Alibaba Cloud
ApsaraDB for RDS

RDS SQL Server Database

Issue: 20200506
**Legal disclaimer**

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

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.
5. By law, all the 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

<table>
<thead>
<tr>
<th>Style</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>![danger]</td>
<td>A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.</td>
<td>![danger] <strong>Danger:</strong> Resetting will result in the loss of user configuration data.</td>
</tr>
<tr>
<td>![warning]</td>
<td>A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.</td>
<td>![warning] <strong>Warning:</strong> Restarting will cause business interruption. About 10 minutes are required to restart an instance.</td>
</tr>
<tr>
<td>![caution]</td>
<td>A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.</td>
<td>![caution] <strong>Notice:</strong> If the weight is set to 0, the server no longer receives new requests.</td>
</tr>
<tr>
<td>![note]</td>
<td>A note indicates supplemental instructions, best practices, tips, and other content.</td>
<td>![note] <strong>Note:</strong> You can use Ctrl + A to select all files.</td>
</tr>
<tr>
<td>[ ] or [a</td>
<td>b]</td>
<td>This format is used for an optional value, where only one item can be selected.</td>
</tr>
</tbody>
</table>

### Style
- **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`
<table>
<thead>
<tr>
<th>Style</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>{} or {a</td>
<td>b}</td>
<td>This format is used for a required value, where only one item can be selected.</td>
</tr>
</tbody>
</table>
Contents

Legal disclaimer......................................................................................................................... I
Document conventions.............................................................................................................. I
1 Preface............................................................................................................................... 1
2 Limits of ApsaraDB RDS SQL Server.................................................................................. 3
3 Quick start........................................................................................................................... 6
  3.1 General workflow to use RDS SQL Server....................................................................... 6
  3.2 Create an RDS SQL Server instance............................................................................. 7
  3.3 Connect to an RDS SQL Server instance...................................................................... 11
  3.4 Configure a whitelist for an RDS SQL Server instance............................................... 13
  3.5 Creating accounts and databases............................................................................... 17
    3.5.1 Create databases and accounts for an ApsaraDB for RDS instance running SQL Server 2019, 2017, 2016, or 2012............................................................... 17
    3.5.2 Create databases and accounts for an RDS instance in SQL Server 2008 R2........................................................................................................................................ 21
  3.6 Read-only instances...................................................................................................... 26
    3.6.1 Introduction to SQL Server read-only instances................................................ 26
    3.6.2 Create an RDS SQL Server read-only instance.................................................. 30
  3.7 Functions supported by different versions and editions of SQL Server.......................... 35
  3.8 Stored procedures......................................................................................................... 41
4 Data migration...................................................................................................................... 49
  4.1 Migrate data from a user-created database to an RDS SQL Server database................. 49
    4.1.1 Migrate data from an on-premises database to ApsaraDB RDS SQL Server 2008 R2 using full backup files................................................................. 49
    4.1.2 Migrate full backup data to ApsaraDB RDS SQL Server 2012, 2016, or 2017.................................................. 56
    4.1.3 Migrate incremental backup data to ApsaraDB RDS SQL Server 2012, 2016, or 2017.................................................. 64
    4.1.4 Migrate data from all SQL Server databases in an instance to ApsaraDB RDS SQL Server.............................................................................................. 77
5 Billing................................................................................................................................... 92
  5.1 Switch from pay-as-you-go billing to subscription billing............................................ 92
  5.2 Manually renew an RDS SQL Server instance............................................................ 93
  5.3 Automatically renew an RDS SQL Server instance..................................................... 95
6 Manage pending events....................................................................................................... 100
7 Version upgrade................................................................................................................ 102
  7.1 Upgrade from Basic Edition to High-availability Edition............................................ 102
  7.2 Upgrade SQL Server 2008 R2 to SQL Server 2012/2016............................................ 107
  7.3 Upgrade an instance from SQL Server 2012 to SQL Server 2016............................... 114
8 Instance.................................................................................. 115
  8.1 Create an RDS SQL Server instance........................................... 115
  8.2 Restart an RDS SQL Server instance........................................... 119
  8.3 Set the maintenance window of an RDS SQL Server instance......... 120
  8.4 Migrate an RDS SQL Server instance across zones in the same region 122
  8.5 Manually or automatically switch over services between the RDS MySQL master and slave instances................................................. 125
  8.6 Change the network type of an RDS SQL Server instance.............. 129
  8.7 Release an RDS SQL Server instance........................................... 135
  8.8 Change the configuration of an RDS SQL Server instance............. 138
  8.9 DBCC features of ApsaraDB RDS SQL Server............................... 141
  8.10 Reconfigure parameters for an RDS for SQL Server instance........... 142
    8.10.1 Reconfigure parameters the in the RDS console.................... 142
    8.10.2 Reconfigure parameters by using SQL commands................ 145
  8.11 Instance recycle bin............................................................. 146

9 Database connection........................................................... 149
  9.1 Connect to an RDS SQL Server instance....................................... 149
  9.2 View the internal and public endpoints and ports of an RDS SQL Server instance.......................................................... 151
  9.3 Apply for a public endpoint for an RDS SQL Server instance............ 152
  9.4 Use DMS to log on to an ApsaraDB for RDS instance.................... 154
  9.5 Configure a hybrid access solution to smoothly migrate an RDS instance from the classic network to a VPC................................. 156
  9.6 Kill connections of ApsaraDB RDS SQL Server............................ 163

10 Read/write splitting.............................................................. 164
  10.1 Introduction to read/write splitting............................................. 164
  10.2 Create an RDS SQL Server read-only instance.............................. 166
  10.3 Enable cluster management for an RDS SQL Server instance.......... 171
  10.4 Modify the read weights............................................................ 176
  10.5 Disable cluster management for an RDS SQL Server instance......... 178
  10.6 Rules of weight distribution by the system................................... 179

11 Account.............................................................................. 181
  11.1 Create an account for an RDS SQL Server instance....................... 181
  11.2 Reset the password of an account for an RDS SQL Server instance... 181
  11.3 Change the permissions of an account for an RDS SQL Server instance... 182
  11.4 Authorize a service account for an RDS SQL Server instance.......... 184
  11.5 Delete an account for an RDS SQL Server instance....................... 186
  11.6 Manage ApsaraDB RDS SQL Server logins.................................. 187
  11.7 Manage ApsaraDB RDS SQL Server users.................................... 188

12 Database............................................................................ 190
  12.1 Create a database for an RDS SQL Server instance........................ 190
  12.2 Delete a database for an RDS SQL Server instance....................... 190
  12.3 Manage databases with SQL statements..................................... 191
12.4 Database replication ................................................................. 193
  12.4.1 Copy database data between instances ............................. 193
  12.4.2 Copy a database of ApsaraDB RDS SQL Server 2008 R2 ...... 196
  12.4.3 Copy a database of ApsaraDB RDS SQL Server 2012 or later ... 199

13 Monitoring and alerts ............................................................. 200
  13.1 View resource and engine monitoring data .......................... 200
  13.2 Set the monitoring frequency ............................................. 202
  13.3 Set an alert rule ................................................................. 203

14 Data security ................................................................. 206
  14.1 Configure a whitelist for an RDS SQL Server instance ............. 206
  14.2 Configure SSL encryption for an RDS SQL Server instance ....... 209
  14.3 Set TDE for an RDS SQL Server instance ............................. 214
  14.4 Configure distributed transaction whitelists ......................... 216
  14.5 Configure disk encryption .................................................. 219

15 Audit ................................................................. 221
  15.1 SQL audit (database engine) ................................................ 221
  15.2 Manage logs ................................................................. 223
  15.3 Event history ................................................................. 225

16 Backup ................................................................. 228
  16.1 Back up the data of an RDS SQL Server instance .................... 228
  16.2 View the quota of free backup space for an RDS SQL Server instance 235
  16.3 Download the data backup files and log backup files of an RDS SQL Server instance ................................................................. 237

17 Restoration ................................................................. 240
  17.1 Restore data of ApsaraDB RDS SQL Server instances through temporary instances ................................................................. 240
  17.2 Log on to a temporary instance .......................................... 244
  17.3 Restore the data of an RDS SQL Server instance .................... 245

18 Disable the database proxy mode ............................................ 251

19 Tag ................................................................. 254
  19.1 Create tags ................................................................. 254
  19.2 Delete tags ................................................................. 256
  19.3 Filter RDS instances by tag ................................................ 257

20 SQL Server ................................................................. 259
  20.1 Create a linked server for SQL Server instances ...................... 259
  20.2 Connect Kingdee K/3 WISE to ApsaraDB RDS SQL Server ......... 260
  20.3 Use SSRS for an ApsaraDB RDS SQL Server instance .......... 268
1 Preface

This topic provides an overview of RDS SQL Server, 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 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

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-premise database</td>
<td>Refers to the database deployed in the local server room or the database not on the ApsaraDB RDS.</td>
</tr>
<tr>
<td>ApsaraDB RDS XX (XX represents one of the following database engines: MySQL, SQL Server, PostgreSQL, and PPAS.)</td>
<td>Indicates the ApsaraDB for RDS of a specific database engine. For example, ApsaraDB RDS MySQL means the database engine of the instance enabled on the RDS is MySQL.</td>
</tr>
</tbody>
</table>
This topic describes the limits of ApsaraDB RDS for SQL Server. You must understand the limits to make instances more stable and secure.

ApsaraDB RDS for SQL Server instances are provided with Microsoft SQL Server licenses. You cannot use your own licenses. The other limits are described in the following table.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of databases</td>
<td>2017 EE</td>
<td>2017 SE</td>
<td>2008 R2</td>
</tr>
<tr>
<td></td>
<td>2016 SE and</td>
<td>2012 SE and</td>
<td>2012 Web and</td>
</tr>
<tr>
<td></td>
<td>2016 EE</td>
<td>2012 EE</td>
<td>2016 Web</td>
</tr>
<tr>
<td></td>
<td>2012 SE and</td>
<td>2012 EE</td>
<td>2012 SE and</td>
</tr>
<tr>
<td></td>
<td>2012 EE</td>
<td>2016 EE</td>
<td>2016 SE</td>
</tr>
<tr>
<td>Maximum number of database accounts</td>
<td>300</td>
<td>300</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>500</td>
</tr>
<tr>
<td></td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Creation of accounts, logon connections,</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>and databases</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Database-level data definition language (DDL)</td>
<td>Supported</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>trigger</td>
<td>Supported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database permission authorization</td>
<td>Supported</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------</td>
<td>---------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td>2017 EE</td>
<td>2017 SE</td>
<td>2008 R2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2016 SE and 2016 EE</td>
<td>2012 Web and 2016 Web</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2012 SE and 2012 EE</td>
<td>2012 SE and 2016 SE</td>
</tr>
<tr>
<td></td>
<td>2016 EE</td>
<td></td>
<td>2012 EE Basic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2016 EE</td>
</tr>
<tr>
<td>KILL permission</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Linked server</td>
<td>Supported</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Distributed transaction</td>
<td>Supported</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>SQL Profiler</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Tuning Advisor</td>
<td>Supported</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Change Data Capture (CDC)</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Change tracking</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows domain account logon</td>
<td>Not supported</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Email</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL Server Integration Services (SSIS)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL Server Analysis Services (SSAS)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL Server Reporting Services (SSRS)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Common Language Runtime (CLR)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Limits of ApsaraDB RDS SQL Server

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2017 EE</td>
<td>2017 SE</td>
<td>2012 Web and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2016 SE and 2016 EE</td>
<td>2016 Web</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2012 SE and 2012 EE</td>
<td>2012 SE and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2016 SE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2012 EE Basic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2016 EE</td>
</tr>
<tr>
<td>Asynchronous communication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy management</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Maximum number of databases

An ApsaraDB for RDS instance that runs SQL Server 2008 R2 supports up to 50 databases. In the other SQL Server versions, the maximum number of databases varies based on the instance type. You can use the following formulas to calculate the maximum number of databases:

- **Cluster and High-availability Editions**

\[
\min\left\{ \left\lfloor \sqrt{\text{CPU}\text{cores}} \right\rfloor \times 50, 300 \right\}
\]

The maximum number obtained from the preceding formula cannot exceed 300.

- **Basic Edition**

\[
\min\left\{ \left\lfloor \sqrt{\text{CPU}\text{cores}} \right\rfloor \times 100, 400 \right\}
\]

The maximum number obtained from the preceding formula cannot exceed 400.
3 Quick start

3.1 General workflow to use RDS SQL Server

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

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

The following flowchart shows the general workflow.

1. Create an RDS SQL Server instance.
2. Configure a whitelist for the RDS SQL Server instance.
3. Apply for a public endpoint for an RDS SQL Server instance.
4. Create databases and accounts for the RDS SQL Server instance. For more information, see the following resources:
   - Create databases and accounts for an ApsaraDB for RDS instance running SQL Server 2019, 2017, 2016, or 2012
   - Create databases and accounts for an RDS instance in SQL Server 2008 R2
5. Connect to the RDS SQL Server instance.
3.2 Create an RDS SQL Server instance

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

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

For information about the pricing of RDS MySQL instances, see #unique_15.

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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 **SQL Server**.  
**Note:** The available DB engines vary depending on the region you select.                                                                                                                                                                                                                                                                                        |
**Note:** The available versions vary depending on the region you select.                                                                                                                                                                                                                                                                                          |
| 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_17. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Storage Type</strong></td>
<td>Select a storage type. Valid values:</td>
</tr>
<tr>
<td></td>
<td>• Local SSD: An SSD that is located on the same node as the DB engine. Storing data to local SSDs reduces I/O latency.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>For more information, see #unique_18.</td>
</tr>
<tr>
<td><strong>Zone</strong></td>
<td>Select a zone.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Multi-zone deployment is more secure because it provides zone-level disaster tolerance.</td>
</tr>
<tr>
<td><strong>Network Type</strong></td>
<td>Select a network type. Valid values:</td>
</tr>
<tr>
<td></td>
<td>• Classic Network: indicates a traditional network.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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_19](#).  
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. |
| **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 fees 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

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_20</td>
<td>Used to create an RDS instance.</td>
</tr>
</tbody>
</table>

3.3 Connect to an RDS SQL Server instance

This topic describes how to connect to an RDS 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 Service (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_21.
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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server type</td>
<td>Select Database Engine</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Server name</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Select SQL Server Authentication.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Enter the account name of the RDS instance.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password of the account of the RDS instance.</td>
</tr>
</tbody>
</table>

4. Click Connect.

3.4 Configure a whitelist for an RDS SQL Server instance

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

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_22</td>
<td>Used to view the IP address whitelist of an RDS instance.</td>
</tr>
<tr>
<td>#unique_23</td>
<td>Used to modify the IP address whitelist of an RDS instance.</td>
</tr>
</tbody>
</table>

### 3.5 Creating accounts and databases

#### 3.5.1 Create databases and accounts for an ApsaraDB for RDS instance running SQL Server 2019, 2017, 2016, or 2012

This topic describes how to create databases and accounts for an ApsaraDB for RDS instance running SQL Server 2019, 2017, 2016, or 2012.

**Note:**
For information about how to create databases and accounts for RDS instances that run other SQL Server versions, see Create databases and accounts for an RDS instance in SQL Server 2008 R2.

### Prerequisites

The RDS instance runs one of the following SQL Server versions:

- SQL Server 2012
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019
Create an account

You can only create a privileged account in the ApsaraDB for RDS console, whereas you can create a standard account in the ApsaraDB for RDS console or by calling an API operation.

Precautions

• Follow the least privilege principle to create accounts and grant them appropriate read-only and read/write permissions on databases. If necessary, you can create more than one account and only grant them permissions on specific databases. If an account does not need to write data to a database, only assign the read-only permission to the account.

• For security purposes, we recommend that you set strong passwords for the database accounts of your RDS instance and change the passwords regularly.

Procedure

1. Log on to the ApsaraDB for RDS console.

2. In the upper-left corner of the page, select the region where the target RDS instance resides.

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

4. In the left-side navigation pane, click Accounts.

5. Click Create Account.

6. Configure the following parameters and click Create.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Account</td>
<td>Enter the name of the account. The name must be 2 to 16 characters in length and can contain lowercase letters, digits, and underscores (_). It must start with a letter and end with a letter or digit.</td>
</tr>
</tbody>
</table>
## Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Account Type**        | - **Privileged Account**: You can only select the Privileged Account option if it is your first time to create an account for the RDS instance. Each RDS instance can only have one privileged account. The privileged account of an RDS instance cannot be deleted.  
  - **Standard Account**: You can only select the Standard Account account after a privileged account is created for the RDS instance. Each RDS instance can have more than one standard account. You must manually grant permissions on databases to standard accounts. |
| **Authorized Databases**| Select the authorized databases of the account. If no databases are created, you can leave this parameter empty.  
You can grant permissions on multiple databases to one account by following these steps:  
  a. In the Unauthorized Databases section, select the databases on which you want to grant permissions to the account.  
  b. Click Add to add the selected databases to the Authorized Databases section.  
  c. In the Authorized Databases section, specify the permissions that the account will gain on each authorized database. The permissions are **Read/Write**, **Read-only**, or **Owner**. You also have the option to specify permissions on all authorized databases simultaneously by clicking the button in the upper-right corner. The button shows **Set All to Read/Write**, **Set All to Read-only**, and **Set All to Owner** as you click it.  
  
**Note:** The account is only authorized to create tables, delete tables, and modify table schemas in a database when it has the **Owner** permission on that database. |
### Parameter | Description
--- | ---
**Password** | Enter the password of the account. The password must meet the following requirements:
- It is 8 to 32 characters in length.
- It contains three of the following character types: uppercase letters, lowercase letters, digits, and special characters.
- The special characters include ! @ # $ % ^ & * ( ) _ + - =

**Re-enter Password** | Enter the password of the account again.

**Description** | Enter a description that helps identify the account. The description can be up to 256 characters in length.

---

Create a database

1. Log on to the ApsaraDB for RDS console.
2. In the upper-left corner of the page, select the region where the target RDS instance resides.
3. Find the target RDS instance and click its ID.
4. In the left-side navigation pane, click **Databases**.
5. Click **Create Database**.
6. Configure the following parameters and click **Create**.

### Parameter | Description
--- | ---
**Database Name** | Enter the name of the database. The name must be 2 to 64 characters in length. It can contain lowercase letters, digits, underscores (_), and hyphens (-). It must start with a letter and end with a letter or digit.
### 3.5.2 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 [Create databases and accounts for an ApsaraDB for RDS instance running SQL Server 2019, 2017, 2016, or 2012](#).

#### Prerequisites

The SQL Server version is 2008 R2.

#### Create an account

Precautions

---

### Table: Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Character Set</td>
<td>Select the character set supported by the database. You can also select all and then select a character set from the drop-down list that appears.</td>
</tr>
<tr>
<td>Authorized Account</td>
<td>Select the account to which you want to grant the permissions on the database. Then, set Account Type to Read/Write, Read-only, or Owner. If no accounts are created, you can leave this parameter empty.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that helps identify the database. The description can be up to 256 characters in length.</td>
</tr>
</tbody>
</table>

### Related operations

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_25</td>
<td>Creates an account for an ApsaraDB for RDS instance.</td>
</tr>
<tr>
<td>#unique_26</td>
<td>Creates a database for an ApsaraDB for RDS instance.</td>
</tr>
</tbody>
</table>
• 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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Database Account</strong></td>
<td>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.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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 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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Name</td>
<td>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.</td>
</tr>
<tr>
<td>Supported Character Set</td>
<td>Select a character set. If the character set you need is not listed, click <strong>All</strong> and select it from the drop-down list.</td>
</tr>
<tr>
<td>Authorized Account</td>
<td>Select the account to which you want to assign permissions. If no accounts have been created, you can leave this parameter blank.</td>
</tr>
<tr>
<td>Account Type</td>
<td>This parameter is displayed after you select an authorized account. You can set this parameter to <strong>Read/Write</strong> or <strong>Read-only</strong>.</td>
</tr>
<tr>
<td>Remarks</td>
<td>Optional. Enter details about the database to better identify it. You can enter up to 256 characters.</td>
</tr>
</tbody>
</table>
7. Click OK.

Resources

#unique_27

APIS

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_25</td>
<td>Used to create an account for an RDS instance.</td>
</tr>
<tr>
<td>#unique_28</td>
<td>Used to create a database for an RDS instance.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Region</th>
<th>rds.mssql.s2.large 2-core 4 GB</th>
<th>rds.mssql.s2.xlarge 2-core 8 GB</th>
<th>rds.mssql.s3.large 4-core 8 GB</th>
<th>rds.mssql.m1.medium 4-core 16 GB</th>
<th>rds.mssql.c1.large 8-core 16 GB</th>
<th>rds.mssql.c1.xlarge 8-core 32 GB</th>
<th>rds.mssql.c2.xlarge 16-core 64 GB</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>China mainland's regions</td>
<td>$0.225</td>
<td>$0.447</td>
<td>$0.459</td>
<td>$0.851</td>
<td>$0.888</td>
<td>$1.732</td>
<td>$3.389</td>
<td>$0.0003/GB</td>
</tr>
<tr>
<td>China (Hong Kong)</td>
<td>$0.264</td>
<td>$0.522</td>
<td>$0.537</td>
<td>$0.993</td>
<td>$1.035</td>
<td>$2.02</td>
<td>$3.954</td>
<td>$0.0004/GB</td>
</tr>
<tr>
<td>US (Virginia)</td>
<td>$0.273</td>
<td>$0.542</td>
<td>$0.556</td>
<td>$1.028</td>
<td>$1.072</td>
<td>$2.093</td>
<td>$4.096</td>
<td>$0.0003/GB</td>
</tr>
<tr>
<td>US (Silicon Valley)</td>
<td>$0.292</td>
<td>$0.579</td>
<td>$0.595</td>
<td>$1.099</td>
<td>$1.146</td>
<td>$2.237</td>
<td>$4.378</td>
<td>$0.0003/GB</td>
</tr>
<tr>
<td>Singapore</td>
<td>$0.311</td>
<td>$0.616</td>
<td>$0.632</td>
<td>$1.170</td>
<td>$1.220</td>
<td>$2.381</td>
<td>$4.661</td>
<td>$0.0004/GB</td>
</tr>
<tr>
<td>Region</td>
<td>rds.mssql.s2.large 2-core 4 GB</td>
<td>rds.mssql.s2.xlarge 2-core 8 GB</td>
<td>rds.mssql.s3.large 4-core 8 GB</td>
<td>rds.mssql.m1.medium 4-core 16 GB</td>
<td>rds.mssql.c1.large 8-core 16 GB</td>
<td>rds.mssql.c1.xlarge 8-core 32 GB</td>
<td>rds.mssql.c2.xlarge 16-core 64 GB</td>
<td>Storage</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Australia</td>
<td>$0.315</td>
<td>$0.622</td>
<td>$0.646</td>
<td>$1.209</td>
<td>$1.259</td>
<td>$2.415</td>
<td>$4.829</td>
<td>$0.0005/GB</td>
</tr>
<tr>
<td>Malaysia</td>
<td>$0.296</td>
<td>$0.586</td>
<td>$0.601</td>
<td>$1.112</td>
<td>$1.159</td>
<td>$2.262</td>
<td>$4.428</td>
<td>$0.0004/GB</td>
</tr>
<tr>
<td>Indonesia</td>
<td>$0.311</td>
<td>$0.616</td>
<td>$0.632</td>
<td>$1.170</td>
<td>$1.220</td>
<td>$2.381</td>
<td>$4.661</td>
<td>$0.0004/GB</td>
</tr>
<tr>
<td>Japan</td>
<td>$0.311</td>
<td>$0.615</td>
<td>$0.632</td>
<td>$1.171</td>
<td>$1.221</td>
<td>$2.381</td>
<td>$4.660</td>
<td>$0.0005/GB</td>
</tr>
<tr>
<td>Germany (Frankfurt)</td>
<td>$0.311</td>
<td>$0.615</td>
<td>$0.632</td>
<td>$1.171</td>
<td>$1.221</td>
<td>$2.381</td>
<td>$4.660</td>
<td>$0.0005/GB</td>
</tr>
<tr>
<td>UK (London)</td>
<td>$0.311</td>
<td>$0.615</td>
<td>$0.632</td>
<td>$1.171</td>
<td>$1.221</td>
<td>$2.381</td>
<td>$4.660</td>
<td>$0.0005/GB</td>
</tr>
<tr>
<td>UAE (Dubai)</td>
<td>$0.327</td>
<td>$0.646</td>
<td>$0.665</td>
<td>$1.230</td>
<td>$1.283</td>
<td>$2.500</td>
<td>$4.895</td>
<td>$0.0007/GB</td>
</tr>
<tr>
<td>India (Mumbai)</td>
<td>$0.296</td>
<td>$0.586</td>
<td>$0.601</td>
<td>$1.112</td>
<td>$1.159</td>
<td>$2.262</td>
<td>$4.428</td>
<td>$0.0004/GB</td>
</tr>
</tbody>
</table>

**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 specificat...
ions 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 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:

<table>
<thead>
<tr>
<th>Database</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server</td>
<td>Up to 7 read-only instances can be created for each master instance.</td>
</tr>
</tbody>
</table>

- 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 SQL Server read-only instance

This topic describes how to create read-only instances for an RDS 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.

```
<table>
<thead>
<tr>
<th>Instance Name</th>
<th>Creation Time</th>
<th>Instance Status</th>
<th>Database Engine</th>
<th>Zone</th>
<th>Network Type</th>
<th>Replication Method</th>
<th>Instance Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Running</td>
<td>SQL Server 2017</td>
<td>China (Hangzhou) Zone</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

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

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_33</td>
<td>Used to create an RDS read-only instance.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Module</th>
<th>Function</th>
<th>High-availability editions</th>
<th>Basic editions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Life cycle</td>
<td>Create an instance</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Restart an instance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Automatic renewal</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change the billing method</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change specifications</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Release an instance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create a temporary instance</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Upgrade the engine version</td>
<td>Coming soon</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Clone an instance</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>Create a read-only instance</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
</tbody>
</table>


2008 R2 Enterprise
<table>
<thead>
<tr>
<th>Module</th>
<th>Function</th>
<th>High-availability editions</th>
<th>Basic editions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance properties</td>
<td>View a list of instances</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>View instance details</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit instance description</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the maintenance time period</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage instance labels</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Migrate to another zone</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Database connection</td>
<td>VPC address</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Public network address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Read/write splitting address</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Service availability</td>
<td>Disaster recovery in a zone</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Cross-zone disaster recovery</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Cross-region disaster recovery</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Module</td>
<td>Function</td>
<td>High-availability editions</td>
<td>Basic editions</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------</td>
<td>----------------------------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2019 Standard</td>
<td>2008 R2 Enterprise</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2017 Standard</td>
<td>2016 Web</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2016 Standard/Enterprise</td>
<td>2012 Web</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2012 Standard/Enterprise</td>
<td>2012 Web</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2008 R2 Enterprise</td>
<td>2012 Enterprise</td>
</tr>
<tr>
<td>Module</td>
<td>Function</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Disaster recovery drill</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Backup and restore</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Full backup</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Incremental backup</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Log backup</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Customize backup policies</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Restore from a backup set</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Restore to time</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Restore from external backup files</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Restore to a clone instance</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>Partial backup</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>Partial restore</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Monitoring and</td>
<td>Resource monitoring</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>alarms</td>
<td>Engine monitoring</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Customize monitoring policies</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

Issue: 20200506
## High-availability editions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregate monitoring items</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter management</td>
<td>Parameter update</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported (T-SQL)</td>
<td>Supported (T-SQL)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Parameter template</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log management</td>
<td>Error logs</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported (T-SQL)</td>
<td>Supported (T-SQL)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Running logs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Data management functions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data management</td>
<td>User management</td>
<td>Supported</td>
<td>Supported (T-SQL)</td>
<td>Supported (T-SQL)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Databases and table management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Table operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Task scheduling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module</td>
<td>Function</td>
<td>High-availability editions</td>
<td>Basic editions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------</td>
<td>----------------------------</td>
<td>----------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data tunnel</td>
<td>Homogeneous data migration</td>
<td>Supported (DTS)</td>
<td>Supported (DTS)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Heterogeneous data migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data synchronization</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data subscription</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Database replication between instances</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data security</td>
<td>IP address whitelist</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Management and operation audit</td>
<td>Supported (IP address whitelist)</td>
<td>Supported (IP address whitelist)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firewall</td>
<td>Supported (IP address whitelist)</td>
<td>Supported (IP address whitelist)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Database audit</td>
<td>Supported</td>
<td>Supported</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Storage encryption</td>
<td>Not supported</td>
<td>Supported</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network encryption</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security group management</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Functions supported by official editions

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifications</td>
<td>16-core 64 GB</td>
<td>24-core 128 GB</td>
<td>None</td>
</tr>
<tr>
<td>High availability</td>
<td>Single host</td>
<td>Mirror HA</td>
<td>Always On availability</td>
</tr>
<tr>
<td>Data compression</td>
<td>Not supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>SQL Profiler</td>
<td>Not supported</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Column-based index</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Table/index partitioning</td>
<td></td>
<td>Supported by SQL Server 2016 but not by SQL Server 2012</td>
<td></td>
</tr>
<tr>
<td>CDC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online DDL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parallel queries</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 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:

```sql
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:

```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:

```sql
EXEC sp_rds_set_db_online 'db'
```

The parameter represents the database to be brought online.

**Set global database privileges**

T-SQL:

```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:

```sql
EXEC sp_rds_drop_database 'db'
```

The parameter represents the database to be deleted.

**Set change tracking**

**T-SQL:**

```sql
sp_rds_change_tracking
```

**Supported editions:**

High-Availability Edition

**Description:**

Sets change tracking for the database.

**Method:**

```sql
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:**

```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_enable_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 procedure does not rename the physical database file.
Method:

```sql
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 Migrate data from a user-created database to an RDS SQL Server database

4.1.1 Migrate data from an on-premises database to ApsaraDB RDS SQL Server 2008 R2 using full backup files

This topic describes how to migrate data from an on-premises database to an ApsaraDB RDS SQL Server 2008 R2 instance using full backup files.

SQL Server 2008 R2 instances allow you to easily migrate data to the cloud. You only need to use Microsoft's official backup feature to back up full data on your own database, and then upload the backup files to Alibaba Cloud Object Storage Service (OSS) to fully migrate the data to the specified database of ApsaraDB for RDS through the RDS console. The backup feature of Microsoft that is fully compatible with ApsaraDB RDS SQL Server, along with OSS, greatly improve the cloud migration efficiency.

Prerequisites

You have created a destination database in your ApsaraDB RDS SQL Server instance. For more information about how to create a database, see Create databases and accounts for an RDS instance in SQL Server 2008 R2.

Note:

The destination database and the on-premises database must have the same name.

Billing

When you migrate data to Alibaba Cloud, no additional fees are incurred on ApsaraDB for RDS, but certain fees are incurred on OSS, as shown in the following figure.
• No fees are incurred when you upload backup files to OSS.
• Fees are incurred when you store backup files in OSS. For more information, see Pricing.
• If you migrate backup files from OSS to ApsaraDB for RDS over your intranet, no fees are incurred. If you migrate over the Internet, OSS incurs fees for outbound traffic over the Internet. For more information, see Pricing.

Note:
The ApsaraDB for RDS instance and OSS bucket can only communicate over an intranet only when they reside in the same region. Therefore, you must upload the backup file to the OSS bucket that is in the same region as the destination ApsaraDB for RDS instance.

Procedure

1. Back up the on-premises database. The procedure is as follows:
   a. Start the Microsoft SQL Server Management Studio (SSMS) client.
   b. Log on to the database to be migrated.
   c. Execute the following statements to check the recovery model:

```sql
use master;
go
select name, case recovery_model
when 1 then 'FULL'
when 2 then 'BULK_LOGGED'
when 3 then 'SIMPLE' end model from sys.databases
where name not in ('master','tempdb','model','msdb');
```
Check the model value of the on-premises database.

- If the model value is not FULL, perform Step iv.
- If the model value is FULL, perform Step v.

d. Execute the following statements to set the recovery model to FULL:

```
ALTER DATABASE [dbname] SET RECOVERY FULL;
go
ALTER DATABASE [dbname] SET AUTO_CLOSE OFF;
go
```

**Note:**
When the recovery model is set to FULL, more logs are generated. Make sure you have sufficient disk space.

e. Execute the following statements to back up the source database (the backup file is named filename.bak):

```
use master;
go
BACKUP DATABASE [testdbdb] to disk = 'd:\backup\filename.bak' WITH COMPRESSION,INIT;
go
```

f. Execute the following statements to check the integrity of the backup file:

```
USE master
GO
RESTORE FILELISTONLY
    FROM DISK = N'D:\Backup\filename.bak';
```

The displayed result indicates that:

- If a result set is returned, the backup file is valid.
- If an error is returned, the backup file is invalid. Perform Step v to back up again.

g. Execute the following statements to reset the recovery model:

```
ALTER DATABASE [dbname] SET RECOVERY SIMPLE;
go
```

**Note:**
If the recovery model of your database is FULL and Step iv is not performed, skip this step.
2. Upload the backup file of your on-premises database to OSS and obtain the URL of the file. The procedure is as follows:

a. Upload the backup file to OSS.
   - For more information about how to upload a file that is smaller than 5 GB, see [Upload an object](#).
   - For more information about how to upload multiple files or a file that is larger than 5 GB, see [Multipart upload and resumable upload](#). For more information about how to use the graphical management tool ossbrowser, see [Quick start](#).

b. In the left-side navigation pane of the [OSS console](#), select the bucket to which you have uploaded the backup file.

c. Click the **Files** tab.

d. Select the backup file.

e. In the **View Details** page, modify Validity Period. We recommend that you specify the value to 28800 seconds, that is, 8 hours.

**Note:**

The URL of the backup file is required when you restore the file from OSS to ApsaraDB for RDS. The data migration will fail when the validity period of the URL expires.
Therefore, we recommend that you specify the parameter value to the maximum one, namely, 28800 seconds.

f. Click Copy File URL. By default, the URL contains the public endpoint of the file.

<table>
<thead>
<tr>
<th>File Name</th>
<th>ETag</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Validity Period (Seconds)</th>
<th>28800</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>HTTPS</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Download | Open File URL | Copy File URL | Copy File Path

If you migrate data over an intranet, you must replace the public endpoint with the internal endpoint in the URL. The internal endpoint varies according to the network type and region. For more information, see Regions and endpoints.

For example, the URL of the backup file is

http://rdstest-yanhua.oss-cn-shanghai.aliyuncs.com/testmigraterds_20170906143807_FULL.bak?Expires=1514189963&OSSAccessKeyId=TMP.AQGVf994YPfArSpw78uix2rdGBi-dPe_FzQSLwOLP7MVIR-XXXX

You must replace the public endpoint oss-cn-shanghai.aliyuncs.com with the internal endpoint oss-cn-shanghai-internal.aliyuncs.com.
3. Restore data to ApsaraDB for RDS using the backup file in OSS.
   a. Log on to the ApsaraDB for RDS console.
   b. In the upper-left corner of the page, select the region where the destination instance is located.
   c. Click the ID of the instance to go to the Basic Information page.
   d. In the left-side navigation pane, select Databases. The Databases page appears.
   e. Find the destination database and click Migrate Backup Files from OSS in the corresponding Actions column.
   f. In the Import Guide wizard, read the prompt message and click Next. The Upload the backup files to OSS page appears.
   g. Read the prompt message and click Next. The Import data page appears.
   h. Enter the URL of the backup file in the OSS URL of the Backup File field.

Note:
ApsaraDB RDS SQL Server 2008 R2 only supports one-time full backup file migration.

i. Click **OK**.

j. In the left-side navigation pane, select **Database Migration to Cloud**. The migration task list appears.

k. Find the target migration task. If **Task Status** is **Success**, the data is migrated to the database in your ApsaraDB for RDS instance. If the migration task is not in the **Success** state for a long time period, you can click **View File Details** in the corresponding Actions column to view the cause. After the problem is solved, you must perform the preceding restoration procedure again.

**Related API operations**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_50</td>
<td>Restores the backup files from OSS to the RDS instances.</td>
</tr>
<tr>
<td>#unique_51</td>
<td>Opens a database when migrating backup data to RDS.</td>
</tr>
<tr>
<td>#unique_52</td>
<td>Queries the list of migration tasks.</td>
</tr>
<tr>
<td>#unique_53</td>
<td>Queries the details of the backup data files which are uploaded to OSS.</td>
</tr>
</tbody>
</table>
4.1.2 Migrate full backup data to ApsaraDB RDS SQL Server 2012, 2016, or 2017

This topic describes how to migrate full backup files from OSS to ApsaraDB RDS SQL Server.

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

- ApsaraDB RDS SQL Server 2012/2016 Web Edition
- ApsaraDB RDS SQL Server 2012 Enterprise Basic Edition

For more information about how to migrate on-premises databases to ApsaraDB for SQL Server 2008 R2 Enterprise High-availability Edition instances, see Migrate data from an on-premises database to ApsaraDB RDS SQL Server 2008 R2 using full backup files.

Limits

Version of backup files

Migrating data from a backup file of a later version to a database of an earlier version is not supported. For example, you cannot migrate data from SQL Server 2016 to ApsaraDB RDS SQL Server 2012.

Type of backup files

Migrating data by using differential backup files or log files is not supported.

Suffix of backup files

The names of backups files can only end with .bak, .diff, .trn, or .log. If you do not use the script in this topic to generate a backup file, you must use the following suffixes:

- bak: indicates a full backup file.
- diff: indicates a differential backup file.
- trn and log: indicate a transaction log backup.

Name of backup files

The names of backup files cannot contain special characters such as at signs (@) or vertical bars (|). Otherwise, the on-premises database cannot be migrated to the instance.

Precautions

AliyunRDSImportRole
After you have granted the access permissions, the system creates a role named AliyunRDSImportRole in RAM. Do not modify or delete this role. Otherwise, you will not be able to download the backup files when you migrate data to the RDS instance. If you modify or delete this role, you must re-authorize your RDS account.

Name of backup files

The names of backup files cannot contain special characters such as at signs (@) or vertical bars (|).

Backup files in OSS

Do not delete backup files stored in OSS before the migration task is completed.

Prerequisites

Instance storage

Make sure that the ApsaraDB RDS SQL Server instance has enough storage space. If not, you must increase the space before migration.

The names of databases in the ApsaraDB RDS SQL Server instance must be unique.

You do not need to create the destination database in the instance as described in Migrate data from an on-premises database to ApsaraDB RDS SQL Server 2008 R2 using full backup files.

If the instance contains a database that has the same name as the source database, you must back up and delete it from the instance before migration.

Create a privileged account for the destination instance

We recommend that you create a privileged account for the destination instance in the ApsaraDB for RDS console. Skip this step if you already have a privileged account. If the destination instance does not have a privileged account, the backup files in OSS can also be migrated to the instance, but you cannot access the destination database. You must refer to the Common error message at the lower part of the page.

For more information about how to create a privileged account, see Create databases and accounts for an ApsaraDB for RDS instance running SQL Server 2019, 2017, 2016, or 2012.

Create an OSS bucket

Create an OSS bucket that is in the same region as the destination instance. Skip this step if you already have an OSS bucket. The method to create an OSS bucket is as follows:
1. Log on to the **OSS console**.
2. Click the plus sign + to the right of Buckets in the left-side navigation pane.
3. Configure Bucket Name, Region, Storage Class, and Access Control List, and click **OK**. (Make sure the OSS bucket and the ApsaraDB RDS SQL Server instance are in the same region. Otherwise, the backup files cannot be selected.)

Execute the DBCC CHECKDB statement

Execute the DBCC CHECKDB('xxx') statement in the on-premises database to make sure that there are no allocation or consistency errors. If the check succeeds, the following messages are returned:

```
... CHECKDB found 0 allocation errors and 0 consistency errors in database 'xxx'. DBCC execution completed. If DBCC printed error messages, contact your system administrator.
```

If the output contains any error messages, you must fix the on-premises database to prevent migration failure.

**Procedure**

You can migrate your on-premises database to an ApsaraDB RDS SQL Server 2012, 2016, or 2017 instance in the following three steps:

1. Back up the on-premises database
2. Upload the backup file to OSS
3. Create the migration task

**Back up the on-premises database**

Before you perform a full backup for on-premises databases, make sure that you have stopped writing data. The data written during the backup process is not backed up.

You can perform a full backup by using any feasible methods or by using the following method:

1. Download the **backup script** and open it with SQL Server Management Studio (SSMS).
2. Modify the following parameters as needed.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>@backup_databases_list</td>
<td>The databases to be backed up. Separate multiple databases with semicolons (;) or commas (,).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>@backup_type</td>
<td>The type of the backup. Valid values:</td>
</tr>
<tr>
<td></td>
<td>• FULL: full backup</td>
</tr>
<tr>
<td></td>
<td>• DIFF: differential backup</td>
</tr>
<tr>
<td></td>
<td>• LOG: log backup</td>
</tr>
<tr>
<td>@backup_folder</td>
<td>The local directory that stores the backup file. A directory will be</td>
</tr>
<tr>
<td></td>
<td>automatically created if not specified.</td>
</tr>
<tr>
<td>@is_run</td>
<td>Specifies whether to perform a backup. Valid values:</td>
</tr>
<tr>
<td></td>
<td>• 1: performs a backup.</td>
</tr>
<tr>
<td></td>
<td>• 0: only performs a check.</td>
</tr>
</tbody>
</table>

3. Run the backup script.

**Upload the backup file to OSS**

Upload the backup file to your OSS bucket after the on-premises database is backed up.

Method 1: Use ossbrowser

We recommend that you use the ossbrowser tool to upload the backup file to OSS. For more information, see [ossbrowser](#).

Method 2: Use the OSS console

If the backup file is smaller than 5 GB, you can upload the file in the OSS console. For more information, see [Upload an object](#).

Method 3: Call OSS API operations

If you want to complete the migration unattended, you can use the OSS API to perform a multipart or resumable upload. For more information, see [Multipart upload and resumable upload](#).

**Create the migration task**

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

```
2.
Account's all Regions
China (Hangzh...
Asia Pacific

Region

China (Hangzhou)
China (Shanghai)
China (Qingdao)
China (Beijing)
```

3. Click the ID of the instance to go to the **Basic Information** page.

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

5. In the upper-right corner of the page, click **Migrate OSS Backup Data to RDS**.

6. If you are using the feature for the first time, you must perform the following steps to authorize the RDS account to access OSS:
   
   a. Click **Authorize** on the **Import data** step of the Import Guide wizard, as shown in the following figure.

   b. Go to the Cloud Resource Access Authorization page and click **Confirm Authorization Policy** to complete the authorization.

7. On the **Import data** step of the **Import Guide** wizard, configure the following parameters and click **OK** to upload the backup file to OSS.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Name</td>
<td>Enter the name of the destination database in the destination instance.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The name of the database must meet the requirements of SQL Server.</td>
</tr>
<tr>
<td>OSS Bucket</td>
<td>Select the OSS bucket to store the backup file.</td>
</tr>
<tr>
<td>OSS Subfolder Name</td>
<td>Enter the name of the OSS subfolder to store the backup file.</td>
</tr>
</tbody>
</table>
### Parameter | Description
--- | ---
**OSS File** | Enter the prefix of the backup file name and click the search icon. A list of files is displayed. The list contains the name, size, and update time of each file that matches the query. Select the backup file that you need to restore.

### Cloud Migration Plan
- **Immediate Access (Full Backup):** You can use a full backup file to migrate your database to the instance. In this operation, select **Immediate Access**, and the parameter BackupMode is set to FULL, the parameter IsOnlineDB is set to True in the CreateMigrateTask operation.
- **Access Pending (Incremental Backup):** You can use a full backup file and a differential or log file to incrementally migrate your database to the instance. By default, this option is selected, and the parameter BackupMode is set to UPDF, IsOnlineDB is set to False in the CreateMigrateTask operation.

### Consistency Check Mode
- **Asynchronous DBCC:** If the database contains a large volume of data, the DBCC CHECKDB statement will take a long time to execute. The DBCC CHECKDB statement is asynchronously executed after the database is opened to decrease the time spent on opening the database and minimize downtime. If your application requires a short downtime, and the result of DBCC CHECKDB does not affect your business, we recommend that you select Asynchronous DBCC. The parameter CheckDBMode is set to SyncExecuteDBCheck in the CreateMigrateTask operation.
- **Synchronous DBCC:** If you need to execute the DBCC CHECKDB statement to identify consistency errors, we recommend that you select Synchronous DBCC. In this case, the database takes more time to be opened. By default, this option is selected, and the parameter CheckDBMode is set to AsyncExecuteDBCheck in the CreateMigrateTask operation.

You can click Refresh to view the latest status of the migration task. If the migration fails, you can view the task description and troubleshoot errors by referring to the "Common errors" section in this topic.

**View migration records**

You can view migration records over a period of time. The procedure is as follows:
On the Backup and Restoration page, click the **Backup Data Upload History** tab. By default, migration records of the last seven days are displayed. You can also modify the time range to view the records over a specific period of time.

**Common errors**

Each restoration record contains the task description and can be used to troubleshoot error causes. Common error messages are as follows:

The database with the same name already exists in the instance.

- **Error message:** The database (xxx) is already exist on RDS, please backup and drop it, then try again.
- **Cause:** To ensure data security, you cannot migrate an on-premises database to an ApsaraDB RDS SQL Server instance that contains a database that has the same name as the on-premises database.
- **Solution:** If you need to overwrite the database in the instance with the on-premises database, you must back up the database, delete it from the instance, and migrate the on-premises database to the instance.

The file is a differential backup file.

- **Error message:** Backup set (xxx.bak) is a Database Differential backup, we only accept a FULL Backup.
- **Cause:** You uploaded a differential backup file. The full migration only supports full backup files.

The file is a log backup file.

- **Error message:** Backup set (xxx.trn) is a Transaction Log backup, we only accept a FULL Backup.
- **Cause:** You uploaded a log backup file. The full migration only supports full backup files.

Failed to verify the backup file.

- **Error message:** Failed to verify xxx.bak, backup file was corrupted or newer edition than RDS.
- **Cause:** The backup file is damaged or the on-premises database is in a later version than the ApsaraDB RDS SQL Server instance. For example, if you migrate an on-premises database of SQL Server 2016 to an ApsaraDB RDS SQL Server 2012 instance, the error message is displayed.
• Solution: If the backup file is damaged, you must perform a full backup for the on-premises database and migrate again. If the database version is unmatched, you must use an instance of the same or later version. For example, you can migrate an on-premises database of SQL Server 2012 to an ApsaraDB RDS SQL Server 2016 instance.

DBCC CHECKDB fails

• Error message: DBCC checkdb failed
• Cause: Consistency errors and allocation errors occur in your databases.
• Solution:
  1. Execute the following statement in the on-premises database. Your data may be lost when you use this statement to fix errors.

        DBCC CHECKDB (DBName, REPAIR_ALLOW_DATA_LOSS) WITH NO_INFOMSGS, ALL_ERRORMSGS

  2. Perform a full backup for the on-premises database.
  3. Upload the full backup file to the OSS bucket.
  4. Migrate the backup file in the ApsaraDB for RDS console.

The space is insufficient.

• Error message: Not Enough Disk Space for restoring, space left (xxx MB) < needed (xxx MB)
• Cause: The unused space of the instance is insufficient for migrating the backup file to the instance.
• Solution: Increase the instance space.

The space is insufficient.

• Error message: Not Enough Disk Space, space left xxx MB < bak file xxx MB
• Cause: The unused space is smaller than the backup file.
• Solution: Increase the instance space.

No privileged account exists.

• Error message: Your RDS doesn’t have any init account yet, please create one and grant permissions on RDS console to this migrated database (XXX).
• Cause: There is no privileged account in the ApsaraDB RDS SQL Server instance, and the database permissions are not granted to any account. However, the task is successful because the backup file is restored to the destination instance.
• Solution:

  1. Create a privileged account. For more information, see Create databases and accounts for an ApsaraDB for RDS instance running SQL Server 2019, 2017, 2016, or 2012.

  2. Log on to the destination database with the privileged account and authorize other accounts.

Related API operations

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_55</td>
<td>Restores the backup files from OSS to the RDS instances.</td>
</tr>
<tr>
<td>#unique_56</td>
<td>Opens a database when migrating backup data to RDS.</td>
</tr>
<tr>
<td>#unique_57</td>
<td>Queries the list of migration tasks.</td>
</tr>
<tr>
<td>#unique_58</td>
<td>Queries the details of the backup data files that are uploaded to OSS.</td>
</tr>
</tbody>
</table>

4.1.3 Migrate incremental backup data to ApsaraDB RDS SQL Server 2012, 2016, or 2017

You can migrate incremental backup data to ApsaraDB RDS SQL Server 2012, 2016, or 2017. Your service will be disconnected for a few minutes during the migration process.

Scenarios

You can migrate incremental backup data in the following scenarios:

• You need to physically migrate data to an ApsaraDB RDS SQL Server instance.

Note:

- Physical migration is the migration of backup files. Logical migration is the migration of data by executing DML statements in the ApsaraDB RDS SQL Server instance.
- Physical migration guarantees 100% consistency between the source and destination databases. Logical migration cannot guarantee 100% consistency of database information such as index fragmentation and statistical information.
• You need to use incremental migration for time-sensitive business to limit the disconnection time to a few minutes.

**Note:**

If your business has a data volume of less than 100 GB, and does not provide time-sensitive services, we recommend that you use full backup data migration. This process will disconnect the business for a longer period of time, such as two hours. For more information, see Migrate full backup data to ApsaraDB RDS SQL Server 2012, 2016, or 2017.

This topic describes how to use the full backup file and differential or log files that are stored in your OSS bucket to incrementally migrate your on-premises SQL Server database to a database in an ApsaraDB RDS SQL Server instance.

**Procedure**

The procedure is explained on a timeline basis.

<table>
<thead>
<tr>
<th>Migration phase</th>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full backup and restoration</td>
<td>Step 1: Before 00:00</td>
<td>Complete the following preparatory work:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Execute the DBCC CHECKDB statement.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Shut down the local backup system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Change the recovery model of the on-premises database to full.</td>
</tr>
<tr>
<td></td>
<td>Step 2: 00:01</td>
<td>Perform full backup on the on-premises database.</td>
</tr>
<tr>
<td></td>
<td>Step 3: 02:00</td>
<td>Full backup is completed. Time taken: one hour. Upload the backup file to the OSS bucket.</td>
</tr>
<tr>
<td></td>
<td>Step 4: 03:00</td>
<td>The backup file is uploaded. Time taken: one hour. Restore data from the backup file to the RDS instance in the ApsaraDB for RDS console.</td>
</tr>
<tr>
<td>Migration phase</td>
<td>Step</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Step 5: 22:00</td>
<td>The backup file is restored. Time taken: 19 hours. Perform incremental log backup and upload the log file to the OSS bucket.</td>
</tr>
<tr>
<td>Incremental backup and restoration</td>
<td>Step 6: 22:20</td>
<td>The log file is backed up and uploaded. Time taken: 20 minutes. Restore incremental data to the RDS instance by using the log file in the ApsaraDB for RDS console.</td>
</tr>
</tbody>
</table>
|                                       | Step 7: 22:30| • The incremental data is restored. Time taken: 10 minutes.  
• Repeat Step 6 and Step 7 to back up and upload log files and restore incremental data to the instance until the last log file is less than 500 MB.  
• Stop writing data to the on-premises database from your on-premises application. Perform incremental log backup and restoration for the last time. |
| Database opening                      | Step 8: 22:34| The last log file is incrementally migrated to the instance. Time taken: four minutes. Prepare to bring the database online.            |
|                                       | Step 9: 22:35| The database comes online. If you choose to execute the DBCC statement asynchronously, the database is opened and can be used in one minute. |
From the preceding procedure, you can see that you do not need to stop your application until the last log file is generated. In this case, you only need to stop your application for five minutes.

**Prerequisites**

- The ApsaraDB RDS SQL Server instance must be one of the following editions:
  - ApsaraDB RDS SQL Server 2012/2016 Web Edition
  - ApsaraDB RDS SQL Server 2012 Enterprise Basic Edition
- Grant access permissions on OSS buckets to your RDS account

  After you have granted the access permissions, the system creates a role named AliyunRDSImportRole in RAM. Do not modify or delete this role. Otherwise, you will not be able to download the backup files when you migrate a database to the RDS instance. If you modify or delete this role, you must re-authorize your RDS account.

- Create an OSS bucket

  Create an OSS bucket that is in the same region as the destination instance. Skip this step if you already have an OSS bucket. For more information about how to create a bucket, see [Create a bucket](#).

- Make sure the database recovery model is full

  If you need to incrementally migrate your database to the RDS instance, the recovery model of the database must be full. If you set the recovery model to simple, the transaction log will not be backed up. Therefore, the migration may take more time if the differential backup file is large.

- Storage requirements for the ApsaraDB RDS SQL Server instance

  Make sure that the ApsaraDB RDS SQL Server instance has enough storage space. If not, you must increase the space before migration.

- The names of databases in the ApsaraDB RDS SQL Server instance must be unique

  If the instance contains a database that has the same name as the source database, you must back up and delete it from the instance before migration.

- Create a privileged account for the ApsaraDB RDS SQL Server instance

  Create a privileged account for the destination instance in the ApsaraDB for RDS console. Skip this step if you already have a privileged account.
• Shut down the local backup system

Shut down the backup system of the local environment to ensure the success of the migration. Otherwise, the migration may fail because the local backup system automatically backs up the on-premises database.

• Execute the DBCC CHECKDB statement

Execute the DBCC CHECKDB('xxx') statement in the on-premises database to make sure that there are no allocation or consistency errors. If the check succeeds, the following messages are returned:

CHECKDB found 0 allocation errors and 0 consistency errors in database 'xxx'.
DBCC execution completed. If DBCC printed error messages, contact your system administrator.

If the output contains any error messages, you must fix the on-premises database to prevent migration failure.

Limits

• Version of backup files

Migrating data from a backup file of a later version to a database of an earlier version is not supported. For example, you cannot migrate from SQL Server 2016 to ApsaraDB RDS SQL Server 2012.

• Suffix of backup files

The names of backups files can only end with .bak, .diff, .trn, or .log. If you do not use the script in this topic to generate a backup file, you must use the following suffixes:

- bak: indicates a full backup file.
- diff: indicates a differential backup file.
- trn and log: indicate a transaction log backup.

• Name of backup files

The names of backup files cannot contain special characters such as at signs (@) or vertical bars (|). Otherwise, the backup data stored in the OSS bucket cannot be migrated to the instance.

Demo

Back up the on-premises database

Note:
Before you make a full backup of the on-premises database, make sure to shut down the backup system for the local environment.

1. Download the backup script and open it with SQL Server Management Studio (SSMS).

2. Modify the following parameters as needed.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>@backup_databases_list</td>
<td>The databases to be backed up. Separate multiple databases with semicolons (;) or commas (,)</td>
</tr>
<tr>
<td>@backup_type</td>
<td>The type of the backup. Valid values:</td>
</tr>
<tr>
<td></td>
<td>• FULL: full backup</td>
</tr>
<tr>
<td></td>
<td>• DIFF: differential backup</td>
</tr>
<tr>
<td></td>
<td>• LOG: log backup</td>
</tr>
<tr>
<td>@backup_folder</td>
<td>The local directory that stores the backup file. A directory will be automatically created if not specified.</td>
</tr>
<tr>
<td>@is_run</td>
<td>Specifies whether to perform a backup. Valid values:</td>
</tr>
<tr>
<td></td>
<td>• 1: performs a backup.</td>
</tr>
<tr>
<td></td>
<td>• 0: only performs a check.</td>
</tr>
</tbody>
</table>

3. Run the backup script.

**Upload the backup file to OSS**

Upload the backup file to your OSS bucket after the on-premises database is backed up.

- Method 1: Use ossbrowser

  We recommend that you use the ossbrowser tool to upload the backup file to OSS. For more information, see [ossbrowser](#).

- Method 2: Use the OSS console

  If the backup file is smaller than 5 GB, you can upload the file in the OSS console. For more information, see [Upload an object](#).

- Method 3: Call OSS API operations

  If you want to complete the migration unattended, you can use the OSS API to perform a multipart or resumable upload. For more information, see [Multipart upload and resumable upload](#).
Create the migration task

1. Log on to the ApsaraDB for RDS console.
2. In the upper-left corner of the page, select the region where the destination instance is located.
3. Click the ID of the instance to go to the Basic Information page.
4. In the left-side navigation pane, click Backup and Restoration.
5. In the upper-right corner of the page, click Migrate OSS Backup Data to RDS.
6. If you are using the feature for the first time, you must perform the following steps to authorize the RDS account to access OSS:
   a. Click Authorize on the Import data step of the Import Guide wizard, as shown in the following figure.
   b. Go to the Cloud Resource Access Authorization page and click Confirm Authorization Policy to complete the authorization.
7. On the **Import data** step of the **Import Guide** wizard, configure the following parameters and click **OK** to upload the backup file to OSS.

![Import Guide](image)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Name</td>
<td>Enter the name of the destination database in the destination instance.</td>
</tr>
<tr>
<td>Note:</td>
<td>The name of the database must meet the requirements of SQL Server.</td>
</tr>
<tr>
<td>OSS Bucket</td>
<td>Select the OSS bucket to store the backup file.</td>
</tr>
<tr>
<td>OSS Subfolder Name</td>
<td>Enter the name of the OSS subfolder to store the backup file.</td>
</tr>
<tr>
<td>OSS File</td>
<td>Enter the prefix of the backup file name and click the search icon. A list of files is displayed. The list contains the name, size, and update time of each file that matches the query. Select the backup file that you need to restore.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Cloud Migration Plan            | • Immediate Access (Full Backup): You can use a full backup file to migrate your database to the instance. Select **Immediate Access (Full Backup)**.  
• Access Pending (Incremental Backup): You can use a full backup file and a differential or log file to incrementally migrate your database to the instance.  |
| Consistency Check Mode          | • Asynchronous DBCC: If the database contains a large volume of data, the DBCC CHECKDB statement will take a long time to execute. The DBCC CHECKDB statement is asynchronously executed after the database is opened to decrease the time spent on opening the database and minimize downtime. If your application requires a short downtime, and the result of DBCC CHECKDB does not affect your business, we recommend that you select Asynchronous DBCC.  
• Synchronous DBCC: If you need to execute the DBCC CHECKDB statement to identify consistency errors, we recommend that you select Synchronous DBCC. In this case, the database takes more time to be opened.  |

You can click Refresh to view the latest status of the migration task. If the migration fails, you can view the task description and troubleshoot errors by referring to the "Common errors" section in this topic.

**Import differential or log files**

After the full backup file of the on-premises database is migrated to the instance, you need to migrate data from the differential or log files. The procedure is as follows.

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

3. Click the ID of the instance to go to the Basic Information page.

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

5. In the upper-right corner of the page, click Migrate OSS Backup Data to RDS.

Find the database that you want to import incremental data to, and click Upload Incremental Files next to the database. The Upload Incremental Files dialog box appears, as shown in the following figure.

6. Configure the parameters and click OK to import the differential or log file.

If you have multiple log files, you can use the same method to import the log files one by one.

When you upload incremental files, ensure that the last file is not larger than 500 MB to reduce the time of incremental migration. You can click Refresh to view the latest status of the migration task.

**Note:**
Before the last log file is generated, you must stop writing data to the on-premises database to ensure the data consistency between the on-premises database and the ApsaraDB RDS SQL Server database.

**Open the database**

After backup files are migrated, the ApsaraDB RDS SQL Server database is in the In Recovery or Restoring state. If your instance is of the High-availability Edition, it is in the In Recovery state. If your instance is of the Basic Edition, it is in the Restoring state. Read and write operations cannot be performed on the database in either state. Perform the following steps to open the database:
1. Log on to the ApsaraDB for RDS console.

2. Select the region where the destination instance is located and click the ID of the destination instance to go to the Basic Information page.

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

4. In the upper-right corner of the page, click Migrate OSS Backup Data to RDS.

5. Find the database that you need to restore backup files to, and click Open Database to the right of the database.

6. In the Open Database dialog box that appears, select a consistency check mode. There are two ways to perform a database consistency check:

   - Asynchronous DBCC: The DBCC CHECKDB statement is asynchronously executed after the database is opened. If the database contains a large volume of data, the DBCC CHECKDB statement will take a long time to execute. Asynchronous DBCC decreases the time spent on opening the database and minimizes downtime. If your application requires a short downtime, and the result of DBCC CHECKDB does not affect your business, we recommend that you select Asynchronous DBCC.
   
   - Synchronous DBCC: If you need to execute the DBCC CHECKDB statement to identify consistency errors, we recommend that you choose Synchronous DBCC.

View migration records

You can view migration records over a period of time. The procedure is as follows:

On the Backup and Restoration page, click the Backup Data Upload History tab. By default, migration records of the past week are displayed. You can also modify the time range to view the records over a specific period of time.

View file details of a migration task

If you need to view the details of all the backup files for a migration task, you can perform the following steps:

On the Backup and Restoration page, click the Backup Data Upload History tab. Click View File Details to the right of the migration task. The View File Details message appears, and displays details of all backup files related to the task.

Common errors

For more information about common errors that may occur during the full backup migration, see Migrate full backup data to ApsaraDB RDS SQL Server 2012, 2016, or 2017. The following errors may occur during incremental migration.
Failed to open the database

Error message:

Failed to open database xxx.

Cause: Some advanced features enabled by the on-premises database are migrated to the ApsaraDB RDS SQL Server database. If your ApsaraDB RDS SQL Server instance does not support these features, the database fails to be opened.

For example, if your on-premises database of the SQL Server Enterprise Edition enables the Data Compression or Partition feature, and you migrate the database to the database of the ApsaraDB RDS SQL Server Web Edition, the error message is displayed.

You can use the following methods to solve the problem:

- Disable the advanced features on the on-premises SQL Server database, back up the data again, and migrate the data by using OSS.
- Purchase an ApsaraDB RDS SQL Server instance that is of the same edition as the on-premises database. For example, if the on-premises database is of the SQL Server 2012 Enterprise Edition, you must purchase an instance of the ApsaraDB RDS SQL Server Enterprise Basic or High-availability Edition.

The log sequence numbers (LSN) in the database backup chain are not in sequence

Error message:

The log in this backup set begins at LSN XXX, which is too recent to apply to the database.

RESTORE LOG is terminating abnormally.

Cause: In SQL Server databases, differential or log files must be restored in order of the LSN sequence. Otherwise, the error message is displayed.

Solution: Restore the differential or log file that has the proper LSN. You can restore the files based on the backup time.

Asynchronous DBCC CHECKDB succeeds

Message:

Success to DBCC checkdb asynchronously.

Description: The DBCC CHECKDB statement consumes a large amount of resources and time. Therefore, you can perform the consistency check by executing the statement asynchronously to improve the efficiency of incremental migration. If this message is displayed, it
indicates that there is no consistency error in your databases. The opposite error message is described in the following section.

Asynchronous DBCC CHECKDB fails

Error message:

```sql
asynchronously DBCC checkdb failed: CHECKDB found 0 allocation errors and 2 consistency errors in table 'XXX' (object ID XXX).
```

Cause: Consistency errors occur in your databases.

You can use the following methods to solve the problem:

• Execute the following statement in the ApsaraDB RDS SQL Server database:

```
DBCC CHECKDB (DBName,REPAIR_ALLOW_DATA_LOSS)
```

**Note:**

Your data may be lost when you use this statement to fix errors.

• 1. Execute the following statement in the on-premises database:

```
DBCC CHECKDB (DBName,REPAIR_ALLOW_DATA_LOSS)
```

2. Back up the on-premises database again.

3. Delete the corresponding database from the ApsaraDB RDS SQL Server instance.

4. Incrementally migrate the on-premises database to the instance again.

The file types are unmatched

Error message:

```sql
Backup set (xxx) is a Database FULL backup, we only accept transaction log or differential backup.
```

Cause: After full migration is finished, you can only upload differential or log files. If you upload a full backup file, the error message is displayed.

Solution: You must upload a differential or log file.

The number of migrated database reaches the limit
Error message:

The database (xxx) migration failed due to databases count limitation.

Cause: You can only migrate 50 databases to an ApsaraDB RDS SQL Server High-availability or Cluster Edition instance. If the limit is exceeded, the error message is displayed. The limit for ApsaraDB RDS SQL Server Basic Edition instances is 100. There is no limit for ApsaraDB RDS SQL Server 2008 R2 instances.

Solution: You can migrate the database to another instance or delete unnecessary databases from the current instance.

Note: Each database in an ApsaraDB RDS SQL Server High-availability or Cluster Edition instance consumes three processes. If there are multiple databases in an instance, the instance will consume a large amount of connection processes. Therefore, the instance becomes unstable because it may fail to connect to resources that are stored in Service Worker. To ensure stability and efficiency, the maximum number of databases in an ApsaraDB RDS SQL Server High-availability or Cluster Edition instance is limited to 50.

Related API operations

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_55</td>
<td>Restores backup files from OSS to the RDS instances.</td>
</tr>
<tr>
<td>#unique_56</td>
<td>Opens a database when migrating backup data to RDS.</td>
</tr>
<tr>
<td>#unique_57</td>
<td>Queries the list of migration tasks.</td>
</tr>
<tr>
<td>#unique_58</td>
<td>Queries the details of the backup data files that are uploaded to OSS.</td>
</tr>
</tbody>
</table>

4.1.4 Migrate data from all SQL Server databases in an instance to ApsaraDB RDS SQL Server

This topic describes how to migrate data from all on-premises or ECS-based user-created SQL Server databases to ApsaraDB RDS SQL Server by using full backup files.

Scenarios

ApsaraDB RDS SQL Server has released the following OSS-based methods to migrate data to ApsaraDB for RDS: Migrate data from an on-premises database to ApsaraDB RDS SQL Server 2008 R2 using full backup files, Migrate full backup data to ApsaraDB RDS SQL Server 2012, 2016, or 2017, and Migrate incremental backup data to ApsaraDB RDS SQL Server
2012, 2016, or 2017. These methods can be used to migrate data from a single on-premises or ECS-based database to ApsaraDB for RDS.

However, these methods are not suitable for the scenarios where dozens or hundreds of SQL Server databases are migrated from an on-premises or ECS-based SQL Server instance. To solve this problem, ApsaraDB RDS SQL Server provides an instance-based data migration feature to allow you to migrate a large number of databases to ApsaraDB for RDS. You only need to upload the full backup files of all databases to a folder in the OSS bucket, and then run the Python script to migrate data from the instance to ApsaraDB for RDS.

Prerequisites

- Only full backup files can be used to migrate instance-based data to ApsaraDB for RDS. This feature allows you to migrate data from all databases in an instance to ApsaraDB for RDS only by using full migration files, but not incremental backup files.

- The ApsaraDB RDS SQL Server instance must be one of the following editions:
  - ApsaraDB RDS SQL Server 2008 R2
  - ApsaraDB RDS SQL Server 2012/2016 Web Edition
  - ApsaraDB RDS SQL Server 2012 Enterprise Basic Edition
  - ApsaraDB RDS SQL Server 2017 Enterprise Cluster Edition

- The OSS bucket is located in the same region as the ApsaraDB RDS SQL Server instance. Make sure that the OSS bucket is located in the same region as the ApsaraDB RDS SQL Server instance, so that you can download full backup files smoothly.

- Both Alibaba Cloud accounts and RAM users can be used to migrate instance-based data to ApsaraDB for RDS, but only Alibaba Cloud accounts have permissions to access
OSS and RDS. To migrate data to ApsaraDB for RDS by using a RAM user, perform the following operations to authorize the RAM user:

1. Choose **Products > Monitor and Management > Resource Access Management** to log on to the RAM console.

2. In the left-side navigation pane, click **Users**. In the user list, find the RAM user you want to authorize, and click **Authorize** in the Actions column. The **Edit User-Level Authorization** dialog box appears.

3. Authorize the account the **AliyunOSSFullAccess**, **AliyunOSSReadOnlyAccess**, **AliyunRDSFullAccess**, and **AliyunRDSReadOnlyAccess** permissions, and click **OK**, as shown in the following figure.

   - Database backup files must meet the naming conventions.

   To ensure that the full backup files of all on-premises or ECS-based databases are used to migrate data to ApsaraDB for RDS, you must name the backup files by following the naming conventions. Each database name can then be obtained from the backup file names.

   Each database backup file must be named in the `databaseName_backupType_backupTime.bak` format, including the database name, backup type, and backup time.

   For example, `TestDb_FULL_20180518153544.bak` indicates the following information:
   - The database name is TestDb.
   - The database backup type is FULL.
   - The backup time is 20180518153544.
   - The backup file is suffixed with bak.

   We recommend that you use the database backup script provided by Alibaba Cloud. For more information, see "Back up all on-premises or ECS-based databases" in the "Preparations" section.

**Preparations**

Make the following preparations only once, including Python installation, dependency package installation, and OSS bucket creation.

1. Install Python.

   Install a version of Python, 2.7.10 recommended, by following the wizard on the [Python official website](https://www.python.org).
2. Check the Python version.

- **Windows OS:**
  
  Run the `C:\>c:\Python27\python.exe -V` command to check the Python version. If Python 2.7.10 is displayed, you have installed Python 2.7.10.

  If it is prompted that the preceding command is not an internal or external command, add the Python installation path and the pip command path to the Path environment variable, as shown in the following figure.

- **Mac, Linux, or Unix OS:**

  Run the `$ python -V` command to check the Python version. If Python 2.7.10 is displayed, you have installed Python 2.7.10.

3. Install the SDK dependency package.

Use either of the following methods to install the SDK dependency package:

- Run the pip command.

  ```bash
  pip install aliyun-python-sdk-rds
  pip install oss2
  ```

- Use the source code.

  # Use the git clone command to clone the API repository.
  git clone https://github.com/aliyun/aliyun-openapi-python-sdk.git
  # Install the SDK core repository of Alibaba Cloud.
  cd aliyun-python-sdk-core
  python setup.py install
  # Install the RDS SDK of Alibaba Cloud.
  cd aliyun-python-sdk-rds
  python setup.py install
  # Use the git clone command to clone the OSS SDK.
  git clone https://github.com/aliyun/aliyun-oss-python-sdk.git
  cd aliyun-oss-python-sdk
  # Install oss2.
  python setup.py install

4. Create an OSS bucket. Make sure that the OSS bucket is in the same region as the destination RDS instance. Skip this step if a bucket already exists.

a. Log on to the OSS console.

b. Click the plus sign + to the right of Buckets in the left-side navigation pane.

c. Configure Bucket Name, Region, Storage Class, and Access Control List, and click **OK**, as shown in the following figure.
5. Create a database for the destination instance.

- If your destination instance is ApsaraDB RDS SQL Server 2012 or later versions, skip this step.
- If your destination instance is ApsaraDB RDS SQL Server 2008 R2, create all databases with the same names in the destination instance through the RDS console, and leave the databases empty. For more information about how to create databases for ApsaraDB RDS SQL Server 2008 R2 instances, see Create databases and accounts for an RDS instance in SQL Server 2008 R2.

6. Back up all on-premises or ECS-based databases.

Before you perform a full backup for on-premises or ECS-based databases, make sure that you have stopped writing data. The data written during the backup process is not backed up.

Under the precondition that database backup files meet the naming conventions, you can perform a full backup by using any feasible methods. We recommend that you use the following method to perform a full backup:

a. Download the backup script and open it with SQL Server Management Studio (SSMS).

b. Modify the following parameters as needed.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>@backup_databases_list</td>
<td>The databases to be backed up. Separate multiple databases with semicolons (;) or commas (,).</td>
</tr>
<tr>
<td>@backup_type</td>
<td>The type of the backup. Valid values:</td>
</tr>
<tr>
<td></td>
<td>• FULL: full backup</td>
</tr>
<tr>
<td></td>
<td>• DIFF: differential backup</td>
</tr>
<tr>
<td></td>
<td>• LOG: log backup</td>
</tr>
<tr>
<td>@backup_folder</td>
<td>The local directory that stores the backup file. A directory will be automatically created if not specified.</td>
</tr>
<tr>
<td>@is_run</td>
<td>Specifies whether to perform a backup. Valid values:</td>
</tr>
<tr>
<td></td>
<td>• 1: performs a backup.</td>
</tr>
<tr>
<td></td>
<td>• 0: only performs a check.</td>
</tr>
</tbody>
</table>

c. Run the backup script.
7. Upload backup files to OSS.

Assume that your database is located in an on-premises or ECS-based user-created SQL Server instance, and the ECS instance resides in a VPC. The upload speed in a VPC can reach a maximum of 100 MB/s. To upload backup files to OSS through the internal network in a more efficient way, use the OSS VPC endpoint when you log on to ossbrowser.

a. Obtain the OSS VPC endpoint, as shown in the following figure.

b. Specify parameters in ossbrowser as follows.

When you use the AccessKey-based method to log on to ossbrowser, select Custom for Endpoint and enter the VPC endpoint such as http://oss-cn-beijing-internal.aliyuncs.com. Enter the AccessKey ID and AccessKey secret.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| Use ossbrowser to upload backup files | • We recommend that you use ossbrowser to upload backup files to OSS.  
|                                      | • For more information, see ossbrowser.                                     |
| Use the OSS console to upload backup files | • If the size of backup files is smaller than 5 GB, you can upload the files in the OSS console.  
|                                      | • For more information, see Upload an object.                               |
| Call OSS API operations to upload backup files | • If you want to complete the migration unattended, you can use the OSS API to perform a multipart or resumable upload.  
|                                      | • For more information, see Multipart upload and resumable upload.          |

Demo

Procedure

1. Download the Python script.

Download the instance-based migration script RDSSQLCreateMigrateTasksBatchly.py.
2. Run the `python ~/Downloads/RDSSQLCreateMigrateTasksBatchly.py -h` command to view the help information.

The following information is displayed:

```
~/Downloads/RDSSQLCreateMigrateTasksBatchly.py -k <access_key_id> -s <access_key_secret> -i <rds_instance_id> -e <oss_endpoint> -b <oss_bucket> -d <directory>
```

Parameter description:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access_key_id</td>
<td>The AccessKey ID of the Alibaba Cloud account.</td>
</tr>
<tr>
<td>access_key_secret</td>
<td>The AccessKey secret of the Alibaba Cloud account.</td>
</tr>
<tr>
<td>rds_instance_id</td>
<td>The ID of the destination ApsaraDB RDS SQL Server instance.</td>
</tr>
<tr>
<td>oss_endpoint</td>
<td>The endpoint of the OSS bucket where backup files are located. For more information about how to obtain the endpoint, see the screenshot in &quot;OSS endpoint errors&quot; in the &quot;Common errors&quot; section.</td>
</tr>
<tr>
<td>oss_bucket</td>
<td>The OSS bucket where backup files are located.</td>
</tr>
<tr>
<td>directory</td>
<td>The directory of backup files in the OSS bucket. If it is the root directory, enter a forward slash (/).</td>
</tr>
</tbody>
</table>
3. Run the instance-based migration script to complete the migration task.

Example 1: Migrate all backup files from the Migration/OPENAPIDemo directory in the OSS bucket named atp-test-on-ecs to the ApsaraDB RDS SQL Server instance named rm-2zesz5774ud8s71i5.

```python
python ~/Downloads/RDSSQLCreateMigrateTasksBatchly.py -k LTAIQazXKPRwwErT -s BMkiUhroubQOLpOMqfA091klqpp4G2k -i rm-2zesz5774ud8s71i5 -e oss-cn-beijing.aliyuncs.com -b atp-test-on-ecs -d Migration/OPENAPIDemo
```

Example 2: Migrate all backup files from the root directory in the OSS bucket named atp-test-on-ecs to the ApsaraDB RDS SQL Server instance named rm-2zesz5774ud8s71i5.

```python
python ~/Downloads/RDSSQLCreateMigrateTasksBatchly.py -k LTAIQazXKPRwwErT -s BMkiUhroubQOLpOMqfA091klqpp4G2k -i rm-2zesz5774ud8s71i5 -e oss-cn-beijing.aliyuncs.com -b atp-test-on-ecs -d /
```

4. View the migration task in the RDS console.

Perform the following operations to view all the submitted migration tasks in the RDS console:

ApsaraDB RDS SQL Server 2008 R2

a. Log on to the ApsaraDB for RDS console.

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

c. Click the ID of the destination instance.

d. In the left-side navigation pane, click Database Migration to Cloud.

e. On the Database Migration to Cloud page, view all the submitted migration tasks.

You can also click Refresh in the upper-right corner of the page to view the latest statuses of migration tasks, as shown in the following figure.

ApsaraDB RDS SQL Server 2012 and later versions
Perform the following operations to view backup migration records within a period of time:

In the left-side navigation pane, click **Backup and Restoration**. Click the Backup Data Upload History tab to view the migration records of the last seven days. You can specify the time range to view the records over a specific period of time.

**Common errors**

**AccessKey ID errors**

**Error information**

HTTP Status: 404 Error:InvalidAccessKeyId.NotFound Specified access key is not found. RequestID: XXXXXXXXXXXXXXXX

**Cause analysis**

The AccessKey ID used to call the API is incorrect.

**Solution**

Use the correct AccessKey ID. You can find your AccessKey ID and AccessKey secret as follows:

1. Log on to the Alibaba Cloud console.
2. Move the pointer over your profile picture in the upper-right corner. A page shown in the following figure appears.
3. Click AccessKey to view your AccessKey ID and AccessKey secret.

**AccessKey secret errors**

**Error information**

HTTP Status: 400 Error:IncompleteSignature The request signature does not conform to Aliyun standards. server string to sign is:......

**Cause analysis**

The AccessKey secret used to call the API is incorrect.

**Solution**

The solution is the same as that for the preceding AccessKey ID errors.

**Failure to support the RDS engine**
ApsaraDB for RDS

RDS SQL Server Database / 4 Data migration

Error information

RDS engine doesn't support, this is only for RDS SQL Server engine.

Cause analysis

The instance-based database migration feature does not support other RDS engines than SQL Server.

Non-existent instance ID

Error information

Couldn't find specify RDS [XXX].

Cause analysis

The ApsaraDB RDS SQL Server instance ID does not exist.

Solution

Check whether the specified ApsaraDB RDS SQL Server instance ID is correct. If not, enter the correct instance ID.

OSS endpoint errors

Error information

{'status': -2, 'request-id': '', 'details': "RequestError: HTTPConnectionPool(host='xxxxxxxxxxxxxxx', port=80): Max retries exceeded with url: /? bucketInfo= (Caused by NewConnectionError('<urllib3.connection.HTTPConnection object at 0x10e996490>: Failed to establish a new connection: [Errno 8] nodename nor servname provided, or not known',))")

Cause analysis

The OSS endpoint is incorrect.

Solution

Make sure that you have entered a correct OSS endpoint. You can view the OSS endpoint as follows:

Log on to the OSS console. On the Overview tab of an OSS bucket, check the endpoint of the OSS bucket. You can use an external endpoint, as shown in the following figure.
Error information

```json
{"status": 404, 'request-id': 'xxxxxxxxx', 'details': {'HostId': 'xxxxxxxxx', 'Message': 'The specified bucket does not exist.', 'Code': 'NoSuchBucket', 'RequestId': 'xxxxxxxxx', 'BucketName': 'aaaatp-test-on-ecs'}}
```

Cause analysis

The OSS bucket used to call the API does not exist.

Solution

Enter the correct OSS bucket name.

Non-existent folder or backup file in the OSS bucket

Error information

```
There is no backup file on OSS Bucket [xxxxxx] under [xxxxxxxxxx] folder, check please.
```

Cause analysis

The corresponding folder does not exist in the OSS bucket, or the folder does not contain SQL Server backup files that meet the conditions.

Solution

Check whether the folder exists in the OSS bucket and whether the folder contains the backup files that meet the conditions.

Invalid backup file names

Error information

```
Warning!!!!!, [autotest_2005_ent_broken_full_dbcc_failed.bak] is not backup file, filtered.
```

Cause analysis

The backup file name that contains the database name fails to meet the naming conventions. For more information, see the naming conventions for backup file names.

Solution

Name the backup files based on the naming conventions.

API error responses
Error information


Cause analysis

An error occurs when the API is called.

Solution

Analyze the specific error cause by checking the error information following HTTP Status.

The following table describes the related error information.

<table>
<thead>
<tr>
<th>HTTP status code</th>
<th>Error code</th>
<th>Error message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>403</td>
<td>InvalidDBName</td>
<td>The specified database name is not allowed.</td>
<td>The error message returned because the specified database name is invalid. For example, an existing database name cannot be used.</td>
</tr>
<tr>
<td>403</td>
<td>IncorrectDBInstanceState</td>
<td>Current DB instance state does not support this operation.</td>
<td>The error message returned because the operation is not supported while the database instance is in the current state, such as creating.</td>
</tr>
<tr>
<td>400</td>
<td>IncorrectDBInstanceType</td>
<td>Current DB instance type does not support this operation.</td>
<td>The error message returned because the operation is not supported by other instances than ApsaraDB RDS SQL Server.</td>
</tr>
<tr>
<td>400</td>
<td>IncorrectDBInstanceLockMode</td>
<td>Current DB instance lock mode does not support this operation.</td>
<td>The error message returned because the operation is not supported while the database instance is in the current lock state.</td>
</tr>
<tr>
<td>HTTP status code</td>
<td>Error code</td>
<td>Error message</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 400              | InvalidDBName. NotFound | Specified one or more DB name does not exist or DB status does not support. | The error message returned because the specified database does not exist.  
  • ApsaraDB RDS SQL Server 2008 R2: A database with the same name must be created first.  
  • ApsaraDB RDS SQL Server 2012 and later versions: The specified database does not exist. |
<p>| 400              | IncorrectDBType        | Current DB type does not support this operation.                             | The error message returned because the operation is not supported by the current database engine.                                          |
| 400              | IncorrectDBState       | Current DB state does not support this operation.                             | The error message returned because the operation is not supported while the database is in the current state, such as creating or migrating. |
| 400              | UploadLimitExceeded    | UploadTime sQuotaExceeded: Exceeding the daily upload times of this DB.       | The error message returned because the number of data uploads exceeds 20 for each database per day.                                       |</p>
<table>
<thead>
<tr>
<th>HTTP status code</th>
<th>Error code</th>
<th>Error message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>ConcurrentTaskExceeded</td>
<td>Concurrent task exceeding the allowed amount.</td>
<td>The error message returned because the number of data uploads exceeds 500 for each instance per day.</td>
</tr>
<tr>
<td>400</td>
<td>IncorrectFileExtension</td>
<td>The file extension does not support.</td>
<td>The error message returned because the backup file extension is invalid.</td>
</tr>
<tr>
<td>400</td>
<td>InvalidOssUrl</td>
<td>Specified oss url is not valid.</td>
<td>The error message returned because the specified OSS download URL is invalid.</td>
</tr>
<tr>
<td>400</td>
<td>BakFileSizeExceeded</td>
<td>Exceeding the allowed bak file size.</td>
<td>The error message returned because the size of backup files exceeds 3 TB.</td>
</tr>
<tr>
<td>400</td>
<td>FileSizeExceeded</td>
<td>Exceeding the allowed file size of DB instance.</td>
<td>The error message returned because the size of restored backup files exceeds the available size of the destination instance.</td>
</tr>
</tbody>
</table>

Insufficient permissions for RAM users

Error information

The similar error information is returned:

HTTP Status: 403 Error:Forbidden.RAM The user is not authorized to operate the specified resource, or this operation does not support RAM. RequestID: xxxxx

```
{
'status': 403, 'request-id': 'xxxx', 'details': {
'HostId': 'atp-test-on-ecs.oss-cn-beijing.aliyuncs.com',
'Message': 'The bucket you visit is not belong to you.',
'Code': 'AccessDenied',
'RequestId': 'xxxx'
}}
```

Cause analysis

The RAM user used to migrate databases to ApsaraDB for RDS does not have sufficient OSS or RDS permissions.
Solution

Authorize the RAM user sufficient permissions by following the authorization method.

Related API operations

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_55</td>
<td>Restores the backup files from OSS to the RDS instances.</td>
</tr>
<tr>
<td>#unique_56</td>
<td>Opens a database when migrating backup data to RDS.</td>
</tr>
<tr>
<td>#unique_57</td>
<td>Queries the list of migration tasks.</td>
</tr>
<tr>
<td>#unique_58</td>
<td>Queries the details of the backup data files which are uploaded to OSS.</td>
</tr>
</tbody>
</table>
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 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_19. 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 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 SQL Server instance**

This topic describes how to manually renew an RDS 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 Use by 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 Renew tab, find the target RDS instance and in the Actions column click Renew.

Note:
- If the target RDS instance is on the Nonrenewal 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 tab, you can click Enable Manual Renew in the Actions column 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 SQL Server instance.

5.3 Automatically renew an RDS SQL Server instance

This topic describes how to automatically renew an RDS 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 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.

5. 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** tab, find the target RDS instance and in the **Actions** column click **Edit Auto Renewal**.

5. Select a renewal duration, 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** tab, find the target RDS instance and in the **Actions** column click **Enable Manual Renewal**.

5. Click **OK**.

**APIs**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_20</td>
<td>Used to create an RDS instance.</td>
</tr>
</tbody>
</table>

**Note:**

Automatic renewal is enabled when you create the instance.
<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_67</td>
<td>Used to renew a subscription-based RDS instance.</td>
</tr>
</tbody>
</table>

**Note:** Automatic renewal is enabled after you create the instance.
6 Manage pending events

This topic describes how to manage pending events. When a pending event occurs for an RDS instance, the RDS console prompts you with the relevant information immediately.

You are notified of RDS O&M events (for example, instance migration events and version upgrade events) not only through SMS, voice, email, and in-site email but also in the RDS console. You can view the type, region, process, precautions of an event and the list of involved RDS instances. You can also manually change the scheduled switchover time.

Prerequisites

Pending O&M events exist.

![Note:](image)

In the upper-right corner of the RDS console, you can obtain the notification through *Pending Events*.

Procedure

1. Log on to the [RDS console](#).
2. In the left-side navigation pane or the upper-right corner, click *Pending Events*.

![Note:](image)

If you have scheduled an O&M event, the system displays a message asking you to complete the event as soon as possible.

3. On the *Pending Events* page, select an event type and a region.

![Note:](image)

The notification, including the event process and precautions, varies depending on the event type.
4. View event details in the instance list. If you want to change the scheduled switchover time, select the RDS instance, and click the button for customizing the operation time. In the displayed dialog box, set the operation time and click **OK**.

**Note:**
- The displayed information varies depending on the event type.
- The scheduled switchover time cannot be later than the last operation time.
7 Version upgrade

7.1 Upgrade from Basic Edition to High-availability Edition

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

#unique_71 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_72 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_73.

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 7-1: Upgrade rules

<table>
<thead>
<tr>
<th>Original version or edition</th>
<th>Higher available version or edition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2012 Enterprise Edition (High-availability Edition)</td>
</tr>
<tr>
<td></td>
<td>2012 Enterprise Edition (High-availability Edition)</td>
</tr>
<tr>
<td>Original version or edition</td>
<td>Higher available version or edition</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Upgrade To</strong></td>
<td>Select the target version. The <strong>Edition</strong>, <strong>Storage Type</strong>, and <strong>Instance Type</strong> settings vary depending on the selected target version.</td>
</tr>
<tr>
<td><strong>Edition</strong></td>
<td>Select <strong>High-availability</strong>: The classic high-availability architecture allows your instance to work in primary/secondary mode to achieve balanced performance in all aspects.</td>
</tr>
</tbody>
</table>
| **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_19. |
| **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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |

### Switching Time

**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.

<table>
<thead>
<tr>
<th>Original network type</th>
<th>Change rule</th>
</tr>
</thead>
</table>
| 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. |

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

This topic describes how to upgrade an RDS 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_75. 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_78.

• 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 switchover 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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade To</td>
<td>Select the target version. The Edition, Storage Type, and Type settings vary depending on the selected target version.</td>
</tr>
<tr>
<td>Edition</td>
<td>Select High-availability: The classic HA architecture allows your instance to work in master/slave mode with balanced performance in all aspects.</td>
</tr>
<tr>
<td>Storage Type</td>
<td>Select SSD or ESSD.</td>
</tr>
<tr>
<td>Zone</td>
<td>Select the zone to which you want to migrate your instance. You can choose a multi-zone combination if available.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Type</td>
<td>Each instance type provides a specific number of CPU cores, memory, maximum number of connections, and maximum IOPS. For more information, see #unique_19.</td>
</tr>
</tbody>
</table>
| 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.
<table>
<thead>
<tr>
<th>If the original network type is</th>
<th>Then after the upgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic network</td>
<td>Two connection addresses are available:</td>
</tr>
<tr>
<td></td>
<td>• The original connection address of the classic network still can be used and will not expire.</td>
</tr>
<tr>
<td></td>
<td>• A VPC connection address is generated for the instance based on the VPC that is specified during the upgrade.</td>
</tr>
<tr>
<td>VPC</td>
<td>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.</td>
</tr>
<tr>
<td>Hybrid mode (Classic network and VPC)</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone</td>
<td>Select the zone where you can create a temporary instance.</td>
</tr>
<tr>
<td>Upgrade To Version</td>
<td>Select the target version. The available target versions are as follows:</td>
</tr>
<tr>
<td></td>
<td>• 2016 SE</td>
</tr>
<tr>
<td></td>
<td>• 2016 EE</td>
</tr>
<tr>
<td></td>
<td>• 2012 EE</td>
</tr>
<tr>
<td>VPC</td>
<td>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.</td>
</tr>
<tr>
<td>VSwitch</td>
<td>Select a VSwitch under the specified VPC.</td>
</tr>
</tbody>
</table>

**Note:**
The temporary instance adopts a default instance type and a default storage type.

Create Temporary Instance of Higher Version

Current Instance: rm-bxxxxxxxxx
Current Availability
Zone: China (Hangzhou) Zone F+ Zone G
Zone: China (Hangzhou) Zone H

Upgrade to Version: 2016 SE
Series: High Availability
Network Type: VPC
VPC: vpc-xxxxxxxxxxxx
VSwitch: vsw-xxxxxxxxxxxx

This temporary instance uses the default settings for the instance type and storage type. The lifetime of this temporary instance is 7 days, after which it will be automatically released.

7. Click OK.

Note:
The temporary instance will be automatically released after seven days.

Related API

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UpgradeDBInstanceEngineVersion</td>
<td>Upgrades the database version of an instance.</td>
</tr>
</tbody>
</table>
7.3 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_73.

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

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.
8 Instance

8.1 Create an RDS SQL Server instance

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

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

For information about the pricing of RDS MySQL instances, see #unique_15.

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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• Select the same region as the corresponding ECS instance to avoid incurring charges for Internet traffic usage and guarantee fast access.</td>
</tr>
<tr>
<td></td>
<td>• Check whether the selected region supports your required MySQL version and whether multi-zone support is available.</td>
</tr>
<tr>
<td>Database Engine</td>
<td>Select a DB engine.</td>
</tr>
<tr>
<td></td>
<td>In this example, select SQL Server.</td>
</tr>
<tr>
<td></td>
<td>Note: The available DB engines vary depending on the region you select.</td>
</tr>
<tr>
<td></td>
<td>Note: The available versions vary depending on the region you select.</td>
</tr>
<tr>
<td>Edition</td>
<td>Select an RDS edition. Valid values:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>Note: The available editions vary depending on the DB engine version you select. For information about the RDS editions, see #unique_17.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Storage Type</td>
<td>Select a storage type. Valid values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Local SSD</strong>: An SSD that is located on the same node as the DB engine. Storing data to local SSDs reduces I/O latency.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Standard SSD</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enhanced SSD</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>For more information, see #unique_18.</td>
</tr>
<tr>
<td>Zone</td>
<td>Select a zone.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Multi-zone deployment is more secure because it provides zone-level disaster tolerance.</td>
</tr>
<tr>
<td>Network Type</td>
<td>Select a network type. Valid values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Classic Network</strong>: indicates a traditional network.</td>
</tr>
<tr>
<td></td>
<td>• <strong>VPC</strong> (recommended): short for Virtual Private Cloud. A VPC is an isolated network environment and therefore provides higher security and performance than a classic network.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **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_19. 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. |
| **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 fees 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

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_20</td>
<td>Used to create an RDS instance.</td>
</tr>
</tbody>
</table>

8.2 Restart an RDS SQL Server instance

This topic describes how to restart an RDS 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, click **Restart Instance**.

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

### APIs

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_83</td>
<td>Used to restart an RDS instance.</td>
</tr>
</tbody>
</table>

#### 8.3 Set the maintenance window of an RDS SQL Server instance

This topic describes how to set the maintenance window of an RDS SQL Server instance so that RDS 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 applications to avoid service disruptions.

Procedure

1. Log on to the RDS 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

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_85</td>
<td>Used to change the maintenance window of an RDS instance.</td>
</tr>
</tbody>
</table>

### 8.4 Migrate an RDS SQL Server instance across zones in the same region

This topic describes how to migrate an RDS 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

<table>
<thead>
<tr>
<th>Migration scenario</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migrate an RDS instance from one zone to another</td>
<td>The zone where the RDS instance is located is overloaded or cannot meet the performance requirements of the instance.</td>
</tr>
</tbody>
</table>
### Migration scenario

<table>
<thead>
<tr>
<th>Migration scenario</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migrate an RDS instance from one zone to multiple zones</td>
<td>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.</td>
</tr>
<tr>
<td>Migrate an RDS instance from multiple zones to one zone</td>
<td>This scenario is provided to meet the requirements of specific functions.</td>
</tr>
</tbody>
</table>

### 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**.

![Maintenance Window](image)

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

### APIs

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_87</td>
<td>Used to migrate an RDS instance across zones.</td>
</tr>
</tbody>
</table>

### 8.5 Manually or automatically switch over services between the RDS MySQL master and slave instances

This topic describes how to manually or automatically switch over services between the RDS MySQL master and slave instances. After the switchover, the master instance becomes the slave instance.

**Prerequisites**

The master instance is in the High-availability Edition.

**Note:**

RDS instances in the Basic Edition do not have slave instances, and therefore do not support service switchovers.

**Background information**

- Automatic switchover: the default switchover mode. When the master instance becomes faulty, your RDS services are automatically switched over to the slave instance.
• Manual switchover: You can manually switch over services between the master and slave instances even when the automatic switchover function is enabled.

Note:
In the High-availability edition, an RDS instance (referred to as the master instance) has a slave instance. Data is synchronized in real time between the master and slave instances. You can only access the master instance. The slave instance is used only as a backup and does not provide services. After a service switchover, the master instance is degraded to the slave instance.

Precautions

• Services may be disconnected during a switchover. Make sure that you configure automatic reconnection policies for your applications to avoid loss of services.
• If read-only RDS instances are mounted to your RDS instance, the data in the read-only RDS instances shows a few minutes' delay after a switchover. This is because it takes time to reestablish replication links and synchronize incremental data.

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**.

---

**Temporarily disable automatic switchover**

The automatic switchover function is enabled by default. In such case, services can be automatically switched over to the slave instance if the master instance becomes faulty. You can disable the automatic switchover function in one of the following situations:

- A sales promotion, during which you do not want a switchover to affect service availability.
- An important application upgrade, during which you do not want a switchover to incur any unexpected issues.
- A major event that requires stable system operation, during which you do not want a switchover to affect system stability.

1. Log on to the [ApsaraDB for RDS console](https://console.aliyun.com).
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 Configure Primary/Secondary Switchover.

   **Note:**
   If the Configure Primary/Secondary Switchover button is unavailable, make sure that the RDS instance is in the High-availability Edition.

6. Select Disable Temporarily, set Deadline, and click OK.

   **Note:**
   - When the specified Deadline arrives, the automatic switchover function is restored to enabled for the RDS instance.
• By default, the automatic switchover function is disabled for one day. You can set the Deadline parameter to 23:59:59 seven days later at tops.

After the setting is complete, you can go to the Service Availability page to check the deadline for disabling the automatic switchover function.

### APIs

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SwitchDBInstanceHA</td>
<td>Switches between the master and slave instances.</td>
</tr>
</tbody>
</table>

### Issue: 20200506

129

#### 8.6 Change the network type of an RDS SQL Server instance

This topic describes how to change the network type of an RDS 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 2017/2019 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 Alibaba Cloud CEN tutorials 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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear</td>
<td>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.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Select</td>
<td>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.</td>
</tr>
</tbody>
</table>

Note: Use the preceding connection string to connect to the instance. You need to change the VIP in the connection string to `Intranet Address (Classic Network)`. For more information, see Configure a hybrid access solution to smoothly migrate an RDS instance from the classic network to a VPC. |

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.

![Whitelist Settings](image)

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

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_96</td>
<td>Used to change the network type of an RDS instance.</td>
</tr>
</tbody>
</table>

### 8.7 Release an RDS SQL Server instance

This topic describes how to release an RDS 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**

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeleteDBInstance</td>
<td>Used to release a pay-as-you-go-based RDS instance. (A subscription-based RDS instance cannot be released by calling an API action.)</td>
</tr>
</tbody>
</table>
8.8 Change the configuration of an RDS SQL Server instance

This topic describes how to change the configuration of an RDS 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 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 PPAS instance, you can create read-only instances. For more information, see Introduction to SQL Server read-only instances and Create an RDS SQL Server read-only instance.

<table>
<thead>
<tr>
<th>Configuration item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Some versions can be upgraded to later versions.</td>
</tr>
<tr>
<td>Edition</td>
<td>The Basic Edition can be upgraded to the High-availability Edition.</td>
</tr>
<tr>
<td>CPU and Memory</td>
<td>All SQL Server DB engine versions and editions support the CPU and memory change.</td>
</tr>
<tr>
<td>Capacity</td>
<td>All SQL Server DB engine versions and editions allow you to increase storage capacity.</td>
</tr>
</tbody>
</table>

**Note:**
- You cannot decrease the storage capacity of an RDS instance.
- For information about the capacity range, see #unique_19.
- 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_73.
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_71 (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_72.

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_101

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 SQL Server instance across...
zones in the same region separately. Alternatively, you can change the zone of an RDS 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.

8.9 DBCC features of ApsaraDB RDS SQL Server

ApsaraDB RDS SQL Server 2012 and later versions support some Database consistency checker (DBCC) statements. You can use the sp_rds_dbcc_trace stored procedure to specify the trace flags to be enabled. You can also execute the DBCC tracerestatus(-1) statement to view whether the trace flags are enabled.

Supported trace flags

- 1222
- 1204
- 1117
- 1118
- 1211
- 1224
- 3604

How to use

You can execute the following statements to use the DBCC feature:

```sql
USE master
GO
--database engine edition
SELECT SERVERPROPERTY('edition')
GO
--create database
CREATE DATABASE testdb
GO
DBCC tracerestatus(-1)
```
exec sp_rds_dbcc_trace 1222,1
WAITFOR DELAY '00:00:10'
DBCC tracestatus(-1)
GO

8.10 Reconfigure parameters for an RDS for SQL Server instance

8.10.1 Reconfigure parameters the in the RDS console

This topic describes how to reconfigure parameters and view the parameter reconfiguration history for an RDS 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_106
- #unique_107
- #unique_108
Parameter reference

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

8.10.2 Reconfigure parameters by using SQL commands

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

Note:
This topic is applicable to RDS 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 edition
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
```
8.11 Instance recycle bin

ApsaraDB for RDS instances are locked when they expire or have overdue payments. You can unlock, recreate, or delete instances in the recycle bin.

Renew and unlock an instance

When an ApsaraDB for RDS instance is locked due to expiration or overdue payments, you can go to the recycle bin to renew and unlock the instance.

Instances that have been locked due to expiration or overdue payments are described as follows:

- Subscription instances are locked and cannot be accessed within seven days after expiration.
- Pay-as-you-go instances cannot be accessed from the second to eighth day after your Alibaba Cloud account incurs overdue payments.

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. In the left-side navigation pane, click Locked Instances.
4. Find a locked instance and click Unlock to renew the instance.

The instance is unlocked after renewal.
Recreate an instance

If an ApsaraDB RDS SQL Server 2008 R2 instance is locked due to expiration or overdue payments, the backup is retained for eight days. You can recreate an instance and restore data to the new instance within the eight days. If the instance has been released for more than eight days, the data cannot be restored.

**Note:**
You cannot recreate ApsaraDB RDS SQL Server 2012 or 2016 instances.

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. In the left-side navigation pane, click **Locked Instances**.
4. Find a released instance and click **Recreate Instance**.

   By default, an instance of the same specifications is created in the zone where the original instance is located. You can also select another zone and specifications.

Delete an instance

When an AsapraDB for RDS instance is locked due to expiration or overdue payments, you can delete the instance from the recycle bin.

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. In the left-side navigation pane, click **Locked Instances**.

4. Find the instance and click **Destroy**.
9 Database connection

9.1 Connect to an RDS SQL Server instance

This topic describes how to connect to an RDS 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 Service (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_21.

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.

![SQL Server connection dialog box]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server type</strong></td>
<td>Select <strong>Database Engine</strong>.</td>
</tr>
<tr>
<td><strong>Server name</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

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. |
| Password       | Enter the password of the account of the RDS instance. |
4. Click Connect.

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

This topic describes how to view the internal and public endpoints and ports of an RDS 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.
9.3 Apply for a public endpoint for an RDS SQL Server instance

This topic describes how to apply for a public endpoint for an RDS 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**

<table>
<thead>
<tr>
<th>Endpoint type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal endpoint</td>
<td>The internal endpoint is generated by default. Use the internal endpoint if all of the following conditions are met:</td>
</tr>
<tr>
<td></td>
<td>• Your application is deployed on an ECS instance.</td>
</tr>
<tr>
<td></td>
<td>• The ECS instance is located in the same region as your RDS instance.</td>
</tr>
<tr>
<td></td>
<td>• The ECS instance has the same network type as your RDS instance.</td>
</tr>
<tr>
<td></td>
<td>The internal endpoint is recommended because accessing RDS through the intranet is most secure and delivers optimal performance.</td>
</tr>
<tr>
<td>Public endpoint</td>
<td>You must manually apply for a public endpoint. You can also release it anytime.</td>
</tr>
<tr>
<td></td>
<td>Use the public endpoint if you cannot access RDS through the intranet.</td>
</tr>
<tr>
<td></td>
<td>Specific scenarios are as follows:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• A server or computer outside Alibaba Cloud accesses your RDS instance.</td>
</tr>
</tbody>
</table>

**Note:**

- The public endpoint and traffic are currently free of charge.
- Using the public 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 public endpoint.
Apply for a public 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 public endpoint is generated.

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

- Connection Type: Select Public Endpoint.
The **Public Endpoint** option is available only after you have applied for a public 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.

<table>
<thead>
<tr>
<th>Change Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection Type</strong>: Internal Endpoint</td>
</tr>
<tr>
<td><strong>Endpoint</strong>: rm-1udka9920x4ss6gp9.sqiserver.rds.aliyuncs.com</td>
</tr>
<tr>
<td>Starts with a lower-case letter, consists of 8 to 64 characters, including letters, digits, or hyphen (-).</td>
</tr>
<tr>
<td><strong>Port</strong>: 3433</td>
</tr>
<tr>
<td>Port Range: 1000 to 5999</td>
</tr>
</tbody>
</table>

### APIs

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_113</td>
<td>Used to apply for a public endpoint for an RDS instance.</td>
</tr>
</tbody>
</table>

### 9.4 Use DMS to log on to an ApsaraDB for RDS instance

You can use DMS to log on to an ApsaraDB for RDS instance.

**Precautions**

You can only use an internal endpoint to log on to DMS.

**Procedure**

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

3. Find the instance and click the instance ID.

4. Click **Log On to DB** in the upper-right corner of the page, as shown in the following figure, to go to the Quick Logon page of the DMS console.

5. On the **Quick Logon** page, set the following parameters:
   - The endpoint and port number of the instance in the `<Internal endpoint>:<Internal port number>` format. Example: rm-bpxxxxxxxx.rds.aliyuncs.com:3433. For more
information about how to view the internal endpoint and port number of an instance, see View the internal and public endpoints and ports of an RDS SQL Server instance.

- The account used to connect to the instance.
- The password used to connect to the instance.

6. Click Log On.

**Note:**
If you want the web browser to remember the password, select Remember Password and click Log On.

7. If the system prompts you to add the CIDR block of the DMS server to the ApsaraDB for RDS whitelist, click Specify for All Instances or Specify for Current Instance.

8. Click Log On.

**9.5 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 VSswitch, 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 Alibaba Cloud CEN tutorials 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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear</td>
<td>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.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 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. |

![Database Connection](image)

*Note: Use the preceding connection string to connect to the instance. You need to change the VIP in the connection string.*

![Original classic endpoint](image)

*Intranet Address (Classic Network): [IP Address]*
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.

![VPC Whitelist Settings](image)

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**.

### 9.6 Kill connections of ApsaraDB RDS SQL Server

**Note:**

This topic is applicable only to ApsaraDB RDS SQL Server 2012 and later versions.

Instances of ApsaraDB RDS SQL Server 2012 and later versions have the kill permissions to kill connections. You can only kill connections of your account and cannot kill other connections such as backup connections.

You can execute the following statement to kill a connection: `KILL (SPID)`
10 Read/write splitting

10.1 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.

10.2 Create an RDS SQL Server read-only instance

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

RDS SQL Server Database / 10 Read/write splitting

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**.

![Instance Management Page]

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.

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_33</td>
<td>Used to create an RDS read-only instance.</td>
</tr>
</tbody>
</table>

10.3 Enable cluster management for an RDS SQL Server instance

This topic describes how to enable the cluster management function for an RDS 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 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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Type</strong></td>
<td>The type of the read/write splitting address.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Intranet address</strong></td>
</tr>
<tr>
<td></td>
<td>- If the network type of the master instance is <strong>VPC</strong>, then the network type of the read/write splitting address is also <strong>VPC</strong>.</td>
</tr>
<tr>
<td></td>
<td>- If the network type of the master instance is <strong>Classic Network</strong>, then the network type of the read/write splitting address is also <strong>Classic Network</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Internet Address</strong>: 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.</td>
</tr>
</tbody>
</table>

* The system distributes the weight automatically. The weights of the subsequent new read-only instances will be automatically distributed according to the system weight distribution rules.
* The weight of the instance will be removed when the instance is in the downtime or when its delay times out. After the instance is restored, the weight will be automatically restored.
* The weight of the instance will be automatically removed after the instance is released.
### Read Weight Distribution

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Weight</td>
<td>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.</td>
</tr>
<tr>
<td>Distribution</td>
<td></td>
</tr>
</tbody>
</table>

- **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.
10.4 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**.

* The system distributes the weight automatically. The weights of the subsequent new readonly instances will be automatically distributed according to the system weight distribution rules.
* The weight of the instance will be removed when the instance is in the downtime or when its delay times out. After the instance is restored, the weight will be automatically restored.
* The weight of the instance will be automatically removed after the instance is released.
## 10.5 Disable cluster management for an RDS SQL Server instance

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

### Prerequisites

The cluster management function is enabled. For more information, see [Enable cluster management for an RDS 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.

10.6 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 10-1: Weights for SQL Server read-only instances

<table>
<thead>
<tr>
<th>Specification code</th>
<th>Specification type</th>
<th>Memory</th>
<th>CPU</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>rds.mssql.s2.large</td>
<td>General-purpose instance</td>
<td>4 GB</td>
<td>2</td>
<td>400</td>
</tr>
<tr>
<td>Specification code</td>
<td>Specification type</td>
<td>Memory</td>
<td>CPU</td>
<td>Weight</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------</td>
<td>---------</td>
<td>-----</td>
<td>--------</td>
</tr>
<tr>
<td>rds.mssql.s3.large</td>
<td>General-purpose instance</td>
<td>8 GB</td>
<td>4</td>
<td>800</td>
</tr>
<tr>
<td>rds.mssql.c1.large</td>
<td>General-purpose instance</td>
<td>16 GB</td>
<td>8</td>
<td>1600</td>
</tr>
<tr>
<td>rds.mssql.s2.xlarge</td>
<td>General-purpose instance</td>
<td>8 GB</td>
<td>2</td>
<td>800</td>
</tr>
<tr>
<td>rds.mssql.m1.medium</td>
<td>General-purpose instance</td>
<td>16 GB</td>
<td>4</td>
<td>1600</td>
</tr>
<tr>
<td>rds.mssql.c1.xlarge</td>
<td>General-purpose instance</td>
<td>32 GB</td>
<td>8</td>
<td>3200</td>
</tr>
<tr>
<td>rds.mssql.c2.xlarge</td>
<td>General-purpose instance</td>
<td>64 GB</td>
<td>16</td>
<td>6400</td>
</tr>
</tbody>
</table>
11 Account

11.1 Create an account for an RDS SQL Server instance

This topic provides information about how to create an account for an RDS 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

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

This topic describes how to reset the password of an account for an RDS 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

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_128</td>
<td>Used to reset the password of a database account.</td>
</tr>
</tbody>
</table>

### 11.3 Change the permissions of an account for an RDS SQL Server instance

This topic describes how to change the permissions of a standard account for an RDS 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 Read-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.

11.4 Authorize a service account for an RDS SQL Server instance

This topic describes how to authorize a service account for an RDS 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**.

![Set Expiration Time dialog box](image)

**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.

![Service Account Permissions tab](image)

### 11.5 Delete an account for an RDS SQL Server instance

This topic describes how to delete a standard account for an RDS 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

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_132</td>
<td>Used to delete an account for an RDS instance.</td>
</tr>
</tbody>
</table>

### 11.6 Manage ApsaraDB RDS SQL Server logins

This topic describes how to use SQL statements to create and manage logins in ApsaraDB RDS SQL Server databases.

#### Prerequisites

The instance version must be ApsaraDB RDS SQL Server 2012 or later.

#### Create a login

You can execute the following statement to create a login:

```
CREATE LOGIN Test11 WITH PASSWORD=N'4C9ED138-C8F5-4185-9E7A-8325465CA9B7'
```

The login will be granted server-level and database-level permissions when created. The following message is displayed in the Messages tab.
Modify the login information

You can execute the following statement to modify the login information:

```
ALTER LOGIN Test11 WITH PASSWORD=N'123',CHECK_POLICY=OFF
```

You can only modify the login that you created. Otherwise, the following error message is displayed:

```
Msg 15151, Level 10, State 1, Line 1
Cannot alter the login 'rds_service', because it does not exist or you do not have permission.
```

Delete a login

You can execute the following statement to delete a login:

```
DROP LOGIN Test11
```

Note:

You can only delete the login that you created. Otherwise, an error message is displayed.

11.7 Manage ApsaraDB RDS SQL Server users

This topic describes how to use SQL statements to create and manage users in ApsaraDB RDS SQL Server databases.

Note:
You can create users only in your databases, but not in system databases.

**Prerequisites**

- The instance version must be ApsaraDB RDS SQL Server 2012 or later.
- A database is created. For more information about the statements to create a database, see [Manage databases with SQL statements](#).
- A login is created and logged on to the database where you need to create a user. For more information about the statements to create a login, see [Manage ApsaraDB RDS SQL Server logins](#).

**Create a user**

You can execute the following statements to create a user in the TestDB database:

```sql
USE TestDB
GO
CREATE USER [Test] FOR LOGIN [Test]
```

**Modify the user information**

You can modify user information by executing the following statements. It is the same as in SQL Server.

```sql
USE TestDB
GO
ALTER USER test WITH LOGIN=test
```

**Delete a user**

You can delete a user by executing the following statements. It is the same as in SQL Server.

```sql
USE TestDB
GO
DROP USER test
```
12 Database

12.1 Create a database for an RDS SQL Server instance

This topic provides information about how to create a database for an RDS 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

12.2 Delete a database for an RDS SQL Server instance

This topic describes how to delete a database for an RDS SQL Server instance by using the RDS console or an SQL command.

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 SQL Server instance.
2. Run the following command to delete a database:

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

### APIs

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_139</td>
<td>Used to delete a database for an RDS instance.</td>
</tr>
</tbody>
</table>

### 12.3 Manage databases with SQL statements

This topic describes how to create and manage databases in an ApsaraDB RDS SQL Server instance by using SQL statements.

#### Prerequisites

The instance version must be ApsaraDB RDS SQL Server 2012 or later.

#### Create a database

Execute the following statement to create a database:

```
CREATE DATABASE TestDb
```

**Note:**

A default path is generated when you create a database in ApsaraDB for RDS. Do not specify any file path.

```
CREATE DATABASE TestDb
```

#### Modify a database

You can modify most database attributes. Do not perform the following operations:

- Do not specify an incorrect file path.

For example, specify an incorrect file path by executing the following statement:

```
ALTER DATABASE [TestDb]MODIFY FILE( NAME = N'TestDb', FILENAME = N'E:\KKKK\DDD\DATA\TestDb.mdf' )
```

The system displays the following error messages:

```
Msg 50000, Level 16, State 1, Procedure ******, Line 152
The file path [E:\KKKK\DDD\DATA\TestDb.mdf] is invalid, please specify correct path folder [ E:\mm\gggg\ ].
Msg 3609, Level 16, State 2, Line 2
```
The transaction ended in the trigger. The batch has been aborted.

• Do not specify the recovery model to a model other than FULL.

For example, specify the recovery model to SIMPLE by executing the following statements:

```
ALTER DATABASE [TestDb]
SET RECOVERY SIMPLE
```

The system displays the following error messages:

```
Msg 50000, Level 16, State 1, Procedure ******, Line 46
Login User [Test11] can't change database [TestDb] recovery model.
Msg 3609, Level 16, State 2, Line 2
The transaction ended in the trigger. The batch has been aborted.
```

• Do not set the database status to ONLINE directly when it is in the OFFLINE state.

For example, set the OFFLINE database to ONLINE by executing the following statements:

```
USE [master]
GO
--set offline
--ALTER DATABASE [TestDb]
--SET OFFLINE
--WITH ROLLBACK AFTER 0
ALTER DATABASE [TestDb]
SET ONLINE
```

The system displays the following error messages:

```
Msg 5011, Level 14, State 9, Line 1
User does not have permission to alter database 'TestDb', the database does not exist, or the database is not in a state that allows access checks.
Msg 5069, Level 16, State 1, Line 1
```
ALTER DATABASE statement failed.

If you need to set the database status to ONLINE, you can use the `sp_rds_set_db_online` stored procedure. Execute the following statement:

```
EXEC sp_rds_set_db_online 'db'
```

**Delete a database**

Execute the following statement to delete a database:

```
DROP DATABASE [TestDb]
```

If you have not backed up the database before deleting, the system displays the following error messages:

```
DROP DATABASE [TestDb]
```

-------------------------------------------------------------------------------------------------

Kindly reminder:
your database [TestDb] does not exist any backup set.

-------------------------------------------------------------------------------------------------

Login User [Test11] has dropped database [TestDb].

### 12.4 Database replication

#### 12.4.1 Copy database data between instances

For ApsaraDB RDS SQL Server 2012 and 2016, you can copy database data from one instance to another in the ApsaraDB for RDS console or by using OpenAPI Explorer.

**Prerequisites**

The following conditions must be met:

- The source and destination instances belong to the same Alibaba Cloud account.
- The engine versions of the source and destination instances are the same. Supported versions: ApsaraDB RDS SQL Server 2012 and 2016.
- The source and destination instances are in the same region and can belong to different zones. The network types must be the same.
- The source and destination instances do not have databases whose names are the same.
- The available storage space of the destination instance is larger than the size of the databases to be copied.
Context

ApsaraDB RDS SQL Server completes a full backup of the source instance before it copies data from the source instance to the destination instance. During the data copy process, incremental data of the source instance is not copied to the destination instance.

You can choose to copy a single database or all databases in the source instance. If the copy task fails, no data is transferred to the destination instance. This ensures data consistency.

For more information about related operations, see #unique_142.

Procedure

1. Log on to the ApsaraDB for RDS console.
2. In the upper-left corner of the page, select the region where the source instance is located.
3. Find the instance and click the instance ID.
4. In the left-side navigation pane, click Databases.
5. Click Replicate to Another Instance.

The parameter configurations are as shown in Table 12-1: Parameter configurations.

Table 12-1: Parameter configurations

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Instance Name</td>
<td>The ID of the source instance.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Target Instance Name</strong></td>
<td>The ID of the destination instance. All instances that are in the same region and have the same version as the source instance are displayed. Select a destination instance. You can also search for your destination instance by instance ID or instance name in the search box.</td>
</tr>
</tbody>
</table>
| **Source Databases**  | Specify the databases to be copied to the destination instance. You can click **Add** or **Delete** to select the databases. If you select multiple or all databases, make sure the following conditions are met:  
  • The available storage space of the destination instance is larger than the size of the databases to be copied.  
  • The source and destination instances do not have databases whose names are the same. |

**Note:** If the source and destination instances have databases whose names are the same, these databases are not copied.
### Users and Authorizations

Specify whether to copy users and permissions to the destination instance.

- **Synchronize Database Users and Authorizations**: The users and permissions of the source databases will be copied to the destination instance. The following scenarios exist.
  - If users of the same names already exist in the destination instance, the users are authorized with permissions of the source instance users.
  - If the destination instance does not have the same user as the user to be copied from the source instance, the user is created in the destination instance and authorized with permissions of the source instance user.

- **Replicate Database Only. Do Not Synchronize Users and Authorizations**: The users and permissions of the source databases will not be copied to the destination instance. This is the default option. You can create user accounts and assign permissions for these databases after the copy is complete. For more information, see Create databases and accounts for an ApsaraDB for RDS instance running SQL Server 2019, 2017, 2016, or 2012.

6. After these parameters are configured, click **OK**.

### 12.4.2 Copy a database of ApsaraDB RDS SQL Server 2008 R2

If you need to create a database that is the same as an existing database, you can copy the database. This topic describes how to copy a database to a new database in the ApsaraDB for RDS console.

#### Prerequisites

The instance version is ApsaraDB RDS SQL Server 2008 R2.

**Note:**

You can only execute SQL statements to copy databases of ApsaraDB RDS SQL Server 2012 and later. For more information, see Copy a database of ApsaraDB RDS SQL Server 2012 or later.

#### Precautions

- Only one database can be copied at a time.
- The names of the new database and the existing database must be different.
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 Databases.
5. Click Copy Database.
6. Enter the information of the new database.

- **Specify the new database name:** Enter a Database Name. Your database name can have 2 to 64 characters including the lowercase letters, digits, underscores, or hyphens. It must begin with a letter and end with a letter or a digit.
- **Select the database to copy:** Select the database that you need to copy from existing databases.
- **Whether to retain the accounts of the source database:** Specify whether to retain the account and authorization information of the source database in the new database. By default, the information is retained. You can retain as needed.
- **Description:** You can enter the information of the database for easy task identification. You can enter up to 256 characters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter a Database Name</td>
<td>The database name must be up to 64 characters in length and can contain lowercase letters, digits, underscores (_), and hyphens (-). It must start with a letter and end with a letter or digit.</td>
</tr>
<tr>
<td>Select the Database to Copy</td>
<td>Select the database that you need to copy from existing databases.</td>
</tr>
<tr>
<td>Do You Want to Keep the Account Information from the Source Database</td>
<td>Specify whether to retain the account and authorization information of the source database in the new database. By default, the information is retained. You can retain as needed.</td>
</tr>
<tr>
<td>Description</td>
<td>You can enter the information of the database for easy task identification. You can enter up to 256 characters.</td>
</tr>
</tbody>
</table>

7. Click **OK**.
12.4.3 Copy a database of ApsaraDB RDS SQL Server 2012 or later

To copy a database, you can execute SQL statements and specify the source and destination databases by using the sp_rds_copy_database stored procedure. The time depends on the database size.

**Note:**
For more information, see [Copy a database of ApsaraDB RDS SQL Server 2008 R2](#).

**Prerequisites**

- Before you copy the database, the unused space of the destination instance must be at least 1.3 times the source database.
- The instance version is ApsaraDB RDS SQL Server 2012 or later.

**Procedure**

Execute the following statements to copy the database:

```sql
USE master
GO
--Query database engine edition
SELECT @@Version
GO
--Create database
CREATE DATABASE testdb
GO
EXEC sp_rds_copy_database 'testdb','testdb_copy'
SELECT *
FROM sys.databases
WHERE name IN ('testdb','testdb_copy')
SELECT
    family_guid,database_guid,*
FROM sys.database_recovery_status
WHERE
    DB_NAME(database_id) IN ('testdb','testdb_copy')
```
13 Monitoring and alerts

13.1 View resource and engine monitoring data

This topic describes how to view the resource and engine monitoring data of an RDS 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.

<table>
<thead>
<tr>
<th>Monitoring type</th>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource Monitoring</strong></td>
<td>Disk Space (MB)</td>
<td>The disk space usage of the RDS instance, including:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Instance Size</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data Usage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Log Size</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Temporary File Size</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Other System File Size</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: MByte.</td>
</tr>
<tr>
<td>Monitoring type</td>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>IOPS</strong> (Input/Output Operations per Second)</td>
<td>IOPS</td>
<td>The number of I/O requests per second for the RDS instance. Unit: Number/second.</td>
</tr>
<tr>
<td><strong>Total Connections</strong></td>
<td>Total Connections</td>
<td>The total number of connections to the RDS instance, including the number of active connections and the total number of connections.</td>
</tr>
<tr>
<td><strong>MSSQL Instance CPU Utilization (percentage in the operating system: %)</strong></td>
<td>MSSQL Instance CPU Utilization</td>
<td>The CPU usage of the RDS instance, including the CPU usage for the operating system.</td>
</tr>
<tr>
<td><strong>SQLServer Average Input/Output Traffic (KB/s)</strong></td>
<td>SQLServer Average Input/Output Traffic</td>
<td>The input and output traffic of the RDS instance per second. Unit: KB.</td>
</tr>
<tr>
<td><strong>Enemy Monitoring</strong></td>
<td>Average Transaction Frequency</td>
<td>The number of transactions processed per second.</td>
</tr>
<tr>
<td></td>
<td>Average QPS</td>
<td>The number SQL statements executed per second.</td>
</tr>
<tr>
<td></td>
<td>Buffer Hit Ratio (%)</td>
<td>The read hit ratio of the buffer.</td>
</tr>
<tr>
<td></td>
<td>Page Write Frequency at Check Point</td>
<td>The number of pages that are written at the check point per second in the RDS instance.</td>
</tr>
<tr>
<td></td>
<td>Login Frequency</td>
<td>The number of logons to the RDS instance per second.</td>
</tr>
<tr>
<td></td>
<td>Average Frequency of Whole Table Scans</td>
<td>The number of full table scans performed per second.</td>
</tr>
<tr>
<td></td>
<td>SQL Compilations per Second</td>
<td>The number of SQL statements that are compiled per second in the RDS instance.</td>
</tr>
<tr>
<td></td>
<td>Lock Timeout Times /s</td>
<td>The number of times that the lock times out per second in the RDS instance.</td>
</tr>
<tr>
<td></td>
<td>Deadlock Frequency</td>
<td>The number of times that the RDS instance is locked per second.</td>
</tr>
<tr>
<td></td>
<td>Lock Wait Frequency</td>
<td>The number of times that the RDS instance enters the waiting state after being locked.</td>
</tr>
</tbody>
</table>
13.2 Set the monitoring frequency

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

Background information

RDS 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.
5. Click the Monitoring tab.
6. Click Set Monitoring Frequency.

Note:
For information about the monitoring metrics supported by the instance, see View resource and engine monitoring data.
7. In the **Set Monitoring Frequency** dialog box, select the monitoring frequency and click **OK**.

---

### APIs

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_148</td>
<td>Used to query the monitoring data of an RDS instance.</td>
</tr>
</tbody>
</table>

---

### 13.3 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.

<table>
<thead>
<tr>
<th>Account's all Re...</th>
<th>China (Hangzh...</th>
<th>Europe &amp; Americas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific</td>
<td></td>
<td></td>
</tr>
<tr>
<td>China (Hangzhou)</td>
<td></td>
<td>Germany (Frankfurt)</td>
</tr>
<tr>
<td>China (Shanghai)</td>
<td></td>
<td>UK (London)</td>
</tr>
<tr>
<td>China (Qingdao)</td>
<td></td>
<td>US (Silicon Valley)</td>
</tr>
<tr>
<td>China (Beijing)</td>
<td></td>
<td>US (Virginia)</td>
</tr>
</tbody>
</table>

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.
14 Data security

14.1 Configure a whitelist for an RDS SQL Server instance

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

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_22</td>
<td>Used to view the IP address whitelist of an RDS instance.</td>
</tr>
<tr>
<td>#unique_23</td>
<td>Used to modify the IP address whitelist of an RDS instance.</td>
</tr>
</tbody>
</table>

### 14.2 Configure SSL encryption for an RDS 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.

Configure SSL

Select Protected Address:

1. rm-1ud1nzb778l830y1a.mysql.rds.aliyuncs.com
2. rm-1ud1nzb778l830y1ako.mysql.rds.aliyuncs.com

Note: When the protected address is changed, the certificate automatically updates and your RDS instance is restarted.
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
```
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 MySQL 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.
14.3 Set TDE for an RDS SQL Server instance

This topic describes how to set Transparent Data Encryption (TDE) for an RDS 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_154` 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_154` 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 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.

   ![RDS console region selection](image)

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.

   ![TDE status switch](image)

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**.

![Database TDE Settings](image)

**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.

### 14.4 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 [Connect Kingdee K/3 WISE to ApsaraDB RDS SQL Server](#).

**Prerequisites**

The ApsaraDB for RDS instance must be one of the following editions:
- 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 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</uicontrol>`.
9. Set the parameters listed in the following table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group Name</strong></td>
<td>The group name must be 2 to 32 characters in length and can contain digits, lowercase letters, and underscores (_). It must start with a lowercase letter and end with a lowercase letter or digit.</td>
</tr>
</tbody>
</table>
### ApsaraDB for RDS

RDS SQL Server Database / 14 Data security

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Whitelist</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rule Direction</strong></td>
<td>Select <strong>Inbound</strong>.</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>Select <strong>Allow</strong>.</td>
</tr>
<tr>
<td><strong>Protocol Type</strong></td>
<td>Select <strong>Customized TCP</strong>.</td>
</tr>
<tr>
<td><strong>Port Range</strong></td>
<td>Enter <strong>135</strong>.</td>
</tr>
</tbody>
</table>

**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. |
| **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.

14.5 Configure disk encryption

This topic describes how to configure disk encryption for an ApsaraDB RDS for SQL Server instance equipped with standard or enhanced SSDs. The disk encryption feature provides maximum protection for your data without interruptions to your business or the need to make changes to your application.

Introduction

The disk encryption feature encrypts the entire disks of your RDS instance based on block storage. Your data cannot be cracked even if it is leaked.

Prerequisites

- Your RDS instance is being created. Disk encryption cannot be enabled after your RDS instance is created. For more information, see Create an RDS SQL Server instance.
- The Standard SSD or Enhanced SSD storage type is selected for your RDS instance. For more information, see #unique_18.
- Your RDS instance resides in the China (Shanghai) or China (Hangzhou) region.

Billing

The disk encryption feature is free of charge. You do not need to pay additional fees for the read or write operations you perform on encrypted disks.

Precautions

- The disk encryption feature cannot be disabled after you enable it.
- After you enable disk encryption for your RDS instance, both the snapshots generated by that RDS instance and the new RDS instances created from those snapshots are automatically encrypted.

Procedure

Create an RDS SQL Server instance with the Standard SSD or Enhanced SSD storage type and the Disk Encryption option selected. Then, select a key used for data encryption.

Note:

For more information, see Manage CMKs.
15 Audit

15.1 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**.

### 15.2 Manage logs

This topic describes how to manage the error logs, slow query logs, and primary/secondary instance switching logs of an ApsaraDB for RDS SQL Server instance through the ApsaraDB for RDS console or by using SQL statements. The logs help you locate faults.

*Note:* For more information about how to archive logs, see [Back up the data of an RDS SQL Server instance](#) and [Download the data backup files and log backup files of an RDS SQL Server instance](#).

**View logs through the ApsaraDB for RDS console**

#### Prerequisites

Your RDS instance runs SQL Server 2008 R2.

#### Procedure

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

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

4. In the left-side navigation pane, click Logs.

5. On the Logs page that appears, click the Error Log, Slow Query Log Summary, or Primary/Secondary Instance Switching Log tab, select a time range, and click Search.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error Log</td>
<td>Records database running errors that occurred within the last month.</td>
</tr>
<tr>
<td>Slow Query Log Summary</td>
<td>Provides statistics and analysis reports on SQL statements that each took more than 1 second to run within the last month. You can change this 1-second threshold by reconfiguring the long_query_time parameter.</td>
</tr>
<tr>
<td>Primary/Secondary Instance Switching Log</td>
<td>Records switchovers between the primary and secondary instances triggered within the last month.</td>
</tr>
</tbody>
</table>

**View logs by using SQL statements**

**Prerequisites**

Your RDS instance runs one of the following three SQL Server versions:

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

**Procedure**
If your RDS instance runs SQL Server 2012 or SQL Server 2016, execute the `sp_rds_read_error_logs` stored procedure to read error logs. This stored procedure operates in a way similar to the `sp_readerrorlog` stored procedure.

Example 1:

```sql
EXEC sp_rds_read_error_logs
```

Example 2:

```sql
EXEC sp_rds_read_error_logs 0,1,’error’
```

If your RDS instance runs SQL Server 2017, execute the `sp_readerrorlog` stored procedure to read error logs.

Example:

```sql
EXEC sp_readerrorlog
```

### 15.3 Event history

This topic describes the event history function. You can use this function to view the events, such as instance creation or parameter reconfiguration, that have occurred within a region over a period of time.

**Prerequisites**

This function is available in the following regions: China (Hangzhou), China (Beijing), China (Qingdao), China (Shanghai), China (Shenzhen), and Singapore.

This function will be rolled out in the other regions soon.

**Pricing**

This function is free of charge in the beta test phase. After the beta test ends, you will be notified if this function is charged.

**Scenarios**

You can use this function to:

- Track instance management operations.
- Audit the security of instance-related operations.
- Audit the compliance of cloud service providers' management operations, for example, whether sectors such as finance and governmental affairs are managed in compliance with the specified security standards.
Enable event history

1. Log on to the ApsaraDB for RDS console.

2. In the upper-left corner of the page, select the region to which you want to enable event history.

3. In the left-side navigation pane, click Event History. A message that prompts you to enable the event history feature appears.

4. Click OK.

Event history parameters

Details about historical events are displayed on the Event History page of ApsaraDB for RDS, such as the resource type, resource name, and event type. They are described as follows.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Type</td>
<td>The RDS resource type. The only resource type is <strong>Instance</strong>.</td>
</tr>
<tr>
<td>Resource Name</td>
<td>The RDS resource name. When <strong>Resource Type</strong> is <strong>Instance</strong>, the instance ID is displayed in the <strong>Resource Name</strong> column.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event Type</td>
<td>The type of the event, such as Instance Management, Database Management, Read/Write Splitting, and Network.</td>
</tr>
<tr>
<td>Event Name</td>
<td>The name of the event. For example, if the event type is Instance Management, the event name may be Create Instance, Delete Instance, Change Specifications, or Restart Instance.</td>
</tr>
<tr>
<td>Run At</td>
<td>The time when the event was executed.</td>
</tr>
<tr>
<td>Event Source</td>
<td>The initiator of the event. Valid values:</td>
</tr>
<tr>
<td></td>
<td>• User: uses the console or API operations to initiate actions.</td>
</tr>
<tr>
<td></td>
<td>• System: performs automatic O&amp;M or periodic system tasks.</td>
</tr>
<tr>
<td></td>
<td>• Internal O&amp;M personnel: use the O&amp;M system to initiate actions.</td>
</tr>
<tr>
<td>Cause</td>
<td>The cause of the event. Valid values:</td>
</tr>
<tr>
<td></td>
<td>• Actions initiated in the console or through API operations.</td>
</tr>
<tr>
<td></td>
<td>• System or manual O&amp;M actions.</td>
</tr>
<tr>
<td>Parameters</td>
<td>The request parameters used to initiate actions in the console.</td>
</tr>
</tbody>
</table>

**Note:**

The displayed event history is collected five minutes earlier.
16 Backup

16.1 Back up the data of an RDS SQL Server instance

This topic describes how to back up the data of an RDS 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 SQL Server instance.
- For information about the billing method and billable items, see #unique_15.
- For information about the pricing of backup space, see ApsaraDB RDS 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

<table>
<thead>
<tr>
<th>DB engine</th>
<th>Data backup</th>
<th>Log backup</th>
</tr>
</thead>
</table>
| 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. |

**Set a backup policy for automatic backup**

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

**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.
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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Retention Period</td>
<td>The data retention period spans from 7 days to 730 days. The default retention period is 7 days.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Backup Cycle</td>
<td>Select one or more workdays.</td>
</tr>
<tr>
<td>Backup Time</td>
<td>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.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Backup Frequency</td>
<td>Valid values:</td>
</tr>
<tr>
<td></td>
<td>• Same as Data Backup</td>
</tr>
<tr>
<td></td>
<td>• Every 30 Minutes</td>
</tr>
<tr>
<td></td>
<td>The log file size remains the same no matter which backup frequency you select.</td>
</tr>
<tr>
<td>Log Retention Period</td>
<td>The value of this parameter is the same as that of the Data Retention Period parameter.</td>
</tr>
</tbody>
</table>

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 SQL Server instance.

FAQ

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

   No, the log backup function must be enabled.

APIs

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_166</td>
<td>Used to create a backup set for an RDS instance.</td>
</tr>
<tr>
<td>#unique_167</td>
<td>Used to query the backup set list of an RDS instance.</td>
</tr>
<tr>
<td>#unique_168</td>
<td>Used to query the backup settings of an RDS instance.</td>
</tr>
</tbody>
</table>
### 16.2 View the quota of free backup space for an RDS SQL Server instance

This topic describes how to calculate and view the quota of free backup space for an RDS 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 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.
16.3 Download the data backup files and log backup files of an RDS SQL Server instance

This topic describes how to download the data backup files and log backup files of an RDS 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_172.

<table>
<thead>
<tr>
<th>DB engine</th>
<th>Data backup download</th>
<th>Log backup download</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server</td>
<td>Supports full physical backup, incremental physical backup, and single-database full physical backup.</td>
<td>Supported.</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Download method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy Internal Download URL</td>
<td>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.</td>
</tr>
<tr>
<td>Copy External Download URL</td>
<td>To copy the external download URL only. This method is suitable when you download the backup file by using other tools.</td>
</tr>
</tbody>
</table>

**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.
17 Restoration

17.1 Restore data of ApsaraDB RDS SQL Server instances through temporary instances

You can restore data by using temporary instances to minimize losses caused by misoperations on the database.

Creating a temporary instance does not affect the current production instance but will provide a temporary instance for data access. You can restore data to the temporary instance and verify the data before migrating to the primary instance to minimize the impacts of data restoration on services.

Prerequisites

- The ApsaraDB RDS SQL Server instance must be one of the following editions:
  - ApsaraDB RDS SQL Server 2012 Enterprise Basic Edition
  - ApsaraDB RDS SQL Server 2012/2016 Web Edition
  - ApsaraDB RDS SQL Server 2008 R2
- The instance has data backup files. If you need to restore by time point, related log backup files are required.

Precautions

- The temporary instance uses the same account and password as the source instance.
- The network type of the instance is the classic network.
- Only one temporary instance can be created at a time. If you need to create a new temporary instance, you must delete the existing temporary instance.
- The temporary instance is free of charge, but will be automatically released after being created within 48 hours.

Procedure

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

3. Find the instance and click the instance ID.

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

5. Click the **Temporary Instance** tab.

6. Select the time period that is closest to the target time point, and the instance will restore data based on the latest backup. Click **Create Temporary Instance**.

7. In the message that appears, click **OK** to create a temporary instance.

8. After the temporary instance is created, go to the Instances page.

9. Click the ID of the instance.

10. In the upper-right corner of the page, click **Create Data Migration Task** to go to the Data Transmission Service (DTS) console.

11. Select **Data Migration** in the left-side navigation pane.
12. Click **Create Migration Task** and specify Task Name, Source Database, and Destination Database information.

Parameter description:

- DTS automatically generates a name for each task. You can change the default name to an informative one for easy task identification.
- **Source Database**
  - Instance Type: The type of the source instance. Select **RDS Instance**.
  - Instance Region: Select the region where the primary instance is located.
  - RDS Instance ID: Select the ID of the temporary instance from the drop-down list.
  - Database Account: The account of the primary instance. This account must have the read/write permissions on the data to be migrated.
  - Database Password: The password of the primary instance.
- **Destination Database**
  - Instance Type: Select RDS Instance.
  - Instance Region: The region where the primary instance is located.
  - RDS instance ID: The ID of the destination RDS instance. Select the ID of the primary instance from the drop-down list.
  - Database Account: The account of the primary instance. This account must have the read and write permissions on the data to be migrated.
  - Database Password: The password of the primary instance.

13. Click **Set Whitelist and Next** to go to the **Configure Migration Types and Objects** wizard.

14. Select Migration Type. Select the objects to be migrated in the **Object to Be Migrated** area, and click > to add the selected objects to the **Selected** area, as shown in the following figure. To modify the name of an object to be migrated in the destination database, move the pointer over the database to be modified in the **Selected** section. The **Edit** button is displayed, as shown in the following figure.

15. Click **Precheck and Start**.
16. If the precheck fails, perform this step. If the precheck succeeds, go to Step 18.

If the precheck fails, click the icon next to the check item with check result as Failed to check the failure details, as shown in the following figure. After troubleshooting, select the current migration task on the Migration Tasks page and perform a precheck again.
17. After all the errors are fixed, on the Migration Tasks page, select the newly created migration task and click **Start**.

18. After the precheck succeeds, click **OK**.

19. On the **Confirm Purchase Configuration** page, confirm configuration information and select **Service Terms of Data Transmission (Pay-As-You-Go)**, and click **Buy and Start Now**.

**Related API operations**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_175</td>
<td>Creates temporary instances.</td>
</tr>
</tbody>
</table>

### 17.2 Log on to a temporary instance

You can create a temporary instance, restore data to the temporary instance, log on to the temporary instance to check whether the data is correct, and restore the data from the temporary instance to the destination instance. This topic describes how to log on to a temporary instance.

**Prerequisites**


**Log on to a temporary instance**

You can log on to temporary instances through the intranet. The intranet is fast, secure, and free of traffic fees within the network.
Log on to an instance through the ECS client

1. Create an ECS instance to access the ApsaraDB for RDS temporary instance. The ECS instance must meet the following requirements:
   - The ECS instance and RDS instance must reside in the same region.
   - The network type must be classic network. This is because ECS and RDS instances must have the same network type for communication over the intranet and the network type of all RDS temporary instances is classic network.

2. Add the intranet IP address of the ECS instance to the whitelist of the RDS temporary instance.

3. Log on to the ECS instance. For more information, see Overview.

4. Access the RDS temporary instance from the ECS instance. For more information, see the "Use a client to connect to an instance" section in Connect to an RDS SQL Server instance.

17.3 Restore the data of an RDS SQL Server instance

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

You can use one of the following methods to restore the data of an RDS 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**.

![Select Restore Method](image-url)
7. Set the following parameters and click OK.

![Restore to Existing Instance](image)

**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 (-).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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 SQL Server instance](#).  
  - **By Backup Set:** You can specify a full or incremental backup set from which you want to restore data. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore Time</td>
<td>Select the time point from which you want to restore data. This parameter is displayed when the <strong>Restore Method</strong> parameter is set to <strong>By Time</strong>.</td>
</tr>
<tr>
<td>Backup Set</td>
<td>Select the backup set from which you want to restore data. This parameter is displayed when the <strong>Restore Method</strong> parameter is set to <strong>By Backup Set</strong>.</td>
</tr>
</tbody>
</table>
| 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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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**. |
| 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. |
<p>| Edition/Zone/      | For more information, see <a href="#">Create an RDS SQL Server instance</a>. |
| CPU and Memory/    | Capacity/Network Type/Duration                                              |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Quantity</strong></td>
<td>Specify the number of RDS instances you want to purchase. You can create up to five RDS instances at a time for data restoration.</td>
</tr>
</tbody>
</table>

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
18 Disable the database proxy mode

This topic describes how to disable the database proxy mode for an RDS 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

<table>
<thead>
<tr>
<th>DB engine version</th>
<th>Supported access modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server 2012/2016/2017</td>
<td>Standard mode</td>
</tr>
<tr>
<td>SQL Server 2008 R2</td>
<td>Standard mode and database proxy mode</td>
</tr>
</tbody>
</table>

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**.

![Switch Access Mode](image)

**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.

![RDS Console](image)

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**.

![Database Proxy Tab](image)

**Note:**
This tab page is available only when you have enabled the database proxy mode.
19 Tag

19.1 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

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AddTagsToResource</td>
<td>Used to bind a tag to RDS instances.</td>
</tr>
</tbody>
</table>

19.2 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 the 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

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#unique_184</td>
<td>Used to unbind a tag from an RDS instance.</td>
</tr>
</tbody>
</table>

19.3 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.

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DescribeTags</td>
<td>Used to query tags.</td>
</tr>
</tbody>
</table>
20 SQL Server

20.1 Create a linked server for SQL Server instances

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

Currently, linked server creation has the following constraints:

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

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

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

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

The following message create successfully is displayed after the linked server is successfully created.
Click the **Messages** tab shown in the preceding figure, and the following information is displayed.

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

### 20.2 Connect Kingdee K/3 WISE to ApsaraDB RDS SQL Server

This topic describes how to connect Kingdee K/3 WISE 15.0 or 15.1 to ApsaraDB RDS SQL Server to implement distributed transactions between RDS and ECS instances.

**Solution**

This solution consists of three steps:

1. **Restore account set data to RDS**: Upload the full backup data of the Kingdee K/3 WISE account set database to OSS, and then restore the backup data to RDS.

2. **Allow distributed transactions**: Adjust the access settings for RDS, ECS, and Windows to guarantee available ports for distributed transactions.

3. **Replace with a new account set management tool**: Replace with a new account set management tool that is compatible with RDS.

**Preparations**

• **Create an RDS SQL Server instance.** Prepare the full backup data of the Kingdee K/3 WISE account set database.

**Note:**
- The ECS instance for installing Kingdee must be in the same region and VPC as the RDS instance.
- You must use one of the following instance editions of RDS SQL Server:
  - SQL Server 2012/2016 Enterprise High-availability Edition
  - SQL Server 2012/2016 Standard Edition

**Restore account set data to RDS**

To upload a backup file of account set data, follow these steps:

1. Log on to the OSS console.
2. In the left-side navigation pane, click the **Create Bucket** icon to create a bucket.

3. Set the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bucket Name</td>
<td>Enter a name for the bucket.</td>
</tr>
<tr>
<td>Region</td>
<td>Select the region where you want to create the bucket. Make sure that the bucket is in the same region as the ECS and RDS instances.</td>
</tr>
<tr>
<td>Storage Class</td>
<td>Select IA.</td>
</tr>
<tr>
<td>Access Control List (ACL)</td>
<td>Select Private.</td>
</tr>
<tr>
<td>Server-side Encryption</td>
<td>Select None.</td>
</tr>
<tr>
<td>Zone-redundant Storage</td>
<td>Select Disable.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Real-time Log Query</td>
<td>Select Disable.</td>
</tr>
</tbody>
</table>

Note:
For more information about the parameters, see Create a bucket.

Create Bucket

1. Note: Storage Class and Region cannot be changed after the bucket is created.

Bucket Name

Region

China (Beijing)

Alibaba Cloud services in the same region can communicate with each other over an internal network. The region cannot be changed after the purchase. Exercise caution when you select a region.

Endpoint

oss-cn-beijing.aliyuncs.com

Storage Class

Standard, IA, Archive

Standard: high reliability, high availability, and high performance. Data of this type is frequently accessed.

How to Choose a Suitable Storage Class

Access Control List (ACL)

Private, Public Read, Public Read/Write

Private: Only the owner or authorized user can read from and write to files.

Server-side Encryption

None, AES256, KMS

Real-time Log Query

Enable, Disable

After a file is uploaded to OSS, it will be automatically encrypted and stored in the bucket. Encryption is provided by KMS, and requires authorization. KMS provides only default CMKS for OSS. To use bring your own key (BYOK) to encrypt data, contact technical support. For more information, see Server-side Encryption Guide.

4. Click OK.

5. In the left-side navigation pane, click the bucket that you have created.
6. Click the **Files** tab, and then click **Upload**.

7. Drag the backup file to be uploaded to the **Upload** section, or click **Upload** and select the backup file.

**Note:**
For more information about the parameters, see **Upload an object**.

To create a premier account, follow these steps:

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

2. In the upper-left corner of the page, 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. Click **Create Account**.

6. Set the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Database Account</strong></td>
<td>Enter a database account. The database account must be 2 to 16 characters in length and can contain lowercase letters, digits, and underscores (_). It must start with a lowercase letter and end with a letter or digit.</td>
</tr>
<tr>
<td><strong>Account Type</strong></td>
<td>Select <strong>Premier Account</strong>.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Set the account password. The requirements are as follows:</td>
</tr>
<tr>
<td></td>
<td>• It must be 8 to 32 characters in length.</td>
</tr>
<tr>
<td></td>
<td>• It must contain three of the following character types: upper case letters, lower case letters, digits, and special characters.</td>
</tr>
<tr>
<td></td>
<td>• The allowed special characters are as follows:</td>
</tr>
<tr>
<td></td>
<td>@ # $ % ^ &amp; * ( ) _ + - =</td>
</tr>
<tr>
<td><strong>Re-enter Password</strong></td>
<td>Enter the password again.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Enter your remarks.</td>
</tr>
</tbody>
</table>

7. Click **OK**.

To migrate backup data from OSS to RDS, follow these steps:

1. Log on to the **ApsaraDB for RDS console**.
2. In the upper-left corner of the page, 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 of the page, click **Migrate OSS Backup Data to RDS**.

    **Note:**
    If this button is not visible, check your instance edition.

6. Click **Next** twice to go to the **Import Data** tab.

7. Set the following parameters.

    | Parameter       | Description                                                                 |
    |-----------------|-----------------------------------------------------------------------------|
    | **Database Name** | Enter the name of the destination database in the destination instance.      |
    | **OSS Bucket**   | Select the OSS bucket where the backup file is located.                      |
    | **OSS Subfolder Name** | Enter the name of the subfolder where the backup file is located.        |
    | **OSS File**     | Enter the prefix of the backup file name and click the search button. A list of files is displayed. The list contains the name, size, and update time of each file that matches the query. Select the backup file that you want to restore. |
    | **Cloud Migration Plan** | Select **Immediate Access**.                                                |
    | **Consistency Check Mode** | Select **Synchronous DBCC**.                                                |

    **Note:**
    If you are migrating backup data from OSS to RDS the first time, RDS prompts you to authorize the OSS access permission to your Alibaba Cloud account. Click **Authorize** and **Confirm Authorization Policy**.

8. Click **OK**.

    **Note:**
    Wait for the data to be imported. You can click **Databases** in the left-side navigation pane to view the database status.
Allow distributed transactions

Follow these steps to set your RDS instance:

1. Log on to the ApsaraDB for RDS console.
2. In the upper-left corner of the page, 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 Edit on the right. In the dialog box that appears, enter the IP address of the ECS instance.

Note:

- If the ECS and RDS instance are in 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 RDS instances are not in the same VPC, enter the public IP address of the ECS instance and apply for a public endpoint for the RDS instance.

6. Click OK.
7. Click the Whitelist for Distributed Transaction tab.
8. Click Create Whitelist.
9. Set the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whitelist Name</td>
<td>The whitelist name must be 2 to 32 characters in length and can contain digits, lowercase letters, and underscores (_). It must start with a lowercase letter and end with a letter or digit.</td>
</tr>
<tr>
<td>Whitelist</td>
<td>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.</td>
</tr>
</tbody>
</table>

Note:
You can view the computer name by choosing Control Panel > System and Security > System.

10. Click OK.

Follow these steps to set your ECS instance:
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 target ECS 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 following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Direction</td>
<td>Select Inbound.</td>
</tr>
<tr>
<td>Action</td>
<td>Select Allow.</td>
</tr>
<tr>
<td>Protocol Type</td>
<td>Select Customized TCP.</td>
</tr>
<tr>
<td>Port Range</td>
<td>Enter 135.</td>
</tr>
<tr>
<td>Priority</td>
<td>Enter 1.</td>
</tr>
<tr>
<td>Authorization Type</td>
<td>Select IPv4 CIDR Block.</td>
</tr>
<tr>
<td>Authorization</td>
<td>View the two IP addresses displayed on the Whitelist for Distributed</td>
</tr>
<tr>
<td>Objects</td>
<td>Transaction tab of the Data Security page. Enter them in Authorization</td>
</tr>
<tr>
<td></td>
<td>Objects.</td>
</tr>
<tr>
<td>Description</td>
<td>It must be 2 to 256 characters in length and cannot start with http:// or</td>
</tr>
<tr>
<td></td>
<td>https://.</td>
</tr>
</tbody>
</table>

Note: 135 is the fixed port of the RPC service.

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

Follow these steps to set your Windows operating system:

1. Log on to the Windows Server 2016 operating system.
2. Locate C:\Windows\System32\drivers\etc\hosts and open the hosts file.
3. View the two IP addresses displayed on the Whitelist for Distributed Transaction tab of the Data Security page. Enter them at the end of the hosts file.
4. Save the hosts file.
5. Choose **Control Panel > System and Security > Administrative Tools**. Double-click **Component Services**.

6. Choose **Component Services > Computer > My Computer > Distributed Transaction Coordinator**.

7. Right-click **Local DTC** and choose **Properties** from the shortcut menu.

8. Click the **Security** tab and set the required parameters.

9. Click **OK**. In the **MSDTC Service** message that appears, click **Yes** to wait for the MSDTC service to restart.

**Replace with a new account set management tool**

Replace with a new account set management tool, and then use it to register and enable an account set for RDS. For more information, see **Attachment**.

**Note:**

Different Kingdee K/3 WISE versions require different account set management tools. Only the account set management tools of Kingdee K/3 WISE 15.0 and 15.1 are provided.

**Next step**

After all the settings are complete, distributed transactions can be implemented between the ECS and RDS instances. You can then use Kingdee K/3 WISE normally.

### 20.3 Use SSRS for an ApsaraDB RDS SQL Server instance

You can install SQL Server Reporting Services (SSRS) on an ECS instance and create reports based on the data in an ApsaraDB RDS SQL Server instance. This topic describes how to use ApsaraDB RDS SQL Server instances as data sources to create reports.

**Context**

Microsoft SQL Server contains server components such as SQL Server database engine, SSRS, and SQL Server Analysis Services (SSAS). The SQL Server database engine is a standard relational database component. ApsaraDB RDS SQL Server is a PaaS that provides this database engine. Components such as SSRS run as Windows services, and are not provided as PaaS services on Alibaba Cloud. If you need to use SSRS on Alibaba Cloud, you must create a Windows-based ECS instance before installing and configuring SSRS.

**Note:**

Issue: 20200506
You cannot create the SSRS configuration database in an ApsaraDB RDS SQL Server instance.

Prerequisites

- You have created an ApsaraDB RDS SQL Server instance. For more information, see Create an RDS SQL Server instance.
- You have created an instance by using the wizard.
- You have installed SQL Server on the ECS instance.

Note:
The version of SQL Server on the ECS instance can be different from the version of the ApsaraDB RDS SQL Server instance.

Procedure

1. Download and install Reporting Services in the ECS instance.

Note:
Report Server Configuration Manager automatically displays all the Report Server instances that are in the ECS instance. Select an instance as needed.
3. In the left-side navigation pane, click **Service Account** and **Web Service URL** and configure parameters based on your business needs.

**Note:**
For more information, see Install SQL Server Reporting Services (2017 and later).
4. In the left-side navigation pane, click **Database**. On the right side of the page, click **Change Database** to create a new report server database in the ECS instance.

   a) Select **Create a new report server database** and click **Next**.
   b) Enter the server name and click **Next**.
   c) Enter the database name and select a language for the script. Click **Next**.
   d) Configure the credentials for the account to connect to the report server and click **Next**.
   e) Confirm the information on the Summary page and click **Next**. Wait for the database to be created.
f) Click **Finish**.

**Note:**
For more information, see [Install SQL Server Reporting Services (2017 and later)](#).
5. In the left-side navigation pane, click **Web Portal URL** and click **Apply**. After the application operation is finished, click the URL to go to the Web portal of the report server.

6. In the upper-right corner of the page, choose **New > Data Source**.

7. Configure the parameters as follows:

<table>
<thead>
<tr>
<th>Section</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties</td>
<td>Name</td>
<td>Enter the name of the data source. The name cannot contain special characters. Special characters include / @ $ &amp; * + = &lt; &gt; : ' , ?</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Specify the description of the data source to identify different data sources.</td>
</tr>
<tr>
<td></td>
<td>Hide</td>
<td>Click to hide the data source.</td>
</tr>
<tr>
<td></td>
<td>Enable</td>
<td>Click to enable the data source.</td>
</tr>
<tr>
<td>Connections</td>
<td>Type</td>
<td>Select a type of the data source. Select <strong>Microsoft SQL Server</strong>.</td>
</tr>
<tr>
<td>Section</td>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Connection</td>
<td>Connection String</td>
<td>Specify the endpoint and the database name of the ApsaraDB RDS SQL Server instance in the Data Source=&lt;RDS SQL Server instance endpoint&gt;; Initial Catalog=&lt;database name&gt; format.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Make sure the IP address of the ECS instance is added to the IP whitelist of the RDS instance. For more information, see Configure a whitelist for an RDS SQL Server instance.</td>
</tr>
<tr>
<td>Credential</td>
<td>Data Source</td>
<td>Select Use the following credentials.</td>
</tr>
<tr>
<td>Login</td>
<td>Credential Type</td>
<td>Select Database username and password.</td>
</tr>
<tr>
<td></td>
<td>Username</td>
<td>Enter the database account of the ApsaraDB RDS SQL Server instance.</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>Enter the password of the database account.</td>
</tr>
</tbody>
</table>

8. Click **Create**.

**What's next**

After the data source is created, you can use software such as Report Builder and Visual Studio to design reports. For more information, see Report Builder in SQL Server.