instance Maintaining state before the maintenance time on the day of maintenance. When the instance is in this state, access to data in the database and query operations such as performance monitoring are not affected. However, apart from account and database management and IP address whitelist configuration, modification operations such as upgrade, downgrade, and restart are temporarily unavailable.**
- **During the maintenance window, the instance is disconnected once or twice. Make sure that you configure automatic reconnection policies for your applicatio ns to avoid service disruptions.**

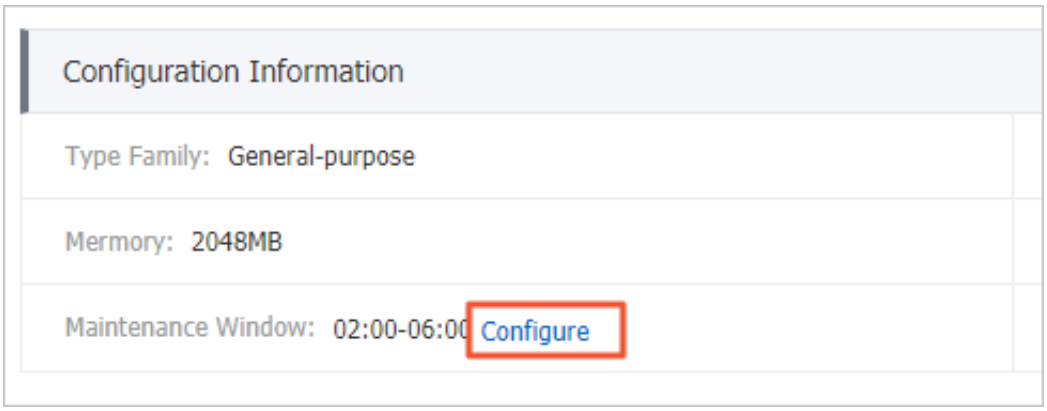
Procedure

1. **Log on to the** *RDS consoleRDS console*.

2. Select the target region.



3. Find the target RDS instance. Then, click the instance ID, or in the Actions column click Manage.
4. On the Basic Information page, find the Configuration Information section and click Configure to the right of Maintenance Window.



5. Select a maintenance window and click Save.

Note:
The maintenance window is in China Standard Time (UTC +8).

APIs

API	Description
#unique_71	Used to change the maintenance window of an RDS instance.

7.3 Migrate an RDS for SQL Server instance across zones in the same region

This topic describes how to migrate an RDS for SQL Server instance across zones in the same region. The attributes, configuration, and connection addresses of

the instance remain unchanged after the migration. The time required for the migration varies depending on the data volume of the instance. In typical cases, the migration takes a few hours.

Migration scenarios

Migration scenario	Description
Migrate an RDS instance from one zone to another	The zone where the RDS instance is located is overloaded or cannot meet the performance requirements of the instance.
Migrate an RDS instance from one zone to multiple zones	The master and slave nodes are located in different equipment rooms in different zones to enhance disaster tolerance. A multi-zone instance is superior to a single-zone instance because it can survive more disasters. For example, a single-zone instance can survive server and rack faults while a multi-zone instance can survive equipment room faults.
Migrate an RDS instance from multiple zones to one zone	This scenario is provided to meet the requirements of specific functions.

Fees

This function is free of charge. No fee is charged even when you migrate an RDS instance from one zone to multiple zones.

Prerequisites

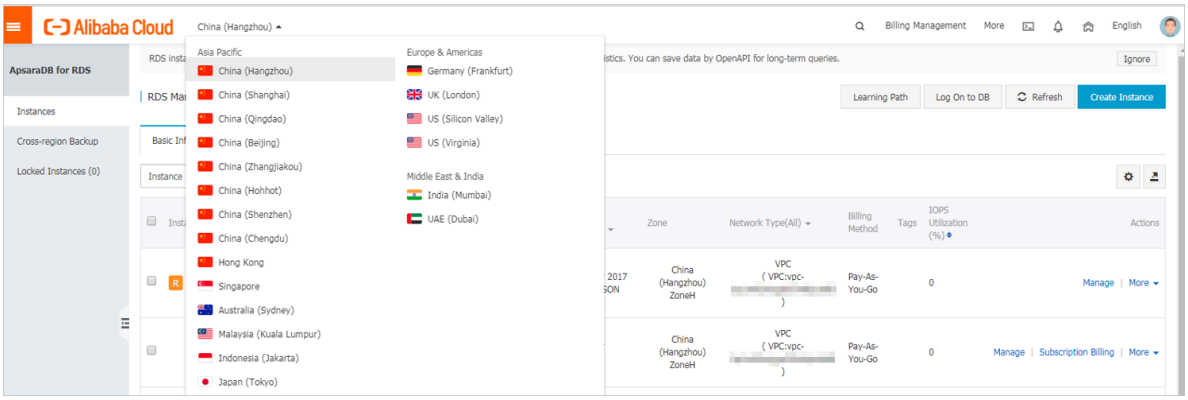
- The DB engine version and edition of the RDS instance are SQL Server 2008 R2.
- The region to which the RDS instance belongs has more than one zone.

Precautions

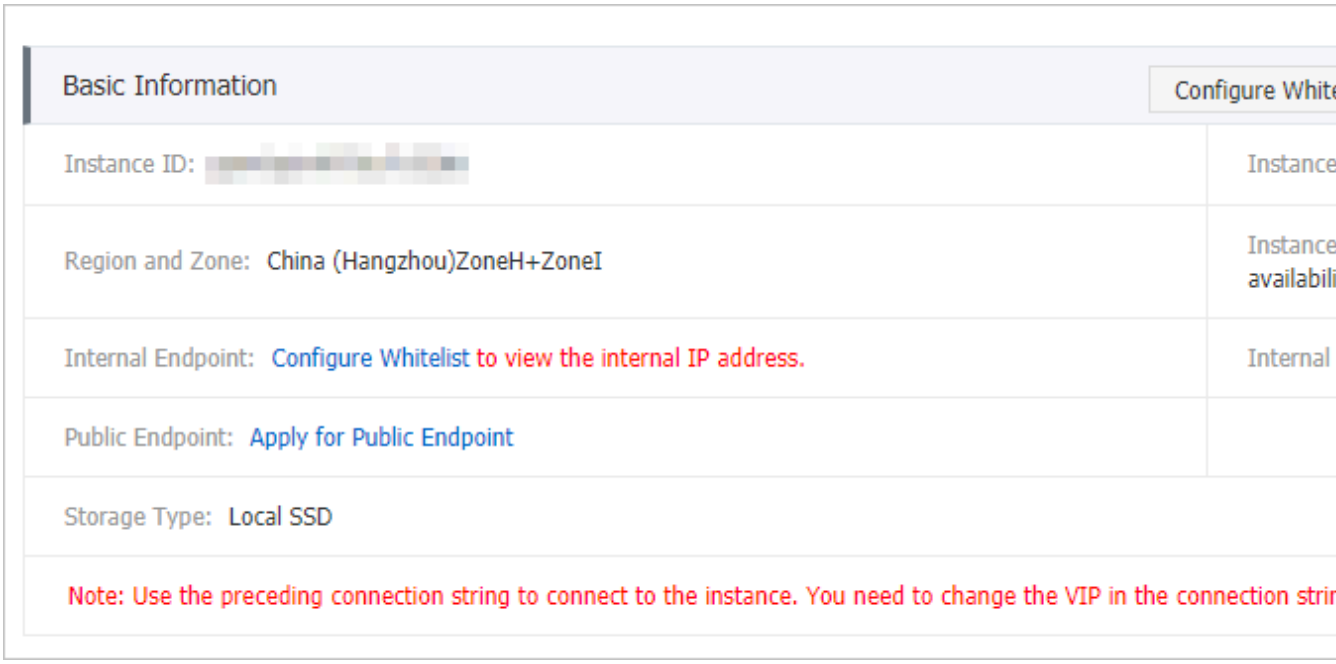
During the migration, the connection to your RDS instance remains unavailable for 30 seconds, and most operations related to databases, accounts, and networks cannot be performed. Make sure that your application can be automatically reconnected to your RDS instance after the migration. Additionally, perform the migration during off-peak hours.

Procedure

1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance and click its ID.**
4. **In the Basic Information section of the Basic Information page, click Migrate Across Zones.**

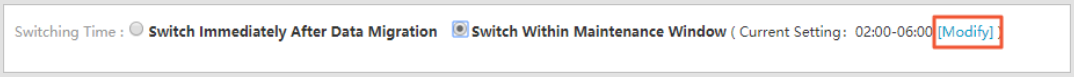


5. **In the displayed dialog box, specify the destination zone, VSwitch, and migration time, and click OK.**

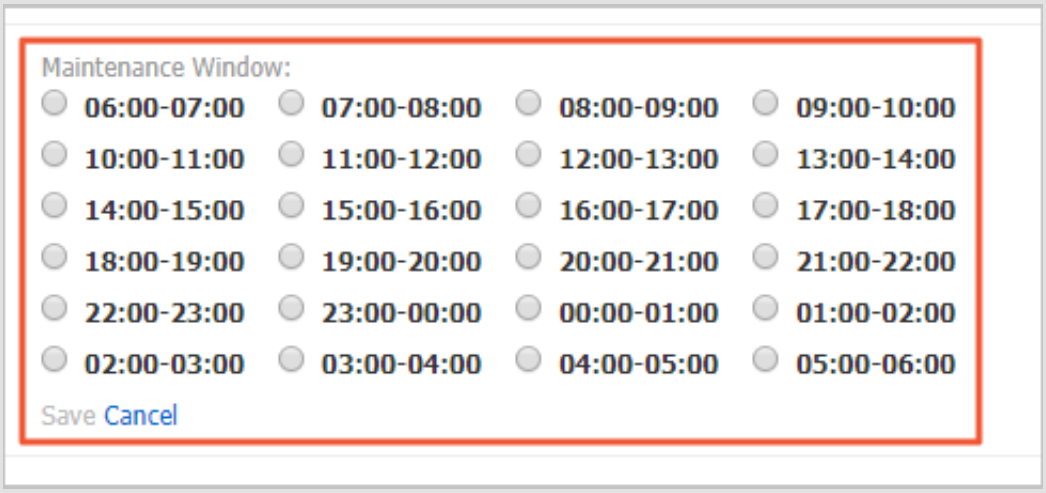
Note:

If you want to change the maintenance window, follow these steps:

a. Click Change.



b. In the Configuration Information section, specify the maintenance window and click Save.



c. Refresh the page, and perform the migration again.

APIs

API	Description
#unique_73	Used to migrate an RDS instance across zones.

7.4 Switch over services between the RDS for SQL Server master and slave instances

This topic describes how to switch over services between the RDS for SQL Server master and slave instances.

A High-availability Edition instance has a slave instance, and the data is synchronized between both instances in real time. You can only access the master instance. The slave instance is a backup instance and cannot be accessed. You can switch your services from the master instance to the slave instance. After the switchover, the original master instance becomes the slave instance.

If the master instance cannot be accessed, your business is automatically switched to the slave instance.

Prerequisites

The RDS instance is in the High-availability Edition.

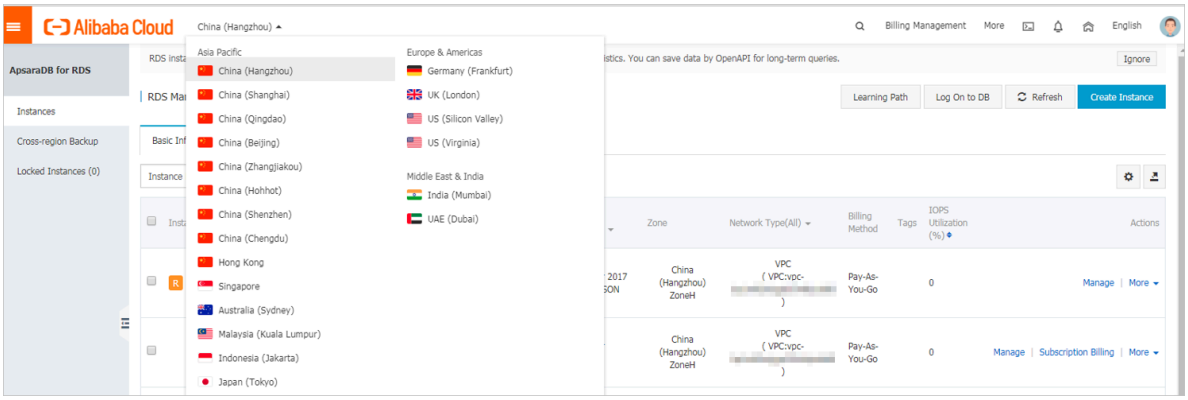
> **Note:**
> **An RDS instance in the Basic Edition does not have a slave instance, and therefore its services cannot be switched over.**

Precautions

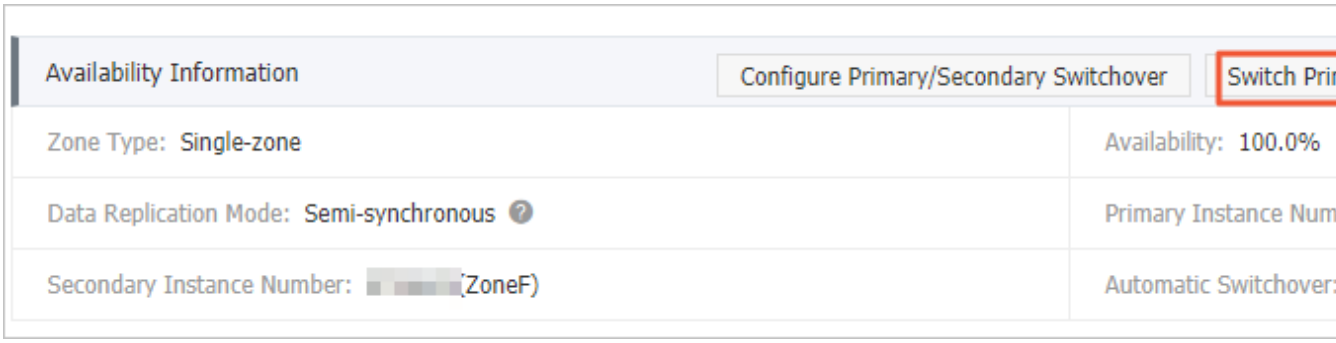
During the switchover, your RDS instance may be disconnected. Make sure that your application can automatically reconnect to your RDS instance after the switchover.

Procedure

1. **Log on to the *ApsaraDB for RDS console*.**
2. **In the upper-left corner of the page, select the region where the instance is located.**

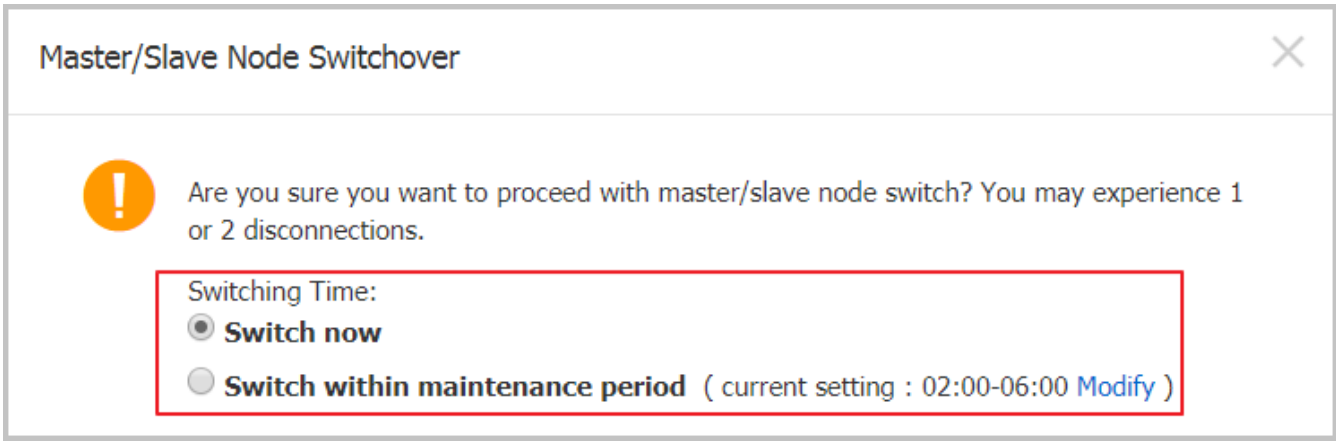


3. **Find the instance and click the instance ID.**
4. **In the left-side navigation pane, click Service Availability.**
5. **In the `Availability Information` section, click Switch Primary/Secondary Instance.**



6. Select an appropriate time to perform the switch, and click OK.

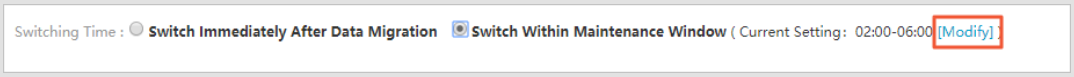
   During the switch, operations such as managing the databases and accounts and switchover the network types cannot be performed. Therefore, we recommend that you select Switch Within Maintenance Window.



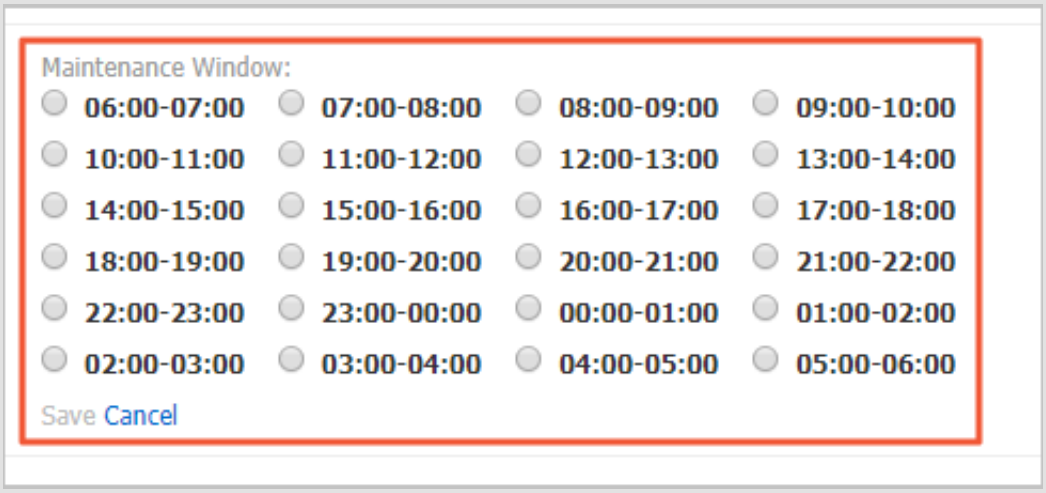
Note:

If you want to change the maintenance window, follow these steps:

a. Click Change.



b. In the Configuration Information section, select a maintenance window and click Save.



c. Return to the Service Availability page, refresh the page, and perform the steps to switch the service.

APIs

Operation	Description
SwitchDBInstanceHA	**Switches between the master and slave instances.**

7.5 Change the network type of an RDS for SQL Server instance

This topic describes how to change the network type of an RDS for SQL Server instance.

Network types

- **Classic network: Instances in a classic network are not isolated. Access control is implemented for instances by using whitelists.**
- **Virtual Private Cloud (VPC): A VPC is an isolated network environment. We recommend that you use VPC because it is more secure.**

  You can customize the routing table, IP address range, and gateway of the VPC. To smoothly migrate applications to the cloud, you can use a leased line or VPN to connect your own data center to a VPC on the cloud to make a virtual data center.

> **Note:**
> **You can use the classic network or VPC and switch between the network types for free.**

Switch from VPC to classic network

Precautions

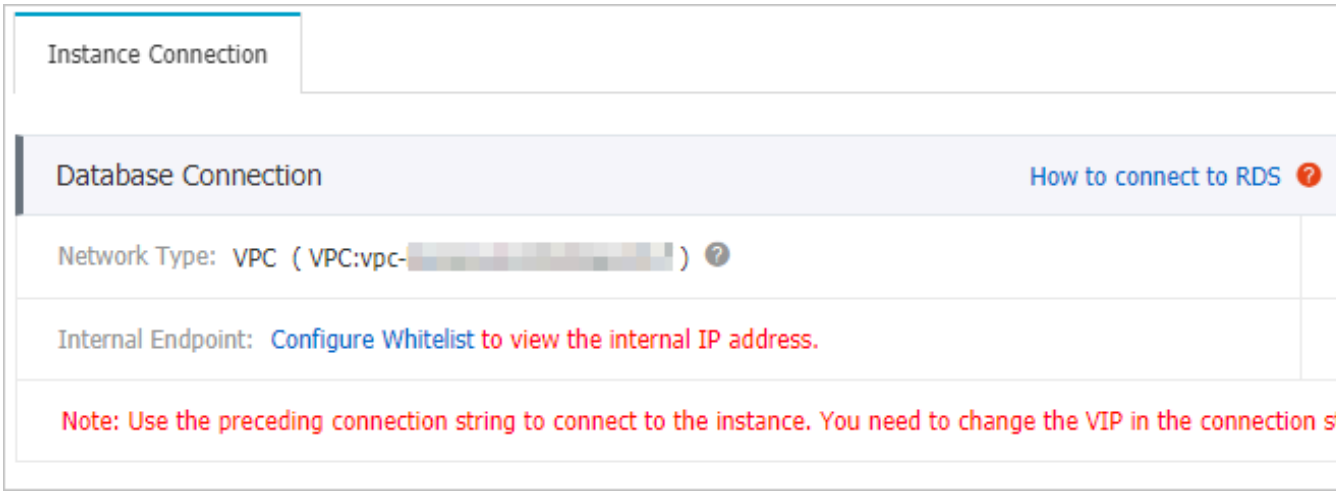
- **After the network type of an RDS instance is switched to classic network, the endpoints remain unchanged, but the corresponding IP addresses change.**
- **After the network type of an RDS instance is switched to classic network, ECS instances in VPCs cannot access the RDS instance by using the internal endpoint. Make sure that you change the endpoint on the application.**
- **Switching the network type may result in a disconnection of 30 seconds. To avoid impacts that arise from this operation, we recommend that you perform the switching during off-peak hours, or configure automatic reconnection policies for your application.**

- **Instances in the SQL Server 2012/2016 High-availability Edition or SQL Server 2017 do not support the classic network. Therefore, you cannot switch these instances to the classic network.**

Procedure

1. **Log on to the *ApsaraDB for RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**

3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Database Connection.**
5. **In the Database Connection section, click Switch to Classic Network.**



6. **In the message that appears, click OK.**

   After the network type is switched, only ECS instances in classic networks can access the RDS instance over the internal network. Make sure that you configure the endpoint of the RDS instance on the ECS instance in the classic network.

7. **Configure the whitelist of the RDS instance to allow access from the ECS instance over the internal network.**

   The RDS instance applies the standard whitelist mode, as shown in the following figure. You must add the internal endpoint of the ECS instance in the classic network to any whitelist of the RDS instance.

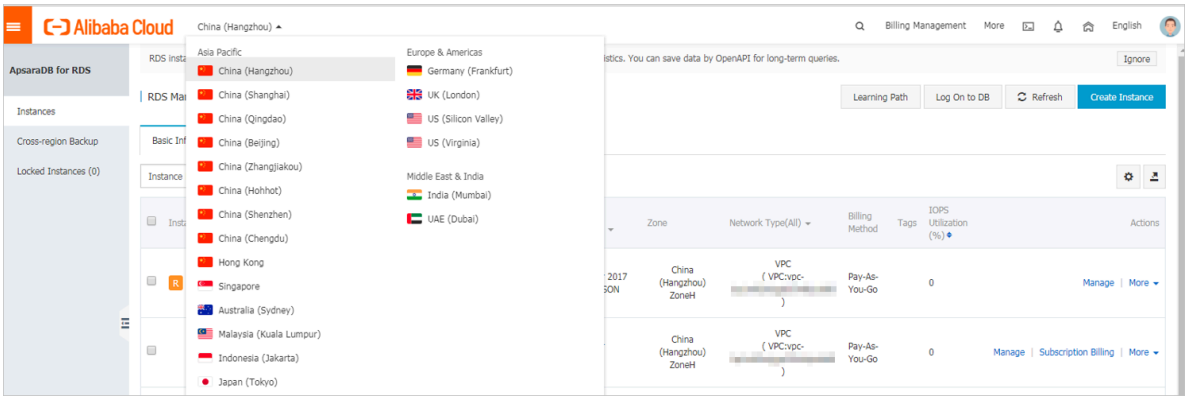
Switch from classic network to VPC

Precautions

- **Instances in the SQL Server 2008 R2 version do not support the network type change from classic network to VPC.**
- **Temporary instances only support the classic network type.**

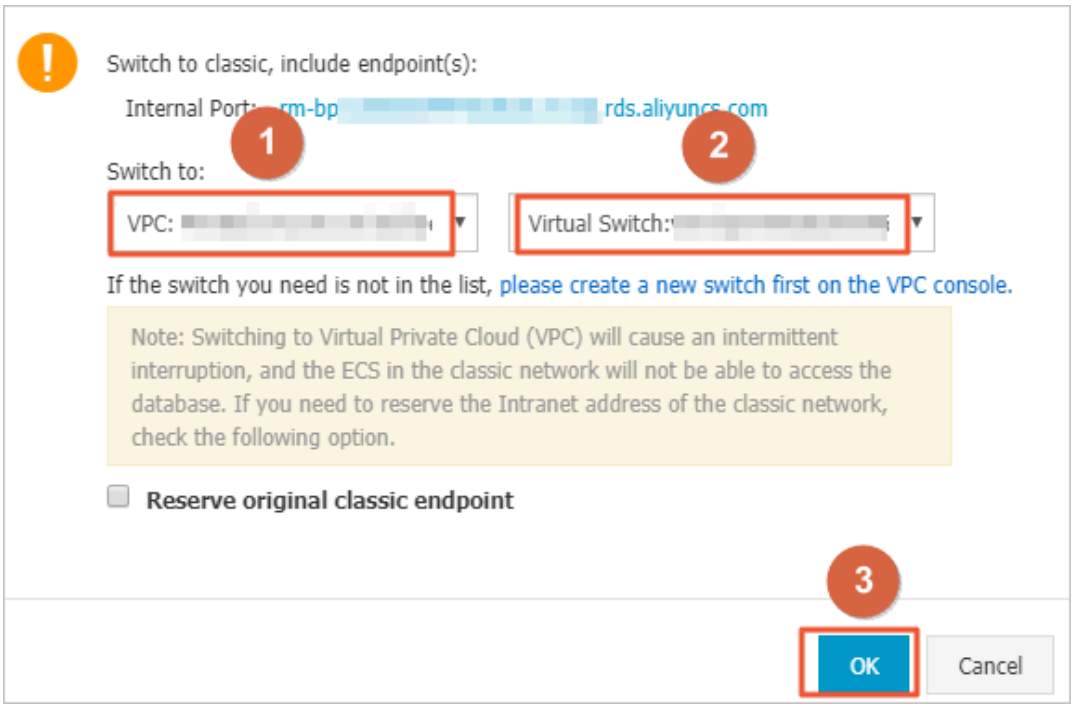
Procedure

1. **Log on to the *ApsaraDB for RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



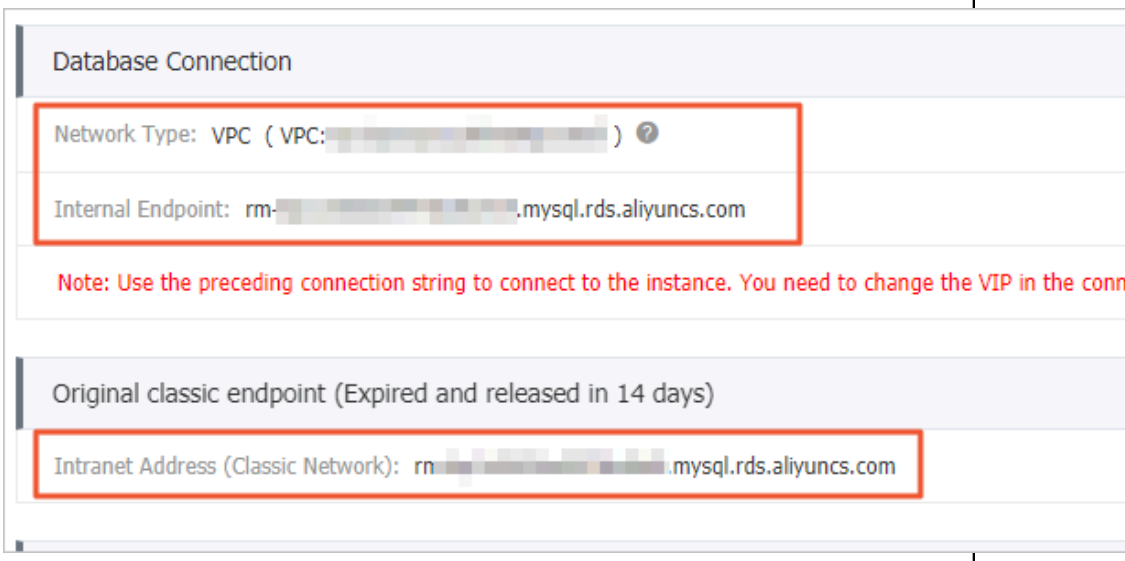
3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Database Connection .**
5. **Click Switch to VPC.**

6. In the dialog box that appears, select a VPC and a VSwitch, and specify whether to retain the classic network address.
   - Select a VPC. We recommend that you select the VPC where your ECS instance is located. Otherwise, the ECS and RDS instances cannot connect to each other over the internal network unless *Express Connect* or *VPN Gateway* are created to connect the two VPCs.
   - Select a VSwitch. If there is no VSwitch in the VPC that you select, as shown in the following figure, you must create a VSwitch in the zone where the instance is located. For more information, see *Manage VSwitches*.



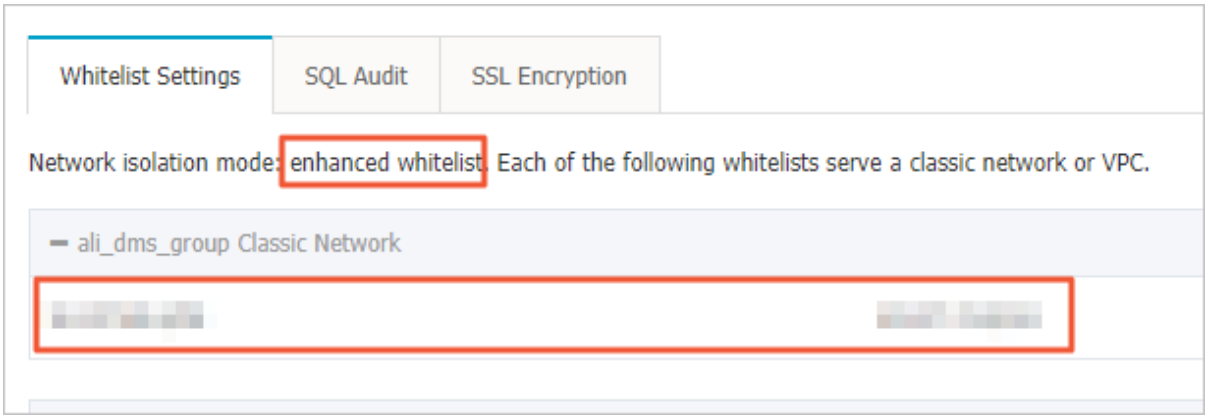
   - Select or clear Reserve Original Classic Endpoint as needed. The following table describes the details.

Action	Description
Clear	The classic network address is not retained. The original classic network address is changed to the VPC address. If you do not retain the classic network address, the RDS instance will be disconnected for 30 seconds, and the access from the ECS instance in the classic network to the RDS instance over the internal network is immediately disconnected when you switch the network type.

Action	Description
Select	The classic network address is retained, and a new VPC address is generated, as shown in the following figure. It indicates that the *hybrid access mode* is enabled, and the RDS instance can be accessed by ECS instances in both a classic network and a VPC. If you retain the classic network address, the RDS instance will not be disconnected when you switch the network type. The internal access from the ECS instance in the classic network to the RDS instance is only disconnected when the classic network address expires. Before the classic network address expires, make sure that the VPC address has been configured in the ECS instance in the VPC to smoothly migrate your services to the VPC. The system will send an SMS message to the phone number bound to your Alibaba Cloud account every day in the seven days before the classic network address expires.  For more information, see *Configure a hybrid access solution to smoothly migrate an RDS instance from the classic network to a VPC*.

7. Add the internal IP address of the ECS instance in the VPC to the VPC whitelist of the RDS instance, so that the ECS instance can access the RDS instance over the

internal network, as shown in the following figure. If there is no VPC whitelist, you must create a new whitelist.



8. Perform one of the following operations as needed:
   - If you retain the classic network address, you must configure the VPC address of the RDS instance in the ECS instance that is in the VPC.
   - If you do not retain the classic network address, the access from the ECS instance in the classic network to the RDS instance over the internal network is immediately disconnected when you switch the network type. You must configure the VPC address of the RDS instance in the ECS instance that is in the VPC.

> **Note:**
> If you need to use the ECS instance in the classic network to access the RDS instance in the VPC, you can use the *ClassicLink* function or migrate the ECS instance to the VPC.

APIs

API	Description
#unique_83	Used to change the network type of an RDS instance.

7.6 Create an RDS for SQL Server read-only instance

This topic describes how to create read-only instances for an RDS for SQL Server master instance to handle a large number of read requests and increase the application throughput. A read-only instance is a read-only replica of the master

instance. Changes to the master instance are automatically synchronized to all read-only instances attached to the master instance.

For more information, see *Introduction to SQL Server read-only instances*.

Prerequisites

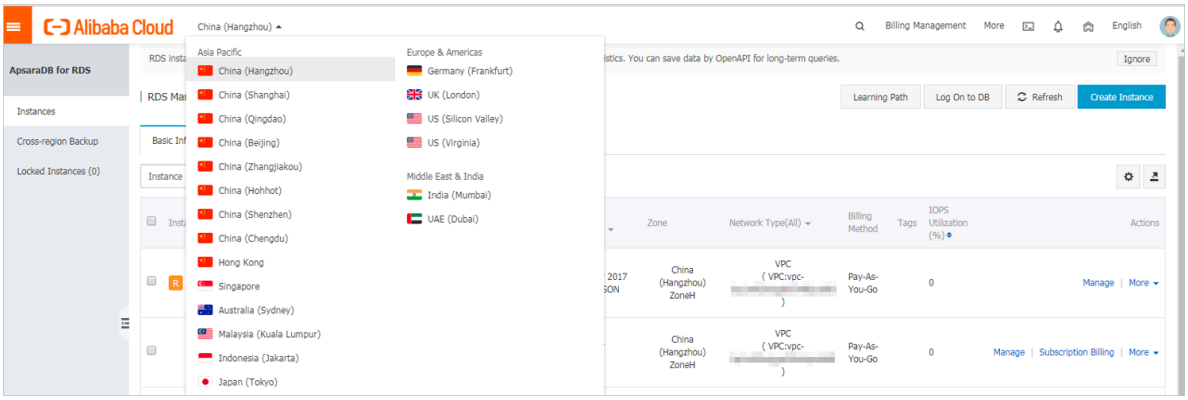
The master instance adopts the Cluster Edition and runs the SQL Server 2017 engine.

Precautions

- You can only create read-only instances under the master instance but cannot switch an existing instance to a read-only instance.
- Creating a read-only instance does not affect the master instance because the read-only instance copies data from the slave instance.
- You can create up to seven read-only instances for the master instance.
- A read-only instance is charged according to the Pay-As-You-Go billing method. That is, fees are deducted once per hour, and the deducted fees vary depending on the specifications of the read-only instance at the time of fee deduction. For more information, see the "Pricing" section in *Introduction to SQL Server read-only instances*.

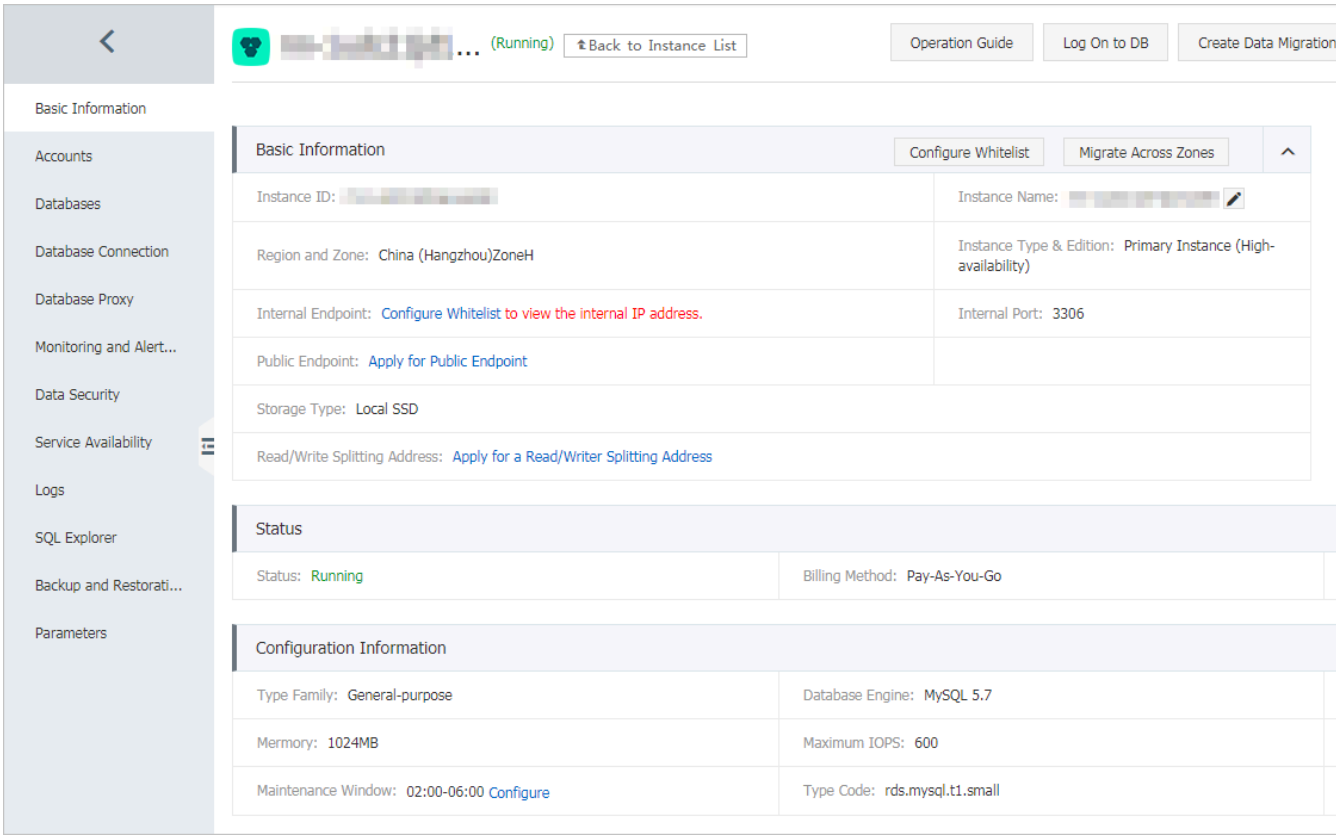
Create a read-only instance

1. Log on to the *RDS console*.
2. In the upper-left corner, select the region where the target instance is located.



3. Find the target instance and click the instance ID.

4. Click Add Read-only Instance.



5. On the purchase 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 greater than or equal to that of the master instance.
- We recommend that you purchase multiple read-only instances based on your business needs to improve availability.

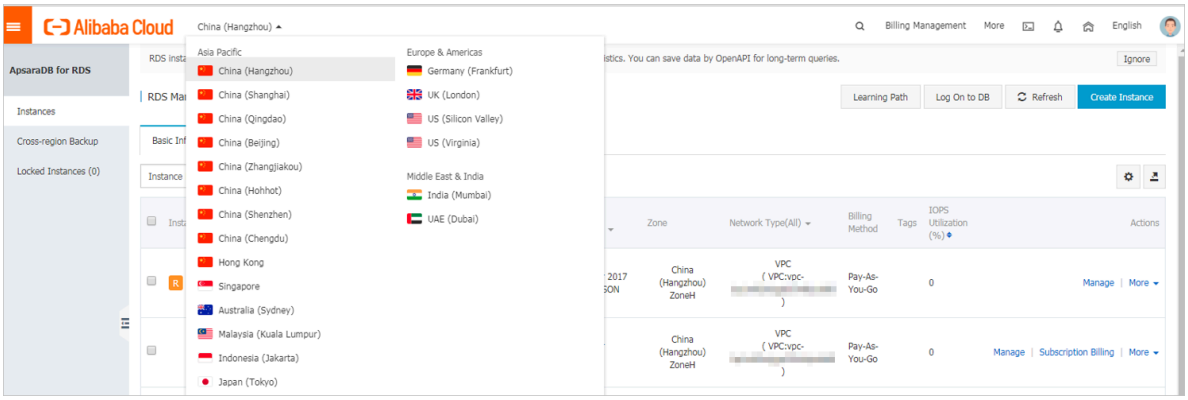
6. On the Order Confirmation page, review the order information, select the terms and agreements as prompted, click Pay Now, and complete the payment.

   The instance creation takes a few minutes.

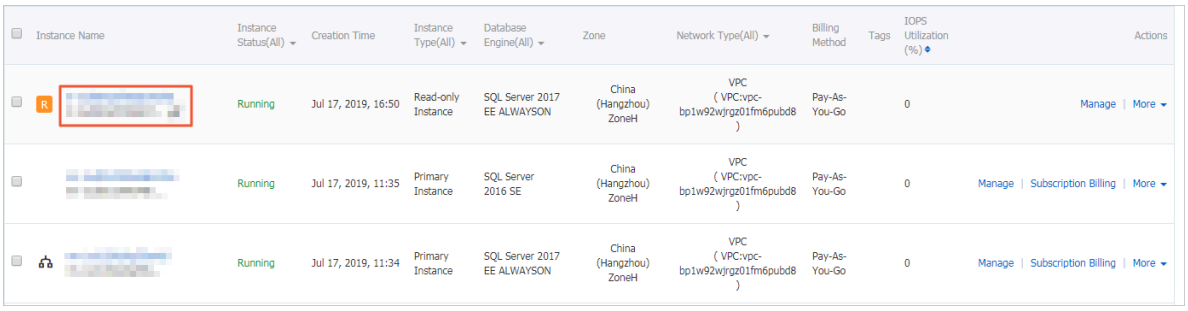
View a read-only instance

View a read-only instance in the instance list

1. Log on to the *RDS console*.
2. Select the region where the read-only instance is located.

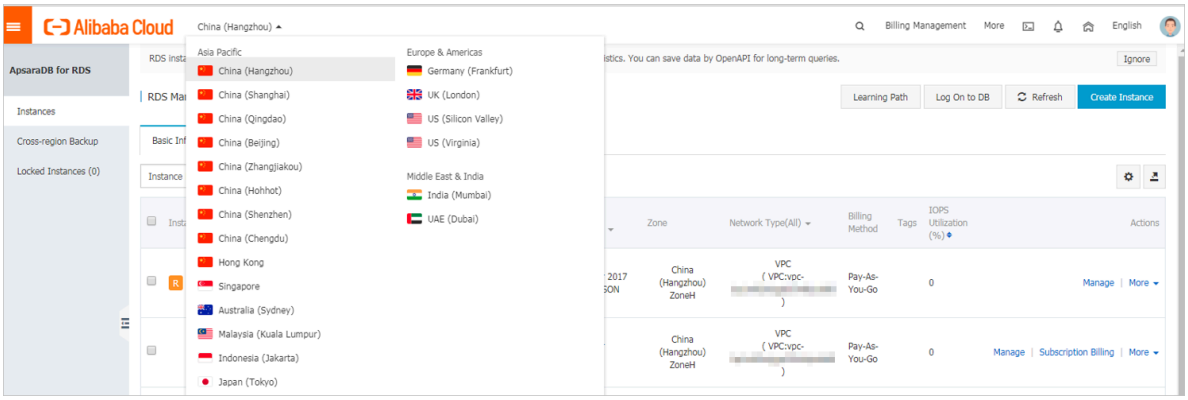


3. In the instance list, find the read-only instance and click its ID.

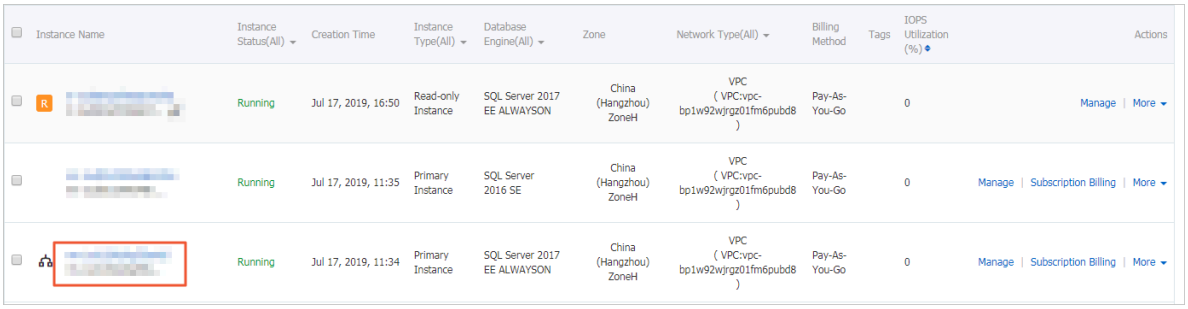


View a read-only instance on the Basic Information page for the master instance

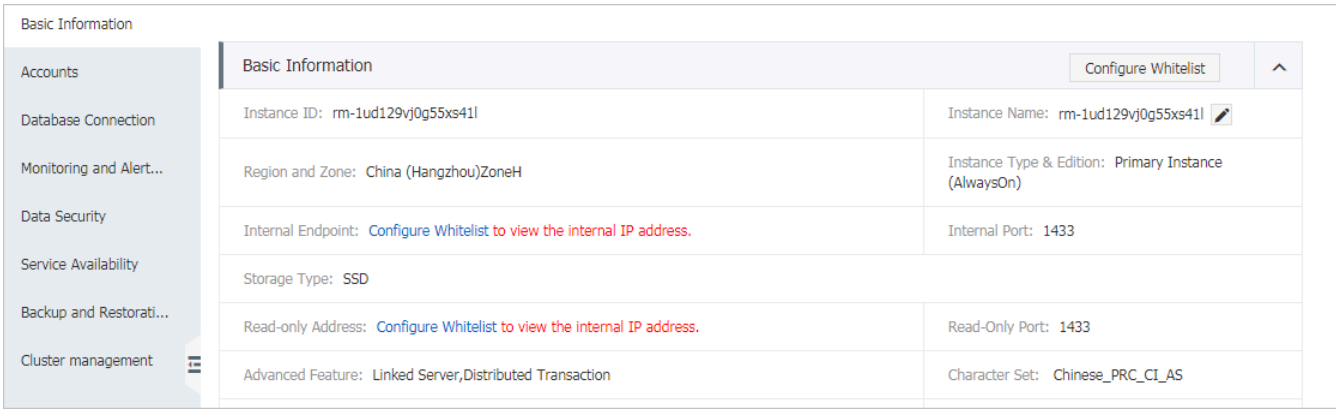
1. Log on to the *RDS console*.
2. Select the region where the master instance is located.



3. In the instance list, find the master instance and click its ID.



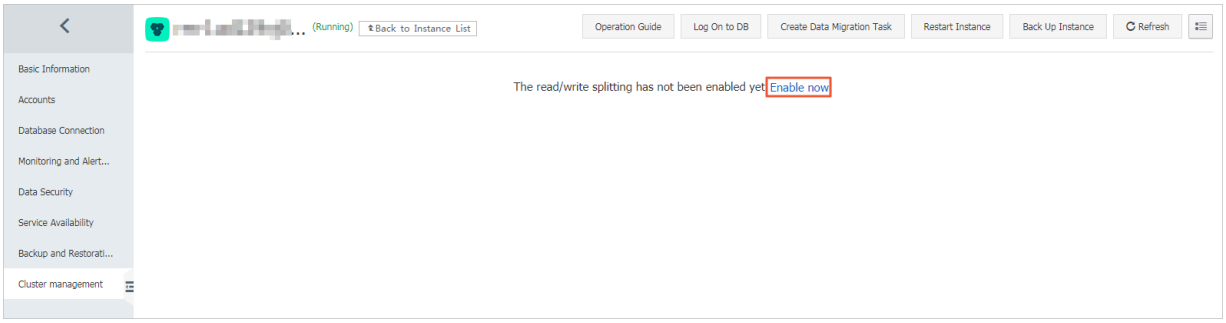
4. On the Basic Information page of the master instance, move the pointer over the number below Read-only Instance and click the ID of the read-only instance.



View a read-only instance on the Cluster management page

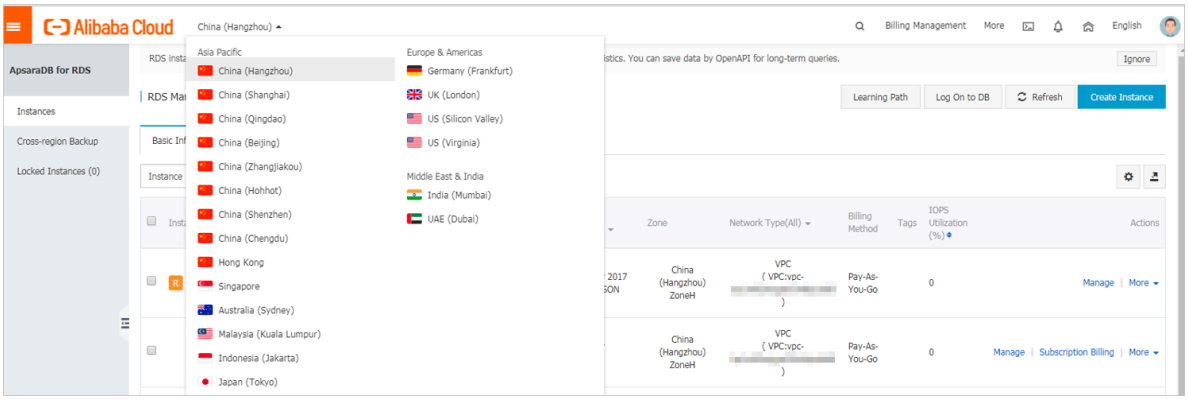
Prerequisites

You have enabled read/write splitting on the Cluster management page. For more information, see *#unique_32*.

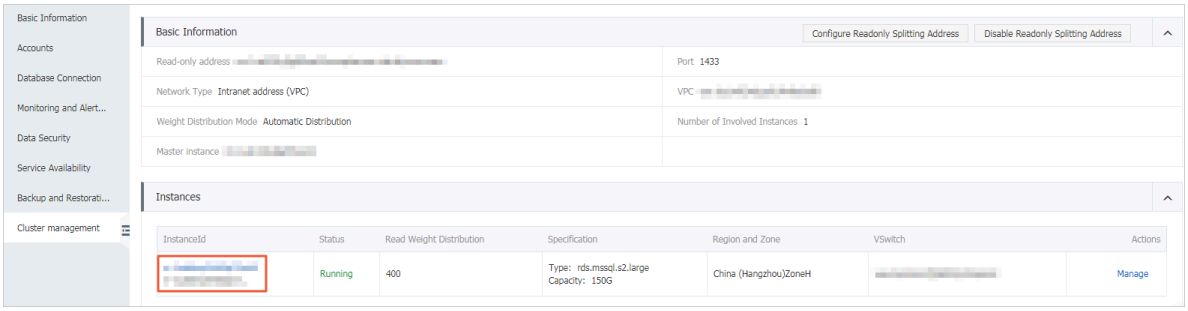


1. Log on to the *RDS console*.

2. Select the region where the master instance is located.

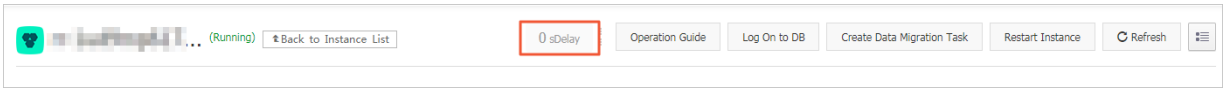


3. In the instance list, find the master instance and click its ID.
4. In the left-side navigation pane, click Cluster management.
5. Find the read-only instance and click its ID.



View the delay time of a read-only instance

When a read-only instance synchronizes data from the master instance, the read-only instance may lag behind the master instance by a small amount of time. You can view the delay on the Basic Information page of the read-only instance.



APIs

API	Description
#unique_33	Used to create an RDS read-only instance.

7.7 Release an RDS for SQL Server instance

This topic describes how to release an RDS for SQL Server instance, which can use the pay-as-you-go or subscription billing method.

> **Note:**
> **After an RDS instance is released, its data is deleted immediately. We recommend that you back up the instance data before you release the instance.**

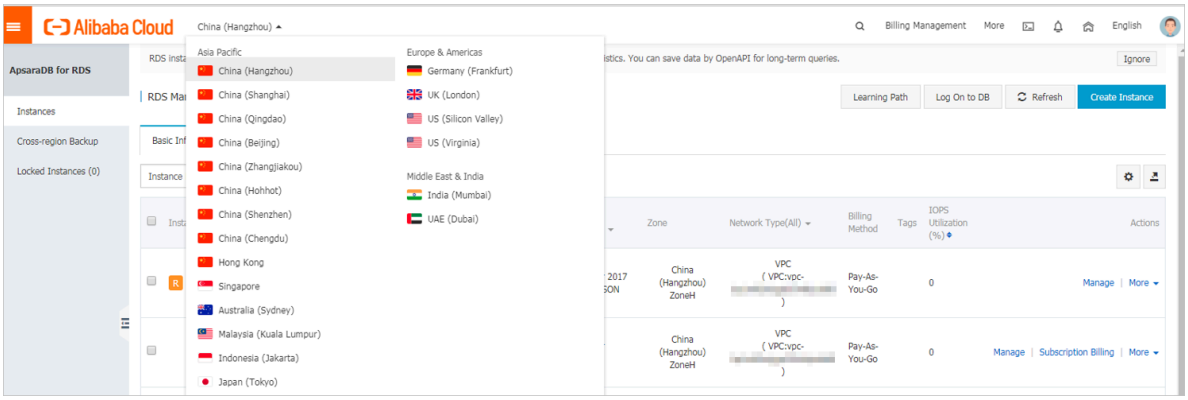
Release a pay-as-you-go-based RDS instance

Precautions

If the RDS instance you want to release is the last read-only instance of a master instance, you must *disable the cluster management function* of the master instance before releasing the last read-only instance.

Procedure

1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



3. Use one of the following two methods to open the Release Instance dialog box:

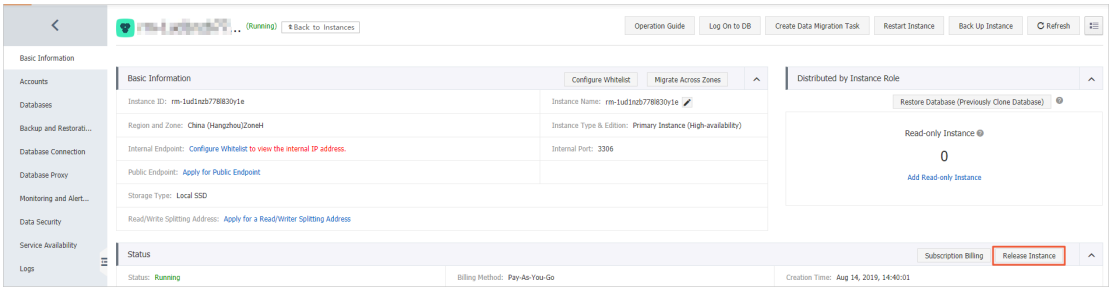
   - Method 1:

     Find the target RDS instance and in the Actions column choose More > Release Instance.

   - Method 2:

     a. Find the target RDS instance and click the instance ID.

     b. On the Basic Information page, find the Status section and click Release Instance.



4. In the Release Instance dialog box, click Confirm.

Release a subscription RDS instance

You can *open a ticket* to apply for releasing a subscription RDS instance.

APIs

API	Description
DeleteDBInstance	Used to release a pay-as-you-go-based RDS instance. (A subscription-based RDS instance cannot be released by calling an API action.)

7.8 Change the configuration of an RDS for SQL Server instance

This topic describes how to change the configuration of an RDS for SQL Server instance, including changing the edition, specifications, storage capacity, storage class, and zone.

Change methods

You can upgrade or downgrade the configuration of an RDS for PPAS instance at any time regardless of whether the instance uses the subscription or pay-as-you-go billing method. The new configuration takes effect immediately after you complete the configuration upgrade or downgrade.

Configuration items

If you want to horizontally scale the read capability of an RDS for PPAS instance, you can create read-only instances. For more information, see *Introduction to SQL Server read-only instances* **and** *Create an RDS for SQL Server read-only instance*.

Configuration item	Description
Version	Some versions can be upgraded to later versions.
Edition	The Basic Edition can be upgraded to the High-availability Edition.
CPU and Memory	All SQL Server DB engine versions and editions support the CPU and memory change.
Capacity	All SQL Server DB engine versions and editions allow you to increase storage capacity. **Note:** · You cannot decrease the storage capacity of an RDS instance. · For information about the capacity range, see #unique_20. · If the storage capacity range of the current specifications cannot meet your requirements, you can change the specifications.

Note:
Changing the preceding configuration does not change the endpoints of the RDS instance.

Billing

For more information, see *#unique_59*.

Prerequisites

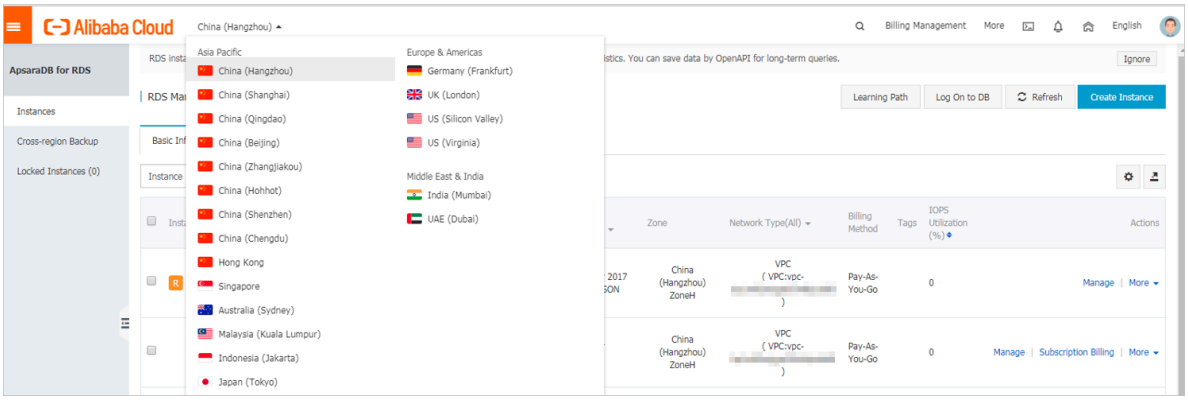
Your Alibaba Cloud account does not have an unpaid renewal order.

Precautions

- **When the new configuration is taking effect, the RDS instance may be disconnected for about 30 seconds and most operations related to databases, accounts, and networks cannot be performed. Therefore, we recommend that you change the configuration during off-peak hours or make sure that your application can automatically reconnect to the RDS instance.**
- **If the RDS instance is in the *#unique_57* (which has no slave node as hot backup), it becomes unavailable for a long time during the configuration change. Therefore, if you have high requirements for database availability, we recommend that you select an edition higher than the Basic Edition. For example, you can select the *#unique_58*.**

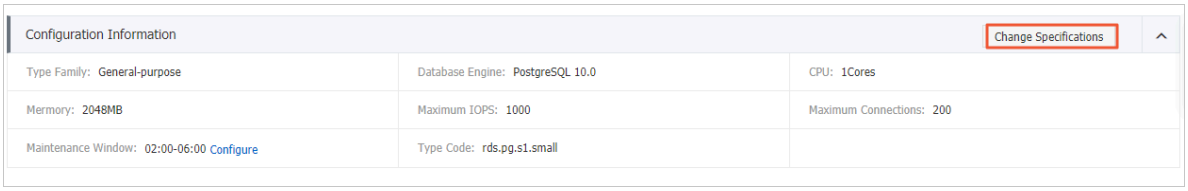
Procedure

1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance and click the instance ID.**

4. On the Basic information page, find the Configuration Information section and click Change Specifications.

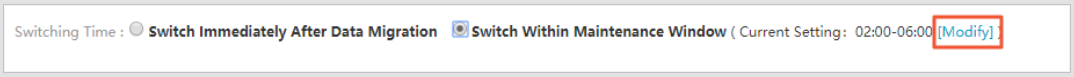


5. Optional. If the RDS instance uses the subscription billing method, click Next in the displayed dialog box.
6. On the Change Specifications page, change the instance configuration. For more information, see *Configuration items*.
7. Specify the time at which you want to change the configuration.
   - Switch Immediately After Data Migration: Change the configuration immediately after the data migration.
   - Switch Within Maintenance Window: Change the configuration during the *maintenance window*.

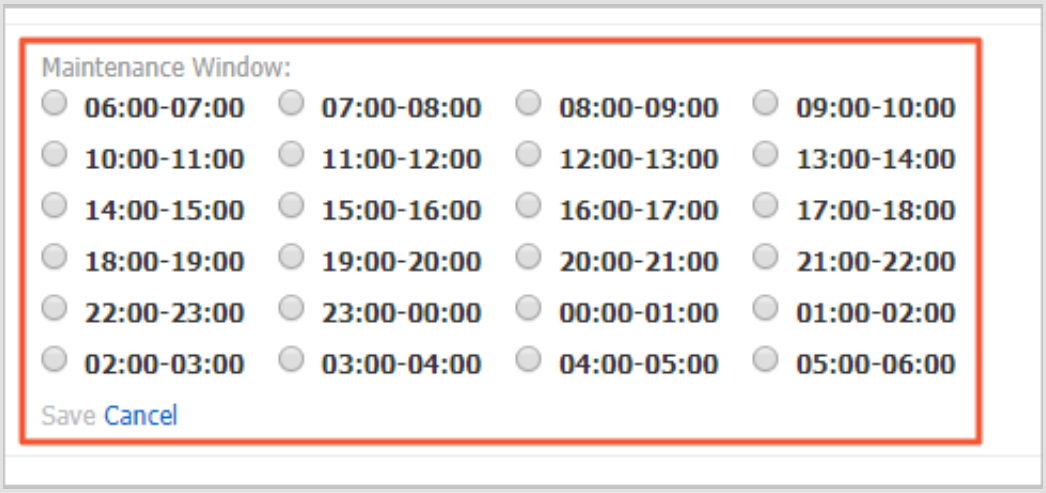
Note:

To change the maintenance window, follow these steps:

a. Click Modify.



b. In the Configuration Information section, select a maintenance window and click Save.



c. Go back to the Change Specifications page, refresh the page, and change the configuration again.

8. **Select Terms of Service, Service Level Agreement, and Terms of Use and click Confirm.**

FAQ

1. **How can I change the storage class (local SSD, SSD, or ESSD) of an RDS instance?**

   See *#unique_88*

2. **Can I change the zone and version of an RDS instance?**

   You can change the zone and version of an RDS instance only when the instance runs the SQL Server 2008 R2 engine. You can *migrate an RDS for SQL Server instance across zones in the same region* **separately. Alternatively, you can change the zone of an RDS for SQL Server instance when you** *upgrade the instance version from SQL Server 2008 R2 to SQL Server 2012/2016***.**

3. **Do I need to migrate data if I only want to expand the storage capacity of an RDS instance?**

   Check whether the server where the RDS instance is located provides sufficient storage capacity for expansion. If yes, you do not need to migrate data and can directly expand the storage capacity. If no, you must migrate data to a server that provides sufficient storage capacity before you expand the storage capacity.

7.9 Reconfigure parameters for an RDS for SQL Server instance

7.9.1 Reconfigure parameters by using SQL commands

This topic describes how to reconfigure parameters for an RDS for SQL Server instance by using SQL commands.

Note:

This topic is applicable to RDS for SQL Server 2012 and later versions. For information about how to reconfigure parameters for an RDS instance that uses the SQL Server 2008 R2 engine, see *Reconfigure parameters the in the RDS console***.**

Parameters supported

- **fill factor (%)**
- **max worker threads**
- **cost threshold for parallelism**

- **max degree of parallelism**
- **min server memory (MB)**
- **max server memory (MB)**
- **blocked process threshold (s)**

Reconfigure parameters

Use `sp_rds_configure` to specify the target configuration item. If the reconfigured parameter requires the RDS instance to restart, the system displays a message to suggest you.

For example, you can run the following command to reconfigure a parameter:

```
USE master
GO
--database engine edtion
SELECT SERVERPROPERTY('edition')
GO
--create database
CREATE DATABASE testdb
GO
SELECT *
FROM sys.configurations
WHERE NAME = 'max degree of parallelism'
EXEC sp_rds_configure 'max degree of parallelism',0
WAITFOR DELAY '00:00:10'
SELECT *
FROM sys.configurations
WHERE NAME = 'max degree of parallelism'
```

7.9.2 Reconfigure parameters the in the RDS console

This topic describes how to reconfigure parameters and view the parameter reconfiguration history for an RDS for SQL Server instance in the RDS console.

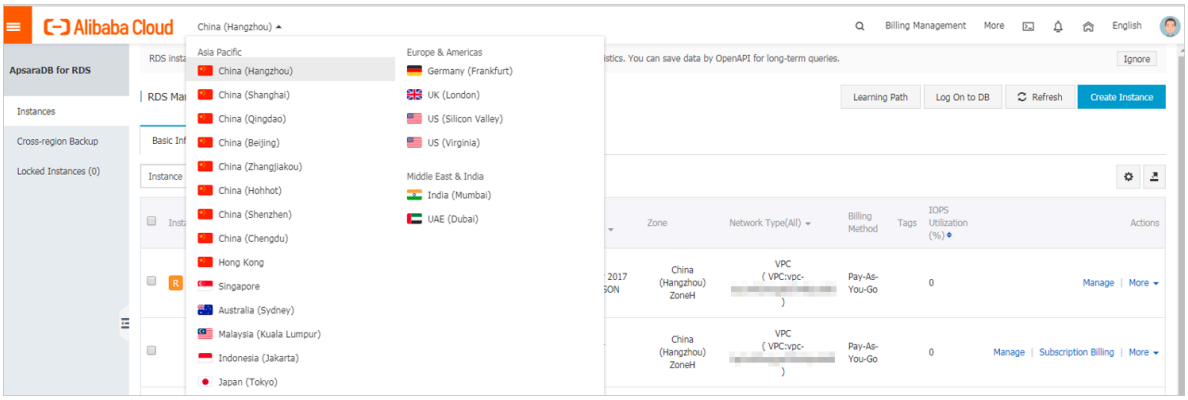
Note:

In SQL Server 2012 or later, you can reconfigure parameters only by using SQL commands. For more information, see *Reconfigure parameters by using SQL commands*.

Reconfigure parameters

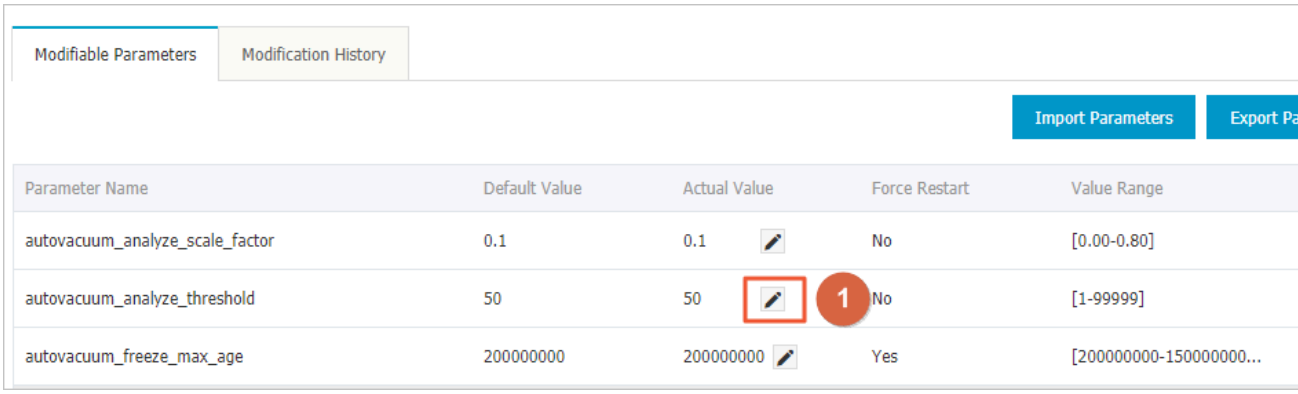
1. **Log on to the** *RDS console*.

2. In the upper-left corner, select the region where the target RDS instance is located.

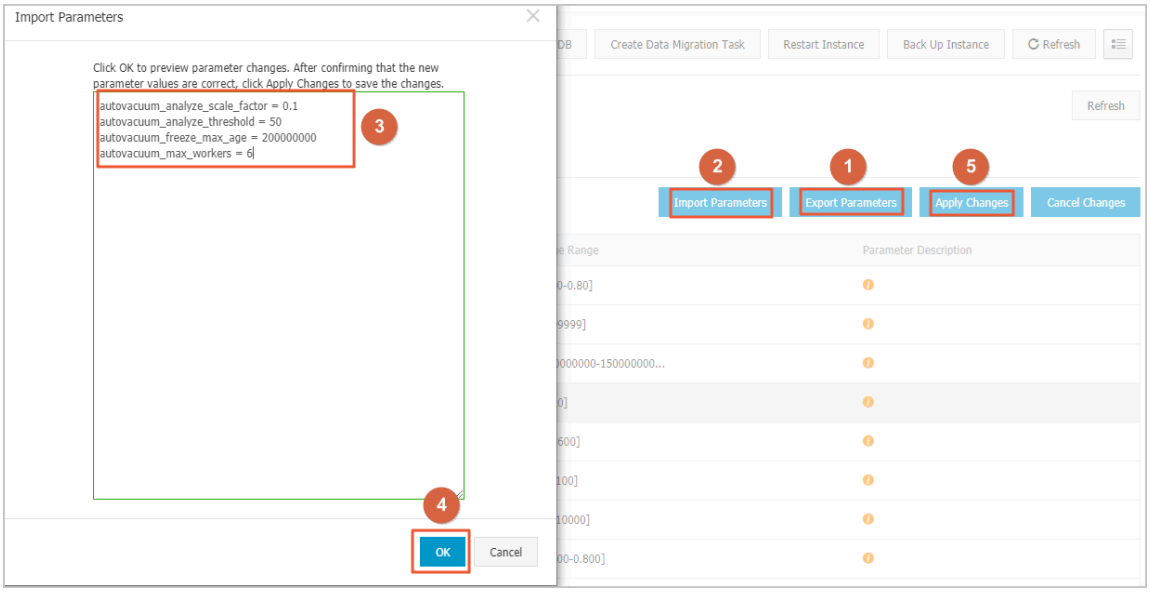


3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Parameters.

5. On the Modifiable Parameters tab, reconfigure one or more parameters as needed.
   - To reconfigure only one parameter of the RDS instance, follow these steps:
     a. Find the parameter you want to reconfigure, and in the Actual Value column click .
     b. In the displayed dialog box, enter a new value within the value range and click Confirm.
     c. In the upper-right corner, click Apply Parameters.
     d. In the displayed dialog box, click Confirm.



   - To reconfigure more than one parameter of the RDS instance, follow these steps:
     a. In the upper-right corner, click Export Parameters to export the parameters as a file to your computer.
     b. Open the parameter file on your computer and reconfigure the parameters.
     c. In the upper-right corner, click Import Parameters.
     d. Copy the parameters and their values from the parameter file and paste them to the Import Parameters dialog box, then click OK.
     e. Verify the parameter values, and click Apply Changes.



View the parameter reconfiguration history

1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**

3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Parameters.**
5. **Click the Modification History tab.**
6. **Select a time range and click Search.**

APIs

- *#unique_92*
- *#unique_93*
- *#unique_94*

Parameter reference

For more information, see *Server Configuration Options (SQL Server)*.

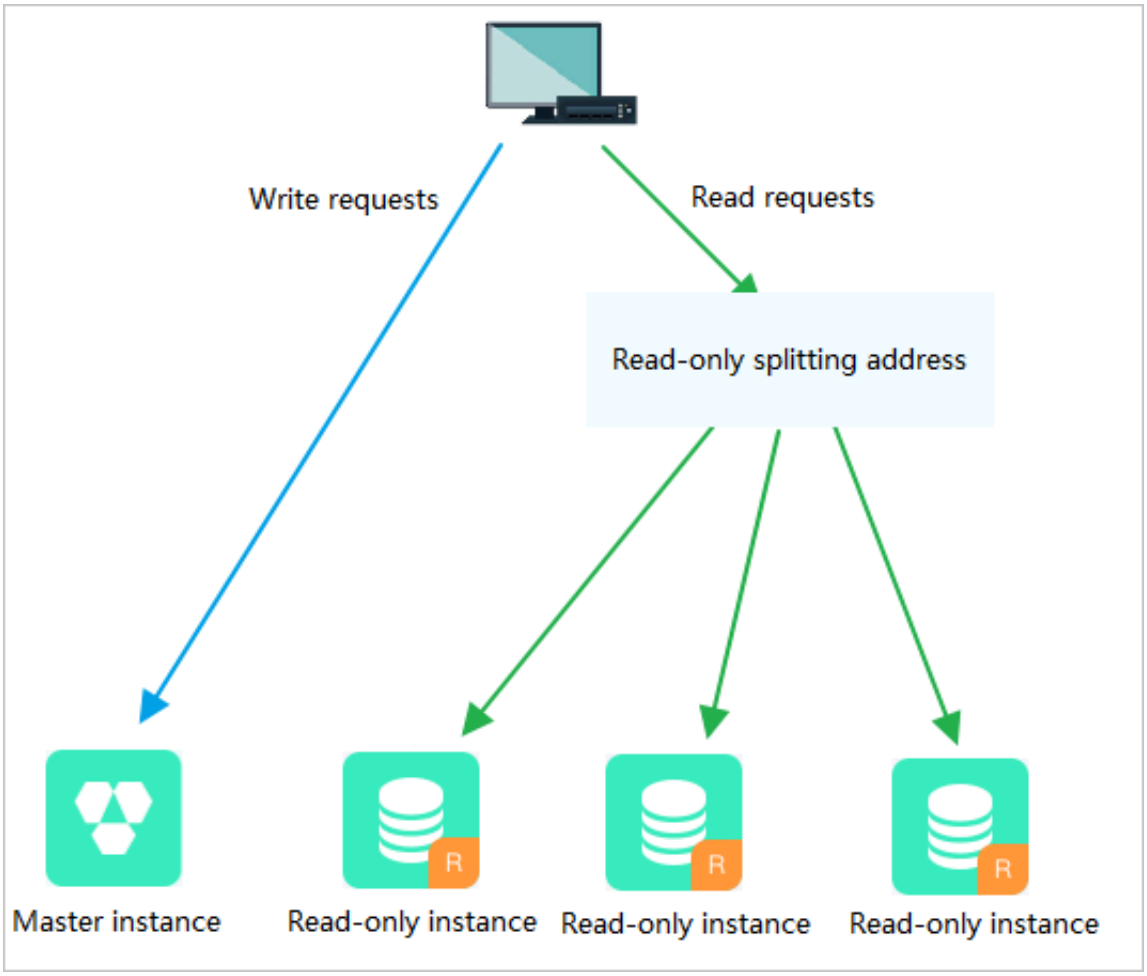
8 SQL Server read/write splitting

8.1 Introduction to read/write splitting

This topic introduces the read/write splitting function of SQL Server. This function enables RDS to distribute read and write requests through a read-only splitting address.

If your application initiates a small number of write requests but a large number of read requests, a single instance may not be able to resist the read pressure. As a result, services 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 and increase the application throughput.

After read-only instances are created, you can enable the cluster management function, and then configure the connection information of the master instance and the automatically generated read-only splitting address in your application. All read and write requests are sent to the read-only splitting address. Then the system distributes the write requests to the master instance and the read requests to the read-only instances based on the read weights of the read-only instances.



Differences between the read-only address and internal and public endpoints

After you enable the read/splitting function for an RDS master instance, a read-only splitting address is generated. You must configure the read-only splitting address in your application. The read requests from the application are sent to the read-only splitting address and then are distributed to the read-only instances of the master instance based on the read weights of the read-only instances.

If the connection address you have configured in your application is the internal or public endpoint of the master instance, all requests are sent to the master instance . Therefore, if you want to use read/write splitting, you must add the connection information and read-weights of the master and read-only instances to your application.

Benefits

- **Facilitates maintenance with a single read-only splitting address.**

  The read/write splitting function provides an additional address called read-only splitting address. You can connect to this address to perform read operations on

the read-only instances, with read requests automatically distributed. Therefore, maintenance costs are reduced.

Additionally, you can increase the processing capability of your DB system by adding read-only instances without making any changes to your application.

- Improves performance with support for the highly secure link.

  For users who build a proxy layer to implement read/write splitting on the cloud, data has to go through multiple components for statement parsing and forwarding before it reaches the database, significantly increasing the response latency. RDS read/write splitting can be directly set in the existing highly secure link without time consumption by any other components, which reduces the latency and improves the processing rate.
- Applies to various scenarios with customizable read weights.

  You can customize the read weights of read-only instances as needed.
- Enhances database availability with instance health checks.

  RDS read/write splitting performs health check automatically for all instances in the distribution system. If any instance fails or its latency exceeds the threshold, RDS automatically removes the instance out of the distribution system (while marking it as unavailable and stopping allocating read requests to it) and allocates read and write requests to the remaining healthy instances by the predefined weights. In this way, applications still run properly even if any single-node read-only instance fails. After the instance resumes, RDS automatically reclaims it into the request distribution system.

   **Note:**
  To prevent single node failures, we recommend that you create at least two read-only instances for each master instance if you are using read/write splitting.
- Reduces resource and maintenance costs with free services.

  The read/write splitting function is free of charge.

   **Note:**
  You only need to pay for the *read-only instances* you use.

8.2 Enable cluster management for an RDS for SQL Server instance

This topic describes how to enable the cluster management function for an RDS for SQL Server master instance. After this function is enabled, the system generates a read-only splitting address. You can configure the connection information of the master instance and the read-only splitting address in your application. The system distributes write requests to the master instance and read requests to the read-only address. The read-only splitting address then distributes the read requests to the read-only instances based on the specified read weights.

Prerequisites

- **The target RDS instance is a master instance.**
- **The used DB engine version and edition are SQL Server 2017 Cluster Edition.**
- **The target RDS instance has at least one read-only instance. For information about how to create a read-only instance, see** *Create an RDS for SQL Server read-only instance*.

Precautions

- **If it is the first time that you enable the read/write splitting function, the system automatically upgrades the backend administration systems of the master and read-only instances to the latest version to guarantee service availability. When the read/write splitting function is being enabled, the master instance is disconnected for 30 seconds or less. Additionally, the read-only instances is inaccessible during the whole restart process. We recommend that you enable the read/write splitting function during off-peak hours and make sure that your application can automatically reconnect to the RDS instance.**
- **If you have restarted or changed the specifications at least once for the master instance and its associated read-only instances after March 8, 2017, the backend administration systems of these instances have been automatically upgraded to the latest version. In such case, when you enable the read/write splitting function, the system does not restart the RDS instance or generate a transient disconnection.**
- **The generated read-only splitting address is fixed. It does not change even when you enable and disable the cluster management function for multiple times.**

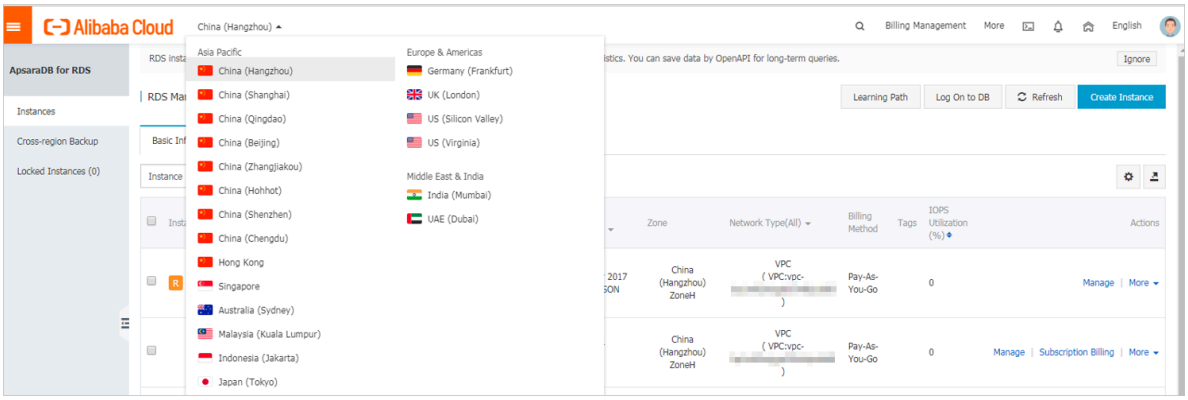
Therefore, you do not need to change the configuration data on your application frequently. This reduces maintenance costs.

> **Note:**
> **The read-only splitting address cannot be changed manually.**

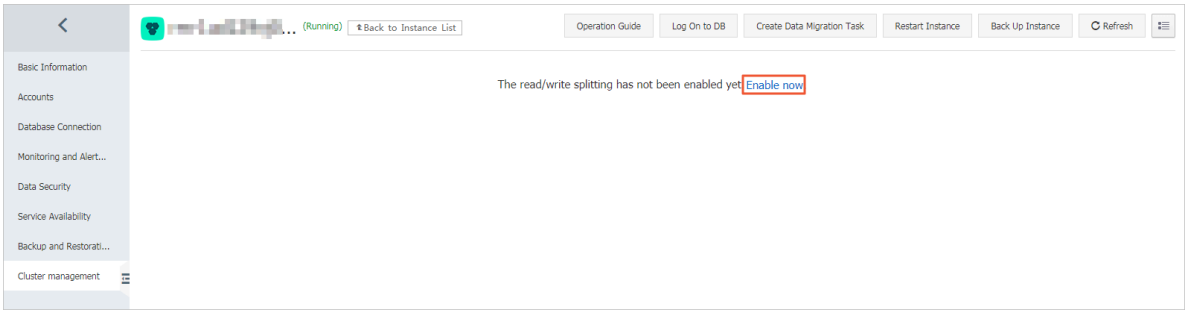
- **The cluster management function is free of charge. You pay only for the *read-only instances* you use.**
- **The cluster management function does not support classic networks.**

Procedure

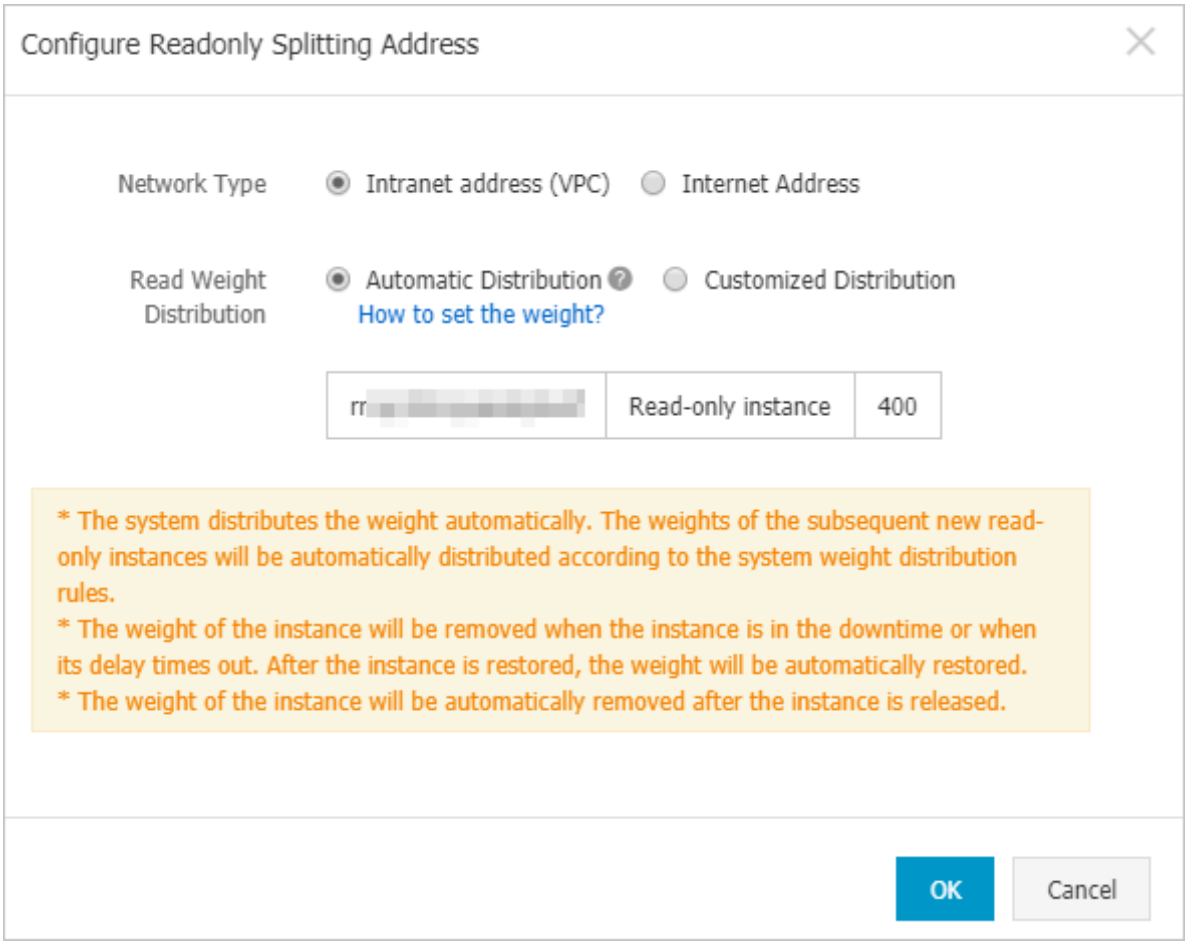
1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Cluster management.**
5. **In the main workspace, click Enable now.**



6. Set the parameters shown in the following figure.



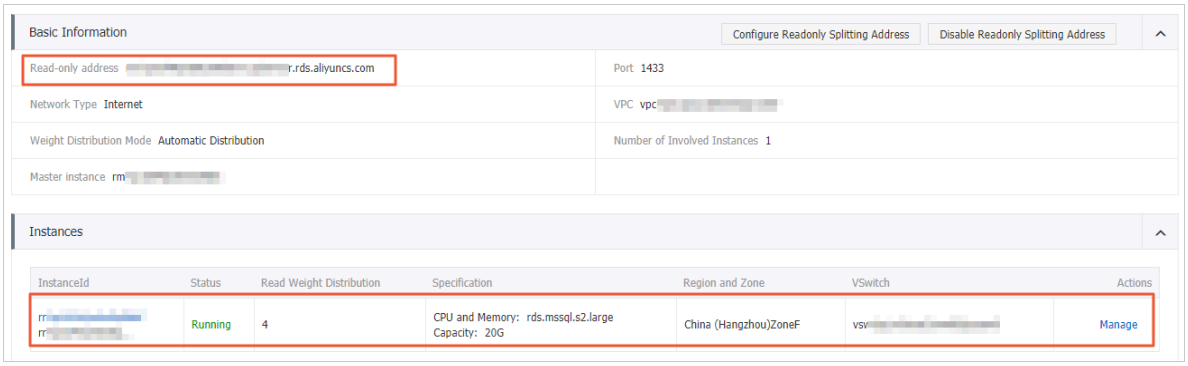
Parameter	Description
Network Type	**The type of the read/write splitting address.** · **Intranet address** - **If the network type of the master instance is VPC, then the network type of the read/write splitting address is also VPC.** - **If the network type of the master instance is Classic Network, then the network type of the read/write splitting address is also Classic Network.** · **Internet Address: used to access the RDS instance from the Internet. The Internet is prone to fluctuations. Therefore, we recommend that you use an internal endpoint to connect to the RDS instance.**

Parameter	Description
Read Weight Distribution	A higher read weight indicates more read requests to process. For example, the master instance has three read-only instances, and their read weights are 0, 100, 200, and 200, respectively. Then the master instance does not process read requests (write requests are still automatically sent to the master instance), and the three read-only instances process read requests at the 1:2:2 ratio. · Automatic Distribution: The system automatically assigns a read weight to each instance based on the instance specifications. After a read-only instance is created, it is automatically added to the read/write splitting link according to the read weight assigned by the system. For more information, see *Rules of weight distribution by the system*. · Customized Distribution: You can manually set the read weight of each instance. The value ranges from `0` to `10000`. After a read-only instance is created, its read weight is `0` by default. You must manually specify a read weight for the read-only instance. **Note:** You cannot specify a read weight for a read-only instance for which a *replication latency* is specified.

7. Click OK.

What to do next

· You can add the connection information of the master instance and the read-only splitting address to the configuration data of your application. After you do so, the system distributes write requests to the master instance and read requests to the read-only splitting address. The read-only splitting address then distributes the read requests to the read-only instances based on the specified read weights.



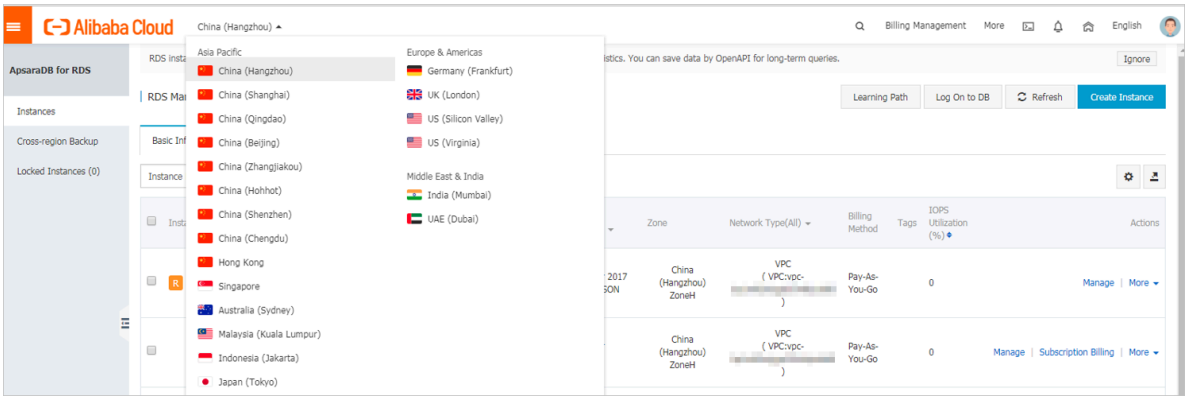
- **You can view the ID, running status, and read weight of each read-only instance. Additionally, you can click Manage in the Actions column for a read-only instance to manage the instance on the page for the instance.**

8.3 Modify the read weights

This topic describes how to modify the read weights when read/write splitting is enabled.

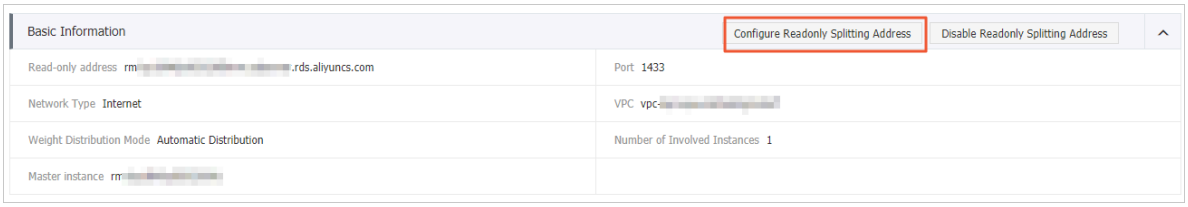
Procedure

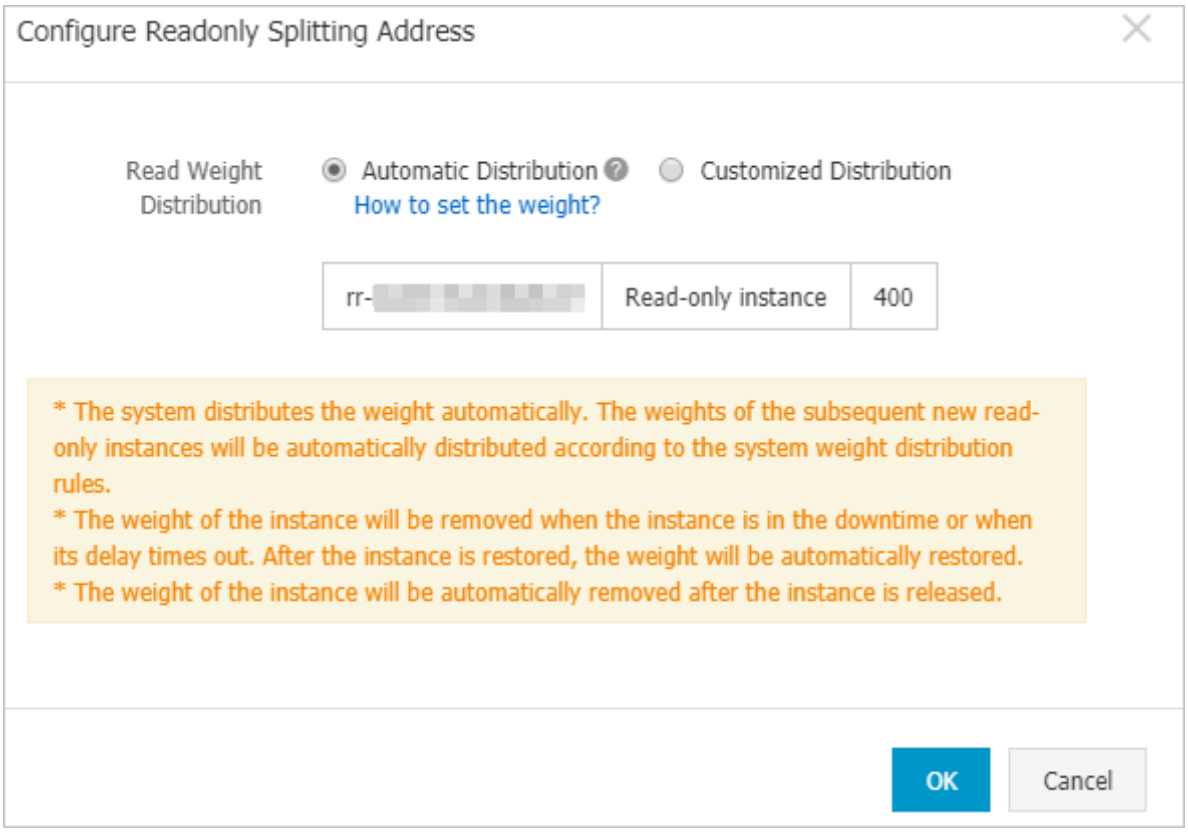
1. **Log on to the *RDS console*.**
2. **Select the target region.**



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Cluster management.**

5. In the left-right corner, click Configure Readonly Splitting Address.





Parameter	Description
Read Weight Distribution	**A higher read weight indicates a larger number of read requests to be processed. For example, if the master instance has three read-only instances whose read weights are 100, 200, and 200, respectively, then the three read-only instances process read requests according to a 1:2:2 radio.** **· Automatic Distribution: The system automatically allocates a read weight to each existing or new read-only instance according to the instance specifications. For more information, see *Rules of weight distribution by the system*.** **· Customized Distribution: You must manually set the read weight of each existing read-only instance. The read weight ranges from 0 to 10000. When a new read-only instance is added, its read weight is 0 by default and you must manually modify its read weight as needed.** **Note:** **When a read-only instance is deleted, its read weight is removed automatically. The read weights of the other read-only instances remain unchanged.**

8.4 Disable cluster management for an RDS for SQL Server instance

This topic describes how to disable the cluster management function for an RDS for SQL Server instance.

Prerequisites

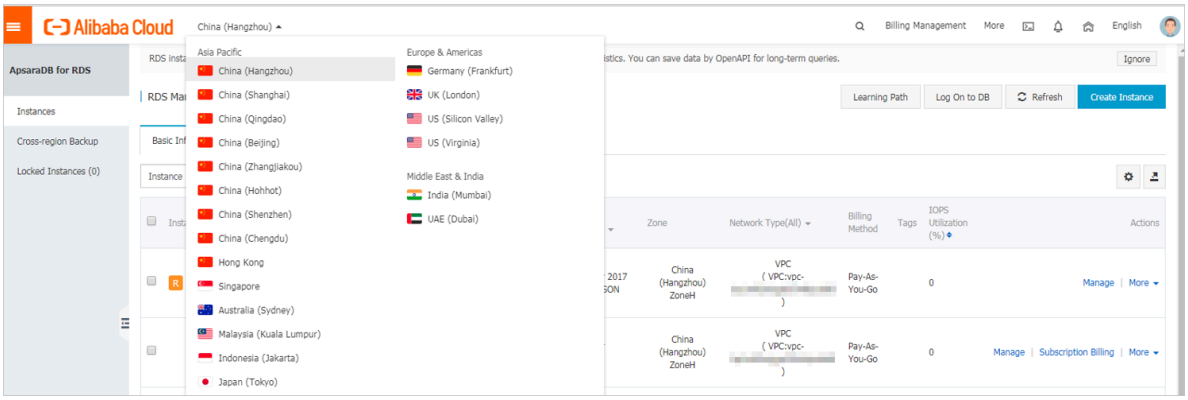
The cluster management function is enabled. For more information, see *Enable cluster management for an RDS for SQL Server instance*.

Precautions

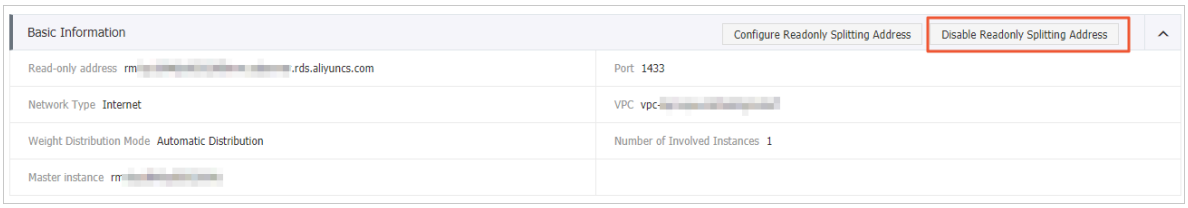
- **When the cluster management function is being disabled, the RDS instance is disconnected for 30 seconds or less. We recommend that you disable this function during off-peak hours and make sure that your application can automatically reconnect to the RDS instance.**
- **After the cluster management function is disabled, the read-only splitting address becomes invalid. Make sure that your application no longer uses the read-only splitting address to connect to the RDS instance.**

Procedure

1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Cluster management.**
5. **In the upper-right corner, click Disable Readonly Splitting Address.**



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

8.5 Rules of weight distribution by the system

This topic introduces the rules of weight distribution by the system.

When the read weights are automatically set for instances by the system, the values of these weights are fixed, as shown in the following table.

Table 8-1: Weights for SQL Server read-only instances

Specification code	Specification type	Memory	CPU	Weight
rds.mssql.s2.large	General-purpose instance	4 GB	2	400

Specification code	Specification type	Memory	CPU	Weight
rds.mssql.s3.large	General-purpose instance	8 GB	4	800
rds.mssql.c1.large	General-purpose instance	16 GB	8	1600
rds.mssql.s2.xlarge	General-purpose instance	8 GB	2	800
rds.mssql.m1.medium	General-purpose instance	16 GB	4	1600
rds.mssql.c1.xlarge	General-purpose instance	32 GB	8	3200
rds.mssql.c2.xlarge	General-purpose instance	64 GB	16	6400

9 Account

9.1 Create an account for an RDS for SQL Server instance

This topic provides information about how to create an account for an RDS for SQL Server instance. The account creation method varies depending on the used SQL Server version.

For more information, see the following resources:

- *SQL Server 2008 R2*
- *SQL Server 2017Standard/2016/2012*
- *SQL Server 2017Cluster (AlwaysOn)*

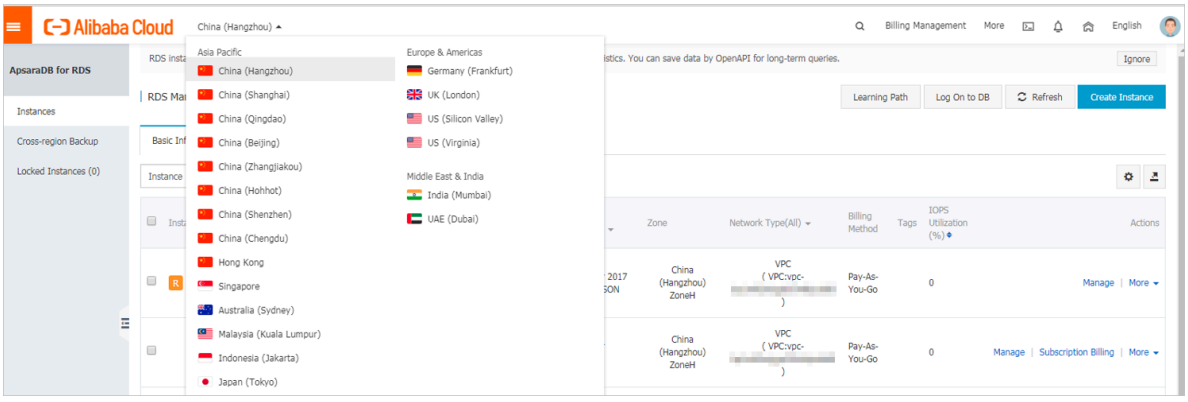
9.2 Reset the password of an account for an RDS for SQL Server instance

This topic describes how to reset the password of an account for an RDS for SQL Server instance in case that the password is lost.

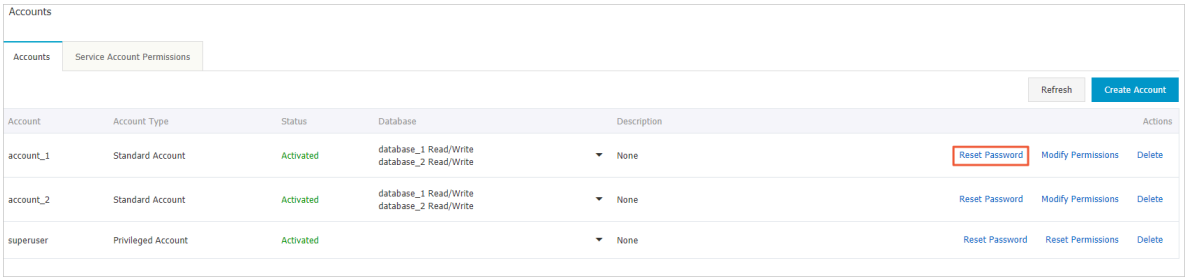
> **Note:**
> **For data security purposes, we recommend you change the password on a regular basis.**

Procedure

1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Accounts.
5. On the Accounts tab, select the account whose password you want to reset, and in the Actions column click Reset Password.



6. In the Reset Account Password dialog box, enter a new password and confirm it, then click OK. The password consists of 6 to 32 characters including letters, digits, hyphen (-), or underscores (_). A previously used password is not recommended.

APIs

API	Description
#unique_104	Used to reset the password of a database account.

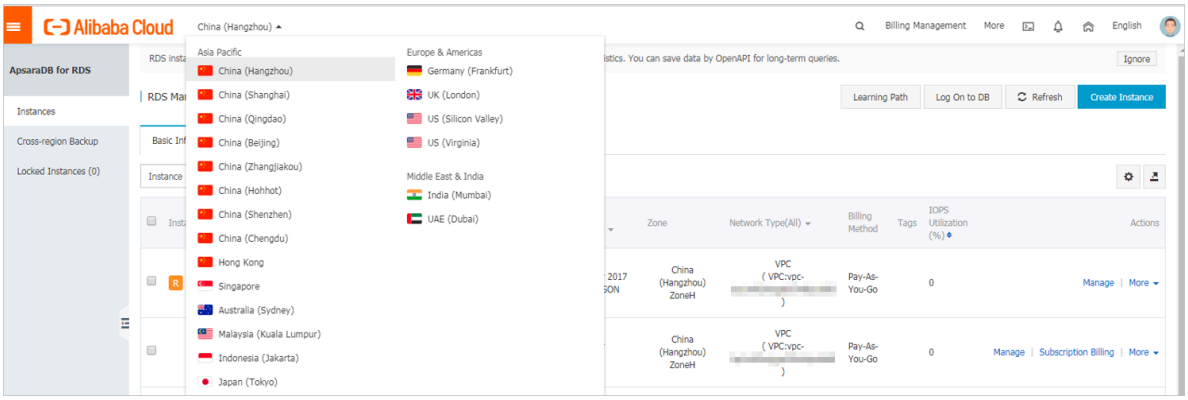
9.3 Change the permissions of an account for an RDS for SQL Server instance

This topic describes how to change the permissions of a standard account for an RDS for SQL Server instance. The permissions of the premier account cannot be changed. You can only reset the premier account if needed.

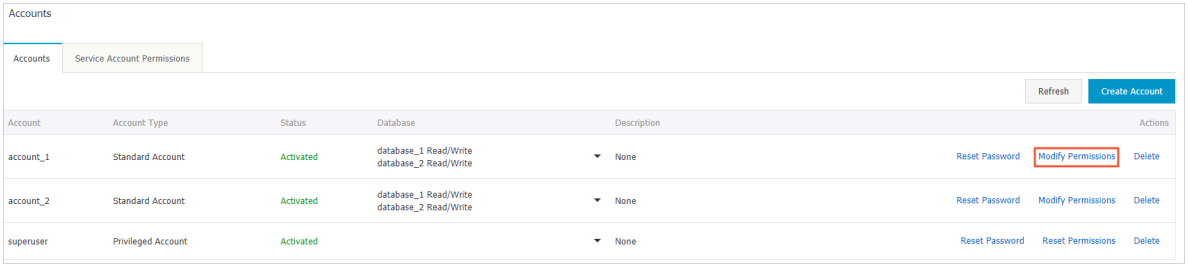
Procedure

1. Log on to the *RDS console*.

2. In the upper-left corner, select the region where the target RDS instance is located.



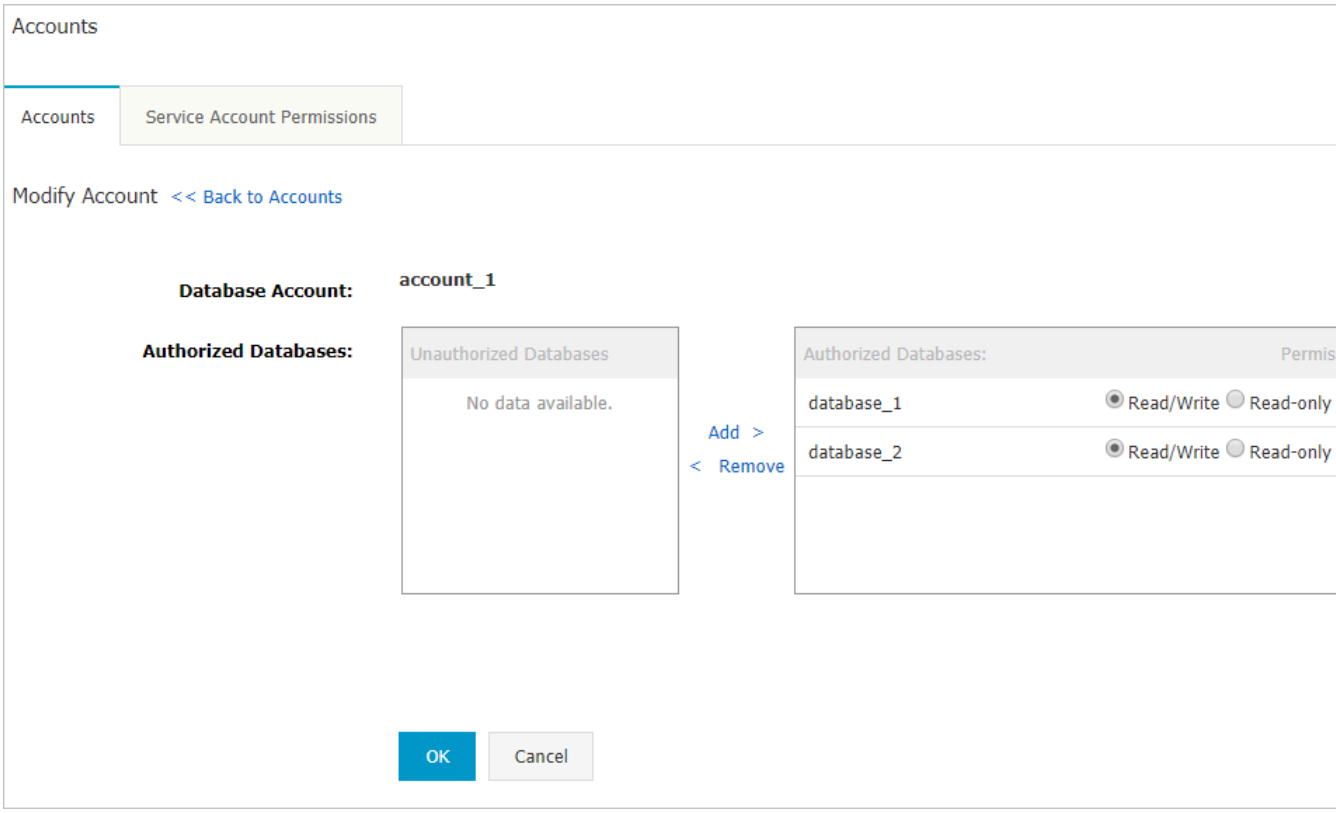
3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Accounts.
5. On the Accounts tab, find the target account and in the Actions column click Modify Permissions.



6. Change the account permissions and click OK.
   - Add an authorized database: Select a database in the Unauthorized Databases section and then click Add > to add it to the Authorized Databases section.
   - Delete an authorized database: Select a database in the Authorized Databases section and then click < Remove to add it to the Unauthorized Databases section.
   - Change the permissions of an authorized database: Find the database in the Authorized Databases section and select Read/Write, Read-only, DDL Only, or DML Only. To change the permissions of more than one authorized database in batches, you can click Full Control Read/Write, Full Control Ready-only, Full Control DDL Only, or Full Control DML Only in the upper-right corner of the Authorized Databases section.

Note:

Either of them is displayed at a time.



9.4 Authorize a service account for an RDS for SQL Server instance

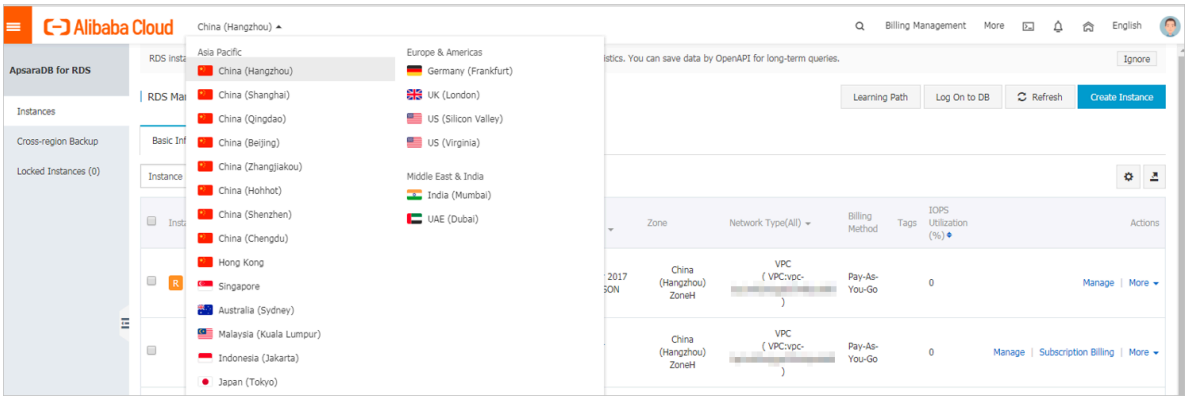
This topic describes how to authorize a service account for an RDS for SQL Server instance. If you are seeking for technical support from Alibaba Cloud and if it is necessary to operate your DB instance during technical support, you must authorize a service account that is used by the technical support staff to provide technical support services. When the authorized account validity period elapses, the system automatically deletes the temporary service account.

Note:
This function is available only to SQL Server 2008 R2.

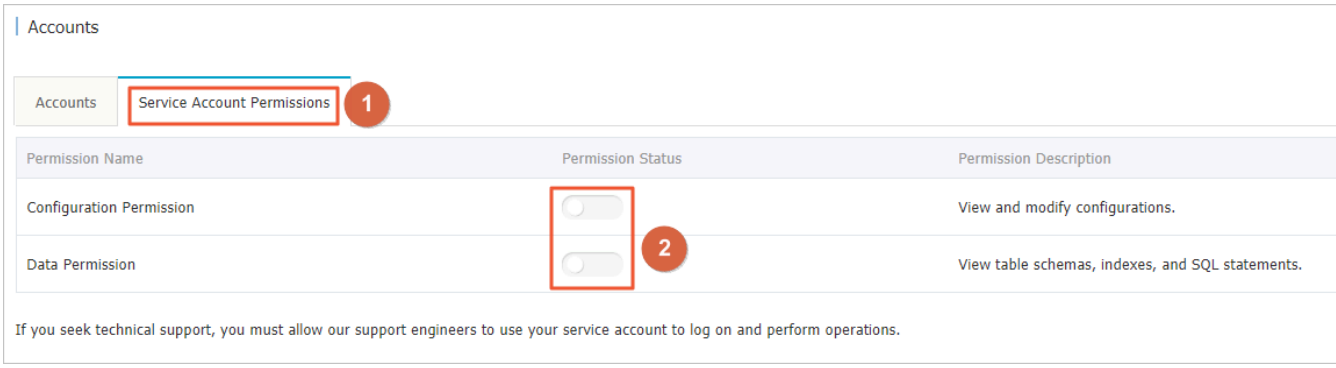
Procedure

1. **Log on to the** *RDS console*.

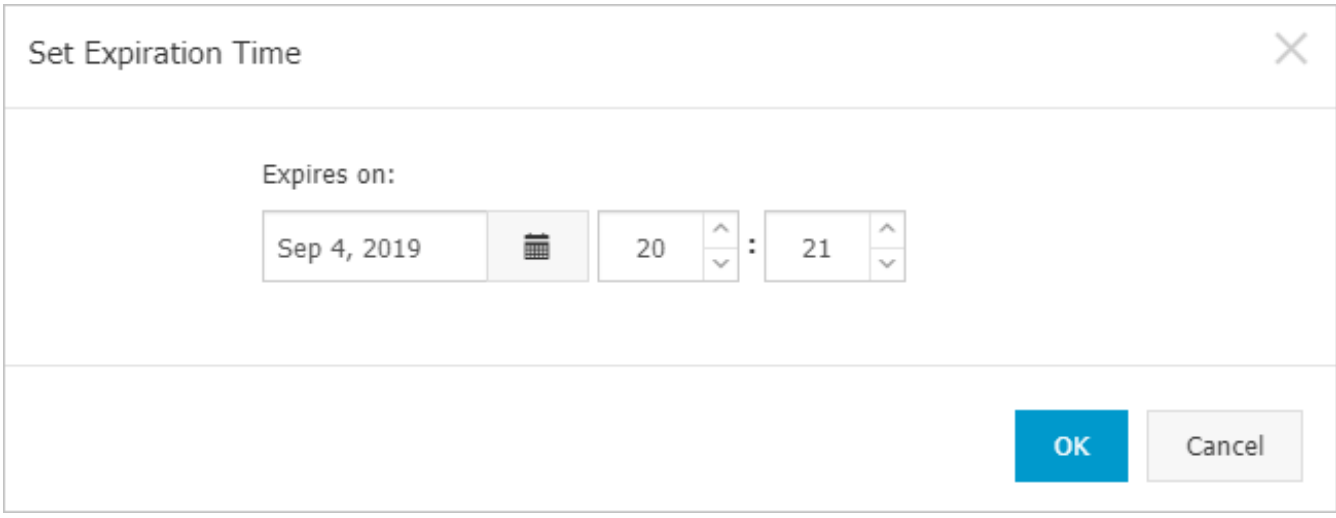
2. In the left-side navigation pane, select the region where the target RDS instance is located.



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Accounts.
5. On the Service Account Permissions tab, select the permission to be authorized to the service account and in the Privilege Status column click the switch.
   - For troubleshooting of the IP address whitelists, database parameters, and other problems, you only need to authorize the Configuration Permission.
   - For the database performance problems caused by your application, you must authorize the Data Permission.

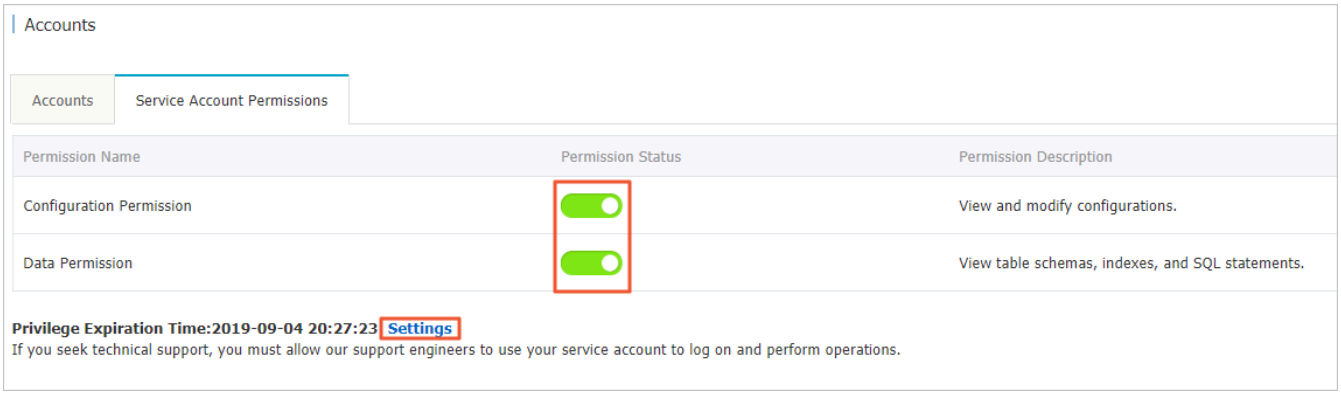


6. In the Set Expiration Time dialog box, set the permission expiration time and click OK.



What to do next

After you authorize permissions to a service account, you can cancel the authorization or change the authorization validity period on the Service Account Permissions tab.



9.5 Delete an account for an RDS for SQL Server instance

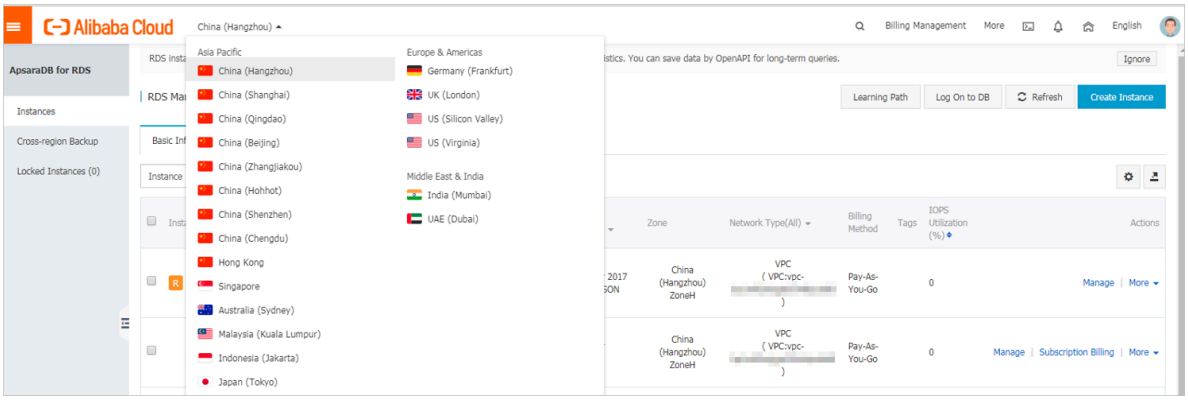
This topic describes how to delete a standard account for an RDS for SQL Server instance in the RDS console.

Note:
If your RDS instance uses the SQL Server engine, the premier account cannot be deleted after being created.

Procedure

1. Log on to the *RDS console*.

2. In the upper-left corner, select the region where the target RDS instance is located.



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Accounts.
5. On the Accounts tab, find the account you want to delete, and in the Actions column click Delete.
6. In the displayed dialog box, click Confirm.

APIs

API	Description
#unique_108	Used to delete an account for an RDS instance.

10 Database

10.1 Create a database for an RDS for SQL Server instance

This topic provides information about how to create a database for an RDS for SQL Server instance. The database creation method varies depending on the used SQL Server version.

For more information, see the following resources:

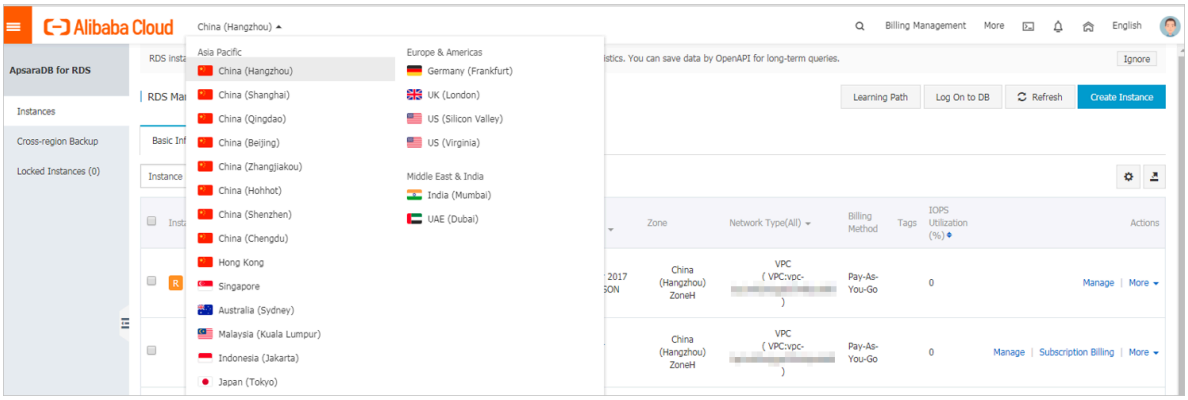
- *SQL Server 2008 R2*
- *SQL Server 2012/2016*
- *SQL Server 2017*

10.2 Delete a database for an RDS for SQL Server instance

This topic describes how to delete a database for an RDS for SQL Server instance by using the RDS console or an SQL command.您可以通过SQL命令或RDS管理控制台删除数据库，但每种方式适合的实例类型不同，请根据实际情况，选择删除方式。

Delete a database by using the RDS console

1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Databases.**
5. **Find the database you want to delete, and in the Actions column click Delete.**
6. **In the displayed dialog box, click Confirm.**

Delete a database by using an SQL command

1. **Connect your database client to the target RDS instance. For more information, see** *Connect to an RDS for SQL Server instance*.
2. **Run the following command to delete a database:**

```
drop database <database name>;
```

APIs

API	Description
#unique_112	**Used to delete a database for an RDS instance.**

11 Database connection

11.1 Configure a hybrid access solution to smoothly migrate an RDS instance from the classic network to a VPC

This topic describes how to configure a hybrid access solution to smoothly migrate an RDS instance from the classic network to a VPC. To meet the increasing needs of migration between different network types, ApsaraDB for RDS introduces the hybrid access solution. This solution enables a smooth migration from the classic network to a VPC without any transient disconnections or service interruptions. The solution also offers the option to migrate a primary instance and its read-only instances separately without any interference with each other.

Background information

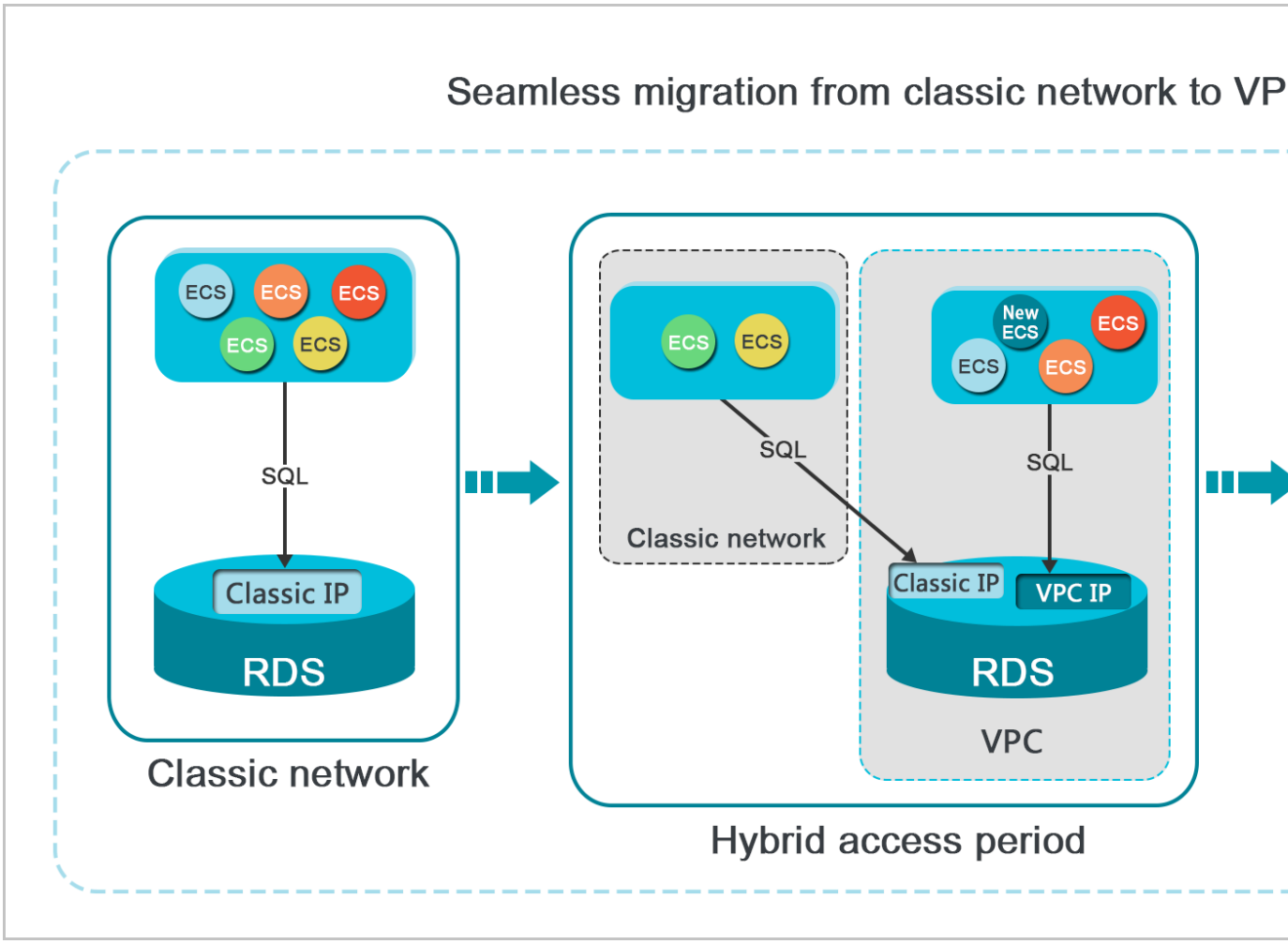
In the past, when migrating an RDS instance from the classic network to a VPC, the internal endpoint of the RDS instance changes. The connection string of the RDS instance remains the same but the IP address bound to the connection string is changed to the corresponding IP address in the VPC. This change will cause a 30-second transient disconnection, and the ECS in the classic network cannot access the RDS instance through the internal endpoint within this period. To migrate the RDS instance across different networks in a smooth manner, ApsaraDB for RDS introduces the hybrid access solution.

Hybrid access refers to the ability of an RDS instance to be accessed by ECS on both the classic network and VPC. During the hybrid access period, the RDS instance reserves the original internal endpoint of the classic network and adds an internal endpoint of VPC. This prevents transient disconnections during the RDS database migration.

For better security and performance, we recommend that you use the internal endpoint of VPC only. Therefore, hybrid access is available for a limited period of time. The internal endpoint of the classic network is released when the hybrid access period expires. In that case, your applications cannot access the RDS database by using the internal endpoint of the classic network. You must configure the internal endpoint of VPC in all your applications during the hybrid access

period. This can guarantee smooth network migration and minimize the impact on your services.

For example, your company wants to use the hybrid access solution to migrate RDS instances from the classic network to a VPC. During the hybrid access period, some applications can access the database through the internal endpoint of the VPC, and the other applications can access the database through the original internal endpoint of the classic network. When all the applications access the database through the internal endpoint of the VPC, the internal endpoint of the classic network can be released. The following figure illustrates the scenario.



Limits

During the hybrid access period, the instance has the following limits:

- Switching to the classic network is not supported.
- Migrating the RDS instance to another zone is not supported.

Prerequisites

- **The network type of the instance is the classic network.**
- **Available VPCs and VSwitches exist in the zone where the RDS instance is located. For more information about how to create VPCs and VSwitches, see *Manage VPCs*.**

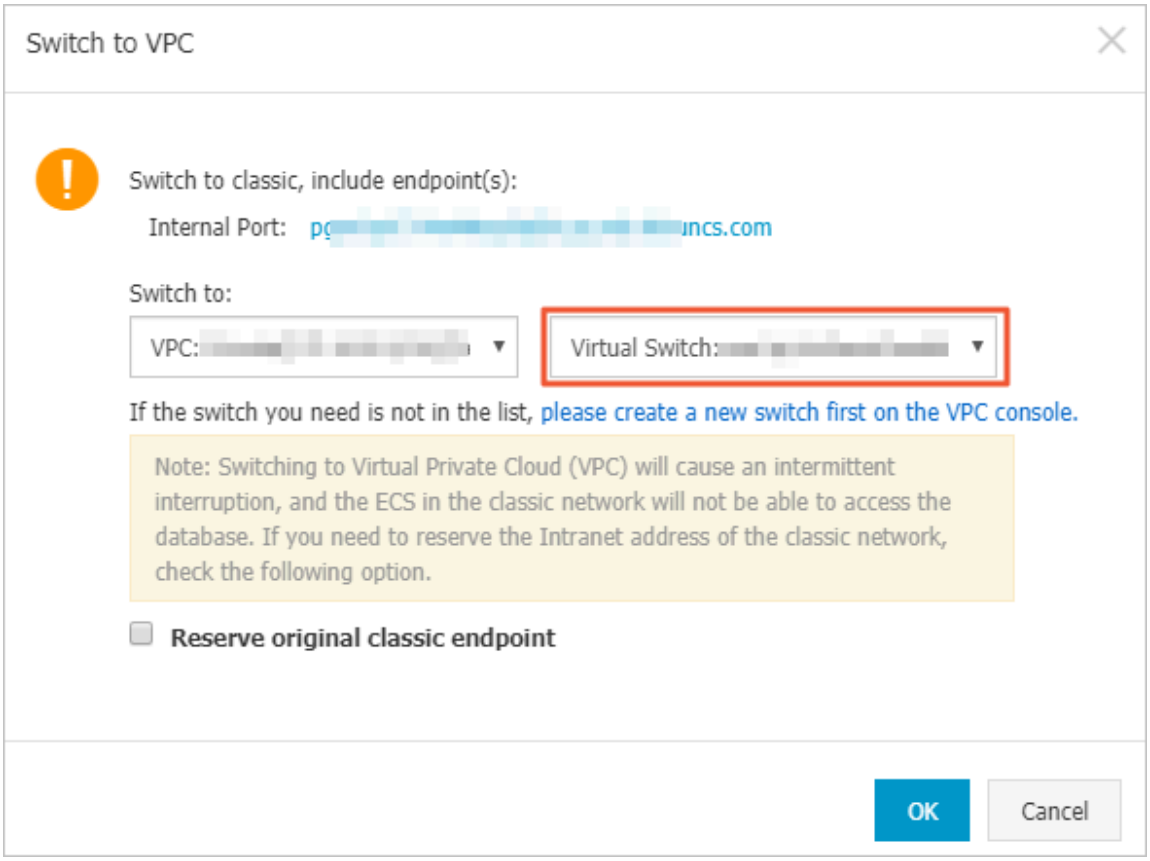
Migrate the RDS instance from the classic network to a VPC

1. **Log on to the *ApsaraDB for RDS console*.**
2. **In the upper-left corner of the page, select the region where the instance is located.**

3. **Find the instance and click the instance ID.**
4. **In the left-side navigation pane, click Database Connections.**
5. **Click Switch to VPC.**
6. **In the dialog box that appears, select a VPC and VSwitch, and select whether to retain the internal and public endpoints of the classic network.**
   - **Select a VPC. We recommend that you select the VPC where your ECS instance is located. Otherwise, the ECS instance and RDS instance cannot communicate**

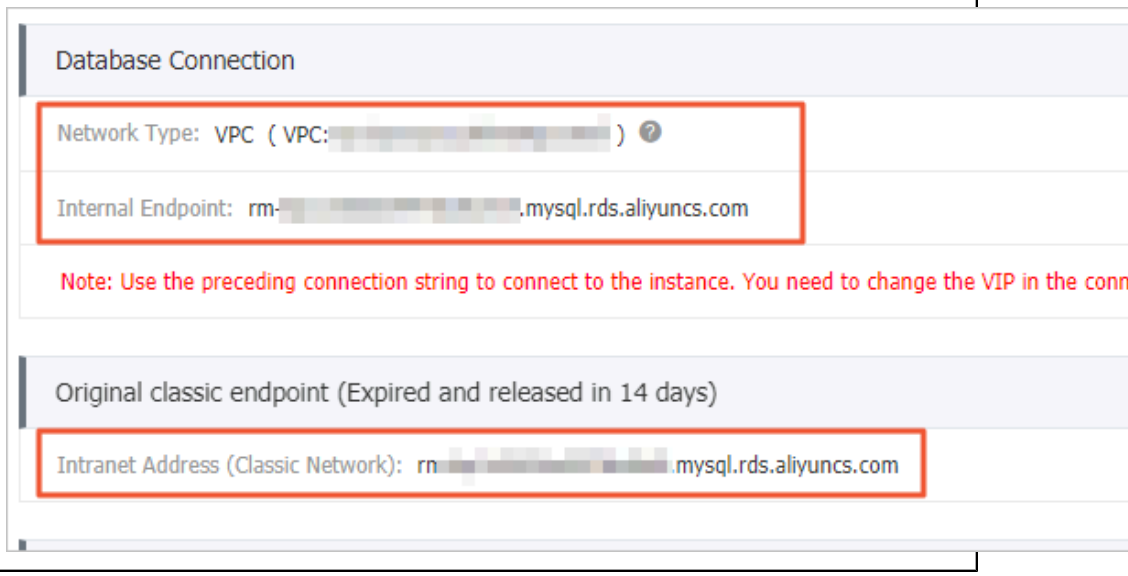
through the internal connections unless you create an express connection or gateway. For more information, see *Express connection* and *VPN gateway*.

- Select a VSwitch. If no VSwitch exists in the selected VPC (as shown in the following figure), create a VSwitch in the same zone as the instance. For more information, see *Manage VSwitches*.



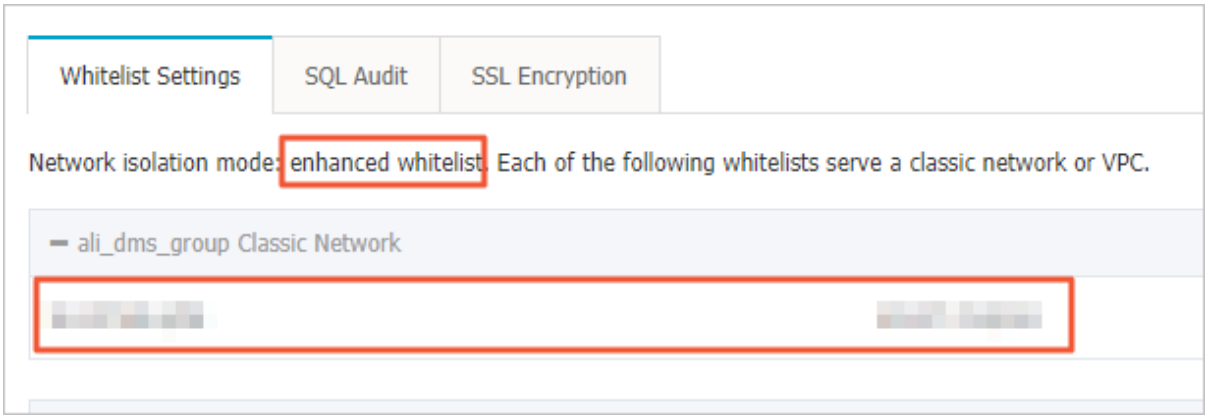
- Decide whether to select Retain Classic Network. The following table describes the different actions.

Action	Description
Clear	The endpoint of the classic network is not retained. The original endpoint is changed to the endpoint of the VPC. If the endpoint of the classic network is not retained, a 30-second transient disconnection will occur to the RDS instance when the network type is changed. The internal access to the RDS instance from the ECS instance that is located in the classic network will be immediately disconnected.

Action	Description
Select	The endpoint of the classic network is retained, and a new endpoint of the VPC is added. Indicates that the hybrid access mode is used and RDS can be simultaneously accessed by ECS instances both in the classic network and VPC through the internal endpoints. If the endpoint of the classic network is retained, the RDS instance will not be immediately disconnected when the network type is changed. The ECS instances in the classic network will not be disconnected from the internal access to the RDS instance until the internal endpoint of the classic network expires. Before the endpoint of the classic network expires, add the endpoint of the VPC to the ECS instance that is located in the same VPC. This makes sure that your business is smoothly migrated to the VPC. Within seven days before the endpoints of the classic network expire, the system will send a text message to the mobile phone bound to your account every day. 

7. Add the internal IP address of the ECS instance in the VPC to the VPC whitelist group of the RDS instance. This makes sure that the ECS instance can access the

RDS instance through the internal network. If no VPC whitelist group exists, create a new group.



8. · If you select Retain Classic Network, add the endpoint of the VPC to the ECS instance before the endpoint of the classic network expires.
   · If you clear Retain Classic Network, the internal connection from the ECS instance in the VPC to the RDS instance is immediately disconnected after the network type is changed. You must add the RDS endpoint of the VPC to the ECS instance.

Note:
To connect an ECS instance in the classic network to an RDS instance in a VPC through the internal network, you can use *ClassicLink* or switch the network type to VPC.

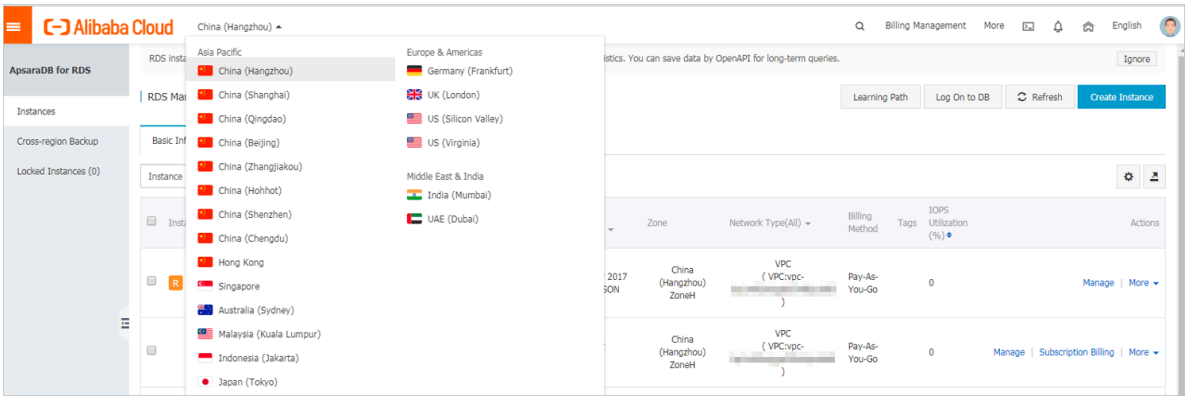
Change the expiration time for the original internal endpoint of the classic network

During the hybrid access period, you can change the retention period for the original internal endpoint of the classic network at any time as needed. The system will update the expiration date based on the modified date. For example, if the original internal endpoint of the classic network is set to expire on August 18, 2017, and you change the expiration time to "14 days later" on August 15, 2017. The internal endpoint of the classic network is released on August 29, 2017.

Follow these steps to change the expiration time:

1. Log on to the *ApsaraDB for RDS console*.

2. In the upper-left corner of the page, select the region where the instance is located.



3. Find the instance and click the instance ID.
4. In the left-side navigation pane, click Database Connections.
5. On the Instance Connection tab, click Change Expiration Time, as shown in the following figure.

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

11.2 Configure endpoints for an RDS for SQL Server instance

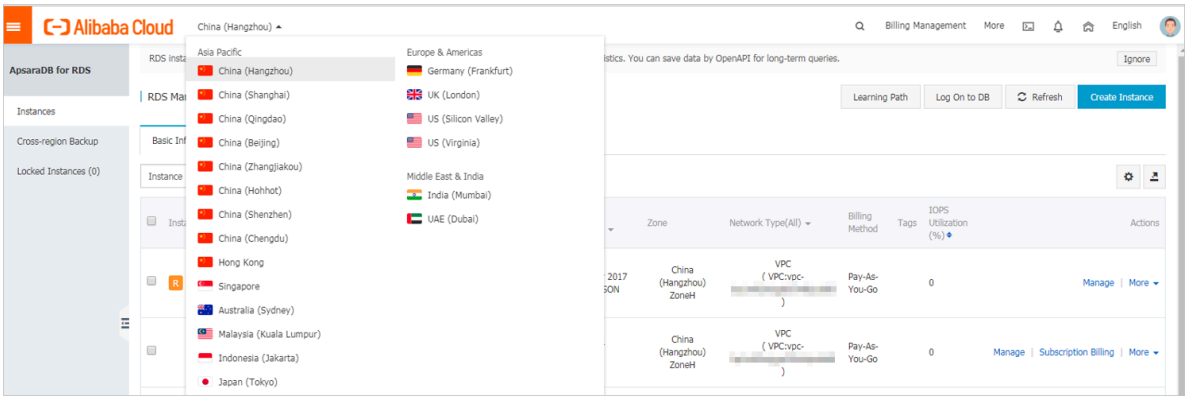
This topic describes how to configure endpoints for an RDS for SQL Server instance, including applying for, changing, and releasing the endpoints. ApsaraDB for RDS provides two types of endpoints: internal endpoints and public endpoints.

Internal and public endpoints

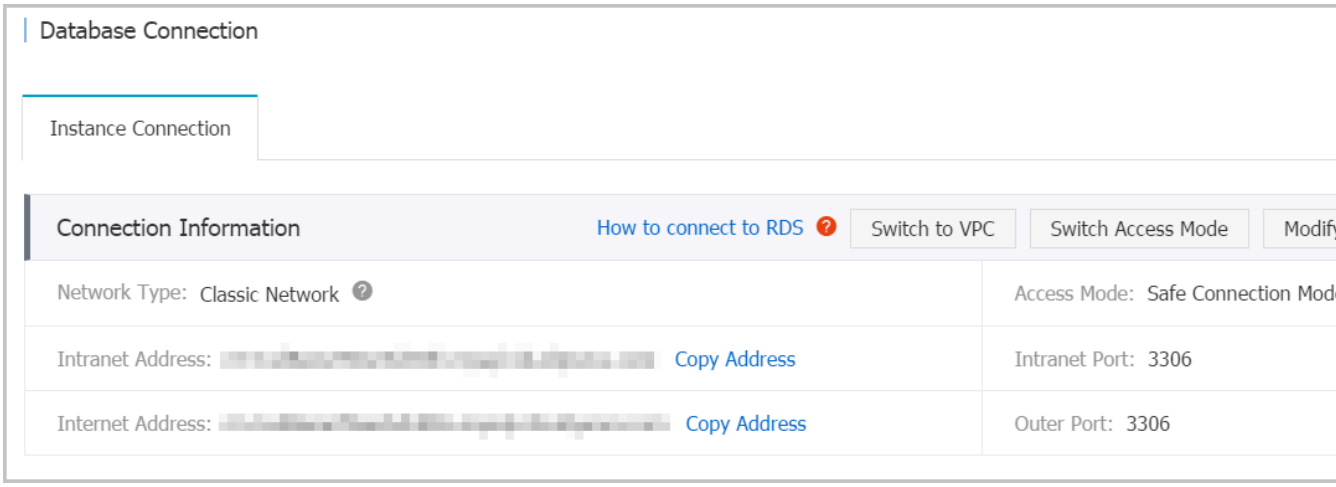
Endpoint type	Description
Internal endpoint	· The internal endpoint is provided by default. You do not need to apply for it and cannot release it. However, you can change the network type. · If your application is deployed on an ECS instance that is in the same region and has the same *network type* as the RDS instance, the ECS and RDS instances can communicate with each other by default. You do not need to apply for a public endpoint for the RDS instance. · Accessing an RDS instance through the internal endpoint achieves the high security and performance of the RDS instance.
Public endpoint	· You must manually apply for a public endpoint. You can release the public endpoint if you do not need it. · When you cannot access an RDS instance through the internal endpoint, you must apply for a public endpoint. The specific scenarios are as follows: - When you access an RDS instance from an ECS instance, where the ECS instance and RDS instance are located in different regions, and their *network types* are different. - When you access an RDS instance from the third-party services or applications. **Note:** · For security purposes, exercise caution when you access your RDS instance through a public endpoint. · We recommend that you migrate your application to an ECS instance in the same region and with the same network type as your RDS instance, and then use the internal endpoint to access your application. This helps to improve transmission speed and data security.

Apply for or release a public endpoint

1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Database Connection.**
5. **·** **If you have not applied for a public endpoint, click Apply for Public Endpoint.**
   · **If you have applied for a public endpoint, click Release Public Endpoint.**

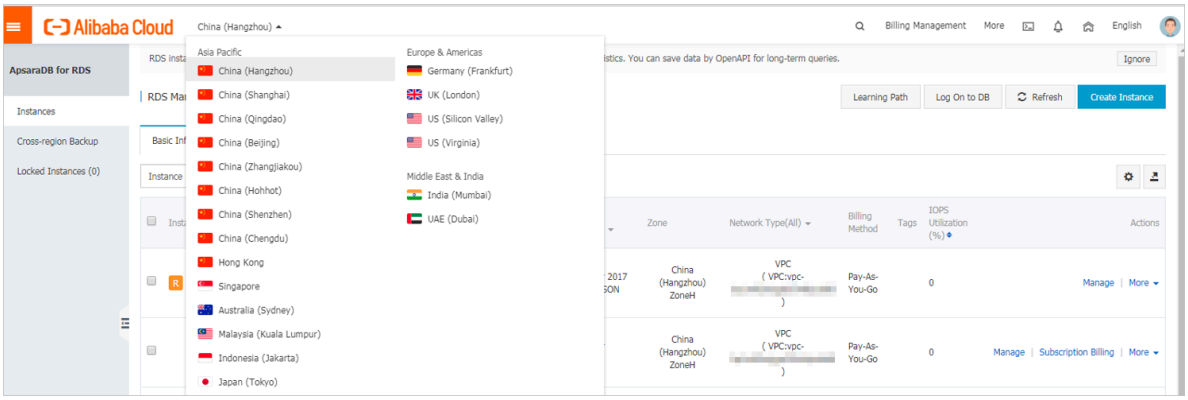


6. **In the message box that appears, click OK.**

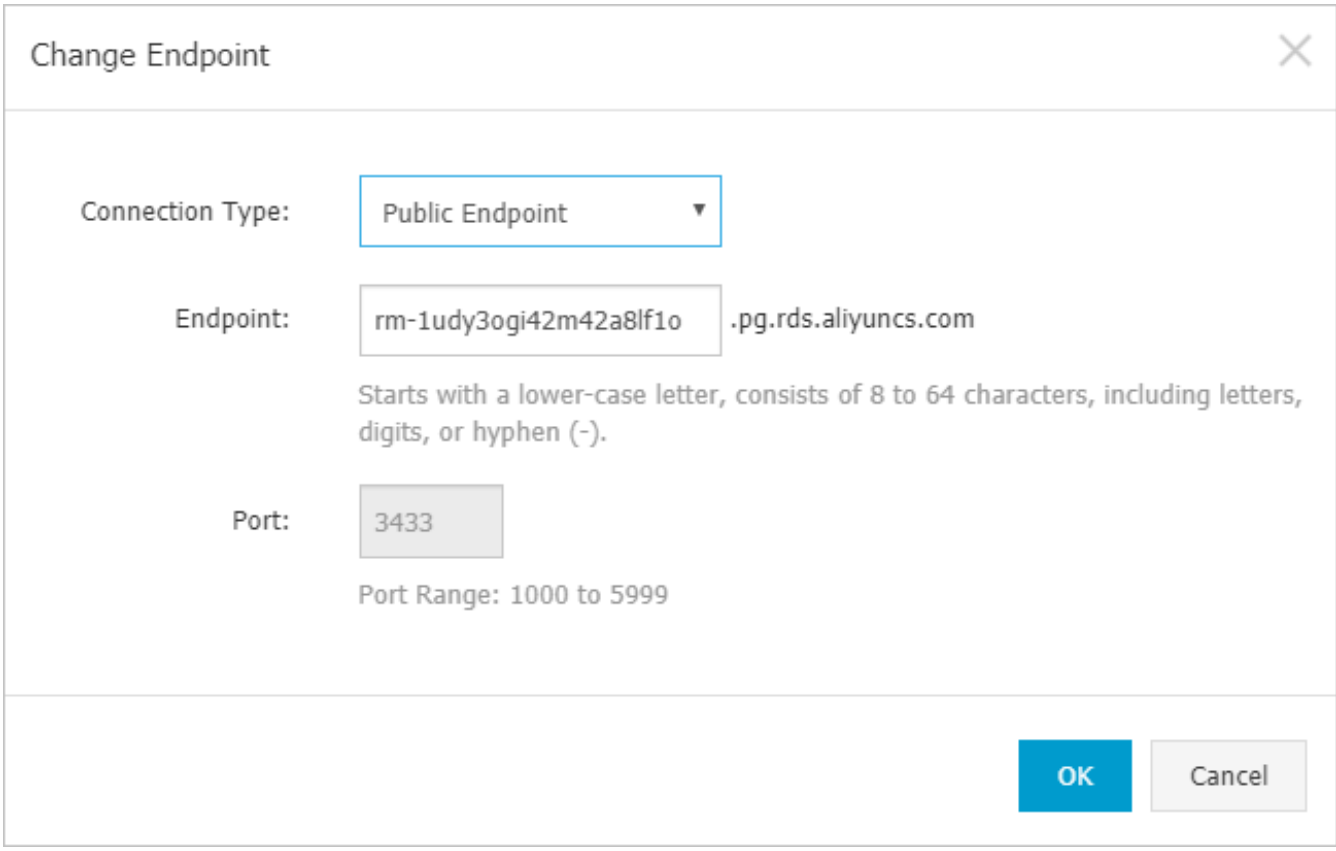
Change the internal and public endpoints

1. **Log on to the *RDS console*.**

2. In the upper-left corner, select the region where the target RDS instance is located.



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Database Connection.
5. Click Change Endpoint.
6. In the dialog box that appears, specify the internal and public endpoints, and click OK.



Note:

- The prefix of the endpoint must be 8 to 64 characters in length and can contain letters, numbers, and hyphens (-). It must start with a lowercase letter.
- In a VPC, either the internal port number or public port number cannot be changed.
- In a classic network, either the internal port number or public port number can be changed.

APIs

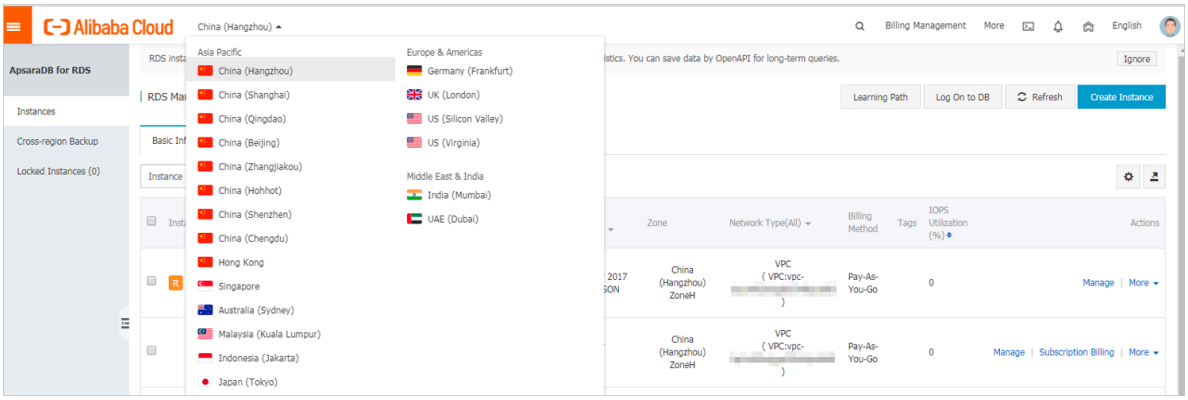
Operation	Description
#unique_119	Used to apply for a public endpoint for an RDS instance.
#unique_120	Used to release the public endpoint of an RDS instance.

11.3 View the internal and public endpoints and ports of an RDS for SQL Server instance

This topic describes how to view the internal and public endpoints and ports of an RDS for SQL Server instance. When connecting to an RDS instance, you must enter its internal or public endpoint and port number.

Procedure

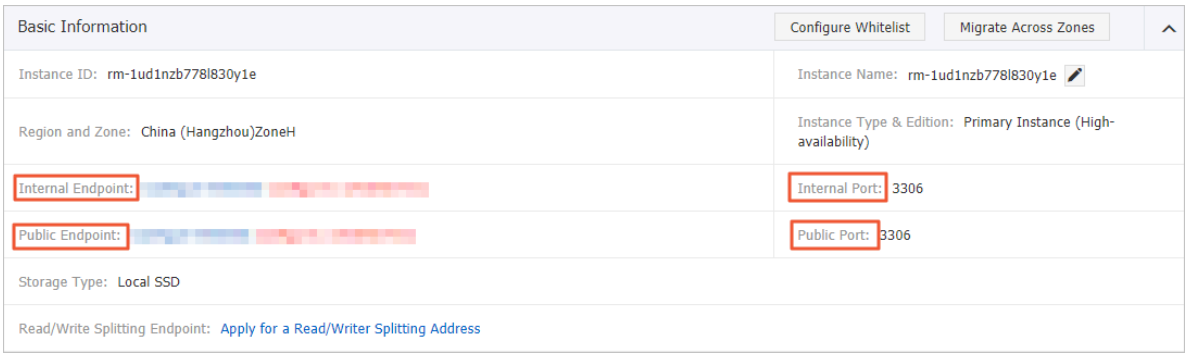
1. Log on to the *RDS console*.
2. In the upper-left corner, select the region where the target RDS instance is located.



3. Find the target RDS instance and click the instance ID.

4. On the Basic Information page, find the Basic Information section, where you can view the internal and public endpoints and ports of the RDS instance.

> **Note:**
>
> - The internal and public endpoints are displayed only after you configure a whitelist.
> - The public endpoint is displayed only after you apply for it.



11.4 Apply for a public endpoint for an RDS for SQL Server instance

This topic describes how to apply for a public endpoint for an RDS for SQL Server instance. Apsara for RDS supports two types of endpoints: internal endpoints and public endpoints. By default, the system provides you with an internal endpoint for connecting to your RDS instance. If you want to connect to your RDS instance through the Internet, you must apply for a public endpoint.

Internal and public endpoints

Endpoint type	Description
Internal endpoint	The internal endpoint is generated by default. Use the internal endpoint if all of the following conditions are met: · Your application is deployed on an ECS instance. · The ECS instance is located in the same region as your RDS instance. · The ECS instance has the same *network type* as your RDS instance. The internal endpoint is recommended because accessing RDS through the intranet is most secure and delivers optimal performance.

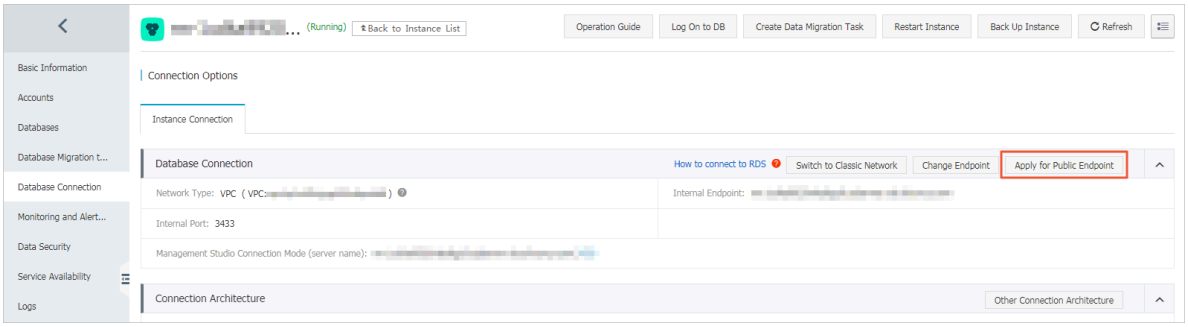
Endpoint type	Description
Public endpoint	You must manually apply for a pubic endpoint. You can also release it anytime. Use the pubic endpoint if you cannot access RDS through the intranet. Specific scenarios are as follows: · An ECS instance accesses your RDS instance but the ECS instance is located in a different region or has a network type different from your RDS instance. · A server or computer outside Alibaba Cloud accesses your RDS instance. **Note:** · The pubic endpoint and traffic are currently free of charge. · Using the pubic endpoint reduces security. Please exercise caution. · To guarantee high security and performance, we recommend that you migrate your application to an ECS instance that is in the same region and has the same network type as your RDS instance and then use the pubic endpoint.

Apply for a pubic endpoint

1. Log on to the *RDS console*.
2. Select the target region.

3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Database Connection.

5. Click Apply for Public Endpoint.



6. In the displayed dialog box, click OK.

   The pubic endpoint is generated.

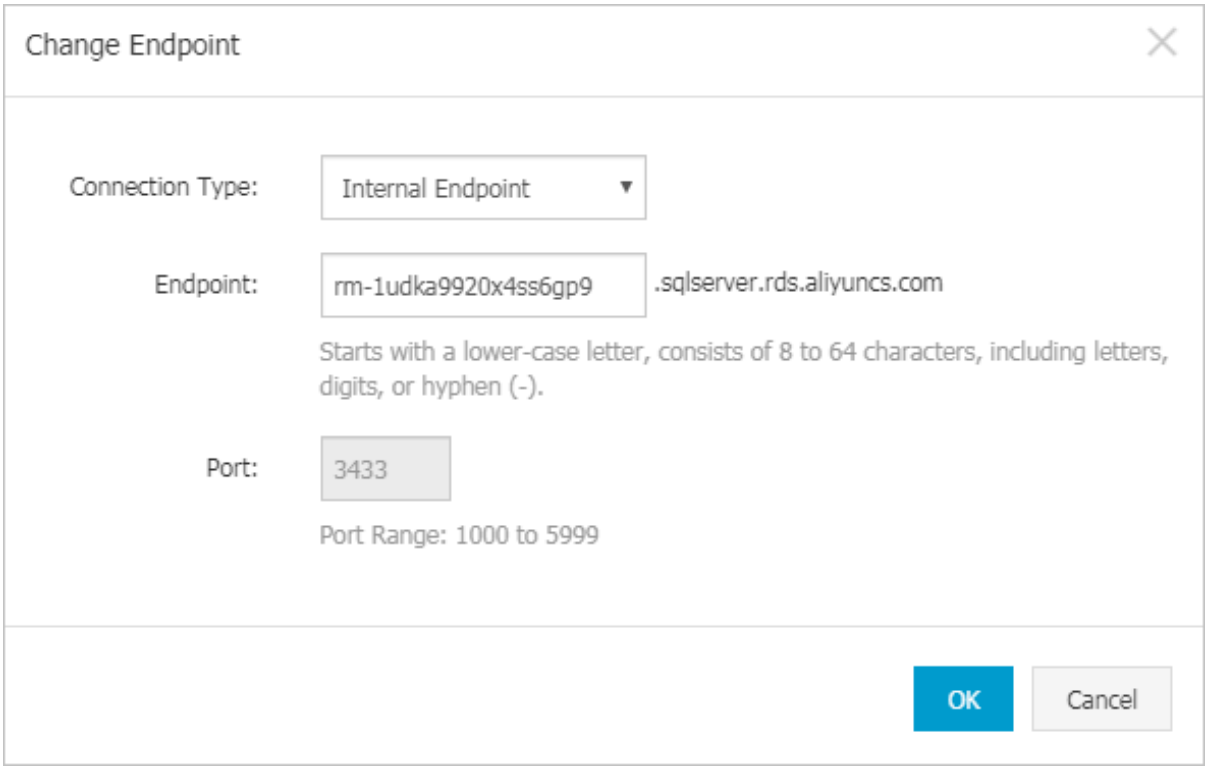
7. Optional. To change the pubic endpoint or port number, click Change Endpoint. In the displayed dialog box, select a connection type, set the pubic endpoint and port number, and click OK.

   - Connection Type: Select Public Endpoint.

   Note:

The Public Endpoint option is available only after you have applied for a pubic endpoint.

- **Endpoint: The endpoint must be 8 to 64 characters in length and can contain letters, numbers, and hyphens (-). It must start with a lowercase letter.**
- **Port: You can change the port number only when the network type of the RDS instance is classic network.**



APIs

API	Description
#unique_119	**Used to apply for a pubic endpoint for an RDS instance.**

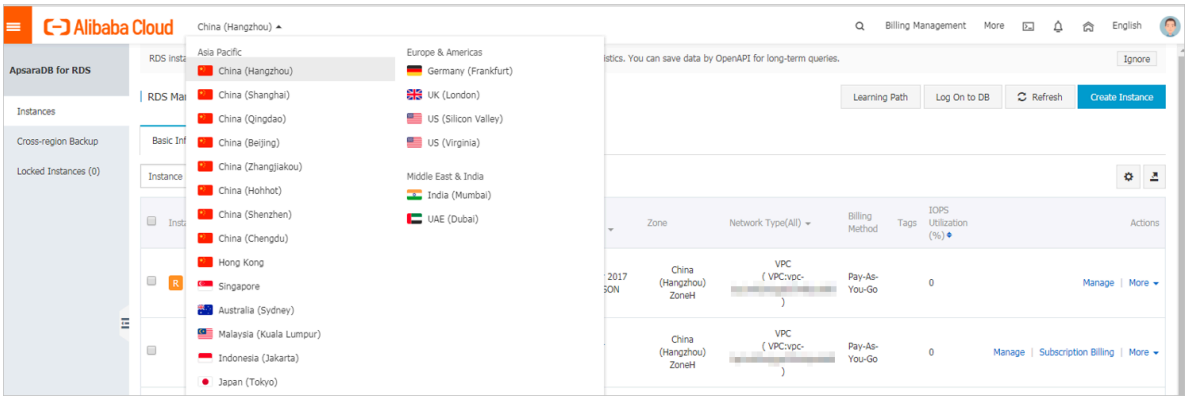
12 Monitoring and alerts

12.1 View resource and engine monitoring data

This topic describes how to view the resource and engine monitoring data of an RDS for SQL Server instance. ApsaraDB for RDS provides a wide range of performance metrics for you to view in the RDS console.

Procedure

1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Monitoring and Alerts.**

5. On the Monitoring tab, select the Resource Monitoring or Engine Monitoring monitoring type and specify the time range. The following table describes the monitoring metrics.

Monitoring type	Metric	Description
Resource Monitoring	Disk Space (MB)	The disk space usage of the RDS instance, including: · Instance Size · Data Usage · Log Size · Temporary File Size · Other System File Size Unit: MByte.
	IOPS (Input/ Output Operations per Second)	The number of I/O requests per second for the RDS instance. Unit: Number/second.
	Total Connections	The total number of connections to the RDS instance, including the number of active connections and the total number of connections.
	MSSQL Instance CPU Utilization (percentage in the operating system: %)	The CPU usage of the RDS instance, including the CPU usage for the operating system.
	SQLServer Average Input/Output Traffic (KB/s)	The input and output traffic of the RDS instance per second. Unit: KB.
Engine Monitoring	Average Transaction Frequency	The number of transactions processed per second.
	Average QPS	The number SQL statements executed per second.
	Buffer Hit Ratio (%)	The read hit ratio of the buffer.

Monitorin type	Metric	Description
	Page Write Frequency at Check Point	The number of pages that are written at the check point per second in the RDS instance.
	Login Frequency	The number of logons to the RDS instance per second.
	Average Frequency of Whole Table Scans	The number of full table scans performed per second.
	SQL Compilations per Second	The number of SQL statements that are compiled per second in the RDS instance.
	Lock Timeout Times/s	The number of times that the lock times out per second in the RDS instance.
	Deadlock Frequency	The number of times that the RDS instance is locked per second.
	Lock Wait Frequency	The number of times that the RDS instance enters the waiting state after being locked.

12.2 Set the monitoring frequency

This topic describes how to set the monitoring frequency for an RDS for SQL Server instance.

Background information

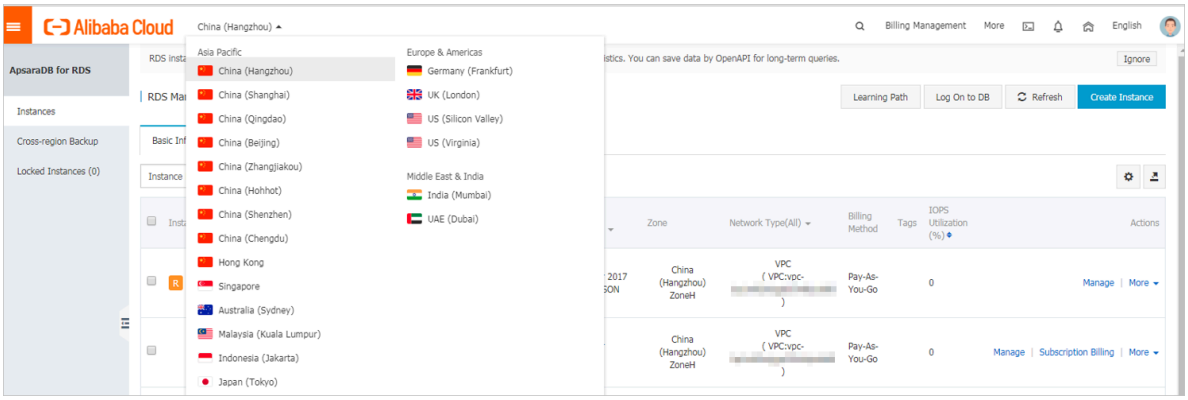
RDS for PPAS supports two monitoring frequencies:

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

Procedure

1. **Log on to the** *RDS console*.

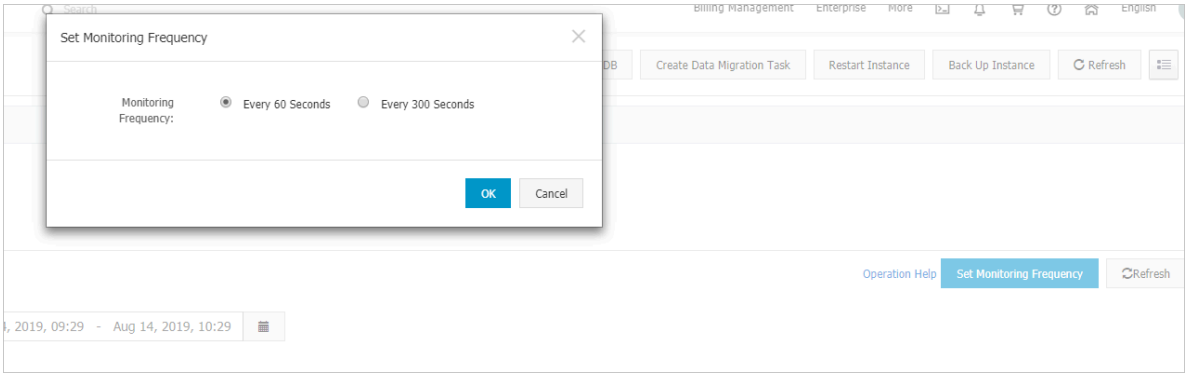
2. In the upper-left corner, select the region where the target RDS instance is located.



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Monitoring and Alerts.

> **Note:**
> For information about the monitoring metrics supported by the instance, see *View resource and engine monitoring data*.

5. Click the Monitoring tab.
6. Click Set Monitoring Frequency.
7. In the Set Monitoring Frequency dialog box, select the monitoring frequency and click OK.



APIs

API	Description
#unique_126	Used to query the monitoring data of an RDS instance.

12.3 Set an alert rule

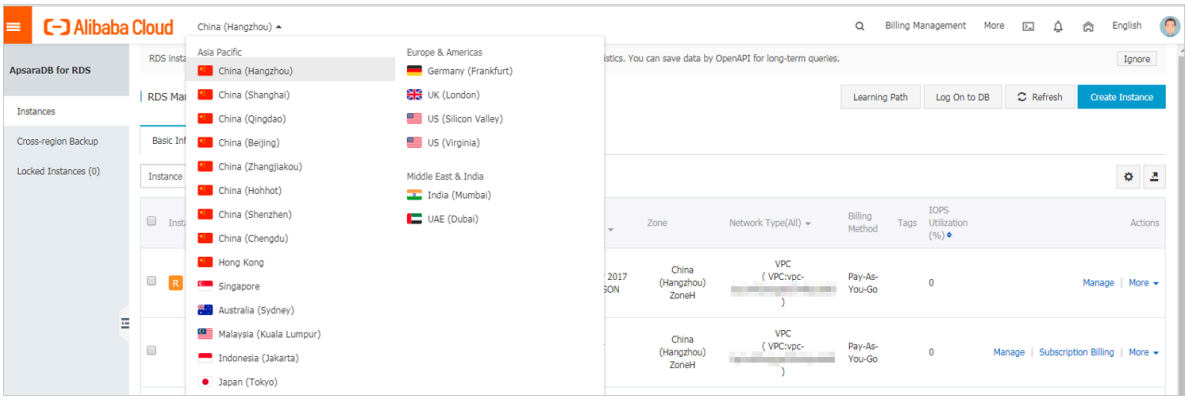
This topic describes how to set an alert rule for an RDS instance. ApsaraDB for RDS offers the instance monitoring function, and sends messages to you after detecting an exception in an instance. In addition, when the instance is locked due to insufficient disk space, the system sends a message to you.

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. **In the upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Monitoring and Alerts.**
5. **Click the Alerts tab.**
6. **Click Set Alert Rule.**

   You are directed to the CloudMonitor console.

> **Note:**
> **You can click Refresh to manually refresh the current status of the alert metrics.**

7. In the left-side navigation pane, choose Alarms > > Alarm Contacts to open the Alarm Contact Management page.

   Note:
   When alert rules are set for the first time, if the alert 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. In the Set Alarm Contact dialog box, enter the alarm contact information and click Send verification code. Then, 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.
   - You can 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. Set `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 alert 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 alert.

16. Click Create Alarm Rule to add a new alert rule.

Note:

You can click Modify, Disable, or Delete for the metrics as needed.

13 Data security

13.1 Configure a whitelist for an RDS for SQL Server instance

This topic describes how to configure a whitelist for an RDS for SQL Server instance.

Configuring a whitelist does not affect the normal running of your RDS instance, but only makes your RDS instance more secure. We recommend that you update the whitelists for your RDS instance on a regular basis.

> **Note:**
> **The default whitelist contains only the default IP address 127.0.0.1. Before you add new IP addresses to the whitelist, no devices can access the RDS instance.**

Precautions

- **The default whitelist can only be edited or cleared. It cannot be deleted.**
- **If you log on to DMS but your IP address has not been added to the whitelist, DMS prompts you to add the IP address and automatically generates a whitelist containing your IP address.**

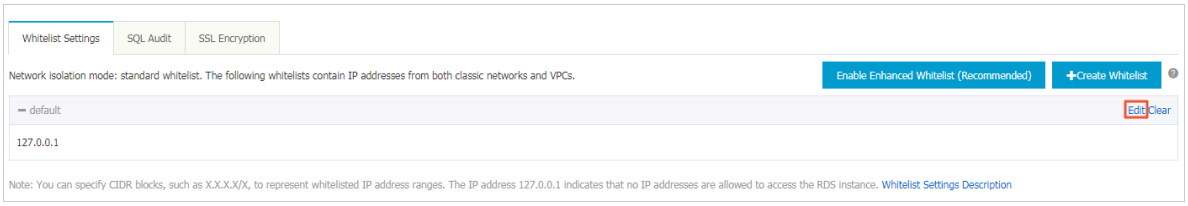
Procedure

1. **Log on to the *RDS console*.**
2. **In the upper-left corner of the page, select the region where the instance is located.**

3. **Find the instance and click its ID.**
4. **In the left-side navigation pane, click Data Security.**

5. On the Whitelist Settings tab page, click Edit corresponding to the default whitelist.

> **Note:**
> You can click Create Whitelist to create a whitelist.

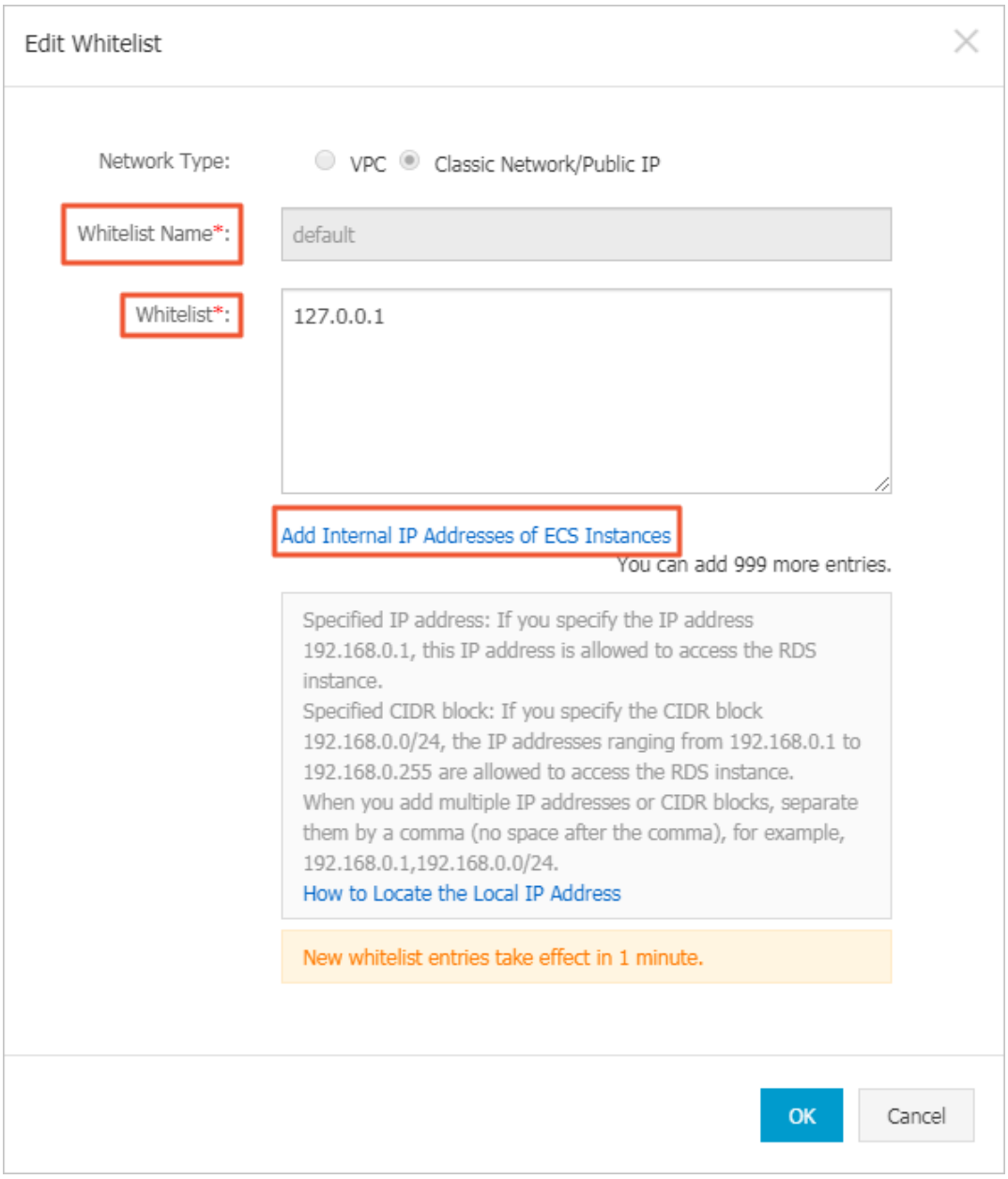


6. In the displayed Edit Whitelist dialog box, specify the IP addresses or CIDR blocks used to access the instance, and then click OK.

   - If you specify the CIDR block 10.10.10.0/24, any IP addresses in the 10.10.10.*X* format are allowed to access the RDS instance.
   - To add multiple IP addresses or CIDR blocks, separate each entry with a comma (without spaces), for example, `192.168.0.1,172.16.213.9`.
   - After you click Add Internal IP Addresses of ECS Instances, the IP addresses of all the ECS instances under your Alibaba Cloud account are displayed. You can quickly add internal IP addresses to the whitelist.

> **Note:**

After you add an IP address or CIDR block to the default whitelist, the default address 127.0.0.1 is automatically deleted.



Common errors

- **The default address 127.0.0.1 in Data Security > Whitelist Settings indicates that no device is allowed to access the RDS instance. Therefore, you must add IP addresses of devices to the whitelist to allow access to the instance.**
- **The IP address in the whitelist is set to 0.0.0.0, but the correct format is 0.0.0.0/0.**

Note:

0.0.0.0/0 indicates that all devices are allowed to access the RDS instance. Exercise caution when using this IP address.

- **The public IP address that you add to the whitelist may not be the real egress IP address. The reasons are as follows:**
  - **The public IP address is not fixed and may dynamically change.**
  - **The tools or websites used to query the public IP addresses provide wrong IP addresses.**

APIs

API	Description
#unique_23	**Used to view the IP address whitelist of an RDS instance.**
#unique_24	**Used to modify the IP address whitelist of an RDS instance.**

13.2 Configure SSL encryption for an RDS for SQL Server instance

This topic describes how to enable Secure Sockets Layer (SSL) encryption and install SSL CA certificates to applications. SSL encrypts data over network connections at the transport layer. This enhances data security and integrity but increases network connection response time.

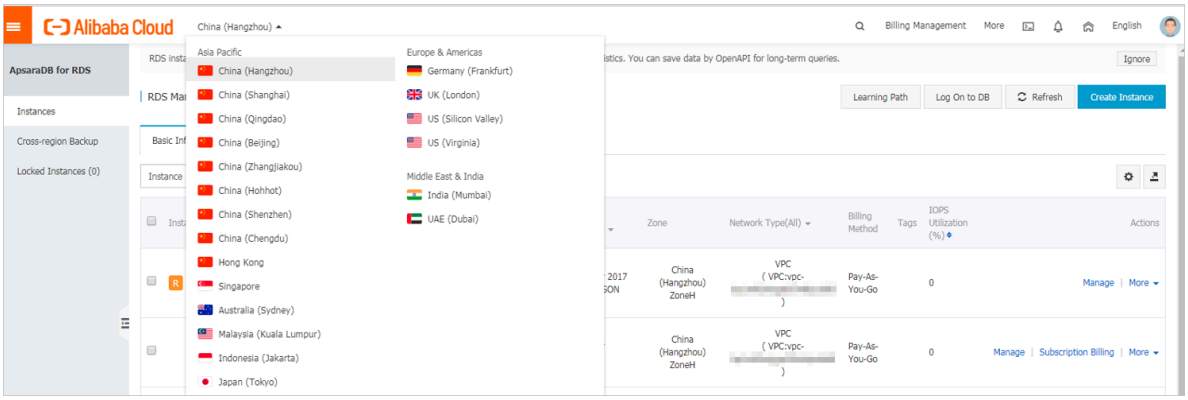
Precautions

- **The validity period of an SSL CA certificate is one year. You must renew the validity period of the SSL CA certificate in your application or client within one year. Otherwise, your application or client that uses an encrypted network connection cannot connect to RDS properly.**
- **SSL encryption increases CPU usage. Therefore, we recommend that you enable SSL encryption only for public endpoints when required. In typical cases, private endpoints do not require SSL encryption.**
- **SSL encryption cannot be disabled once it is enabled.**
- **An RDS instance that uses a read-only address does not support SSL encryption.**

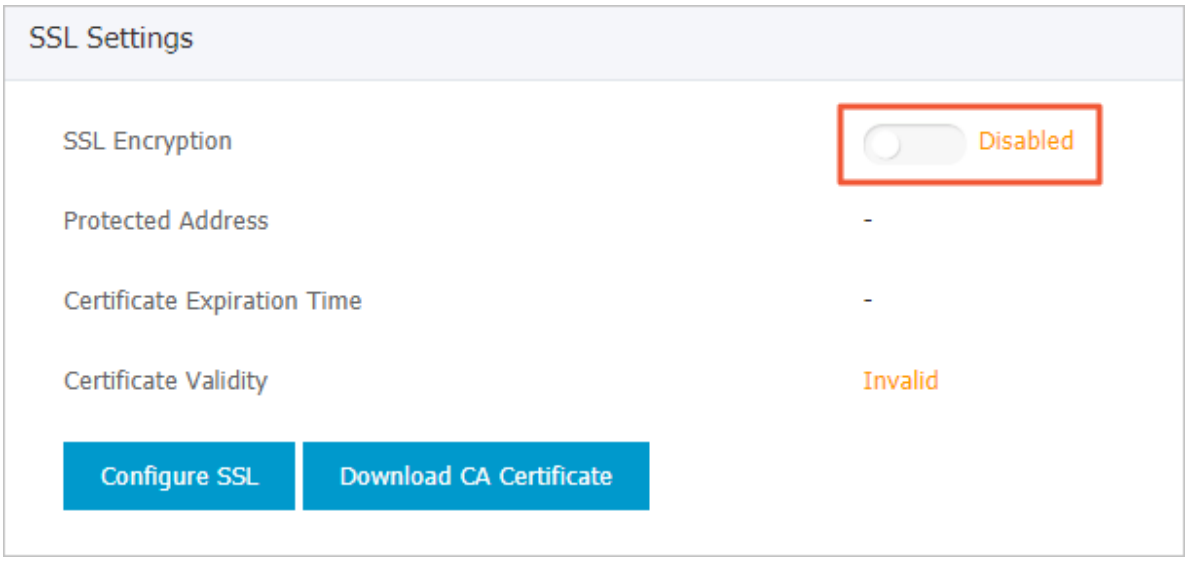
Enable SSL encryption

1. **Log on to the *RDS console*.**

2. In the upper-left corner, select the region where the target RDS instance is located.



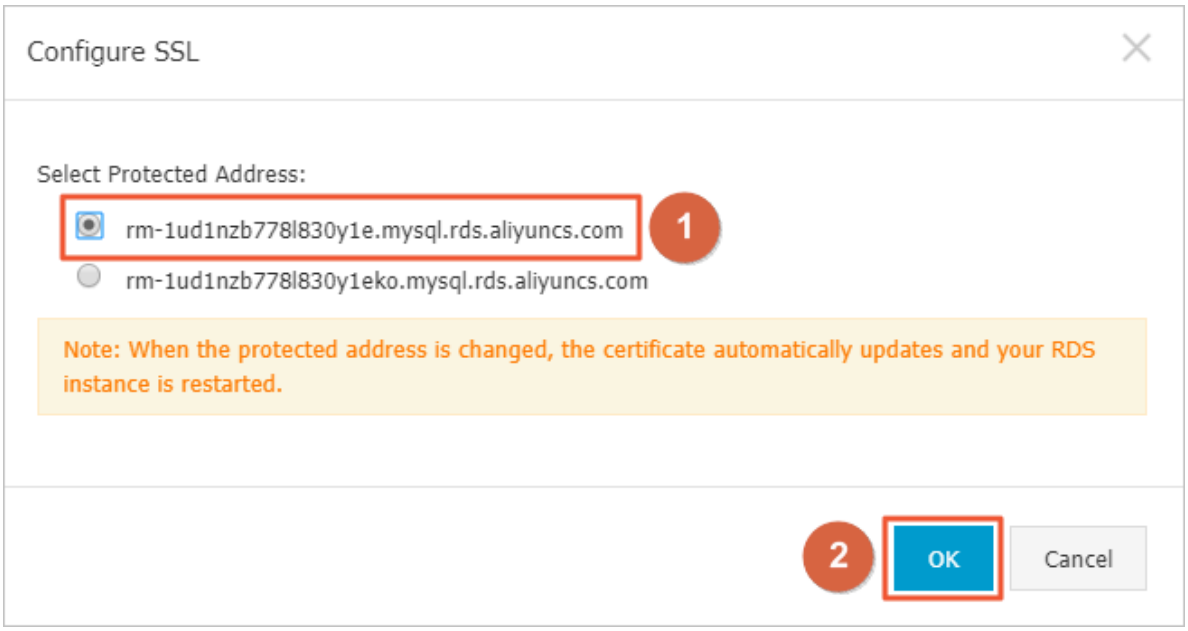
3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Data Security.
5. Click the SSL Encryption tab.
6. Click the switch next to Disabled in the SSL Encryption parameter.



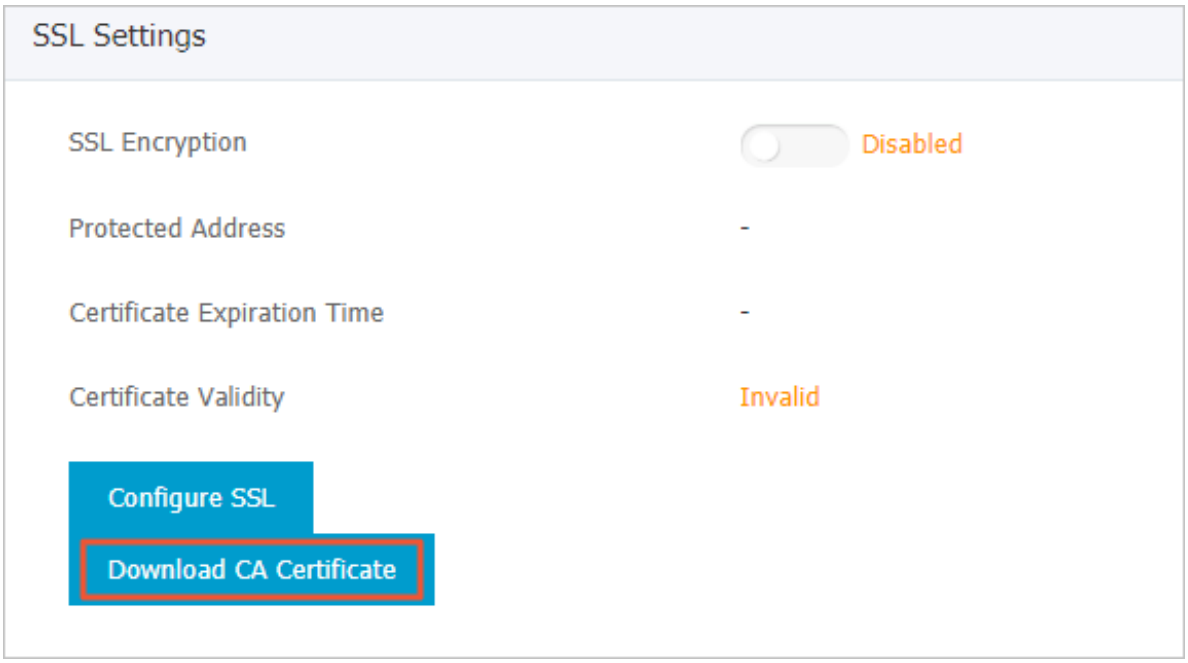
7. In the Configure SSL dialog box, select the endpoint for which you want to enable SSL encryption, then click OK.

Note:

You can choose to encrypt the private or public endpoint, but note that you can encrypt only one endpoint.



8. **Click Download CA Certificate to download the SSL CA certificate files in a compressed package.**



The compressed package consists of the following three files:

- **.p7b file: used to import CA certificate files in Windows operating systems.**
- **.pem file: used to import CA certificate files in other systems or applications.**
- **.jks file: used to import link CA certificate files in Java-based applications. The .jks file is stored in the TrustStore of Java.**

> **Note:**
> **When you use the .jks file in JDK 7 or JDK 8, you must modify the default JDK security configuration. Specifically, you must find the** *jre/lib/security/java.security* **file on the server where the database you want to access through SSL is located, and then reconfigure the file as follows:**

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, DH keySize < 224
```

```
jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 1024
```

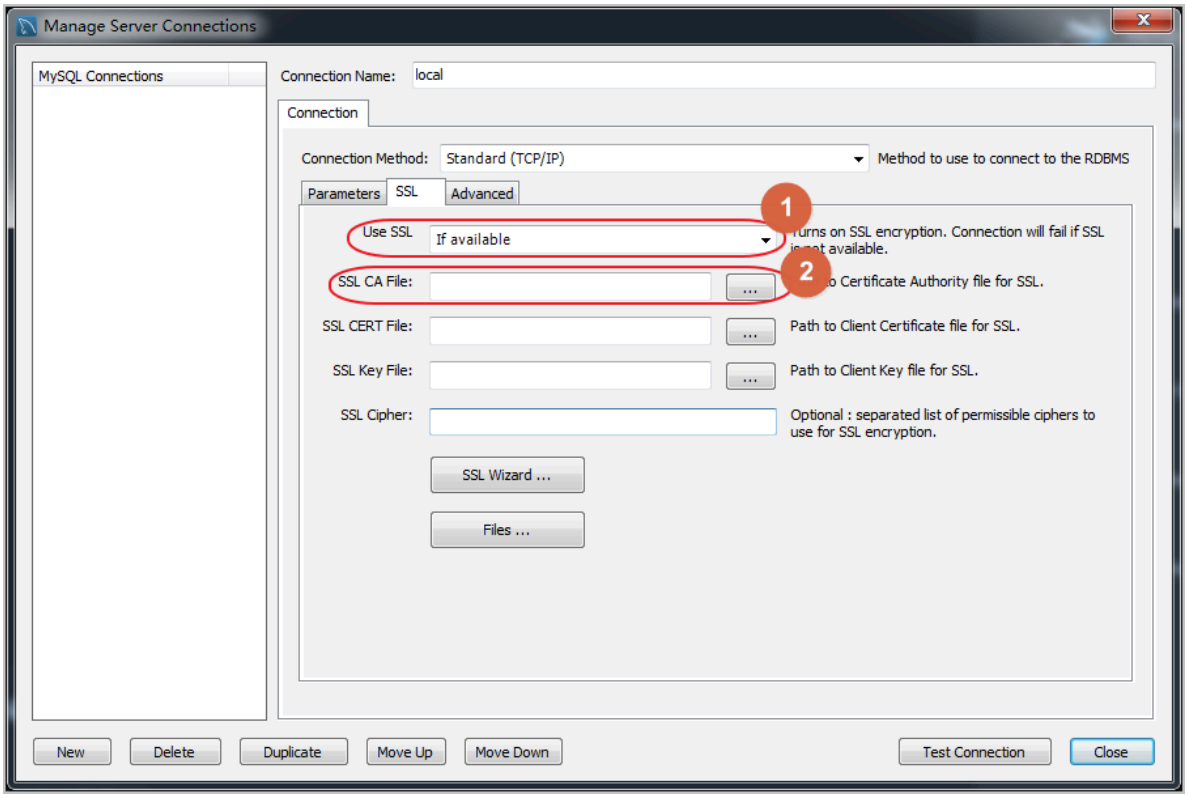
If you do not modify the JDK security configuration, the system reports errors similar to the following:

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

Configure the SSL CA certificate

After SSL encryption is enabled, you must configure the SSL CA certificate for your application or client when connecting to RDS. This section uses MySQL Workbench as an example to describe how to install the SSL CA certificate.

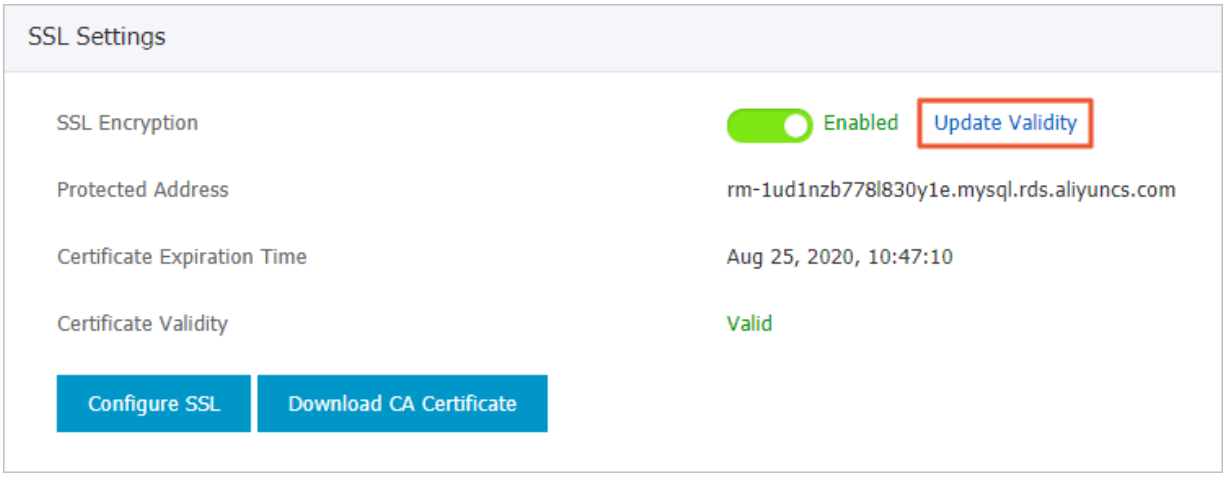
1. **Start MyQL Workbench.**
2. **Choose Database > Manage Connections.**
3. **Enable Use SSL and import the SSL CA certificate files.**



Renew the validity period of the SSL CA certificate

Note:

This operation causes your RDS instance to restart. You must make proper service arrangements before this operation.



13.3 Set TDE for an RDS for SQL Server instance

This topic describes how to set Transparent Data Encryption (TDE) for an RDS for SQL Server instance. With TDE enabled, RDS can encrypt and decrypt incoming and outgoing data files in real time. Specifically, RDS encrypts data before the data is written into the disk, and decrypts data when the data is read from the disk to the memory. TDE does not increase the size of data files. Developers can use the TDE function without changing any applications.

For data security purposes, we recommend that you use the RDS console or call the *#unique_132* API action to enable TDE for your RDS instance.

Background information

To improve data security, you can use the RDS console or call the *#unique_132* API action to enable TDE, which can encrypt data.

Precautions

- **Instance-level TDE can be enabled but cannot be disabled. Database-level TDE can be enabled or disabled as needed.**
- **The keys used for data encryption are generated and managed by Key Management Service (KMS). RDS does not provide the keys or certificates used for data encryption. After TDE is activated, if you want to restore data to your computer, you must first use RDS to *decrypt data*.**
- **TDE increases CPU usage.**

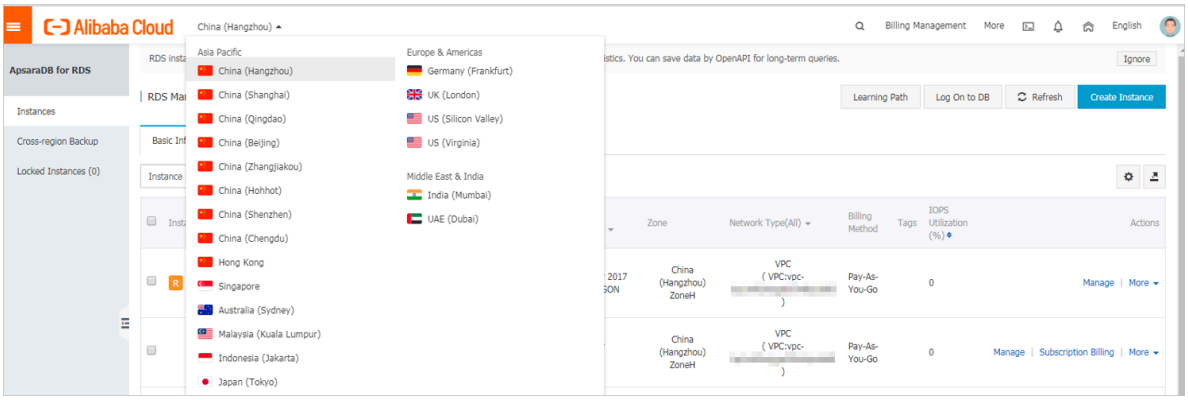
Prerequisites

- **The used DB engine version is RDS for SQL Server.**

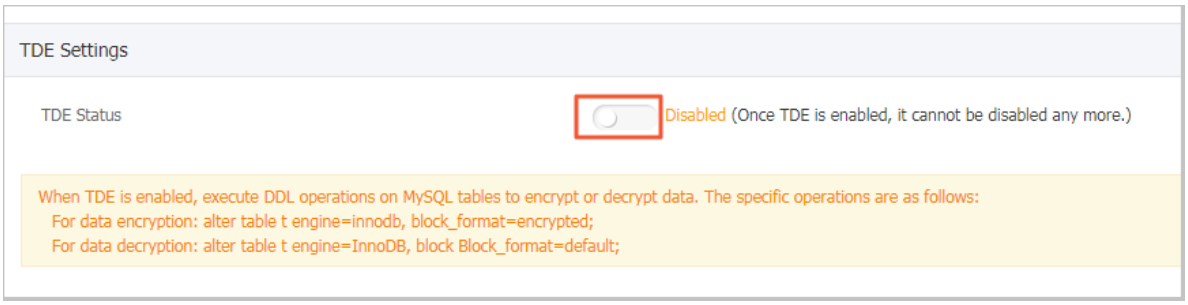
- You have logged in to the Alibaba Cloud console by using your Alibaba Cloud account.
- KMS has been activated. If you have not activated KMS, you can activate it as instructed when activating TDE.

Enable TDE

1. Log on to the *RDS console*.
2. In the upper-left corner, select the region where the target RDS instance is located.

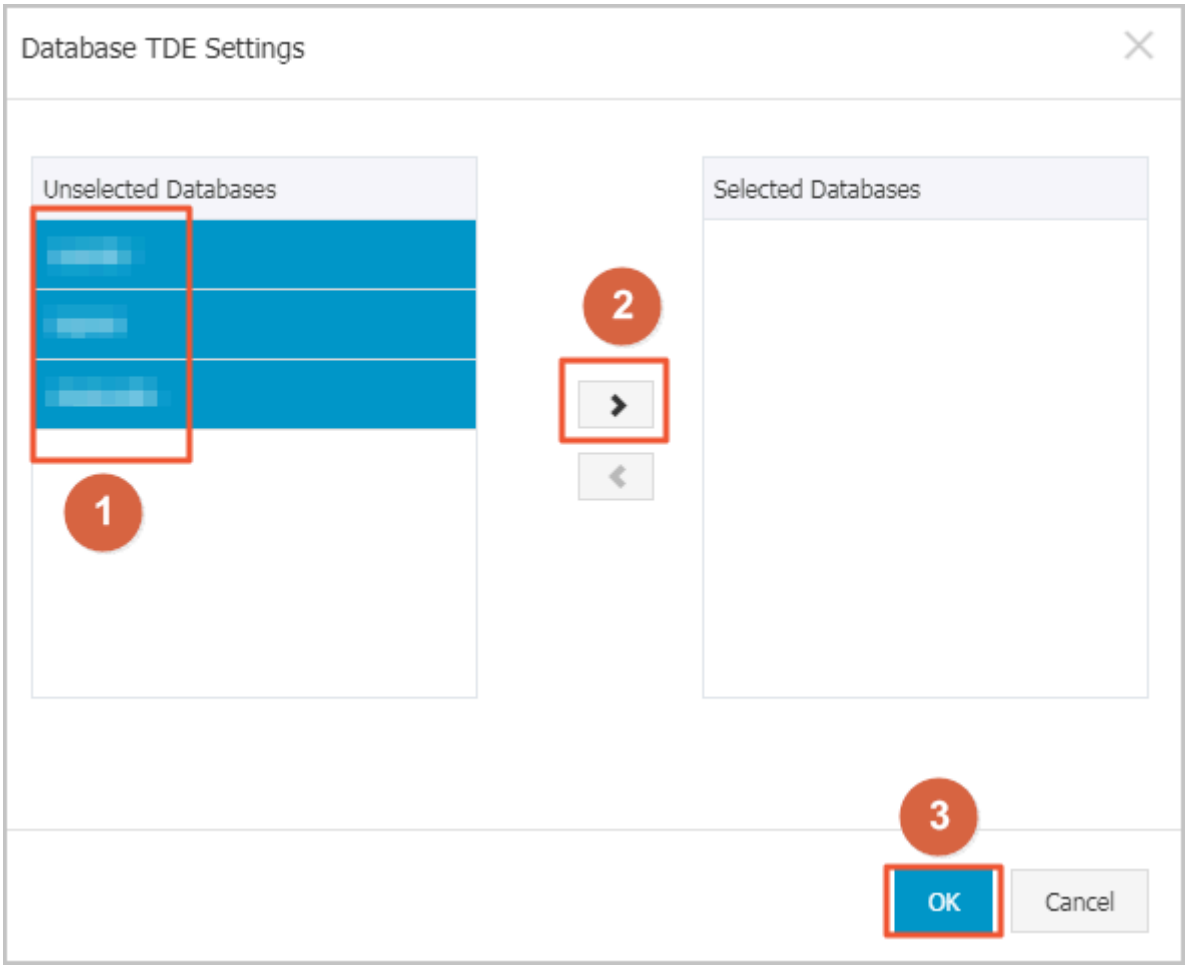


3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Data Security.
5. On the TDE tab, find TDE Status and click the switch next to Disabled.



6. In the displayed dialog box, click Confirm.

7. **Click the button for setting TDE. In the Database TDE Settings dialog box, select the databases you want to encrypt from the Unselected Databases list, click the right arrow to add them to the Selected Databases list, and click OK.**



Decrypt data

If you want to decrypt a database that is encrypted by TDE, you can remove the database from the Selected Databases list in the Database TDE Settings dialog box.

13.4 Configure distributed transaction whitelists

Distributed transaction whitelists allow for distributed transactions between an ECS instance and an ApsaraDB for RDS instance.

For more information about related best practices, see *#unique_134*.

Prerequisites

The ApsaraDB for RDS instance must be one of the following editions:

- **SQL Server 2012/2016 Enterprise Edition (High-availability Edition)**

- **SQL Server 2012/2016 Standard Edition**

RDS settings

1. **Log on to the *ApsaraDB for RDS console*.**
2. **In the upper-left corner of the page, select the region where the target ApsaraDB for RDS instance is located.**
3. **Find the instance and click the instance ID.**
4. **In the left-side navigation pane, click Data Security.**
5. **Click Edit on the right. In the dialog box that appears, enter the IP address of the ECS instance.**

   Note:

   - **If the ECS and ApsaraDB for RDS instances belong to the same VPC, enter the private IP address of the ECS instance. You can view the private IP address on the Instance Details page.**
   - **If the ECS and ApsaraDB for RDS instances do not belong to the same VPC, enter the public IP address of the ECS instance and apply for a public endpoint for the ApsaraDB for RDS instance. For more information, see *Apply for a public endpoint for an RDS for SQL Server instance*.**
6. **Click OK.**
7. **Click the Whitelist for Distributed Transaction tab.**
8. **Click <uicontrol data-spm-anchor-id="a2762.11472859.0.i130.2a23203bxY1y9R">Create Whitelist.**
9. **Set the parameters listed in the following table.**

Parameter	Description
Whitelist Name	The whitelist name must be 2 to 32 characters in length and can contain digits, lowercase letters, and underscore s (_). It must start with a lowercase letter and end with a lowercase letter or digit.

Parameter	Description
Whitelist	Enter the IP address and Windows computer name of the ECS instance, and separate them with a comma (,). Example: 192.168.1.100,k3ecstest. Enter multiple entries in different lines. **Note:** You can view the computer name by choosing Control Panel > System and Security > System.

10. Click OK.

ECS settings

1. Log on to the *ECS console*.
2. In the upper-left corner of the page, select the region where the target ECS instance is located.
3. Find the instance and click the instance ID.
4. In the left-side navigation pane, click Security Groups.
5. Click Add Rules on the right.
6. In the upper-right corner of the page, click Add Security Group Rule.
7. Set the parameters listed in the following table.

Parameter	Description
Rule Direction	Select Inbound.
Action	Select Allow.
Protocol Type	Select Customized TCP.
Port Range	Enter 135. **Note:** 135 is the fixed port of the RPC service.
Priority	Enter 1.
Authorization Type	Select IPv4 CIDR Block.
Authorization Objects	View the two IP addresses displayed on the Whitelist for Distributed Transaction tab of the Data Security page. Enter them in the Authorization Objects field. >

Parameter	Description
Description	The description must be 2 to 256 characters in length and cannot start with http:// or https://.

8. Click OK.
9. Add another security group rule by entering 1024/65535 in the Port Range field and specifying the other parameters in the same way as the previous rule.

14 Audit

14.1 SQL audit (database engine)

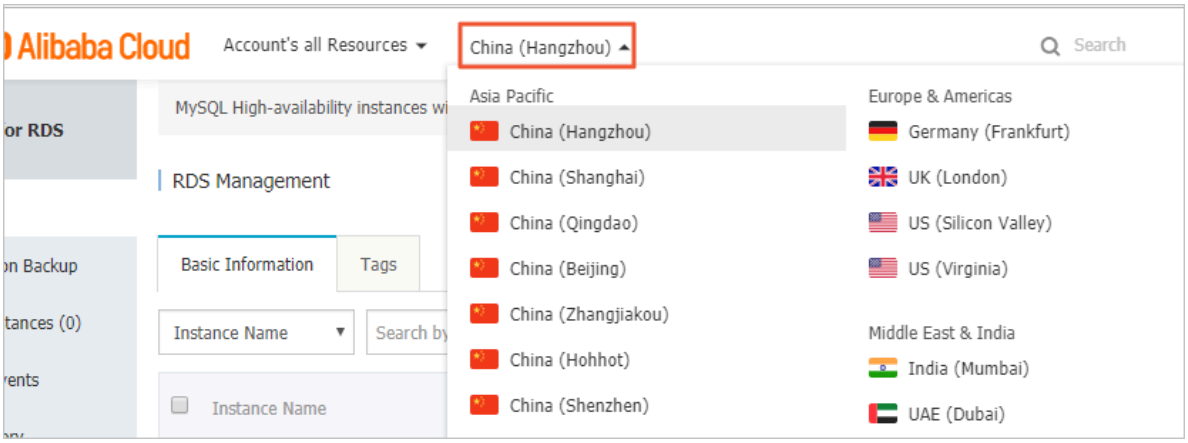
This topic describes the SQL audit function. You can use this function to audit SQL executions and check the details. Enabling SQL audit does not affect the instance performance.

Precautions

- **You cannot view the records that were generated before SQL audit is enabled.**
- **Enabling SQL audit does not affect the instance performance.**
- **SQL audit records are retained for 30 days.**
- **Files exported from SQL audit can be retained for two days. The system deletes the files that are older than two days.**
- **The SQL audit is disabled by default. When this feature is enabled, the instance incurs additional fees. For more information, see *ApsaraDB for RDS pricing*.**

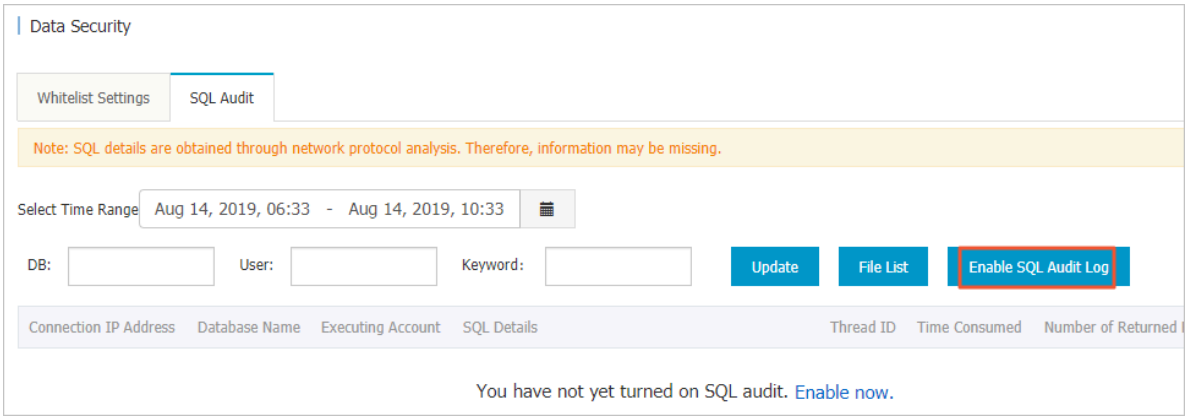
Enable SQL audit

1. **Log on to the *ApsaraDB for RDS console*.**
2. **In the upper-left corner of the page, select the region where the instance is located.**



3. **Find the instance and click the instance ID.**
4. **In the left-side navigation pane, click Data Security.**

5. Select the SQL Audit tab, and click Enable SQL Audit Log.



6. In the message box that appears, click OK.

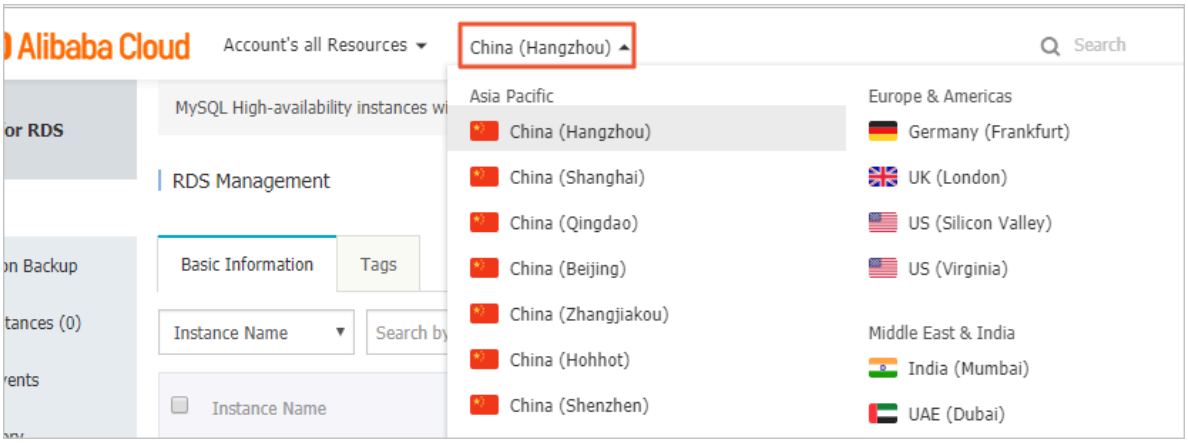
   After enabling SQL audit, you can query SQL information based on criteria such as time, database, user, and other key words.

Disable SQL audit

You can disable the SQL audit feature when you do not need to audit SQL to save costs. To disable SQL audit, follow these steps:

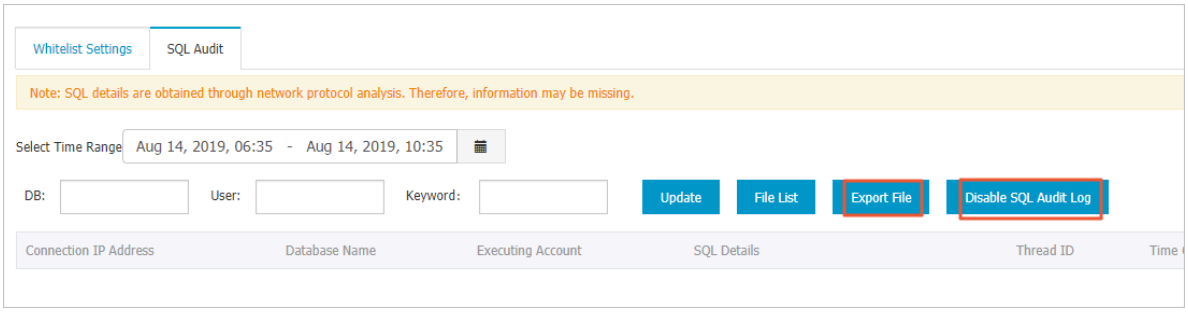
> **Note:**
> When the SQL audit feature is disabled, all the SQL audit records are cleared. We recommend that you export and store the audit records locally before disabling SQL audit.

1. Log on to the *ApsaraDB for RDS console*.
2. In the upper-left corner of the page, select the region where the instance is located.



3. Find the instance and click the instance ID.
4. In the left-side navigation pane, click Data Security.

5. Select the SQL Audit tab, click Export, and then store the exported file locally.
6. After the file is exported, click Disable SQL Audit Log.



7. In the message box that appears, click OK.

14.2 Manage logs

This topic describes how to manage logs through the RDS console or by using SQL statements. You can query error logs and slow query logs. The log query results help you to locate faults.

- For information about log backup policies and rules, see *Back up the data of an RDS for SQL Server instance*.
- For information about how to download log backup files, see *Download the data backup files and log backup files of an RDS for SQL Server instance*.
- For information about how to restore data through log backup files, see *Restore the data of an RDS for SQL Server instance*.

View logs by using the RDS console

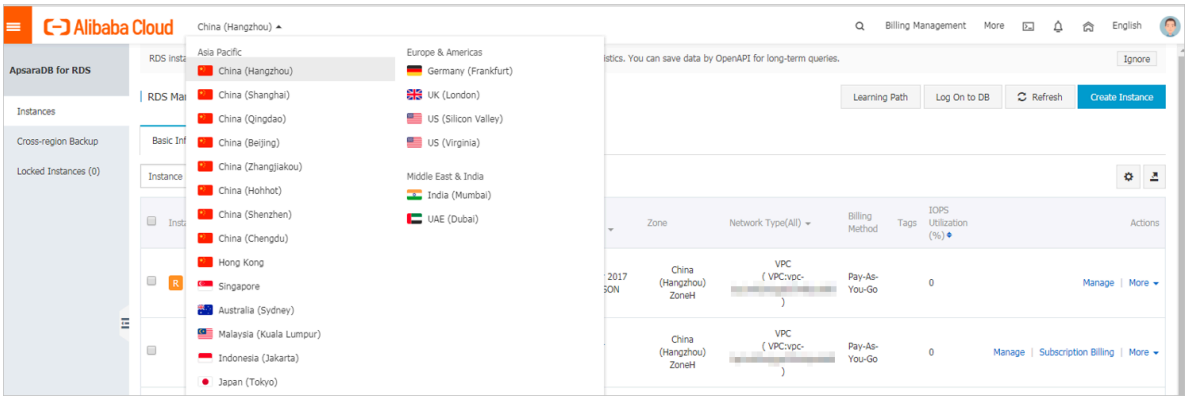
Prerequisites

The DB engine version is SQL Server 2008 R2.

Procedure

1. Log on to the *RDS console*.

2. In the upper-left corner, select the region where the target RDS instance is located.



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Log Management.
5. On the Log Management page, select Error Log, Slow Query Log, Slow Query Log Summary, or Primary/Secondary Instance Switch Log, select a time range, and click Search.

Query item	Description
Error Log	Records the SQL statements that are failed to be executed within the last one month.
Slow Query Log	Records the SQL statements that lasted for more than 1 second within the last one month. (You can reconfigure the `long_query_time` parameter to change this time threshold.)
Primary/Secondary Instance Switch Log	Records logs related to the switchovers between the master and slave instances within the last one month.

View logs by using SQL statements

Prerequisites

The DB engine version is one of the following:

- **SQL Server 2012**
- **SQL Server 2016**
- **SQL Server 2017**

Procedure

If the used DB engine version is SQL Server 2012 or SQL Server 2016, you can read error logs only by using the `sp_rds_read_error_logs` stored procedure, which works in the same way as the `sp_readerrorlog` stored procedure.

Example 1:

```
EXEC sp_rds_read_error_logs
```

Example 2:

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

If the used DB engine version is SQL Server 2017, you can read error logs by using the `sp_readerrorlog` stored procedure.

Example :

```
EXEC sp_readerrorlog
```

15 Data backup

15.1 Back up the data of an RDS for SQL Server instance

This topic describes how to back up the data of an RDS for SQL Server instance. You can specify a data and log backup cycle, according to which the system automatically backs up data and logs. Alternatively, you can manually back up the instance data.

Precautions

- **The backup files occupy the backup space of the RDS instance. If the used backup space exceeds the quota of free backup space, additional fees are incurred. For more information, see** *View the quota of free backup space for an RDS for SQL Server instance*.
- **For information about the billing method and billable items, see** *#unique_16*.
- **For information about the pricing of backup space, see** *ApsaraDB RDS for MySQL pricing*.
- **Do not perform DDL operations during the backup. Otherwise, tables are locked and consequently the backup fails.**
- **Back up data and logs during off-peak hours.**
- **If the data volume is large, the backup may take a long time.**
- **Backup files are retained for a specified time period. Download the backup files to your computer before they are deleted.**
- **You cannot manually delete backup files.**

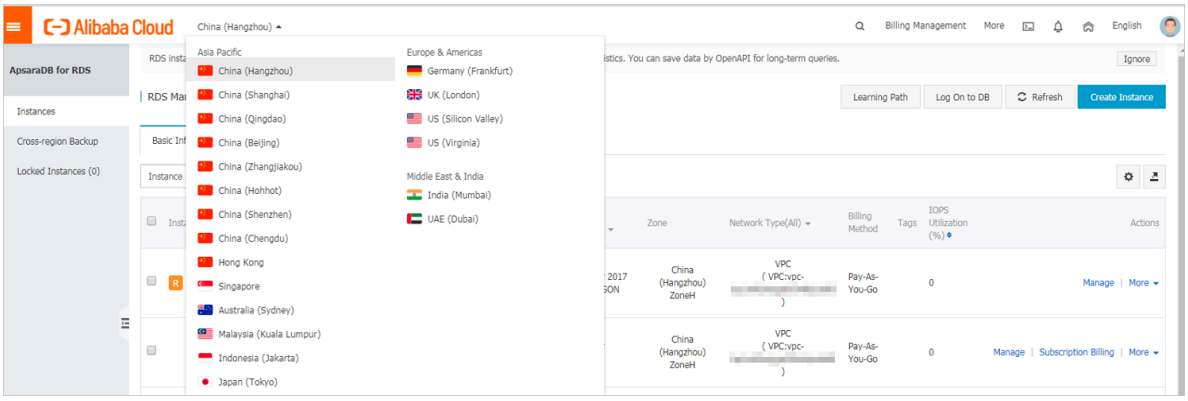
Overview

DB engine	Data backup	Log backup
SQL Server	· Full physical backup and incremental physical backup are supported, but logical backup is not supported. · Automatic backup is performed by cycle. A cycle consists of three phases: full backup, incremental backup, and incremental backup again. - For example, if a full backup is performed on Monday, then an incremental backup is performed on Tuesday and Wednesday separately. Next, a full backup is performed on Thursday, and an incremental backup is performed on Friday and Saturday separately. - If a manual full backup is performed within a backup cycle, then the manual full backup is followed by two automatic consecutive incremental backups. · Single-database backup is supported. You can back up the data of one or more databases in an RDS instance. · SQL Server shrinks transaction logs during each backup. You can log on to the RDS console, find the target RDS instance, and on the Backup and Restoration page click Shrink Transaction Log to manually shrink transaction logs.	· The system automatically generates log backup files. You can specify the log file backup frequency in the RDS console: - Same as Data Backup - Every 30 Minutes The log file size remains the same no matter which backup frequency you select. · The log backup function cannot be disabled. · You can specify the log retention period, which ranges from 7 days to 730 days. · You can download log backup files. Note: When the Backup Frequency parameter is set to Every 30 Minutes for an RDS instance, you can restore the instance to the time point when log backup files of the last 30 minutes were generated, in case that the instance becomes abnormal due to SSD damage or other faults.

Set a backup policy for automatic backup

ApsaraDB for RDS can automatically back up databases according to the backup policy you set.

1. **Log on to the *RDS console*.**
2. **Select the target region.**



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Backup and Restoration.**
5. **On the Backup and Restoration page, click the Backup Settings tab. On the Backup Settings tab, click Edit.**
6. **In the Backup Settings dialog box, set the backup parameters and click OK. The following table describes the parameters.**

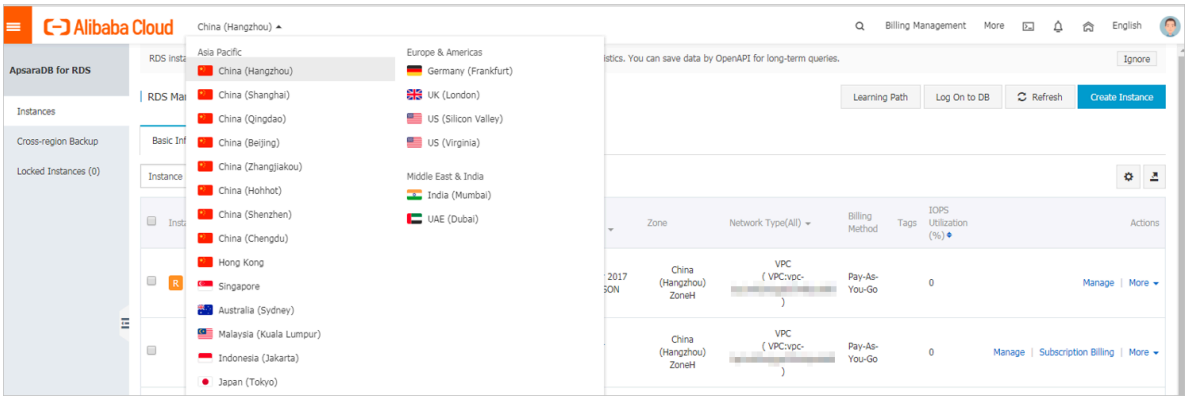
Parameter	Description
Data Retention Period	The data retention period spans from 7 days to 730 days. The default retention period is 7 days.

Parameter	Description
Backup Cycle	Select one or more workdays.
Backup Time	You can select any time period, which is measured in the unit of hour. We recommend that you select a time period during off-peak hours.

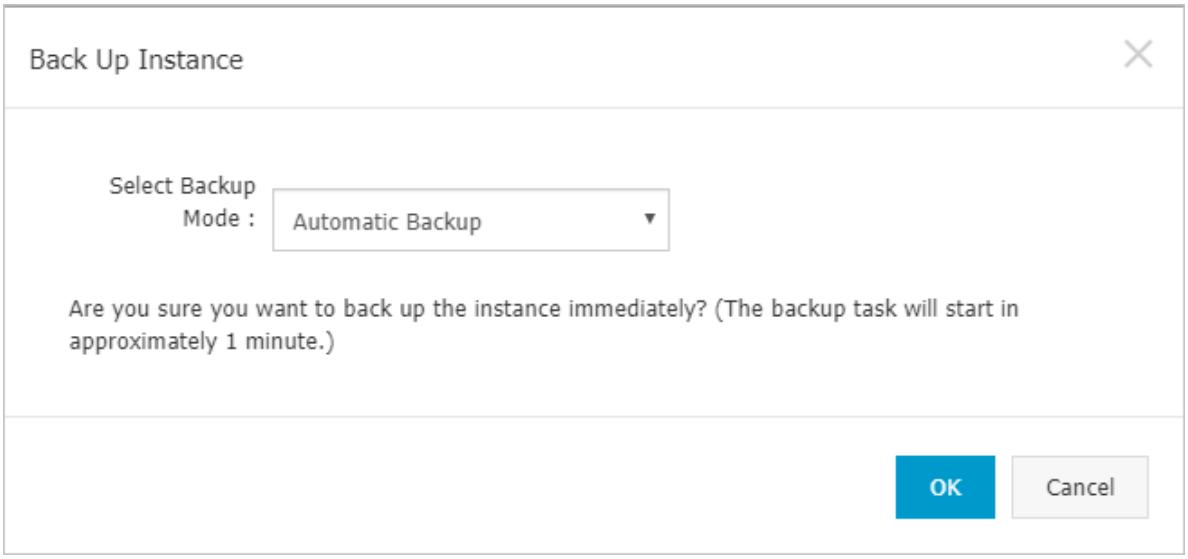
Parameter	Description
Backup Frequency	Valid values: · Same as Data Backup · Every 30 Minutes The log file size remains the same no matter which backup frequency you select.
Log Retention Period	The value of this parameter is the same as that of the Data Retention Period parameter.

Manually back up data

1. **Log on to the *RDS console*.**
2. **Select the target region.**



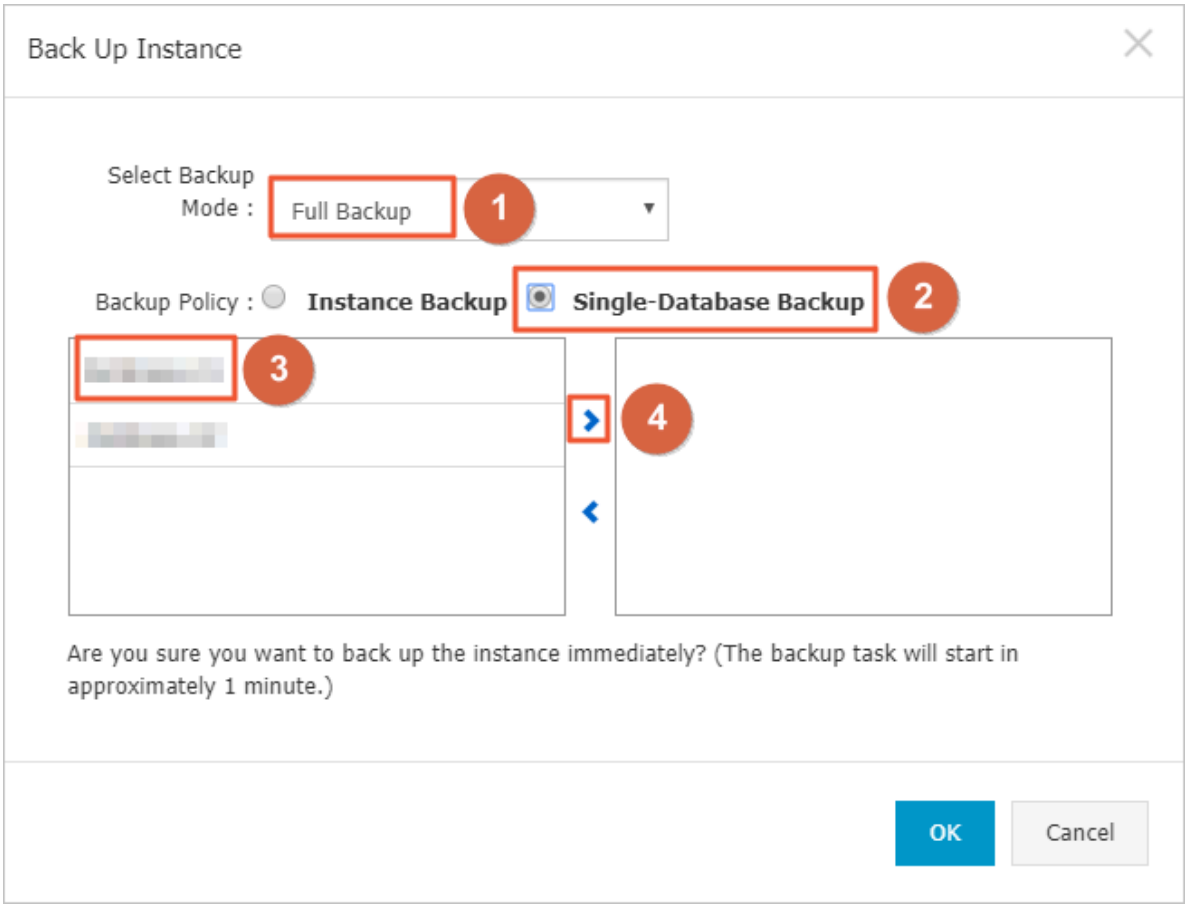
3. **Find the target RDS instance and click the instance ID.**
4. **In the upper-right corner of the Basic Information page, click Back Up Instance.**
5. **In the Back Up Instance dialog box, set the backup parameters and click OK.**



Note:

If you set the Select Backup Mode parameter to Full Backup and the Backup Policy parameter to Single-Database Backup, select a database from the left and click > to add the database to the list on the right. If the RDS instance does not

have a database, you must create databases according to *Create a database for an RDS for SQL Server instance*.



FAQ

1. **Can I disable the data backup function for an RDS for SQL Server instance?**

   No, the data backup function must be enabled. However, you can lower the backup frequency to at least two times a week.

2. **Can I disable the log backup function for an RDS for SQL Server instance?**

   No, the log backup function must be enabled.

APIs

API	Description
#unique_143	**Used to create a backup set for an RDS instance.**
#unique_144	**Used to query the backup set list of an RDS instance.**

API	Description
#unique_145	Used to query the backup settings of an RDS instance.
#unique_146	Used to modify the backup settings of an RDS instance.
#unique_147	Used to query the backup task list of RDS instance.
#unique_148	Used to query the log backup files of an RDS instance.

15.2 View the quota of free backup space for an RDS for SQL Server instance

This topic describes how to calculate and view the quota of free backup space for an RDS for SQL Server instance. The quota varies depending on the used DB engine version and edition. Additionally, this topic describes how to calculate the backup space beyond the quota.

Backup files occupy backup space. Each RDS instance has a specific quota of free backup space. If the total size of backup files exceeds the quota, additional fees are incurred.

Calculate the quota of free backup space and the backup space beyond the quota

Quota of free backup space = Round up (50% × Storage space purchased for the RDS instance) (Unit: GB)

Backup space beyond the quota = Backup data size + Backup log size - Round up (50 % × Storage space purchased for the RDS instance) (Unit: GB)

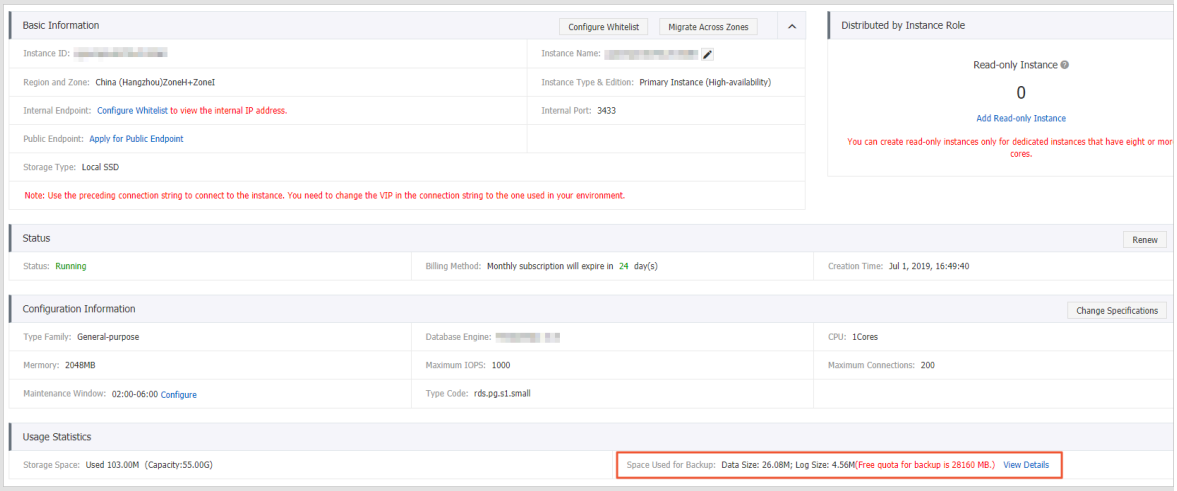
For example, the backup data size is 30 GB, the backup log size is 10 GB, and the storage space is 60 GB, then you must pay for 10-GB storage space every hour:

```
Hourly fees = 30 + 10 - 50% × 60 = 10 (GB)
```

Note:

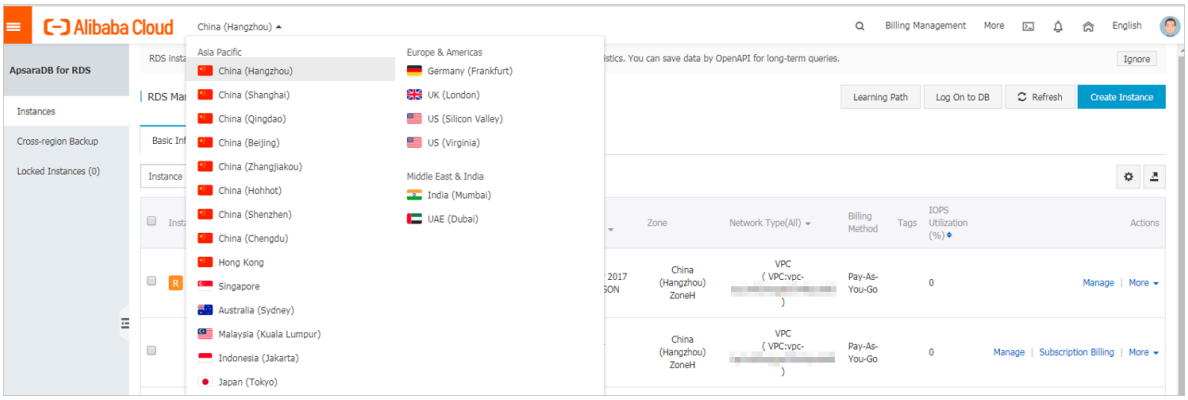
- **For more information about the hourly fees for the backup space beyond the quota, see** *ApsaraDB RDS for MySQL pricing*.

- **The Basic Editions of some DB engines store backup files generated within the last seven days for free. For more information, log on to the RDS console.**



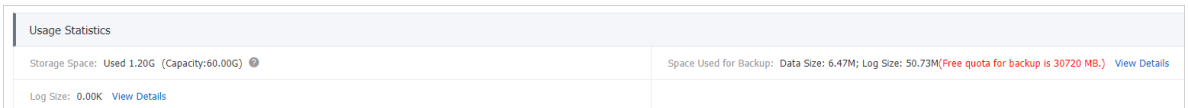
View the quota of free backup space in the RDS console

1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance and click its ID.**
4. **In the Usage Statistics section of the Basic Information page, view the data size next to Space Used for Backup. The data size is the quota of free backup space.**

> **Note:**
> **The quota of free backup space varies depending on the instance type. The following figure is only an example.**



15.3 Download the data backup files and log backup files of an RDS for SQL Server instance

This topic describes how to download the data backup files and log backup files of an RDS for SQL Server instance. The downloaded log backup files are not encrypted. You can save the backup files for archiving or use them to restore the instance to an on-premises database.

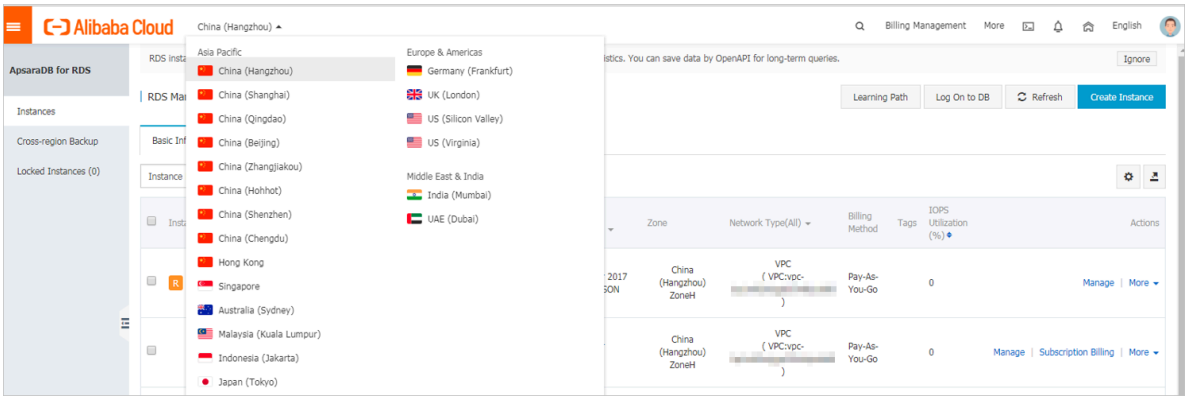
Limits

A RAM user who has only the read-only permissions cannot download backup files. You can add the required permissions to a RAM user in the RAM console. For more information, see *#unique_149*.

DB engine	Data backup download	Log backup download
SQL Server	Supports full physical backup, incremental physical backup, and single-database full physical backup.	Supported.

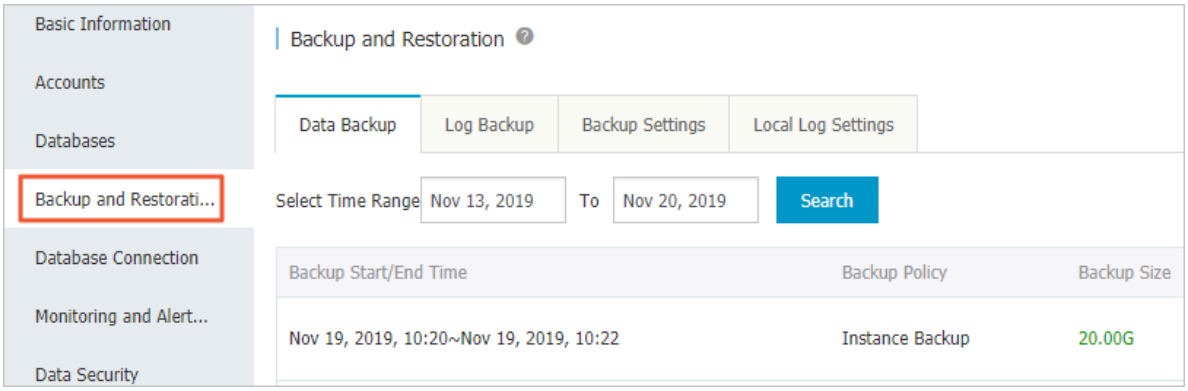
Procedure

1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance and click the instance ID.**

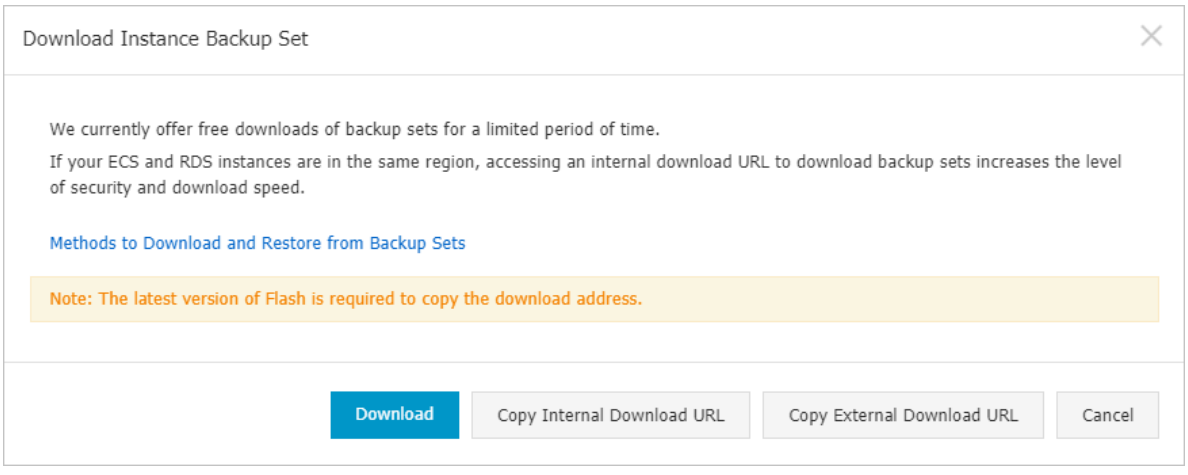
4. In the left-side navigation pane, click Backup and Restoration.



5. Click the Data Backup or Log Backup tab.
   - If you want to download data backup files, click Data Backup.
   - If you want to download log backup files, click Log Backup
6. Select a time range and click Search.
7. Find the data or log backup file you want to download, and in the Actions column click Download.

> **Note:**
> If you want to use the downloaded data backup file for data restoration, we recommend that you select the data backup file that was generated at the time point closest to the time point from which you want to restore data.

8. In the Download Instance Backup Set dialog box, select a download method.



Download method	Description
Download	To download the backup file through the public connection address.

Download method	Description
Copy Internal Download URL	To copy the internal download URL only. When your ECS instance is located in the same region as the RDS instance, you can log on to your ECS instance and then use the internal download URL to download the backup file. This is faster and more secure.
Copy External Download URL	To copy the external download URL only. This method is suitable when you download the backup file by using other tools.

Note:

In a Linux operating system, you can run the following command to download a data backup file:

```
wget -c '<Download URL of the data backup file>' -O <User-defined
file name>.tar.gz
```

- **The `-c` parameter is used to enable resumable download.**
- **The `-O` parameter is used to save the downloaded result as a file with the specified name (the file extension is .tar.gz or .xb.gz as included in the URL).**
- **If you enter more than one download URL, then you must include each download URL in a pair of single quotation marks ('). Otherwise, the download fails.**

16 Data restoration

16.1 Restore the data of an RDS for SQL Server instance

This topic describes how to restore the data of an RDS for SQL Server instance by using a data backup.

You can use one of the following methods to restore the data of an RDS for SQL Server instance:

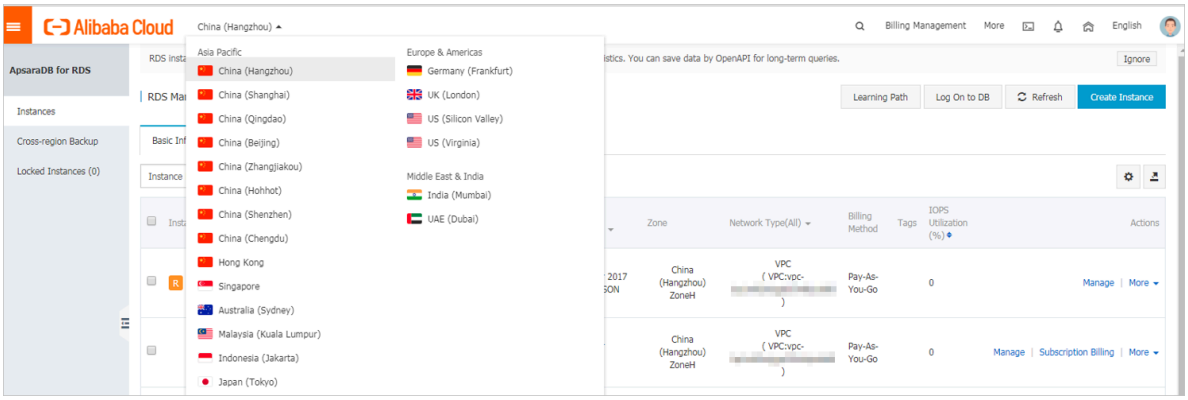
- *Restore data to an existing RDS instance*
- *Restore data to a new RDS instance*
- *Restore data to the source RDS instance through a temporary instance*

Restore data to an existing RDS instance

You can restore the data of one or more databases from an RDS instance by backup set or time to this RDS instance or to another existing RDS instance.

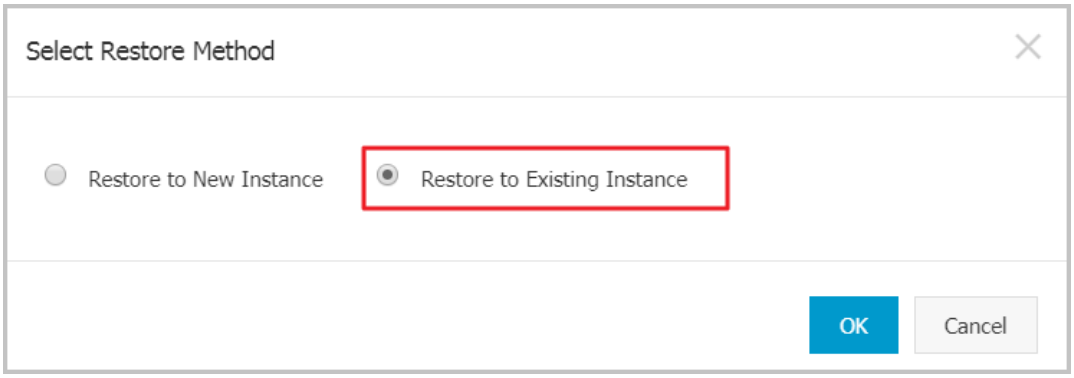
This function is available to SQL Server 2012 and SQL Server 2016.

1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**

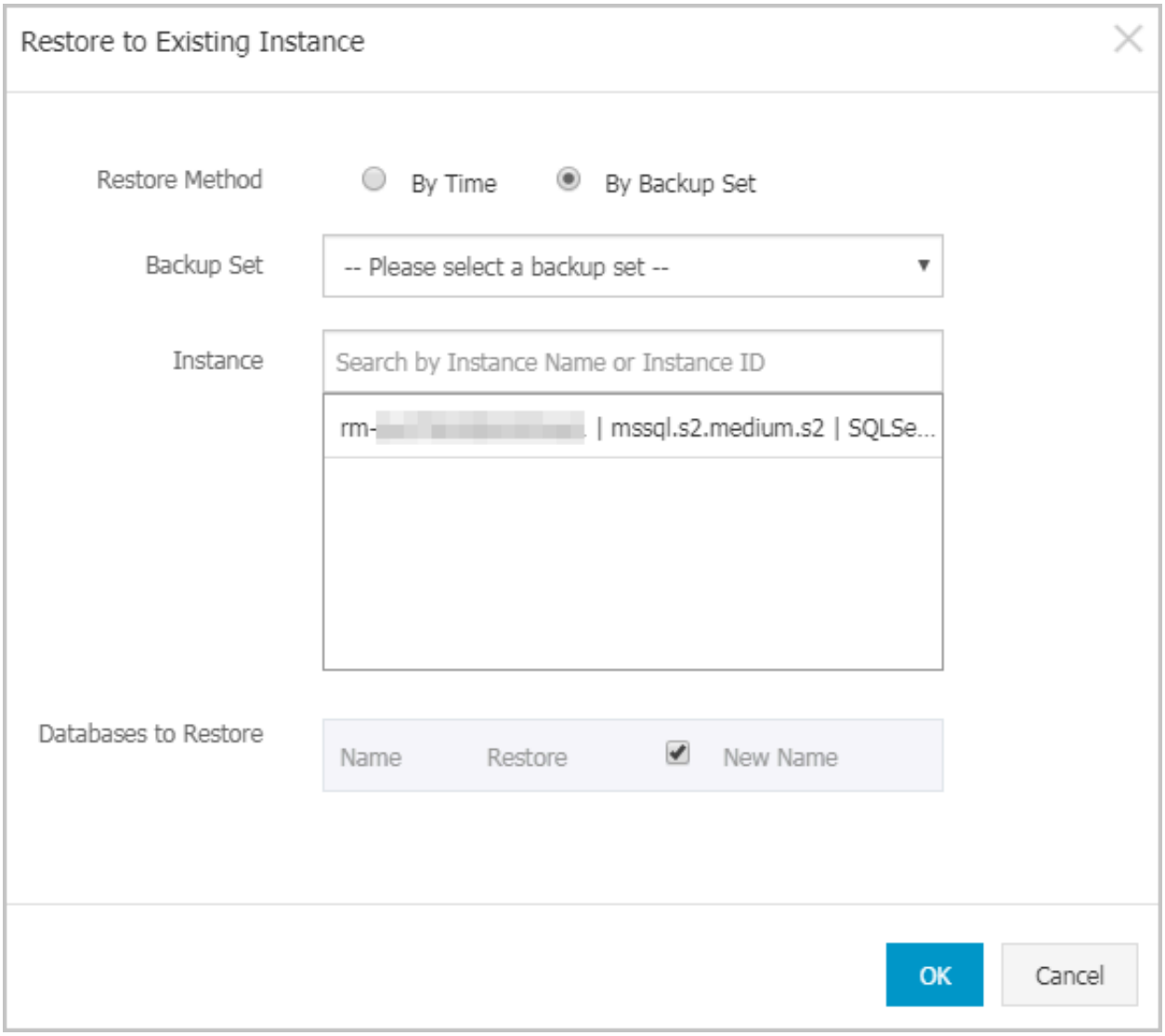


3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Backup and Restoration.**
5. **In the upper-right corner, click Restore.**

6. In the displayed dialog box, select Restore to Existing Instance and click OK.



7. Set the following parameters and click OK.



Note:

- **If two databases have the same name, you must select New Name and modify the database names.**

- A new database name can contain lowercase letters, digits, underscores (_), and hyphens (-).

Parameter	Description
Restore Method	· By Time: You can select any time point within the specified log retention period. For more information about how to view or change the log retention period, see *Back up the data of an RDS for SQL Server instance*. · By Backup Set: You can specify a full or incremental backup set from which you want to restore data.
Restore Time	Select the time point from which you want to restore data. This parameter is displayed when the Restore Method parameter is set to By Time.
Backup Set	Select the backup set from which you want to restore data. This parameter is displayed when the Restore Method parameter is set to By Backup Set.
Instance	Select the destination RDS instance to which you want to restore data. By default, the system displays the RDS instances (including the source RDS instance) that are created by the same Alibaba Cloud account, located in the same region, and use the same DB engine version as the source RDS instance. Note: If a large number of RDS instances are displayed, you can enter keywords in the search field to find the RDS instance you want.
Databases to Restore	a. Select the databases you want to restore. By default, all databases of the source RDS instance are displayed and selected. · If you want to restore the data of the whole instance, make sure that all databases are selected. · If you want to restore one or more databases, make sure that these databases are selected. b. Set the names of the restored databases. By default, the system uses the original database names. Note: The names of the restored databases cannot be the same as those of the existing databases in the destination RDS instance.

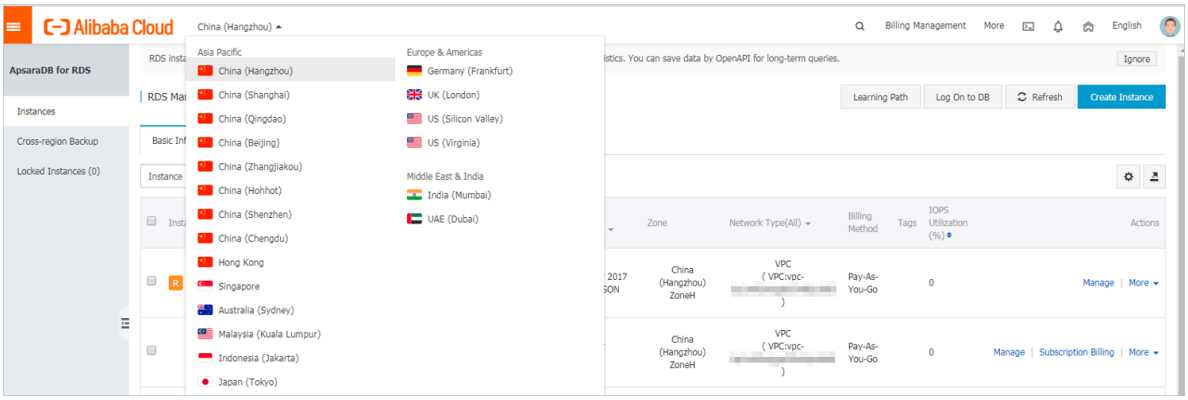
Restore data to a new RDS instance

You can restore the data of an RDS instance by backup set or time to a new RDS instance. If you choose to restore data by backup set, you can restore some or all databases in the selected backup set.

You must pay for the new RDS instance.

This function is available to SQL Server 2012, SQL Server 2016, and SQL Server 2017.

1. **Log on to the *RDS instance*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Backup and Restoration.**
5. **In the upper-right corner, click Restore.**
6. **In the displayed dialog box, select Restore to New Instance and click OK.**
7. **Select a billing method and set the parameters of the new RDS instance.**

Parameter	Description
Restore Mode	· By Time: You can select any time point within the specified log retention period. · By Backup Set: You can specify a full or incremental backup set from which you want to restore data.
Restore Point	Select the time point from which you want to restore data. This parameter is displayed when the Restore Method parameter is set to By Time.
Backup Set	Select the backup set from which you want to restore data. This parameter is displayed when the Restore Method parameter is set to By Backup Set.

Parameter	Description
Database	· All: to restore all databases in the selected backup set. · Part: to restore some databases in the selected backup set. If you select this option, you must select the databases you want to restore from the left list, and add them to the right list.
Edition/Zone/ CPU and Memory/ Capacity/ Network Type/ Duration	For more information, see *Create an RDS for SQL Server instance*.
Quantity	Specify the number of RDS instances you want to purchase. You can create up to five RDS instances at a time for data restoration.

8. Click Buy Now.
9. On the Order Confirmation page, select Terms of Service, Service Level Agreement, and Terms of Use, and click Pay Now to complete the payment.

Restore data to the source RDS instance through a temporary instance

This function is available to the following DB engine versions and editions:

- **SQL Server 2012 Enterprise Basic Edition**
- **SQL Server 2012/2016 Web Basic Edition**
- **SQL Server 2008 R2**

17 Disable the database proxy mode

This topic describes how to disable the database proxy mode for an RDS for SQL Server instance. Disabling the database proxy mode means switching to the standard mode, which helps improve the performance of the RDS instance.

Precautions

- **In the database proxy mode, the multi-statement function is enabled by default at the protocol layer. Therefore, after you disable the database proxy mode, if you do not enable the multi-statement function but run multiple SQL statements, the system reports errors in the SQL statements. To prevent this problem, you must check and add connection parameters in advance. For example, you can add the `allowMultiQueries` parameter to JDBC as follows:**

  ```
  dbc:mysql:///test?allowMultiQueries=true
  ```

- **You can only disable the database proxy mode (that is, switch from the database proxy mode to the standard mode). You cannot enable the database proxy mode (that is, switch from the standard mode to the database proxy mode).**
- **Switching the access mode may cause a 30-second transient disconnection. Therefore, we recommend that you switch the access mode during off-peak hours or make sure that your application can automatically reconnect to the RDS instance.**
- **If the RDS instance uses the SQL Server 2008 R2 version and runs in a VPC, the database proxy mode is used by default and cannot be switched to the standard mode.**
- **If the RDS instance uses the SQL Server 2008 R2 version and runs in a classic network, the standard mode is used by default and cannot be switched to the database proxy mode. Additionally, the RDS instance cannot be migrated to a VPC.**

Access modes

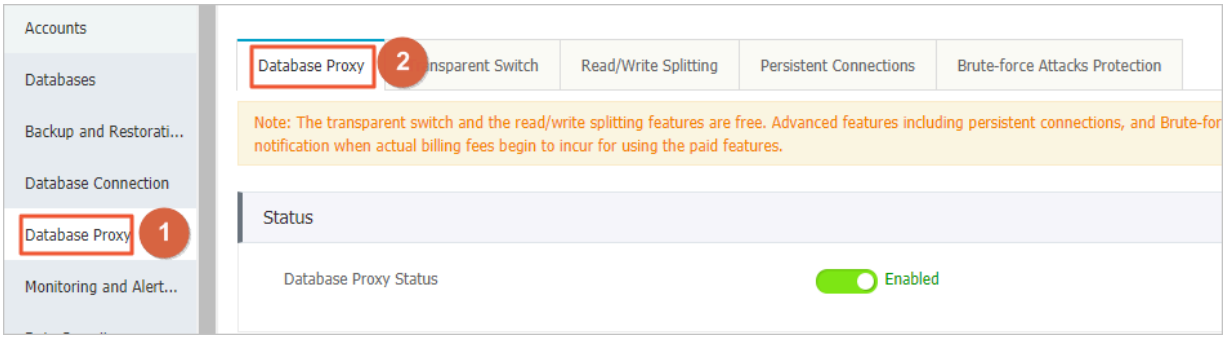
DB engine version	Supported access modes
SQL Server 2012/2016/2017	Standard mode
SQL Server 2008 R2	Standard mode and database proxy mode

Prerequisites

The database proxy mode is enabled for your RDS instance.

Note:

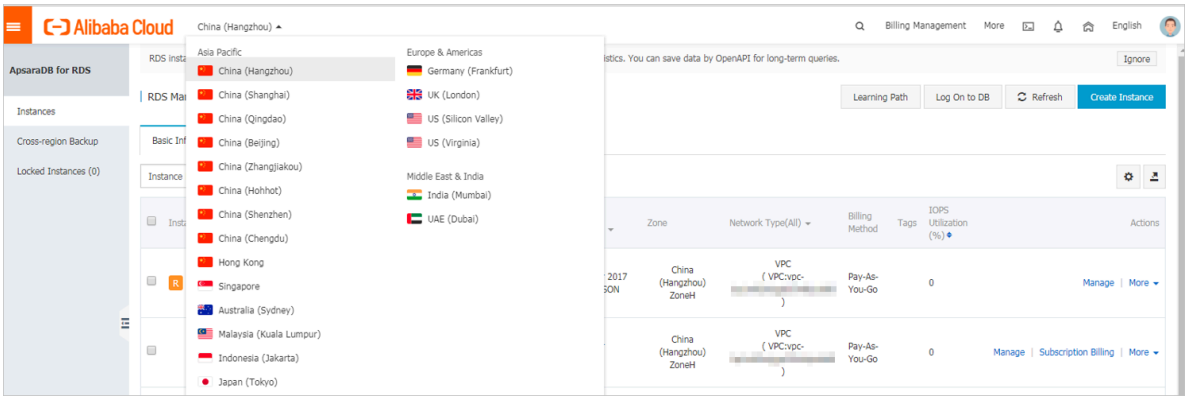
- **If the Database Proxy tab is displayed, the database proxy mode is enabled and you can proceed with the operations described in this topic.**
- **If the Database Proxy tab is not displayed, the database proxy mode is not displayed and you can skip this topic.**



Procedure

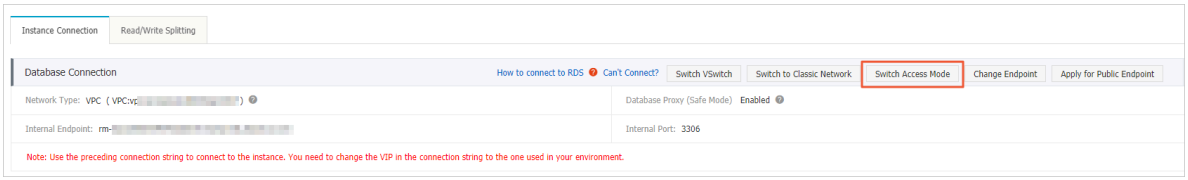
Method 1

1. **Log on to the *RDS console*.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance and click the instance ID.**
4. **In the left-side navigation pane, click Database Connection.**

5. Click Switch Access Mode and in the displayed dialog box, click Confirm.

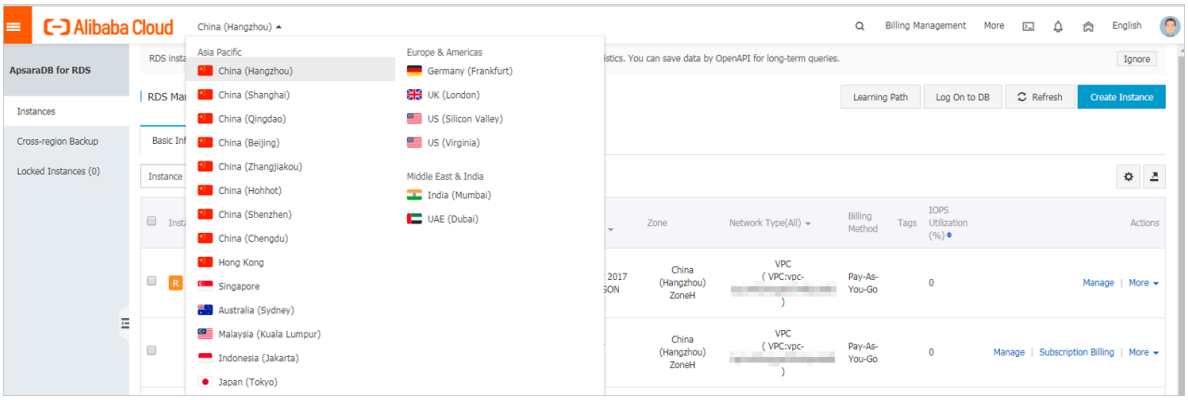


Note:

This button is available only when you have enabled the database proxy mode.

Method 2

1. Log on to the *RDS console*.
2. In the upper-left corner, select the region where the target RDS instance is located.



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click Database Proxy.
5. On the Database Proxy tab, click the slider next to the database proxy status and in the displayed dialog box, click Confirm.

Note:

This tab page is available only when you have enabled the database proxy mode.

18 Tag

18.1 Create tags

This section describes how to create tags for one or more RDS instances. If you have a large number of RDS instances, you can create tags and then bind the tags to the instances so that you can classify and better manage the instances. Each tag consists of a key and a value.

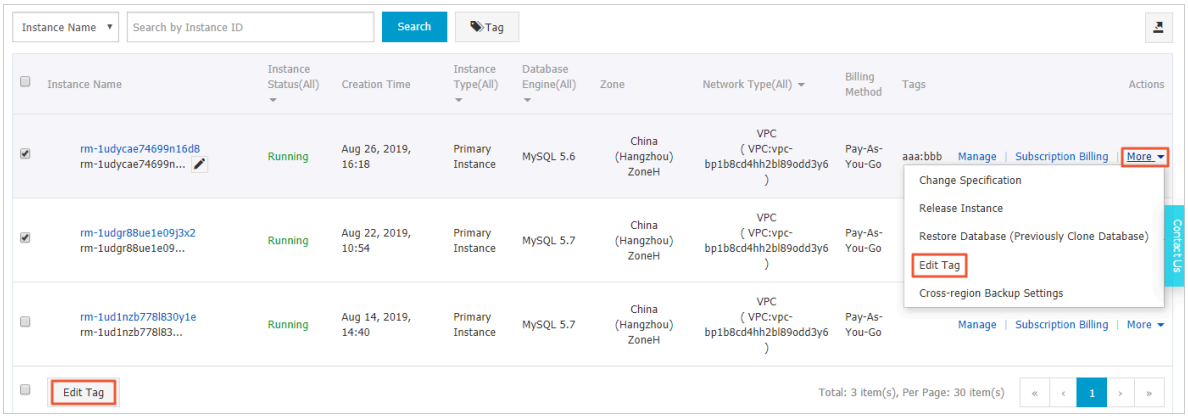
Limits

- **Up to 10 tags can be bound to each RDS instance, and each tag must have a unique key. Tags with the same key are overwritten.**
- **You can bind or unbind up to five tags at a time.**
- **Tag information is independent in different regions.**
- **After you unbind a tag from an RDS instance, the tag is deleted if it is not bound to any other RDS instance.**

Procedure

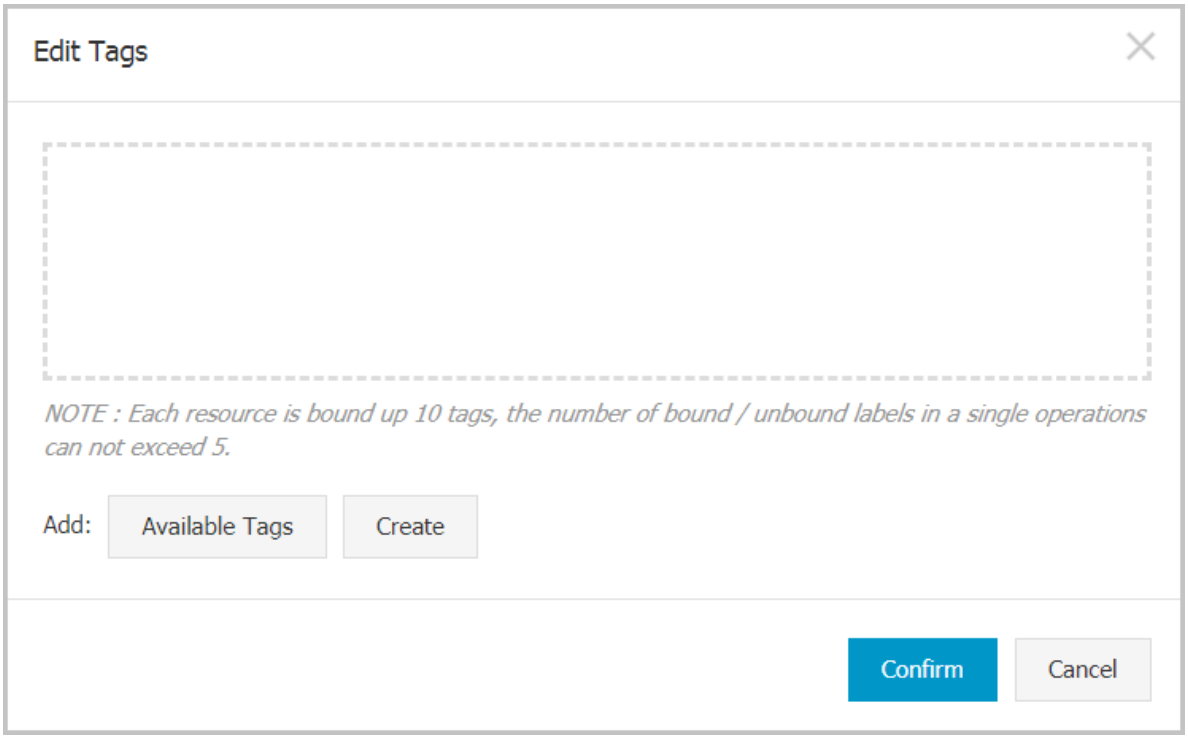
1. **Log on to the *RDS console* and in the left-side navigation pane, click Instances.**
2. **In the upper-left corner, select the region where the target RDS instance is located.**

3. Specify the method of adding tags.
   - If you want to add tags to only one RDS instance, find the RDS instance and in the Actions column choose More > Edit Tag.
   - If you want to add tags to more than one RDS instance, select the RDS instances and click Edit Tag



4. Click Add, enter the Key and Value, and click Confirm.

> **Note:**
> If you have already created tags, you can click Available Tags and select an existing tag.



5. After you add all the tags you need, click Confirm.

APIs

API	Description
AddTagsToResource	Used to bind a tag to RDS instances.

18.2 Delete tags

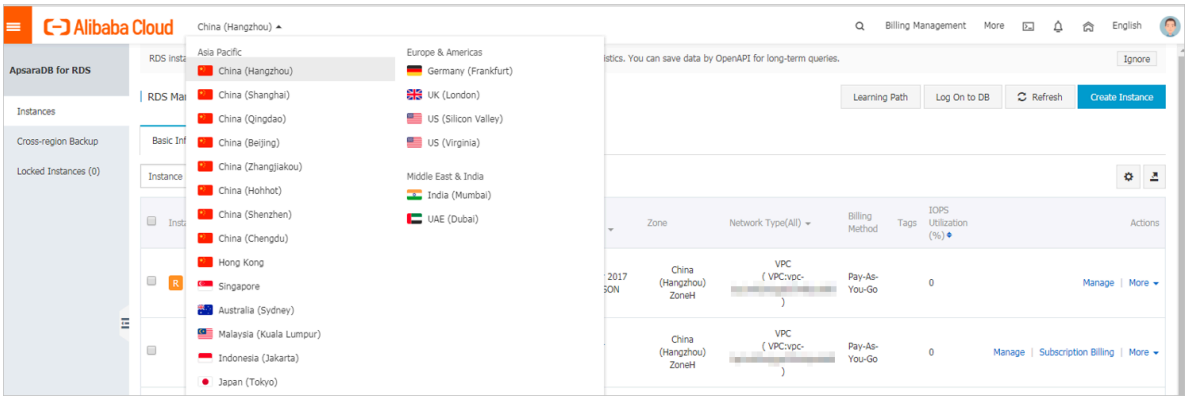
This topic describes how to delete tags from an RDS instance when you no longer need the tags or due to adjustments to the instance.

Limits

- **You can bind or unbind up to five tags at a time.**
- **After you unbind a tag from an RDS instance, the tag is deleted if it is not bound to any other instance.**

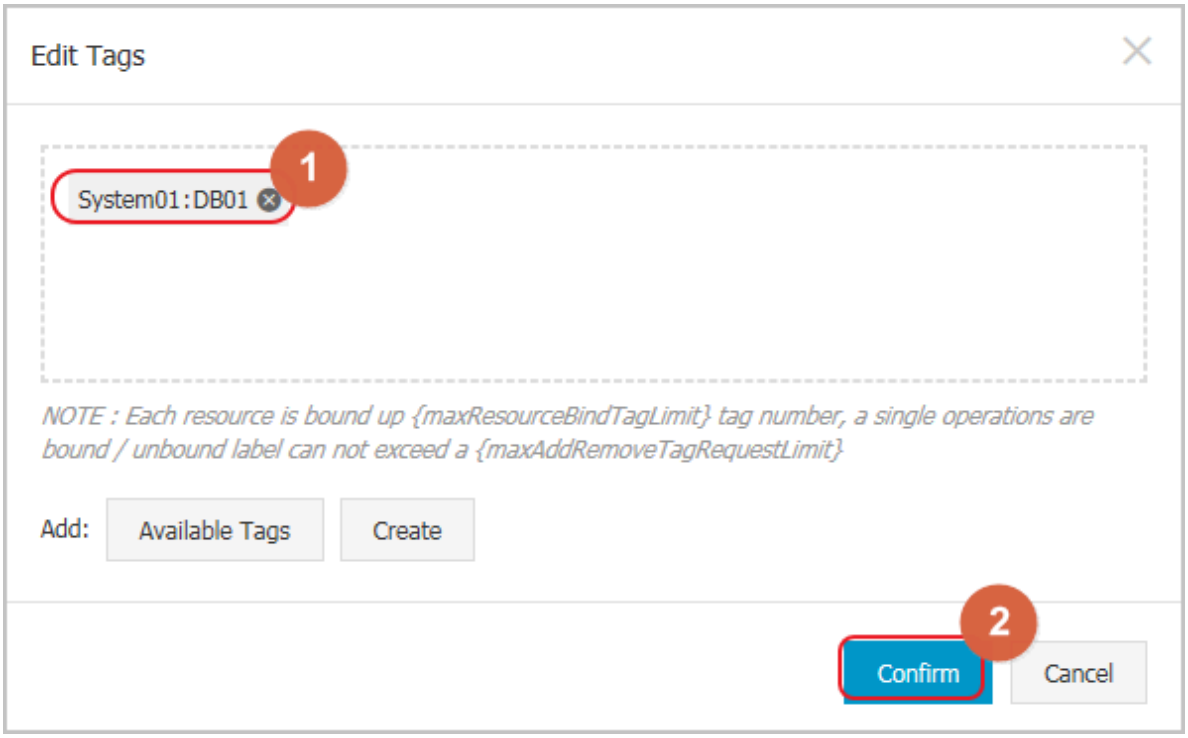
Procedure

1. **Log on to the *RDS console* and in the left-side navigation pane, click Instances.**
2. **In tne upper-left corner, select the region where the target RDS instance is located.**



3. **Find the target RDS instance and in the Actions column, choose More > Edit Tag.**

4. Find the tag you want to delete, and click the X button following the tag.



5. Click Confirm.

APIs

API	Description
#unique_156	Used to unbind a tag from an RDS instance.

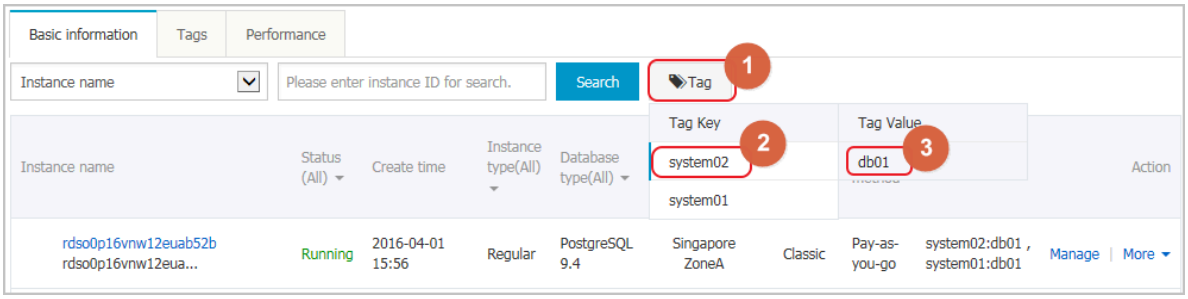
18.3 Filter RDS instances by tag

This topic describes how to filter RDS instances by tag.

1. Log on to the *RDS console* and in the left-side navigation pane click Instances.
2. On the Basic Information tab, click the Tag button next to Search and select a tag key and a tag value.

Note:

You can click the X button following the tag key to cancel the filter operation.



APIs

API	Description
DescribeTags	Used to query tags.