

Alibaba Cloud

ApsaraDB for RDS
RDS SQL Server Database

Document Version: 20220712

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions









Style	Description	Example
 Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
 Note	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type .
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1. Overview of ApsaraDB RDS for SQL Server	10
2. Limits of ApsaraDB RDS for SQL Server	12
3. Features	15
3.1. SQL Server 2019	15
3.2. SQL Server 2017	26
3.3. SQL Server 2016	38
3.4. SQL Server 2012	55
3.5. SQL Server 2008 R2	71
4. Release notes	78
5. Specifications	79
5.1. Primary ApsaraDB RDS for SQL Server instance types	79
5.2. Read-only ApsaraDB RDS for SQL Server instance types	79
5.3. 旧版skip	81
6. Quick start	85
6.1. General workflow to use ApsaraDB RDS for SQL Server	85
6.2. Create an ApsaraDB RDS for SQL Server instance	85
6.3. Set a whitelist	91
6.3.1. Configure an IP address whitelist for an ApsaraDB RDS...	91
6.3.2. Errors and FAQ about IP address whitelist settings in ...	93
6.4. Create databases and accounts	95
6.4.1. Create accounts and databases for an ApsaraDB RDS i...	95
6.4.2. Create an account and a database for an ApsaraDB R...	98
6.4.3. Create an account and a database for an ApsaraDB R...	100
6.5. Connect to an ApsaraDB RDS for SQL Server instance	103
6.6. Read-only instances	104
6.6.1. Overview of read-only ApsaraDB RDS for SQL Server in...	104

6.6.2. Create a read-only ApsaraDB RDS for SQL Server insta...	106
6.7. Features of ApsaraDB RDS instances that run different SQL..	111
7.Data migration	119
7.1. Data migration solutions	119
7.2. Migrate data from a user-created database to an RDS SQL...	119
7.2.1. Migrate the full backup data of a self-managed SQL Se...	119
7.2.2. Migrate the full backup data of a self-managed SQL S...	125
7.2.3. Migrate the incremental backup data of a self-manage...	131
7.2.4. Migrate data from a self-managed SQL Server instance...	139
7.3. Migrate the data of an ApsaraDB RDS for SQL Server data..	149
7.4. Migrate data between ApsaraDB RDS for SQL Server insta...	150
8.Billing	163
8.1. Switch an ApsaraDB RDS for SQL Server instance from pay..	163
8.2. Switch an ApsaraDB RDS for MySQL instance from subscri...	164
8.3. Manually renew an ApsaraDB RDS for SQL Server instance	165
8.4. Enable auto-renewal for an ApsaraDB RDS for SQL Server...	166
9.Manage pending events	170
10.Version upgrade	173
10.1. Upgrade an instance from SQL Server 2012 to SQL Serve...	173
10.2. Upgrade an ApsaraDB RDS for SQL Server instance from...	173
10.3. Upgrade an ApsaraDB RDS for SQL Server instance with ...	178
10.4. Update the minor engine version of an ApsaraDB RDS fo...	183
11.Instance	186
11.1. Create an ApsaraDB RDS for SQL Server instance	186
11.2. Change the specifications of an ApsaraDB RDS for SQL S...	192
11.3. Restart an ApsaraDB RDS for SQL Server instance	195
11.4. Switch workloads over between primary and secondary A...	196
11.5. Set the maintenance window of an ApsaraDB RDS for SQ...	199

11.6. Migrate an ApsaraDB RDS for SQL Server instance across...	200
11.7. Release or unsubscribe from an ApsaraDB RDS for SQL S...	201
11.8. DBCC features of ApsaraDB RDS SQL Server	202
11.9. View the data replication mode of an ApsaraDB RDS for ...	203
11.10. Reconfigure parameters for an RDS for SQL Server insta...	204
11.10.1. Reconfigure the parameters of an ApsaraDB RDS for ...	204
11.10.2. Reconfigure the parameters of an ApsaraDB RDS for ...	206
11.11. Manage ApsaraDB RDS for SQL Server instances in the r...	207
12.Database connection	209
12.1. Connect to an ApsaraDB RDS for SQL Server instance	209
12.2. Apply for or release a public endpoint on an ApsaraDB ...	210
12.3. View and change the internal and public endpoints and ..	212
12.4. Use DMS to log on to an ApsaraDB RDS for SQL Server ...	213
12.5. Configure the hybrid access solution for an ApsaraDB RD...	215
12.6. Switch an ApsaraDB RDS for SQL Server instance to a di...	218
12.7. Change the network type of an ApsaraDB RDS for SQL S...	220
12.8. Close a connection to an ApsaraDB RDS for SQL Server i...	222
13.Read/write splitting	223
13.1. Overview of read/write splitting	223
13.2. Create a read-only ApsaraDB RDS for SQL Server instance	225
13.3. Enable the read-only routing endpoint of an ApsaraDB R...	229
13.4. Modify the read weight of an ApsaraDB RDS for SQL Se...	231
13.5. Disable the read-only routing endpoint of an ApsaraDB ...	232
13.6. Default read weights	233
13.7. Configure the read attribute for a secondary RDS instanc...	233
14.Account	235
14.1. Create an account for an RDS SQL Server instance	235
14.2. Reset the password of an account on an ApsaraDB RDS ...	235

14.3. Account permission	236
14.3.1. Modify the permissions of a standard account on an	236
14.3.2. Account permissions in an ApsaraDB RDS for SQL Ser...	237
14.4. Grant permissions to the service account of an ApsaraDB...	243
14.5. Delete an account for an RDS SQL Server instance	244
14.6. Manage ApsaraDB RDS SQL Server logins	244
14.7. Manage ApsaraDB RDS SQL Server users	246
14.8. Create a system admin account on an ApsaraDB RDS for...	246
14.9. Create a host account for an ApsaraDB RDS for SQL Serv...	249
14.10. System accounts of an ApsaraDB RDS for SQL Server in...	259
15.Database	260
15.1. Create a database on an ApsaraDB RDS for SQL Server in...	260
15.2. Delete a database from an ApsaraDB RDS for SQL Server...	260
15.3. Change the character set collation and time zone of syst...	261
15.4. Create and manage databases on an ApsaraDB RDS for	265
15.5. Database replication	267
15.5.1. Replicate databases between ApsaraDB RDS for SQL S...	267
15.5.2. Replicate a database of an ApsaraDB RDS instance th...	269
15.5.3. Replicate a database of an ApsaraDB RDS instance th...	270
16.Stored procedures	272
17.Monitoring and alerts	279
17.1. View the resource metrics and engine metrics of an Apsar...	279
17.2. Set the monitoring frequency of an ApsaraDB RDS for SQ...	280
17.3. Configure an alert rule for an ApsaraDB RDS for SQL Ser...	281
18.Data security and encryption	283
18.1. Set a whitelist	283
18.1.1. Configure an IP address whitelist for an ApsaraDB RD...	283
18.1.2. Errors and FAQ about IP address whitelist settings in	285

18.2. Configure SSL encryption on an ApsaraDB RDS for SQL S...	287
18.3. Configure TDE for an ApsaraDB RDS for SQL Server insta...	290
18.4. Configure a distributed transaction whitelist for an Apsar...	295
18.5. Enable or disable the release protection feature for an A...	297
18.6. Configure disk encryption for an ApsaraDB RDS for SQL ...	299
19.Audit	301
19.1. Use the SQL Audit feature on an ApsaraDB RDS for SQL ...	301
19.2. View the error logs of an ApsaraDB RDS for SQL Server ...	302
19.3. View the event history of an ApsaraDB RDS instance	304
20.Backup	309
20.1. Enable snapshot backups for an ApsaraDB RDS for SQL S...	309
20.2. Backup storage fees for an ApsaraDB RDS for SQL Server...	312
20.3. Back up an ApsaraDB RDS for SQL Server instance	313
20.4. Enable cross-region backups for an ApsaraDB RDS for SQ...	318
20.5. Download the data backup files and log backup files of ...	324
21.Restoration	328
21.1. Restore the data of an ApsaraDB RDS for SQL Server inst...	328
21.2. Restore the data of an ApsaraDB RDS for SQL Server ins...	332
21.3. Restore the data of an ApsaraDB RDS for SQL Server ins...	335
21.4. Log on to a temporary ApsaraDB RDS for SQL Server ins...	338
22.Disable the database proxy mode on an ApsaraDB RDS for S...	339
23.Performance optimization and diagnosis	341
23.1. Troubleshoot the issues of high CPU utilization on an Ap...	341
23.2. Troubleshoot the issues of high I/O on an ApsaraDB RDS...	345
23.3. Troubleshoot the issues of insufficient storage space on a...	350
23.4. Introduction to CloudDBA in ApsaraDB RDS for SQL Serv...	356
23.5. View the storage information of an ApsaraDB RDS for SQ...	358
23.6. Performance optimization	363

23.6.1. View the index usage statistics of an ApsaraDB RDS f...	363
23.6.2. View the performance statistics of an ApsaraDB RDS ...	365
23.6.3. View the SQL statement statistics of an ApsaraDB RD...	367
23.6.4. View the top N objects of an ApsaraDB RDS for SQL ...	371
23.7. Lock optimization	376
23.7.1. View the deadlock statistics of an ApsaraDB RDS for S...	376
23.7.2. View the blocking statistics of an ApsaraDB RDS for S...	379
23.8. Analyze the slow SQL statements on an ApsaraDB RDS f...	382
23.9. Use the monitoring dashboard feature	385
24.Tag	390
24.1. Create tags	390
24.2. Delete tags	392
24.3. Use tags to filter ApsaraDB RDS for SQL Server instances	393
25.Best practices	394
25.1. Connect an ApsaraDB RDS for SQL Server instance to a s...	394
25.2. Connect Kingdee K/3 WISE to ApsaraDB RDS for SQL Se...	405
25.3. Use SSRS for an ApsaraDB RDS SQL Server instance	416

1. Overview of ApsaraDB RDS for SQL Server

This topic provides an overview of ApsaraDB RDS for SQL Server and describes the related concepts.

ApsaraDB for RDS is a stable, reliable, and scalable online database service. It is designed based on the Apsara Distributed File System and high-performance SSD storage media of Alibaba Cloud. It supports five database engines: MySQL, SQL Server, PostgreSQL, and MariaDB. It also provides a complete suite of solutions for various scenarios, such as disaster recovery, backup, restoration, monitoring, and migration. These solutions facilitate database operation and maintenance (O&M). For more information about the benefits of ApsaraDB for RDS, see [Competitive advantages of ApsaraDB RDS instances over self-managed databases](#).

You can submit a if you require technical support. If your workloads are complex, you can purchase a support plan on [the Alibaba Cloud After-Sales Support page](#). This allows you to seek advice from instant messaging (IM) enterprise groups, technical account managers (TAMs), and service managers.


For more information about ApsaraDB for RDS, visit [the ApsaraDB RDS for MySQL product page](#).

Disclaimer

Some features or functions that are described in this document may be unavailable. For more information, see the specific terms and conditions in your commercial contract. This document serves as a user guide that is for reference only. No content in this document can constitute any expressed or implied warranty.

ApsaraDB RDS for SQL Server

ApsaraDB RDS for SQL Server is built on top of a high-availability architecture and supports the restoration of data to a specific point in time. These highlights enable ApsaraDB RDS for SQL Server to support various enterprise applications. In addition, ApsaraDB RDS for SQL Server includes Microsoft-issued licenses, which eliminates the need to purchase licenses and reduces costs.

 **Note** The license for an ApsaraDB RDS for SQL Server instance is approved based on the number of cores that are configured for the instance. You do not need to obtain a client access license.

ApsaraDB RDS for SQL Server provides the following advanced features:

- ApsaraDB for MyBase dedicated clusters: An ApsaraDB for MyBase dedicated cluster consists of multiple hosts, such as Elastic Compute Service (ECS) instances of the ecs.i2.xlarge instance type and ECS Bare Metal instances. You can deploy RDS instances on these hosts based on your varying business requirements. For more information, see [What is ApsaraDB for MyBase?](#)
- Disk encryption: This feature encrypts the entire data disks of your RDS instance based on block storage. Your data cannot be accessed even if data leaks occur. For more information, see [Configure disk encryption for an ApsaraDB RDS for SQL Server instance](#). This feature does not interrupt your workloads. You can use this feature without the need to modify your application.
- Read-only RDS instances: If the number of read requests that your database system needs to process is significantly greater than the number of write requests, a single primary RDS instance may not be able to efficiently process read requests and your workloads may be interrupted. To offload read requests from the primary RDS instance, you can create one or more read-only RDS instances. For more information, see [Create a read-only ApsaraDB RDS for SQL Server instance](#). This way, you can increase

the read capability of your database system and increase the throughput of your application.

- **Read/write splitting:** After read-only RDS instances are created, you can enable the read-only routing endpoint and add the endpoint of the primary RDS instance and the read-only routing endpoint to your application. Your database system forwards write requests to the primary RDS instance and read requests to the read-only routing endpoint. Then, the read-only routing endpoint forwards the read requests to the read-only RDS instances based on the read weights of the read-only RDS instances. For more information, see [Overview of read/write splitting](#).

For more information about the features that are supported by ApsaraDB RDS for SQL Server, see [SQL Server 2019](#).

Basic terms

- **Instance:** An RDS instance is a database process that consumes independent physical memory resources. You can specify a specific memory size, disk capacity, and database type for an RDS instance. The performance of an RDS instance varies based on the specified memory size. After an RDS instance is created, you can change its specifications or delete the instance.
- **Database:** A database is a logical unit that is created on an RDS instance. One RDS instance can have multiple databases. Each database must have a unique name on the RDS instance where it is created.
- **Region and zone:** Each region is a physical data center. Each region contains a number of isolated locations that are known as zones. Each zone has an independent power supply and network. For more information, visit [the Alibaba Cloud's Global Infrastructure page](#).

General terms

Term	Description
On-premises database	A database that is deployed in an on-premises data center or a database that is not deployed on an ApsaraDB for RDS instance.
ApsaraDB RDS for XX (XX represents one of the following database engines: MySQL, SQL Server, PostgreSQL, and MariaDB.)	ApsaraDB for RDS with a specific database engine. For example, ApsaraDB RDS for MySQL indicates an ApsaraDB for RDS instance that runs MySQL.


2.Limits of ApsaraDB RDS for SQL Server

This topic describes the limits of ApsaraDB RDS for SQL Server. Before you use ApsaraDB RDS for SQL Server, we recommend that you familiarize yourself with these limits to ensure the stability and security of your database system.

Item	RDS Cluster Edition	RDS High-availability Edition		RDS Basic Edition
	SQL Server 2019 EE SQL Server 2017 EE	SQL Server 2019 SE SQL Server 2017 SE SQL Server 2016 SE and SQL Server 2016 EE SQL Server 2012 SE and SQL Server 2012 EE	SQL Server 2008 R2 R2	SQL Server 2012 Web and SQL Server 2016 Web SQL Server 2012 SE and SQL Server 2016 SE SQL Server 2012 EE Basic SQL Server 2016 EE
Maximum number of databases (For more information, see the " Maximum number of databases " section of this topic.)	300	300	50	400
Maximum number of database accounts	Unlimited	Unlimited	500	Unlimited
Creation of accounts, logon connections, and databases	Supported	Supported	Supported	Supported
Database-level DDL triggers	Supported	Supported	Not supported	Supported
Database permission authorization	Supported	Supported	Not supported	Supported
Permissions to terminate threads	Supported	Supported	Supported	Supported

Item	RDS Cluster Edition	RDS High-availability Edition		RDS Basic Edition
	SQL Server 2019 EE SQL Server 2017 EE	SQL Server 2019 SE SQL Server 2017 SE SQL Server 2016 SE and SQL Server 2016 EE SQL Server 2012 SE and SQL Server 2012 EE	SQL Server 2008 R2 R2	SQL Server 2012 Web and SQL Server 2016 Web SQL Server 2012 SE and SQL Server 2016 SE SQL Server 2012 EE Basic SQL Server 2016 EE
Linked Server	Supported (Linked servers are not supported for the shared instance family.)	Supported (Linked servers are not supported for the shared instance family.)	Not supported	Not supported
Distributed transactions	Supported	Supported	Not supported	Not supported
SQL Profiler	Supported	Supported	Supported	Supported
Tuning Advisor	Supported	Supported	Not supported	Supported
Change data capture (CDC)	Supported	Not supported	Not supported	Not supported
Change tracking	Supported	Supported	Not supported	Supported
Windows domain account logon	Supported (Windows domain account logon is not supported for the shared instance family.)	Supported (Windows domain account logon is not supported for the shared instance family.)		
Email				
SQL Server Integration Services (SSIS)				
SQL Server Analysis Services (SSAS)				
SQL Server Reporting Services (SSRS)				
R Services				

Item	RDS Cluster Edition	RDS High-availability Edition	Not supported	RDS Basic Edition
	Not supported	SQL Server 2019 SE Not supported SQL Server 2017 SE		SQL Server 2012 Web and SQL Server 2016 Web
	SQL Server 2019 EE SQL Server 2017 EE	SQL Server 2016 SE and SQL Server 2016 EE SQL Server 2012 SE and SQL Server 2012 EE	SQL Server 2008 R2 R2	SQL Server 2012 SE and SQL Server 2016 SE SQL Server 2012 EE Basic SQL Server 2016 EE
Common Language Runtime (CLR)				
Asynchronous communication				
Replication				
Policy management				

 **Note** If you want to know more about the limits, you can submit a .

Maximum number of databases

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

- RDS Cluster Edition and RDS High-availability Edition $\min\{\lfloor\sqrt{CPUcores}\rfloor * 50, 300\}$

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

- RDS Basic Edition $\min\{\lfloor\sqrt{CPUcores}\rfloor * 100, 400\}$

The maximum number that is obtained from the preceding formula cannot exceed 400.

3.Features

3.1. SQL Server 2019

This topic provides an overview of the features supported by ApsaraDB RDS instances that run SQL Server 2019. In the following table, ticks (✔️) indicate that a feature is supported, and crosses (❌) indicate that a feature is not supported.

Category	Feature	SQL Server 2019 EE		SQL Server 2019 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Data migration	Migrate the data of an ApsaraDB RDS for SQL Server instance	✔️	✔️	✔️	✔️	✔️	✔️
	Create an ApsaraDB RDS for SQL Server instance	✔️	✔️	✔️	✔️	✔️	✔️
	Change the specifications of an ApsaraDB RDS for SQL Server instance	✔️	✔️	✔️	✔️	✔️	✔️

Category	Feature	SQL Server 2019 EE		SQL Server 2019 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Instance management	Migrate an ApsaraDB RDS for SQL Server instance across zones in the same region	☐	☐	☐	☐	☐	☐
	Switch workloads over between primary and secondary ApsaraDB RDS for SQL Server instances	✔☺	✔☺	✔☺	✔☺	☐	☐
	Restart an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Set the maintenance window of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2019 EE		SQL Server 2019 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
	Release an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Manage ApsaraDB RDS for SQL Server instances in the recycle bin	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Use DBCC statements on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Create an account on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2019 EE		SQL Server 2019 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Account management	Reset the password of an account of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Modify the permissions of an account of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Grant permissions to the service account of an ApsaraDB RDS for SQL Server instance	☐	☐	☐	☐	☐	☐
	Delete an account from an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2019 EE		SQL Server 2019 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Database management	Create a database on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Delete a database from an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Replicate a database from an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Connect to an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Configure endpoints for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2019 EE		SQL Server 2019 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Database connection	View and change the internal and public endpoints and port numbers of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Switch an ApsaraDB RDS for SQL Server instance to a different vSwitch	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Apply for a public endpoint for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2019 EE		SQL Server 2019 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Monitoring and alerting	View the resource metrics, engine metrics, and deployment metrics of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Set the monitoring frequency of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Configure an alert rule for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Create a read-only ApsaraDB RDS for SQL Server instance	✔☺	✔☺	☐	☐	☐	☐

Category	Feature	SQL Server 2019 EE		SQL Server 2019 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Read-only instance and read/write splitting	Enable the read/write splitting feature for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	☐	☐	☐	☐
	Modify the read weights of read-only ApsaraDB RDS for SQL Server instances	✔☺	✔☺	☐	☐	☐	☐
	Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Configure SSL encryption for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2019 EE		SQL Server 2019 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Security management	Configure TDE for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	☐	☐
	Configure a distributed transaction whitelist for an ApsaraDB RDS for SQL Server instance	☐	☐	✔☺	✔☺	☐	☐
	Configure disk encryption for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Use the SQL Audit feature on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2019 EE		SQL Server 2019 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Audit	Manage the logs of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	View the event history of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Back up an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Enable snapshot backups for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2019 EE		SQL Server 2019 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Backup	Enable cross-region backups for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Provide a free quota for backup storage for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Download the backup files of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
Restoration	Restore the data of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2019 EE		SQL Server 2019 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Diagnosis and optimization	Introduction to CloudDBA in ApsaraDB RDS for SQL Server	✔☹	✔☹	✔☹	✔☹	✔☹	✔☹
Tag management	Create tags	✔☹	✔☹	✔☹	✔☹	✔☹	✔☹
	Delete tags	✔☹	✔☹	✔☹	✔☹	✔☹	✔☹
	Use tags to filter ApsaraDB RDS for SQL Server instances	✔☹	✔☹	✔☹	✔☹	✔☹	✔☹

3.2. SQL Server 2017

This topic provides an overview of the features supported by ApsaraDB RDS instances that run SQL Server 2017. In the following table, ticks (☹✔☹) indicate that a feature is supported, and crosses (☹) indicate that a feature is not supported.

Category	Feature	SQL Server 2017 EE		SQL Server 2017 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1

Category	Feature	SQL Server 2017 EE		SQL Server 2017 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Data migration	Migrate the data of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Create an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Change the specifications of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Migrate an ApsaraDB RDS for SQL Server instance across zones in the same region	☐	☐	☐	☐	☐	☐

Category	Feature	SQL Server 2017 EE		SQL Server 2017 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Instance management	Switch workloads over between primary and secondary ApsaraDB RDS for SQL Server instances	✔☺	✔☺	✔☺	✔☺	☐	☐
	Restart an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Set the maintenance window of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Release an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2017 EE		SQL Server 2017 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
	Manage ApsaraDB RDS for SQL Server instances in the recycle bin	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Use DBCC statements on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Create an account on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Reset the password of an account of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2017 EE		SQL Server 2017 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Account management	Modify the permissions of an account of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Grant permissions to the service account of an ApsaraDB RDS for SQL Server instance	☐	☐	☐	☐	☐	☐
	Delete an account from an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Create a database on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2017 EE		SQL Server 2017 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Database management	Delete a database from an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Replicate a database from an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
Database management	Connect to an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Configure endpoints for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2017 EE		SQL Server 2017 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Database connection	View and change the internal and public endpoints and port numbers of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Switch an ApsaraDB RDS for SQL Server instance to a different vSwitch	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Apply for a public endpoint for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2017 EE		SQL Server 2017 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Monitoring and alerting	View the resource metrics, engine metrics, and deployment metrics of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Set the monitoring frequency of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Configure an alert rule for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Create a read-only ApsaraDB RDS for SQL Server instance	✔☺	✔☺	☐	☐	☐	☐

Category	Feature	SQL Server 2017 EE		SQL Server 2017 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Read-only instance and read/write splitting	Enable the read/write splitting feature for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	☐	☐	☐	☐
	Modify the read weights of read-only ApsaraDB RDS for SQL Server instances	✔☺	✔☺	☐	☐	☐	☐
	Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Configure SSL encryption for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2017 EE		SQL Server 2017 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Security management	Configure TDE for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	☐	☐	☐	☐
	Configure a distributed transaction whitelist for an ApsaraDB RDS for SQL Server instance	☐	☐	✔☺	✔☺	☐	☐
	Configure disk encryption for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Use the SQL Audit feature on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2017 EE		SQL Server 2017 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Audit	Manage the logs of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	View the event history of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Back up an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Enable snapshot backups for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2017 EE		SQL Server 2017 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Backup	Enable cross-region backups for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Provide a free quota for backup storage for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Download the backup files of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
Restoration	Restore the data of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2017 EE		SQL Server 2017 SE		SQL Server 2019 Web	
		RDS Cluster Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Diagnosis and optimization	Introduction to CloudDBA in ApsaraDB RDS for SQL Server	✔☹	✔☹	✔☹	✔☹	✔☹	✔☹
Tag management	Create tags	✔☹	✔☹	✔☹	✔☹	✔☹	✔☹
	Delete tags	✔☹	✔☹	✔☹	✔☹	✔☹	✔☹
	Use tags to filter ApsaraDB RDS for SQL Server instances	✔☹	✔☹	✔☹	✔☹	✔☹	✔☹

3.3. SQL Server 2016

This topic provides an overview of the features supported by ApsaraDB RDS instances that run SQL Server 2016. In the following table, ticks (☹✔) indicate that a feature is supported, and crosses (☐) indicate that a feature is not supported.

Category	Feature	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
Data migration	Migrate the data of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Create an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Change the specifications of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
Instance management	Migrate an ApsaraDB RDS for SQL Server instance across zones in the same region	☐	☐	☐	☐	☐	☐	☐	☐
	Switch workloads over between primary and secondary ApsaraDB RDS for SQL Server instances	✔☺	✔☺	☐	☐	✔☺	✔☺	☐	☐
	Restart an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
	Set the maintenance window of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Release an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Manage ApsaraDB RDS for SQL Server instances in the recycle bin	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
	Use DBCC statements on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
Instance upgrade	Upgrade the RDS edition of an ApsaraDB RDS for SQL Server instance from Basic Edition to High-availability Edition	☐	☐	✔☺	✔☺	☐	☐	✔☺	✔☺
	Create an account on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
Account management	Reset the password of an account of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Modify the permissions of an account of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Grant permissions to the service account of an ApsaraDB RDS for SQL Server instance	☐	☐	☐	☐	☐	☐	☐	☐

Category	Feature	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
	Delete an account from an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
Database management	Create a database on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Delete a database from an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
	Replicate a database from an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Connect to an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Configure endpoints for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
Database connection	View and change the internal and public endpoints and port numbers of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Switch an ApsaraDB RDS for SQL Server instance to a different vSwitch	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
	Apply for a public endpoint for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	View the resource metrics, engine metrics, and deployment metrics of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Monitoring and alert in Category	Feature	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
	Set the monitoring frequency of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Configure an alert rule for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Create a read-only ApsaraDB RDS for SQL Server instance	☐	☐	☐	☐	☐	☐	☐	☐

Category	Feature	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
Read-only instance and read/write splitting	Enable the read/write splitting feature for an ApsaraDB RDS for SQL Server instance	☐	☐	☐	☐	☐	☐	☐	☐
	Modify the read weights of read-only ApsaraDB RDS for SQL Server instances	☐	☐	☐	☐	☐	☐	☐	☐

Category	Feature	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
Security	Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Configure SSL encryption for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Configure TDE for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	☐	☐	☐	☐

management	Category	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
	Configure a distributed transaction whitelist for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	☐	☐	✔☺	✔☺	☐	☐
	Configure disk encryption for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Use the SQL Audit feature on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
Audit									
	Manage the logs of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	View the event history of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Back up an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
Backup	Enable snapshot backups for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Enable cross-region backups for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Provide a free quota for backup storage for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
	Download the backup files of an ApsaraDB RDS for SQL Server instance	✔	✔	✔	✔	✔	✔	✔	✔
Restoration	Restore the data of an ApsaraDB RDS for SQL Server instance	✔	✔	✔	✔	✔	✔	✔	✔
Diagnosis and optimization	Introduction to CloudDBA in ApsaraDB RDS for SQL Server	✔	✔	✔	✔	✔	✔	✔	✔
	Create tags	✔	✔	✔	✔	✔	✔	✔	✔
	Delete tags	✔	✔	✔	✔	✔	✔	✔	✔

Category	Feature	SQL Server 2016 EE				SQL Server 2016 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD
	Use tags to filter ApsaraDB RDS for SQL Server instances	✔☹	✔☹	✔☹	✔☹	✔☹	✔☹	✔☹	✔☹

3.4. SQL Server 2012

This topic provides an overview of the features supported by ApsaraDB RDS instances that run SQL Server 2012. In the following table, ticks (✔☹) indicate that a feature is supported, and crosses (☹) indicate that a feature is not supported.

Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Data migration	Migrate the data of an ApsaraDB RDS for SQL Server instance	✔☹	✔☹	✔☹	✔☹	✔☹	✔☹	✔☹	✔☹

Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
	Create an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Change the specifications of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Migrate an ApsaraDB RDS for SQL Server instance across zones in the same region	☐	☐	☐	☐	☐	☐	☐	☐

Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Instance management	Switch workloads over between primary and secondary ApsaraDB RDS for SQL Server instances	✔☺	✔☺	☐	☐	✔☺	✔☺	☐	☐
	Restart an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Set the maintenance window of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
	Release an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Manage ApsaraDB RDS for SQL Server instances in the recycle bin	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Use DBCC statements on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Instance upgrade	Upgrade the RDS edition of an ApsaraDB RDS for SQL Server instance from Basic Edition to High-availability Edition	☐	☐	✔☺	✔☺	☐	☐	✔☺	✔☺
	Upgrade the database engine version of an ApsaraDB RDS instance from SQL Server 2012 to SQL Server 2016	☐	☐	✔☺	✔☺	☐	☐	✔☺	✔☺

Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Account management	Create an account on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Reset the password of an account of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Modify the permissions of an account of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
	Grant permissions to the service account of an ApsaraDB RDS for SQL Server instance	☐	☐	☐	☐	☐	☐	☐	☐
	Delete an account from an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Create a database on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Database management	Delete a database from an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Replicate a database from an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Connect to an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Database connection	Configure endpoints for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	View and change the internal and public endpoints and port numbers of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
	Switch an ApsaraDB RDS for SQL Server instance to a different vSwitch	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Apply for a public endpoint for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Monitoring and alerting	View the resource metrics, engine metrics, and deployment metrics of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Set the monitoring frequency of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
	Configure an alert rule for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
Read-only instance and read/write	Create a read-only ApsaraDB RDS for SQL Server instance	☐	☐	☐	☐	☐	☐	☐	☐
	Enable the read/write splitting feature for an ApsaraDB RDS for SQL Server instance	☐	☐	☐	☐	☐	☐	☐	☐

Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
	Modify the read weights of read-only ApsaraDB RDS for SQL Server instances	☐	☐	☐	☐	☐	☐	☐	☐
	Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Configure SSL encryption for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Security Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Security Category	Configure TDE for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	☐	☐	☐	☐
	Configure a distributed transaction whitelist for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	☐	☐	✔☺	✔☺	☐	☐
Audit	Manage the logs of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Backup	Back up an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Enable snapshot backups for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Enable cross-region backups for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
	Provide a free quota for backup storage for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Download the backup files of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
Restoration	Restore the data of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Create tags	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

Category	Feature	SQL Server 2012 EE		SQL Server 2012 EE Basic		SQL Server 2012 SE		SQL Server 2019 Web	
		RDS High-availability Edition		RDS Basic Edition		RDS High-availability Edition		RDS Basic Edition	
		Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3	Standard SSD	ESSD of PL1
Tag management	Delete tags	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺
	Use tags to filter ApsaraDB RDS for SQL Server instances	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺	✔☺

3.5. SQL Server 2008 R2

This topic provides an overview of the features supported by ApsaraDB RDS instances that run SQL Server 2008 R2. In the following table, ticks (✔☺) indicate that a feature is supported, and crosses (☹) indicate that a feature is not supported.

Category	Feature	RDS High-availability Edition		
		Local SSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3
Data migration	Migrate the data of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Create an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Change the specifications of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺

Category	Feature	RDS High-availability Edition		
		Local SSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3
Instance management	Migrate an ApsaraDB RDS for SQL Server instance across zones in the same region	✔☺	☐	☐
	Switch workloads over between primary and secondary ApsaraDB RDS for SQL Server instances	✔☺	✔☺	✔☺
	Restart an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Set the maintenance window of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Release an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Manage ApsaraDB RDS for SQL Server instances in the recycle bin	✔☺	✔☺	✔☺
	Use DBCC statements on an ApsaraDB RDS for SQL Server instance	☐	✔☺	✔☺

Category	Feature	RDS High-availability Edition		
		Local SSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3
Instance upgrade	Upgrade the database engine version of an ApsaraDB RDS for SQL Server instance from SQL Server 2008 R2 to SQL Server 2012 or SQL Server 2016	✔☺	☐	☐
Account management	Create an account on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Reset the password of an account of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Modify the permissions of an account of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Grant permissions to the service account of an ApsaraDB RDS for SQL Server instance	✔☺	☐	☐
	Delete an account from an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Create a database on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Delete a database from an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺

Database management Category	Feature	RDS High-availability Edition		
		Local SSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3
	Replicate a database from an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
Database connection	Connect to an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Configure endpoints for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	View and change the internal and public endpoints and port numbers of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Switch an ApsaraDB RDS for SQL Server instance to a different vSwitch	☐	✔☺	✔☺
	Apply for a public endpoint for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	View the resource metrics, engine metrics, and deployment metrics of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺

Monitoring and alerting Category	Feature	RDS High-availability Edition		
		Local SSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3
	Set the monitoring frequency of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Configure an alert rule for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
Read-only instance and read/write splitting	Create a read-only ApsaraDB RDS for SQL Server instance	☐	☐	☐
	Enable the read/write splitting feature for an ApsaraDB RDS for SQL Server instance	☐	☐	☐
	Modify the read weights of read-only ApsaraDB RDS for SQL Server instances	☐	☐	☐
Security management	Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Configure SSL encryption for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Configure TDE for an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺

Category	Feature	RDS High-availability Edition		
		Local SSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3
	Configure a distributed transaction whitelist for an ApsaraDB RDS for SQL Server instance	☐	☐	☐
	Configure disk encryption for an ApsaraDB RDS for SQL Server instance	☐	✔☺	✔☺
Audit	Use the SQL Audit feature on an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Manage the logs of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	View the event history of an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
Backup	Back up an ApsaraDB RDS for SQL Server instance	✔☺	✔☺	✔☺
	Enable snapshot backups for an ApsaraDB RDS for SQL Server instance	☐	✔☺	✔☺
	Enable cross-region backups for an ApsaraDB RDS for SQL Server instance	☐	✔☺	✔☺

Category	Feature	RDS High-availability Edition		
		Local SSD	Standard SSD	ESSD of PL1, ESSD of PL2, or ESSD of PL3
	Provide a free quota for backup storage for an ApsaraDB RDS for SQL Server instance	✓☺	✓☺	✓☺
	Download the backup files of an ApsaraDB RDS for SQL Server instance	✓☺	✓☺	✓☺
Restoration	Restore the data of an ApsaraDB RDS for SQL Server instance	✓☺	✓☺	✓☺
Diagnosis and optimization	Introduction to CloudDBA in ApsaraDB RDS for SQL Server	✓☺	☐	☐
Tag management	Create tags	✓☺	✓☺	✓☺
	Delete tags	✓☺	✓☺	✓☺
	Use tags to filter ApsaraDB RDS for SQL Server instances	✓☺	✓☺	✓☺

4. Release notes

ApsaraDB RDS for SQL Server is developed based on Microsoft SQL Server. The minor versions of ApsaraDB RDS for SQL Server are the same as the minor versions of Microsoft SQL Server. This topic provides links to the Microsoft documentation that describes these minor SQL Server versions.

If you want to use the new features that are provided by a new minor SQL Server version, update the minor SQL Server version of your RDS instance. For more information, see the following topics:

- [View the minor engine version of your RDS instance](#)
- [Update the minor version of your RDS instance](#)

RDS SQL Server 2019

Minor SQL Server version	Release date	Link to Microsoft documentation
15.0.4138.2	2021-12-17	Cumulative Update 11 for SQL Server 2019
15.0.4073.23	2021-04-25	Cumulative Update 8 for SQL Server 2019

RDS SQL Server 2017

Minor SQL Server version	Release date	Link to Microsoft documentation
14.0.3421.10	2021-12-17	Cumulative Update 27 for SQL Server 2017
14.0.3381.3	2021-04-29	Cumulative Update 23 for SQL Server 2017

RDS SQL Server 2016

Minor SQL Server version	Release date	Link to Microsoft documentation
13.0.5888.11	2021-04-29	Cumulative Update 17 for SQL Server 2016 SP2

RDS SQL Server 2012

Minor SQL Server version	Release date	Link to Microsoft documentation
11.0.7507.2	2021-05-28	Description of the security update for SQL Server 2012 SP4 GDR

5. Specifications

5.1. Primary ApsaraDB RDS for SQL Server instance types

This topic provides an overview of the primary instance types that are supported for ApsaraDB RDS for SQL Server. This overview includes the most recent instance types, the earlier instance types, and the specifications for each instance type.

Note

- The memory capacity that is supported by an instance type includes the memory that is occupied by the RDS-related management services, the database service, and the underlying operating system. For example, the memory capacity includes the memory reserved for BIOS, the memory occupied by the kernel of the operating system, and the memory occupied by the hypervisor. Therefore, the available memory that you can view may be less than the memory capacity that is supported by the instance type.
- RDS instances that use standard SSDs or enhanced SSDs (ESSDs) are deployed on Elastic Compute Service (ECS) instances. The performance of these RDS instances varies based on the instance families of the ECS instances. For more information, see [Instance family](#).

5.2. Read-only ApsaraDB RDS for SQL Server instance types


This topic provides an overview of read-only ApsaraDB RDS for SQL Server instance types. This overview includes the most recent instance types and the specifications for each instance type.

Read-only ApsaraDB RDS for SQL Server instances

Role	Database engine version	Instance family	Instance type	CPU and memory specifications	Maximum number of connections	Maximum IOPS	Storage capacity
		General	rds.mssql.s2.large	2 cores, 4 GB			
			rds.mssql.s3.large	4 cores, 8 GB			
			rds.mssql.c1.large	8 cores, 16 GB			
			rds.mssql.s2.xlarge	2 cores, 8 GB			
			-				

Role	Database engine version	purpose instance family	Instance type	CPU and memory specifications	Maximum number of connections	Maximum IOPS	Storage capacity
Read-only instance management	SQL Server 2017 EE and SQL Server 2019 EE		rds.mssql.m1.medium	4 cores, 16 GB	Unlimited	For more information, see Maximum IOPS for standard SSDs and ESSDs .	20GB-4000GB
			rds.mssql.c1.xlarge	8 cores, 32 GB			
			rds.mssql.c2.xlarge	16 cores, 64 GB			
		Dedicated instance family	mssql.x4.medium.ro	2 cores, 8 GB			
			mssql.x4.large.ro	4 cores, 16 GB			
			mssql.x4.xlarge.ro	8 cores, 32 GB			
			mssql.x4.2xlarge.ro	16 cores, 64 GB			
			mssql.x4.4xlarge.ro	32 cores, 128 GB			
			mssql.x4.8xlarge.ro	64 cores, 256 GB			
			mssql.x8.medium.ro	2 cores, 16 GB			
			mssql.x8.large.ro	4 cores, 32 GB			
			mssql.x8.xlarge.ro	8 cores, 64 GB			
			mssql.x8.2xlarge.ro	16 cores, 128 GB			
			mssql.x8.4xlarge.ro	32 cores, 256 GB			
			mssql.x8.7xlarge.ro	56 cores, 480 GB			
mssql.x8.8xlarge.ro	64 cores, 512 GB						



5.3. 旧版skip

 Note

- Primary ApsaraDB RDS for SQL Server instance types

	Data migration solutions			
	Create an ApsaraDB RDS for SQL Server instance			
	Change the specifications of an ApsaraDB RDS for SQL Server instance			
	Migrate an ApsaraDB RDS for SQL Server instance across zones in the same region			
	<div data-bbox="507 965 849 1048" style="background-color: #e1f5fe; padding: 5px;">  Note </div>			
	Switch workloads over between primary and secondary ApsaraDB RDS for SQL Server instances			
	Restart an ApsaraDB RDS for SQL Server instance			
	Set the maintenance window of an ApsaraDB RDS for SQL Server instance			
	Release or unsubscribe from an ApsaraDB RDS for SQL Server instance			
	Manage ApsaraDB RDS for SQL Server instances in the recycle bin			
	DBCC			
	Create an account for an RDS SQL Server instance			
	Reset the password of an account on an ApsaraDB RDS for SQL Server instance			

	Modify the permissions of a standard account on an ApsaraDB RDS for SQL Server instance			
	Grant permissions to the service account of an ApsaraDB RDS for SQL Server instance			
	<div style="border: 1px solid #ccc; background-color: #e1f5fe; padding: 5px; margin-bottom: 5px;"> ? Note </div>			
	Delete an account for an RDS SQL Server instance			
	Create a database on an ApsaraDB RDS for SQL Server instance			
	Delete a database from an ApsaraDB RDS for SQL Server instance			
	Replicate a database of an ApsaraDB RDS instance that runs SQL Server 2012 or later			
	Connect to an ApsaraDB RDS for SQL Server instance			
	Configure endpoints for an RDS instance			
	View and change the internal and public endpoints and port numbers of an ApsaraDB RDS for SQL Server instance			
	Switch an ApsaraDB RDS for SQL Server instance to a different vSwitch			
	Apply for or release a public endpoint on an ApsaraDB RDS for SQL Server instance			
	View the resource metrics and engine metrics of an ApsaraDB RDS for SQL Server instance			
	Set the monitoring frequency of an ApsaraDB RDS for SQL Server instance			

	Configure an alert rule for an ApsaraDB RDS for SQL Server instance			
 Note	Overview of read-only ApsaraDB RDS for SQL Server instances			
	Overview of read/write splitting			
	Modify the read weight of an ApsaraDB RDS for SQL Server instance			
	Configure the read attribute for a secondary RDS instance of a primary ApsaraDB RDS for SQL Server instance			
	Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance			
	Configure SSL encryption on an ApsaraDB RDS for SQL Server instance			
	Configure TDE for an ApsaraDB RDS for SQL Server instance		<ul style="list-style-type: none"> • • 	
	Configure a distributed transaction whitelist for an ApsaraDB RDS for SQL Server instance			
	 Note			
	Configure disk encryption for an ApsaraDB RDS for SQL Server instance			
	Connect an ApsaraDB RDS for SQL Server instance to a self-managed domain			
	Use the SQL Audit feature on an ApsaraDB RDS for SQL Server instance			
	View the error logs of an ApsaraDB RDS for SQL Server instance			

	View the event history of an ApsaraDB RDS instance			
	Back up an ApsaraDB RDS for SQL Server instance			
	Enable snapshot backups for an ApsaraDB RDS for SQL Server instance			
	Enable cross-region backups for an ApsaraDB RDS for SQL Server instance			
	Backup storage fees for an ApsaraDB RDS for SQL Server instance			
	Download the data backup files and log backup files of an ApsaraDB RDS for SQL Server instance			
	Restore the data of an ApsaraDB RDS for SQL Server instance			
	CloudDBA			
	Create tags			
	Delete tags			
	Use tags to filter ApsaraDB RDS for SQL Server instances			

6. Quick start

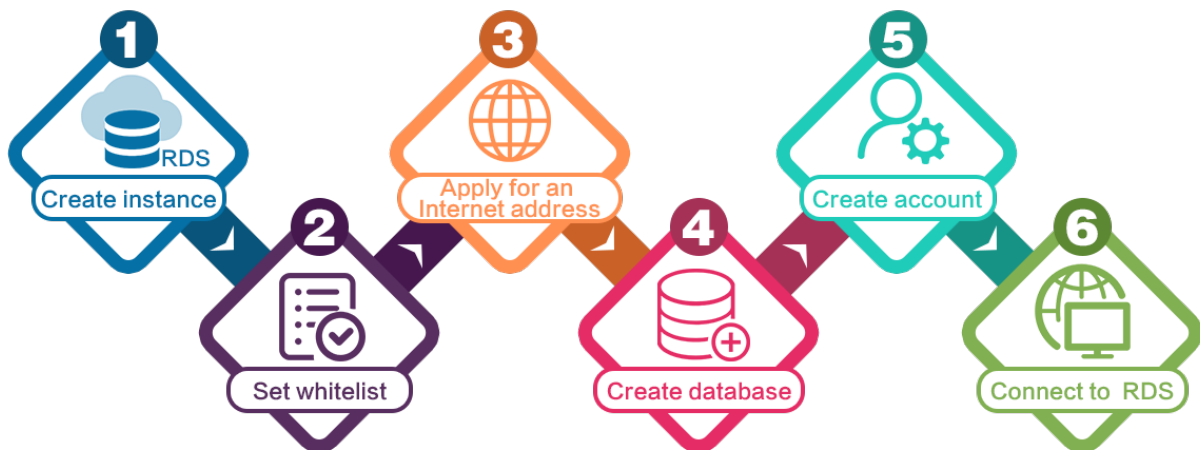
6.1. General workflow to use ApsaraDB RDS for SQL Server

This topic describes how to create and use an ApsaraDB RDS for SQL Server instance.

Quick start flowchart

If this is the first time that you use ApsaraDB RDS for SQL Server, we recommend that you familiarize yourself with the limits of ApsaraDB RDS for SQL Server. For more information, see [Limits of ApsaraDB RDS for SQL Server](#).

The following flowchart shows the operations that you must perform before you use an ApsaraDB RDS for SQL Server instance.



1. [Create an ApsaraDB RDS for SQL Server instance](#)
2. [Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance](#)
3. [Apply for or release a public endpoint on an ApsaraDB RDS for SQL Server instance](#)
4. Create databases and accounts for the RDS instance. For more information, see the following topics:
 - [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2012, 2014, 2016, 2017 SE, or 2019 SE](#)
 - [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2008 R2](#)
5. [Connect to an ApsaraDB RDS for SQL Server instance](#)

6.2. Create an ApsaraDB RDS for SQL Server instance

This topic describes how to create an ApsaraDB RDS for SQL Server instance in the ApsaraDB RDS console. You can also call an API operation to create an ApsaraDB RDS for SQL Server instance.

Billing



For more information, see [Pricing, billable items, and billing methods](#).



Prerequisites

You have an Alibaba Cloud account. For more information, see [Sign up with Alibaba Cloud](#).

Procedure

1. Log on to the [ApsaraDB RDS console](#).
2. Configure the following parameters.

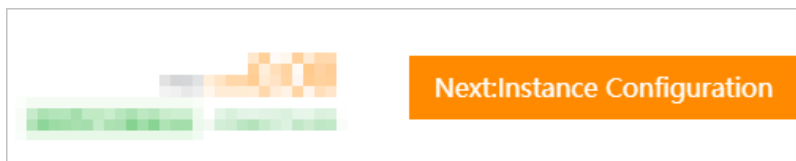
Parameter	Description
Billing Method	<ul style="list-style-type: none"> ◦ Subscription: A subscription instance is an instance that you can subscribe to for a specified period and pay for up front. For long-term use, the subscription billing method is more cost-effective than the pay-as-you-go billing method. You can receive larger discounts for longer subscription periods. ◦ Pay-As-You-Go: A pay-as-you-go instance is charged per hour based on your actual resource usage. The pay-as-you-go billing method is suitable for short-term use. If you no longer need your pay-as-you-go instance, you can release it to reduce costs. <p> Note A maximum of 30 pay-as-you-go RDS instances are allowed per Alibaba Cloud account. To increase this quota, you must submit a ticket.</p>
Region	<p>The region to which the RDS instance belongs.</p> <ul style="list-style-type: none"> ◦ After you confirm the purchase order, you cannot change the selected region. ◦ We recommend that you select a region that is in close proximity to the geographic location where your users reside. This allows you to increase the access speeds of your users. ◦ The RDS instance must reside in the same region as the ECS instance that you want to connect. If the RDS and ECS instances reside in different regions, these instances cannot communicate over an internal network. In this case, these instances must communicate over the Internet and therefore cannot deliver optimal performance.
Database Engine	<p>The database engine and version that the RDS instance runs. Select Microsoft SQL Server. The supported SQL Server versions are 2008 R2, 2012, 2016, 2017, and 2019.</p> <p> Note The available database engines and versions vary based on the region that you select.</p>

Parameter	Description
Edition	<ul style="list-style-type: none"> ◦ Basic: The database system consists of only a primary RDS instance. Computing is separated from storage to increase cost-effectiveness. ◦ High-availability: The database system consists of a primary RDS instance and a secondary RDS instance. These instances work in the high-availability architecture. ◦ Cluster: The database system consists of a primary RDS instance, a secondary RDS instance, and up to seven read-only RDS instances. The read capability of the database system improves with the number of read-only RDS instances. <div style="background-color: #e1f5fe; padding: 10px; margin-top: 10px;"> <p> Note The available RDS editions vary based on the region and database engine version that you select. For more information, see Overview of ApsaraDB RDS editions.</p> </div>
Storage Type	<ul style="list-style-type: none"> ◦ Local SSD: A local SSD resides on the same server as the database engine. You can store data on local SSDs to reduce I/O latency. ◦ Enhanced SSD: An enhanced SSD is an ultra-high performance disk that is developed by Alibaba Cloud based on the next-generation distributed block storage architecture. It integrates 25 Gigabit Ethernet and remote direct memory access (RDMA) technologies. This type of storage media reduces one-way latency and delivers up to 1 million random input/output operations per second (IOPS). Three enhanced SSD options are provided in the ApsaraDB RDS console. Each option represents a specific performance level (PL). <ul style="list-style-type: none"> ▪ ESSD PL1: This option represents an enhanced SSD of PL1. ▪ ESSD PL2: An enhanced SSD of PL2 delivers IOPS and throughput that are twice higher than those delivered by an enhanced SSD of PL1. ▪ ESSD PL3: An enhanced SSD of PL3 delivers IOPS that is 20 times higher than the IOPS delivered by an enhanced SSD of PL1. It also delivers throughput that is 11 times higher than the throughput delivered by an enhanced SSD of PL1. Enhanced SSDs of PL3 are suitable for workloads that require high I/O performance to process concurrent requests. Enhanced SSDs of PL3 are also suitable for workloads that require stable read/write latency. ◦ Standard SSD: A standard SSD is an elastic block storage device that is designed based on the distributed storage architecture. You can store data on standard SSDs to separate computing from storage. <p>For more information, see Storage types.</p> <div style="background-color: #e1f5fe; padding: 10px; margin-top: 10px;"> <p> Note If you select the standard SSD or enhanced SSD storage type, you can enable Disk Encryption. This allows you to maximize protection for your data. For more information, see Configure disk encryption for an ApsaraDB RDS for SQL Server instance.</p> </div>

Parameter	Description
<p>Zone of Primary Node and Zone of Secondary Node</p>	<p>A zone is an independent physical location within a region. The Zone of Primary Node parameter specifies the zone to which the primary RDS instance belongs. The Zone of Secondary Node parameter specifies the zone to which the secondary RDS instance belongs.</p> <p>You can select the Single-zone Deployment or Multi-zone Development method.</p> <ul style="list-style-type: none"> ◦ Single-zone Deployment: If you select this deployment method, the Zone of Primary Node and the Zone of Secondary Node are the same. ◦ Multi-zone Development: This is the recommended deployment method. If you select this deployment method, the Zone of Primary Node and the Zone of Secondary Node are different. This allows you to provide zone-level disaster recovery. You must manually specify the Zone of Primary Node and the Zone of Secondary Node. <div style="background-color: #e1f5fe; padding: 10px; border: 1px solid #cfcfcf;"> <p>Note</p> <ul style="list-style-type: none"> ◦ After the RDS instance is created, you can view information about the RDS instance and its secondary RDS instance on the Service Availability page. ◦ If you select the RDS Basic Edition, the database system consists of only one primary RDS instance and supports only the single-zone deployment method. </div>
<p>Instance Type</p>	<ul style="list-style-type: none"> ◦ General-purpose (Entry-level): specifies the general-purpose instance family. A general-purpose instance exclusively occupies the allocated memory and I/O resources. However, it shares CPU and storage resources with the other general-purpose instances that are deployed on the same server. ◦ Dedicated (Enterprise-level): specifies the dedicated instance family or the dedicated host instance family. A dedicated instance exclusively occupies the allocated CPU, memory, storage, and I/O resources. The dedicated host instance family is the highest configuration of the dedicated instance family. A dedicated host instance exclusively occupies all the CPU, memory, storage, and I/O resources of the server on which the instance is deployed. ◦ Dedicated: A dedicated cluster exclusively occupies all the resources on a VM or physical host. The permissions to manage hosts in a dedicated cluster can be authorized to you. This allows you to create multiple database instances on a host. For more information, see Add hosts. <div style="background-color: #e1f5fe; padding: 10px; border: 1px solid #cfcfcf;"> <p>Note Each instance type supports a specific number of CPU cores, memory capacity, maximum number of connections, and maximum IOPS. For more information, see Primary instance types.</p> </div>

Parameter	Description
Capacity	<p>The storage capacity that is provided for the RDS instance to store data files, system files, binary log files, and transaction files. You can adjust the storage capacity in increments of 5 GB.</p> <p>Note Dedicated instances are allocated exclusive resources. Therefore, the storage capacity of a dedicated instance that is equipped with local SSDs varies based on the instance type. For more information, see Primary ApsaraDB RDS instance types.</p>

3. Click **Next: Instance Configuration**.
4. In the lower-right corner of the page, click **Next: Instance Configuration**.



5. Configure the following parameters.

Parameter	Description
Network Type	<p>Set the network type.</p> <ul style="list-style-type: none"> ◦ Classic Network: the traditional type of network. ◦ VPC: the recommended type of network. A virtual private cloud (VPC) is an isolated virtual network that provides higher security and higher performance than the classic network. <p>After you select the VPC network type, you must specify the VPC and VSwitch of Primary Node parameters. If you set the Deployment Method parameter in the previous step to Multi-zone deployment, you must also specify the VSwitch of Secondary Node parameter.</p> <p>Note The RDS instance must have the same network type as the ECS instance that you want to connect. If the RDS and ECS instances both have the VPC network type, these instances must also reside in the same VPC. Otherwise, these instances cannot communicate over an internal network.</p>

6. Click **Next: Confirm Order**.
7. Confirm the settings in the **Parameters** section, specify the **Purchase Plan** parameter and the **Duration** parameter, read and select Terms of Service, and then click **Pay Now** to complete the payment. You must specify the Duration parameter only when the RDS instance uses the subscription billing method.

Note When you create a subscription RDS instance, we recommend that you select Auto-Renew Enabled. This relieves the need to manually renew the RDS instance on a regular basis. This also allows you to avoid interruptions to your workloads due to overdue payments.

The screenshot displays the 'Confirm Order' step in the ApsaraDB RDS console. The interface is divided into three main sections: 'Basic Configuration', 'Instance Configuration', and 'Confirm Order'. The 'Purchase Plan' section is highlighted with a red box and includes the following details:

- Purchase Plan:** A quantity of 1 instance.
- Duration:** A dropdown menu with options for 1 Month, 2 Months, 3 Months, 6 Months, 1 Year, 2 Year, 3 Year, 4 Year, and 5 Year. The '1 Year' option is currently selected.
- Auto-Renew:** A checkbox labeled 'Auto-Renew Enabled' which is checked.
- Terms of Service:** A link to 'Terms of Service' and a note: 'Subscription instances enjoy 5-day money-back guarantee. | Usage Instructions'.

On the ApsaraDB RDS homepage, click **Instances** in the left-side navigation pane, select the region where the RDS instance resides in the top navigation bar, and then find the RDS instance based on the **Creation Time**.

What to do next

After the RDS instance is created, you must specify whitelist settings and create accounts on the RDS instance. If you want to connect to the RDS instance over the Internet, you must also apply for a public endpoint. After you connect to the RDS instance, you can migrate data to the RDS instance. For more information, see the following topics:

- [Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance](#)
- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2008 R2](#)
- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2012, 2014, 2016, 2017 SE, or 2019 SE](#)
- [Create accounts and databases for an ApsaraDB RDS instance that runs SQL Server 2017 EE or 2019 EE](#)
- [Apply for or release a public endpoint on an ApsaraDB RDS for SQL Server instance](#)
- [Connect to an ApsaraDB RDS for SQL Server instance](#)

FAQ

- After I submit the order for purchasing an RDS instance, why does the ApsaraDB RDS console not respond and why am I unable to find the created RDS instance?

The issue may occur due to the following reasons:

- The RDS instance does not reside in the region that you selected.

In the top navigation bar, select the region where the RDS instance resides. Then, you can find the RDS instance.

- The zone that you selected cannot provide sufficient resources.

Resources in zones are dynamically allocated. After you submit the purchase order, the zone that you selected may be unable to provide sufficient resources. As a result, the RDS instance cannot be created. We recommend that you select a different zone and try again. If the RDS instance still cannot be created, you can go to the [Orders page](#) in the Billing Management console to view the refunded fee.

- How do I authorize a RAM user to manage my RDS instance?

For more information, see [Use RAM to manage ApsaraDB RDS permissions](#).

Related operations

Operation	Description
Create an instance	Creates an ApsaraDB RDS instance.

6.3. Set a whitelist

6.3.1. Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance

This topic describes how to configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance. After an RDS instance is created, you must configure IP address whitelists or security groups for the instance. A device can access the RDS instance only after you add the IP address of the device to an IP address whitelist or security group of the RDS instance.

For more information about how to configure an IP address whitelist for an RDS instance that runs a different database engine, see the following topics:

- [Configure an IP address whitelist for an ApsaraDB RDS for MySQL instance](#)
- [Configure an IP address whitelist for an ApsaraDB RDS for PostgreSQL instance](#)
- [Configure an IP address whitelist for an ApsaraDB RDS for MariaDB TX instance](#)

Scenarios

An IP address whitelist of an RDS instance consists of IP addresses and CIDR blocks that are granted access to the RDS instance. You can configure IP address whitelists for an RDS instance to provide high-level access control and security protection for the RDS instance. We recommend that you update the configured IP address whitelists on a regular basis.

You can configure an IP address whitelist in the following scenarios:


- Scenario 1


After an RDS instance is created, you must add the IP addresses of specific devices to an IP address whitelist of the RDS instance. These devices can access the RDS instance only after the IP addresses of these devices are added to an IP address whitelist of the RDS instance.

- Scenario 2

An RDS instance cannot be connected. You must check whether the IP address whitelists of the instance are correctly configured.

The following table provides the IP address whitelist configurations in various connection scenarios.

 **Note** A virtual private cloud (VPC) is an isolated network on Alibaba Cloud and provides higher security than the classic network. For more information, see [What is a VPC?](#)

Connection scenario	Network type	IP address whitelist configuration
Connect an Elastic Compute Service (ECS) instance to an RDS instance	The ECS instance and the RDS instance reside in the same VPC. This is the recommended connection scenario.	Add the private IP address of the ECS instance to an IP address whitelist of the RDS instance.
	The ECS instance and the RDS instance reside in different VPCs.	Instances in different VPCs cannot communicate with each other over internal networks. Make sure that the ECS instance and the RDS instance reside in the same VPC and add the private IP address of the ECS instance to an IP address whitelist of the RDS instance.
	The ECS instance and the RDS instance reside in the classic network.	Add the private IP address of the ECS instance to an IP address whitelist of the RDS instance.
	The ECS instance resides in the classic network. The RDS instance resides in a VPC.	<p>Instances of different network types cannot communicate with each other over internal networks. Perform the following operations:</p> <ol style="list-style-type: none"> i. Migrate the ECS instance from the classic network to the VPC to which the RDS instance belongs. For more information, see Migrate an ECS instance from the classic network to a VPC. <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 10px; margin: 10px 0;"> <p> Note This operation is supported only when the ECS instance and the RDS instance reside in the same region. If the ECS instance and the RDS instance reside in different regions, we recommend that you use Data Transmission Service (DTS) to migrate the RDS instance to the region where the ECS instance resides. This way, you can ensure the stability of your database service. For more information, see Migrate data between ApsaraDB RDS for SQL Server instances.</p> </div> <ol style="list-style-type: none"> ii. Add the private IP address of the ECS instance to an IP address whitelist of the RDS instance.

Connection scenario	Network type	IP address whitelist configuration
	<p>The ECS instance resides in a VPC.</p> <p>The RDS instance resides in the classic network.</p>	<p>Instances of different network types cannot communicate with each other over internal networks. Perform the following operations:</p> <ol style="list-style-type: none"> i. Migrate the RDS instance from the classic network to the VPC to which the ECS instance belongs. For more information, see Change the network type of an ApsaraDB RDS for SQL Server instance. <div style="background-color: #e1f5fe; padding: 10px; margin: 10px 0;"> <p>Note This operation is supported only when the ECS instance and the RDS instance reside in the same region. If the ECS instance and the RDS instance reside in different regions, we recommend that you use DTS to migrate the RDS instance to the region where the ECS instance resides. This way, you can ensure the stability of your database service. For more information, see Migrate data between ApsaraDB RDS for SQL Server instances.</p> </div> <ol style="list-style-type: none"> ii. Add the private IP address of the ECS instance to an IP address whitelist of the RDS instance.
<p>Connect a self-managed host outside the cloud to an RDS instance</p>	<p>None</p>	<p>Add the public IP address of the self-managed host to an IP address whitelist of the RDS instance.</p> <div style="background-color: #e1f5fe; padding: 10px; margin: 10px 0;"> <p>Note</p> <ul style="list-style-type: none"> ○ The applications that run on the self-managed host connect to the public endpoint of the RDS instance. ○ For more information about how to obtain the public IP address of the self-managed host, see How SQL Server determines the public IP address of an external Server or client </div>

Procedure


What to do next

- [Create accounts and databases for an ApsaraDB RDS instance that runs SQL Server 2017 EE or 2019 EE](#)
- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2012, 2014, 2016, 2017 SE, or 2019 SE](#)
- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2008 R2](#)

6.3.2. Errors and FAQ about IP address whitelist settings in ApsaraDB RDS for SQL Server

This topic describes the common errors and provides answers to some commonly asked questions about the IP address whitelist settings of an ApsaraDB RDS for SQL Server instance.

Common errors

Error	Description	Solution
No IP address whitelists are configured. Your RDS instance has only one default IP address whitelist. The default IP address whitelist contains only the 127.0.0.1 IP address.	The 127.0.0.1 IP address indicates that no devices can access your RDS instance.	Add the IP addresses of the specified devices to an IP address whitelist.
The 0.0.0.0 entry is added to an IP address whitelist during a connectivity test.	The format of the 0.0.0.0 entry is invalid.	Change the 0.0.0.0 IP address to the 0.0.0.0/0 Classless Inter-Domain Routing (CIDR) block. <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;"> <p> Notice The 0.0.0.0/0 CIDR block indicates that all IP addresses are granted access to your RDS instance. We recommend that you add this CIDR block only for a connectivity test. When you run online workloads, do not add this CIDR block to an IP address whitelist.</p> </div>
The public IP addresses in a configured IP address whitelist are inaccessible.	<ul style="list-style-type: none"> The public IP addresses dynamically change. The tool or website that you use to query public IP addresses returns inaccurate results. 	For more information, see How SQL Server determines the public IP address of an external Server or client .

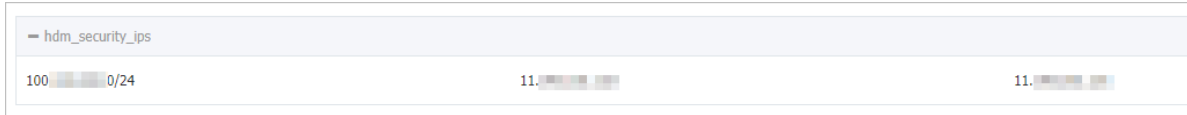
FAQ

- After I configure an IP address whitelist for my RDS instance, does the IP address whitelist immediately take effect?

After you configure an IP address whitelist for your RDS instance, the IP address whitelist requires about 1 minute to take effect.

- What are the IP address whitelists labeled `ali_dms_group` and `hdm_security_ips`?

When you connect to your RDS instance from other Alibaba Cloud services, these services generate IP address whitelists upon your authorization. The generated IP address whitelists contain the IP addresses of the servers on which these services run. The IP address whitelist labeled `ali_dms_group` is generated by [Data Management \(DMS\)](#). The IP address whitelist labeled `hdm_security_ips` is generated by Database Autonomy Service (DAS). Do not modify or delete the IP address whitelists. If you modify or delete the IP address whitelists, these services cannot access your RDS instance. These services do not perform operations on your business data.



- If I disable Internet access and enable only internal network access, is my RDS instance exposed to security risks? We recommend that you migrate your RDS instance to a virtual private cloud (VPC). For more information, see [Change the network type of an ApsaraDB RDS for SQL Server instance](#).

6.4. Create databases and accounts

6.4.1. Create accounts and databases for an ApsaraDB RDS instance that runs SQL Server 2017 EE or 2019 EE

This topic describes how to create accounts and databases for an ApsaraDB RDS instance that runs SQL Server 2017 EE or 2019 EE.

Prerequisites

Your RDS instance runs SQL Server 2017 EE or 2019 EE.

Note For more information about how to create accounts and databases for an RDS instance that runs a different SQL Server version, see the following topics:

- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2012, 2014, 2016, 2017 SE, or 2019 SE](#)
- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2008 R2](#)

Precautions

- Databases on the same RDS instance share all the resources that belong to the RDS instance. You can manage standard accounts and databases by using SQL statements.
- You must follow the principle of least privilege to create accounts and grant the read-only permissions or the read and write permissions to the accounts based on the required roles. If necessary, you can create more than one account and grant each account only the permissions to access the data of specific databases within its authorized workloads. If an account does not need to write data to a database, you must grant only the read-only permissions on the database to the account.
- For security purposes, we recommend that you configure strong passwords for the created accounts and change the passwords on a regular basis.

Create an account

- 1.
2. In the left-side navigation pane, click **Accounts**.
3. Click **Create Account**.
4. Configure the following parameters.


Parameter	Description		
Database Account :	Enter the username of the account. The username must be 2 to 64 characters in length. It can contain lowercase letters, digits, and underscores (_). It must start with a lowercase letter and end with a lowercase letter or a digit.		
Account Type:	<ul style="list-style-type: none"> ◦ Privileged Account : You can select the Privileged Account option only when the account is the first account that you create for your RDS instance. This is because the first account that you create must be a privileged account. Each RDS instance can have only one privileged account. The privileged account of an RDS instance cannot be deleted. ◦ Standard Account : You can select the Standard Account option only after you have created a privileged account for your RDS instance. Each RDS instance can have more than one standard account. You must manually grant the permissions on specific databases to each standard account. 		
Authorized Databases :	<p>Select the authorized databases of the account. If no databases are created, you can leave this parameter empty.</p> <p>You can perform the following steps to grant the permissions on more than one database to the account:</p> <ol style="list-style-type: none"> In the Unauthorized Databases section, select the required databases. Click the > icon to move the selected databases to the Authorized Databases: section. In the Authorized Databases section, specify the permissions that the account will be granted on each authorized database. The supported permissions are Read/Write (DML), Read-only, and Owner. <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Note The account is authorized to create tables, delete tables, and modify schemas in a database only when it has the Owner permissions on the database.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Authorized Databases:</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="border: 1px solid #ccc; width: 50%; padding: 5px;">Unauthorized Databases</td> <td style="border: 1px solid #ccc; width: 50%; padding: 5px;"> Authorized Databases: <input type="checkbox"/> tetete <input checked="" type="radio"/> Read/Write (DML) <input type="radio"/> Read-only <input type="radio"/> Owner </td> </tr> </table> </div>	Unauthorized Databases	Authorized Databases: <input type="checkbox"/> tetete <input checked="" type="radio"/> Read/Write (DML) <input type="radio"/> Read-only <input type="radio"/> Owner
Unauthorized Databases	Authorized Databases: <input type="checkbox"/> tetete <input checked="" type="radio"/> Read/Write (DML) <input type="radio"/> Read-only <input type="radio"/> Owner		
Password :	<p>Enter the password of the account. The password must meet the following requirements:</p> <ul style="list-style-type: none"> ◦ The password must be 8 to 32 characters in length. ◦ The password must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. ◦ The password can contain any of the following special characters: ! @ # \$ % ^ & * () _ + - = 		
Confirm Password :	Enter the password of the account again.		

Parameter	Description
Description	Enter a description that is used to identify the account. The description can be up to 256 characters in length.

5. Click **OK**.

Create a database

- 1.
2. In the left-side navigation pane, click **Databases**.
3. Click **Create Database**.
4. Configure the following parameters.

Parameter	Description
Database Name	Enter the name of the database. The name must be 2 to 64 characters in length. It can contain letters, digits, underscores (_), and hyphens (-). It must start with a letter and end with a letter or a digit.
Supported Character Set	Select the character set that is supported by the database.
Authorized Account:	<p>Select the account to which you want to grant the permissions on the database. Then, you must set the Account Type parameter to Read/Write, Read-only, or Owner.</p> <p>If no accounts are created, you can leave this parameter empty.</p> <div style="background-color: #e0f2f7; padding: 5px; border: 1px solid #ccc;"> <p> Note An account is authorized to create tables, delete tables, and modify schemas in a database only when it has the Owner permissions on the database.</p> </div>
Description	Enter a description that is used to identify the database. The description can be up to 256 characters in length.

5. Click **Create**.

FAQ

After I create accounts on my primary RDS instance, can I manage the accounts on its read-only RDS instances?

No, although the accounts created on your primary RDS instance are synchronized to its read-only RDS instances, you cannot manage the accounts on the read-only RDS instances. The accounts have only read permissions on the read-only RDS instances.


6.4.2. Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2012, 2016, 2017 SE, or 2019 SE

This topic describes how to create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2012, 2016, 2017 SE, or 2019 SE. You can create accounts and databases by using the ApsaraDB RDS console.

Prerequisites

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

- SQL Server 2012
- SQL Server 2016
- SQL Server 2017 SE
- SQL Server 2019 SE

 **Note** For more information about how to create an account and a database for an RDS instance that runs a different SQL Server version, see the following topics:

- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2017 EE or 2019 EE](#)
- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2008 R2](#)

Create an account

You can create both privileged accounts and standard accounts by using the ApsaraDB RDS console. Take note of that you can create a privileged account only by using the ApsaraDB RDS console.

Precautions

- Databases on the same RDS instance share all the resources that belong to the RDS instance. You can manage standard accounts and databases by using SQL statements.
- You must follow the principle of least privilege to create accounts and grant the read-only permissions or the read and write permissions to the accounts based on the required roles. If necessary, you can create more than one account and grant each account only the permissions to access the data of specific databases within its authorized workloads. If an account does not need to write data to a database, you must grant only the read-only permissions on the database to the account.
- For security purposes, we recommend that you configure strong passwords for the created accounts and change the passwords on a regular basis.

Procedure

- 1.
2. In the left-side navigation pane, click **Accounts**.
3. Click **Create Account**.
4. Configure the following parameters.


Parameter	Description
Database Account :	Enter the username of the account. The username must be 2 to 64 characters in length. It can contain lowercase letters, digits, and underscores (_). It must start with a lowercase letter and end with a lowercase letter or a digit.
Account Type:	<ul style="list-style-type: none"> ◦ Privileged Account : You can select the Privileged Account option only when the account is the first account that you create for your RDS instance. This is because the first account that you create must be a privileged account. Each RDS instance can have only one privileged account. The privileged account of an RDS instance cannot be deleted. ◦ Standard Account : You can select the Standard Account option only after you have created a privileged account for your RDS instance. Each RDS instance can have more than one standard account. You must manually grant the permissions on specific databases to each standard account.
Authorized Databases :	<p>Select the authorized databases of the account. If no databases are created, you can leave this parameter empty.</p> <p>You can perform the following steps to grant the permissions on more than one database to the account:</p> <ol style="list-style-type: none"> In the Unauthorized Databases section, select the required databases. Click the > icon to move the selected databases to the Authorized Databases: section. In the Authorized Databases section, specify the permissions that the account will be granted on each authorized database. The supported permissions are Read/Write (DML), Read-only, and Owner. <div style="background-color: #e1f5fe; padding: 10px; margin: 10px 0;"> <p>Note The account is authorized to create tables, delete tables, and modify schemas in a database only when it has the Owner permissions on the database.</p> </div> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Authorized Databases:</p> <div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid #ccc; padding: 5px; width: 45%;"> <p>Unauthorized Databases</p> </div> <div style="border: 1px solid #ccc; padding: 5px; width: 45%;"> <p>Authorized Databases:</p> <p><input type="checkbox"/> tetete <input checked="" type="radio"/> Read/Write (DML) <input type="radio"/> Read-only <input type="radio"/> Owner</p> </div> </div> </div>
Password :	<p>Enter the password of the account. The password must meet the following requirements:</p> <ul style="list-style-type: none"> ◦ The password must be 8 to 32 characters in length. ◦ The password must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. ◦ The password can contain any of the following special characters: ! @ # \$ % ^ & * () _ + - =
Confirm Password :	Enter the password of the account again.

Parameter	Description
Description	Enter a description that is used to identify the account. The description can be up to 256 characters in length.

5. Click **OK**.

Create a database

- 1.
2. In the left-side navigation pane, click **Databases**.
3. Click **Create Database**.
4. Configure the following parameters.

Parameter	Description
Database Name	Enter the name of the database. The name must be 2 to 64 characters in length. It can contain letters, digits, underscores (_), and hyphens (-). It must start with a letter and end with a letter or a digit.
Supported Character Set	Select the character set that is supported by the database.
Authorized Account:	<p>Select the account to which you want to grant the permissions on the database. Then, you must set the Account Type parameter to Read/Write, Read-only, or Owner.</p> <p>If no accounts are created, you can leave this parameter empty.</p> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #d9e1f2;"> <p> Note An account is authorized to create tables, delete tables, and modify schemas in a database only when it has the Owner permissions on the database.</p> </div>
Description	Enter a description that is used to identify the database. The description can be up to 256 characters in length.


5. Click **Create**.

6.4.3. Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2008 R2

This topic describes how to create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2008 R2. You can create accounts and databases by using the ApsaraDB RDS console.

Prerequisites

Your RDS instance runs SQL Server 2008 R2.

 **Note** For more information about how to create an account and a database for an RDS instance that runs a different SQL Server version, see the following topics:

- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2017 EE or 2019 EE](#)
- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2012, 2014, 2016, 2017 SE, or 2019 SE](#)

Create an account

Precautions

- Databases on the same RDS instance share all the resources that belong to the RDS instance. You can manage standard accounts and databases by using SQL statements.
- You must follow the principle of least privilege to create accounts and grant the read-only permissions or the read and write permissions to the accounts based on the required roles. If necessary, you can create more than one account and grant each account only the permissions to access the data of specific databases within its authorized workloads. If an account does not need to write data to a database, you must grant only the read-only permissions on the database to the account.
- For security purposes, we recommend that you configure strong passwords for the created accounts and change the passwords on a regular basis.

Procedure

- 1.
2. In the left-side navigation pane, click **Accounts**.
3. Click **Create Account**.
4. Configure the following parameters.

Parameter	Description
Database Account	<ul style="list-style-type: none"> ◦ The username of the account must be 2 to 64 characters in length and can contain lowercase letters, digits, and underscores (_). ◦ The username of the account must start with a lowercase letter and end with a lowercase letter or a digit. ◦ The username cannot be the same as the username of an existing account.
Account Type	<ul style="list-style-type: none"> ◦ If your RDS instance uses local SSDs, select Standard Account. ◦ If your RDS instance uses standard or enhanced SSDs, select Privileged Account or Standard Account.

Parameter	Description
Authorized Databases	<p>Select the authorized databases of the account. If no databases are created, you can leave this parameter empty.</p> <p>You can perform the following steps to grant the permissions on more than one database to the account:</p> <ol style="list-style-type: none"> In the Unauthorized Databases section, select the required databases. Click the > icon to move the selected databases to the Authorized Databases: section. In the Authorized Databases section, specify the permissions that the account will be granted on each authorized database. The supported permissions are Read/Write and Read-only.
Password	<p>Enter the password of the account. The password must meet the following requirements:</p> <ul style="list-style-type: none"> ○ The password must be 8 to 32 characters in length. ○ The password must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. ○ The password can contain any of the following special characters: ! @ # \$ % ^ & * () _ + - =
Confirm 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.

5. Click **OK**.

Create a database

- 1.
2. In the left-side navigation pane, click **Databases**.
3. Click **Create Database**.
4. Configure the following parameters.

Parameter	Description
Database Name	Enter the name of the database. The name must be 2 to 64 characters in length. It can contain letters, digits, underscores (_), and hyphens (-). It must start with a letter and end with a letter or a digit.
Supported Character Set	Select the character set that is supported by the database. You can also select all and then select a character set from the drop-down list that appears.

Parameter	Description
Authorized Account	Select the authorized account of the database. If no accounts are created, you can leave this parameter empty.
Account Type	Specify the type of the authorized account. This parameter appears only after you select an authorized account. You can set this parameter to Read/Write , Read-only , or Owner .
Description	Enter a description that helps identify the database. The description can be up to 256 characters in length.

5. Click **Create**.

References

[Migrate data from an on-premises database to ApsaraDB RDS SQL Server 2008 R2 using full backup files](#)

6.5. Connect to an ApsaraDB RDS for SQL Server instance

This topic describes how to connect to an ApsaraDB RDS for SQL Server instance. After you complete the initial configuration for an RDS instance, you can connect to the RDS instance from your Elastic Compute Service (ECS) instance or your computer.

Prerequisites

- [Create an ApsaraDB RDS for SQL Server instance](#)
- [Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance](#)
- [Create an account for an RDS SQL Server instance](#)


Use DMS to connect to an RDS instance

Data Management (DMS) is a graphical data management service that provides various features for you to manage relational databases and NoSQL databases. These features include data management, schema management, user authorization, security audit, trend analysis, data tracking, business intelligence (BI) charting, and performance analysis and optimization.

For more information, see [Use DMS to log on to an ApsaraDB RDS for SQL Server instance](#).

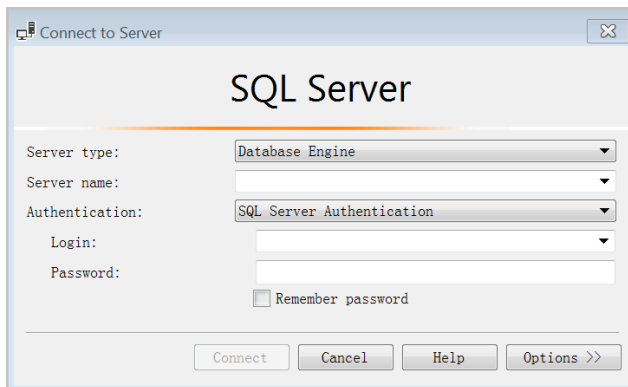
Use a database client to connect to an RDS instance

In this section, the Microsoft SQL Server Management Studio (SSMS) client is used as an example. For more information, visit the [Microsoft SQL Server Management Studio](#) page.

 **Note** We recommend that you download the latest version of SSMS to support all SQL Server versions.

1. Start the SSMS client on your ECS instance or your computer.
2. Choose **Connect > Database Engine**.
3. In the **Connect to Server** dialog box, enter the information that is used to log on to the RDS

instance.



Parameter	Description
Server type	Select Database Engine .
Server name	Enter the endpoint and port number that are used to connect to the RDS instance. The endpoint and the port number are separated by a comma (,). Example: <code>rm-bptest.sqlserver.rds.aliyuncs.com,3433</code> . For more information about how to view the internal and public endpoints and port numbers of an RDS instance, see View and change the internal and public endpoints and port numbers of an ApsaraDB RDS for SQL Server instance .
Authentication	Select SQL Server Authentication .
Login	Enter the username of the account that is authorized to log on to the RDS instance.
Password	Enter the password of the preceding account.

4. Click **Connect**.

FAQ

How do I use Function Compute to obtain data from my RDS instance?

You can install third-party dependencies on Function Compute. Then, you can obtain data from your RDS instance by using the built-in modules that are provided by the third-party dependencies in Function Compute. For more information, see [Install third-party dependencies on Function Compute](#).

6.6. Read-only instances

6.6.1. Overview of read-only ApsaraDB RDS for SQL Server instances

This topic provides an overview of read-only ApsaraDB RDS for SQL Server instances. If your database system receives a small number of write requests but a large number of read requests, the primary RDS instance may be overwhelmed by the read requests and your workloads may be interrupted. In this case, you can create one or more read-only RDS instances to offload read requests from the primary RDS instance. This increases the read capability of your database system and the throughput of your application.

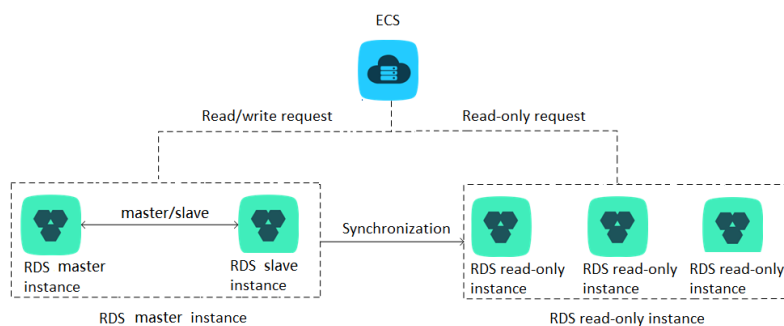
Background information

When you create a read-only RDS instance, it replicates data from the secondary RDS instance to the read-only RDS instance. The data of the created read-only RDS instance is consistent with that of the primary RDS instance. Data updates on the primary RDS instance are synchronized to all the read-only RDS instances that are attached with the primary RDS instance.

Note

- You can create read-only RDS instances only when the primary RDS instance runs SQL Server 2017 EE or 2019 EE.
- Each read-only RDS instance runs in a single-node architecture. In this architecture, no secondary RDS instance is provided as a standby for a read-only RDS instance.

The following figure shows the topology of read-only RDS instances.



Billing

Read-only RDS instances are charged on a pay-as-you-go or subscription basis. For more information about pricing, see [Read-only ApsaraDB RDS instance types](#).

Features

- Read-only RDS instances support both the pay-as-you-go and subscription billing methods. The pay-as-you-go billing method is flexible, and allows you to release your read-only RDS instances when the instances are no longer needed. The subscription billing method is cost-effective for long-term commitments.
- Read-only RDS instances reside in the same region as the primary RDS instance, but possibly in different zones.
- The specifications of read-only RDS instances can differ from the specifications of the primary RDS instance. You can change the specifications of read-only RDS instances at any time. We recommend that the specifications of read-only RDS instances be higher than or equal to the specifications of the primary RDS instance. If the specifications of a read-only RDS instance are lower than the specifications of the primary RDS instance, the read-only RDS instance may encounter issues such as high latency or heavy load.

- The network types of read-only RDS instances can differ from the network type of the primary RDS instance.
- You do not need to manage accounts or databases on read-only RDS instances. The account and database data on read-only RDS instances is synchronized from the primary RDS instance.
- When you create a read-only RDS instance, ApsaraDB RDS replicates the IP address whitelists of the primary RDS instance to the read-only RDS instance. However, the IP address whitelists on the read-only RDS instance are independent of the IP address whitelists on the primary RDS instance. For more information about how to modify the IP address whitelists of a read-only RDS instance, see [Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance](#).
- Read-only RDS instances support monitoring and alerting. You can monitor about 20 metrics, such as the disk usage, input/output operations per second (IOPS), number of connections, CPU utilization, and network traffic.

Limits

- You can create up to seven read-only RDS instances for each primary RDS instance.
- You cannot configure backup policies or manually create backups for read-only RDS instances. These are configured and created on the primary RDS instance.
- You cannot create a temporary RDS instance from a data backup file or to a specific point in time. In addition, you cannot overwrite the data of a read-only RDS instance by using a data backup file.
- After a read-only RDS instance is created, you cannot use a data backup file to overwrite the data on the primary RDS instance.
- You cannot migrate data to read-only RDS instances.
- You cannot create or delete databases on read-only RDS instances.
- You cannot create or delete accounts, grant the permissions on specific databases to accounts, or change the passwords of accounts on read-only RDS instances.

FAQ

After I create accounts on my primary RDS instance, can I manage the accounts on the read-only RDS instances?

No, although the accounts created on the primary RDS instance are replicated to its read-only RDS instances, you cannot manage the accounts on the read-only RDS instances. The accounts have only the read permissions on the read-only RDS instances.

6.6.2. Create a read-only ApsaraDB RDS for SQL Server instance

This topic describes how to create a read-only ApsaraDB RDS for SQL Server instance. Read-only RDS instances allow your database system to process a large number of read requests. This increases the throughput of your application. Each read-only RDS instance is a replica of the primary RDS instance. This means that each read-only RDS instance has the same data as the primary RDS instance. Data updates on the primary RDS instance are also synchronized to each read-only RDS instance.

For more information about read-only RDS instances, see [Overview of read-only ApsaraDB RDS for SQL Server instances](#).

Prerequisites

The primary RDS instance runs SQL Server 2017 EE or 2019 EE.

Precautions

- You can create read-only RDS instances for the primary RDS instance. However, you cannot convert existing RDS instances into read-only RDS instances.
- When you create a read-only RDS instance, ApsaraDB RDS replicates data from the secondary RDS instance to the read-only RDS instance. This prevents interruptions to your workloads on the primary RDS instance.
- You can create up to seven read-only RDS instances for each primary RDS instance.
- Read-only RDS instances support both the pay-as-you-go and subscription billing methods. For more information, see [Overview of read-only ApsaraDB RDS for SQL Server instances](#).

Create a read-only RDS instance



- 1.
2. In the **Distributed by Instance Role** section of the **Basic Information** page, click **Add**.

Note If you are using the original ApsaraDB RDS console, click **Create Read-only Instance**.

Basic Information	Configure Whitelist
Instance ID	rm-bp-XXXXXX
Zone ?	China (Hangzhou) ZoneH
Network Type	VPC See Detail
Advanced Feature:	Linked Server, Distributed Transaction
Time Zone:	China Standard Time
Distributed by Instance Role	
Read-only Instance ?	2 Add

3. Configure the following parameters and click **Next : Instance Configuration**.

Parameter	Description
-----------	-------------

Parameter	Description
Storage Type	<ul style="list-style-type: none"> ◦ Standard SSD: A standard SSD is an elastic block storage device that is designed based on the distributed storage architecture. You can store data on standard SSDs to separate computing from storage. ◦ Enhanced SSD: An enhanced SSD is an ultra-high performance disk that is designed by Alibaba Cloud based on the next-generation distributed block storage architecture. It integrates 25 Gigabit Ethernet and remote direct memory access (RDMA) technologies. This reduces one-way latency and delivers up to 1 million random input/output operations per second (IOPS). Supported enhanced SSDs come in the following three performance levels (PLs): <ul style="list-style-type: none"> ■ PL1: An enhanced SSD of PL1 is a regular enhanced SSD. ■ PL2: An enhanced SSD of PL2 delivers IOPS and throughput that are about twice higher than those delivered by an enhanced SSD of PL1. ■ PL3: An enhanced SSD of PL3 delivers IOPS that is 20 times higher than the IOPS delivered by an enhanced SSD of PL1. It also delivers throughput that is 11 times higher than the throughput delivered by an enhanced SSD of PL1. Enhanced SSDs of PL3 are ideal for workloads that require high I/O performance in processing concurrent requests and high stability in read and write latencies. <p>For more information about storage types, see Storage types.</p>
Zone	<p>The zone where the read-only RDS instance resides. Each zone is an independent physical location within a region.</p>
Instance Type	<ul style="list-style-type: none"> ◦ General-purpose (Entry-level): belongs to the general-purpose instance family. A general-purpose instance exclusively occupies the allocated memory and I/O resources. However, it shares CPU and storage resources with the other general-purpose instances that are deployed on the same server. ◦ Dedicated Instance (Enterprise-level): belongs to the dedicated instance family or the dedicated host instance family. A dedicated instance exclusively occupies the allocated CPU, memory, storage, and I/O resources. The dedicated host instance family is the top configuration of the dedicated instance family. A dedicated host instance occupies all the CPU, memory, storage, and I/O resources on the server where it is deployed. <div style="background-color: #e6f2ff; padding: 10px; margin-top: 10px;"> <p> Note Each instance type supports a specific number of cores, memory capacity, maximum number of connections, and maximum IOPS. For more information, see Primary ApsaraDB RDS instance types.</p> </div>
Capacity	<p>The storage capacity that the read-only RDS instance has available to store data files, system files, binary log files, and transaction files. The storage capacity increases in increments of 5 GB.</p> <div style="background-color: #e6f2ff; padding: 10px; margin-top: 10px;"> <p> Note The dedicated instance family supports exclusive allocations of resources. Therefore, the storage capacity of each instance type with local SSDs in this family is fixed. For more information, see Primary ApsaraDB RDS instance types.</p> </div>

Note If you want to ensure the I/O performance that is required for data synchronization, we recommend that the specifications of the read-only RDS instance be higher than or equal to the specifications of the primary RDS instance. In this situation, the specifications refer to the memory capacity.

4. Configure the following parameters.

Parameter	Description
Network Type	<ul style="list-style-type: none"> Classic Network: the traditional type of network. VPC: A virtual private cloud (VPC) is an isolated network that provides higher security and better performance than the classic network. If you select the VPC network type, you must also specify the VPC parameter and the vSwitch of Primary Node parameter. <p>Note The read-only RDS instance must have the same network type as the Elastic Compute Service (ECS) instance to which you want to connect. If both the read-only RDS instance and the ECS instance use the VPC network type, make sure that they reside in the same VPC. Otherwise, they cannot communicate over an internal network.</p>
Resource Group	The resource group to which the read-only RDS instance belongs.

5. Click **Next: Confirm Order**, confirm the settings in the **Parameters** section, specify the **Purchase Plan** parameter, read and select Terms of Service, click **Pay Now**, and then complete the payment.

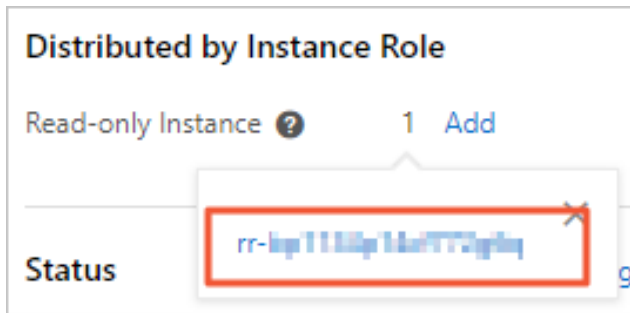
A few minutes are required to create the read-only RDS instance.

View a read-only RDS instance

- To view a read-only RDS instance on the Instances page, perform the following steps:
 - Log on to the [ApsaraDB RDS console](#). In the left-side navigation pane, click **Instances**. In the top navigation bar, select the region where the read-only RDS instances reside.
 - Find the read-only RDS instance and click its ID.



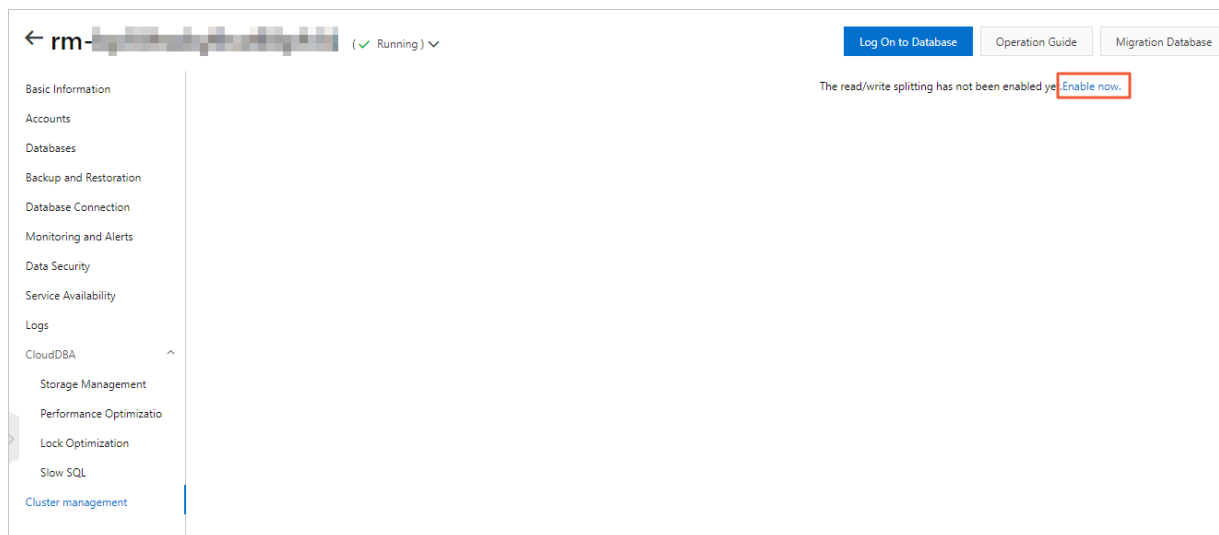
- To view a read-only RDS instance on the Basic Information page of the primary RDS instance, perform the following steps:
 - Log on to the [ApsaraDB RDS console](#). In the left-side navigation pane, click **Instances**. In the top navigation bar, select the region where the primary RDS instance resides.
 - Find the primary RDS instance and click its ID.
 - On the **Basic Information** page, move the pointer over the number of read-only RDS instances and click the ID of the read-only RDS instance that you want to view.



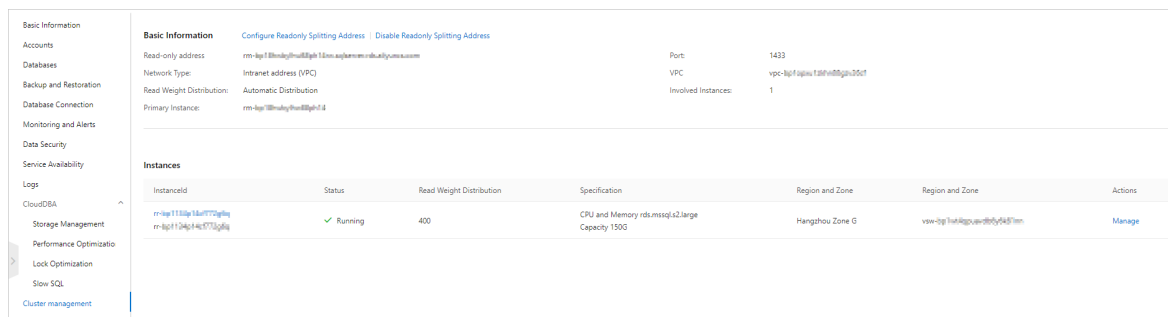
View a read-only RDS instance on the Cluster management page

Prerequisites

The read/write splitting feature is enabled on the **Cluster management** page of the primary RDS instance to which the read-only RDS instance is attached. For more information, see [Enable read/write splitting](#).



1. Log on to the [ApsaraDB RDS console](#)
2. Find the primary RDS instance and click its ID.
3. In the left-side navigation pane, click **Cluster management**.
4. Find the read-only instance and click its ID.



Related operations

Operation	Description
Create a read-only instance	Creates a read-only ApsaraDB RDS instance.

6.7. Features of ApsaraDB RDS instances that run different SQL Server versions and RDS editions

This topic describes the features of ApsaraDB RDS instances that run different SQL Server versions and RDS editions.

Basic features

Category	Feature	RDS Cluster Edition	RDS High-availability Edition		RDS Basic Edition
		SQL Server 2019 EE SQL Server 2017 EE	SQL Server 2019 SE SQL Server 2017 SE SQL Server 2016 SE and 2016 EE SQL Server 2012 SE and 2012 EE	SQL Server 2008 R2	SQL Server 2016 Web SQL Server 2012 Web SQL Server 2012 EE
	Create an RDS instance	Supported	Supported	Supported	Supported
	Restart an RDS instance				
	Enable auto-renewal for an RDS instance				
	Change the billing method of an RDS instance				
	Change the specifications of an RDS instance				

Lifecycle Category	Feature	RDS Cluster Edition	RDS High-availability Edition		RDS Basic Edition
		SQL Server 2019 EE SQL Server 2017 EE	SQL Server 2019 SE SQL Server 2017 SE SQL Server 2016 SE and 2016 EE SQL Server 2012 SE and 2012 EE	SQL Server 2008 R2	SQL Server 2016 Web SQL Server 2012 Web SQL Server 2012 EE
	Release an RDS instance				
	Create a temporary RDS instance	Not supported	Not supported	Supported	Supported
	Upgrade the database engine version of an RDS instance	Available soon	Available soon	Supported	Available soon
	Clone an RDS instance	Supported	Supported	Not supported	Supported
	Create a read-only RDS instance	Supported	Not supported	Not supported	Not supported
Instance properties	View a list of RDS instances	Supported	Supported	Supported	Supported
	Query the details of an RDS instance				
	Change the description of an RDS instance				
	Set the maintenance window of an RDS instance				
	Manage tags				

Category	Feature	RDS Cluster Edition	RDS High-availability Edition		RDS Basic Edition
		SQL Server 2019 EE SQL Server 2017 EE	SQL Server 2019 SE SQL Server 2017 SE SQL Server 2016 SE and 2016 EE SQL Server 2012 SE and 2012 EE	SQL Server 2008 R2	SQL Server 2016 Web SQL Server 2012 Web SQL Server 2012 EE
	Manage zones	Not supported	Not supported	Supported	Not supported
Database connection	VPC endpoint	Supported	Supported	Supported	Supported
	Public endpoint				
	Read/write splitting endpoint	Not supported	Not supported	Not supported	Not supported
Service availability	Disaster recovery inside a zone	Supported	Supported	Supported	Supported
	Cross-zone disaster recovery	Supported	Supported	Supported	Not supported
	Geo-disaster recovery	Not supported	Not supported	Not supported	Not supported
	Disaster recovery drill				
	Full backup				
	Incremental backup				
	Log backup				
	Customize backup policies for an RDS instance				

Category	Feature	RDS Cluster Edition	RDS High-availability Edition		RDS Basic Edition
		SQL Server 2019 EE Supported SQL Server 2017 EE	SQL Server 2019 SE SQL Server 2017 SE SQL Server 2016 SE and 2016 EE SQL Server 2012 SE and 2012 EE	Supported SQL Server 2008 R2	SQL Server 2016 Web Supported SQL Server 2012 Web SQL Server 2012 EE
Backup and restoration	Restore the data of an RDS instance from a data backup file that is stored on another RDS instance				
	Restore the data of an RDS instance to a specific point in time				
	Restore the data of an RDS instance from a data backup file that is stored on your computer	Supported (full backup, differential backup, and log backup)	Supported (full backup, differential backup, and log backup)	Supported (full backup)	Supported (full backup, differential backup, and log backup)
	Restore the data of an RDS instance to a cloned RDS instance	Supported	Supported	Not supported	Available soon
	Back up the partial data of an RDS instance				
	Restore the partial data of an RDS instance				

Category	Feature	RDS Cluster Edition	RDS High-availability Edition	RDS Basic Edition	RDS Basic Edition
		Supported	Supported	Not supported	Not supported
		SQL Server 2019 EE SQL Server 2017 EE	SQL Server 2019 SE SQL Server 2017 SE SQL Server 2016 SE and 2016 EE SQL Server 2012 SE and 2012 EE	SQL Server 2008 R2	SQL Server 2016 Web SQL Server 2012 Web SQL Server 2012 EE
Monitoring and alerting	Monitor the resources of an RDS instance	Supported	Supported	Supported	Supported
	Monitor the database engine and storage engine of an RDS instance				
	Customize monitoring policies				
	Aggregate monitoring items				
Parameter management	Parameter update	Supported (T-SQL)	Supported (T-SQL)	Supported	Supported (T-SQL)
	Parameter template				
Log management	Error logs	Supported (T-SQL)	Supported (T-SQL)	Supported	Supported (T-SQL)
	Operational logs				

Data management features

Category	Feature	RDS Cluster Edition	RDS High-availability Edition		RDS Basic Edition
		SQL Server 2019 EE SQL Server 2017 EE	SQL Server 2017 SE SQL Server 2016 SE and 2016 EE SQL Server 2012 SE and 2012 EE	SQL Server 2008 R2	SQL Server 2016 Web SQL Server 2012 Web SQL Server 2012 EE
Data management	User management	Supported (T-SQL)	Supported (T-SQL)	Supported	Supported (T-SQL)
	Database and table management			Supported (T-SQL)	
	Data operation			Supported (T-SQL)	
	Scheduled task				
Data tunnel	Homogeneous data migration	Supported (DTS)	Supported (DTS)	Supported (DTS)	Supported (DTS)
	Heterogeneous data migration				
	Data synchronization				
	Data subscription	Not supported	Not supported	Not supported	Not supported
	Database replication between RDS instances	Supported	Supported	Not supported	Supported
	IP address whitelist				
	Management and operation audit				

Category	Feature	Supported	Supported	Supported	Supported
		RDS Cluster Edition	RDS High Availability Edition	RDS Basic Edition	RDS Basic Edition
Data security	SQL Server 2019 EE	SQL Server 2017 SE	SQL Server 2016 SE and 2016 EE	SQL Server 2012 SE and 2012 EE	SQL Server 2016 Web
	SQL Server 2017 EE	SQL Server 2008 R2	SQL Server 2012 Web	SQL Server 2012 EE	SQL Server 2012 Web
	Firewall	Supported (IP address whitelist)	Supported (IP address whitelist)	Supported (IP address whitelist)	Supported (IP address whitelist)
	Database audit	Supported	Supported	Supported	Supported
	Storage encryption	Not supported	Not supported	Supported	Not supported
Performance optimization	Network encryption	Supported	Supported	Supported	Supported
	Security group management	Not supported	Not supported	Not supported	Not supported
	Expert service	Supported	Supported	Supported	Supported
	Resource analysis	Not supported	Not supported	Not supported	Not supported
	Engine analysis				
Engine and code optimization					

Features provided by Microsoft SQL Server

The following table describes the features that are provided by Microsoft SQL Server Web Edition, Standard Edition, and Enterprise Edition.

Feature	Microsoft SQL Server Web Edition	Microsoft SQL Server Standard Edition	Microsoft SQL Server Enterprise Edition

Feature	Microsoft SQL Server Web Edition	Microsoft SQL Server Standard Edition	Microsoft SQL Server Enterprise Edition
Specifications	16 cores and 64 GB of capacity	24 cores and 128 GB of capacity	None
High availability (HA)	Standalone	Mirror HA	Always On HA
Data compression	Not supported	Supported	Supported
SQL Profiler			
Column-based index			
Table and index partitioning		Supported by SQL Server 2016 Not supported by SQL Server 2012	
Change data capture (CDC)			
Online DDL		Not supported	
Parallel indexed operations			
Parallelism adjustment of partitioned tables			
TDE			
Advanced R integration			

- For more information about the feature differences between SQL Server 2016 Web Edition, Standard Edition, and Enterprise Edition), see [Editions and supported features of SQL Server 2016](#).
- For more information about the feature differences between SQL Server 2012 Web Edition, Standard Edition, and Enterprise Edition), see [Features Supported by the Editions of SQL Server 2012](#).
- For more information about the feature differences between various SQL Server editions, see [Addressing Key Business Needs Efficiently and Cost-Effectively with Different Editions of ApsaraDB For SQL Server](#). This article is written by Alibaba Cloud engineers.

7. Data migration

7.1. Data migration solutions

ApsaraDB RDS provides various data migration solutions that can fulfill different business requirements, such as migration to the cloud and migration between cloud service providers. These solutions allow you to migrate data to ApsaraDB RDS without interruptions to your business.

You can use Alibaba Cloud Data Transmission Service (DTS) to implement schema or full migrations of SQL Server databases. For more information, see [Data Transmission Service \(DTS\)](#).

The following table lists the cloud deployment, cloud migration, and data export scenarios that are supported by ApsaraDB RDS. The following table also provides links to the related operations.

Scenario	Operation
Migrate data from an on-premises database to an RDS instance	<ul style="list-style-type: none"> • Migrate data from a self-managed SQL Server instance to an ApsaraDB RDS for SQL Server instance • Migrate full data from a self-managed SQL Server database to an ApsaraDB RDS for SQL Server instance • Migrate the full backup data of a self-managed SQL Server database to an ApsaraDB RDS instance that runs SQL Server 2012, 2016, 2017, or 2019 • Migrate the incremental backup data of a self-managed SQL Server database to an ApsaraDB RDS instance (SQL Server 2012, 2014, 2016, 2017, and 2019) • Migrate the full backup data of a self-managed SQL Server database to an ApsaraDB RDS instance that runs SQL Server 2008 R2
Migrate data between RDS instances	<ul style="list-style-type: none"> • Migrate data between databases that have different names • Migrate data between RDS instances
Migrate data from an RDS instance to an on-premises database.	Migrate the data of an ApsaraDB RDS for SQL Server database to an on-premises SQL Server database

7.2. Migrate data from a user-created database to an RDS SQL Server database

7.2.1. Migrate the full backup data of a self-managed SQL Server database to an ApsaraDB RDS instance that runs SQL Server 2008 R2

ApsaraDB RDS instances that run SQL Server 2008 R2 allow you to easily migrate data to the cloud. You need to only use the backup feature of Microsoft to back up full data on your own database. Then, upload the backup files to an Object Storage Service (OSS) bucket to fully migrate the data to the specified database of your ApsaraDB RDS for SQL Server instance by using the ApsaraDB RDS console. The backup feature of Microsoft is compatible with ApsaraDB RDS for SQL Server.

Prerequisites

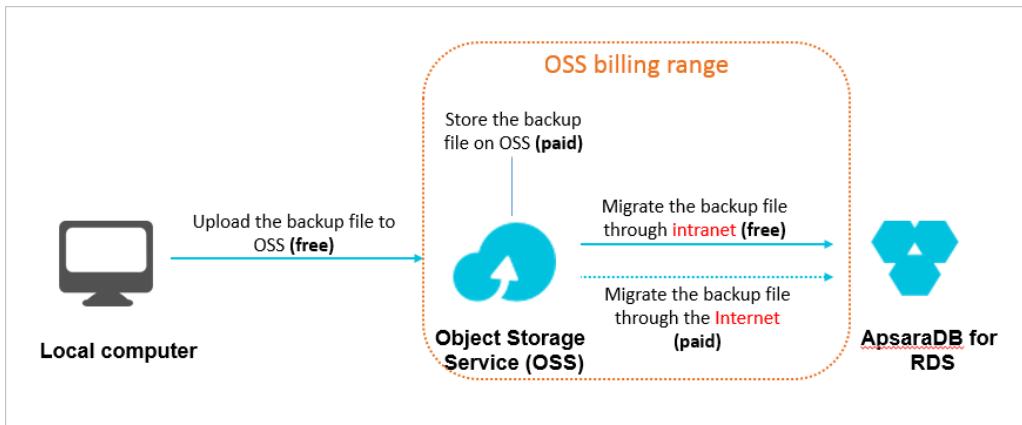
- A destination database that has the same name as the self-managed database is created on your RDS instance. For more information, see [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2008 R2](#).

Usage notes

The migration method that is described in this topic is at the database level. You can migrate the full backup data only of a single self-managed database to your RDS instance at a time. If you want to migrate the full backup data of multiple or all databases in a self-managed instance at a time, we recommend that you use an instance-level migration method. For more information, see [Migrate data from a self-managed SQL Server instance to an ApsaraDB RDS for SQL Server instance](#).

Billing

If you use the method described in this topic to migrate data, you are charged only for the use of OSS buckets.



Scenario	Fee
Upload backup files to an OSS bucket	Free of charge.
Store backup files in an OSS bucket	You are charged storage fees. For more information, visit the Pricing page of OSS.
Migrate backup files from an OSS bucket to your RDS instance	<ul style="list-style-type: none"> • If you migrate backup files from an OSS bucket to your RDS instance over an internal network, no fees are generated. • If you migrate backup files over the Internet, fees are generated for outbound traffic over the Internet on OSS. For more information, visit the Pricing page of OSS.

Procedure


1. Back up the self-managed database.
 - i. Start the Microsoft SQL Server Management Studio (SSMS) client.
 - ii. Log on to the source database.
 - iii. Execute the following statements to check the recovery model:

```
use master;
go
select name, case recovery_model
when 1 then 'FULL'
when 2 then 'BULD_LOGGED'
when 3 then 'SIMPLE' end model from sys.databases
where name not in ('master','tempdb','model','msdb');
go
```

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

- iv. 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
```


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

- v. Execute the following statements to back up the source database. In this example, the `dbtest` database is backed up to the `backup.bak` file.

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


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

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

 **Notice**


- If a result set is returned, the backup file is valid.
- If an error is returned, the backup file is invalid. In this case, you must back up the source database again.

- vii. (Optional) Execute the following statement to reset the recovery model:


 **Notice** If the recovery model of your database is `FULL`, skip this step.

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

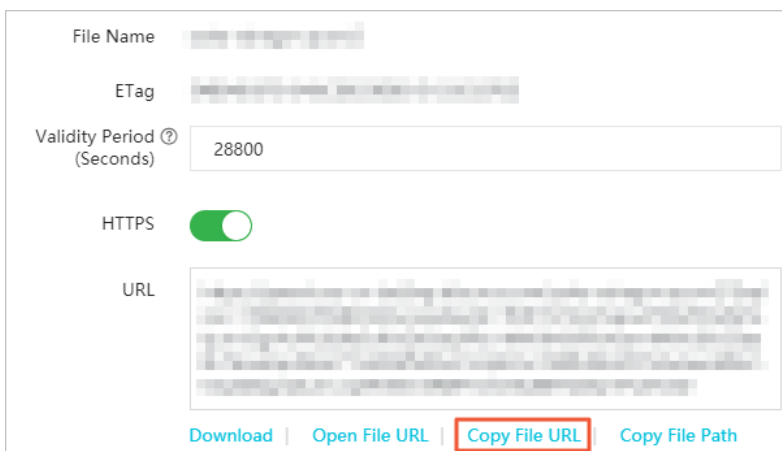
2. Upload the backup file of your self-managed database to an OSS bucket.
 - o For more information about how to upload a file that is smaller than 5 GB in size, see [Upload an object](#).
 - o For more information about how to upload multiple files or a file that is larger than 5 GB in size, see [Multipart upload and resumable upload](#). For more information about how to use the graphical management tool ossbrowser, see [ossbrowser](#).

 **Notice** Your RDS instance and OSS bucket can communicate over an internal network only when they reside in the same region. Therefore, you must upload the backup file to the OSS bucket that resides in the same region as your RDS instance.

3. Set the validity period and obtain the URL of the backup file.
 - i. Log on to the [OSS console](#).
 - ii. In the left-side navigation pane, click **Buckets**.
 - iii. Find the bucket to which you have uploaded the backup file and click its name.
 - iv. In the left-side navigation pane, click **Files**.
 - v. Select the backup file.
 - vi. In the panel that appears, change the value of the **Validity Period (Seconds)** parameter to 28800 (8 hours).

 **Notice** The URL of the backup file is required when you migrate the file from the OSS bucket to your RDS instance. The data migration fails when the validity period of the URL expires.

- vii. Click **Copy File URL**.



File Name `xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx`

ETag `xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx`

Validity Period (Seconds)


HTTPS

URL `https://xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx.oss-cn-xxxx-xxxx.aliyuncs.com/xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx`

[Download](#) | [Open File URL](#) | [Copy File URL](#) | [Copy File Path](#)

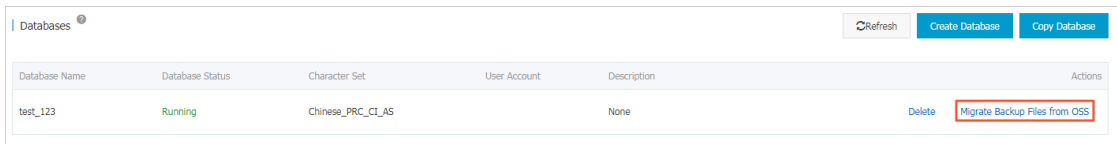
viii. Modify the backup file URL that you obtain.

By default, the URL contains the public endpoint of the file. If you migrate data over an internal network, you must replace the public endpoint with the internal endpoint in the URL. For example, the URL of the backup file is `http://rdstest.oss-cn-shanghai.aliyuncs.com/testmigraterds_20170906143807_FULLL.bak?Expires=15141****&OSSAccessKeyId=TMP****`. You must replace the public endpoint `oss-cn-shanghai.aliyuncs.com` with the internal endpoint `oss-cn-shanghai-internal.aliyuncs.com`.

 **Notice** The internal endpoint varies based on the network type and region. For more information, see [Regions and endpoints](#).

4. Restore data to your RDS instance by using the backup file in the OSS bucket.

- i.
- ii. In the left-side navigation pane, click **Databases**.
- iii. Find the destination database and click **Migrate Backup Files from OSS** in the **Actions** column.



- iv. In the **Import Guide** wizard, read the on-screen instructions and click **Next**.
- v. Read the on-screen instructions and click **Next**.

- vi. Enter the URL of the backup file in the **OSS URL of the Backup File** field.

Note ApsaraDB RDS instances that run SQL Server 2008 R2 support only one-time migration of full backup files.

- vii. Click **OK**.

In the left-side navigation pane, click **Database Migration to Cloud**. Then, find the migration task in the migration task list.

Notice If **Task Status** is not **Success**, you can click **Task Description** or **View File Details** in the **Actions** column to view the cause. Fix the problem and repeat the preceding migration procedure again.

Related operations

Operation	Description
Create a migration task	Creates a migration task
Open the database to which backup data is migrated	Opens a database.
Query migration tasks	Queries the migration tasks.
Query backup data files of migration task	Queries the details about the backup files that are uploaded to an OSS bucket.

7.2.2. Migrate the full backup data of a self-managed SQL Server database to an ApsaraDB RDS instance that runs SQL Server 2012, 2016, 2017, or 2019

This topic describes how to migrate the full backup data of a self-managed SQL Server database from an Object Storage Service (OSS) bucket to an ApsaraDB RDS for SQL Server instance.

Prerequisites

- The RDS instance runs one of the following SQL Server versions and RDS editions:
 - SQL Server 2017 EE or 2019 EE on RDS Cluster Edition
 - SQL Server 2012 SE, 2012 EE, SQL Server 2016 SE, 2016 EE, 2017 SE, or 2019 SE on RDS High-availability Edition
 - SQL Server 2012 EE Basic, 2012 Web, or 2016 Web on RDS Basic Edition

Note For more information about how to migrate the full backup data of a self-managed database to an RDS instance that runs SQL Server 2008 R2 on RDS High-availability Edition, see [Migrate the full backup data of a self-managed SQL Server database to an ApsaraDB RDS instance that runs SQL Server 2008 R2](#).

- The available storage of the RDS instance is sufficient. If the available storage is insufficient, you must expand the storage capacity of the RDS instance before you start the migration.
- No existing databases on the RDS instance have the same name as the self-managed database.
- A privileged account is created for the RDS instance. For more information, see [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2012, 2014, 2016, 2017 SE, or 2019 SE](#).
- The OSS bucket that stores the full backup data of the self-managed database resides in the same region as the RDS instance. For more information about how to create an OSS Bucket, see [Create buckets](#).
- The DBCC CHECKDB statement is executed, and the return result indicates that no allocation errors or consistency errors occur.

Note If no allocation errors or consistency errors occur, the following execution result is 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.
```

Precautions


- The migration method that describes in this topic is at the database level. You can use this method to migrate the full backup data of a single self-managed database to the cloud at a time. If you want to migrate the full backup data of multiple or all self-managed databases at a time, we recommend that

you use an instance-level migration method. For more information, see [Migrate data from a self-managed SQL Server instance to an ApsaraDB RDS for SQL Server instance](#).

- The migration from a later SQL Server version to an earlier SQL Server version is not supported. For example, if the self-managed database runs SQL Server 2016 and the RDS instance runs SQL Server 2012, you cannot migrate the full backup data of the self-managed database to the RDS instance.
- Differential backup files and log backup files are not supported.
- The name of the full backup file that is used for the migration cannot contain special characters, such as at signs (@) and vertical bars (|). If the name contains special characters, the migration fails.
- After you authorize the service account of the RDS instance to access the OSS bucket, a role named **AliyunRDSImportRole** is created in Resource Access Management (RAM). Do not modify or delete this role. If you modify or delete this role, you cannot download full backup files from the OSS bucket. In addition, if you modify or delete this role, you must re-authorize the service account of the RDS instance by using the migration wizard.
- The RDS instance does not carry over the accounts of the self-managed database. After the migration is complete, you must create accounts on the RDS instance in the ApsaraDB RDS console.
- Before the migration is complete, do not delete the backup files from the OSS bucket. If you delete the backup files before the migration is complete, the migration fails.
- The names of backup files must be suffixed by bak, diff, tm, or log. If the full backup files are not generated by using the backup script that is provided in this topic, you must add one of the following suffixes to the file names:
 - bak: indicates a full backup file.
 - diff: indicates a differential backup file.
 - tm or log: indicates a transaction log backup file.

 **Note** By default, the full backup files of the RDS instance are in the ZIP format. If you download a full backup file that is in the ZIP format, you must decompress the full backup file to obtain a full backup file whose name is suffixed by bak. Then, you can use the full data backup file to migrate the data to the cloud.

Back up the self-managed database

 **Note** Before you perform a full backup, you must stop all data writes to the self-managed database. The data that is written to the self-managed database during the full backup process cannot be backed up.

1. Download the [backup script file](#). Then, open the file by using SQL Server Management Studio (SSMS).
2. Configure the following parameters.

Parameter	Description
@backup_databases_list	The name of the self-managed database that you want to back up. In other migration scenarios, this parameter also allows you to specify multiple databases. If you specify multiple databases, separate the names of these databases with semicolons (;) or commas (,).

Parameter	Description
@backup_type	The type of backup that you want to perform. Valid values: <ul style="list-style-type: none"> ◦ FULL: full backup ◦ DIFF: differential backup ◦ LOG: log backup
@backup_folder	The directory that is used to store backup files on the self-managed database. If the specified directory does not exist, the system automatically creates the directory.
@is_run	Specifies whether to perform a backup or a check. Valid values: <ul style="list-style-type: none"> ◦ 1: Specifies to perform a backup. ◦ 0: Specifies to perform a check.

3. Execute the backup script.

Upload the generated full backup file to the OSS bucket

After the full backup on the self-managed database is complete, you must use one of the following methods to upload the generated full backup file to the OSS bucket:

- Method 1: Use the ossbrowser tool

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

- Method 2: Use the OSS console


If the size of the generated full backup file is less than 5 GB, you can upload the full backup file in the OSS console. For more information, see [Upload objects](#).

- Method 3: Use the OSS API


You can call an OSS API operation to upload the generated full backup file by using the resumable upload method. For more information, see [Multipart upload and resumable upload](#).

Create a migration task

- 1.
2. In the left-side navigation pane, click **Backup and Restoration**.
3. In the upper-right corner of the page, click **Migrate OSS Backup Data to RDS**.
4. In the **Import Guide** wizard, click **Next** twice.

 **Note** If you use the OSS-based migration wizard for the first time, you must authorize the service account of the RDS instance to access the OSS bucket. In this case, you must click **Authorize** and complete the authorization. Otherwise, the **OSS Bucket** drop-down list in the **Import Data** step is empty.

5. In the **Import Data** step, configure the following parameters.

Parameter	Description
Database Name	<p>Enter the name of the destination database on the RDS instance. The destination database stores the data that is migrated from the self-managed database. The name of the destination database must be different from the name of the self-managed database.</p> <p> Note The name of the destination database must meet the requirements of open source SQL Server.</p>
OSS Bucket	Select the OSS bucket that stores the full backup file.
OSS Subfolder Name	Enter the name of the OSS subfolder that stores the full backup file.
OSS File	Specify the full backup file that you want to import. You can enter a prefix in the search box and click the search icon to search for the full backup file by using a fuzzy match. ApsaraDB RDS displays the name, size, and update time of each full backup file that is returned. Select the backup file that you want to migrate to the cloud.
Cloud Migration Plan	<ul style="list-style-type: none"> Immediate Access (Full Backup): If you want to migrate only a full backup file, select this migration plan. For this example, select Immediate Access (Full Backup). In this case, the following parameter settings take effect in the CreateMigrateTask operation: <code>BackupMode = FULL</code> and <code>IsOnlineDB = True</code>. Access Pending (Incremental Backup): If you want to migrate a full backup file and a log or differential backup file, select this migration plan. In this case, the following parameter setting takes effect in the CreateMigrateTask operation: <code>BackupMode = UPDF</code> and <code>IsOnlineDB = False</code>.
Consistency Check Mode	<ul style="list-style-type: none"> Asynchronous DBCC: The DBCC CHECKDB statement is executed after the destination database is opened. This reduces the time that is required to open the destination database and minimizes the downtime of your application. If the destination database is large, a long period of time is required to execute the DBCC CHECKDB statement. Therefore, if your application is sensitive to downtime but insensitive to the result of the DBCC CHECKDB statement, we recommend that you select this consistency check mode. In this case, the following parameter setting takes effect in the CreateMigrateTask operation: <code>CheckDBMode = AsyncExecuteDBCheck</code>. Synchronous DBCC: The DBCC CHECKDB statement is executed at the same time when the destination database is opened. If you want to identify consistency errors between the self-managed database and the destination database based on the result of the DBCC CHECKDB statement, we recommend that you select this consistency check mode. In this case, the following parameter setting takes effect in the CreateMigrateTask operation: <code>CheckDBMode = SyncExecuteDBCheck</code>. However, the amount of time that is required to open the destination database increases.

6. Click **OK**.

Wait until the migration task is completed. You can click **Refresh** to view the latest status of the migration task. If the migration task fails, you can troubleshoot the failure based on the description of the migration task. For more information, see the "**Common errors**" section of this topic.

View the migration task

If you want to view details about the migration task, go to the **Backup and Restoration** page and click the **Backup Data Upload History** tab. By default, this tab displays the migration tasks over the last week.

Common errors

Each migration task record on the Backup Data Upload History tab of the Backup and Restoration page contains a task description. If the migration task fails or an error message is reported, you can troubleshoot the failure or error based on the task description. The following common errors may occur:

- A database with the same name as the self-managed database is found on the RDS instance.
 - Error message: The database (xxx) is already exist on RDS, please backup and drop it, then try again.
 - Cause: If an existing database on the RDS instance has the same name as the self-managed database, the migration is not supported. This mechanism is designed to ensure the security of your data.
 - Solution: If you want to overwrite an existing database on the RDS instance, back up the database, delete the database from the RDS instance, and then create and run a migration task again.
- A differential backup file is used.
 - Error message: Backup set (xxx.bak) is a Database Differential backup, we only accept a FULL Backup.
 - Cause: The file that you upload is a differential backup file rather than a full backup file. The migration solution in this topic supports only full backup files.
- A log backup file is used.
 - Error message: Backup set (xxx.trn) is a Transaction Log backup, we only accept a FULL Backup.
 - Cause: The file that you upload is a log backup file rather than a full backup file. The migration solution in this topic supports only full backup files.
- The full backup file fails the verification.
 - Error message: Failed to verify xxx.bak, backup file was corrupted or newer edition than RDS.
 - Cause: The full backup file is corrupted, or the self-managed database runs a later SQL Server version than the RDS instance. For example, this error occurs if the self-managed database runs SQL Server 2016 and the RDS instance runs SQL Server 2012.
 - Solution: If the full backup file is corrupted, perform a full backup on the self-managed database again. Then, create and run a migration task again. If the self-managed database runs a later SQL Server version than the RDS instance, select a different RDS instance that runs the same or later version than the self-managed database.
- The DBCC CHECKDB statement fails.
 - Error message: DBCC checkdb failed.
 - Cause: The self-managed database encounters allocation or consistency errors.

- Solution: Execute the following statement on the self-managed database to fix the errors. Then, create and run a migration task again.

 **Note** If you execute the following statement, your data may be lost.

```
DBCC CHECKDB (DBName, REPAIR_ALLOW_DATA_LOSS) WITH NO_INFOMSGS, ALL_ERRORMSGS
```

- The available storage of the RDS instance is insufficient.
 - Error message: Not Enough Disk Space for restoring, space left (xxx MB) < needed (xxx MB).
 - Cause: The available storage of the RDS instance is less than the minimum storage that is required for the full backup file.
 - Solution: Expand the storage capacity of the RDS instance.
- The available storage of the RDS instance is insufficient.
 - Error message: Not Enough Disk Space, space left xxx MB < bak file xxx MB.
 - Cause: The available storage of the RDS instance is less than the minimum storage that is required for the full backup file.
 - Solution: Expand the storage capacity of the RDS instance.
- No privileged account is created on the RDS instance.
 - 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: No privileged account is created on the RDS instance. As a result, the migration task cannot find the account that requires authorization. However, the full backup file has been restored to the RDS instance, and the migration task is successful.
 - Solution: Create a privileged account on the RDS instance. For more information, see [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2012, 2014, 2016, 2017 SE, or 2019 SE](#).

Related operations

Operation	Description
Create a migration task	Creates a migration task to restore the data of a backup file from an OSS bucket to an ApsaraDB RDS instance.
Open the database to which backup data is migrated	Opens the database to which backup data is migrated on an ApsaraDB RDS instance.
Query migration tasks	Queries the migration tasks of an ApsaraDB RDS instance.
Query backup data files of migration task	Queries the details about the backup data files that are uploaded to OSS.

7.2.3. Migrate the incremental backup data of a self-managed SQL Server database to an ApsaraDB RDS instance (SQL Server 2012, 2016, 2017, and 2019)

This topic describes how to migrate the incremental backup data of a self-managed SQL Server database to an ApsaraDB RDS for SQL Server instance. The incremental backup data of the self-managed database is stored in an Object Storage Service (OSS) bucket. You can upload the incremental backup data as a file from the OSS bucket to the RDS instance. This migration solution reduces downtime to minutes.

Prerequisites

- Your RDS instance runs one of the following SQL Server versions and RDS editions:
 - SQL Server 2017 EE or 2019 EE on RDS Cluster Edition
 - SQL Server 2012 SE, 2012 EE, 2016 SE, 2016 EE, 2017 SE, or 2019 SE on RDS High-availability Edition
 - SQL Server 2012 EE Basic, 2012 Web, or 2016 Web on RDS Basic Edition
- The OSS bucket that stores the incremental backup data of the self-managed database resides in the same region as your RDS instance. For more information about how to create an OSS bucket, see [Create buckets](#).
- The self-managed database uses the FULL recovery model.

Note If the self-managed database uses the SIMPLE recovery model, transaction logs cannot be backed up. In this case, you can use only a differential backup file. However, the differential backup file may be large, which increases the time that is required to complete the migration.

- The remaining storage space of your RDS instance is sufficient. If the remaining storage space is insufficient, you must expand the storage capacity of your RDS instance before you start the migration.
- No existing databases on your RDS instance have the same name as the self-managed database.
- A privileged account is created on your RDS instance. For more information, see [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2012, 2014, 2016, 2017 SE, or 2019 SE](#).
- The DBCC CHECKDB statement is executed. The execution result indicates that no allocation or consistency errors occur.


Note If no allocation or consistency errors occur, the following execution result is 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.
```

Context


The migration solution in this topic is suitable for the following scenarios:

- Migrate data to your RDS instance in physical mode rather than in logical mode.

 **Note**

- Physical migration allows you to migrate data by using a physical backup file. Logical migration allows you to write the executed data manipulation language (DML) statements to your RDS instance.
- Physical migration ensures 100% data consistency between the self-managed database and the destination database on your RDS instance. Logical migration cannot ensure 100% data consistency. For example, index fragmentation and statistical information may change after the migration.

- Migrate data with minute-level downtime.

 **Note** We recommend that you migrate the data of the self-managed database to your RDS instance by using a full backup file. This applies if your application is insensitive to downtime (for example, your application can tolerate a 2-hour interruption) and the self-managed database has less than 100 GB of data. For more information, see [Migrate the full backup data of a self-managed SQL Server database to an ApsaraDB RDS instance that runs SQL Server 2012, 2016, 2017, or 2019](#).

In this topic, the migration is performed by using a full backup file and a log or differential backup file. These files are stored in the OSS bucket.

Precautions

- The migration solution in this topic is at the database level. It allows you to migrate the incremental backup data of a single self-managed database at a time. If you want to migrate the incremental backup data of multiple or all self-managed databases at a time, we recommend that you use the instance-level migration solution. For more information, see [Migrate data from a self-managed SQL Server instance to an ApsaraDB RDS for SQL Server instance](#).
- The migration from a later SQL Server version to an earlier SQL Server version is not supported. For example, the self-managed database runs SQL Server 2016 and your RDS instance runs SQL Server 2012. In this case, you cannot migrate the incremental backup data of the self-managed database to your RDS instance.
- The names of the backup files cannot contain special characters, such as at signs (@) and vertical bars (|). If the names of the backup files contain special characters, the migration fails.
- After you authorize the service account of your RDS instance to access the OSS bucket, a role named **AliyunRDSImportRole** is created in Resource Access Management (RAM). Do not modify or delete this role. If you modify or delete this role, you cannot download the backup files from the OSS bucket. In addition, if you modify or delete this role, you must re-authorize the service account of your RDS instance by using the migration wizard.
- The migration does not carry over the accounts of the self-managed database. After the migration is complete, you must create accounts on your RDS instance by using the ApsaraDB RDS console.
- Before the migration is complete, do not delete the backup files from the OSS bucket. If you delete the backup files before the migration is complete, the migration fails.
- The names of the backup files can be suffixed only by using bak, diff, trn, or log. If the backup files are not generated by using the backup script that is provided in this topic, you must add one of the following suffixes to the file names:

- o bak: indicates a full backup file.
- o diff: indicates a differential backup file.
- o tm or log: indicates a transaction log backup file.

Migration process



The following flowchart shows the migration process on a timeline.

Migration phase	Step	Description
Full backup and restoration	Step 1. Before 00:00	Complete the following preparations: <ul style="list-style-type: none"> • Execute the DBCC CHECKDB statement on the self-managed database and verify that no allocation or consistency errors occur. • Shut down the backup system of the self-managed database. • Change the recovery model of the self-managed database to FULL.
	Step 2. 00:01	Perform a full backup on the self-managed database. Time required: about 1 hour.
	Step 3. 02:00	Upload the full backup file to the OSS bucket. Time required: about 1 hour.
	Step 4. 03:00	Restore data from the full backup file to your RDS instance by using the ApsaraDB RDS console. Time required: about 19 hours.

Migration phase	Step	Description
Incremental backup and restoration	Step 5. 22:00	Perform a log backup on the self-managed database. Time required: about 20 minutes.
	Step 6. 22:20	Upload the log backup file to the OSS bucket. Time required: about 10 minutes.
	Step 6. 22:30	<ul style="list-style-type: none"> Repeat Step 5 and Step 6 to perform a log backup on the self-managed database, upload the log backup file to the OSS bucket, and then restore data from the log backup file to your RDS instance. Perform these operations until the size of the last log backup file can be less than 500 MB. Stop data writes to the self-managed database, perform the last log backup, and then upload the last log backup file to the OSS bucket.
Database opening	Step 8. 22:34	Restore data from the last log backup file to your RDS instance. Time required: about 4 minutes.
	Step 9. 22:35	Open the destination database on your RDS instance. If you execute the DBCC statement in asynchronous mode, the destination database can be opened in 1 minute.

The preceding migration provides an example of how to minimize downtime. Your application can continue to run, and you do not need to stop your application until the last log backup. In this example, the downtime of your application does not exceed 5 minutes.

Back up the self-managed database

1. Download the [backup script file](#). Then, open the file by using SQL Server Management Studio (SSMS).
2. Configure the following parameters.

Parameter	Description
@backup_databases_list	Specify the name of the self-managed database that you want to back up. In the other scenarios, this parameter also allows you to specify multiple databases. If you specify more than one database name, separate these database names with semicolons (;) or commas (,).

Parameter	Description
@backup_type	Specify the type of backup that you want to perform. Valid values: <ul style="list-style-type: none"> ◦ FULL: full backup ◦ DIFF: differential backup ◦ LOG: log backup
@backup_folder	Specify the local directory that is used to store the backup files of the self-managed database. If the specified directory does not exist, ApsaraDB RDS automatically creates the directory.
@is_run	Specify whether to perform a backup or a check. Valid values: <ul style="list-style-type: none"> ◦ 1: specifies to perform a backup. ◦ 0: specifies to perform a check.

3. Run the backup script.

Upload the full backup file to the OSS bucket

After the full backup and the log or differential backup are complete, you must use one of the following methods to upload the backup files to the OSS bucket:

- Method 1: Use the ossbrowser tool

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

- Method 2: Use the OSS console


If the sizes of the backup files are less than 5 GB, you can upload the backup files by using the OSS console. For more information, see [Upload objects](#).

- Method 3: Use the OSS API


You can call an OSS API operation to upload the backup files in resumable mode. For more information, see [Multipart upload and resumable upload](#).

Create a migration task

- 1.
2. In the left-side navigation pane, click **Backup and Restoration**.
3. In the upper-right corner of the page, click **Migrate OSS Backup Data to RDS**.
4. In the **Import Guide** wizard, click **Next** twice.

 **Note** If you run the OSS-based migration wizard for the first time, you must authorize the service account of your RDS instance to access the OSS bucket. In this case, you must click **Authorize** and complete the authorization. Otherwise, the **OSS Bucket** drop-down list in the **Import Data** step is empty.

5. In the **Import Data** step, configure the following parameters.

Parameter	Description
Database Name	<p>Enter the name of the destination database on your RDS instance. The destination database stores the data that is migrated from the self-managed database. The name of the destination database must be different from the name of the self-managed database</p> <p> Note The name of the destination database must meet the requirements of open source SQL Server.</p>
OSS Bucket	Select the OSS bucket that stores the full backup file.
OSS Subfolder Name	Enter the name of the OSS subfolder that stores the full backup file.
OSS File	Specify the full backup file that you want to import. You can click the search icon to search for the full backup file by using a prefix-based fuzzy match. ApsaraDB RDS displays the name, size, and update time of the full backup file.
Cloud Migration Method	<p>Select Immediate Access (Full Backup).</p> <ul style="list-style-type: none"> Immediate Access (Full Backup): If you want to migrate only a full backup file, select this migration method. In this case, the following parameter settings take effect in the CreateMigrateTask operation: <code>BackupMode = FULL</code> and <code>IsOnlineDB = True</code>. Access Pending (Incremental Backup): If you want to migrate a full backup file and a differential or log backup file, select this migration method. In this case, the following parameter settings take effect in the CreateMigrateTask operation: <code>BackupMode = UPDF</code> and <code>IsOnlineDB = False</code>.


6. Click **OK**.

After the migration task is complete, you can click **Refresh** to view the latest status of the migration task.

Import the log or differential backup file

After the full backup file of the self-managed database is imported into your RDS instance, you must import the log or differential backup file.

- 1.
2. In the left-side navigation pane, click **Backup and Restoration**. On the page that appears, click **Backup Data Upload History**.
3. Find the destination database and click **Upload Incremental Files**. In the dialog box that appears, configure the parameters, select the log or differential backup file, and then click **OK**.


 **Note**

- If you have multiple log backup files, you must use the same method to upload these log backup files one by one.
- Make sure that the size of the last log or differential backup file does not exceed 500 MB. This minimizes the time that is required to complete the migration.
- Before the last log backup file is generated, you must stop data writes to the self-managed database. This ensures data consistency between the self-managed database and the destination database on your RDS instance.

Open the destination database

After you import all the backup files into the destination database on your RDS instance, the destination database is in the In Recovery or Restoring state. If your RDS instance runs the High-availability Edition, the destination database is in the In Recovery state. If your RDS instance runs the Basic Edition, the destination database is in the Restoring state. In these cases, you cannot perform read or write operations on the destination database. Before you can perform read and write operations, you must open the destination database.

- 1.
2. In the left-side navigation pane, click **Backup and Restoration**. On the page that appears, click **Backup Data Upload History**.
3. Find the destination database and click **Open Database**.
4. In the dialog box that appears, select a consistency check mode and click **OK**.

 **Note** ApsaraDB RDS provides the following consistency check modes:

- Asynchronous DBCC: The DBCC CHECKDB statement is executed after the destination database is opened. This reduces the time that is required to open the destination database and minimizes the downtime of your application. If the destination database is large, a long period of time is required to execute the DBCC CHECKDB statement. Therefore, if your application is sensitive to downtime but insensitive to the result of the DBCC CHECKDB statement, we recommend that you select this consistency check mode. In this case, the following parameter setting takes effect in the CreateMigrateTask operation: `CheckDBMode = AsyncExecuteDBCheck`.
- Synchronous DBCC: The DBCC CHECKDB statement is executed at the same time when the destination database is opened. If you want to identify consistency errors between the self-managed database and the destination database based on the result of the DBCC CHECKDB statement, we recommend that you select this consistency check mode. In this case, the following parameter setting takes effect in the CreateMigrateTask operation: `CheckDBMode = SyncExecuteDBCheck`. However, the time that is required to open the destination database increases.


View details about the imported backup files

If you want to view details about the backup files that are imported by using a migration task, perform the following operations: Open the **Backup and Restoration** page. Click the **Backup Data Upload History** tab. Find the migration task and click **View File Details**. In the dialog box that appears, view details about the imported backup files.

Common errors

For more information about the common errors that may occur during the migration of full backup data, see [Migrate full backup data to ApsaraDB RDS for SQL Server 2012, 2014, 2016, 2017, or 2019](#). During the migration of incremental backup data, you may encounter the following errors:

- The destination database cannot be opened.
 - Error message: Failed to open database xxx.
 - Cause: Some advanced features are enabled for the self-managed database. However, these advanced features are not supported by your RDS instance. For example, the self-managed database runs an Enterprise Edition of SQL Server and your RDS instance runs a Web edition of SQL Server. In this case, if the data compression and partition features are enabled for the self-managed database, this error is reported when you open the destination database.
 - Solution:
 - Disable the advanced features for the self-managed database, back up data again, and then migrate the data by using OSS.
 - Purchase an RDS instance that runs the same SQL Server edition as the self-managed database. Then, migrate the data of the self-managed database to the purchased RDS instance.
- The log sequence numbers (LSNs) in the backup chain are not consecutive.
 - 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: The LSNs in the log or differential backup file are different from the LSNs in the previous backup file that is used for the restoration.
 - Solution: Select the log or differential backup file whose LSNs are the same as the LSNs of the previous backup file that is used for the restoration.
- The DBCC CHECKDB statement cannot be executed in asynchronous mode.
 - Error message: asynchronously DBCC checkdb failed: CHECKDB found 0 allocation errors and 2 consistency errors in table 'XXX' (object ID XXX).
 - Cause: After data is restored to your RDS instance with the Asynchronous DBCC consistency check mode selected, ApsaraDB RDS executes the DBCC CHECKDB statement. If the destination database fails the consistency check, consistency errors occur in the self-managed database.
 - Solution:
 - Execute the following statement on the destination database:

```
DBCC CHECKDB (DBName, REPAIR_ALLOW_DATA_LOSS)
```
 -  **Note** If you use this statement to fix the error, data may be lost.
 - Execute the following statement on the self-managed database to fix the error, and then perform the migration again:

```
DBCC CHECKDB (DBName, REPAIR_ALLOW_DATA_LOSS)
```
- The selected backup file is a full backup file.
 - Error message: Backup set (xxx) is a Database FULL backup, we only accept transaction log or differential backup.

- Cause: After the full backup file is restored to your RDS instance, you can select and restore only a log or differential backup file. If you select a full backup file again, this error is reported.
- Solution: Select and restore a log or differential backup file.
- The number of specified self-managed databases exceeds the upper limit.
 - Error message: The database (xxx) migration failed due to databases count limitation.
 - Cause: If the number of specified self-managed databases exceeds the upper limit, this error is reported.
 - Solution: Migrate the data of excess self-managed databases to another RDS instance. Otherwise, delete unnecessary databases from the current RDS instance.

Related operations

Operation	Description
Create a migration task	Creates a migration task that is used to restore backup files from an OSS bucket to an ApsaraDB RDS instance.
Open the database to which backup data is migrated	Opens the destination database on an ApsaraDB RDS instance.
Query migration tasks	Queries the migration tasks of an ApsaraDB RDS instance.
Query backup data files of migration task	Queries details about the backup files that are migrated by using a migration task to an ApsaraDB RDS instance.

7.2.4. Migrate data from a self-managed SQL Server instance to an ApsaraDB RDS for SQL Server instance

This topic describes how to migrate the data of some or all databases from a self-managed SQL Server instance to an ApsaraDB RDS for SQL Server instance by using full backup files.

Prerequisites

- The RDS instance runs one of the following SQL Server versions and RDS editions:
 - SQL Server 2017 EE or SQL Server 2019 EE on RDS Cluster Edition
 - SQL Server 2008 R2, SQL Server 2012 SE, SQL Server 2012 EE, SQL Server 2016 SE, SQL Server 2016 EE, SQL Server 2017 SE, or SQL Server 2019 SE on RDS High-availability Edition
 - SQL Server 2012 EE Basic, SQL Server 2012 Web, or SQL Server 2016 Web on RDS Basic Edition
- The source database is a self-managed SQL Server database.
- If the credentials of a Resource Access Management (RAM) user are used to migrate data, make sure that the AliyunOSSFullAccess and AliyunRDSFullAccess policies are attached to the RAM user. For more information about how to grant permissions to RAM users, see [Use RAM to manage OSS permissions](#) and [Use RAM to manage ApsaraDB RDS permissions](#).

Context

To migrate data from multiple databases to RDS instances, ApsaraDB RDS for SQL Server provides an **instance-level migration method** to migrate the data of some or all databases from a self-managed instance to an RDS instance. You need to only upload the full backup files of these databases to the same folder in an Object Storage Service (OSS) bucket, and then run the required script to migrate data to an RDS instance.

Note If you use a **database-level migration method**, you can migrate the data of only one database at a time. ApsaraDB RDS for SQL Server provides the following OSS-based cloud migration methods:

- **Migrate the full backup data of a self-managed SQL Server database to an ApsaraDB RDS instance that runs SQL Server 2008 R2**
- **Migrate the full backup data of a self-managed SQL Server database to an ApsaraDB RDS instance that runs SQL Server 2012, 2016, 2017, or 2019**
- **Migrate the incremental backup data of a self-managed SQL Server database to an ApsaraDB RDS instance (SQL Server 2012, 2014, 2016, 2017, and 2019)**

Usage notes

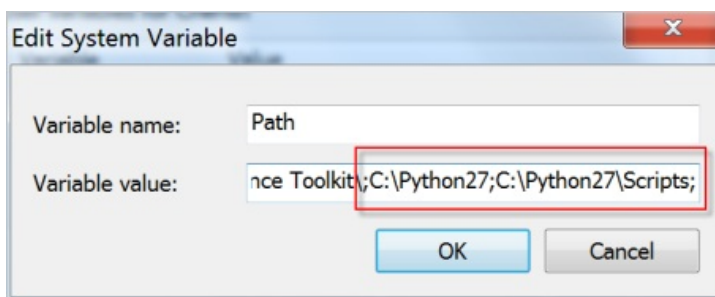
Only full backup files can be used for the data migration.

Preparations

1. Install Python 2.7.18. For more information, visit the [Python official website](#).
2. Check whether Python 2.7.18 is installed.
 - o Windows operating systems

Run the `c:\Python27\python.exe -V` command to check the Python version. If `Python 2.7.18` is displayed, Python 2.7.18 is installed.

If the system prompts 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.



- o Mac, Linux, or Unix operating systems

Run the `python -V` command to check the Python version. If `Python 2.7.18` is displayed, Python 2.7.18 is installed.


3. Use one of the following methods to install the SDK dependency package:
 - o Run the pip command.

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


- o Use the source code.

```
# 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 ApsaraDB RDS SDK.
cd aliyun-python-sdk-rds
python setup.py install
# 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 resides in the same region as the RDS instance. For more information, see [Create buckets](#).

 **Note** Skip this step if an OSS bucket that resides in the same region as the RDS instance already exists.


5. Create databases on the RDS instance. Make sure that each database whose data you want to migrate from the self-managed instance has a counterpart with an identical name on the RDS instance. In addition, keep the created databases empty.
 - o If the RDS instance runs SQL Server 2012 or later, skip this step.
 - o If the RDS instance runs SQL Server 2008 R2, create databases based on the descriptions in [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2008 R2](#).
6. Back up some or all databases on the self-managed instance.

 **Warning**

- o For data consistency purposes, we recommend that you stop data writes to these databases during the full backup.
- o If you do not use the backup script to perform the full backup, the names of the generated backup files must follow the `Database name_Backup type_Backup time.bak` format. Example: `Testdb_FULL_20180518153544.bak` .

- i. Download the [backup script file](#).
- ii. Double-click the backup script file to open it by using Microsoft SQL Server Management Studio (SSMS).

iii. Configure the following parameters.

Parameter	Description
@backup_databases_list	The name of the self-managed database that you want to back up. If you specify multiple databases, separate the names of these databases with semicolons (;) or commas (,).
@backup_type	The backup type. Valid values: <ul style="list-style-type: none"> ▪ <i>FULL</i>: full backup ▪ <i>DIFF</i>: incremental backup ▪ <i>LOG</i>: log backup <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;">  Notice In this example, set the value to <i>FULL</i>. </div>
@backup_folder	The directory that is used to store backup files on the self-managed database. If the specified directory does not exist, the system automatically creates one.
@is_run	Specifies whether to perform a backup or a check. Valid values: <ul style="list-style-type: none"> ▪ <i>1</i>: performs a backup. ▪ <i>0</i>: performs a check.



Examples:

```


SELECT
  /**
   * Databases list needed to backup, delimiter is : or ,
   * empty('') or null: means all databases excluding system database
   * example: '[testdb]: TestDR, Test, readonly'
   **/
  @backup_databases_list = N'[dtstestdata],[testdb]'
  @backup_type = N'FULL', -- Backup Type? FULL: FULL backup; DIF
F: Differential backup; LOG: Log backup
  @backup_folder = N'C:\BACKUP' -- Backup folder to store backup files
.
  @is_run = 1 -- Check or run? 1, run directly; 0, j
ust check


```

iv. Run the backup script to back up the specified databases and store the backup files in the specified directory.

 dtstestdata_FULL_20200408154821.bak
 testdb_FULL_20200408154821.bak

7. Use one of the following methods to upload the backup files to the OSS bucket that you created.

 **Warning** Make sure that the OSS bucket and the RDS instance reside in the same region. This allows the RDS instance to read the backup files at faster speeds. This also helps prevent failures that may occur if the backup files cannot be downloaded.

Method	Description
Use ossbrowser to upload backup files	<p>We recommend that you use ossbrowser to upload backup files to the OSS bucket. For more information, see Use ossbrowser.</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 10px; margin-top: 10px;"> <p> Notice If the self-managed instance is deployed in an Elastic Compute Service (ECS) instance that resides in a virtual private cloud (VPC), you can upload the backup files to the specified OSS bucket by using the VPC endpoint of the OSS bucket. This improves upload efficiency.</p> </div>
Use the OSS console to upload backup files	If the size of backup files is smaller than 5 GB, you can upload the files by using the OSS console. For more information, see Upload objects .
Call OSS API operations to upload backup files	If you want to upload the backup files unattended, use the OSS API operations to perform resumable uploads. For more information, see Multipart upload .

Procedure

1. Download the [migration script package](#).
2. Decompress the migration script package and run the following command to view the parameters that you need to specify:

```
python ~/Downloads/RDSSQLCreateMigrateTasksBatchly.py -h
```

A similar result is returned:

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

Parameters

Parameter	Description
access_key_id	The AccessKey ID of the Alibaba Cloud account to which the RDS instance belongs.
access_key_secret	The AccessKey secret of the Alibaba Cloud account to which the RDS instance belongs.
rds_instance_id	The ID of the RDS instance.
oss_endpoint	The endpoint of the OSS bucket that stores the backup files. For more information about how to obtain the endpoint, see Bucket overview .
oss_bucket	The name of the OSS bucket that stores the backup files.
directory	The folder that stores the backup files in the OSS bucket. If the backup files are stored in the root folder, enter a forward slash (/).

3. Run the migration script to complete the migration task.

Examples:

You can run the migration script to migrate all the backup files that meet the specified conditions from the *Migrationdata* folder in the OSS bucket named testdatabucket to the RDS instance whose ID is rm-2zesz5774ud8s****.

```
python ~/Downloads/RDSSQLCreateMigrateTasksBatchly.py -k LTAIQ**** -s BMKIUhroub*****
-i rm-2zesz5774ud**** -e oss-cn-beijing.aliyuncs.com -b testdatabucket -d Migrationdata
```

4. View the progress of the migration task.

- i.
- ii. Perform the following steps based on the SQL Server version that is run on your RDS instance:
 - SQL Server 2008 R2

In the left-side navigation pane, click **Database Migration to Cloud**. You can view all the migration tasks that you have submitted.

Note You can click **Refresh** in the upper-right corner of the page to view the latest status of the migration tasks.

No.	Database Name	Task Start Time	Task End Time	Task Status	Task Type	Task Description	Actions
169043	testdb	2020-04-09 09:32:39	2020-04-09 09:33:55	Success	Immediate Access (Full Backup)	Success	View File Details
169042	dtstestdata	2020-04-09 09:32:36	2020-04-09 09:33:25	Success	Immediate Access (Full Backup)	Success	View File Details

- SQL Server 2012 and later

In the left-side navigation pane, click **Backup and Restoration**. Then, click the **Backup Data Upload History** tab.

Note By default, the migration records over the last seven days are displayed. You can specify a time range to view the migration tasks over the specified time range.

序号	数据库名	任务开始时间	任务结束时间	任务状态	任务类型	任务描述	Actions
169016	testdb	Apr 9, 2020, 09:18:19	Apr 9, 2020, 09:20:04	成功	Immediate Access (Full Backup)	Success	View File Details
169015	dtstestdata	Apr 9, 2020, 09:18:17	Apr 9, 2020, 09:19:11	成功	Immediate Access (Full Backup)	Success	View File Details

Common errors

Error message	Cause	Solution
<pre>HTTP Status: 404 Error:InvalidAccessKeyId.NotFound Specified access key is not found. RequestID: XXXXXXXXXXXXXXXXXXXX</pre>	<p>The AccessKey ID that is used to call API operations is invalid.</p>	<p>Use the valid AccessKey ID and AccessKey secret. For more</p>

Error message	Cause	Resolution
<pre>HTTP Status: 400 Error:IncompleteSignature The request signature does not conform to Aliyun standards. server string to sign is:.....</pre>	The AccessKey secret that is used to call API operations is invalid.	AccessKey secret. For more information, see FAQ about AccessKey pairs .
<pre>RDS engine doesn't support, this is only for RDS SQL Server engine.</pre>	The RDS instance to which you want to migrate data does not run SQL Server.	Use an RDS instance that runs SQL Server.
<pre>Couldn't find specify RDS [XXX].</pre>	The ID of the RDS instance does not exist.	Check whether the ID of the RDS instance is valid. If the ID of the RDS instance is invalid, enter the valid instance ID.
<pre>{'status': -2, 'request-id': '', 'details': "RequestError: HTTPConnectionPool(host='xxxxxxxxxxxxxxxx', 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',))"}"</pre>	The endpoint that is used to connect to the OSS bucket is invalid.	Check whether the endpoint that is used to connect to the OSS bucket is valid. If the endpoint is invalid, enter the valid endpoint. For more information, see Bucket overview .
<pre>{'status': 404, '-id': 'xxxxxxxx', 'details': {'HostId': 'xxxxxxxx', 'Message': 'The specified bucket does not exist.', 'Code': 'NoSuchBucket', 'RequestId': 'xxxxxxxx', 'BucketName': 'aaaatp-test-on-ecs'}}</pre>	The OSS bucket does not exist.	Check whether the entered name of the OSS bucket is valid. If the entered name is invalid, enter the valid name.

Error message	Cause	Solution
<pre>There is no backup file on OSS Bucket [xxxxxxx] under [xxxxxxxxxx] folder, check please.</pre>	<p>The required folder does not exist in the OSS bucket, or the folder does not contain the backup files that meet the specified conditions.</p>	<p>Check whether the folder exists in the OSS bucket and whether the folder contains the backup files that meet the specified conditions. If the folder does not exist in the OSS bucket and the folder does not contain backup files that meet the specified conditions, create the folder in the OSS bucket and import backup files that meet the specified conditions.</p>
<pre>Warning!!!!, [autotest_2005_ent_broken_fu ll_dbcc_failed.bak] is not backup file, filtered.</pre>	<p>The names of the backup files do not meet the naming conventions.</p>	<p>If you do not use the backup script to perform the full backup, the names of the generated backup files must follow the <code>Database name_Backup type_Backup time.bak</code> format. Example: <code>Testdb_FULL_20180518153544 .bak</code></p>
<pre>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'}}}</pre>	<p>The RAM user does not have the required permissions.</p>	<p>Attach the AliyunOSSFullAccess and AliyunRDSFullAccess policies to the RAM user. For more information about how to authorize a RAM user, see Authorize a RAM user.</p>
<pre>OPENAPI Response Error !!!! : HTTP Status: <Http Status Code> Error:<Error> <Description>. RequestID: 32BB6886-775E-4BB7-A054- 635664****</pre>	<p>An error occurs when an API operation is called.</p>	<p>Analyze the specific error cause based on the error information that is described in Error codes.</p>

Error codes

HTTP status code	Error code	Description	Description
403	InvalidDBName	The specified database name is not allowed.	The error message returned because the specified database names are invalid. For example, if the name of a database is the same as the name of a system database, the name of the database is invalid.
403	IncorrectDBInstanceState	Current DB instance state does not support this operation.	The error message returned because the RDS instance is not in a required state. For example, the RDS instance is in the Creating state.
400	IncorrectDBInstanceType	Current DB instance type does not support this operation.	The error message returned because the RDS instance does not run SQL Server.
400	IncorrectDBInstanceLockMode	Current DB instance lock mode does not support this operation.	The error message returned because the RDS instance is in a locking state that does not support the operation.
400	InvalidDBName.NotFound	Specified one or more DB name does not exist or DB status does not support.	<p>The error message returned because the specified databases cannot be found.</p> <ul style="list-style-type: none"> SQL Server 2008 R2: Create databases on the RDS instance before the data migration. Make sure that each database whose data you want to migrate from the self-managed instance has a counterpart with an identical name on the RDS instance. SQL Server 2012 and later: Make sure that each database whose data you want to migrate from the self-managed instance does not have a counterpart with an identical name on the RDS instance.
400	IncorrectDBType	Current DB type does not support this operation.	The error message returned because the operation is not supported by the database engine that is run on the RDS instance.
400	IncorrectDBState	Current DB state does not support this operation.	The error message returned because the databases are being created or receiving data from another migration task.

HTTP status code	Error code	Description	Description
400	UploadLimitExceeded	UploadTimesQuotaExceeded: Exceeding the daily upload times of this DB.	The error message returned because the number of data migration tasks that are performed on a single database on the day exceeds 20.
400	ConcurrentTaskExceeded	Concurrent task exceeding the allowed amount.	The error message returned because the number of data migration tasks that are performed on a single database on the day exceeds 500.
400	IncorrectFileExtension	The file extension does not support.	The error message returned because the file name extensions of the backup files are invalid.
400	InvalidOssUrl	Specified oss url is not valid.	The error message returned because the specified URL to download backup files from the OSS bucket is invalid.
400	BakFileSizeExceeded	Exceeding the allowed bak file size.	The error message returned because the total size of the backup files exceeds 3 TB.
400	FileSizeExceeded	Exceeding the allowed file size of DB instance.	The error message returned because the size of the data restored from the backup files exceeds the available storage of the RDS instance.

Related operations

Operation	Description
Create a migration task	Creates a migration task.
Open the database to which backup data is migrated	Opens a database.
Query migration tasks	Queries the migration tasks.
Query backup data files of migration task	Queries the details about the backup data files that are uploaded to an OSS bucket.

7.3. Migrate the data of an ApsaraDB RDS for SQL Server database to an on-premises SQL Server database

This topic describes how to migrate the data of an ApsaraDB RDS for SQL Server database to an on-premises SQL Server database by using a physical backup file.

You can also use Alibaba Cloud Data Transmission Service (DTS) to migrate the incremental data of an ApsaraDB RDS for SQL Server database to an on-premises SQL Server database.

Procedure

1. Download the full and incremental physical backup files of the source database and upload them to the server where the destination database resides.

For more information, see [Download the data backup files and log backup files of an ApsaraDB RDS for SQL Server instance](#).

If the server can communicate with the RDS instance on which the source database resides, you can run the `wget "url"` command to download the files. In this command, the `url` parameter specifies the URL from which you can download the files.

2. Decompress the full and incremental physical backup files that you downloaded.

Note The full and incremental physical backup files have the same name after decompression. We recommend that you rename the files in the following format: `<Database name>+<Backup method>+<Date>`. Examples:

- `testdb_datafull_201901071320.bak`, where `datafull` indicates a full backup
- `testdb_datadiff_201901071330.bak`, where `datadiff` indicates an incremental backup

3. Obtain the decompressed full and incremental physical backup files. Examples of the file save paths:

- `/tmp/testdb_datafull_201901071320.bak`: the save path of the full physical backup file
- `/tmp/testdb_datadiff_201901071330.bak`: the save path of the incremental physical backup file

4. Log on to the on-premises SQL Server console. Then, query the full and incremental physical backup files to obtain the logical names of the data and log files in the source database.

```
restore filelistonly from disk='/tmp/testdb_datafull_201901071320.bak'
go
```

In this example, the logical names of data and log files are `testdb` and `testdb_log`, respectively.

	LogicalName	PhysicalName	Type	FileGroupName	Size	MaxSize	FileId	CreateLSN	DropLSN
1	testdb	E:\SQLDATA\DATA\testdb.mdf	D	PRIMARY	4259840	35184372080640	1	0	0
2	testdb_log	E:\SQLDATA\DATA\testdb_log.ldf	L	NULL	1064960	2199023255552	2	0	0

5. Load the full physical backup file.


```
restore database testdb from disk='/tmp/testdb_datafull_201901071320.bak' with replace,
norecovery,stats=10,
move 'testdb' to '/var/opt/mssql/data/testdb.mdf',
move 'testdb_log' to '/var/opt/mssql/data/testdb_log.ldf'
go
```

Note

- `/var/opt/mssql/data/testdb.mdf` is the save path of the data file, and `testdb.mdf` is the logical name of the data file.
- `/var/opt/mssql/data/testdb_log.ldf` is the save path of the log file, and `testdb_log.ldf` is the logical name of the log file.

You can log on to the destination database and obtain the save paths of the data and log files from the file attributes.

After the full physical backup file is loaded, the status of the testdb database indicates that the database is being restored.

 **Note** If you only want to restore the data of the full physical backup file, skip step 6. Perform step 6 only when you want to restore the data of the incremental physical backup file.

6. Load the incremental physical backup file.

```
restore database testdb from disk='/tmp/testdb_datadiff_201901071330.bak' with replace,
norecovery,stats=10,
move 'testdb' to '/var/opt/mssql/data/testdb.mdf',
move 'testdb_log' to '/var/opt/mssql/data/testdb_log.ldf'
go
```

After the incremental physical backup file is loaded, the status of the testdb database indicates that the database is being restored.

7. Restore the testdb database.

```
restore database testdb with recovery
go
```

After the restoration is complete, the status of the testdb database indicates that the database is properly running.

7.4. Migrate data between ApsaraDB RDS for SQL Server instances

This topic describes how to use Data Transmission Service (DTS) to migrate data between RDS instances. DTS supports schema migration, full data migration, and incremental data migration. When you configure a data migration task, you can select all of the supported migration types to ensure service continuity.


Prerequisites

The database types of the RDS instances meet the following requirements.

Source database	Destination database
ApsaraDB RDS for MySQL ApsaraDB RDS for MariaDB TX	ApsaraDB RDS for MySQL ApsaraDB RDS for MariaDB TX
ApsaraDB RDS for SQL Server	ApsaraDB RDS for SQL Server
ApsaraDB RDS for PostgreSQL	ApsaraDB RDS for PostgreSQL

Precautions

- The data migration does not affect the data of the source RDS instance. During the data migration, DTS reads the data of the source RDS instance and replicates the data to the destination RDS instance. DTS does not delete the data of the source RDS instance. For more information, see [Design concept of data migration](#).
- DTS uses read and write resources of the source and destination databases during full data migration. This may increase the loads of the database servers. If the database performance is unfavorable, the specification is low, or the data volume is large, database services may become unavailable. For example, DTS occupies a large amount of read and write resources in the following cases: a large number of slow SQL queries are performed on the source database, the tables have no primary keys, or a deadlock occurs in the destination database. Before you migrate data, evaluate the impact of data migration on the performance of the source and destination databases. We recommend that you migrate data during off-peak hours. For example, you can migrate data when the CPU utilization of the source and destination databases is less than 30%.
- The tables to be migrated in the source database must have PRIMARY KEY or UNIQUE constraints and all fields must be unique. Otherwise, the destination database may contain duplicate data records.
- For data consistency purposes, we recommend that you do not write data to the source RDS instance during the data migration. This applies if you select the full data migration type.
- If the data migration task fails, DTS can automatically resume the task. Before you switch your workloads over to the destination RDS instance, you must stop or release the data migration task. Otherwise, the data on the source RDS instance overwrites the data on the destination RDS instance after the data migration task is resumed.
- DTS automatically creates databases on the destination RDS instance. If the name of a source database is invalid, you must log on to the destination RDS instance and create a destination database for that source database. This is required before you create the data migration task. In addition, the name of the created destination database must comply with the database naming conventions of Alibaba Cloud.

 **Note** For more information about how to create a database and the database naming conventions, see [Create accounts and databases for an ApsaraDB RDS instance that runs SQL Server 2017 EE](#).

- After the switchover of your workloads is complete, new log sequence numbers (LSNs) on the destination RDS instance do not increment from the largest LSN that is generated on the source RDS instance. Therefore, before you start the switchover, you must obtain the largest LSN that is generated on the source RDS instance. Then, you must specify the obtained LSN as the start LSN on the destination RDS instance. You can run the following commands to obtain the largest LSN that is generated on the source RDS instance:

```

do language plpgsql $$
declare
    nsp name;
    rel name;
    val int8;
begin
    for nsp,rel in select nspname,relname from pg_class t2 , pg_namespace t3 where t2.relname
espace=t3.oid and t2.relkind='S'
    loop
        execute format($_$select last_value from %I.%I$_$, nsp, rel) into val;
        raise notice '%',
            format($_$select setval('%I.%I'::regclass, %s);$_$, nsp, rel, val+1);
    end loop;
end;
$$;

```

Billing

Migration type	Task configuration fee	Internet traffic fee
Schema migration and full data migration	Free of charge.	Charged only when data is migrated from Alibaba Cloud over the Internet. For more information, see Pricing .
Incremental data migration	Charged. For more information, see Pricing .	

Migration types

- Schema migration

DTS migrates the schemas of the required objects from the source RDS instance to the destination RDS instance.



- Full data migration

DTS migrates historical data of the required objects from the source RDS instance to the destination RDS instance.

- Incremental data migration


After full data migration is completed, DTS synchronizes incremental data from the source RDS instance to the destination RDS instance. Incremental data migration allows you to ensure service continuity when you migrate data between RDS instances.

SQL operations that can be synchronized during incremental data migration

Scenario	Operation type	SQL statement
<ul style="list-style-type: none"> Migrate data between ApsaraDB RDS for MySQL instances Migrate data between ApsaraDB RDS for MariaDB TX instances Migrate data from an ApsaraDB RDS for MariaDB TX instance to an ApsaraDB RDS for MySQL instance 	DML	INSERT, UPDATE, DELETE, and REPLACE
	DDL	<ul style="list-style-type: none"> ALTER TABLE and ALTER VIEW CREATE FUNCTION, CREATE INDEX, CREATE PROCEDURE, CREATE TABLE, and CREATE VIEW DROP INDEX and DROP TABLE RENAME TABLE TRUNCATE TABLE
Migrate data between ApsaraDB RDS for SQL Server instances	DML	INSERT, UPDATE, and DELETE  Note If an UPDATE operation updates only the large fields, DTS does not synchronize the operation.
	DDL	<ul style="list-style-type: none"> ALTER TABLE, including only ADD COLUMN, DROP COLUMN, and RENAME COLUMN CREATE TABLE and CREATE INDEX  Note If a CREATE TABLE operation creates a partitioned table or a table that contains functions, DTS does not synchronize the operation. <ul style="list-style-type: none"> DROP TABLE RENAME TABLE TRUNCATE TABLE
Migrate data between ApsaraDB RDS for PostgreSQL instances Migrate data between ApsaraDB RDS for PPAS instances	DML	INSERT, UPDATE, and DELETE

Permissions required for database accounts

Scenario	Database	Schema migration	Full data migration	Incremental data migration
<ul style="list-style-type: none"> Migrate data between ApsaraDB RDS for MySQL instances Migrate data between ApsaraDB RDS for MariaDB TX instances Migrate data from an ApsaraDB RDS for MariaDB TX instance to an ApsaraDB RDS for MySQL instance 	Source instance	The SELECT permission	The SELECT permission	The REPLICATION SLAVE, REPLICATION CLIENT, SHOW VIEW, and SELECT permissions
	Destination instance	The read and write permissions	The read and write permissions	The read and write permissions
Migrate data between ApsaraDB RDS for SQL Server instances	Source instance	The SELECT permission	The SELECT permission	The owner permission on the objects to be migrated <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;"> ? Note A privileged account has the required permissions. </div>
	Destination instance	The read and write permissions	The read and write permissions	The read and write permissions




Scenario	Database	Schema migration	Full data migration	Incremental data migration
Migrate data between ApsaraDB RDS for PostgreSQL instances	Source instance	The USAGE permission on pg_catalog	The SELECT permission on the objects to be migrated	rds_superuser <div style="background-color: #e0f2f7; padding: 10px; border: 1px solid #ccc;"> <p> Note</p> <ul style="list-style-type: none"> • A standard account of an ApsaraDB RDS for PostgreSQL instance has the required permissions. • If you receive a message indicating that the database account does not have the permissions of the superuser role, you must upgrade the kernel version of the RDS instance. </div>

Scenario	Database	Schema migration	Full data migration	Incremental data migration
	Destination instance	The CREATE and USAGE permissions on the objects to be migrated	<p>The permissions of the database owner, including the permissions to perform the INSERT, UPDATE, and DELETE operations</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p>Note A standard account of an ApsaraDB RDS for PostgreSQL instance has the required permissions.</p> </div>	<p>The permissions of the database owner, including the permissions to perform the INSERT, UPDATE, and DELETE operations</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p>Note A standard account of an ApsaraDB RDS for PostgreSQL instance has the required permissions.</p> </div>


Procedure

1. Log on to the [DTS console](#).
2. In the left-side navigation pane, click **Data Migration**.
3. In the upper part of the **Migration Tasks** page, select the region where the RDS instance resides.
4. In the upper-right corner of the page, click **Create Migration Task**.
5. Configure the source and destination RDS instances.


The screenshot displays the '1. Configure Source and Destination' step of the migration task creation process. At the top, there are four progress indicators: '1. Configure Source and Destination' (active), '2. Configure Migration Types and Objects', '3. Map name modification', and '4. Precheck'. Below this, the 'Task Name' is set to 'RDS_TO_RDS'. The 'Source Database' section includes fields for Instance Type (RDS Instance), Instance Region (Singapore), RDS Instance ID, Database Account (dtstest), and Database Password. A 'Test Connectivity' button shows a 'Passed' status. The 'Destination Database' section has identical fields and a 'Test Connectivity' button also showing 'Passed'. At the bottom right, there are 'Cancel' and 'Set Whitelist and Next' buttons.

Section	Parameter	Description
None	Task Name	Enter the name that DTS generates for the data migration task. We recommend that you specify an informative name for easy identification. You do not need to specify a unique name.
Source Database	Instance Type	Select RDS Instance .
	Instance Region	Select the region where the source RDS instance resides.
	RDS Instance ID	Select the ID of the source RDS instance. <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p> Note The source and destination RDS instances can be the same or different. In theory, you can use DTS to migrate data within the same RDS instance or between two different RDS instances.</p> </div>
	Database Name	Enter the name of the source database on the source RDS instance. <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p> Note This parameter appears and needs to be set only when the source RDS instance runs PostgreSQL.</p> </div>
	Database Account	Enter the username of the account that you want to use to log on to the source RDS instance. For more information about the permissions required for the account, see Permissions required for database accounts .
	Database Password	Enter the password of the account that you want to use to log on to the source RDS instance. <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p> Note After you specify the information about the self-managed Oracle database, you can click Test Connectivity next to Database Password to check whether the information is valid. If the information is valid, the Passed message appears. If the Failed message appears, click Check next to Failed. Then, modify the information based on the check results.</p> </div>

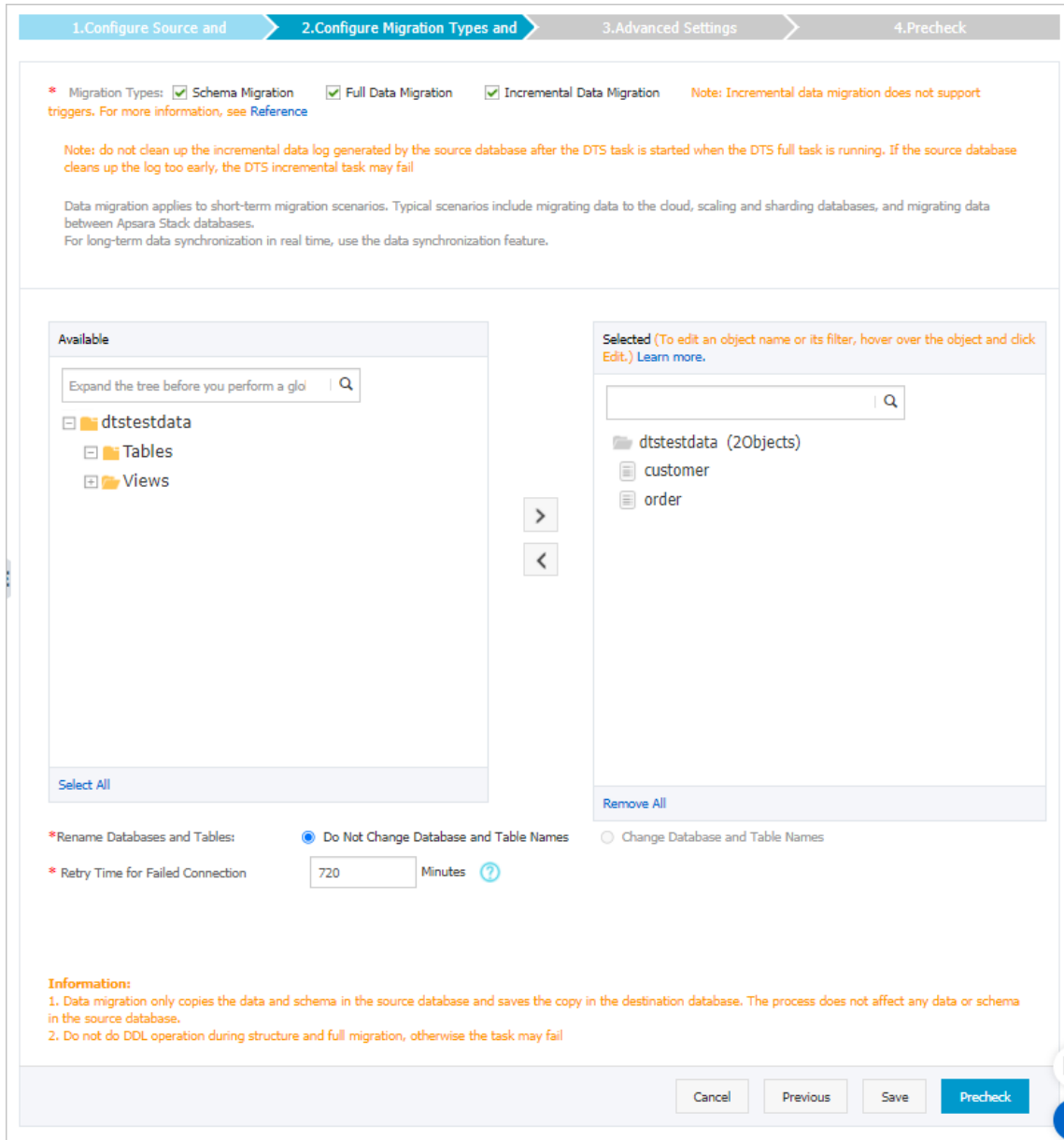
Section	Parameter	Description
	Encryption	<p>The type of connection that you want to establish. Select Non-encrypted or SSL-encrypted. If you select SSL-encrypted, you must enable SSL encryption for the source RDS instance before you create the data migration task. For more information, see Configure SSL encryption on an ApsaraDB RDS for SQL Server instance.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #d9e1f2;"> <p>Note</p> <p>This parameter appears and needs to be set only when the source RDS instance runs MySQL.</p> <p>The Encryption parameter is supported only in the Alibaba Cloud regions in mainland China and in the China (Hong Kong) region.</p> </div>
Destination Database	Instance Type	Select RDS Instance .
	Instance Region	Select the region where the destination RDS instance resides.
	RDS Instance ID	Select the ID of the destination RDS instance.
	Database Name	Enter the name of the destination database on the destination RDS instance. The name of the destination database can be different from the name of the source database.
	Database Account	Enter the username of the account that you want to use to log on to the destination RDS instance. For more information about the permissions required for the account, see Permissions required for database accounts .
	Database Password	Enter the password of the account that you want to use to log on to the destination RDS instance.
		<div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #d9e1f2;"> <p>Note</p> <p>After you specify the information about the RDS instance, you can click Test Connectivity next to Database Password to check whether the information is valid. If the information is valid, the Passed message appears. If the Failed message appears, click Check next to Failed. Then, modify the information based on the check results.</p> </div>

Section	Parameter	Description
	Encryption	<p>The type of connection that you want to establish. Select Non-encrypted or SSL-encrypted. If you select SSL-encrypted, you must enable SSL encryption for the destination RDS instance before you create the data migration task. For more information, see Configure SSL encryption on an ApsaraDB RDS for SQL Server instance.</p> <p> Note This parameter appears and needs to be set only when the destination RDS instance runs MySQL.</p> <p>The Encryption parameter is supported only in the Alibaba Cloud regions in mainland China and in the China (Hong Kong) region.</p>



6. In the lower-right corner of the page, click **Set Whitelist and Next**.

 **Note** In this step, DTS adds the IP address of the DTS server to the IP address whitelists of the source and destination RDS instances. This way, the DTS server can connect to the source and destination RDS instances.


7. Select the migration types and the objects that you want to migrate.




Parameter	Description
Migration Types	<p>Select the migration types based on your business requirements. The migration types must be supported by the database engine that is used.</p> <ul style="list-style-type: none"> ◦ If you want to migrate only the existing full data, select Schema Migration and Full Data Migration. ◦ If you want to migrate data without downtime, select Schema Migration, Full Data Migration, and Incremental Data Migration. <p>Note If the Incremental Data Migration type is not selected, do not write data to the source RDS instance during the data migration. This ensures data consistency between the source and destination RDS instances.</p>

Parameter	Description
Available	<p>Select one or more objects from the Available section and click the  icon to move the selected objects to the Selected section.</p> <div style="background-color: #e1f5fe; padding: 10px; border: 1px solid #cfcfcf;"> <p> Note</p> <ul style="list-style-type: none"> ○ You can select columns, tables, or databases as the objects to be migrated. If you select tables or columns as the objects to be migrated, DTS does not migrate other objects such as views, triggers, and stored procedures to the destination database. ○ By default, after an object is migrated to the destination database, the name of the object remains unchanged. You can use the object name mapping feature to rename the objects that are migrated to the destination database. For more information, see Object name mapping. ○ If you use the object name mapping feature to rename an object, other objects that are dependent on the object may fail to be migrated. </div>

8. Click **Precheck**.

 **Note**

- A precheck is performed before the migration task starts. The migration task only starts after the precheck succeeds.
- If the precheck fails, click the  icon next to each failed check item to view the related details. Fix the issues as instructed and run the precheck again.

9. After the data migration task passes the precheck, click **Next**.

10. In the **Confirm Settings** dialog box, configure the **Channel Specification** parameter. Then, read and select **Data Transmission Service (Pay-as-you-go) Service Terms**.


11. Click **Buy and Start** to start the data migration task.

○ Full data migration

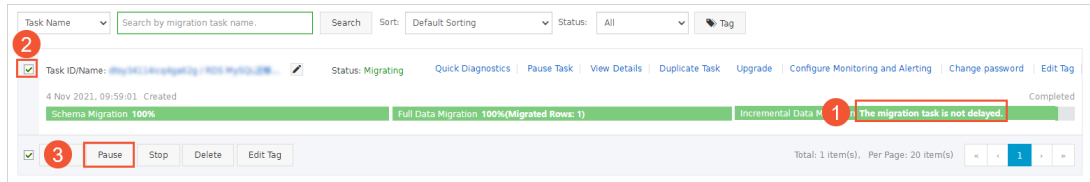
Do not manually stop a full data migration task. If you manually stop a full data migration task, the data that is migrated to the RDS instance may be incomplete. You can wait until the full data migration task automatically stops.

○ Incremental data migration

An incremental data migration task does not automatically stop. You must manually stop the task.

 **Note** We recommend that you manually stop an incremental data migration task at an appropriate point in time. For example, you can stop the task during off-peak hours or before you switch your workloads over to the RDS instance.

- a. Wait until **Incremental Data Migration** and **The data migration task is not delayed** appear in the progress bar of the data migration task. Then, stop writing data to the self-managed Oracle database for a few minutes. The delay time of **incremental data migration** may be displayed in the progress bar.
- b. Wait until the status of **incremental data migration** changes to **The data migration task is not delayed**. Then, manually stop the migration task.



8. Billing

8.1. Switch an ApsaraDB RDS for SQL Server instance from pay-as-you-go to subscription

This topic describes how to switch an ApsaraDB RDS for SQL Server instance from pay-as-you-go to subscription.

Prerequisites

- The instance type of your RDS instance is not phased out. For more information, see [Primary instance types](#). If your RDS instance uses a phased-out instance type, you must change the instance type before you switch your RDS instance from pay-as-you-go to subscription. For more information, see [Change the specifications of an ApsaraDB RDS for SQL Server instance](#).
- Your RDS instance uses the pay-as-you-go billing method.
- Your RDS instance is in the Running state.
- Your RDS instance does not have an unpaid subscription order.

Impacts


A billing method change for your RDS instance does not affect the workloads on your RDS instance.

Precautions

If your RDS instance has an unpaid subscription order, the order becomes invalid when you change the instance type. In this case, you must cancel the order in the [Billing Management](#) console. Then, you can change the billing method of your RDS instance again.

Procedure

1. Log on to the [ApsaraDB RDS console](#). In the left-side navigation pane, click **Instances**. In the top navigation bar, select the region where your RDS instance resides.
2. Find your RDS instance and use one of the following methods to go to the **Switch to Subscription Billing** page:
 - Click **Switch to Subscription Billing** in the **Billing Method** column.
 - Click the ID of your RDS instance. In the **Status** section of the page that appears, click **Subscription Billing** on the right of **Billing Method**.
3. Configure the **Duration** parameter. Then, read and select Terms of Service.
4. Click **Pay Now**.

 **Note** ApsaraDB RDS generates a subscription order. You must pay for the order. If the order is not paid or canceled, you cannot purchase an RDS instance or change the billing method of your RDS instance from pay-as-you-go to subscription. You can pay for or cancel the order in the [Billing Management](#) console.

5. Complete the payment.

Related operations

Operation	Description
Change the billing method	Changes the billing method of an ApsaraDB RDS instance.

8.2. Switch an ApsaraDB RDS for MySQL instance from subscription to pay-as-you-go

This topic describes how to switch an ApsaraDB RDS for MySQL instance from the subscription billing method to the pay-as-you-go billing method based on your business requirements.

Prerequisites


- Your RDS instance uses the subscription billing method. For more information about the billing methods of ApsaraDB RDS, see [Billable items, billing methods, and pricing](#).
- Your RDS instance is in the Running state.
- Your RDS instance does not use a phased-out instance type. For more information, see [Primary instance types](#). If your RDS instance uses a phased-out instance type, you must change the instance type before you switch your RDS instance to the pay-as-you-go billing method.

Billing

After you switch your RDS instance to the pay-as-you-go billing method, a refund is returned based on the payment method that is used.


Refund = Fee actually paid - Fee for consumed resources

- The fee actually paid is the money that you paid and does not include the part that is covered by coupons or vouchers.
- The fee for consumed resources is calculated based on the following formula: Fee for consumed resources = Daily fee x Consumed subscription duration x Discount for the consumed subscription duration. The daily fee is equal to the order-specific fee divided by 30.

 **Note** The consumed subscription duration is accurate to the day. The part that is less than one day is counted as one day.

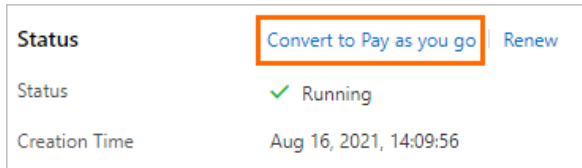
Impacts

When you switch your RDS instance to the pay-as-you-go billing method, the workloads on your RDS instance run as normal.

 **Note** The subscription billing method is more cost-effective than the pay-as-you-go billing method, and you are offered higher discounts for longer subscription periods. For long-term use, we recommend that you select the subscription billing method.

Procedure

- 1.
2. In the Status section of the **Basic Information** page, click **Convert to Pay as you go**.



3. Confirm the configuration of your RDS instance, read and select Terms of Service, click **Pay Now**, and then complete the payment.


Related operations

Operation	Description
Change the billing method	Changes the billing method of an ApsaraDB RDS instance.

8.3. Manually renew an ApsaraDB RDS for SQL Server instance

This topic describes how to manually renew an ApsaraDB RDS for SQL Server instance. If your RDS instance uses subscription billing, you must renew it before it expires. This allows you to prevent service interruptions and data loss.

For more information about the impacts caused by subscription expiration, see [Unlock or rebuild an expired or overdue ApsaraDB for RDS instance](#).

 **Note** RDS instances that use the pay-as-you-go billing method do not expire and therefore do not require renewal.

You can manually renew your RDS instance before it expires or within 15 days after it expires.

Method 1: Renew an RDS instance in the ApsaraDB RDS console

Renew a single RDS instance

- 1.
2. In the **Status** section of the page that appears, click **Renew** on the right.
3. On the **Renew** page, configure the **Duration** parameter. You are offered lower prices for longer subscription periods.
4. Read and select Terms of Service, click **Pay Now**, and then complete the payment.

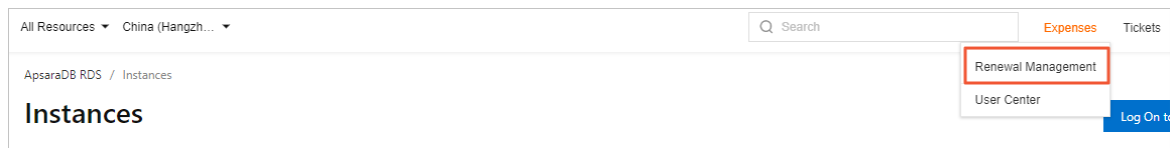
Renew multiple RDS instances at a time

- 1.
2. Select the RDS instances that you want to renew and click **Renew** below the instance list.
3. In the **Renew** dialog box, confirm the selected RDS instances and click **OK** to go to the **Renewal** page.
4. On the **Manual** tab, select the RDS instances and click **Batch Renew** in the lower part of the page.

- Configure the **Duration** parameter of each RDS instance, click **Pay**, and then complete the payment.

Method 2: Renew the instance in the Billing Management console

- Log on to the [ApsaraDB RDS console](#).
- In the top navigation bar, choose **Expenses > Renewal Management**.



- On the **Manual** tab of the Renewal page, find the RDS instances that you want to renew. You can renew one or more RDS instances at a time.

- o **Renew a single RDS instance**

- Find the RDS instance that you want to renew and click **Renew** in the Actions column.

Note If the RDS instance is displayed on the **Auto** or **Nonrenewal** tab, you can click **Enable Manual Renewal** in the Actions column and then click **OK** in the message that appears to manually renew the RDS instance.

- On the page that appears, configure the Duration parameter, click **Pay Now**, and then complete the payment.

- o **Renew multiple RDS instances at a time**

- Select the RDS instances that you want to renew and click **Batch Renew** in the lower part of the page.
- Configure the **Duration** parameter of each RDS instance, click **Pay**, and then complete the payment.

Enable auto-renewal

If you enable auto-renewal for your RDS instance, you do not need to manually renew your RDS instance. If your Alibaba Cloud account has a sufficient balance, your RDS instance never expires. For more information, see [Enable auto-renewal for an ApsaraDB RDS for SQL Server instance](#).

8.4. Enable auto-renewal for an ApsaraDB RDS for SQL Server instance

This topic describes how to enable auto-renewal for an ApsaraDB RDS for SQL Server instance. If your RDS instance uses subscription billing, you can enable auto-renewal. This relieves the need to manually renew your RDS instance. Make sure that your Alibaba Cloud account has a sufficient balance, and your RDS instance will never expire.

If your RDS instance uses the subscription billing method, subscription instances can expire. If you do not renew your RDS instance before it expires, your service is interrupted and data may be lost. For more information, see [Unlock or rebuild an expired or overdue ApsaraDB for RDS instance](#).

Note RDS instances that use the pay-as-you-go billing method do not expire and therefore do not require renewal.

Precautions

- If you enable auto-renewal, the first time when the system deducts fees from your Alibaba Cloud account comes at 08:00:00 three days before your RDS instance expires. If the deduction fails, the system will attempt to deduct the fee every day for the next two days.

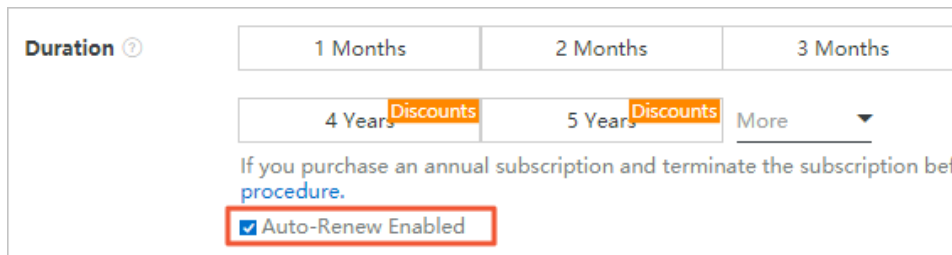
Note Make sure that the balance of your Alibaba Cloud account is sufficient. Otherwise, the renewal fails. If all the three automatic fee deduction attempts fail, you must manually renew your RDS instance in a timely manner to avoid service interruption and data loss.

- If you manually renew your RDS instance before the automatic fee deduction, the system will automatically renew the instance next time before the expiration.
- After you enable auto-renewal, it takes effect the next day. If your RDS instance is due to expire the next day, renew it manually to avoid service interruption. For more information, see [Manually renew an ApsaraDB RDS for SQL Server instance](#).

Enable auto-renewal when you purchase an RDS instance

Note If you select auto-renewal when you purchase an RDS instance, the system automatically renews the RDS instance based on the specified renewal cycle. The renewal cycle is one month or one year. For example, if you select auto-renewal when you purchase an RDS instance with a six-month subscription, the system automatically renews the RDS instance with a one-month subscription each time the instance is due to expire.

When you purchase a subscription RDS instance, select **Auto-Renew Enabled**.

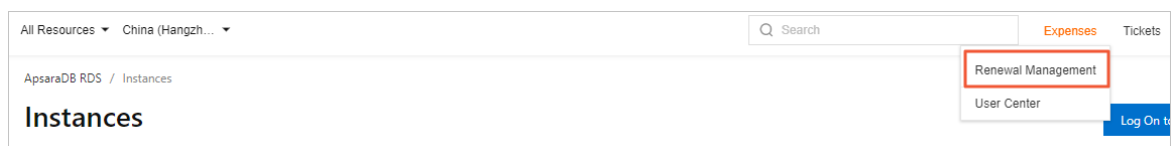


The screenshot shows a selection interface for RDS instance duration. It includes buttons for '1 Months', '2 Months', and '3 Months' in the top row, and '4 Years Discounts', '5 Years Discounts', and 'More' in the bottom row. Below the buttons, there is a note: 'If you purchase an annual subscription and terminate the subscription before the expiration date, you must follow the cancellation procedure.' At the bottom, there is a checkbox labeled 'Auto-Renew Enabled' which is checked and highlighted with a red box.

Enable auto-renewal after you purchase an RDS instance

Note After you enable auto-renewal for a created RDS instance, the system automatically renews the RDS instance based on the selected renewal cycle. For example, if you select a three-month renewal cycle, you are charged for a three-month subscription in each renewal cycle.

1. Log on to the [ApsaraDB RDS console](#).
2. In the top navigation bar, choose **Expenses > Renewal Management**.



3. On the **Manual** or **Nonrenewal** tab, specify the filter conditions to find the RDS instance for which you want to enable auto-renewal. You can enable auto-renewal for one or more RDS instances at a time.

- o Enable auto-renewal for a single RDS instance.
 - a. Find the RDS instance and in the Actions column click **Enable Auto Renewal**.

ApsaraDB for RDS	rm-1-...	-	China (Hangzhou)	17 Days	Subscription	2020-05-21 10:00:31 2020-07-24 00:00:00	Renew Enable Auto Renewal Nonrenewal
ApsaraDB for RDS	rm-1-...	-	China (Hangzhou)	47 Days	Subscription	2020-05-20 16:03:49 2020-08-23 00:00:00	Renew Enable Auto Renewal Nonrenewal

- b. In the dialog box that appears, specify the **Unified Auto Renewal Cycle** parameter and click **Auto Renew**.

The following **1** instances will be automatically renewed after expiration. The uniform **Unified Auto Renewal Cycle** is set to **1 Month**

Instance ID/Name	Expire At	Expire Within
rm-1-... / -	2020-07-24 00:00:00	17 Days

Auto Renew Activate Later

- o Enable auto-renewal for multiple RDS instances.

Select the RDS instances and click **Enable Auto Renewal** below the instance list.

Manual 4

Auto 6

Nonrenewal

-	Instance	Instance ID/Name	Database type
<input type="checkbox"/>	ApsaraDB for RDS	rm-1-...	-
<input type="checkbox"/>	ApsaraDB for RDS	rm-1-...	-
<input checked="" type="checkbox"/>	ApsaraDB for RDS	rm-1-...	-
<input checked="" type="checkbox"/>	ApsaraDB for RDS	rm-1-...	-

-
2 items selected

Bulk Renewal

Enable Auto Renewal

Set as Nonrenewal

Export Renewal Bill

- o In the dialog box that appears, specify the **Unified Auto Renewal Cycle** parameter and click **Auto Renew**.

Enable Auto Renewal ✕

1. After you enable auto renewal, the service fee is deducted 9 days before the instance expires. Ensure that the payment account balance is sufficient. If your instance expires on the next day, please manually renew the instance.
2. If you manually renew the instance before the fee deduction date, the system automatically renews the instance based on its new validity period. Auto renewal takes effect on the next day after you enable it. Vouchers can be used in renewal.
3. Auto renewal takes effect on the next day after you enable it. Vouchers can be used in renewal.

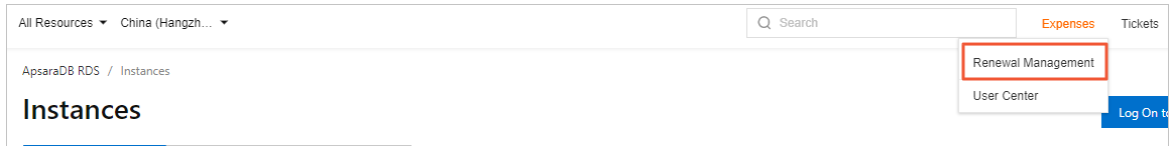
The following **2** instances will be automatically renewed after expiration. The uniform **Unified Auto Renewal Cycle** is set to **1 Month**

Instance ID/Name	Expire At	Expire Within
rm-1-... / -	2020-08-23 00:00:00	47 Days
rm-1-... / -	2021-05-22 00:00:00	319 Days

Auto Renew Activate Later

Change the auto-renewal cycle

1. Log on to the [ApsaraDB RDS console](#).
2. In the top navigation bar, choose **Expenses > Renewal Management**.



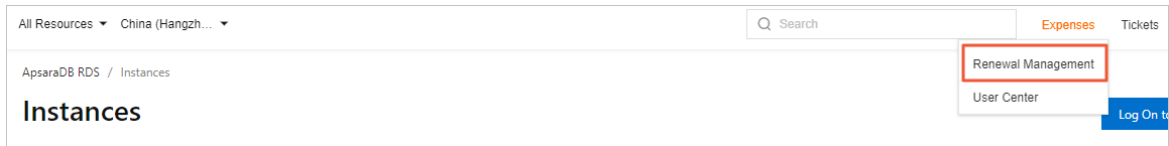
- On the **Auto** tab, specify filter conditions to find the RDS instance for which you want to enable auto-renewal. Then, select the RDS instance and click **Edit Auto Renewal** in the Actions column.



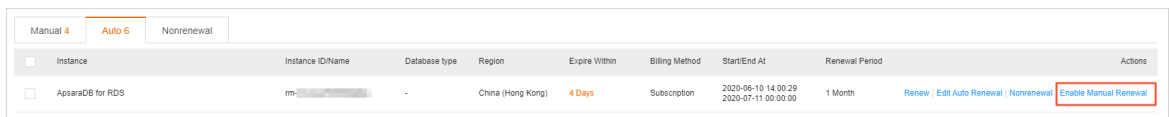
- In the dialog box that appears, change the auto-renewal cycle and click **OK**.

Disable auto-renewal

- Log on to the [ApsaraDB RDS console](#).
- In the top navigation bar, choose **Expenses > Renewal Management**.



- On the **Auto** tab, specify filter conditions to find the RDS instance for which you want to enable auto-renewal. Then, select the RDS instance and click **Enable Manual Renewal** in the Actions column.



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

Related operations

Operation	Description
Create an instance	<p>Creates an ApsaraDB RDS instance.</p> <p>Note You can call this operation to enable auto-renewal for an RDS instance that you want to create.</p>
Manually renew an ApsaraDB for RDS instance	<p>Renews an ApsaraDB RDS instance.</p> <p>Note You can call this operation to enable auto-renewal for a created RDS instance.</p>

9. Manage pending events

If your ApsaraDB RDS instance has an event pending to be processed, the ApsaraDB RDS console notifies you of the event, so you can handle the event at your earliest opportunity.

You can receive text messages, voice messages, and emails that notify you of pending events such as instance migration and version upgrade events. In addition, after you log on to the ApsaraDB RDS console, you are prompted to manage the pending events. You can view the types, regions, processes, precautions, and affected instances of the pending events. You can also change the value of the Scheduled Disconnection Time parameter.

Prerequisites

A pending event is found, which is an O&M event.

Note If pending events are found, you can see notification badges on the **Pending Events** button in the upper-right corner of the ApsaraDB RDS homepage.

Precautions

You are notified of ApsaraDB for Redis pending events such as instance migrations or version upgrades at least three days before the events occur. Notifications for high-risk vulnerability fixes are sent three or fewer days before execution due to the urgency of these events. Event notifications are sent by using phone calls, emails, internal messages, or the ApsaraDB for Redis console. To use this feature, log on to the [Message Center](#) console, enable **ApsaraDB Fault or Maintenance Notifications**, and then specify a contact. We recommend that you specify an O&M engineer as the contact.

Message Center settings

Message Center	<input type="checkbox"/> Fault Message	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Internal Messages	<input type="checkbox"/> ECS Fault Notifications	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Account Contact Modify
Message Settings	<input type="checkbox"/> ApsaraDB Fault or Maintenance Notifications	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Account Contact Modify
Common Settings	<input type="checkbox"/> Emergency Risk Warnings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Account Contact Modify

Procedure

1. Log on to the [ApsaraDB RDS console](#).
2. Click **Events Center** in the left-side navigation pane or click **Pending Events** upper-right corner of the ApsaraDB RDS homepage.

Note If a pending event requires you to schedule the time to handle the event, a message appears, which prompts you to schedule the time at your earliest opportunity.

3. On the **Pending Events** page, select the type and region of the event that you want to handle.

Note The content of the notification for an event varies based on the value of **Event Type**. The notification provides the process and precautions for the event.

4. View details about the event in the instance list. If you want to change the value of **Scheduled**


Disconnect ion Time, select an RDS instance and click **Specify Disconnect ion Time**. In the dialog box that appears, specify the time and click **OK**.

Note

- The information that is displayed for an event varies based on the type of the event.
- The value of **Scheduled Disconnect ion Time** cannot be later than the time that is displayed in the **Set Before** column.

Causes and impacts of events

Cause	Impact type	Impact description
Instance migration	Transient connections	<p>From the time specified by the RDS instance is subject to the following impacts:</p> <ul style="list-style-type: none"> • The RDS instance or its database shards experience transient connections and stay in the read-only state for up to 30 seconds until all data is synchronized. We recommend that you perform the operation during off-peak hours and make sure that your application is configured to automatically reconnect to your database system. • The RDS instance cannot work as expected for Data Management (DMS) or Data Transmission Service (DTS). After the operation is complete, the RDS instance is automatically recovered. <p>Scheduled Disconnect ion Time</p>
Primary/secondary switchover		
SSL certificate update		
Backup mode change		
Minor engine version update	Transient connections	<p>From the time specified by the RDS instance is subject to the following impacts:</p> <ul style="list-style-type: none"> • The RDS instance or its database shards experience transient connections and stay in the read-only state for up to 30 seconds until all data is synchronized. We recommend that you perform the operation during off-peak hours and make sure that your application is configured to automatically reconnect to your database system. • The RDS instance cannot work as expected for Data Management (DMS) or Data Transmission Service (DTS). After the operation is complete, the RDS instance is automatically recovered.
	Differences between minor engine versions	<p>Different minor engine versions provide different features. Before you update the minor engine version of the RDS instance, you must take note of the differences between the previous and new minor engine versions. For more information, see the release notes of minor engine versions.</p> <ul style="list-style-type: none"> • ApsaraDB RDS: Release notes of minor AliSQL versions, Release notes of minor AliPG versions, and Release notes of minor ApsaraDB RDS for SQL Server versions. • Engine release notes, Release notes and Release notes.

Cause	Impact type	Impact description
Proxy version upgrade	Transient connections	<p>From the time specified by the RDS instance is subject to the following impacts:</p> <ul style="list-style-type: none"> The RDS instance or its database shards experience transient connections and stay in the read-only state for up to 30 seconds until all data is synchronized. We recommend that you perform the operation during off-peak hours and make sure that your application is configured to automatically reconnect to your database system. The RDS instance cannot work as expected for Data Management (DMS) or Data Transmission Service (DTS). After the operation is complete, the RDS instance is automatically recovered.
	Differences between proxy versions	Different proxy versions provide different features. Before you upgrade the proxy version of the RDS instance, you must take note of the differences between the previous and new proxy versions.
Network upgrade	Transient connections	<p>From the time specified by the RDS instance is subject to the following impacts:</p> <ul style="list-style-type: none"> The RDS instance or its database shards experience transient connections and stay in the read-only state for up to 30 seconds until all data is synchronized. We recommend that you perform the operation during off-peak hours and make sure that your application is configured to automatically reconnect to your database system. The RDS instance cannot work as expected for Data Management (DMS) or Data Transmission Service (DTS). After the operation is complete, the RDS instance is automatically recovered.
	VIP connection errors	<p>Network upgrades may involve cross-zone data migration. In this case, the virtual IP address (VIP) of the RDS instance changes. If a database client uses a VIP to connect to the RDS instance, the connection is interrupted.</p> <div style="background-color: #e1f5fe; padding: 10px; border: 1px solid #cfcfcf;"> <p> Note We recommend that you use a domain name to connect to the RDS instance and disable the DNS cache of your application and the DNS cache of the server on which your application runs.</p> </div>

10. Version upgrade

10.1. 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 [Features of ApsaraDB RDS instances that run different SQL Server versions and RDS editions](#).

Billing description

For details about the billing for version upgrade, see [Specification change fees](#).

Impact

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


Prerequisites

The SQL Server version and RDS edition are as follows:

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

Precautions

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

 **Warning** We recommend that you [create a pay-as-you-go instance](#) to test the version compatibility before the upgrade.

Procedure

For more information, see [Upgrade from Basic Edition to High-availability Edition](#).

10.2. Upgrade an ApsaraDB RDS for SQL Server instance 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.

In the Basic Edition, your RDS instance does not have a secondary instance as a hot standby. For more information, see [RDS Basic Edition](#). If you are changing the specifications or upgrading the SQL Server version of your RDS instance, your database service becomes unavailable. If your RDS instance fails unexpectedly, your database service also becomes unavailable. The unavailability may last for a long period.

In the High-availability Edition, your RDS instance has a secondary RDS instance as a hot standby. For more information, see [High-availability Edition](#). Data is synchronized in real time between your RDS instance and its secondary instance. If your RDS instance cannot be connected, your workloads are automatically switched over to the secondary instance. The High-availability Edition provides a complete suite of features, including auto scaling, backup and restoration, performance optimization, and read/write splitting.

For more information about the features that are provided by different SQL Server versions on each RDS edition, see [Features of ApsaraDB RDS instances that run different SQL Server versions and RDS editions](#).

Fee


For more information about the upgrade fee, see [Specification change fees](#).

Impacts

After the upgrade is complete, you must switch over your workloads. The downtime caused by the switchover varies based on the data volume of your RDS instance. In most cases, the switchover requires approximately 20 minutes. We recommend that you switch over your workloads during the specified maintenance window. Make sure that your applications are configured to automatically reconnect to your database system.


Prerequisites

Your RDS instance runs Basic Edition.

 **Note** You can view the edition of your RDS instance on the [Basic Information](#) page.

Precautions

- After the upgrade is complete, your RDS instance cannot be rolled back to an earlier version or edition.

 **Warning** Before you start the upgrade, we recommend that you create a pay-as-you-go RDS instance that uses the destination SQL Server version and RDS edition. Also, configure other settings for this new RDS instance the same as those of your existing RDS instance. Then, you can test the compatibility between the two instances. For more information, see [Create an ApsaraDB RDS for SQL Server instance](#).

- The following table lists upgrade rules. Upgrade rules


Source SQL Server version and RDS edition	Destination SQL Server version and RDS edition
SQL Server 2016 EE on RDS Basic Edition	SQL Server 2016 EE on RDS High-availability Edition
SQL Server 2012 EE Basic on RDS Basic Edition	SQL Server 2016 EE on RDS High-availability Edition
	SQL Server 2012 EE on RDS High-availability Edition

Source SQL Server version and RDS edition	Destination SQL Server version and RDS edition
SQL Server 2016 SE on RDS Basic Edition	SQL Server 2016 SE on RDS High-availability Edition
	SQL Server 2016 EE on RDS High-availability Edition
SQL Server 2012 SE on RDS Basic Edition	SQL Server 2016 EE on RDS High-availability Edition
	SQL Server 2016 SE on RDS High-availability Edition
	SQL Server 2012 EE on RDS High-availability Edition
	SQL Server 2012 SE on RDS High-availability Edition
SQL Server 2016 Web on RDS Basic Edition	SQL Server 2016 EE on RDS High-availability Edition
	SQL Server 2016 SE on RDS High-availability Edition
SQL Server 2012 Web on RDS Basic Edition	SQL Server 2016 EE on RDS High-availability Edition
	SQL Server 2016 SE on RDS High-availability Edition
	SQL Server 2012 EE on RDS High-availability Edition
	SQL Server 2012 SE on RDS High-availability Edition

Procedure

- 1.
2. On the **Basic Information** page, click **Upgrade Version**. In the message that appears, click **OK**.
3. On the **Upgrade Engine Version** page, configure the following parameters.

Parameter	Description
Upgrade To	Select the destination SQL Server version. The available Edition , Storage Type , and CPU and Memory settings vary based on the selected destination SQL Server version.
Edition	Select High-availability . The High-availability Edition allows your RDS instance to stand as a primary instance and have a secondary instance as a hot standby. The primary and secondary RDS instances work in the classic high-availability architecture to achieve balanced performance in all aspects.
Storage Type	<ul style="list-style-type: none"> ◦ Standard SSD: A standard SSD is an elastic block storage device that is designed based on the distributed storage architecture. You can store data on standard SSDs to separate computing from storage. ◦ Enhanced SSD: An enhanced SSD is an ultra-high performance disk that is designed by Alibaba Cloud based on the next-generation distributed block storage architecture. It integrates 25 Gigabit Ethernet and remote direct memory access (RDMA) technologies. This reduces one-way latency and delivers up to 1 million random input/output operations per second (IOPS).

Parameter	Description
Zone	Select the destination zone. Multi-zone deployment is supported.
CPU and Memory	Select the new specifications. Each instance type supports a specific number of CPU cores, memory capacity, maximum number of connections, and maximum IOPS. For more information, see Primary ApsaraDB RDS instance types .
Network Type	<p>Classic Network is unavailable. You must specify the VPC information.</p> <ul style="list-style-type: none"> ◦ If your RDS instance is connected over the classic network before the upgrade, you can change its network type to VPC and configure a vSwitch. ◦ If your RDS instance is connected over a VPC or over both the classic network and a VPC before the upgrade, you cannot change its VPC. However, you can change its vSwitch.
vSwitch	<p>Select the destination vSwitch. If you select multiple zones for your RDS instance, you must select multiple destination vSwitches.</p> <div style="background-color: #e1f5fe; padding: 10px; border: 1px solid #cfe2f3;"> <p> Note</p> <ul style="list-style-type: none"> ◦ If your RDS instance is connected over a VPC or over both the classic network and a VPC before the upgrade, you cannot change its VPC. However, you can change its vSwitch. The available vSwitches vary based on the specified zone and VPC. ◦ If you select the default VPC, the destination vSwitch can be either the default vSwitch or a custom vSwitch. ◦ If you do not select the default VPC, the destination vSwitch must be a custom vSwitch. </div>
Switching Time	<ul style="list-style-type: none"> ◦ Switch Immediately After Data Migration: Data is migrated and workloads are switched over immediately. ◦ Switch Within Maintenance Window: Data is migrated immediately, and workloads are switched over during the specified maintenance window.

Upgrade To : 2016 SE ▼

Edition : High-availability [Learn more](#) ⓘ

Storage Type : Enhanced SSD
(Recommended) ESSD PL2
(Recommended) ESSD PL3
(Recommended) [Learn more](#)

Zone : Hangzhou Zone H ▼

CPU and Memory : 2核4GB (通用型) ▼
(Instance Type: mssql.s2.medium.s2) ⓘ
This instance type does not limit the number of connections and IOPS.

Network Type : Classic Network VPC [Learn more](#) ⓘ

Private(172.16.0.0/16)(Default) ▼

To create a VPC or VSwitch, go to the [VPC console](#). If you cannot find the latest VPC in the drop-down list, click [here](#) to refresh the list.

VSwitch : vsw-bp10aqj6o4lclxdrm6nb5(172.16.192.0/20) ▼

Location:ZoneH, Available Private IPs: 4016

Switching Time : **Switch Immediately After Data Migration**
 Switch Within Maintenance Window (Current Setting: 02:00-06:00 [\[Modify\]](#))
 Switch at Specified Time

After the version upgrade is complete, there is switchover downtime. The switchover downtime depends on the instance size and usually takes less than 20 minutes. We recommend that you perform the switchover during the maintenance period. Make sure that your applications can automatically reconnect to the database when the connection becomes available again.

4. Select Product Terms of Service and click **Confirm**.

Change the endpoints of your RDS instance

After the upgrade, your RDS instance resides in a VPC. The following table describes how to change the endpoints of your RDS instance after the upgrade based on the original network type of your RDS instance.

Original network type	Change rule
Classic network	<p>After the upgrade, your RDS instance is connected over both the classic network and a VPC:</p> <ul style="list-style-type: none"> The original classic network endpoint remains available and never expires. A VPC endpoint is generated for your RDS instance based on the specified VPC.
VPC	<p>After the upgrade, your RDS instance is connected over a VPC. The original VPC endpoint remains available. However, the virtual IP address (VIP) that is bound to the original VPC endpoint may change.</p>
Classic network and VPC	<p>After the upgrade, your RDS instance is connected over both the classic network and a VPC. The original classic network and VPC endpoints remain available. The expiration time of the classic network endpoint remains unchanged.</p>

10.3. Upgrade an ApsaraDB RDS for SQL Server instance with local SSDs from SQL Server 2008 R2 to SQL Server 2012 or SQL Server 2016

This topic describes how to upgrade an ApsaraDB RDS for SQL Server instance with local SSDs from SQL Server 2008 R2 to SQL Server 2012 or 2016. During the upgrade, you can also migrate the RDS instance across zones.

Alibaba Cloud has stopped providing security updates for ApsaraDB RDS for SQL Server 2008 R2 instances that were purchased on and after July 9, 2019. For more information, see [\[Notice\] Supplementary service agreement for RDS SQL Server 2008 R2](#). We recommend that you upgrade your SQL Server version at the earliest opportunity.

For more information about the features that are provided by different SQL Server versions on each RDS edition, see [Features of ApsaraDB RDS instances that run different SQL Server versions and RDS editions](#).

Billing


For more information about the upgrade fees, see [Specification change fees](#).

Impacts

After the upgrade is complete, you must switch over your workloads. The downtime caused by the switchover varies based on the data volume of your RDS instance. In most cases, the switchover requires approximately 20 minutes. We recommend that you switch over your workloads during the specified maintenance window. Make sure that your applications are configured to automatically reconnect to your database system.

Prerequisites

- Your RDS instance runs SQL Server 2008 R2 with local SSDs.
- The total storage capacity of your RDS instance is no less than 20 GB.
- The Transparent Data Encryption (TDE) feature is disabled for the RDS instance. For more information, see [TDE](#).

 **Note** If the TDE feature is enabled, you must disable the TDE feature for all databases. Then, you must submit a ticket to disable TDE for your RDS instance.

Precautions

- After the upgrade is complete, your RDS instance cannot be rolled back to an earlier version.

 **Warning** Before you start the upgrade, we recommend that you create a temporary RDS instance that runs the destination SQL Server version. Also, configure other settings for this new RDS instance the same as those of your existing RDS instance. Then, you can test the compatibility between the two instances. For more information, see [Create a temporary RDS instance that runs the destination SQL Server version](#).

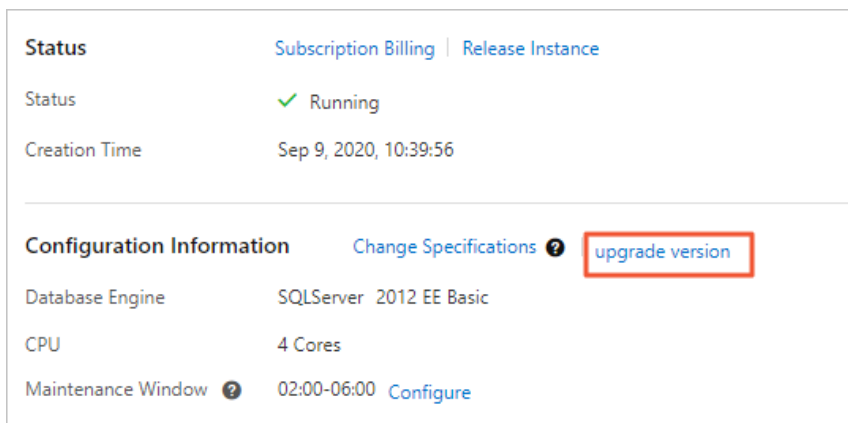
- You can upgrade your RDS instance with local SSDs from SQL Server 2008 R2 to the following versions:
 - SQL Server 2012 EE
 - SQL Server 2016 SE
 - SQL Server 2016 EE
- If you upgrade your RDS instance to SQL Server 2012 EE or 2016 EE, the TDE feature remains available. If you upgrade your RDS instance to SQL Server 2016 SE, the TDE feature becomes unavailable.

Limits

If the SSL encryption feature is enabled for the RDS instance, you cannot directly upgrade the RDS instance. In this case, you can submit a .


Procedure

-
- On the **Basic Information** page, click **Upgrade Version**. In the message that appears, click **OK**.



- On the **Upgrade Engine Version** page, configure the following parameters.

Parameter	Description
Upgrade To	Select the destination SQL Server version. The available Edition , Storage Type , and CPU and Memory settings vary based on the selected destination SQL Server version.
Edition	Select High-availability . The High-availability Edition allows your RDS instance to stand as a primary instance and have a secondary instance as a hot standby. The primary and secondary RDS instances work in the classic high-availability architecture to achieve balanced performance in all aspects.
Storage Type	<ul style="list-style-type: none"> Standard SSD: A standard SSD is an elastic block storage device that is designed based on the distributed storage architecture. You can store data on standard SSDs to separate computing from storage. Enhanced SSD: An enhanced SSD (ESSD) is an ultra-high performance disk that is designed by Alibaba Cloud based on the next-generation distributed block storage architecture. ESSDs deliver ultra high storage performance. ESSDs are integrated with 25 Gigabit Ethernet and remote direct memory access (RDMA) technologies. ESSDs can help you reduce one-way latencies and process up to 1 million read and write requests at random per second.

Parameter	Description
Zone	Select the destination zone. Multi-zone deployment is supported.
CPU and Memory	Select the new specifications. Each instance type supports a specific number of CPU cores, memory capacity, maximum number of connections, and maximum IOPS. For information, see Primary ApsaraDB RDS instance types .
Network Type	<p>Classic Network is unavailable. You must specify the virtual private cloud (VPC) information.</p> <ul style="list-style-type: none"> ◦ If your RDS instance is connected over the classic network before the upgrade, you can change its network type to VPC and configure a vSwitch. ◦ If your RDS instance is connected over a VPC or over both the classic network and a VPC before the upgrade, you cannot change its VPC. However, you can change its vSwitch. The available vSwitches vary based on the specified Zone and VPC.
vSwitch	<p>Select the destination vSwitch. If you select multiple zones for your RDS instance, you must select multiple destination vSwitches.</p> <div style="background-color: #e1f5fe; padding: 10px; border: 1px solid #cfe2f3;"> <p> Note</p> <ul style="list-style-type: none"> ◦ If you select the default VPC, the destination vSwitch can be either the default vSwitch or a custom vSwitch. ◦ If you do not select the default VPC, the destination vSwitch must be a custom vSwitch. </div>
Switching Time	<ul style="list-style-type: none"> ◦ Switch Immediately After Data Migration: Data is migrated and workloads are switched over immediately. ◦ Switch Within Maintenance Window: Data is migrated immediately, and workloads are switched over during the specified maintenance window.

Upgrade To : 2016 SE ▼

Edition : High-availability [Learn more](#) ⓘ

Storage Type : Enhanced SSD
(Recommended) ESSD PL2
(Recommended) ESSD PL3
(Recommended) [Learn more](#)

Zone : Hangzhou Zone H ▼

CPU and Memory : 2核4GB (通用型) ▼
(Instance Type: mssql.s2.medium.s2) ⓘ
This instance type does not limit the number of connections and IOPS.

Network Type : Classic Network VPC [Learn more](#) ⓘ

Private(172.16.0.0/16)(Default) ▼

To create a VPC or VSwitch, go to the [VPC console](#). If you cannot find the latest VPC in the drop-down list, click [here](#) to refresh the list.

VSwitch : vsw-bp10aqj6o4lclxdrm6nb5(172.16.192.0/20) ▼

Location:ZoneH, Available Private IPs: 4016

Switching Time : **Switch Immediately After Data Migration**
 Switch Within Maintenance Window (Current Setting: 02:00-06:00 [\[Modify\]](#))
 Switch at Specified Time

After the version upgrade is complete, there is switchover downtime. The switchover downtime depends on the instance size and usually takes less than 20 minutes. We recommend that you perform the switchover during the maintenance period. Make sure that your applications can automatically reconnect to the database when the connection becomes available again.

4. Select Product Terms of Service and click **Confirm**.

Change the endpoints of your RDS instance

After the upgrade, your RDS instance resides in a VPC. The following table describes how to change the endpoints of your RDS instance after the upgrade based on the original network type of your RDS instance.

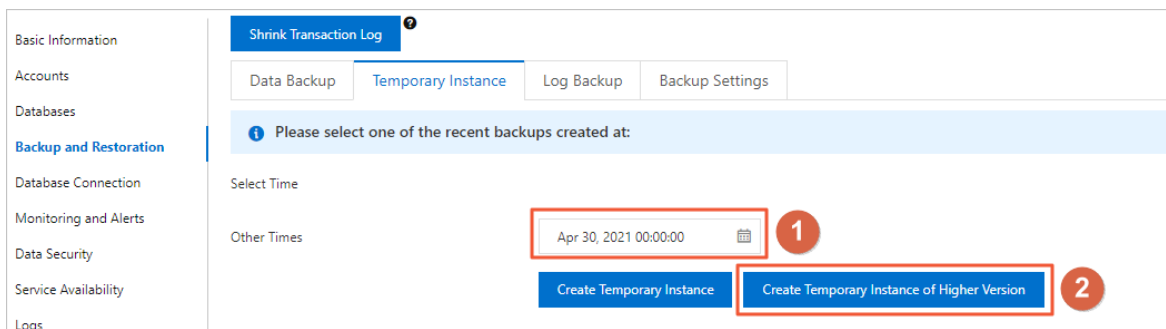
Original network type	Change rule
Classic network	After the upgrade, your RDS instance is connected over both the classic network and a VPC: <ul style="list-style-type: none"> • The original classic network endpoint remains available and never expires. • A VPC endpoint is generated for your RDS instance based on the specified VPC.
VPC	A VPC endpoint is generated for your RDS instance based on the specified VPC. This endpoint replaces the original VPC endpoint of your RDS instance.
Classic network and VPC	After the upgrade, your RDS instance is connected over both the classic network and a VPC. The original classic network and VPC endpoints remain available. The expiration time of the classic network endpoint remains unchanged.

Create a temporary RDS instance that runs the destination SQL Server version

Before you start the upgrade, we recommend that you create a temporary RDS instance that runs the destination SQL Server version. Also, configure other settings for this new RDS instance the same as those of your existing RDS instance. Then, you can test the compatibility between the two instances.

Note You can create the temporary RDS instance only for an RDS instance that runs SQL Server 2008 R2 with TDE and SSL disabled.

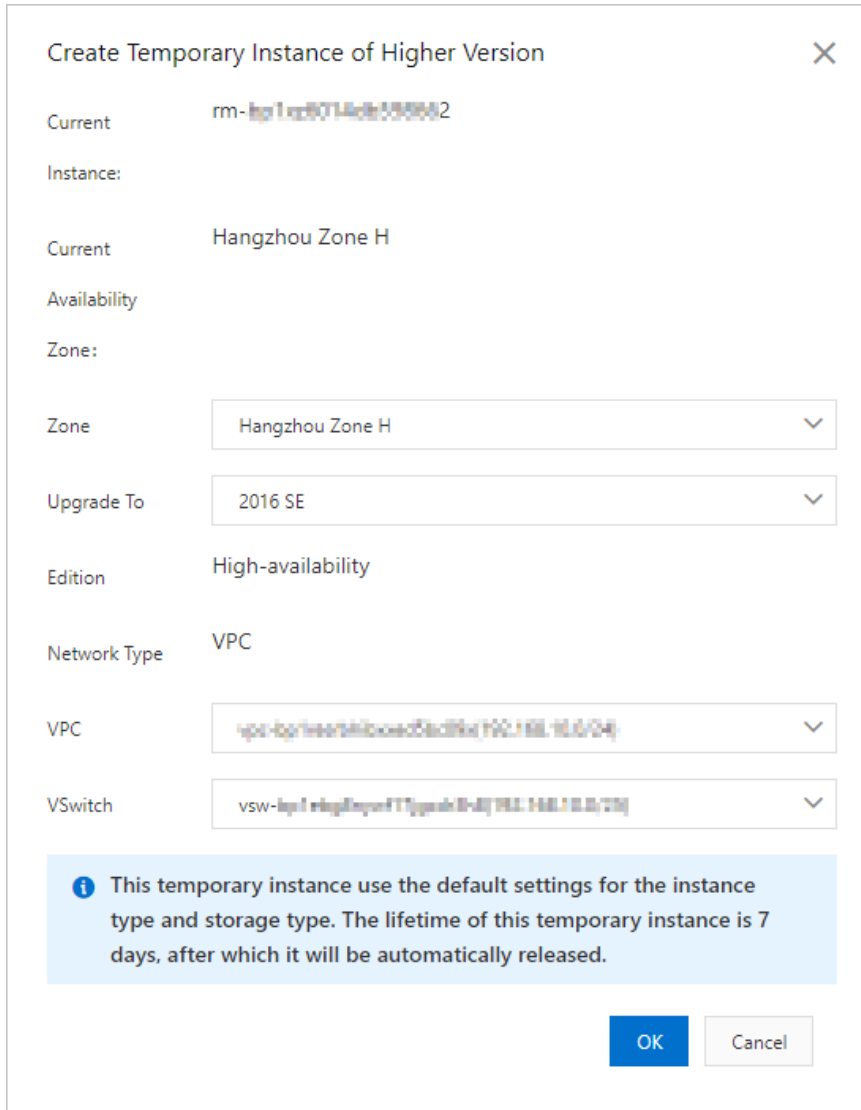
- 1.
2. In the left-side navigation pane, click **Backup and Restoration**.
3. On the **Temporary Instance** tab, specify the point in time at which you want to clone data and click **Create Temporary Instance of Higher Version**.



4. Configure the following parameters.

Parameter	Description
Zone	Select the zone in which you want to create the temporary RDS instance.
Upgrade To	Select the SQL Server version that the temporary RDS instance runs. Valid values: <ul style="list-style-type: none"> SQL Server 2016 SE SQL Server 2016 EE SQL Server 2012 EE
VPC	Select the VPC to which the temporary RDS instance belongs. You must select the VPC of the ECS instance to which you want to connect. Otherwise, the temporary RDS instance cannot communicate with the ECS instance over the internal network.
VSwitch	Select a vSwitch from the specified VPC.

Note ApsaraDB RDS provides a default instance type and storage type for the temporary RDS instance. The temporary RDS instance is available for seven days. After the seven-day validity period elapses, ApsaraDB RDS releases the temporary RDS instance.



5. Click OK.

10.4. Update the minor engine version of an ApsaraDB RDS for SQL Server instance

This topic describes how to update the minor engine version of an ApsaraDB RDS for SQL Server instance. These updates are used to enhance database performance, introduce new features, or fix known bugs.

For more information about the minor engine versions of ApsaraDB RDS for SQL Server, see [Release notes](#).

For more information about how to update the minor engine version of an RDS instance that runs a different database engine, see the following topics:


- [Update the minor engine version of an ApsaraDB RDS for MySQL instance](#)
- [Update the minor engine version of an ApsaraDB RDS for PostgreSQL instance](#)

Prerequisites

- Your RDS instance runs SQL Server 2017 EE or SQL Server 2019 EE.
- The database engine version of your RDS instance is SQL Server 2012, SQL Server 2016, SQL Server 2017, or SQL Server 2019.
- Your RDS instance runs RDS High-availability Edition. For more information, see [Overview](#).
- Your RDS instance belongs to the general-purpose instance family or the dedicated instance family. For more information, see [ApsaraDB RDS instance families](#).

Precautions

- An update requires 20 minutes to 30 minutes based on the data volume of your RDS instance. We recommend that you perform an update during off-peak hours. In addition, make sure that your application is configured to automatically reconnect to your RDS instance.
- After you update the minor engine version of your RDS instance, you cannot roll the minor engine version of the instance back to the previous version.

 **Warning** Before you perform an update, we recommend that you create an RDS instance that runs the destination minor engine version. Then, migrate the data of your RDS instance to the new RDS instance to test overall compatibility. For more information, see [Restore data to a new RDS instance](#).

- After you update the minor engine version of your RDS instance, the value of **Backup Size** on the **Basic Information** page of the ApsaraDB RDS console may be displayed as 0. After the next scheduled backup is complete, this error is automatically fixed.


View the minor engine version of your RDS instance

You can use one of the following methods to view the minor engine version of your RDS instance:

- Log on to the [ApsaraDB RDS console](#) and go to the **Basic Information** page of the RDS instance.
- Connect to your RDS instance and execute the `SELECT @@VERSION` statement to view the minor engine version of your RDS instance. For more information, see [Connect to an ApsaraDB RDS for SQL Server instance](#).

Update the minor version of your RDS instance

- 1.
2. In the **Configuration Information** section of the page that appears, click **Upgrade Minor Engine Version**.

 **Note** If you cannot find where to click **Upgrade Minor Engine Version**, the minor engine version of your RDS instance is the latest version or your RDS instance does not meet the requirements that are described in [Prerequisites](#).

3. In the dialog box that appears, configure the **Available Upgrade** and parameters and click **OK**.

Upgrade kernel minor version ✕

Current Version 15.0.4033.1

Available Upgrade ?

Upgrade Time

Migrate Immediately

Switch Within Maintenance Window 02:00-06:00 [Change](#)

Start From

! RDS minor version upgrade requires underlying data migration, please wait patiently. The switch will be performed after the migration is completed, and there will be an interruption of about 20-30 minutes during the switch. Please ensure that the application has a reconnection mechanism.

11.Instance

11.1. Create an ApsaraDB RDS for SQL Server instance

This topic describes how to create an ApsaraDB RDS for SQL Server instance in the ApsaraDB RDS console. You can also call an API operation to create an ApsaraDB RDS for SQL Server instance.

Billing


For more information, see [Pricing, billable items, and billing methods](#).



Prerequisites


You have an Alibaba Cloud account. For more information, see [Sign up with Alibaba Cloud](#).



Procedure

1. Log on to the [ApsaraDB RDS console](#).
2. Configure the following parameters.

Parameter	Description
Billing Method	<ul style="list-style-type: none">◦ Subscription: A subscription instance is an instance that you can subscribe to for a specified period and pay for up front. For long-term use, the subscription billing method is more cost-effective than the pay-as-you-go billing method. You can receive larger discounts for longer subscription periods.◦ Pay-As-You-Go: A pay-as-you-go instance is charged per hour based on your actual resource usage. The pay-as-you-go billing method is suitable for short-term use. If you no longer need your pay-as-you-go instance, you can release it to reduce costs. <div style="background-color: #e6f2ff; padding: 5px;"><p> Note A maximum of 30 pay-as-you-go RDS instances are allowed per Alibaba Cloud account. To increase this quota, you must submit a ticket.</p></div>
Region	<p>The region to which the RDS instance belongs.</p> <ul style="list-style-type: none">◦ After you confirm the purchase order, you cannot change the selected region.◦ We recommend that you select a region that is in close proximity to the geographic location where your users reside. This allows you to increase the access speeds of your users.◦ The RDS instance must reside in the same region as the ECS instance that you want to connect. If the RDS and ECS instances reside in different regions, these instances cannot communicate over an internal network. In this case, these instances must communicate over the Internet and therefore cannot deliver optimal performance.

Parameter	Description
Database Engine	<p>The database engine and version that the RDS instance runs. Select Microsoft SQL Server. The supported SQL Server versions are 2008 R2, 2012, 2016, 2017, and 2019.</p> <p> Note The available database engines and versions vary based on the region that you select.</p>
Edition	<ul style="list-style-type: none"> ◦ Basic: The database system consists of only a primary RDS instance. Computing is separated from storage to increase cost-effectiveness. ◦ High-availability: The database system consists of a primary RDS instance and a secondary RDS instance. These instances work in the high-availability architecture. ◦ Cluster: The database system consists of a primary RDS instance, a secondary RDS instance, and up to seven read-only RDS instances. The read capability of the database system improves with the number of read-only RDS instances. <p> Note The available RDS editions vary based on the region and database engine version that you select. For more information, see Overview of ApsaraDB RDS editions.</p>

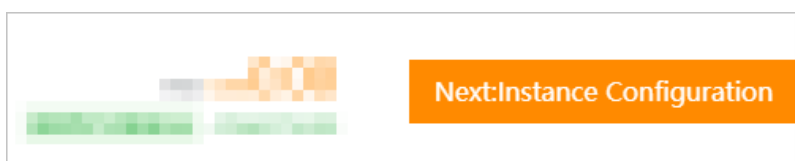
Parameter	Description
Storage Type	<ul style="list-style-type: none"> ◦ Local SSD: A local SSD resides on the same server as the database engine. You can store data on local SSDs to reduce I/O latency. ◦ Enhanced SSD: An enhanced SSD is an ultra-high performance disk that is developed by Alibaba Cloud based on the next-generation distributed block storage architecture. It integrates 25 Gigabit Ethernet and remote direct memory access (RDMA) technologies. This type of storage media reduces one-way latency and delivers up to 1 million random input/output operations per second (IOPS). Three enhanced SSD options are provided in the ApsaraDB RDS console. Each option represents a specific performance level (PL). <ul style="list-style-type: none"> ▪ ESSD PL1: This option represents an enhanced SSD of PL1. ▪ ESSD PL2: An enhanced SSD of PL2 delivers IOPS and throughput that are twice higher than those delivered by an enhanced SSD of PL1. ▪ ESSD PL3: An enhanced SSD of PL3 delivers IOPS that is 20 times higher than the IOPS delivered by an enhanced SSD of PL1. It also delivers throughput that is 11 times higher than the throughput delivered by an enhanced SSD of PL1. Enhanced SSDs of PL3 are suitable for workloads that require high I/O performance to process concurrent requests. Enhanced SSDs of PL3 are also suitable for workloads that require stable read/write latency. ◦ Standard SSD: A standard SSD is an elastic block storage device that is designed based on the distributed storage architecture. You can store data on standard SSDs to separate computing from storage. <p>For more information, see Storage types.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #d9e1f2;"> <p> Note If you select the standard SSD or enhanced SSD storage type, you can enable Disk Encryption. This allows you to maximize protection for your data. For more information, see Configure disk encryption for an ApsaraDB RDS for SQL Server instance.</p> </div>

Parameter	Description
<p>Zone of Primary Node and Zone of Secondary Node</p>	<p>A zone is an independent physical location within a region. The Zone of Primary Node parameter specifies the zone to which the primary RDS instance belongs. The Zone of Secondary Node parameter specifies the zone to which the secondary RDS instance belongs.</p> <p>You can select the Single-zone Deployment or Multi-zone Development method.</p> <ul style="list-style-type: none"> ◦ Single-zone Deployment: If you select this deployment method, the Zone of Primary Node and the Zone of Secondary Node are the same. ◦ Multi-zone Development: This is the recommended deployment method. If you select this deployment method, the Zone of Primary Node and the Zone of Secondary Node are different. This allows you to provide zone-level disaster recovery. You must manually specify the Zone of Primary Node and the Zone of Secondary Node. <div style="background-color: #e1f5fe; padding: 10px; margin-top: 10px;"> <p> Note</p> <ul style="list-style-type: none"> ◦ After the RDS instance is created, you can view information about the RDS instance and its secondary RDS instance on the Service Availability page. ◦ If you select the RDS Basic Edition, the database system consists of only one primary RDS instance and supports only the single-zone deployment method. </div>
<p>Instance Type</p>	<ul style="list-style-type: none"> ◦ General-purpose (Entry-level): specifies the general-purpose instance family. A general-purpose instance exclusively occupies the allocated memory and I/O resources. However, it shares CPU and storage resources with the other general-purpose instances that are deployed on the same server. ◦ Dedicated (Enterprise-level): specifies the dedicated instance family or the dedicated host instance family. A dedicated instance exclusively occupies the allocated CPU, memory, storage, and I/O resources. The dedicated host instance family is the highest configuration of the dedicated instance family. A dedicated host instance exclusively occupies all the CPU, memory, storage, and I/O resources of the server on which the instance is deployed. ◦ Dedicated: A dedicated cluster exclusively occupies all the resources on a VM or physical host. The permissions to manage hosts in a dedicated cluster can be authorized to you. This allows you to create multiple database instances on a host. For more information, see Add hosts. <div style="background-color: #e1f5fe; padding: 10px; margin-top: 10px;"> <p> Note Each instance type supports a specific number of CPU cores, memory capacity, maximum number of connections, and maximum IOPS. For more information, see Primary instance types.</p> </div>

Parameter	Description
Capacity	<p>The storage capacity that is provided for the RDS instance to store data files, system files, binary log files, and transaction files. You can adjust the storage capacity in increments of 5 GB.</p> <p>Note Dedicated instances are allocated exclusive resources. Therefore, the storage capacity of a dedicated instance that is equipped with local SSDs varies based on the instance type. For more information, see Primary ApsaraDB RDS instance types.</p>

3. Click **Next: Instance Configuration**.

4. In the lower-right corner of the page, click **Next: Instance Configuration**.



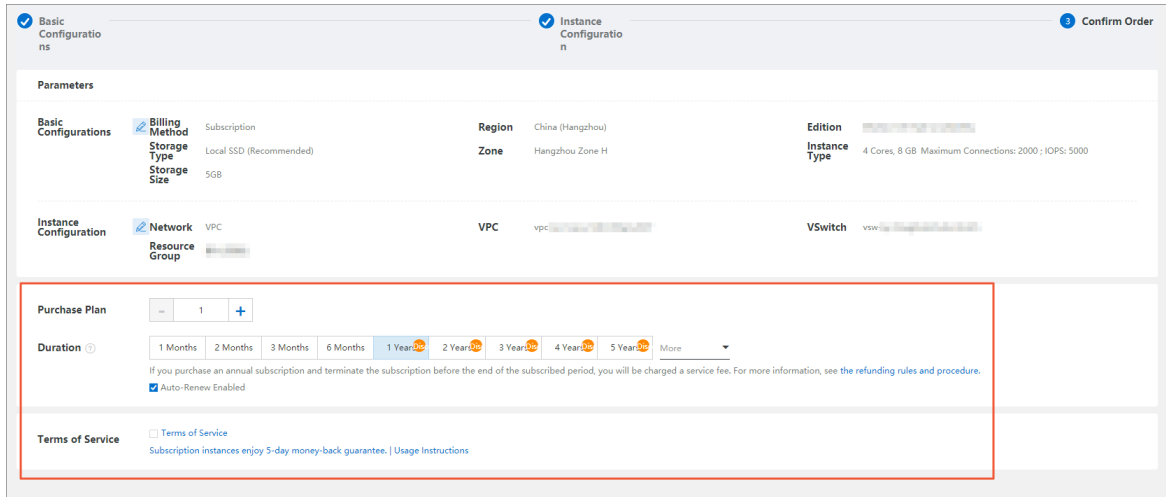
5. Configure the following parameters.

Parameter	Description
Network Type	<p>Set the network type.</p> <ul style="list-style-type: none"> ◦ Classic Network: the traditional type of network. ◦ VPC: the recommended type of network. A virtual private cloud (VPC) is an isolated virtual network that provides higher security and higher performance than the classic network. <p>After you select the VPC network type, you must specify the VPC and VSwitch of Primary Node parameters. If you set the Deployment Method parameter in the previous step to Multi-zone deployment, you must also specify the VSwitch of Secondary Node parameter.</p> <p>Note The RDS instance must have the same network type as the ECS instance that you want to connect. If the RDS and ECS instances both have the VPC network type, these instances must also reside in the same VPC. Otherwise, these instances cannot communicate over an internal network.</p>

6. Click **Next: Confirm Order**.

7. Confirm the settings in the **Parameters** section, specify the **Purchase Plan** parameter and the **Duration** parameter, read and select Terms of Service, and then click **Pay Now** to complete the payment. You must specify the Duration parameter only when the RDS instance uses the subscription billing method.

Note When you create a subscription RDS instance, we recommend that you select Auto-Renew Enabled. This relieves the need to manually renew the RDS instance on a regular basis. This also allows you to avoid interruptions to your workloads due to overdue payments.



On the ApsaraDB RDS homepage, click **Instances** in the left-side navigation pane, select the region where the RDS instance resides in the top navigation bar, and then find the RDS instance based on the **Creation Time**.

What to do next

After the RDS instance is created, you must specify whitelist settings and create accounts on the RDS instance. If you want to connect to the RDS instance over the Internet, you must also apply for a public endpoint. After you connect to the RDS instance, you can migrate data to the RDS instance. For more information, see the following topics:

- [Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance](#)
- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2008 R2](#)
- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2012, 2014, 2016, 2017 SE, or 2019 SE](#)
- [Create accounts and databases for an ApsaraDB RDS instance that runs SQL Server 2017 EE or 2019 EE](#)
- [Apply for or release a public endpoint on an ApsaraDB RDS for SQL Server instance](#)
- [Connect to an ApsaraDB RDS for SQL Server instance](#)

FAQ

- After I submit the order for purchasing an RDS instance, why does the ApsaraDB RDS console not respond and why am I unable to find the created RDS instance?

The issue may occur due to the following reasons:

- The RDS instance does not reside in the region that you selected.
In the top navigation bar, select the region where the RDS instance resides. Then, you can find the RDS instance.
- The zone that you selected cannot provide sufficient resources.
Resources in zones are dynamically allocated. After you submit the purchase order, the zone that you selected may be unable to provide sufficient resources. As a result, the RDS instance cannot be created. We recommend that you select a different zone and try again. If the RDS instance still cannot be created, you can go to the [Orders page](#) in the Billing Management console to view the refunded fee.

- How do I authorize a RAM user to manage my RDS instance?

For more information, see [Use RAM to manage ApsaraDB RDS permissions](#).

Related operations

Operation	Description
Create an instance	Creates an ApsaraDB RDS instance.

11.2. Change the specifications of an ApsaraDB RDS for SQL Server instance

This topic describes how to change the specifications of an ApsaraDB RDS for SQL Server instance. The specifications include the RDS edition, instance type, storage capacity, storage type, and zone.

Prerequisites


Your Alibaba Cloud account does not have overdue renewal orders.


Note You cannot directly upgrade an RDS instance from a shared instance type to a general-purpose or dedicated instance type. This feature is in development. You can create an RDS instance that uses a specific general-purpose or dedicated instance type. Then, you can use Alibaba Cloud Data Transmission Service (DTS) to migrate data to the new RDS instance. For more information, see [Data migration solutions](#).

Change items

You can create read-only RDS instances to increase the read capability of your database system. The read-only RDS instances can offload queries from the primary RDS instance. For more information, see [Overview of read-only ApsaraDB RDS for SQL Server instances](#) and [Create a read-only ApsaraDB RDS for SQL Server instance](#).

Change item	Description
Database engine version	The database engine versions of specific RDS instances can be upgraded to later versions. For more information, see the following topics: <ul style="list-style-type: none"> Upgrade an ApsaraDB RDS for SQL Server instance with local SSDs from SQL Server 2008 R2 to SQL Server 2012 or SQL Server 2016 Upgrade an instance from SQL Server 2012 to SQL Server 2016
RDS edition	You can upgrade the RDS edition of an RDS instance from Basic Edition to High-availability Edition. For information, see Upgrade an ApsaraDB RDS for SQL Server instance from Basic Edition to High-availability Edition .
Instance type	You can change the instance types of all RDS instances.
Storage type	<ul style="list-style-type: none"> You can upgrade the storage type of an RDS instance from standard SSD to enhanced SSD (ESSD). This upgrade is supported for RDS instances that do not run RDS Cluster Edition. You cannot downgrade the storage type of the RDS instance from ESSD to standard SSD. You can change the performance levels (PLs) of ESSDs for all RDS instances.

Change item	Description
Storage capacity	<p>You can increase the storage capacity of all RDS instances.</p> <div style="background-color: #e1f5fe; padding: 10px; border: 1px solid #cfcfcf;"> <p> Note</p> <ul style="list-style-type: none"> • You cannot decrease the storage capacity of an RDS instance. • The new storage capacity that you specify for an RDS instance must be within the storage capacity range that is supported by the instance type of the RDS instance. For more information, see Primary ApsaraDB RDS instance types. • The storage capacity of a read-only RDS instance cannot be less than the storage capacity of the primary RDS instance to which the read-only RDS instance is attached. If a read-only RDS instance is attached to a primary RDS instance and you want to increase the storage capacity for the instances, you must increase the storage capacity of the read-only RDS instance before you can increase the storage capacity of the primary RDS instance. • If the storage capacity range that is supported by an instance type does not meet your business requirements, we recommend that you select another instance type. • When you increase the storage capacity of an RDS instance that runs SQL Server on RDS High-availability Edition with standard SSDs or ESSDs, a 30-second transient connection may occur. During the transient connection, you cannot perform most of the operations that are related to databases, accounts, and network settings on the RDS instance. We recommend that you increase the storage capacity of your RDS instance during off-peak hours or make sure that your application is configured to automatically reconnect to your RDS instance. </div>

 **Note** The endpoints of an RDS instance remain unchanged after you change the preceding specifications of the RDS instance.

Billing


For more information, see [Specification change fees](#).

Precautions

- A specification change may trigger a data migration. After the migration is complete, ApsaraDB RDS switches over your workloads during the switching time that you specify. The switchover does not interrupt the synchronization of incremental data. During the switchover, a 30-second transient connection may occur, and you cannot perform most of the operations that are related to databases, accounts, and networks on the RDS instance. We recommend that you change the specifications during off-peak hours or make sure that your application is configured to automatically reconnect to your RDS instance.
- After you change the specifications of your RDS instance, you do not need to manually restart the instance.
- If your RDS instance runs RDS Basic Edition, no secondary RDS instance is provided as a hot standby. In this case, if your RDS instance unexpectedly exits, your database service may be unavailable for a long period of time. If you change the specifications or upgrade the database engine version of your RDS instance, your database service may also be unavailable for a long period of time. If you have high requirements for service availability, we recommend that you do not use RDS Basic Edition.

Procedure

- 1.
2. In the **Configuration Information** section of the Basic Information page, click **Change Specifications**.
3. In the dialog box that appears, select a specification change method and click **Next step**. This step is required only when the RDS instance uses the subscription billing method.

-  **Note** You can select one of the following specification change methods:
- **Upgrade or Downgrade**: After you submit a specification change order, the new specifications immediately take effect. Both specification change methods are supported for subscription RDS instances and pay-as-you-go RDS instances.
 - **Elastic Upgrade**: Elastic Upgrade allows you to upgrade the instance type and expand the storage capacity to improve the overall performance of the RDS instance. The instance type specifies the number of cores and the memory size. This method is not provided in the ApsaraDB RDS console. If you want to use this method, you must submit a **ticket**. When the date that is specified by the Restore Point-in-time parameter arrives, the instance type is automatically restored to the instance type that is used at the point in time before an elastic upgrade is performed. The storage capacity is not restored.

After you submit a specification change order, ApsaraDB RDS synchronizes the data of the RDS instance from the disk to a new RDS instance. Then, ApsaraDB RDS switches the information, such as the ID and endpoints, about the RDS instance over to the new RDS instance based on the specification change method that you select.

4. Change the specifications of the RDS instance. For more information, see [Change items](#).
5. Specify the Switching Time parameter. Valid values:
 - **Switch Immediately After Data Migration**: The specification change triggers a data migration to a new RDS instance. If you select this option, ApsaraDB RDS immediately applies the specification change and switches your workloads over to the new RDS instance after the migration is complete.
 - **Switch Within Maintenance Window**: When the specification change is being applied, a transient connection that lasts approximately 30 seconds may occur and you cannot perform most of the operations that are related to databases, accounts, and network settings. If you select this option, ApsaraDB RDS applies the specification change during the maintenance window that you specify. For more information, see [Set the maintenance window of an ApsaraDB RDS for SQL Server instance](#).
6. Read and select Terms of Service, click **Pay Now**, and then complete the payment.

Warning

- After you submit a specification change order, you cannot cancel the order. Therefore, before you submit a specification change order, we recommend that you evaluate whether the new specifications meet your business requirements.
- After you submit a specification change order, do not perform DDL operations before the specification change is applied.

FAQ

1. Can I change the zone and database engine version of my RDS instance?

You can change the zone and database engine version of your RDS instance only when the instance runs SQL Server 2008 R2 with local SSDs. You can change only the zone. You can also change the zone while you upgrade the database engine version. For more information, see [Migrate an ApsaraDB RDS for SQL Server instance across zones in the same region](#) and [Upgrade an ApsaraDB RDS for SQL Server instance with local SSDs from SQL Server 2008 R2 to SQL Server 2012 or 2016](#).

2. Do I need to migrate the data of my RDS instance to a new RDS instance when I increase the storage capacity of my RDS instance?

No, you do not need to manually migrate the data when you increase the storage capacity of your RDS instance. When you increase the storage capacity, ApsaraDB RDS checks whether the host on which your RDS instance resides can provide sufficient storage. If the host can provide sufficient storage, ApsaraDB RDS increases the storage capacity of your RDS instance without requiring you to migrate the data. If the host cannot provide sufficient storage, ApsaraDB RDS migrates the data to a new RDS instance before ApsaraDB RDS increases the storage capacity. The new RDS instance must be created on a host that provides sufficient storage.

Related operations


Operation	Description
ModifyDBInstanceSpec	Changes the specifications of an ApsaraDB RDS instance.

11.3. Restart an ApsaraDB RDS for SQL Server instance

This topic describes how to manually restart an ApsaraDB RDS for SQL Server instance. This applies if the number of connections exceeds the specified threshold or a performance issue occurs.

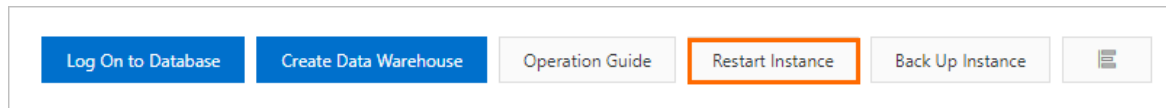
Impacts

A restart causes a network interruption that lasts about 30 seconds. Before you restart your RDS instance, we recommend that you make proper service arrangements. Proceed with caution.

 **Note** The Basic Edition does not provide a secondary RDS instance as a hot standby for the primary RDS instance. If the primary RDS instance unexpectedly exits, your database service may be unavailable for a long period of time. If you change the specifications or upgrade the database engine version of the primary RDS instance, your database service may also be unavailable for a long period of time. If you require high service availability, we recommend that you do not select the Basic Edition. For example, you can select the High-availability Edition. Some primary RDS instances support the upgrade from the Basic Edition to the High-availability Edition. For more information, see [Upgrade an RDS instance to the High-availability Edition](#).

Procedure

- 1.
2. In the upper-right corner of the Basic Information page, click **Restart Instance**.



3. In the message that appears, click OK.

Related operations

Operation	Description
Restart an ApsaraDB for RDS instance	Restarts an ApsaraDB RDS instance.

11.4. Switch workloads over between primary and secondary ApsaraDB RDS for SQL Server instances

ApsaraDB RDS for SQL Server provides the switchover feature to ensure high availability. If the primary RDS instance of your database system fails, ApsaraDB RDS automatically switches your workloads over from the primary RDS instance to the secondary RDS instance. After the primary/secondary switchover is complete, the secondary RDS instance becomes the new primary RDS instance. The endpoint that is used to connect to your database system remains unchanged. Your application can automatically connect to the new primary RDS instance by using the endpoint. This ensures high availability. You can also manually switch your workloads over between the primary RDS instance and the secondary RDS instance.

Prerequisites

The primary RDS instance runs RDS High-availability Edition or RDS Enterprise Edition.

Note If you use RDS Basic Edition, no secondary RDS instances are provided. Therefore, RDS Basic Edition does not support primary/secondary switchover feature.

Context

- **Automatic primary/secondary switchover:** By default, the automatic primary/secondary switchover feature is enabled. If the primary RDS instance fails, ApsaraDB RDS automatically switches your workloads over to the secondary RDS instance. For more information about the causes of primary/secondary switchovers, see [Reasons for primary/secondary switchovers](#).
- **Manual primary/secondary switchover:** You can manually switch your workloads over between the primary RDS instance and the secondary RDS instance even if the automatic primary/secondary switchover feature is enabled. You can perform manual primary/secondary switchovers for disaster recovery drills. You can also perform manual primary/secondary switchovers if you use the multi-zone deployment method and want to connect your application to the RDS instance in the zone that is closest to your application.

Note Data is synchronized between the primary RDS instance and the secondary RDS instance in real time. You can access only the primary RDS instance. The secondary RDS instance runs only as a standby.

Limits

By default, the primary/secondary switchover feature is disabled for RDS instances that run RDS Enterprise Edition. You need to submit a request to be added to a whitelist and then enable this feature free of charge.

Precautions


- Transient connections may occur during a primary/secondary switchover. Make sure that your application is configured to automatically reconnect to your database system.
- After a primary/secondary switchover, the read-only RDS instances that are attached to the primary RDS instance must re-establish the connections that are used to replicate data to and synchronize incremental data from the primary RDS instance. As a result, the data on the read-only RDS instances shows latencies of a few minutes.
- The primary/secondary synchronization mechanism of ApsaraDB RDS for SQL Server ensures full data synchronization between the primary RDS instance and secondary RDS instance of your database system. However, not all parameter settings of the ALTER LOGIN statement are synchronized. Only the settings of the SID, login_name, and password parameters in the ALTER LOGIN statement are synchronized. ApsaraDB RDS for SQL Server uses the default values for all the other parameters in the ALTER LOGIN statement. For more information, see [ALTER LOGIN \(Transact-SQL\)](#).
- You can view primary/secondary switchover logs only when the primary RDS instance runs SQL Server 2008 R2 with local SSDs.

Impacts

- Transient connections may occur during a primary/secondary switchover. Make sure that your application is configured to automatically reconnect to your database system.
- After a primary/secondary switchover, the read-only RDS instances that are attached to the primary RDS instance must re-establish the connections that are used to replicate data to and synchronize incremental data from the primary RDS instance. As a result, the data on the read-only RDS instances shows latencies of a few minutes.
- A primary/secondary switchover does not cause changes to the endpoints that are used to connect to your database system.

Perform a manual primary/secondary switchover

- 1.
2. In the left-side navigation pane, click **Service Availability**.
3. In the **Availability Information** section of the page that appears, click **Switch Primary/Secondary Instance**.
4. Specify the time at which you want to perform a primary/secondary switchover. Then, click **OK**.

 **Note** You cannot perform specific operations during a primary/secondary switchover. For example, you cannot manage databases and accounts or change the network type. We recommend that you select **Switch Within Maintenance Window**.

Disable automatic primary/secondary switchovers for a short period of time

By default, the automatic primary/secondary switchover feature is enabled. If the primary RDS instance fails, ApsaraDB RDS automatically switches your workloads over from the primary RDS instance to the secondary RDS instance. You can disable the automatic primary/secondary switchover feature in the following situations:

- A large-scale sales promotion during which you do not want a primary/secondary switchover to affect system availability
- An important application upgrade during which you do not want a primary/secondary switchover to cause unexpected issues
- A major event during which you do not want a primary/secondary switchover to affect system stability

1.

2. In the left-side navigation pane, click **Service Availability**.

3. In the **Availability Information** section of the page that appears, click **Configure Primary/Secondary Switchover**.

Note If you cannot find **Configure Primary/Secondary Switchover**, you must check whether the primary RDS instance meets all prerequisites.

4. Select **Disable Temporarily**, configure the **Deadline** parameter, and then click **OK**.

Note

- When the date and time specified by the **Deadline** parameter arrives, the automatic primary/secondary switchover feature is enabled.
- If you do not configure the **Deadline** parameter, the automatic primary/secondary switchover is disabled for one day. You can set the **Deadline** parameter to 23:59:59 seven days later at most.

After you disable the automatic primary/secondary switchover feature, you can go to the **Service Availability** page to check the deadline after which the automatic primary/secondary switchover feature can be automatically enabled.

View primary/secondary switchover logs

1.

2. In the left-side navigation pane, click **Service Availability**.

3. In the **Primary/Secondary Switching Logs** section of the page that appears, select a time range and view the primary/secondary switchover logs that are generated over the selected time range.

The screenshot shows the 'Availability Information' page with the following details:

- Series Architecture: High-availability Edition (Dual-node)
- Data Replication Mode: Semi-synchronous
- Primary Instance No.: 20 (ZoneH)
- Automatic Switchover: Enable (Default)
- Availability: 100.0%
- Availability Check Mode: Persistent Connection
- Secondary Instance No.: 20 (ZoneH)

The **Primary/Secondary Switching Logs** section is highlighted with a red box and contains the following table:

Switching Event ID	Start Time of Switching	End Time of Switching	Reason for Switching
f7	Mar 16, 2022, 11:29:22	Mar 16, 2022, 11:29:25	[Colorful bar chart]
8c	Mar 16, 2022, 11:27:22	Mar 16, 2022, 11:27:25	[Colorful bar chart]

At the bottom right of the logs section, there is a pagination control showing 'Items per Page' set to 30, and navigation buttons for 'Previous', '1', and 'Next'.

FAQ

- Can I access the secondary RDS instance of my database system?

No, you cannot access the secondary RDS instance of your database system. You can access only the primary RDS instance of your database system. The secondary RDS instance runs only as a standby.

- Do I need to manually switch my workloads over from the secondary RDS instance to the primary RDS instance after a primary/secondary switchover?

No, you do not need to manually switch your workloads over from the secondary RDS instance to the primary RDS instance after a primary/secondary switchover. The data in the primary RDS instance is the same as the data in the secondary RDS instance. After a primary/secondary switchover, the secondary RDS instance serves as the new primary RDS instance. No additional operations are required.

- Each time a primary/secondary switchover is performed, my RDS instance does not run as expected 10 minutes after the primary/secondary switchover is complete. What are the possible causes? How do I handle the issue?

If an exception on your RDS instance triggers a primary/secondary switchover to ensure high availability, your application may fail to identify and respond to the changes to the connections. If no timeout periods are specified for socket connections, your application waits for the database to return the results. In most cases, your application is disconnected after hundreds of seconds. During this period, some connections to the database cannot work as expected, and a large number of SQL statements fail to be executed. To avoid invalid connections, we recommend that you configure the `connectTimeout` and `socketTimeout` parameters to prevent your application from waiting for a long period of time due to network errors. This reduces the time required to recover from failures.

You must configure these parameters based on your workloads and usage modes. For online transactions, we recommend that you set `connectTimeout` to 1 to 2 seconds and `socketTimeout` to 60 to 90 seconds. This configuration is for reference only.

Related operations

Operation	Description
Switch services between a primary ApsaraDB for RDS instance and its secondary instance	Switches workloads over between primary and secondary ApsaraDB RDS instances.
Enable or disable automatic primary/secondary switchover	Enables or disables the automatic primary/secondary switchover feature for an ApsaraDB RDS instance.
Query settings of automatic primary/secondary switchover	Queries the settings of the automatic primary/secondary switchover feature for an ApsaraDB RDS instance.

11.5. Set the maintenance window of an ApsaraDB RDS for SQL Server instance


This topic describes how to set the maintenance window of an ApsaraDB RDS for SQL Server instance. The backend system performs maintenance on the RDS instance during the maintenance window. This ensures the stability of the RDS instance. The default maintenance window spans from 02:00:00 to 06:00:00 UTC+8. We recommend that you set the maintenance window to an off-peak hour. This allows you to avoid interruptions to your workloads.

Precautions

- Before the maintenance starts, ApsaraDB RDS sends emails to the contacts that are associated with your Alibaba Cloud account. We recommend that you check your email box on a regular basis to obtain up-to-date information.
- When the maintenance window arrives, your RDS instance enters the **Maintaining Instance** state. This ensures a smooth maintenance process. Database access and query operations such as performance monitoring are not affected while the instance is in this state. However, except for account and database management and IP address whitelist configuration, modification operations such as upgrade, downgrade, and restart are temporarily unavailable.
- During the maintenance window, one or two transient connections may occur. Make sure that your application is configured to automatically reconnect to your RDS instance.

Modify the maintenance window of a single RDS instance

- 1.
2. In the **Configuration Information** section, click **Configure** next to **Maintenance Window**.
3. Select an appropriate maintenance window and click **OK** to save the setting.

 **Note** The time zone of the maintenance window is the same as that of the computer that you use to log on to the ApsaraDB RDS console.

Related operations

Operation	Description
Modify the maintenance time	Modifies the maintenance window of an ApsaraDB RDS instance.


11.6. Migrate an ApsaraDB RDS for SQL Server instance across zones in the same region

This topic describes how to migrate an ApsaraDB RDS for SQL Server instance across zones in the same region. After the migration is complete, the attributes, configuration, and endpoints of the RDS instance remain unchanged. The time that is required to complete the migration is based on the amount of data to be migrated. The migration can take a few hours.

Prerequisites

- Your RDS instance runs SQL Server 2008 R2 with local SSDs.
- The region where your RDS instance resides consists of multiple zones. For more information about regions and zones, see [Regions and zones](#).
-
-

•  Note


-
- 

- [Fix database shard connections](#)
- [What is DTS?](#)

Procedure

- 1.
2. In the upper-right corner of the Basic Information section, click **Migrate Across Zones**.
3. In the dialog box that appears, specify the destination zone, vSwitch, and switching time. Then, click **OK**.

After you click **OK**, ApsaraDB RDS starts to copy the data of your RDS instance to the destination zone. This does not interrupt the running of your RDS instance. After all the data is copied to the destination zone, your workloads are switched over to the destination zone at the specified switching time (**Switch Now** or **Switch Within Maintenance Window**).

 Note

- During the switchover, a transient connection error of about 30 seconds occurs. Make sure that your application is configured to automatically reconnect to your RDS instance. Otherwise, you must manually reconnect your application to your RDS instance.
- If the DNS records cached on the client are not immediately updated after the migration is complete, some of your workloads may be switched over to the destination zone 10 minutes later. This causes another transient connection error.

Operation	
Migrate an instance across zones	

11.7. Release or unsubscribe from an ApsaraDB RDS for SQL Server instance

This topic describes how to manually release a pay-as-you-go-billed ApsaraDB RDS for SQL Server instance or unsubscribe from a subscription-billed ApsaraDB RDS for SQL Server instance.

Precautions

- After you release or unsubscribe from an RDS instance, the RDS instance and its data are immediately deleted. Before you release or unsubscribe from an RDS instance, we recommend that you [back up the RDS instance](#) and [download the required backup file](#).


- If you want to release the last read-only RDS instance that is attached with a primary RDS instance, you must disable the read/write splitting function for the primary RDS instance. For more information, see [Disable the read-only routing endpoint of an ApsaraDB RDS for SQL Server instance](#).

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

FAQ

If I release a read-only RDS instance, will my workloads be interrupted?

Yes, if you release a read-only RDS instance, your workloads on the read-only instance will be interrupted. Before you release a read-only RDS instance, we recommend that you set the [read weight](#) of the read-only RDS instance to 0.

 **Note** The cached connections with the read-only RDS instance that you have released remains valid. You must close these connections and establish new connections.

11.8. 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 tracestatus(-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:

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

11.9. View the data replication mode of an ApsaraDB RDS for SQL Server instance

This topic describes how to view the data replication mode between a primary ApsaraDB RDS for SQL Server instance and its secondary ApsaraDB RDS for SQL Server instance.

Limits

- The RDS instance runs RDS High-availability Edition or Cluster Edition. For more information, see [High-availability Edition](#) and [Cluster Edition](#).
- You cannot change the data replication mode of the RDS instance.

Data replication modes

- Synchronous mode

After an update that is initialized by your application is complete on a primary RDS instance, the log is synchronized to the secondary RDS instance. After the secondary RDS instance receives the log, the update transaction is considered committed. Your database system does not need to wait for the log to be replayed.

If a secondary RDS instance is unavailable or the communication between a primary RDS instance and a secondary RDS instance is abnormal, the synchronous mode degrades to the asynchronous mode.

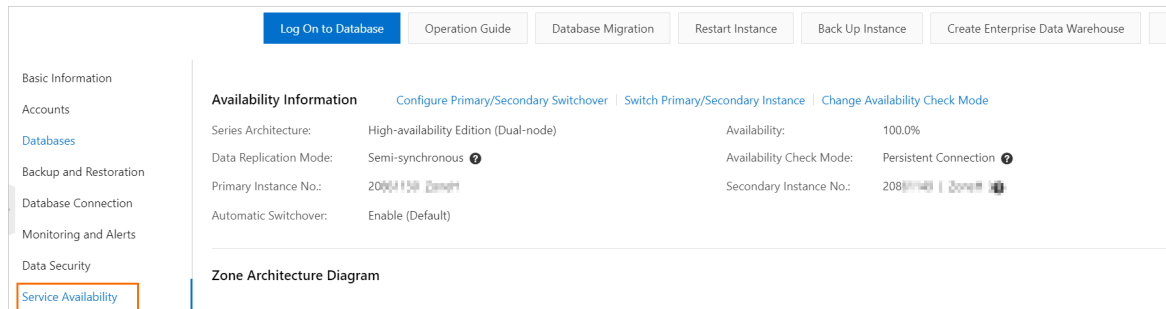
- Asynchronous mode

After an add, delete, or modify operation originated from an application is complete on a primary RDS instance, the primary RDS instance immediately responds to the application. At the same time, the primary RDS instance asynchronously replicates the added, deleted, or modified data to the secondary RDS instance of the primary RDS instance. In asynchronous mode, the workloads on the primary RDS instance run as expected even if the secondary RDS instance is unavailable. However, if the primary RDS instance is unavailable, errors may occur due to data inconsistencies between the primary RDS instance and the secondary RDS instance.

View the data replication mode

- 1.

- In the left-side navigation pane, click **Service Availability** to view the data replication mode of the RDS instance.



11.10. Reconfigure parameters for an RDS for SQL Server instance

11.10.1. Reconfigure the parameters of an ApsaraDB RDS for SQL Server instance by using the ApsaraDB RDS console

This topic describes how to view and reconfigure some parameters of an ApsaraDB RDS for SQL Server instance by using the ApsaraDB RDS console or API operations. You can also query the parameter reconfiguration history.

Prerequisites

Your RDS instance runs SQL Server 2008 R2 with local SSDs.

Precautions

- After you reconfigure some parameters, your RDS instance restarts when you click **Apply Changes**. For more information, check the **Force Restart** column on the **Editable Parameters** tab in the ApsaraDB RDS console. We recommend that you reconfigure these parameters during off-peak hours and make sure that your application is configured to automatically reconnect to your RDS instance.
- To ensure instance stability, the ApsaraDB RDS console allows you to reconfigure only some parameters. If you cannot find the parameter that you want to reconfigure, submit a .
- When you reconfigure parameters, you can view the valid values of these parameters in the **Value Range** column on the **Editable Parameters** tab in the ApsaraDB RDS console.
- If your RDS instance runs SQL Server 2012 or later, you can reconfigure parameters only by using SQL statements. For more information, see [Reconfigure the parameters of an ApsaraDB RDS for SQL Server instance by using SQL statements](#).

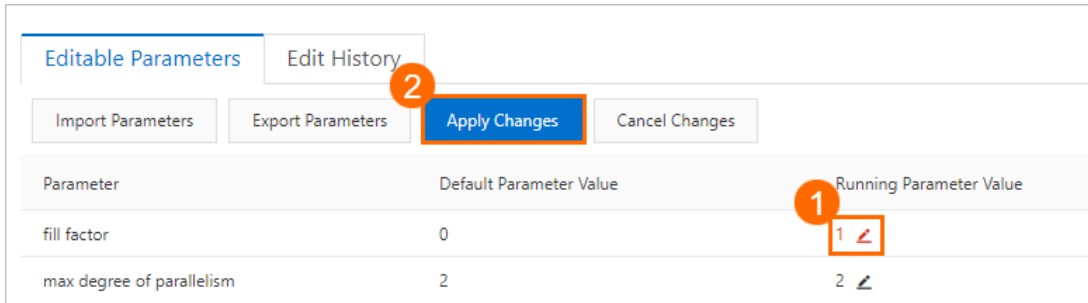
Reconfigure parameters

-
- In the left-side navigation pane, click **Parameters**.
- On the **Editable Parameters** tab, reconfigure one or more parameters.
 - To reconfigure a single parameter, perform the following steps:

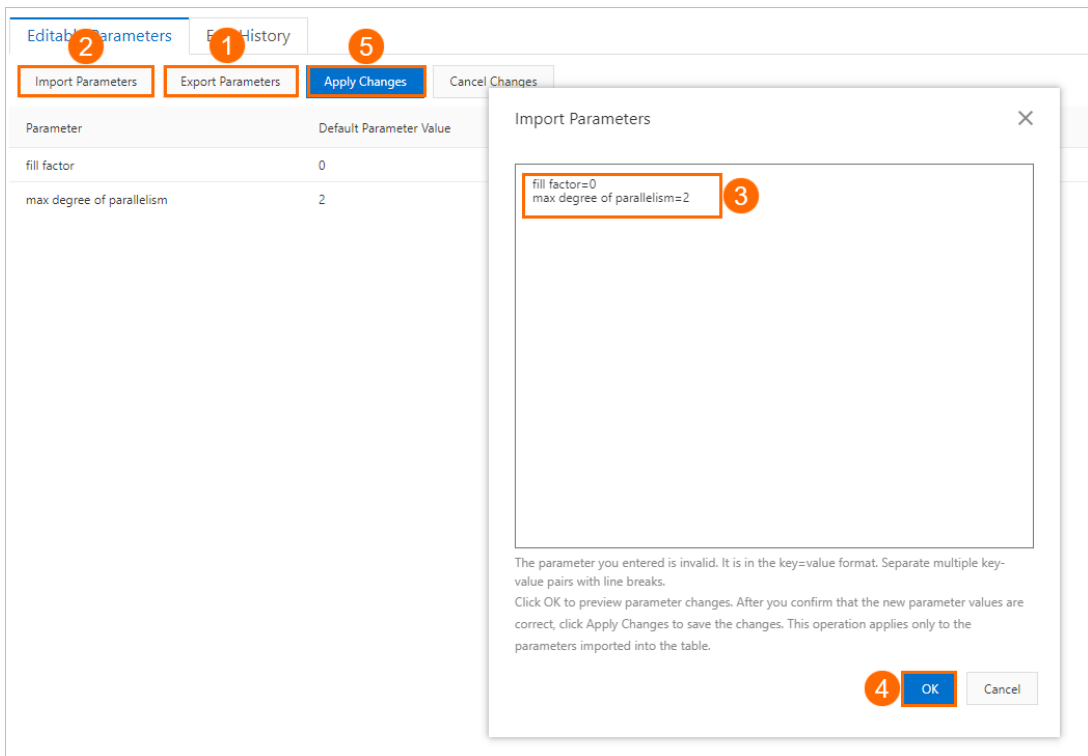
- a. Find the parameter and in the Running Parameter Value column click



- b. In the dialog box that appears, enter a new value within the value range and click OK.
- c. Click **Apply Changes**. In the message that appears, click **OK**.



- o To reconfigure more than one parameter at a time, perform the following steps:
 - a. Click **Export Parameters** to download the parameters and their values as a file to your computer.
 - b. Open the file and reconfigure parameters.
 - c. Click **Import Parameters**.
 - d. In the **Import Parameters** dialog box, paste the parameters and their new values copied from the file and click **OK**.
 - e. Verify the parameter values and click **Apply Changes**.



View the parameter reconfiguration history

- 1.

2. In the left-side navigation pane, click **Parameters**.
3. Click the **Edit History** tab.
4. Select a time range and click **OK**.

Parameters


For more information, see [Server Configuration Options \(SQL Server\)](#).

Related operations

Operation	Description
Modify parameters of an ApsaraDB for RDS instance	Reconfigures the parameters of an ApsaraDB RDS instance.
Query the parameter template of an ApsaraDB for RDS instance	Queries the parameter templates available to an ApsaraDB RDS instance.
Query parameter configurations	Queries the parameter settings of an ApsaraDB RDS instance.

11.10.2. Reconfigure the parameters of an ApsaraDB RDS for SQL Server instance by using SQL statements

You can reconfigure the parameters of an ApsaraDB RDS for SQL Server instance by using SQL statements or the ApsaraDB RDS console. This topic describes how to reconfigure the parameters by using SQL statements.

 **Note** The SQL statements described in this topic are supported only for RDS instances that run SQL Server 2012 or later. For information about how to reconfigure the parameters of an RDS instance that runs SQL Server 2008 R2, see [Reconfigure the parameters of an ApsaraDB RDS for SQL Server instance by using the ApsaraDB RDS console](#).

Supported parameters

- 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 the `sp_rds_configure` stored procedure to specify the parameters that you want to reconfigure. If the new settings of the specified parameters take effect only after your RDS instance restarts, ApsaraDB RDS displays a message.

Example:

```
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
WHERE NAME = 'max degree of parallelism'
```

11.11. Manage ApsaraDB RDS for SQL Server instances in the recycle bin

This topic describes how to manage ApsaraDB RDS for SQL Server instances that expired or have overdue payments in the recycle bin. You can unlock, re-create, or destroy the RDS instances in the recycle bin.


Description

If an RDS instance is manually released or expires, the RDS instance is moved to the recycle bin. If the payment for an RDS instance is refunded, the RDS instance is also moved to the recycle bin. An RDS instance is not moved to the recycle bin in the following situations:

- The payment for the RDS instance is refunded or the RDS instance is manually released within seven days after the instance is created.
- The RDS instance is a pay-as-you-go RDS instance and is automatically released due to overdue payments.
- The RDS instance is a read-only RDS instance.


Re-create an RDS instance

After a subscription RDS instance that runs SQL Server 2008 R2 is released due to expiration or overdue payments, ApsaraDB RDS continues to retain the data backup files of the instance for eight days. During the eight-day retention period, you can restore the data of the RDS instance to a new RDS instance by using the data backup files. After the eight-day retention period elapses, ApsaraDB RDS deletes the data backup files, and you can no longer restore the data of the RDS instance.

 **Note** You cannot re-create RDS instances that run SQL Server 2012 or SQL Server 2016.

Destroy an RDS instance

If an RDS instance is locked due to expiration or overdue payments, you can destroy the RDS instance in the recycle bin.

 **Warning** After you destroy an RDS instance, all data backup files of the instance are destroyed. Proceed with caution.

12. Database connection

12.1. Connect to an ApsaraDB RDS for SQL Server instance

This topic describes how to connect to an ApsaraDB RDS for SQL Server instance. After you complete the initial configuration for an RDS instance, you can connect to the RDS instance from your Elastic Compute Service (ECS) instance or your computer.

Prerequisites

- [Create an ApsaraDB RDS for SQL Server instance](#)
- [Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance](#)
- [Create an account for an RDS SQL Server instance](#)

Use DMS to connect to an RDS instance

Data Management (DMS) is a graphical data management service that provides various features for you to manage relational databases and NoSQL databases. These features include data management, schema management, user authorization, security audit, trend analysis, data tracking, business intelligence (BI) charting, and performance analysis and optimization.

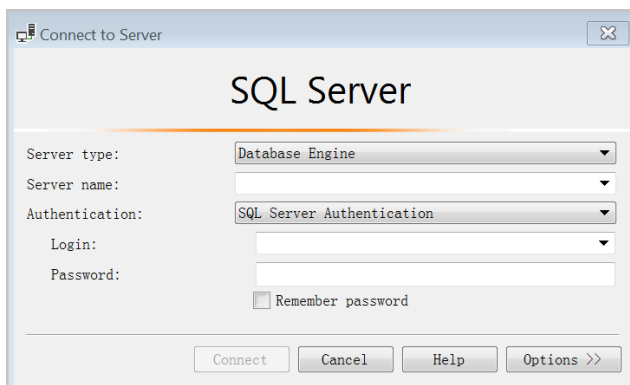
For more information, see [Use DMS to log on to an ApsaraDB RDS for SQL Server instance](#).

Use a database client to connect to an RDS instance

In this section, the Microsoft SQL Server Management Studio (SSMS) client is used as an example. For more information, visit the [Microsoft SQL Server Management Studio](#) page.

Note We recommend that you download the latest version of SSMS to support all SQL Server versions.

1. Start the SSMS client on your ECS instance or your computer.
2. Choose **Connect > Database Engine**.
3. In the **Connect to Server** dialog box, enter the information that is used to log on to the RDS instance.



Parameter	Description
Server type	Select Database Engine .
Server name	Enter the endpoint and port number that are used to connect to the RDS instance. The endpoint and the port number are separated by a comma (.). Example: <code>rm-bptest.sqlserver.rds.aliyuncs.com,3433</code> . For more information about how to view the internal and public endpoints and port numbers of an RDS instance, see View and change the internal and public endpoints and port numbers of an ApsaraDB RDS for SQL Server instance .
Authentication	Select SQL Server Authentication .
Login	Enter the username of the account that is authorized to log on to the RDS instance.
Password	Enter the password of the preceding account.

4. Click **Connect**.

FAQ

How do I use Function Compute to obtain data from my RDS instance?

You can install third-party dependencies on Function Compute. Then, you can obtain data from your RDS instance by using the built-in modules that are provided by the third-party dependencies in Function Compute. For more information, see [Install third-party dependencies on Function Compute](#).

12.2. Apply for or release a public endpoint on an ApsaraDB RDS for SQL Server instance

ApsaraDB RDS for SQL Server supports two types of endpoints: internal endpoints and public endpoints. By default, you are provided with an internal endpoint that is used to connect to your RDS instance. If you want to connect to your RDS instance over the Internet, you must apply for a public endpoint.

Internal and public endpoints

Endpoint type	Description
---------------	-------------

Endpoint type	Description
Internal endpoint	<ul style="list-style-type: none"> An internal endpoint is provided by default. You do not need to apply for this endpoint. In addition, you cannot release this endpoint. However, you can change the network type of your RDS instance. If an Elastic Compute Service (ECS) instance resides in the same region and has the same network type as your RDS instance, these instances can communicate over an internal network. If your application is deployed on such an ECS instance, you do not need to apply for a public endpoint. For more information, see Change the network type of an ApsaraDB RDS for SQL Server instance. For security and performance purposes, we recommend that you connect to your RDS instance by using the internal endpoint.
Public endpoint	<ul style="list-style-type: none"> You must manually apply for a public endpoint. You can release this endpoint if it is no longer required. If you cannot connect to your RDS instance by using the internal endpoint, you must apply for a public endpoint. This includes the following scenarios: <ul style="list-style-type: none"> Connect to your RDS instance from an ECS instance that resides in a different region or has a different network type from your RDS instance. For more information, see Change the network type of an ApsaraDB RDS for SQL Server instance. Connect to your RDS instance from a device outside Alibaba Cloud. <div style="background-color: #e6f2ff; padding: 10px; margin-top: 10px;"> <p>Note</p> <ul style="list-style-type: none"> You are not charged for the public endpoint or the traffic that is consumed. If you connect to your RDS instance by using the public endpoint, security is compromised. Proceed with caution. We recommend that you migrate your application to an ECS instance that resides in the same region and has the same network type as your RDS instance. This allows you to connect to your RDS instance by using the internal endpoint. The connection expedites transmission and improves security. </div>

Procedure

- 1.
2. In the left-side navigation pane, click **Database Connection**.
3. Apply for or release a public endpoint for your RDS instance:
 - o If you have not applied for a public endpoint, you can click **Apply for Public Endpoint**.
 - o If you have applied for a public endpoint, you can click **Release Public Endpoint**.
4. In the message that appears, click **OK**.

Related operations

Operation	Description
Apply for a public endpoint	Applies for a public endpoint for an ApsaraDB RDS instance.

Operation	Description
Release a public endpoint	Releases the public endpoint of an ApsaraDB RDS instance.

12.3. View and change the internal and public endpoints and port numbers of an ApsaraDB RDS for SQL Server instance

When you connect to an ApsaraDB RDS for SQL Server instance, you must enter its internal or public endpoint and port number. This topic describes how to view and change the internal and public endpoints and port numbers of an RDS instance in the ApsaraDB RDS console.

View the internal and public endpoints and port numbers of an RDS instance (in the new ApsaraDB RDS console)


- 1.
2. In the **Basic Information** section of the Basic Information page, click **See Detail** next to Network Type. In the pane that appears, view the internal and public endpoints and port numbers of your RDS instance.

Note

- The internal and public endpoints of your RDS instance appear only after you specify whitelist settings. For more information, see [Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance](#).
- The public endpoint of your RDS instance appears only after you apply for a public endpoint. For more information, see [Apply for or release a public endpoint on an ApsaraDB RDS for SQL Server instance](#).

Change the internal or public endpoint and port number of an RDS instance

- 1.
2. In the left-side navigation pane, click **Database Connection**.
3. Click **Change Endpoint**.
4. In the dialog box that appears, select a connection type, enter the prefix of the new endpoint, specify the port number, and then click **OK**.

 **Note**

- The prefix can contain lowercase letters, digits, and hyphens (-). The prefix must start with a lowercase letter and end with a lowercase letter or a digit.
- The prefix must contain at least 8 characters, and the total length of the endpoint cannot exceed 63 characters. The total length includes the prefix and suffix of the endpoint.
- The port number must be within the range of 1000 to 65534.

FAQ

- After I change an endpoint or a port number of my RDS instance, do I need to update the endpoint or port number information in my application?

Yes, after you change an endpoint or a port number of your RDS instance, you must update the endpoint or port number information on your application. If you do not update the information, your application cannot connect to your RDS instance.

- After I change an endpoint or a port number of my RDS instance, does the change immediately take effect? Do I need to restart my RDS instance?

After you change an endpoint or a port number of your RDS instance, the change immediately takes effect. You do not need to restart your RDS instance.

- After I change or release an endpoint of my RDS instance, can I use the endpoint for another RDS instance?

Yes, after you change or release an endpoint of your RDS instance, you can use the endpoint of your RDS instance for another RDS instance.

- Does a primary/secondary switchover trigger changes to the endpoints of my RDS instance?

No, a primary/secondary switchover does not trigger changes to the endpoints of your RDS instance. However, the IP addresses that are associated with the endpoints change. Your application can still connect to your RDS instance by using the endpoints.

12.4. Use DMS to log on to an ApsaraDB RDS for SQL Server instance

This topic describes how to log on to an ApsaraDB RDS for SQL Server instance by using Alibaba Cloud Data Management (DMS).

Context

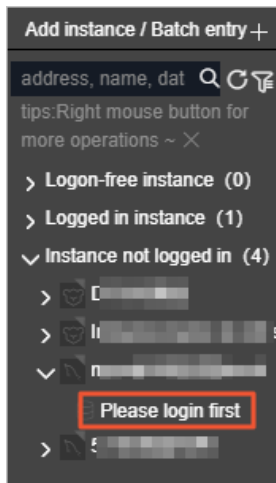
DMS offers an integrated solution for data, schema, and server management, user authorization, security audit, trend analysis, data tracking, business intelligence (BI) charts, and performance analysis and optimization.

Log on to your RDS instance by using the new DMS console

Prerequisites

1. Log on to the [DMS console](#).
2. In the left-side navigation pane, select your RDS instance and click **Please login first**.

Note If your RDS instance uses the **Security Collaboration** control mode, you need only to click **Logon-free Instances** and double-click the instance. You do not need to enter the username and password of the account that is used for the logon.



- In the dialog box that appears, enter the username and password of the account used for the logon and click **OK**.

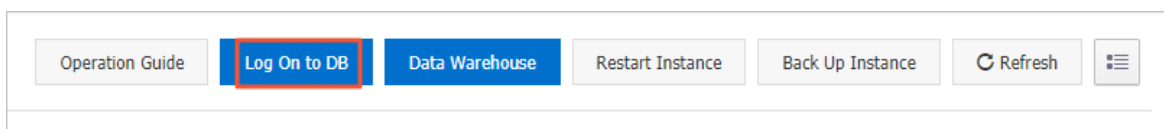
Note The account used for the logon must have permissions on the required database. Otherwise, the required database is not displayed in the left-side navigation pane. For more information about how to modify the permissions of an account, see [Modify the permissions of a standard account on an ApsaraDB RDS for SQL Server instance](#).

- In the left-side navigation pane, click **Instances Connected** and double-click your RDS instance to switch to the instance.

Log on to your RDS instance by using the original DMS console

Note If you have upgraded DMS to the new version, we recommend that you use the new DMS console to log on to your RDS instance.

-
- In the upper-right corner of the page, click **Log On to Database** to open the RDS Database Logon page.



Note Alibaba Cloud directs you to the original or new DMS console based on your logon history.

- Configure the following parameters.

Parameter	Description
Endpoint:Port number	The endpoint and port number that are used to log on to your RDS instance. The endpoint and port number are in the <code><Endpoint>:<Port number></code> format. Example: <code>rm-bpxxxxxxx.rds.aliyuncs.com:3433</code> . For more information about how to view the endpoint and port number that are used to log on to your RDS instance, see View and change the internal and public endpoints and port numbers of an ApsaraDB RDS for SQL Server instance .
Database Username	The username of the account that is used to log on to your RDS instance.
Password	The password of the preceding account.

4. Click **Log On**.

Note If you want the browser to save the password, select **Remember Password** before you click **Log On**.

- If you are prompted to add the Classless Inter-Domain Routing (CIDR) block that contains the IP address of the DMS server to an IP address whitelist of your RDS instance, click **Specify for All Instances** or **Specify for Current Instance**.
- After the CIDR block is added, click **Log On**.

12.5. Configure the hybrid access solution for an ApsaraDB RDS for SQL Server instance

This topic describes how to configure the hybrid access solution for an ApsaraDB RDS for SQL Server instance. This solution allows you to retain both the classic network endpoint and virtual private cloud (VPC) endpoint of your RDS instance. This way, you can migrate your RDS instance from the classic network to a VPC with no downtime.

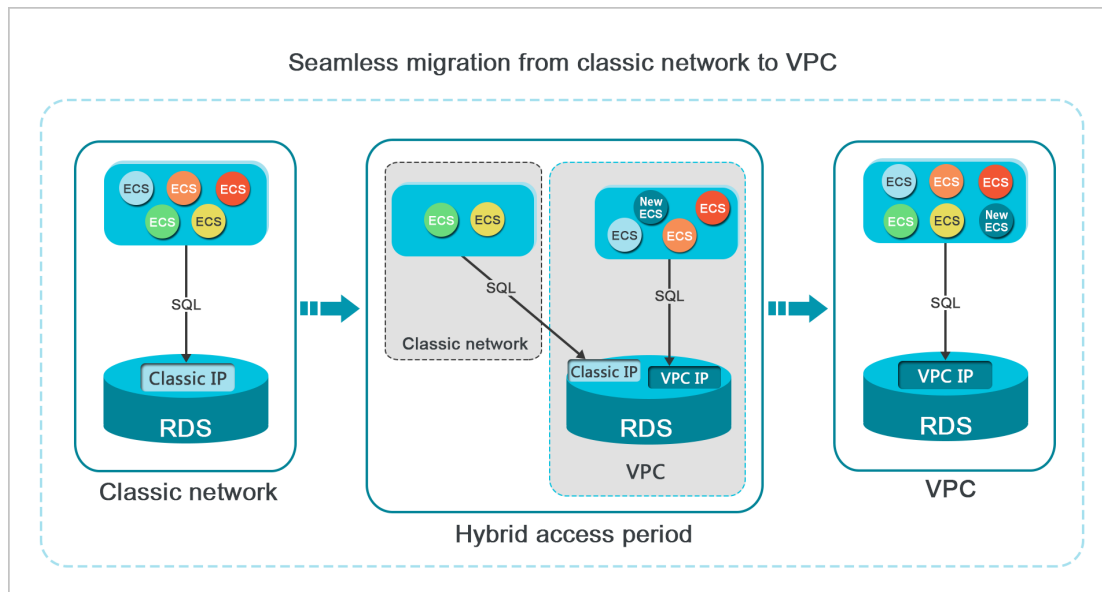
Background information

When you migrate your RDS instance from the classic network to a VPC, the internal classic network endpoint of the instance changes to the internal VPC endpoint. In this case, the endpoint itself remains unchanged. However, the IP address that is bound to the endpoint changes. This change causes a temporary loss of connection of up to 30 seconds, and no classic network-housed Elastic Compute Service (ECS) instances can connect to your RDS instance over an internal network. To migrate your RDS instance from the classic network to a VPC without no downtime, ApsaraDB RDS provides the hybrid access solution.

Hybrid access refers to the ability of your RDS instance to be connected by both classic network-housed ECS instances and VPC-housed ECS instances. During the hybrid access period, ApsaraDB RDS retains the internal classic network endpoint and generates an internal VPC endpoint. When you migrate your RDS instance from the classic network to a VPC, no temporary loss of connection occurs.

For security and performance purposes, we recommend that you use only the internal VPC endpoint. Therefore, ApsaraDB RDS allows the configured hybrid access solution to remain valid only for a specific period of time. When the hybrid access period elapses, ApsaraDB RDS releases the internal classic network endpoint. In this case, your applications cannot connect to your RDS instance by using the internal classic network endpoint. You must add the internal VPC endpoint to all of your applications during the hybrid access period. This ensures a smooth network migration and prevents interruptions to your workloads.

For example, a company uses the hybrid access solution to migrate their RDS instance from the classic network to a VPC. During the hybrid access period, some applications connect to the RDS instance by using the internal VPC endpoint, whereas the other applications connect to the RDS instance by using the internal classic network endpoint. When all applications of the company can connect to the RDS instance by using the internal VPC endpoint, the internal classic network endpoint can be released.



Limits

During the hybrid access period, your RDS instance does not support the following operations:

- Change the network type of your RDS instance to the classic network.
- Migrate your RDS instance to a different zone.

Prerequisites


- Your RDS instance resides in the classic network.
- The zone where your RDS instance resides provides available VPCs and vSwitches. For more information

about how to create VPCs and vSwitches, see [Work with VPCs](#).

- If your RDS instance runs SQL Server 2008 R2, you cannot change the network type from classic network to VPC.
- Temporary RDS instances support only the classic network type. If your RDS instance is a temporary RDS instance, you cannot change the network type from classic network to VPC. For more information about how to log on to a temporary RDS instance, see [Log on to a temporary ApsaraDB RDS for SQL Server instance](#).

Change the network type from classic network to VPC

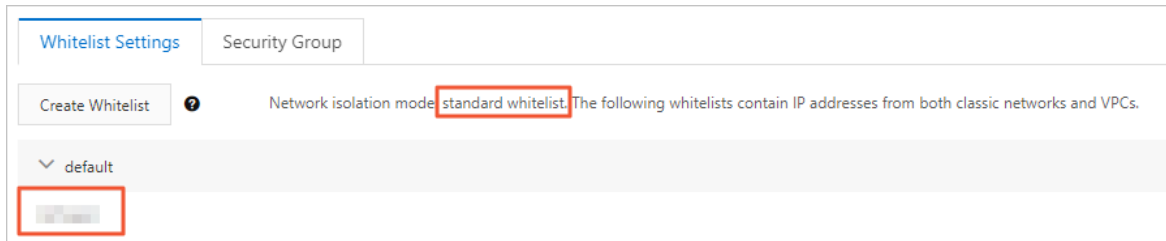
- 1.
2. In the left-side navigation pane, click **Database Connection**.
3. Click **Switch to VPC**.

 **Note** If the **Switch to VPC** button cannot be found, you must check that the RDS instance meets all prerequisites.

4. In the dialog box that appears, select a VPC and a vSwitch, and specify whether to retain the classic network endpoint.
 - Select a VPC. We recommend that you select the VPC where the required ECS instance resides. If the ECS instance and the RDS instance reside in different VPCs, these instances cannot communicate over an internal network unless you create a Cloud Enterprise Network (CEN) instance or an IPsec-VPN connection between the VPCs of these instances. For more information, see [Overview of Alibaba Cloud CEN](#) and [Establish IPsec-VPN connections between two VPCs](#).
 - Select a vSwitch. If no vSwitches are available in the selected VPC, create a vSwitch in the zone where the RDS instance resides. For more information, see [Work with vSwitches](#).
 - Clear or select the **Reserve original classic endpoint** option. For more information, see the following table.

Action	Description
Clear the Reserve original classic endpoint option	The classic network endpoint is not retained and changes to a VPC endpoint. When you change the network type from classic network to VPC, a temporary loss of connection of 30 seconds occurs. In this case, the connection between each classic network-hosted ECS instance and the RDS instance is closed.
Select the Reserve original classic network option	<p>The classic network endpoint is retained, and a new VPC endpoint is generated. In this case, the RDS instance runs in hybrid access mode. Both classic network-hosted ECS instances and VPC-hosted ECS instances can connect to the RDS instance over an internal network.</p> <p>When you change the network type from classic network to VPC, no temporary loss of connection occurs. The connection between each classic network-hosted ECS instance and the RDS instance remains available until the classic network endpoint expires.</p> <p>Before the classic network endpoint expires, you must add the VPC endpoint of the RDS instance to the required VPC-hosted ECS instance. This way, ApsaraDB RDS can migrate your workloads to the selected VPC with no downtime.</p>

5. Add the private IP address of the required ECS instance to an IP address whitelist of the VPC network type on the RDS instance. This way, the ECS instance can connect to the RDS instance over an internal network.



6.
 - o If you have selected the Reserve original classic endpoint option, you must add the generated VPC endpoint to each VPC-housed ECS instance before the classic network endpoint expires.
 - o If you have cleared the Reserve original classic endpoint option, the connection between each classic network-hosted ECS instance and the RDS instance over an internal network is immediately closed after the network type is changed from classic network to VPC. You must add the generated VPC endpoint to each VPC-housed ECS instance.

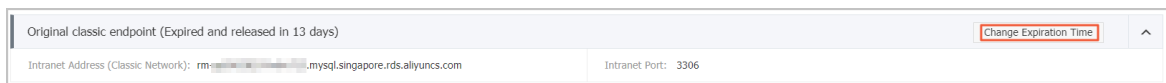
Note If the RDS instance resides in a VPC and you want to connect a classic network-hosted ECS instance to the RDS instance over an internal network, you can use ClassicLink to establish a connection. Alternatively, you can migrate the ECS instance to the VPC where the RDS instance resides. For more information, see [Overview of ClassicLink](#).

Change the expiration date of the internal classic network endpoint

During the hybrid access period, you can change the expiration date of the classic network endpoint at any time based on your business requirements. The expiration date is immediately recalculated starting from the day when you make the change. For example, the classic network endpoint is configured to expire on August 18, 2017, and you extend the validity period of the classic network endpoint by 14 days on August 15, 2017. In this case, ApsaraDB RDS releases the classic network endpoint on August 29, 2017.

To change the validity period of the classic network endpoint, perform the following steps:

- 1.
2. In the left-side navigation pane, click **Database Connection**.
3. On the **Instance Connection** tab, click **Change Expiration Time**.




4. In the **Change Expiration Time** dialog box, select an expiration date and click **OK**.

12.6. Switch an ApsaraDB RDS for SQL Server instance to a different vSwitch

This topic describes how to switch an ApsaraDB RDS for SQL Server instance to a different vSwitch based on your business requirements.

Prerequisites

Your RDS instance is equipped with standard SSDs or enhanced SSDs (ESSDs).

 **Note** For more information about how to switch an RDS instance that runs a different database engine to a different virtual private cloud (VPC) and a different vSwitch, see the following topics:

- [Switch an ApsaraDB RDS for MySQL instance to a different VPC and a different vSwitch](#)
- [Switch an ApsaraDB RDS for PostgreSQL instance to a different vSwitch](#)

Precautions


You cannot switch an ApsaraDB RDS for SQL Server instance to a different VPC.

Impacts

- When your RDS instance is being switched to a different vSwitch, you may encounter a network interruption that lasts approximately 30 seconds. Make sure that your application is configured to automatically reconnect to your RDS instance.
- After your RDS instance is switched to a different vSwitch, the virtual IP addresses (VIPs) of your RDS instance change. We recommend that you connect your application to your RDS instance by using an endpoint. For more information, see [View and change the internal and public endpoints and port numbers of an ApsaraDB RDS for SQL Server instance](#).
- VIP changes interrupt the connection between your RDS instance and [Data Management \(DMS\)](#) and the connection between your RDS instance and [Data Transmission Service \(DTS\)](#) for a short period of time. After the VIPs are changed and your RDS instance is switched to a different vSwitch, the connections are automatically resumed.
- After your RDS instance is switched to a different vSwitch, you can only read data from your RDS instance. You cannot write data to your RDS instance due to the data that is cached on your database client. In this case, we recommend that you immediately clear the cache on your database client.

Procedure

- 1.
2. In the left-side navigation pane, click **Database Connection**.
3. Click **Switch vSwitch**.
4. Select a destination vSwitch. Then, click **OK**.

-  **Note**
- You can switch the RDS instance only between the vSwitches that belong to the same zone.
 - If you want to create a VPC or a vSwitch, you can click [go to the VPC console](#).

5. In the message that appears, click **Switch**.

Related operations

Operation	Description
Change VPC or vSwitch	Switches an ApsaraDB RDS instance to a different VPC or a different vSwitch.

12.7. Change the network type of an ApsaraDB RDS for SQL Server instance

This topic describes how to change the network type of an ApsaraDB RDS for SQL Server instance from the classic network type to the virtual private cloud (VPC) network type.

Network types

- **Classic network:** RDS instances in the classic network are not isolated. To block unauthorized access to these instances, you must configure IP address whitelists or security groups.
- **VPC:** Each VPC is an isolated network. VPCs are more secure than the classic network. Therefore, we recommend that you select the VPC network type.

You can customize route tables, CIDR blocks, and gateways for a VPC. In addition, you can connect your data center to a VPC by using leased lines or VPNs. The data center and the VPC comprise a virtual data center. You can use the virtual data center to migrate your workloads to the cloud with no downtime.

Note

- You can select the classic or VPC network type and can switch your RDS instance between these network types free of charge.
- You can change the network type of an RDS instance only from classic network to VPC. You cannot change the network type of an RDS instance from VPC to classic network.

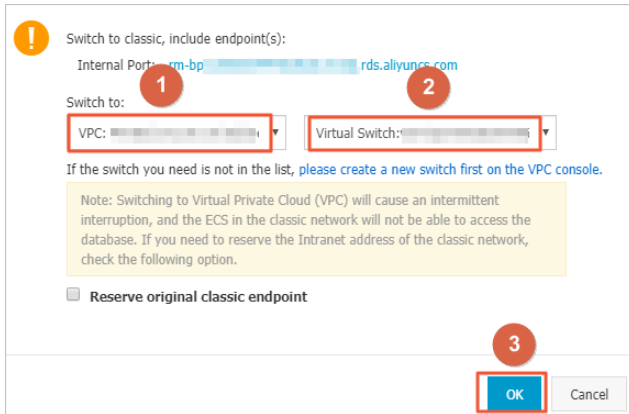
Procedure

Precautions

- If your RDS instance runs SQL Server 2008 R2, you cannot change the network type from classic network to VPC.
- Temporary RDS instances support only the classic network type. If your RDS instance is a temporary RDS instance, you cannot change the network type from classic network to VPC. For more information about how to log on to a temporary RDS instance, see [Log on to a temporary ApsaraDB RDS for SQL Server instance](#).

Procedure

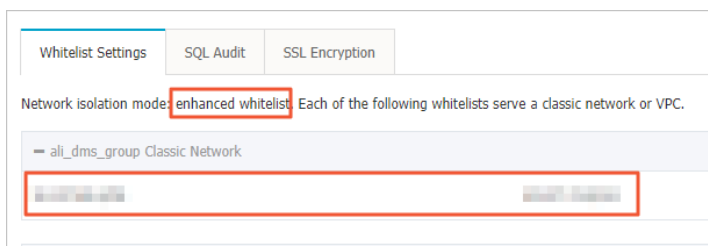
- 1.
2. In the left-side navigation pane, click **Database Connection**.
3. Click **Switch to VPC**.
4. In the dialog box that appears, select a VPC and a vSwitch, and specify whether to retain the classic network endpoint.
 - Select a VPC. We recommend that you select the VPC where the required ECS instance resides. If the ECS instance and the RDS instance reside in different VPCs, these instances cannot communicate over an internal network unless you create a Cloud Enterprise Network (CEN) instance or an IPsec-VPN connection between the VPCs of these instances. For more information, see [Overview of Alibaba Cloud CEN](#) and [Establish IPsec-VPN connections between two VPCs](#).
 - Select a vSwitch. If no vSwitches are available in the selected VPC, create a vSwitch in the zone where the RDS instance resides. For more information, see [Create a vSwitch](#).




- o Clear or select the **Reserve original classic endpoint** option. For more information, see the following table.

Action	Description
Clear the Reserve original classic endpoint option	The classic network endpoint is not retained and changes to a VPC endpoint. When you change the network type from classic network to VPC, a temporary loss of connection of about 30 seconds occurs. In this case, the connection between each classic network-hosted ECS instance and the RDS instance is closed.
Select the Reserve original classic endpoint option	The classic network endpoint is retained, and a new VPC endpoint is generated. In this case, the RDS instance runs in hybrid access mode. Both classic network-hosted ECS instances and VPC-hosted ECS instances can connect to the RDS instance over an internal network. For more information, see Configure the hybrid access solution for an ApsaraDB RDS for SQL Server instance . When you change the network type from classic network to VPC, no temporary loss of connection occurs. The connection between each classic network-hosted ECS instance and the RDS instance remains available until the classic network endpoint expires. Before the classic network endpoint expires, you must add the generated VPC endpoint to the required VPC-hosted ECS instance. This way, ApsaraDB RDS can migrate your workloads to the selected VPC with no downtime. Before the classic network endpoint expires, ApsaraDB RDS sends a text message to the phone number that is bound to your Alibaba Cloud account for seven consecutive days. For more information, see Configure the hybrid access solution for an ApsaraDB RDS for SQL Server instance .

5. Add the private IP address of the required VPC-hosted ECS instance to an IP address whitelist of the VPC network type on the RDS instance. This way, the ECS instance can access the RDS instance over an internal network. If no IP address whitelists of the VPC network type are available, create one.



6. Add the VPC endpoint of the RDS instance to the required ECS instance.
 - o If you have selected the Reserve original classic endpoint option, you must add the generated VPC endpoint to each VPC-housed ECS instance before the classic network endpoint expires.
 - o If you have cleared the Reserve original classic endpoint option, the connection between each classic network-hosted ECS instance and the RDS instance over an internal network is immediately closed after the network type is changed. You must add the generated VPC endpoint to each VPC-housed ECS instance.

 **Note** If you want to connect a classic network-housed ECS instance to the VPC-housed RDS instance over an internal network, you can use ClassicLink to establish a connection. Alternatively, you can migrate the ECS instance to the VPC where the RDS instance resides. For more information, see [Overview](#).

FAQ


How do I change the VPC of my RDS instance?

Purchase a new RDS instance that resides in the required VPC. Then, migrate the data of your RDS instance to the new RDS instance. For more information, see [Migrate data between RDS instances](#).

Related operations

Operation	Description
Change the network type of an ApsaraDB RDS instance	Changes the network type of an ApsaraDB RDS instance.

12.8. Close a connection to an ApsaraDB RDS for SQL Server instance

 **Note** This topic describes how to close a connection to an ApsaraDB RDS instance that runs SQL Server 2012 or later by using the KILL statement.

You can close only the connections initiated by you and cannot close other connections, such as backup connections.

You can execute the following statement to close a connection: `KILL (SPID)`

13. Read/write splitting

13.1. Overview of read/write splitting

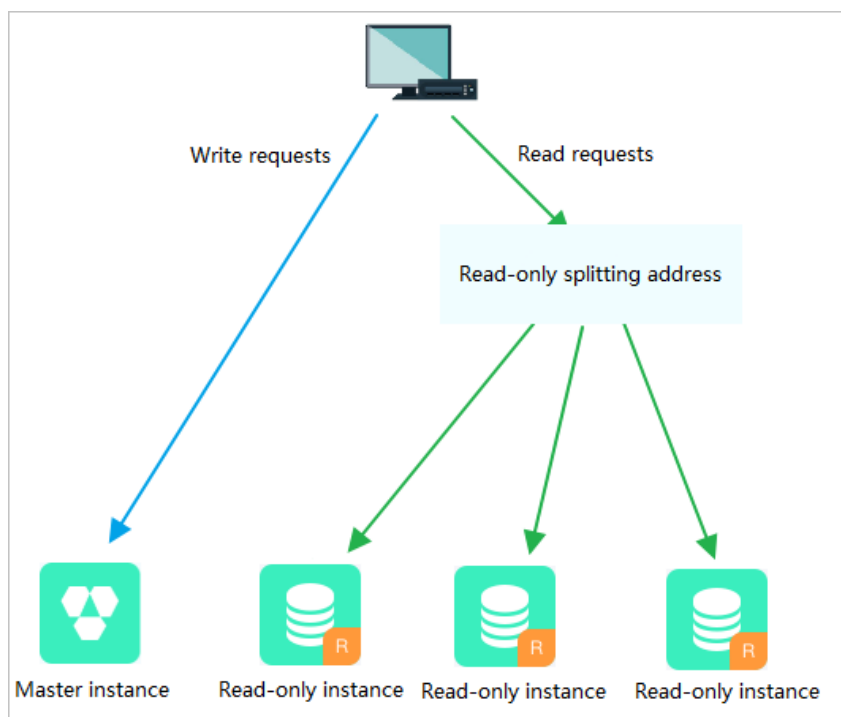
This topic introduces the read/write splitting feature of ApsaraDB RDS for SQL Server. This feature allows ApsaraDB RDS to distribute read requests to read-only RDS instances based on the read weights of these instances. This is implemented by using a read-only routing endpoint.

If your database system receives a large number of read requests but a small number of write requests, a single primary RDS instance may not be able to efficiently process the read requests. This may even interrupt your workloads. In this case, you can create one or more read-only RDS instances to offload read requests from the primary RDS instance. This allows you to scale the read capability of your database system. For more information, see [Overview of read-only ApsaraDB RDS for SQL Server instances](#).

After read-only RDS instances are created, you can enable the read/write splitting feature. You must add the endpoint of the primary RDS instance and the read-only routing endpoint to your application. Then, ApsaraDB RDS routes write requests to the primary RDS instance and read requests to the read-only routing endpoint. The read-only routing endpoint distributes the read requests to read-only RDS instances based on the read weights of these instances. For more information about how to enable the read/write splitting feature, see [Enable the read-only routing endpoint of an ApsaraDB RDS for SQL Server instance](#).

Note The read/write splitting feature works differently between ApsaraDB RDS for SQL Server and ApsaraDB RDS for MySQL.

- ApsaraDB RDS for SQL Server: You must add the endpoint of the primary RDS instance and the read-only routing endpoint to your application to achieve read/write splitting.
- ApsaraDB RDS for MySQL: You must add the read/write splitting endpoint to your application to achieve read/write splitting.



Differences between the read-only routing endpoint and the internal and public endpoints

After you enable the read/write splitting feature, a read-only routing endpoint is generated. You must add the read-only routing endpoint to your application. The read requests from your application are routed to the read-only routing endpoint and then are distributed to the read-only RDS instances based on the read weights of these instances.

If only the internal or public endpoint of the primary RDS instance is added to your application, all requests are routed to the primary RDS instance. To implement read/write splitting, you must add the endpoint of the primary RDS instance, the read-only routing endpoint, and the read weights of read-only RDS instances to your application.

Benefits

- Easier maintenance by using a unified read-only routing endpoint

You are provided with a unified read-only routing endpoint that can distribute read requests to read-only RDS instances. The read-only routing endpoint reduces maintenance costs.

In addition, you can scale the read capability of your database system by creating read-only RDS instances. This way, you do not need to modify the configuration data on your application.

- Higher performance by using a native RDS link


If you build a proxy layer on the cloud, data must be parsed and forwarded by a number of components before the data reaches your database system. This increases the response latency. The read/write splitting feature that is provided by ApsaraDB RDS precludes the additional components, shortens the response latency, and increases the processing speed.

- Ideal in various scenarios based on configurable read weights

You can specify the read weights of read-only RDS instances.


- Highly available with instance-level health checks

The cluster management feature actively performs health checks on read-only RDS instances. If a read-only RDS instance unexpectedly exits or its data replication latency exceeds the specified threshold, ApsaraDB RDS stops routing read requests to the instance and redirects these read requests to other healthy instances. Instance-level health checks allow you to ensure service availability in the event of faults on a single read-only RDS instance. After the faulty read-only RDS instance is recovered, ApsaraDB RDS resumes routing read requests to the instance.

 **Note** We recommend that you create at least two read-only RDS instances to avoid single points of failure (SPOFs).

- Free of charge

The read-only routing endpoint is free of charge.

 **Note** You must pay for the read-only RDS instances that you use. The pay-as-you-go billing method is used. For more information, see [Overview of read-only ApsaraDB RDS for SQL Server instances](#).

13.2. Create a read-only ApsaraDB RDS for SQL Server instance

This topic describes how to create a read-only ApsaraDB RDS for SQL Server instance. Read-only RDS instances allow your database system to process a large number of read requests. This increases the throughput of your application. Each read-only RDS instance is a replica of the primary RDS instance. This means that each read-only RDS instance has the same data as the primary RDS instance. Data updates on the primary RDS instance are also synchronized to each read-only RDS instance.

For more information about read-only RDS instances, see [Overview of read-only ApsaraDB RDS for SQL Server instances](#).

Prerequisites


The primary RDS instance runs SQL Server 2017 EE or 2019 EE.

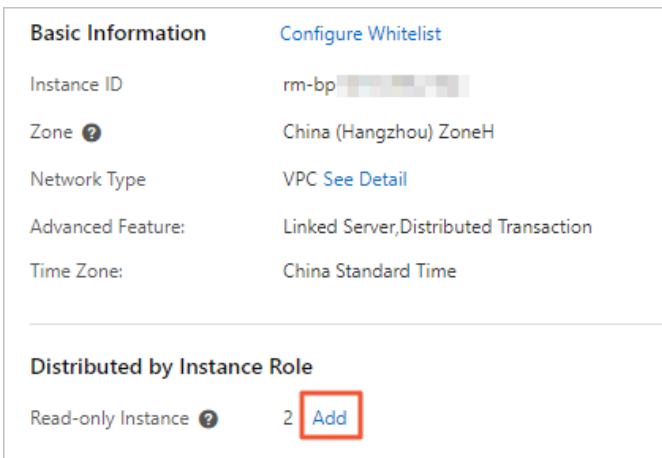
Precautions

- You can create read-only RDS instances for the primary RDS instance. However, you cannot convert existing RDS instances into read-only RDS instances.
- When you create a read-only RDS instance, ApsaraDB RDS replicates data from the secondary RDS instance to the read-only RDS instance. This prevents interruptions to your workloads on the primary RDS instance.
- You can create up to seven read-only RDS instances for each primary RDS instance.
- Read-only RDS instances support both the pay-as-you-go and subscription billing methods. For more information, see [Overview of read-only ApsaraDB RDS for SQL Server instances](#).



Create a read-only RDS instance

- 1.
2. In the **Distributed by Instance Role** section of the **Basic Information** page, click **Add**.

 **Note** If you are using the original ApsaraDB RDS console, click **Create Read-only Instance**.



3. Configure the following parameters and click **Next : Instance Configuration**.

Parameter	Description
Storage Type	<ul style="list-style-type: none"> ◦ Standard SSD: A standard SSD is an elastic block storage device that is designed based on the distributed storage architecture. You can store data on standard SSDs to separate computing from storage. ◦ Enhanced SSD: An enhanced SSD is an ultra-high performance disk that is designed by Alibaba Cloud based on the next-generation distributed block storage architecture. It integrates 25 Gigabit Ethernet and remote direct memory access (RDMA) technologies. This reduces one-way latency and delivers up to 1 million random input/output operations per second (IOPS). Supported enhanced SSDs come in the following three performance levels (PLs): <ul style="list-style-type: none"> ▪ PL1: An enhanced SSD of PL1 is a regular enhanced SSD. ▪ PL2: An enhanced SSD of PL2 delivers IOPS and throughput that are about twice higher than those delivered by an enhanced SSD of PL1. ▪ PL3: An enhanced SSD of PL3 delivers IOPS that is 20 times higher than the IOPS delivered by an enhanced SSD of PL1. It also delivers throughput that is 11 times higher than the throughput delivered by an enhanced SSD of PL1. Enhanced SSDs of PL3 are ideal for workloads that require high I/O performance in processing concurrent requests and high stability in read and write latencies. <p>For more information about storage types, see Storage types.</p>
Zone	The zone where the read-only RDS instance resides. Each zone is an independent physical location within a region.
Instance Type	<ul style="list-style-type: none"> ◦ General-purpose (Entry-level): belongs to the general-purpose instance family. A general-purpose instance exclusively occupies the allocated memory and I/O resources. However, it shares CPU and storage resources with the other general-purpose instances that are deployed on the same server. ◦ Dedicated Instance (Enterprise-level): belongs to the dedicated instance family or the dedicated host instance family. A dedicated instance exclusively occupies the allocated CPU, memory, storage, and I/O resources. The dedicated host instance family is the top configuration of the dedicated instance family. A dedicated host instance occupies all the CPU, memory, storage, and I/O resources on the server where it is deployed. <div style="background-color: #e6f2ff; padding: 10px; margin-top: 10px;"> <p> Note Each instance type supports a specific number of cores, memory capacity, maximum number of connections, and maximum IOPS. For more information, see Primary ApsaraDB RDS instance types.</p> </div>
Capacity	<p>The storage capacity that the read-only RDS instance has available to store data files, system files, binary log files, and transaction files. The storage capacity increases in increments of 5 GB.</p> <div style="background-color: #e6f2ff; padding: 10px; margin-top: 10px;"> <p> Note The dedicated instance family supports exclusive allocations of resources. Therefore, the storage capacity of each instance type with local SSDs in this family is fixed. For more information, see Primary ApsaraDB RDS instance types.</p> </div>

Note If you want to ensure the I/O performance that is required for data synchronization, we recommend that the specifications of the read-only RDS instance be higher than or equal to the specifications of the primary RDS instance. In this situation, the specifications refer to the memory capacity.

4. Configure the following parameters.

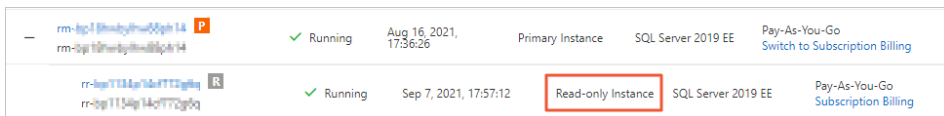
Parameter	Description
Network Type	<ul style="list-style-type: none"> ◦ Classic Network: the traditional type of network. ◦ VPC: A virtual private cloud (VPC) is an isolated network that provides higher security and better performance than the classic network. If you select the VPC network type, you must also specify the VPC parameter and the vSwitch of Primary Node parameter. <div style="background-color: #e0f2f7; padding: 5px; margin-top: 10px;"> <p>Note The read-only RDS instance must have the same network type as the Elastic Compute Service (ECS) instance to which you want to connect. If both the read-only RDS instance and the ECS instance use the VPC network type, make sure that they reside in the same VPC. Otherwise, they cannot communicate over an internal network.</p> </div>
Resource Group	The resource group to which the read-only RDS instance belongs.

5. Click **Next: Confirm Order**, confirm the settings in the **Parameters** section, specify the **Purchase Plan** parameter, read and select Terms of Service, click **Pay Now**, and then complete the payment.

A few minutes are required to create the read-only RDS instance.

View a read-only RDS instance

- To view a read-only RDS instance on the Instances page, perform the following steps:
 - Log on to the [ApsaraDB RDS console](#). In the left-side navigation pane, click **Instances**. In the top navigation bar, select the region where the read-only RDS instances reside.
 - Find the read-only RDS instance and click its ID.



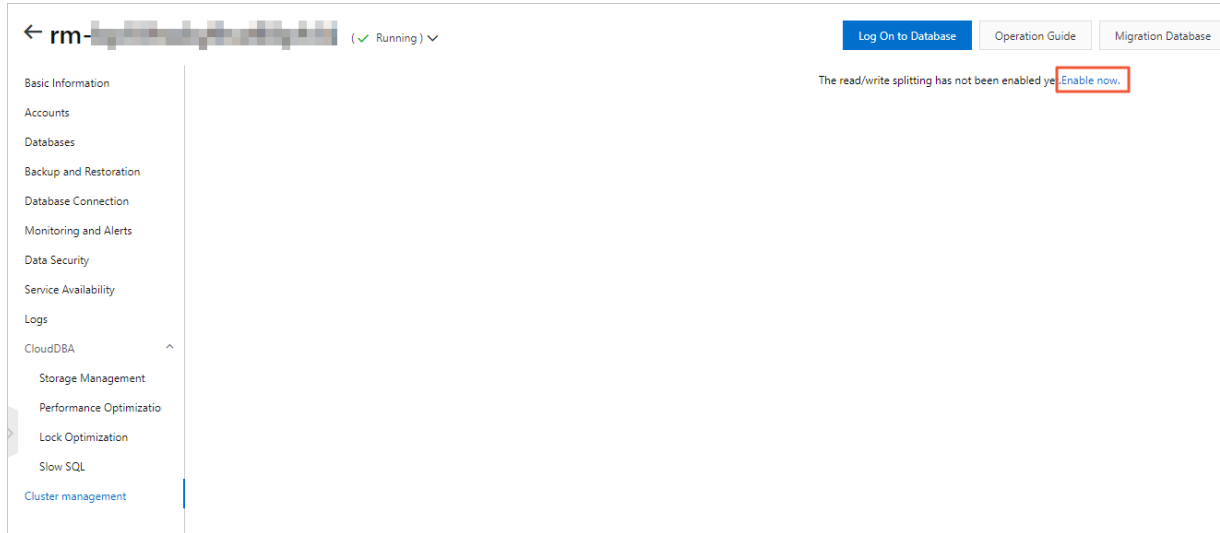
- To view a read-only RDS instance on the Basic Information page of the primary RDS instance, perform the following steps:
 - Log on to the [ApsaraDB RDS console](#). In the left-side navigation pane, click **Instances**. In the top navigation bar, select the region where the primary RDS instance resides.
 - Find the primary RDS instance and click its ID.
 - On the **Basic Information** page, move the pointer over the number of read-only RDS instances and click the ID of the read-only RDS instance that you want to view.



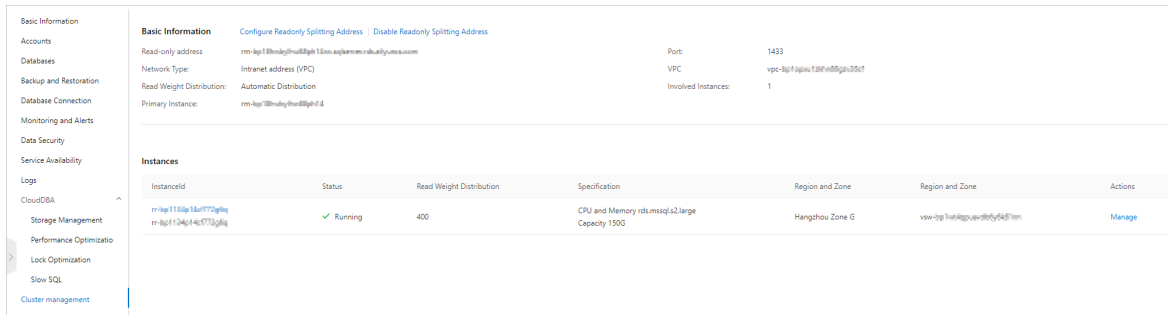
View a read-only RDS instance on the Cluster management page

Prerequisites

The read/write splitting feature is enabled on the **Cluster management** page of the primary RDS instance to which the read-only RDS instance is attached. For more information, see [Enable read/write splitting](#).



1. Log on to the [ApsaraDB RDS console](#)
2. Find the primary RDS instance and click its ID.
3. In the left-side navigation pane, click **Cluster management**.
4. Find the read-only instance and click its ID.



Related operations

Operation	Description
Create a read-only instance	Creates a read-only ApsaraDB RDS instance.

13.3. Enable the read-only routing endpoint of an ApsaraDB RDS for SQL Server instance

This topic describes how to enable the read-only routing endpoint of an ApsaraDB RDS for SQL Server instance. ApsaraDB RDS allows you to manage the read-only RDS instances in your database system and provides a read-only routing endpoint. You can add the endpoint of the primary RDS instance and the read-only routing endpoint to your application. In this case, ApsaraDB RDS routes write requests to the primary RDS instance and read requests to the read-only routing endpoint. Then, the read-only routing endpoint distributes the read requests to the read-only RDS instances based on the read weights of these instances.

Prerequisites

- The RDS instance is a primary instance.
- The RDS instance runs SQL Server 2017 EE or 2019 EE.
- The RDS instance has at least one read-only RDS instance. For more information about how to create a read-only RDS instance, see [Overview of read-only ApsaraDB RDS for SQL Server instances](#).

Precautions

- If you enable the read-only routing endpoint for the first time, ApsaraDB RDS automatically upgrades the backend administration systems of the primary and read-only RDS instances to the latest version. This ensures service availability. When you enable the read-only routing endpoint, the primary RDS instance encounters a transient connection of 30 seconds or less. During this period, all the read-only RDS instances of the primary RDS instance are inaccessible. We recommend that you enable the read-only routing endpoint during off-peak hours and make sure that your application is configured to automatically reconnect to your database system. This prevents interruptions to your business.
- If you restarted or changed the specifications of the primary and read-only RDS instances at least once after March 8, 2017, the backend administration systems of these instances are automatically upgraded to the latest version. In this situation, when you enable the read-only routing endpoint, your database system does not restart these instances, and no transient connections occur.
- The read-only routing endpoint does not change after it is generated. It does not change even when you enable or disable the read-only routing endpoint multiple times. You do not need to update the configuration data on your application on a regular basis. This reduces maintenance costs.

 **Note** The read-only routing endpoint cannot be manually modified.

- The read-only routing endpoint is free of charge. However, you still need to pay for the read-only RDS instances that you use. For more information, see [Overview of read-only ApsaraDB RDS for SQL Server instances](#).
- The read-only routing endpoint is not supported in the classic network.

Procedure

- 1.
2. In the left-side navigation pane, click **Cluster management**.
3. Click **Enable now**.
4. Configure the following parameters.

Configure Readonly Splitting Address
✕

Network Type Intranet address (VPC) Internet Address

Read Weight Distribution Automatic Distribution Customized Distribution
[How to set the weight?](#)

rr	Read-only instance	400
----	--------------------	-----

* 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.

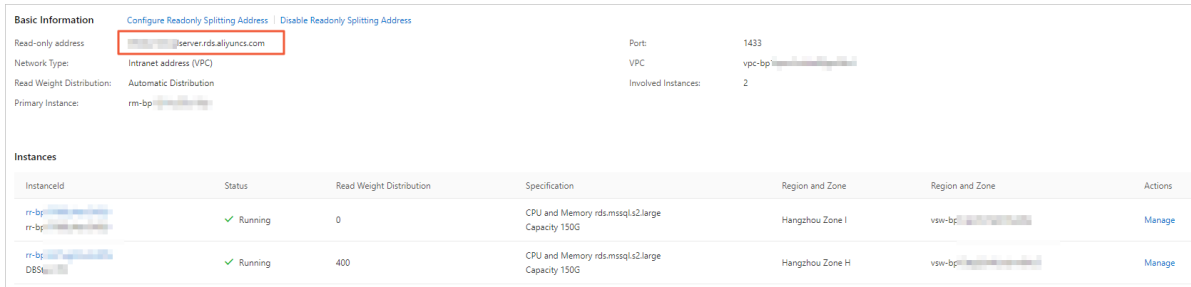
OK
Cancel

Parameter	Description
Network Type	<p>The type of the read-only routing endpoint.</p> <ul style="list-style-type: none"> ◦ Intranet address (VPC): RDS instances that run SQL Server 2017 EE or 2019 EE support only the virtual private cloud (VPC) network type. Therefore, the read-only routing endpoint must be of the VPC network type. ◦ Internet address: The read-only routing endpoint is connected over the Internet. However, the Internet is prone to fluctuations. We recommend that you connect to the read-only routing endpoint over an internal network.
Read Weight Distribution	<p>The method that is used to assign read weights. A higher read weight indicates more read requests to process. For example, if the primary RDS instance has three read-only RDS instances whose read weights are 100, 200, and 200, the three read-only RDS instances process read requests at the 1:2:2 ratio.</p> <ul style="list-style-type: none"> ◦ Automatic Distribution: ApsaraDB RDS assigns a read weight to each read-only RDS instance based on the specifications of the instance. After you create a read-only RDS instance, ApsaraDB RDS automatically assigns a read weight to the created read-only RDS instance. You do not need to manually specify a read weight for the created read-only RDS instance. For more information, see Default read weights. ◦ Customized Distribution: You must manually specify a read weight for each RDS instance in your database system. Valid values: 0 to 10000. After you create a read-only RDS instance, ApsaraDB RDS sets the read weight of the created read-only RDS instance to 0. You must manually modify the read weight of the created read-only RDS instance.

5. Click **OK**.

What to do next

- After you add the endpoint of the primary RDS instance and the read-only routing endpoint to your application, ApsaraDB RDS routes write requests to the primary RDS instance and read requests to the read-only routing endpoint. Then, the read-only routing endpoint distributes the read requests to the read-only RDS instances based on the read weights of these instances.



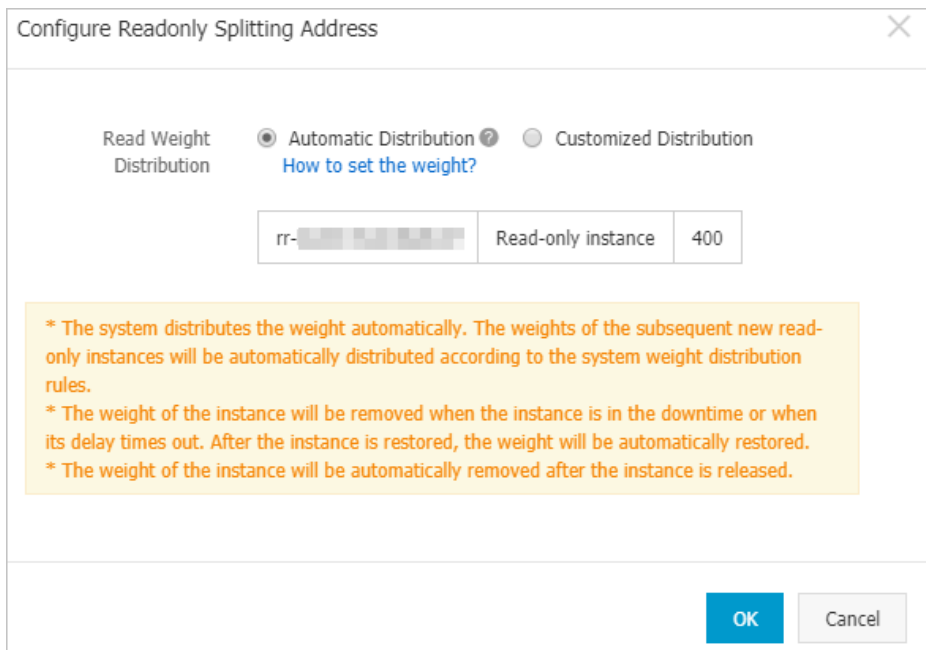
- You can view the ID, status, and read weight of each read-only RDS instance. You can also click **Manage** in the Actions column for a read-only RDS instance to manage the instance.


13.4. Modify the read weight of an ApsaraDB RDS for SQL Server instance

After you enable the read/write splitting feature of ApsaraDB RDS for SQL Server, you can modify the read weight of each RDS instance based on your business requirements.

Procedure

- 1.
2. In the left-side navigation pane, click **Cluster management**.
3. On the page that appears, click **Set Read-only Routing Endpoint**.



Parameter	Description
Read Weight Distribution	<p>The method to assign read weights. A higher read weight indicates more read requests to process. For example, if a primary RDS instance has three read-only RDS instances whose read weights are 100, 200, and 200, the three read-only RDS instances process read requests at the 1:2:2 ratio.</p> <ul style="list-style-type: none"> ◦ Automatic Distribution: ApsaraDB RDS assigns a read weight to each read-only RDS instance based on the instance specifications. After you create a read-only RDS instance, ApsaraDB RDS assigns a read weight to the instance and adds the instance to the read/write splitting link. No manual operations are required. For more information, see Default read weights. ◦ Customized Distribution: You must manually specify a read weight for each RDS instance. Valid values: 0 to 10000. After you create a read-only RDS instance, the read weight of the instance is 0 by default. You must manually specify a new read weight for the instance. <div style="background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p> Note If you delete a read-only RDS instance, its read weight is also removed, but the read weights of other RDS instances remain unchanged.</p> </div>

13.5. Disable the read-only routing endpoint of an ApsaraDB RDS for SQL Server instance

If your ApsaraDB RDS for SQL Server instance no longer needs the read/write splitting feature, you can disable the read-only routing endpoint of your RDS instance.

Prerequisites

The cluster management feature is enabled. For more information, see [Enable the read-only routing endpoint of an ApsaraDB RDS for SQL Server instance](#).

Precautions

- When you disable the read-only routing endpoint, a transient connection error of up to 30 seconds occurs. We recommend that you disable the read-only routing endpoint during off-peak hours and make sure that your application is configured to automatically reconnect to your database system. This prevents interruptions to your workloads.
- After you disable the read-only routing endpoint, it becomes invalid. Before you disable the read-only routing endpoint, make sure that your application no longer needs this endpoint.

Procedure

- 1.
2. In the left-side navigation pane, click **Cluster management**.
3. Click **Disable Readonly Splitting Address**.
4. In the message that appears, click **OK**.

13.6. Default read weights

This topic describes the default read weights of ApsaraDB RDS for SQL Server instances that have different specifications.

ApsaraDB RDS provides default read weights for read-only RDS instances.

Default read weights of read-only RDS instances

Instance type	Instance family	Memory	CPU	Default read weight
rds.mssql.s2.large	General-purpose	4 GB	2	400
rds.mssql.s3.large	General-purpose	8 GB	4	800
rds.mssql.c1.large	General-purpose	16 GB	8	1600
rds.mssql.s2.xlarge	General-purpose	8 GB	2	800
rds.mssql.m1.medium	General-purpose	16 GB	4	1600
rds.mssql.c1.xlarge	General-purpose	32 GB	8	3200
rds.mssql.c2.xlarge	General-purpose	64 GB	16	6400

13.7. Configure the read attribute for a secondary RDS instance of a primary ApsaraDB RDS for SQL Server instance

ApsaraDB RDS allows you to read data from secondary RDS instances of their primary ApsaraDB RDS for SQL Server instances that run RDS Cluster Edition. This topic describes how to configure the read attribute for a secondary RDS instance of a primary RDS instance. By default, after you create a primary RDS instance that runs RDS Cluster Edition, you can read data from the secondary RDS instance of the primary RDS instance. The secondary RDS instance serves as a read-only RDS instance, which reduces the cost of cloud migration.

Prerequisites

- The RDS instance runs SQL Server 2017 EE or SQL Server 2019 EE. For more information, see [Primary ApsaraDB RDS for SQL Server instance types](#).
- The RDS instance is a primary RDS instance.
- The read/write splitting feature is enabled for the primary RDS instance. For more information, see [Enable the read-only routing endpoint of an ApsaraDB RDS for SQL Server instance](#).

Functionality

- After you create an RDS instance that runs RDS Cluster Edition, a primary RDS instance and a secondary RDS instance are provisioned. By default, the secondary RDS instance is read-only. Therefore, the secondary RDS instance can serve as a read-only instance.
- After the read/write splitting feature is enabled for the primary RDS instance, you can configure read weights for the primary, secondary, and read-only RDS instances. For more information, see [Procedure](#).
- If an existing primary RDS instance runs RDS Cluster Edition and the read/write splitting feature is enabled for the primary RDS instance, you can directly read data from the secondary RDS instance of the primary RDS instance. If the read/write splitting feature is disabled, you must enable the feature and configure a read-only routing endpoint. For more information, see [Procedure](#).

Procedure

- 1.
2. In the left-side navigation pane, click **Cluster management**.
3. On the page that appears, click **Configure Readonly Splitting Address** next to **Basic Information** to configure read weights.

Related operations

Operation	Description
AllocateReadWriteSplittingConnection	Applies for a read-only routing endpoint for a primary ApsaraDB RDS instance.

14.Account

14.1. 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:

- [Create accounts and databases for an ApsaraDB RDS instance that runs SQL Server 2017 EE or 2019 EE](#)
- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2012, 2014, 2016, 2017 SE, or 2019 SE](#)
- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2008 R2](#)

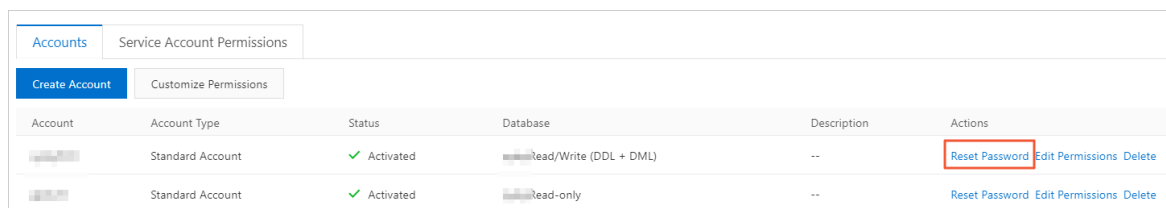
14.2. Reset the password of an account on an ApsaraDB RDS for SQL Server instance

This topic describes how to reset the password of an account on your ApsaraDB RDS for SQL Server instance. If the password is lost, you can reset the password in the ApsaraDB for RDS console.

Procedure

Note For data security purposes, we recommend that you change the password of each account on a regular basis.

- 1.
2. In the left-side navigation pane, click **Accounts**.
3. Find the account whose password you want to reset, and click **Reset Password** in the Actions column.



Account	Account Type	Status	Database	Description	Actions
██████████	Standard Account	✓ Activated	██████████ Read/Write (DDL + DML)	--	Reset Password Edit Permissions Delete
██████████	Standard Account	✓ Activated	██████████ Read-only	--	Reset Password Edit Permissions Delete

4. In the dialog box that appears, specify a new password, confirm the new password, and then click **Create**.

- Note** The password must meet the following requirements:
- The password must be 8 to 32 characters in length.
 - The password must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters.
 - The password can contain any of the following characters:
! @ # \$ % ^ & * () _ + - =

Related operations

Operation	Description
ResetAccountPassword	Resets the password of an account on an ApsaraDB RDS instance.

14.3. Account permission

14.3.1. Modify the permissions of a standard account on an ApsaraDB RDS for SQL Server instance

This topic describes how to modify the permissions of a standard account on an ApsaraDB RDS for SQL Server instance. The permissions of a privileged account can only be reset to the default settings but cannot be modified.

Procedure

-
- In the left-side navigation pane, click **Accounts**.
- Find the standard account whose permissions you want to modify, and click **Edit Permissions** in the Actions column.

Account	Account Type	Status	Database	Description	Actions
	Standard Account	Activated		None	Reset Password Edit Permissions Delete

- In the **Modify Account Permissions** panel, modify the permissions of the standard account.
 - If you want to add or remove an authorized database, select the database and click the > or < icon.
 - If you want to modify the permissions on an authorized database, select the database and then select the **Read/Write (DML)**, **Read-only**, or **Owner** permissions in the **Authorized Databases** section.
- Click **OK**.

14.3.2. Account permissions in an ApsaraDB RDS for SQL Server instance

This topic describes the accounts that you can use in an ApsaraDB RDS for SQL Server instance. This topic also describes the roles and permissions of the accounts.

Precautions

- For security purposes, ApsaraDB RDS restricts specific permissions. The restricted permissions are encapsulated in stored procedures. You can run the stored procedures to perform the operations on which the permissions are restricted. For more information, see [Stored procedures](#).
- To obtain the permissions of a superuser account, you must submit a . A superuser account has the highest management permissions. After you obtain the permissions of a superuser account, the [service level agreement \(SLA\)](#) for ApsaraDB RDS is no longer in effect.

Account permissions

Account type	Authorized object	Permission type	Role	Permission
				<input type="checkbox"/> Server-level permission <ul style="list-style-type: none"> • CONNECT SQL • ALTER ANY LOGIN • ALTER ANY LINKED SERVER • ALTER ANY CONNECTION • ALTER TRACE • VIEW ANY DATABASE • VIEW SERVER STATE • ALTER SERVER STATE <input type="checkbox"/> Database-level permission <ul style="list-style-type: none"> • CREATE TABLE • CREATE VIEW • CREATE PROCEDURE • CREATE FUNCTION • CREATE RULE • CREATE DEFAULT • CREATE TYPE • CREATE ASSEMBLY • CREATE XML SCHEMA COLLECTION • CREATE SCHEMA • CREATE SYNONYM • CREATE AGGREGATE • CREATE ROLE • CREATE MESSAGE TYPE

Account type	Authorized object	Permission type	Role	Permission
<ul style="list-style-type: none"> Privilege 	..	Owner	<ul style="list-style-type: none"> Server-level role <ul style="list-style-type: none"> public processadmin setupadmin Database-level role <ul style="list-style-type: none"> public db_owner 	<ul style="list-style-type: none"> CREATE SERVICE CREATE CONTRACT CREATE REMOTE SERVICE BINDING CREATE ROUTE CREATE QUEUE CREATE SYMMETRIC KEY CREATE ASYMMETRIC KEY CREATE FULLTEXT CATALOG CREATE CERTIFICATE CREATE DATABASE DDL EVENT NOTIFICATION CONNECT CONNECT REPLICATION CHECKPOINT SUBSCRIBE QUERY NOTIFICATIONS AUTHENTICATE SHOWPLAN ALTER ANY USER ALTER ANY ROLE ALTER ANY APPLICATION ROLE ALTER ANY COLUMN ENCRYPTION KEY ALTER ANY COLUMN MASTER KEY ALTER ANY SCHEMA ALTER ANY ASSEMBLY ALTER ANY DATABASE SCOPED CONFIGURATION ALTER ANY DATASPACE ALTER ANY EXTERNAL DATA SOURCE ALTER ANY EXTERNAL FILE FORMAT ALTER ANY MESSAGE TYPE ALTER ANY CONTRACT ALTER ANY SERVICE ALTER ANY REMOTE SERVICE BINDING ALTER ANY ROUTE ALTER ANY FULLTEXT CATALOG ALTER ANY SYMMETRIC KEY ALTER ANY ASYMMETRIC KEY ALTER ANY CERTIFICATE ALTER ANY SECURITY POLICY SELECT INSERT UPDATE DELETE REFERENCES

Account type	User database object	Permission type	Role	Permission
<ul style="list-style-type: none"> Standard account 				<ul style="list-style-type: none"> EXECUTE ALTER ANY DATABASE DDL TRIGGER ALTER ANY DATABASE EVENT NOTIFICATION ALTER ANY DATABASE AUDIT ALTER ANY DATABASE EVENT SESSION KILL DATABASE CONNECTION VIEW ANY COLUMN ENCRYPTION KEY DEFINITION VIEW ANY COLUMN MASTER KEY DEFINITION VIEW DATABASE STATE VIEW DEFINITION TAKE OWNERSHIP ALTER ALTER ANY MASK UNMASK EXECUTE ANY EXTERNAL SCRIPT CONTROL
		Read permissions	<ul style="list-style-type: none"> Server-level role <ul style="list-style-type: none"> public processadmin setupadmin Database-level role <ul style="list-style-type: none"> public db_datareader 	<ul style="list-style-type: none"> <input type="checkbox"/> Server-level permission <ul style="list-style-type: none"> CONNECT SQL ALTER ANY LOGIN ALTER ANY LINKED SERVER ALTER ANY CONNECTION ALTER TRACE VIEW ANY DATABASE VIEW SERVER STATE ALTER SERVER STATE <input type="checkbox"/> Database-level permission <ul style="list-style-type: none"> CONNECT SHOWPLAN SELECT KILL DATABASE CONNECTION VIEW ANY COLUMN ENCRYPTION KEY DEFINITION VIEW ANY COLUMN MASTER KEY DEFINITION VIEW DATABASE STATE

Account type	Authorized object	Permission type	Role	Permission
		Read and write permissions (DML)	<ul style="list-style-type: none"> • Server-level role <ul style="list-style-type: none"> ◦ public ◦ processadmin ◦ setupadmin • Database-level role <ul style="list-style-type: none"> ◦ public ◦ db_datareader ◦ db_datawriter 	<input type="checkbox"/> Server-level permission <ul style="list-style-type: none"> • CONNECT SQL • ALTER ANY LOGIN • ALTER ANY LINKED SERVER • ALTER ANY CONNECTION • ALTER TRACE • VIEW ANY DATABASE • VIEW SERVER STATE • ALTER SERVER STATE <input type="checkbox"/> Database-level permission <ul style="list-style-type: none"> • CONNECT • SHOWPLAN • SELECT • INSERT • UPDATE • DELETE • KILL DATABASE CONNECTION • VIEW ANY COLUMN ENCRYPTION KEY DEFINITION • VIEW ANY COLUMN MASTER KEY DEFINITION • VIEW DATABASE STATE
				<input type="checkbox"/> Server-level permission <ul style="list-style-type: none"> • CONNECT SQL • SHUTDOWN • CREATE ENDPOINT • CREATE ANY DATABASE • CREATE AVAILABILITY GROUP • ALTER ANY LOGIN • ALTER ANY CREDENTIAL • ALTER ANY ENDPOINT • ALTER ANY LINKED SERVER • ALTER ANY CONNECTION • ALTER ANY DATABASE • ALTER RESOURCES • ALTER SETTINGS • ALTER TRACE

Account type	Authorized object	Permission type	Role	Permission
Superuser account	All databases	All permission	<ul style="list-style-type: none"> Server-level role: sysadmin 	<ul style="list-style-type: none"> ALTER ANY AVAILABILITY GROUP ADMINISTER BULK OPERATIONS AUTHENTICATE SERVER EXTERNAL ACCESS ASSEMBLY VIEW ANY DATABASE VIEW ANY DEFINITION VIEW SERVER STATE CREATE DDL EVENT NOTIFICATION CREATE TRACE EVENT NOTIFICATION ALTER ANY EVENT NOTIFICATION ALTER SERVER STATE UNSAFE ASSEMBLY ALTER ANY SERVER AUDIT CREATE SERVER ROLE ALTER ANY SERVER ROLE ALTER ANY EVENT SESSION CONNECT ANY DATABASE IMPERSONATE ANY LOGIN SELECT ALL USER SECURABLES CONTROL SERVER <p><input type="checkbox"/> Database-level permission</p> <ul style="list-style-type: none"> CREATE TABLE CREATE VIEW CREATE PROCEDURE CREATE FUNCTION CREATE RULE CREATE DEFAULT BACKUP DATABASE BACKUP LOG CREATE DATABASE CREATE TYPE CREATE ASSEMBLY CREATE XML SCHEMA COLLECTION CREATE SCHEMA CREATE SYNONYM CREATE AGGREGATE CREATE ROLE CREATE MESSAGE TYPE CREATE SERVICE CREATE CONTRACT CREATE REMOTE SERVICE BINDING CREATE ROUTE CREATE QUEUE

Account type	Authorized object	Permission type	Database-level Role: db_owner	Permission
				<ul style="list-style-type: none"> • CREATE SYMMETRIC KEY • CREATE ASYMMETRIC KEY • CREATE FULLTEXT CATALOG • CREATE CERTIFICATE • CREATE DATABASE DDL EVENT NOTIFICATION • CONNECT • CONNECT REPLICATION • CHECKPOINT • SUBSCRIBE QUERY NOTIFICATIONS • AUTHENTICATE • SHOWPLAN • ALTER ANY USER • ALTER ANY ROLE • ALTER ANY APPLICATION ROLE • ALTER ANY COLUMN ENCRYPTION KEY • ALTER ANY COLUMN MASTER KEY • ALTER ANY SCHEMA • ALTER ANY ASSEMBLY • ALTER ANY DATABASE SCOPED CONFIGURATION • ALTER ANY DATASPACE • ALTER ANY EXTERNAL DATA SOURCE • ALTER ANY EXTERNAL FILE FORMAT • ALTER ANY MESSAGE TYPE • ALTER ANY CONTRACT • ALTER ANY SERVICE • ALTER ANY REMOTE SERVICE BINDING • ALTER ANY ROUTE • ALTER ANY FULLTEXT CATALOG • ALTER ANY SYMMETRIC KEY • ALTER ANY ASYMMETRIC KEY • ALTER ANY CERTIFICATE • ALTER ANY SECURITY POLICY • SELECT • INSERT • UPDATE • DELETE • REFERENCES • EXECUTE • ALTER ANY DATABASE DDL TRIGGER • ALTER ANY DATABASE EVENT NOTIFICATION • ALTER ANY DATABASE AUDIT

Account type	Authorized object	Permission type	Role	Permissions
				<ul style="list-style-type: none"> ALTER ANY DATABASE EVENT SESSION KILL DATABASE CONNECTION VIEW ANY COLUMN ENCRYPTION KEY DEFINITION VIEW ANY COLUMN MASTER KEY DEFINITION VIEW DATABASE STATE VIEW DEFINITION TAKE OWNERSHIP ALTER ALTER ANY MASK UNMASK EXECUTE ANY EXTERNAL SCRIPT CONTROL

14.4. Grant permissions to the service account of an ApsaraDB RDS for SQL Server instance

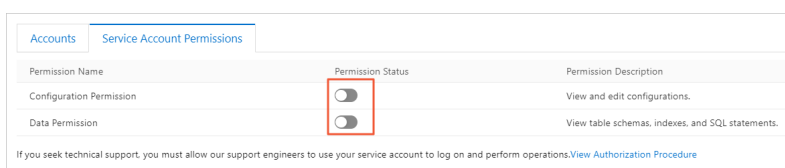
When you seek help from Alibaba Cloud technical support to locate problems that occurred on your ApsaraDB RDS for SQL Server instance, you may need to grant permissions to the service account of your RDS instance. The service account is used by Alibaba Cloud technical support to perform operations on the databases of your RDS instance. After the specified expiration time elapses, ApsaraDB RDS deletes the service account.

Prerequisites

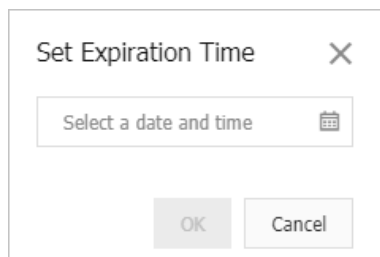
Your RDS instance runs SQL Server 2008 R2 with local SSDs.

Procedure

- 1.
2. In the left-side navigation pane, click **Accounts**
3. On the **Service Account Permissions** tab, find the permission that you want to grant to the service account, and turn on the switch in the **Permission Status** column.
 - o For problems that are related to IP address whitelists or database parameters, you can grant only the **Configuration Permission** to the service account.
 - o For database performance problems that are caused by applications, you must grant the **Data Permission** to the service account.



- In the dialog box that appears, specify the expiration time of the service account and click OK.



What to do next

After you grant permissions to the service account, you can revoke the permissions or change the expiration time on the **Service Account Permissions** tab at any time.

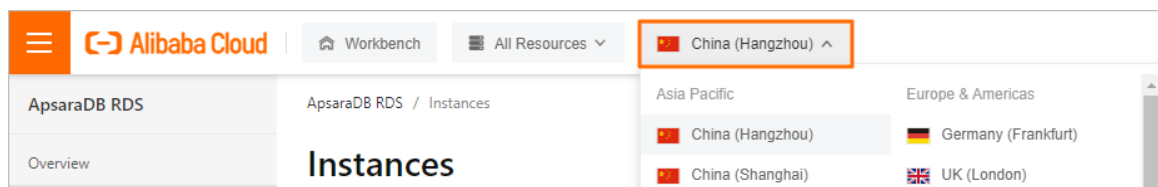
14.5. Delete an account for an RDS SQL Server instance

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

- Log on to the [RDS console](#).
- In the upper-left corner, select the region where the target RDS instance is located.



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

APIs

API	Description
Delete an account	Used to delete an account for an RDS instance.

14.6. 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.

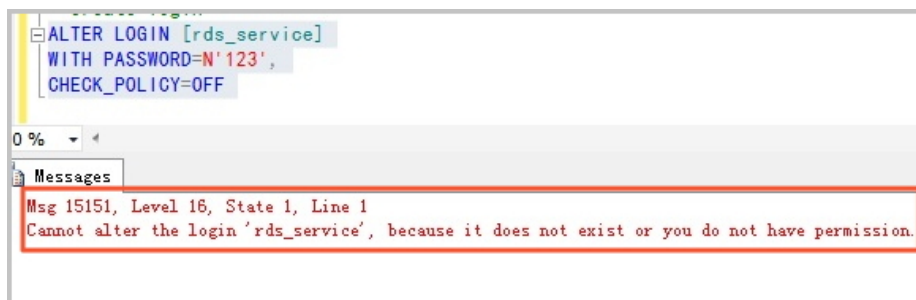


Modify the login information

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:



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.

14.7. 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 [Create and manage databases on an ApsaraDB RDS for SQL Server instance by using 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:

```
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.

```
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.

```
USE TestDB
GO
DROP USER test
```

14.8. Create a system admin account on an ApsaraDB RDS for SQL Server instance

This topic describes how to create a system admin account on an ApsaraDB RDS for SQL Server instance. You can use the system admin account to migrate the data of an on-premises SQL Server instance to the RDS instance.


Prerequisites

- The RDS instance runs one of the following SQL Server versions and RDS Editions:
 - SQL Server 2017 EE or 2019 EE on RDS Cluster Edition
 - SQL Server 2012 SE, 2012 EE, 2016 SE, 2016 EE, 2017 SE, and 2019 SE on RDS High-availability Edition
- The RDS instance belongs to the general-purpose instance family or the dedicated instance family.
- Your Alibaba Cloud account is used to log on to the ApsaraDB RDS console.
- The RDS instance is created on or after January 1, 2021.

Note

- This feature is available only to specific customers. If you want to use this feature, submit a or contact your customer manager.
- You can view the **Creation Time** parameter of an RDS instance in the **Status** section of the **Basic Information** page in the ApsaraDB RDS console.

Precautions

 **Warning** After a system admin account is created, you cannot disable the system admin account or roll back the creation operation. Proceed with caution. If you create a system admin account, the service levels in the service level agreement (SLA) cannot be guaranteed. For more information, see [SLA](#).

- You can create only one system admin account per RDS instance.
- RDS instances in the Cloud Tmall system do not support system admin accounts.
- You cannot use the following usernames for system admin accounts:

```
rootadmieagleyemasteraurorasysadminadministratormssqlpublicsecurityadminserveradminsetup
adminprocessadmindiskadmindbcraorbulkadmintempdbmsdbmodeldistributionmssqlsystemresource
guestaddexceptpercentallexecplanalterexecuteprecisionandexistsprimaryanyexitprintasfetchpr
ocascfileprocedureauthorizationfillfactorpublicbackupforraiserrorbeginforeignreadbetweenfr
eetextreadtextbreakfreetexttableconfigurebrowsefromreferencesbulkfullreplicationbyfuncti
onrestorecascadegotorestrictcasegrantreturncheckgrouprevokecheckpointhavingrightcloseholdl
ockrollbackclusteredidentityrowcountcoalesceidentity_insertrowguidcolcollateidentitycolrul
ecolumnifsavecommitinschemacomputeindexselectconstraintinnersession_usercontainsinsertsetc
ontainstableintersectsetusercontinueintoshutdownconvertissomecreatejoinstatisticscrosskeys
ystem_usercurrentkilltablecurrent_datelefttextsizecurrent_timelikethencurrent_timestamplin
enotocurrent_userloadtopcursornationaltrandatabasenochecktransactiondbccnonclusteredtrigge
rdeallocatenottruncatedeclarenulltsequaldefaultnullifuniondeleteofuniquedenyoffupdatedesco
ffsetsupdatetextdiskonusedistinctopenuserdistributedopendatasourcevaluesdoubleopenqueryvar
yingdropopenrowsetviewdummyopenxmlwaitfordumpoptionwhenelseorwhereendorderwhileerrlvlouter
withescapeoverwritetextdbologinsysdrc_rds$
```

Procedure

- 1.

- In the left-side navigation pane, click **Accounts**.
- Click **Create Account** and configure the following parameters.

Create Account
✕

*** Database Account:**

The account name can be up to 64 characters in length and can contain lowercase letters, digits, and underscores (_). It must start with a letter and end with a letter or digit.

*** Account Type ?**

Privileged Account
 Standard Account
 System Admin Account

The RDS SLA cannot be guaranteed after a system admin account is created because this account has the most permissions.

I have read and agree to changes to the [RDS Service Level Agreement](#) caused by the creation of a system admin account.

*** Password**

The password must be 8 to 32 characters in length and must contain at least three of the following types: uppercase letters, lowercase letter, digits, and special characters. Special characters include ! @ # \$ % ^ & * () _ + - =

*** Confirm Password**

Description

0/256

The description must be 0 to 256 characters in length.

Determine
Cancel

Parameter	Description
Database Account	Enter the username of the account. The username must be 2 to 64 characters in length and can contain lowercase letters, digits, and underscores (_). The username must start with a lowercase letter and end with a lowercase letter or a digit.
Account Type	Select System Admin Account . Then, read the agreement and select I have read and agree to changes to the RDS Service Level Agreement caused by the creation of a system admin account . <div style="background-color: #fff9c4; padding: 10px; margin-top: 10px;"> ⚠ Warning After a system admin account is created, you cannot disable the system admin account or roll back the creation operation. Proceed with caution. If you create a system admin account, the service levels in the SLA cannot be guaranteed. For more information, see SLA. </div>

Parameter	Description
Password	<p>Enter the password for the account. The password must meet the following requirements:</p> <ul style="list-style-type: none"> The password of the account must be 8 to 32 characters in length. The password must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. The password can contain any of the following characters: ! @ # \$ % ^ & * () _ + - =
Confirm 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.

4. Click OK.

Create Account					
Account	Account Type	Status	Database	Description	Actions
testsa	System Admin Account	✓ Activated	All Databases, All Permissions	System Admin Permissions	Reset Password Deactivate Account Delete

14.9. Create a host account for an ApsaraDB RDS for SQL Server instance and use the host account for logons

This topic describes how to create a host account for an ApsaraDB RDS for SQL Server instance. You can use the created host account in the Bastionhost console to connect to and manage the hosts on which the RDS instance and its secondary RDS instance run.


Prerequisites

- The RDS instance runs one of the following SQL Server versions and RDS Editions:
 - SQL Server 2017 EE or 2019 EE on RDS Cluster Edition
 - SQL Server 2012 SE, 2012 EE, 2016 SE, 2016 EE, 2017 SE, or 2019 SE on RDS High-availability Edition
- The RDS instance belongs to the general-purpose instance family or the dedicated instance family.
- Your Alibaba Cloud account is used to log on to the ApsaraDB RDS console.
- The RDS instance was created on or after January 1, 2021.

Note

- Host accounts are available only to specific customers. If you want to use host accounts, you must submit a or contact your customer manager.
- You can view the **Creation Time** of the RDS instance in the **Status** section of the **Basic Information** page.

Precautions

 **Warning** The host account of an RDS instance has the highest management permissions on the RDS instance. After you create a host account for an RDS instance, ApsaraDB RDS does not provide the service availability that is specified in Alibaba Cloud [service level agreement \(SLA\)](#) for the RDS instance.

- RDS instances in CloudTmall system do not support host accounts.
- The following usernames cannot be used for host accounts:

```
root|admin|eagleeye|master|aurora|sysadmin|administrator|mssqld|public|securityadmin|server
admin|setupadmin|processadmin|diskadmin|dbcreator|bulkadmin|tempdb|msdb|model|distribution
|mssqlsystemresource|guest|add|except|percent|all|exec|plan|alter|execute|precision|and|ex
ists|primary|any|exit|print|as|fetch|proc|asc|file|procedure|authorization|fillfactor|publ
ic|backup|for|raiserror|begin|foreign|read|between|freetext|readtext|break|freetexttable|r
econfigure|browse|from|references|bulk|full|replication|by|function|restore|cascade|goto|r
estRICT|case|grant|return|check|group|revoke|checkpoint|having|right|close|holdlock|rollba
ck|clustered|identity|rowcount|coalesce|identity_insert|rowguidcol|collate|identitycol|rul
e|column|if|save|commit|in|schema|compute|index|select|constraint|inner|session_user|conta
ins|insert|set|containstable|intersect|setuser|continue|into|shutdown|convert|is|some|crea
te|join|statistics|cross|key|system_user|current|kill|table|current_date|left|textsize|cur
rent_time|like|then|current_timestamp|lineno|to|current_user|load|top|cursor|national|tran
|database|nocheck|transaction|dbcc|nonclustered|trigger|deallocate|not|truncate|declare|nu
ll|tsequal|default|nullif|union|delete|of|unique|deny|off|update|desc|offsets|updatetext|d
isk|on|use|distinct|open|user|distributed|opendatasource|values|double|openquery|varying|d
rop|openrowset|view|dummy|openxml|waitfor|dump|option|when|else|or|where|end|order|while|e
rrlvl|outer|with|escape|over|writetext|dbo|login|sys|drc_rds
```

Procedure

- [Step 1: Create a host account](#)
- [Step 2: Configure a bastion host](#)
- [Step 3: Connect to the hosts of the RDS instance and its secondary RDS instance in the Bastionhost console](#)

Step 1: Create a host account

- 1.
2. In the left-side navigation pane, click **Accounts**.
3. On the **Host Accounts** tab, click **Create Account** and configure the following parameters.

Parameter	Description
Host Account Name	Enter the username of the account. The username must be 2 to 64 characters in length and can contain lowercase letters, digits, and underscores (_). The username must start with a lowercase letter and end with a lowercase letter or a digit.
Account Type	Select Standard Account.

Parameter	Description
Password	Enter the password of the account. The password must meet the following requirements: <ul style="list-style-type: none"> The password must be 8 to 32 characters in length. The password must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. The password can contain any of the following special characters: ! @ # \$ % ^ & * () _ + - =
Confirm 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.

- Select **I have read and agree to the changes to the RDS Service Level Agreement caused by the creation of a host account**.
- Click **OK**.
- Optional. Click **Reset Password** or **Delete** in the Actions column to reset the password of the host account or delete the host account.

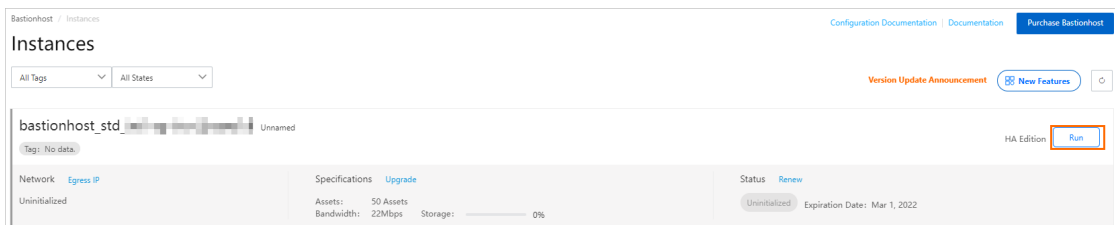
Step 2: Configure a bastion host

After you create a host account, you must configure a bastion host in the Bastionhost console to connect to and manage the hosts on which the RDS instance and its secondary RDS instance run.

- Create a bastion host. For more information, see [Purchase a bastion host](#).

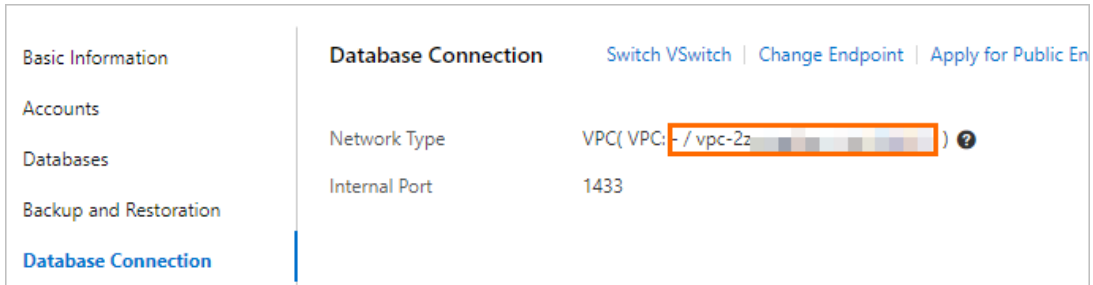
Note The bastion host needs to connect to the RDS instance over an internal network. Make sure that the bastion host resides in the same region as the RDS instance.

- Run the bastion host.
 - Log on to the [Bastionhost console](#).
 - In the top navigation bar, select the region where the bastion host resides.
 - Find the bastion host and click **Run** on the right.



iv. Select a **VPC** and a **vSwitch** in the Select Network section, select a **security group** in the Select Security Group section, and then click **Next**.

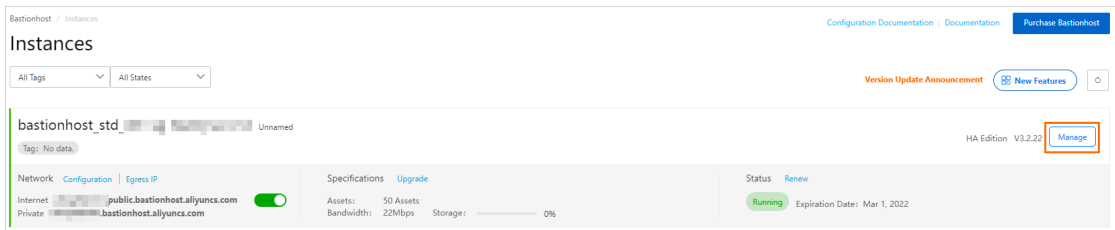
- Virtual private cloud (VPC): Select the VPC to which the RDS instance belongs. You can check the VPC of the RDS instance on the Database Connection page in the ApsaraDB RDS console.



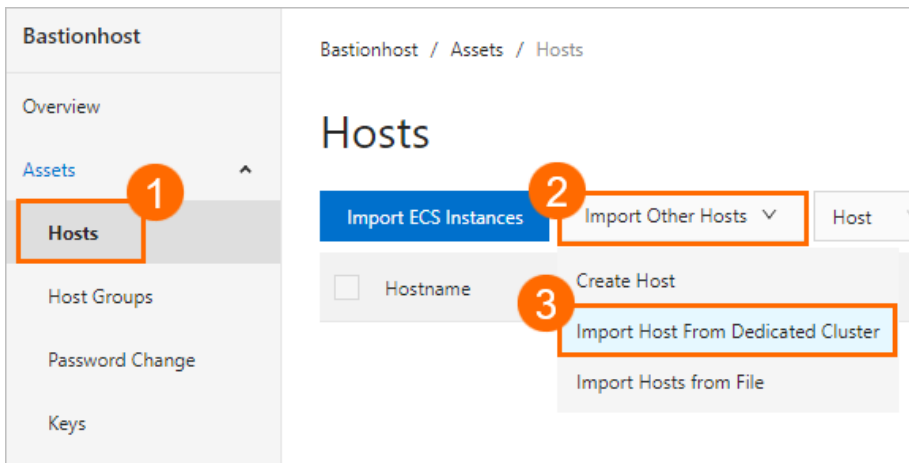
- vSwitch: Select a vSwitch that is associated with the specified VPC.
- Security group: Select the security group that you want to use to manage the connection between the bastion host and the Elastic Compute Service (ECS) instance. You cannot use this security group to manage the connections between the bastion host and the hosts of the RDS instance and its secondary RDS instance. You can select one of the available security groups.

3. Import the hosts of the RDS instance and its secondary RDS instance into the bastion host.

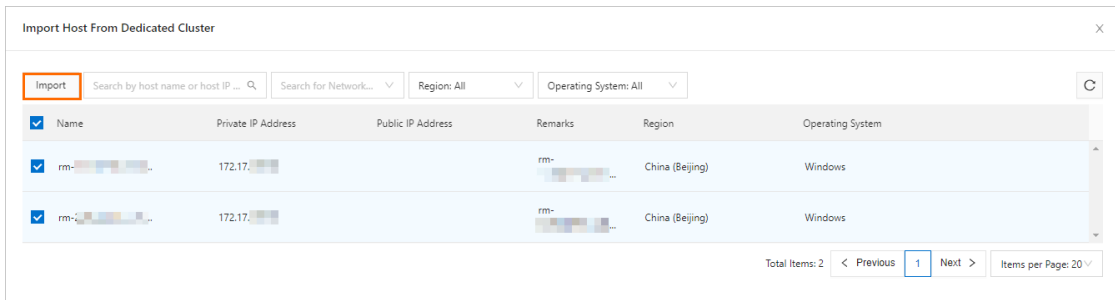
i. Find the bastion host and click **Manage** on the right side of the bastion host.



ii. Choose **Assets > Hosts** and select **Import Hosts From Dedicated Clusters** from the **Import Other Hosts** drop-down list.

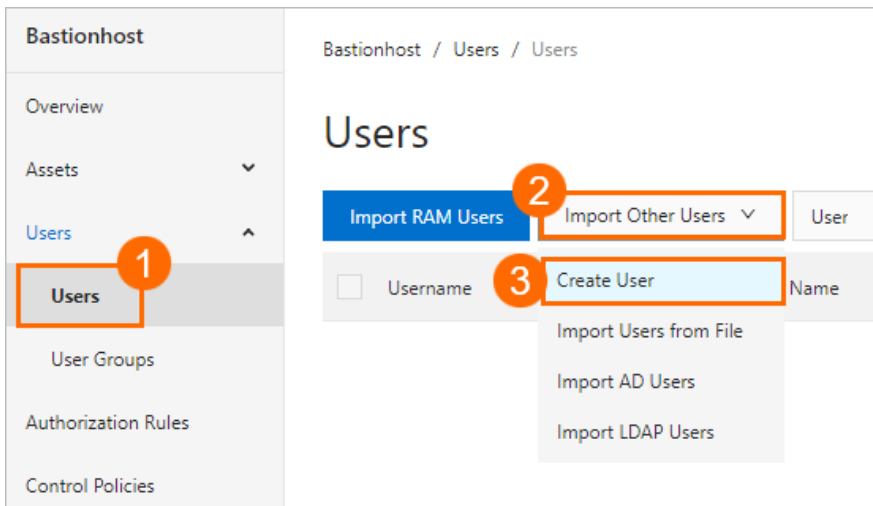


- iii. Enter the ID of the RDS instance in the search box, select the RDS instance and its secondary RDS instance, and then click **Import**.



Note In the search results, the hosts of the RDS instance are named `rdsld_master` and `rdsld_slave`. The `rdsld_master` host is the host of the primary RDS instance and the `rdsld_slave` host is the host of the secondary RDS instance.

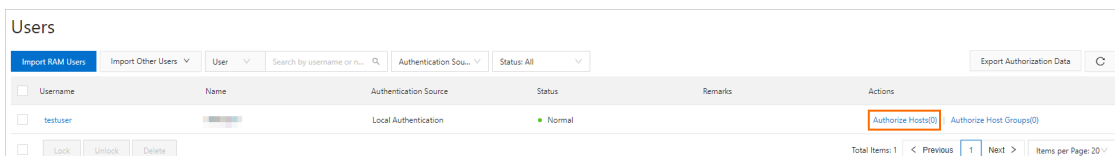
- 4. Create a bastion host user that is used to log on to the Bastionhost console.
 - i. Choose **Users > Users** and select **Create User** from the **Import Other Users** drop-down list.



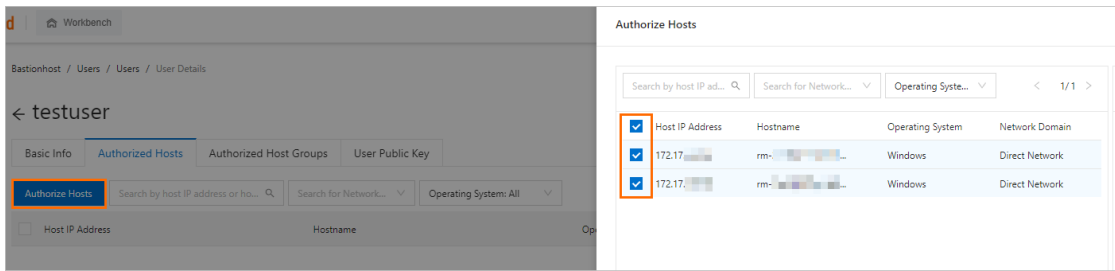
- ii. Specify the information of the user. The user information includes **Username** and **Password**. Then, click **Create**.

Note For more information, see [Manage users](#).

- 5. Grant the permissions on the imported hosts to the bastion host user.
 - i. Find the bastion host user and click **Authorize Hosts** in the Actions column.

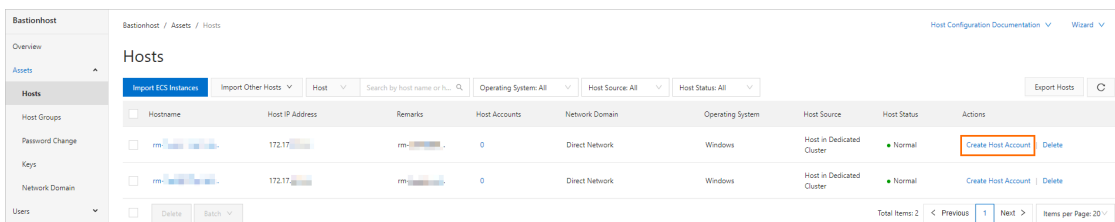


- ii. On the **Authorized Hosts** tab, click **Authorized Hosts**, select the imported hosts, and then click **OK**.



6. Create host accounts for the imported hosts.

- i. Choose **Assets > Hosts**, find the imported hosts, and then click **Create Host Account** in the **Actions** column to add host accounts for the hosts of the RDS instance and its secondary RDS instance.



ii. In the **Create Host Account** dialog box, configure the following parameters.

×

Make sure that the corresponding operating system account has been created in the host or ECS instance. Bastionhost does not synchronize host accounts to the host or ECS instance.

*** Protocol**

RDP
▼

*** Logon Name**

host_testuser

Authentication Type

Password
▼

Password

.....
🗑️
?

Verify

Parameter	Description
Protocol	Select RDP.
Logon Name	Enter the username of the host account. The username must be the same as the username of the host account that you created in the " Step 1: Create a host account " section of this topic.
Authentication Type	Select Password.
Password	Enter the password of the host account. The password must be the same as the password that you specified in the " Step 1: Create a host account " section of this topic.

7. Grant the permissions on the imported hosts to the host accounts that you created.

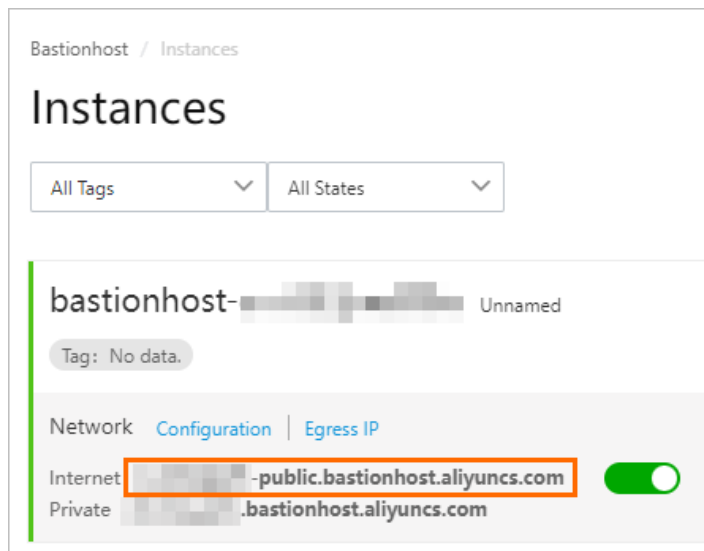
- i. Choose **Users > Users**, find the created bastion host user, and then click the username of the bastion host user to go to the **Basic Information** page.

- ii. Click the **Authorized Hosts** tab. Then, click **None. Authorize accounts** in the **Authorized accounts** column to grant permissions on the imported hosts to the host accounts that are created in **Step 6**.

Host IP Address	Hostname	Operating System	Network Domain	Authorized Accounts
<input type="checkbox"/> 172.17.227.93	rm-2ze68j253q1c46...	Windows	Direct Network	None. Authorize accounts
<input type="checkbox"/> 172.17.227.92	rm-2ze68j253q1c46...	Windows	Direct Network	None. Authorize accounts

Step 3: Connect to the hosts of the RDS instance and its secondary RDS instance in the Bastionhost console

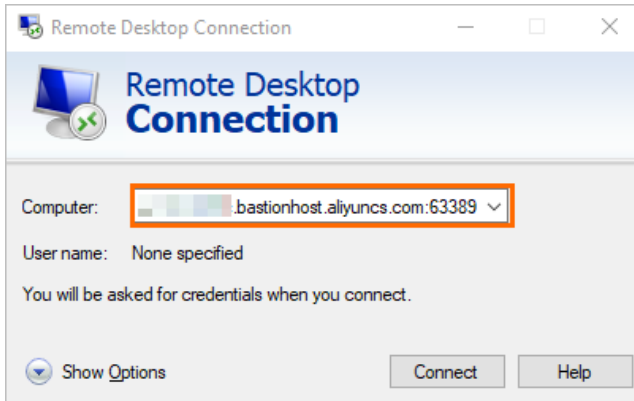
1. Log on to the **Bastionhost console**.
2. In the top navigation bar, select the region where the bastion host resides.
3. Obtain the public endpoint of the bastion host.



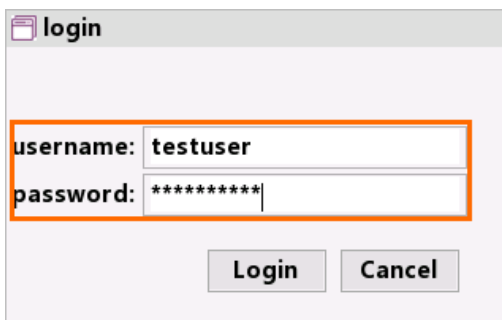
4. Log on to the bastion host.
 - o If you use a Windows operating system, perform the following operations:

- a. Open **Remote Desktop Connection**, enter the public endpoint and port number 63389 of the bastion host for the **Computer** parameter. The value of this parameter must be in the following format: `xxxx.bastionhost.aliyuncs.com:63389`.

Note You can press `Ctrl+Q` to open Remote Desktop Connection



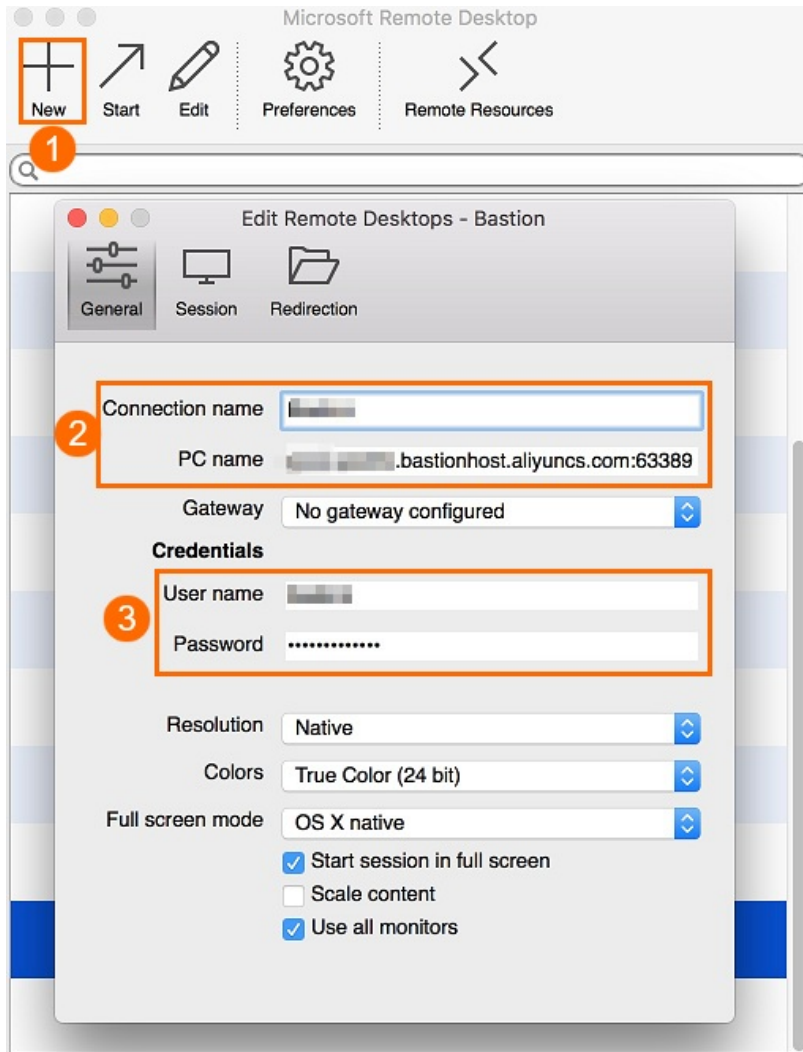
- b. Enter the username and password of the bastion host user.



Note The username and password must be the same as the username and password that you specified in the "Step 2: Configure a bastion host" section of this topic.

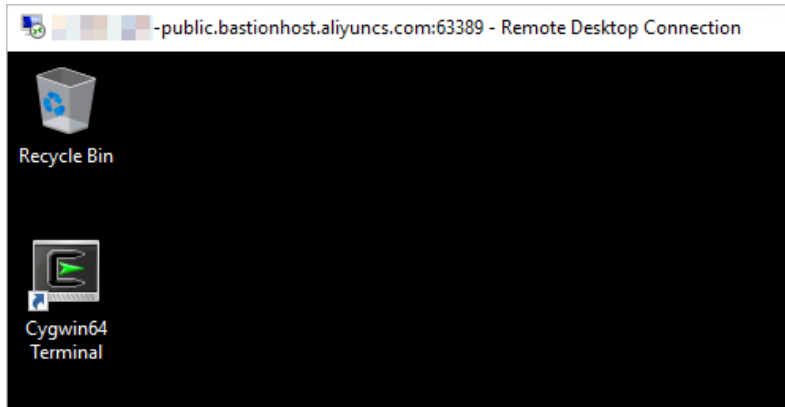
- o If you use a macOS operating system, perform the following operations:

We recommend that you use the **Microsoft Remote Desktop** tool to connect to the bastion host. You must configure the following parameters: **Connection name**, **PC name**, **User name**, and **Password**.



Parameter	Sample value	Description
Connection name	ServerHostConnection	The name of the connection. Enter a custom connection name.
PC name	xxxx.bastionhost.aliyuncs.com:63389	The public endpoint and port number of the bastion host.
User name and Password	User name: testuser	The username and password of the bastion host user. For more information, see the " Step 2: Configure a bastion host " section of this topic.

5. Double-click the host of the RDS instance or its secondary RDS instance. Then, the bastion host connects to the host.



14.10. System accounts of an ApsaraDB RDS for SQL Server instance

This topic describes the system accounts that are provided in an ApsaraDB RDS for SQL Server instance. In most cases, you do not need to manage the permissions and authorized operations of these system accounts.

Account	Description
<Hostname>\Administrator	The account that is used to locally manage the RDS instance. For example, you can use this account to reconfigure the parameters that are related to the database engine and query the status of the RDS instance.
<ul style="list-style-type: none"> aurora rds_service 	The accounts that are used to remotely manage the RDS instance. If the RDS instance is faulty, you can provide these accounts to an Alibaba Cloud engineer. The engineer can use these accounts to log on to and manage the RDS instance. For example, the engineer can perform a primary/secondary switchover and monitor the RDS instance.
<ul style="list-style-type: none"> sqlsa sa 	The default accounts that are provided with SQL Server. These accounts are disabled to prevent security risks.
<ul style="list-style-type: none"> rds_ha_sec_user rds_ag_sec_user 	The accounts that are used to replicate data from the RDS instance to its secondary RDS instance. These accounts are available only in RDS High-availability Edition and RDS Cluster Edition.

15.Database

15.1. Create a database on an ApsaraDB RDS for SQL Server instance

This topic describes how to create a database on an ApsaraDB RDS for SQL Server instance.

Prerequisites

[Create an ApsaraDB RDS for SQL Server instance](#)

Terms

- **Instance:** a virtualized database server, on which you can create and manage a number of databases.
- **Database:** a set of organized data that can be shared by a number of users. A database provides the minimal redundancy and is independent of applications. You can consider a database to be a warehouse that is used to store data.
- **Character set:** a collection of letters, special characters, and encoding rules that are used in a database.

Procedure

For more information, see the following topics:

- [Create accounts and databases for an ApsaraDB RDS instance that runs SQL Server 2017 EE or 2019 EE](#)
- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2012, 2014, 2016, 2017 SE, or 2019 SE](#)
- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2008 R2](#)

What to do next

[Connect to an ApsaraDB RDS for SQL Server instance.](#)

15.2. Delete a database from an ApsaraDB RDS for SQL Server instance

This topic describes how to delete a database from an ApsaraDB RDS for SQL Server instance. You can delete a database by using the ApsaraDB for RDS console or an SQL statement.

Delete a database by using the ApsaraDB for RDS console

- 1.
2. In the left-side navigation pane, click **Databases**.
3. In the **Actions** column click **Delete**.
4. In the message that appears, click **OK**.

Delete a database by using an SQL statement

1. Connect to the RDS instance to which the database belongs. For more information, see [Connect to an](#)

ApsaraDB RDS for SQL Server instance.

- Execute the following statement to delete the database:

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

Note If the RDS instance runs SQL Server 2012 or later on RDS High-availability Edition, run the following stored procedure. This stored procedure deletes the specified database, removes the associated image, and closes the connection to the database.

```
EXEC sp_rds_drop_database 'database name'
```

Related operations

Operation	Description
DeleteDatabase	Deletes a database from an ApsaraDB RDS instance.

15.3. Change the character set collation and time zone of system databases on an ApsaraDB RDS for SQL Server instance

This topic describes how to change the character set collation and time zone of system databases on an ApsaraDB RDS for SQL Server instance. ApsaraDB RDS provides four system databases: master, msdb, tempdb, and model.

Background information

- The default character set collation is Chinese_PRC_CI_AS.
- The default time zone is China Standard Time.

Note

- You can view the available character set collations and time zones in the ApsaraDB RDS console. For more information, see the "Procedure" section of this topic.
- To change the character set collation of a self-managed database, you can run the `alter database <The name of the self-managed database> collate <The character set collation that you want to use>` command.

Prerequisites

- Your RDS instance runs one of the following SQL Server versions:
 - SQL Server 2019
 - SQL Server 2017
 - SQL Server 2016

- SQL Server 2012
- SQL Server 2008 R2 with standard or enhanced SSDs (ESSDs)
- Your RDS instance does not belong to the **shared instance family** or a **dedicated cluster**. For more information, see [ApsaraDB RDS instance families](#).
- No user databases are created on your RDS instance. User databases are different from system databases.

Note If you have just deleted databases from your RDS instance, the deletion task may be pending on the secondary RDS instance. Before you can change the character set collation and time zone, make sure that neither your RDS instance nor its secondary RDS instance contains user databases. This prevents conflicts.

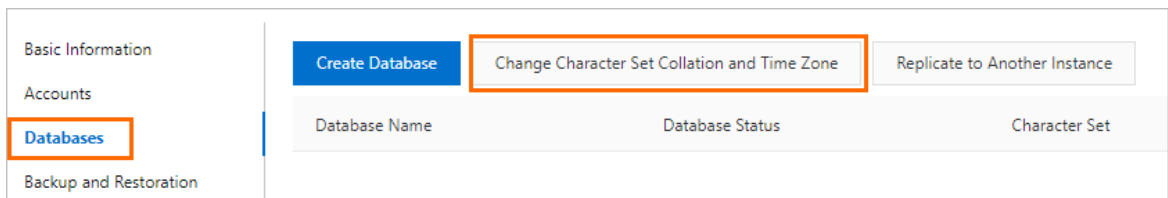
Precautions

When you change the character set collation and time zone of system databases on an RDS instance, the RDS instance is restarted. During the restart, the RDS instance is unavailable. It requires 2 minutes to 10 minutes to change the character set collation and about 1 minute to change the time zone.

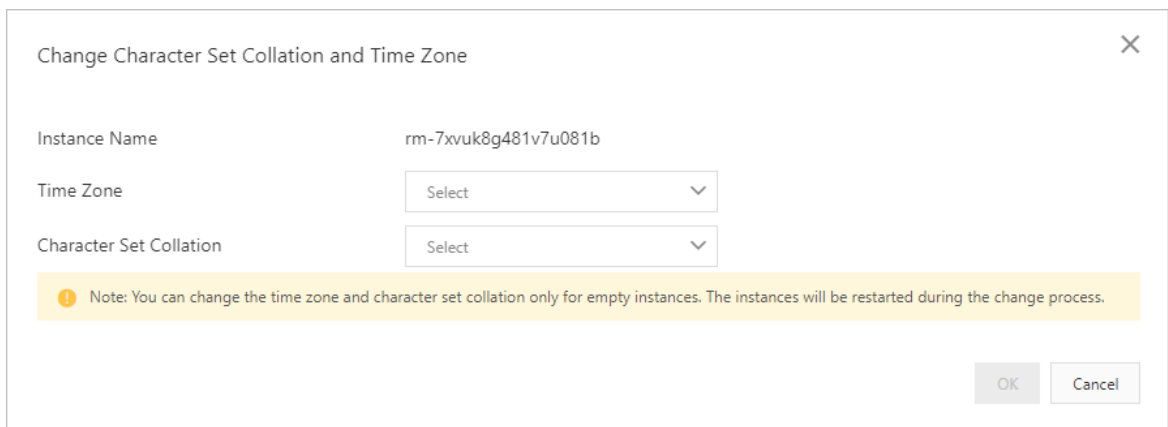
Procedure

- 1.
2. In the left-side navigation pane, click **Databases**.
3. On the **Databases** page, click **Change Character Set Collation and Time Zone**.

Note If you cannot find the Change Character Set Collation and Time Zone button, you must verify that your RDS instance meets the requirements that are described in the ["Prerequisites"](#) section of this topic.

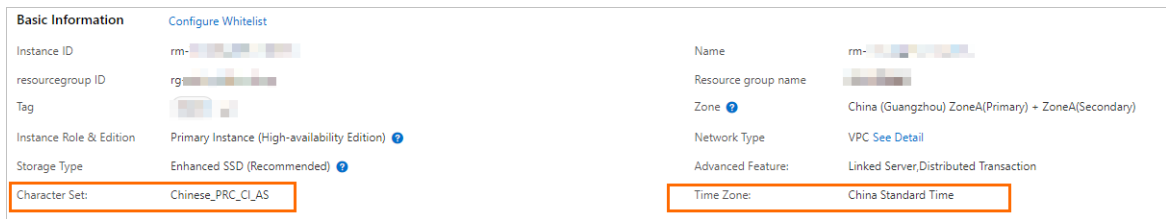


4. In the dialog box that appears, set the **Time Zone** and **Character Set Collation** parameters.



5. Then, click **OK**.

6. Go to the **Basic Information** page and view the new character set collation and time zone.



Time zones and UTC offsets

Time zone	UTC offset	Description
Afghanistan Standard Time	(UTC+04:30)	Kabul
Alaskan Standard Time	(UTC-09:00)	Alaska
Arabian Standard Time	(UTC+04:00)	Abu Dhabi, Muscat
Atlantic Standard Time	(UTC-04:00)	Atlantic Time (Canada)
AUS Central Standard Time	(UTC+09:30)	Darwin
AUS Eastern Standard Time	(UTC+10:00)	Canberra, Melbourne, Sydney
Belarus Standard Time	(UTC+03:00)	Minsk
Canada Central Standard Time	(UTC-06:00)	Saskatchewan
Cape Verde Standard Time	(UTC-01:00)	Cabo Verde Is.
Cen. Australia Standard Time	(UTC+09:30)	Adelaide
Central America Standard Time	(UTC-06:00)	Central America
Central Asia Standard Time	(UTC+06:00)	Astana
Central Brazilian Standard Time	(UTC-04:00)	Cuiaba
Central Europe Standard Time	(UTC+01:00)	Belgrade, Bratislava, Budapest, Ljubljana, Prague
Central European Standard Time	(UTC+01:00)	Sarajevo, Skopje, Warsaw, Zagreb
Central Pacific Standard Time	(UTC+11:00)	Solomon Islands, New Caledonia
Central Standard Time	(UTC-06:00)	Central Time (US and Canada)
Central Standard Time (Mexico)	(UTC-06:00)	Guadalajara, Mexico City, Monterrey
China Standard Time	(UTC+08:00)	Beijing, Chongqing, Hong Kong, Urumqi
E. Africa Standard Time	(UTC+03:00)	Nairobi

Time zone	UTC offset	Description
E. Australia Standard Time	(UTC+10:00)	Brisbane
E. Europe Standard Time	(UTC+02:00)	Chisinau
E. South America Standard Time	(UTC-03:00)	Brasilia
Eastern Standard Time	(UTC-05:00)	Eastern Time (US and Canada)
Georgian Standard Time	(UTC+04:00)	Tbilisi
GMT Standard Time	(UTC)	Dublin, Edinburgh, Lisbon, London
Greenland Standard Time	(UTC-03:00)	Greenland
Greenwich Standard Time	(UTC)	Monrovia, Reykjavik
GTB Standard Time	(UTC+02:00)	Athens, Bucharest
Hawaiian Standard Time	(UTC-10:00)	Hawaii
India Standard Time	(UTC+05:30)	Chennai, Kolkata, Mumbai, New Delhi
Jordan Standard Time	(UTC+02:00)	Amman
Korea Standard Time	(UTC+09:00)	Seoul
Middle East Standard Time	(UTC+02:00)	Beirut
Mountain Standard Time	(UTC-07:00)	Mountain Time (US and Canada)
Mountain Standard Time (Mexico)	(UTC-07:00)	Chihuahua, La Paz, Mazatlan
US Mountain Standard Time	(UTC-07:00)	Arizona
New Zealand Standard Time	(UTC+12:00)	Auckland, Wellington
Newfoundland Standard Time	(UTC-03:30)	Newfoundland
Pacific SA Standard Time	(UTC-03:00)	Santiago
Pacific Standard Time	(UTC-08:00)	Pacific Time (US and Canada)
Pacific Standard Time (Mexico)	(UTC-08:00)	Baja California
Russian Standard Time	(UTC+03:00)	Moscow, St. Petersburg, Volgograd
SA Pacific Standard Time	(UTC-05:00)	Bogota, Lima, Quito, Rio Branco
SE Asia Standard Time	(UTC+07:00)	Bangkok, Hanoi, Jakarta
China Standard Time	(UTC+08:00)	Kuala Lumpur, Singapore

Time zone	UTC offset	Description
Tokyo Standard Time	(UTC+09:00)	Osaka, Sapporo, Tokyo
US Eastern Standard Time	(UTC-05:00)	Indiana (East)
UTC	UTC	Coordinated Universal Time
UTC-02	(UTC-02:00)	Coordinated Universal Time-02
UTC-08	(UTC-08:00)	Coordinated Universal Time-08
UTC-09	(UTC-09:00)	Coordinated Universal Time-09
UTC-11	(UTC-11:00)	Coordinated Universal Time-11
UTC+12	(UTC+12:00)	Coordinated Universal Time+12
W. Australia Standard Time	(UTC+08:00)	Perth
W. Central Africa Standard Time	(UTC+01:00)	West Central Africa
W. Europe Standard Time	(UTC+01:00)	Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

15.4. Create and manage databases on an ApsaraDB RDS for SQL Server instance by using SQL statements


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

Prerequisites

The RDS instance runs SQL Server 2012 or later.

Create a database

Execute the following statement to create a database:

 **Note** When you create a database, do not specify a file path. ApsaraDB RDS generates a default file path.

```
CREATE DATABASE TestDb
```

Modify a database

You can modify most database attributes. Take note of the following points:

- Do not specify an invalid file path.

For example, specify an invalid 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:\mmmm\gggg\
].
Msg 3609, Level 16, State 2, Line 2
The transaction ended in the trigger. The batch has been aborted.
```

- Do not set the recovery model to a model other than FULL.

For example, set 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 change the database status to ONLINE when the database is in the OFFLINE state.

For example, change the database status from OFFLINE 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 want to change the database status from OFFLINE to ONLINE, you can use the `sp_rds_set_db_online` stored procedure. Execute the following statement:

```
EXEC sp_rds_set_db_online 'TestDb'
```

Delete a database

Execute the following statement to delete a database:

```
DROP DATABASE [TestDb]
```

If you have not backed up the database before deletion, the system displays the following error message:

```
DROP DATABASE [TestDb]
-----
-----
Kindly reminder:
  your database [TestDb] does not exist any backup set.
-----
-----
Login User [Test11] has dropped database [TestDb] .
```

15.5. Database replication

15.5.1. Replicate databases between ApsaraDB RDS for SQL Server instances

This topic describes how to replicate databases between ApsaraDB RDS instances that run SQL Server 2012 or SQL Server 2016 by using the ApsaraDB RDS console or API operations.

Prerequisites

The source and destination RDS instances meet the following requirements:

- The source and destination RDS instances belong to the same Alibaba Cloud account.
- The source and destination RDS instances run the same version of database engine. Supported database engine versions are SQL Server 2012 and SQL Server 2016.
- The source and destination RDS instances reside in the same region and use the same network type. Their zones can be different.
- The source and destination RDS instances do not have databases whose names are the same.
- The available storage capacity of the destination RDS instance is larger than the size of the databases that you want to replicate from the source RDS instance.

Context


During the replication process, ApsaraDB RDS first performs a full backup of the source RDS instance and then replicates databases to the destination RDS instance. If the source RDS instance is written during the replication process, incremental data of the source RDS instance is not replicated to the destination RDS instance.

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

Procedure

1. Go to the **Databases** page.

- i.
 - ii.
2. Click **Replicate to Another Instance**. In the dialog box that appears, configure the following parameters.

Parameter	Description
Source Instance Name	The ID of the source RDS instance.
Target Instance Name	The ID of the destination RDS instance. The drop-down list displays all the RDS instances that reside in the same region and use the same SQL Server version as the source RDS instance. You can select the destination RDS instance from the drop-down list.
Source Databases	<p>The databases that you want to replicate to the destination RDS instance. You can click the > or < icon to select the databases.</p> <p>If you select more than one database or all databases, make sure that the following conditions are met:</p> <ul style="list-style-type: none"> ◦ The available storage capacity of the destination RDS instance is larger than the size of the databases that you want to replicate from the source RDS instance. ◦ The source and destination RDS instances do not have databases whose names are the same. <div style="background-color: #e1f5fe; padding: 5px; margin-top: 10px;"> <p> Note If the source and destination RDS instances have databases whose names are the same, these databases are not replicated.</p> </div>

Parameter	Description
Users and Authorizations	<p>Specify whether to replicate accounts and account permissions to the destination RDS instance.</p> <ul style="list-style-type: none"> ○ Synchronize Database Users and Authorizations: Accounts and account permissions are replicated to the destination RDS instance. Take note of the following two scenarios: <ul style="list-style-type: none"> ■ If the destination RDS instance has accounts whose usernames are the same as those of accounts on the source RDS instance, the accounts on the destination RDS instance are granted the same permissions as the accounts on the source RDS instance. ■ If the destination RDS instance does not have the same accounts, the accounts are first created on the destination RDS instance and then granted the same permissions as the accounts on the source RDS instance. ○ Replicate Database Only. Do Not Synchronize Users and Authorizations: Accounts and account permissions are not replicated to the destination RDS instance. This option is the default value. After replication is complete, you can create accounts on the destination RDS instance and grant permissions on the selected databases. For more information, see Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2012, 2014, 2016, 2017 SE, or 2019 SE.


3. Click OK.

15.5.2. Replicate a database of an ApsaraDB RDS instance that runs SQL Server 2008 R2

If you want to create a database that is the same as an existing database, you can replicate the existing database. This topic describes how to replicate a database of an ApsaraDB RDS instance that runs SQL Server 2008 R2 in the ApsaraDB RDS console.

Prerequisites

The RDS instance runs SQL Server 2008 R2.

 **Note** If the RDS instance runs SQL Server 2012 or later, you can replicate its databases only by executing SQL statements. For more information, see [Replicate a database of an ApsaraDB RDS instance that runs SQL Server 2012 or later](#).

Precautions

- Only one database can be replicated at a time.
- The names of the new database and the existing database must be different.

Procedure

- 1.
2. In the left-side navigation pane, click **Databases**.


- 3. Click Copy Database.
- 4. In the dialog box that appears, configure parameters for the new database.

Parameter	Description
Enter a Database Name	Enter a name for the new database. The name can 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 a digit.
Select the Database to Copy	Select the database that you want to replicate.
Do You Want to Keep the Account Information from the Source Database	Specify whether to retain the account and account permissions of the existing database in the new database. By default, the account and account permissions are retained.
Description	Enter an informative description of the database. The description can be up to 256 characters in length.

- 5. Click OK.

15.5.3. Replicate a database of an ApsaraDB RDS instance that runs SQL Server 2012 or later

If you want to replicate a database of an ApsaraDB RDS instance that runs SQL Server 2012 or later, you must execute SQL statements and specify the existing and new databases by using the `sp_rds_copy_database` stored procedure. The time required for replication depends on the size of the existing database.

 **Note** For more information about how to replicate a database of an ApsaraDB RDS instance that runs SQL Server 2008 R2, see [Replicate a database of an ApsaraDB RDS instance that runs SQL Server 2008 R2](#).

Prerequisites

- The RDS instance runs SQL Server 2012 or later.
- The available storage capacity of the destination RDS instance is at least 1.3 times larger than the size of the existing database.

Procedure

Execute the following statements to replicate an existing database:

```
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')
```

16. Stored procedures

This topic describes the stored procedures that are supported by ApsaraDB RDS instances that run SQL Server 2012, SQL Server 2016, SQL Server 2017, and SQL Server 2019.

- [Replicate data between the databases of an RDS instance](#)
- [Set a database to the online mode](#)
- [Grant the permissions on some or all databases of an RDS instance to a user](#)
- [Delete a database](#)
- [Configure change tracking for a database](#)
- [Enable change data capture](#)
- [Disable change data capture](#)
- [Configure a parameter for an RDS instance](#)
- [Add a linked server to an RDS instance](#)
- [Configure a trace flag for an RDS instance](#)
- [Rename a database](#)

Replicate data between the databases of an RDS instance

T-SQL command:


```
sp_rds_copy_database
```

Instance configuration:

- RDS High-availability Edition
- RDS Basic Edition

Description:

This stored procedure is used to replicate the data of a source database to a specified destination database. The source database and the destination database are created on the same RDS instance.

 **Note** The available storage of the RDS instance must be at least 1.3 times the size of the source database.

Usage:

```
EXEC sp_rds_copy_database 'db', 'db_copy'
```

- The first parameter specifies the name of the source database.
- The second parameter specifies the name of the destination database.

Set a database to the online mode

T-SQL command:

```
sp_rds_set_db_online
```

Instance configuration:

- RDS High-availability Edition
- RDS Basic Edition

Description:

After you set a database to the offline mode, you cannot execute the ALTER DATABASE statement to set the database to the online mode. In this case, you can use this stored procedure to set the database to the online mode.

Usage:

```
EXEC sp_rds_set_db_online 'db'
```

The parameter specifies the name of the database that you want to set to the online mode.

Grant the permissions on some or all databases of an RDS instance to a user

T-SQL command:


```
sp_rds_set_all_db_privileges
```

Instance configuration:

- RDS High-availability Edition
- RDS Basic Edition

Description:

This stored procedure is used to grant the permissions on some or all databases of an RDS instance to a user.

 **Note** The permissions of the user on the specified databases must be higher than or equal to the permissions that you want to grant to the user.

Usage:

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

- The first parameter specifies the name of the user to whom you want to grant permissions.
- The second parameter specifies the database role that you want to grant to the user.
- The third parameter specifies the names of the databases whose permissions you want to grant to the user. You can enter one or more database names. If you enter more than one database name, you must separate the database names with commas (.). If you do not configure this parameter, all databases are specified.


Delete a database

T-SQL command:

```
sp_rds_drop_database
```

Instance configuration:

RDS High-availability Edition

 **Note** RDS Basic Edition does not support this stored procedure. If you want to delete a database from an RDS instance that runs RDS Basic Edition, you can execute the `DROP DATABASE db` statement.

Description:

This stored procedure is used to delete a database from an RDS instance. During the deletion process, ApsaraDB RDS deletes all objects that are associated with the database. If the RDS instance runs RDS High-availability Edition, ApsaraDB RDS also deletes the associated images and closes the connections to the database.

Usage:

```
EXEC sp_rds_drop_database 'db'
```

The parameter specifies the name of the database that you want to delete.

Configure change tracking for a database

T-SQL command:

```
sp_rds_change_tracking
```

Instance configuration:

RDS High-availability Edition

Description:

This stored procedure is used to configure change tracking for a database.

Usage:

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

- The first parameter specifies the name of the database for which you want to configure change tracking.
- The second parameter specifies whether to enable change tracking. Valid values:
 - 1: enables change tracking.
 - 0: disables change tracking.


Enable change data capture

T-SQL command:

```
sp_rds_cdc_enable_db
```

Instance configuration:

RDS High-availability Edition

 **Note** If you enable the Always On Availability Groups feature, we recommend that you disable change data capture.

Description:

This stored procedure is used to enable change data capture for a database.

Usage:

```
USE db
GO
sp_rds_cdc_enable_db
```


Disable change data capture

T-SQL command:

```
sp_rds_cdc_disable_db
```

Instance configuration:

RDS High-availability Edition

 **Note** If you enable the Always On Availability Groups feature, we recommend that you disable change data capture.

Description:

This stored procedure is used to disable change data capture for a database.

Usage:

```
USE db
GO
sp_rds_cdc_disable_db
```

Configure a parameter for an RDS instance

T-SQL command:

```
sp_rds_configure
```

Instance configuration:

- RDS High-availability Edition
- RDS Basic Edition

Description:

This stored procedure is used to configure a parameter for an RDS instance. If the RDS instance is provided with a secondary RDS instance as a standby, ApsaraDB RDS synchronizes the new parameter setting to the secondary RDS instance.

This stored procedure supports the following parameters:

- 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)

Usage:

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

- The first parameter specifies the name of the parameter that you want to configure.
- The second parameter specifies the value of the parameter.


Add a linked server to an RDS instance

T-SQL command:

```
sp_rds_add_linked_server
```

Instance configuration:

- SQL Server 2012 SE, SQL Server 2016 SE, SQL Server 2017 SE, and SQL Server 2019 SE Standard on RDS High-availability Edition (general-purpose instance family or dedicated instance family)
- SQL Server 2012 EE, and SQL Server 2016 EE on RDS High-availability Edition (general-purpose instance family or dedicated instance family)
- SQL Server 2017 EE and SQL Server 2019 EE on RDS Cluster Edition (general-purpose instance family or dedicated instance family)

 **Note** The shared instance family does not support this stored procedure. For more information, see [Primary instance types](#).

Description:

This stored procedure is used to add a linked server to an RDS instance. This stored procedure supports distributed transactions. After you add a linked server to the RDS instance, ApsaraDB RDS replicates the configuration of the linked server to the associated secondary RDS instance. This way, you do not need to add the linked server after a primary/secondary switchover.

Usage:


```
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
```

Configure a trace flag for an RDS instance

T-SQL command:

`sp_rds_dbcc_trace`

Instance configuration:

- RDS High-availability Edition
- RDS Basic Edition

Description:

This stored procedure is used to configure a trace flag for an RDS instance. This stored procedure supports only some trace flags. The trace flag that you have configured on the RDS instance is automatically replicated to the associated secondary RDS instance.

Usage:

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

- The first parameter specifies the trace flag that you want to configure for the RDS instance.
- The second parameter specifies whether to enable the trace flag. Valid values:
 - 1: enables the trace flag.
 - 0: disables the trace flag.

Rename a database

T-SQL command:

`sp_rds_modify_db_name`

Instance configuration:

- RDS High-availability Edition
- RDS Cluster Edition
- RDS Basic Edition

Description:

This stored procedure is used to rename a database. After you rename a database on an RDS instance that runs RDS High-availability Edition or RDS Cluster Edition, ApsaraDB RDS automatically rebuilds the replication configuration between the RDS instance and its secondary instance. During the rebuild process, the data of the RDS instance is backed up and restored. If the database occupies a large amount of storage space, make sure that the available storage space of the RDS instance is sufficient.

Usage:

```
EXEC sp_rds_modify_db_name 'db', 'new_db'
```

- The first parameter specifies the original name of the database.
- The second parameter specifies the new name of the database.

17. Monitoring and alerts


17.1. View the resource metrics and engine metrics of an ApsaraDB RDS for SQL Server instance

This topic describes how to view the resource metrics and engine metrics of an ApsaraDB RDS for SQL Server instance in the ApsaraDB RDS console.

Procedure

- 1.
2. In the left-side navigation pane, click **Monitoring and Alerts**.
3. On the **Standard Monitoring** tab, click **Resource Monitoring** or **Engine Monitoring** and specify a time range. Then, view the metrics that appear. The following table describes the metrics.

Monitoring type	Metric	Description
Resource Monitoring	Disk Space (MB)	<p>The disk usage of your RDS instance. The disk usage provides the following information:</p> <ul style="list-style-type: none"> ◦ Instance Size ◦ Data Usage ◦ Log Size ◦ Temporary File Size ◦ Other system file size <p>Unit: MB.</p>
	IOPS (Input/Output Operations per Second)	The number of input and output operations that are performed per second. Unit: times/second.
	Total Connections	The total number of connections that are established to your RDS instance.
	MSSQL Instance CPU Utilization (percentage in the operating system: %)	The CPU utilization of your RDS instance. The CPU utilization includes the CPU utilization for the operating system that is used.

Monitoring type	Metric	Description
	SQL Server Average Input/Output Traffic (KB/s)	<p>The inbound and outbound traffic of your RDS instance per second. Unit: KB.</p> <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e0f0ff;"> <p> Note To provide bandwidth usage that is more accurate, ApsaraDB RDS allows your RDS instance to collect traffic statistics from the network interface controllers of Windows operating systems. This is supported only when your RDS instance runs the RDS Basic Edition, High-availability Edition, or Cluster Edition in a Windows operating system.</p> </div>
Engine Monitoring	Average Transaction Frequency	The number of transactions that are processed per second.
	Average QPS	The number of SQL statements that are executed per second
	Buffer Hit Ratio (%)	The percentage of read queries that are hit in the buffer pool.
	Page Write Frequency at Check Point	The number of checkpoints that are written to pages per second.
	Login Frequency	The number of logons to your RDS instance per second.
	Average Frequency of Whole Table Scans	The number of full table scans that are performed per second.
	SQL Compilations per Second	The number of SQL statements that are compiled per second.
	Lock Timeout Times/s	The number of lock time-outs that occur per second.
	Deadlock Frequency	The number of deadlocks that occur per second.
	Lock Wait Frequency	The number of lock waits that occur per second.

17.2. Set the monitoring frequency of an ApsaraDB RDS for SQL Server instance


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

Context

ApsaraDB RDS for SQL Server provides the following monitoring frequencies:


- Every 10 Seconds
- Every 60 Seconds

- Every 300 Seconds

 **Note**

Procedure

- 1.
2. In the left-side navigation pane, click **Monitoring and Alerts**.

 **Note** For more information about the supported metrics, see [View the resource metrics and engine metrics of an ApsaraDB RDS for SQL Server instance](#).

3. Click the **Standard monitoring** tab.
4. Click **Set Monitoring Frequency**.
5. In the **Set Monitoring Frequency** dialog box, select a monitoring frequency and click **OK**.

17.3. Configure an alert rule for an ApsaraDB RDS for SQL Server instance

This topic describes how to configure an alert rule for an ApsaraDB RDS for SQL Server instance. ApsaraDB RDS offers the monitoring and alerting feature. If exceptions are detected on your RDS instance or if your RDS instance is locked due to low disk capacity, ApsaraDB RDS can send notifications to you.

Context

The monitoring and alerting feature of ApsaraDB RDS is implemented by using Cloud Monitor. Cloud Monitor allows you to configure metrics and alert rules. You can also associate alert groups with metrics. If a metric meets the conditions that are specified in an alert rule, alerts are sent as emails to all the contacts in the alert group that is associated with the metric.

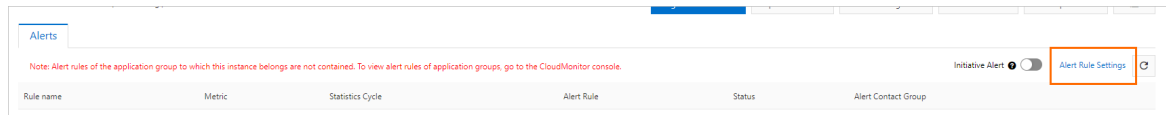
Enable the initiative alert feature

The initiative alert feature allows you to establish an alert system for multiple metrics in RDS. An alert notification is sent if an exception of a key metric occurs. You can then handle the exception at the earliest opportunity. For more information, see [Enable the initiative alert feature](#).

- 1.
2. In the left-side navigation pane, click **Monitoring and Alerts**.
3. Click the **Alerts** tab.
4. In the right-side section of the page, turn on the **Initiative Alert** switch.

Create an alert rule

- 1.
2. In the left-side navigation pane, click **Monitoring and Alerts**.
3. Click the **Alerts** tab.
4. Click **Set Alert Rule** to go to the Cloud Monitor console.

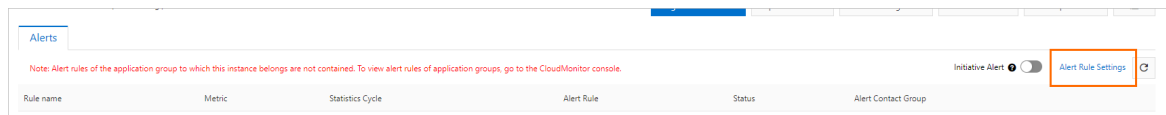


5. Create an alert group. For more information, see [Create an alert contact or alert contact group](#).
6. Create an alert rule. For more information, see [Create an alert rule](#).

Note You can also configure Cloud Monitor to automatically monitor resources based on tags. For more information, see [Monitor resources based on tags](#).

Manage an alert rule

- 1.
2. In the left-side navigation pane, click **Monitoring and Alerts**.
3. Click the **Alerts** tab.
4. Click **Set Alert Rule** to go to the Cloud Monitor console.



5. On the **Alert Rules** page, find the alert rule that you want to manage, and select one of the following operations in the Actions column:
 - View: View details about the alert rule.
 - Alert Logs: View the alerts that were triggered by the alert rule over a specific time range.
 - Modify: Modify the alert rule. For more information, see [Create an alert rule](#).
 - Disable: Disable the alert rule. After you disable the alert rule, no alerts are triggered even if the metric meets the conditions that are specified in the alert rule.
 - Delete: Delete the alert rule. After you delete the alert rule, the alert rule cannot be restored. You can only re-create the alert rule if necessary.

RDS SQL Server

18.Data security and encryption

18.1. Set a whitelist

18.1.1. Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance

This topic describes how to configure an IP address whitelist on an ApsaraDB RDS for SQL Server instance. An IP address whitelist allows only the specified devices to access your RDS instance.

For more information about how to configure an IP address whitelist for an RDS instance that runs a different database engine, see the following topics:

- [Configure an IP address whitelist for an ApsaraDB RDS for MySQL instance](#)
- [Configure an IP address whitelist for an ApsaraDB RDS for PostgreSQL instance](#)
- [Configure an IP address whitelist for an ApsaraDB RDS for MariaDB TX instance](#)

Scenarios

An IP address whitelist of an RDS instance consists of IP addresses and CIDR blocks that are granted access to the RDS instance. You can configure IP address whitelists for an RDS instance to provide high-level access control and security protection for the RDS instance. We recommend that you update the configured IP address whitelists on a regular basis.


You can configure an IP address whitelist in the following scenarios:

- **Scenario 1**
After an RDS instance is created, you must add the IP addresses of specific devices to an IP address whitelist of the RDS instance. These devices can access the RDS instance only after the IP addresses of these devices are added to an IP address whitelist of the RDS instance.
- **Scenario 2**
An RDS instance cannot be connected. You must check whether the IP address whitelists of the instance are correctly configured.

The following table provides the IP address whitelist configurations in various connection scenarios.

Note A virtual private cloud (VPC) is an isolated network on Alibaba Cloud and provides higher security than the classic network. For more information, see [What is a VPC?](#)

Connection scenario	Network type	IP address whitelist configuration
---------------------	--------------	------------------------------------

Connection scenario	Network type	IP address whitelist configuration
Connect an Elastic Compute Service (ECS) instance to an RDS instance	The ECS instance and the RDS instance reside in the same VPC. This is the recommended connection scenario.	Add the private IP address of the ECS instance to an IP address whitelist of the RDS instance.
	The ECS instance and the RDS instance reside in different VPCs.	Instances in different VPCs cannot communicate with each other over internal networks. Make sure that the ECS instance and the RDS instance reside in the same VPC and add the private IP address of the ECS instance to an IP address whitelist of the RDS instance.
	The ECS instance and the RDS instance reside in the classic network.	Add the private IP address of the ECS instance to an IP address whitelist of the RDS instance.
	<p>The ECS instance resides in the classic network.</p> <p>The RDS instance resides in a VPC.</p>	<p>Instances of different network types cannot communicate with each other over internal networks. Perform the following operations:</p> <ol style="list-style-type: none"> i. Migrate the ECS instance from the classic network to the VPC to which the RDS instance belongs. For more information, see Migrate an ECS instance from the classic network to a VPC. <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 10px; margin: 10px 0;"> <p> Note This operation is supported only when the ECS instance and the RDS instance reside in the same region. If the ECS instance and the RDS instance reside in different regions, we recommend that you use Data Transmission Service (DTS) to migrate the RDS instance to the region where the ECS instance resides. This way, you can ensure the stability of your database service. For more information, see Migrate data between ApsaraDB RDS for SQL Server instances.</p> </div> <ol style="list-style-type: none"> ii. Add the private IP address of the ECS instance to an IP address whitelist of the RDS instance.

Connection scenario	Network type	IP address whitelist configuration
	<p>The ECS instance resides in a VPC.</p> <p>The RDS instance resides in the classic network.</p>	<p>Instances of different network types cannot communicate with each other over internal networks. Perform the following operations:</p> <ol style="list-style-type: none"> i. Migrate the RDS instance from the classic network to the VPC to which the ECS instance belongs. For more information, see Change the network type of an ApsaraDB RDS for SQL Server instance. <div style="background-color: #e1f5fe; padding: 10px; margin: 10px 0;"> <p>Note This operation is supported only when the ECS instance and the RDS instance reside in the same region. If the ECS instance and the RDS instance reside in different regions, we recommend that you use DTS to migrate the RDS instance to the region where the ECS instance resides. This way, you can ensure the stability of your database service. For more information, see Migrate data between ApsaraDB RDS for SQL Server instances.</p> </div> <ol style="list-style-type: none"> ii. Add the private IP address of the ECS instance to an IP address whitelist of the RDS instance.
<p>Connect a self-managed host outside the cloud to an RDS instance</p>	<p>None</p>	<p>Add the public IP address of the self-managed host to an IP address whitelist of the RDS instance.</p> <div style="background-color: #e1f5fe; padding: 10px; margin: 10px 0;"> <p>Note</p> <ul style="list-style-type: none"> ○ The applications that run on the self-managed host connect to the public endpoint of the RDS instance. ○ For more information about how to obtain the public IP address of the self-managed host, see How SQL Server determines the public IP address of an external Server or client </div>

Procedure


What to do next

- [Create accounts and databases for an ApsaraDB RDS instance that runs SQL Server 2017 EE or 2019 EE](#)
- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2012, 2014, 2016, 2017 SE, or 2019 SE](#)
- [Create an account and a database for an ApsaraDB RDS instance that runs SQL Server 2008 R2](#)

18.1.2. Errors and FAQ about IP address whitelist settings in ApsaraDB RDS for SQL Server

This topic describes the common errors and provides answers to some commonly asked questions about the IP address whitelist settings of an ApsaraDB RDS for SQL Server instance.

Common errors

Error	Description	Solution
No IP address whitelists are configured. Your RDS instance has only one default IP address whitelist. The default IP address whitelist contains only the 127.0.0.1 IP address.	The 127.0.0.1 IP address indicates that no devices can access your RDS instance.	Add the IP addresses of the specified devices to an IP address whitelist.
The 0.0.0.0 entry is added to an IP address whitelist during a connectivity test.	The format of the 0.0.0.0 entry is invalid.	Change the 0.0.0.0 IP address to the 0.0.0.0/0 Classless Inter-Domain Routing (CIDR) block. <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Notice The 0.0.0.0/0 CIDR block indicates that all IP addresses are granted access to your RDS instance. We recommend that you add this CIDR block only for a connectivity test. When you run online workloads, do not add this CIDR block to an IP address whitelist.</p> </div>
The public IP addresses in a configured IP address whitelist are inaccessible.	<ul style="list-style-type: none"> The public IP addresses dynamically change. The tool or website that you use to query public IP addresses returns inaccurate results. 	For more information, see How SQL Server determines the public IP address of an external Server or client .

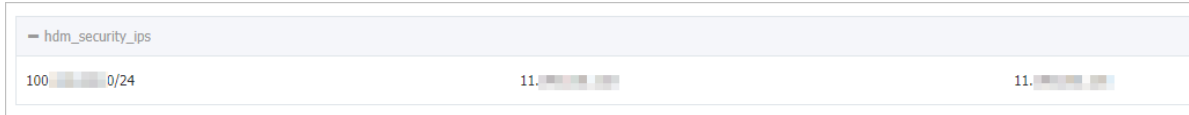
FAQ

- After I configure an IP address whitelist for my RDS instance, does the IP address whitelist immediately take effect?

After you configure an IP address whitelist for your RDS instance, the IP address whitelist requires about 1 minute to take effect.

- What are the IP address whitelists labeled `ali_dms_group` and `hdm_security_ips`?

When you connect to your RDS instance from other Alibaba Cloud services, these services generate IP address whitelists upon your authorization. The generated IP address whitelists contain the IP addresses of the servers on which these services run. The IP address whitelist labeled `ali_dms_group` is generated by [Data Management \(DMS\)](#). The IP address whitelist labeled `hdm_security_ips` is generated by Database Autonomy Service (DAS). Do not modify or delete the IP address whitelists. If you modify or delete the IP address whitelists, these services cannot access your RDS instance. These services do not perform operations on your business data.




- If I disable Internet access and enable only internal network access, is my RDS instance exposed to security risks? We recommend that you migrate your RDS instance to a virtual private cloud (VPC). For more information, see [Change the network type of an ApsaraDB RDS for SQL Server instance](#).

18.2. Configure SSL encryption on an ApsaraDB RDS for SQL Server instance

This topic describes how to configure Secure Sockets Layer (SSL) encryption on your ApsaraDB RDS for SQL Server instance. You must enable SSL encryption on your RDS instance and install the SSL certificates issued by certificate authorities (CAs) on your application. SSL is used at the transport layer to encrypt network connections. This allows you to enhance the security and integrity of the transmitted data. However, SSL increases the response time.

Context

SSL is developed by Netscape to provide encrypted communication between a web server and a browser. SSL supports various encryption algorithms, such as RC4, MD5, and RSA. The Internet Engineering Task Force (IETF) upgrades SSL 3.0 to TLS. However, the term "SSL encryption" is retained because it is more common in the communications industry. In this topic, SSL encryption refers to TLS encryption.


 **Note** ApsaraDB RDS supports TLS 1.0, 1.1, and 1.2.

Precautions

- An SSL certificate remains valid for one year. Before the used SSL certificate expires, you must update its validity period. In addition, you must download the required SSL certificate file and configure the SSL certificate again. Otherwise, clients cannot connect to your RDS instance over an encrypted connection.
- SSL encryption may cause a significant increase in CPU utilization. We recommend that you enable SSL encryption only when you want to encrypt the connections with the public endpoint of your RDS instance. In most cases, connections with the internal endpoint of your RDS instance are secure and do not require SSL encryption.
- SSL encryption cannot be disabled after it is enabled. Proceed with caution.
- SSL encryption is not supported for the connections with the read/write splitting endpoint of your RDS instance.

Enable SSL encryption

- 1.
2. In the left-side navigation pane, click **Data Security**.
3. Click the **SSL Encryption** tab.

 **Note** If the SSL Encryption tab cannot be found, you must check whether the RDS instance meets all requirements that are described in the "Prerequisites" section of this topic.

4. In the SSL Settings section, turn on **SSL Encryption**.

5. In the dialog box that appears, select the endpoint that you want to protect and click **OK**.

Note You can encrypt the link to the internal or public endpoint based on your business requirements. You can encrypt only one link.

6. Click **Download CA Certificate** to download the SSL certificate files as a compressed package.

The downloaded package contains the following files:

- o P7B file: the SSL certificate file that is used for a Windows operating system
- o PEM file: the SSL certificate file that is used for an operating system other than Windows or an application that is not run on Windows
- o JKS file: the SSL certificate file that is stored in the Java-supported trust store. You can use this file to import the SSL certificate files from an SSL certificate chain into Java-based applications. The default password is `apsaradb`.

Note When you use the JKS file in JDK 7 or JDK 8, you must modify the following default JDK security configuration items in the `jre/lib/security/Java.security` file on the host on which your application resides:

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

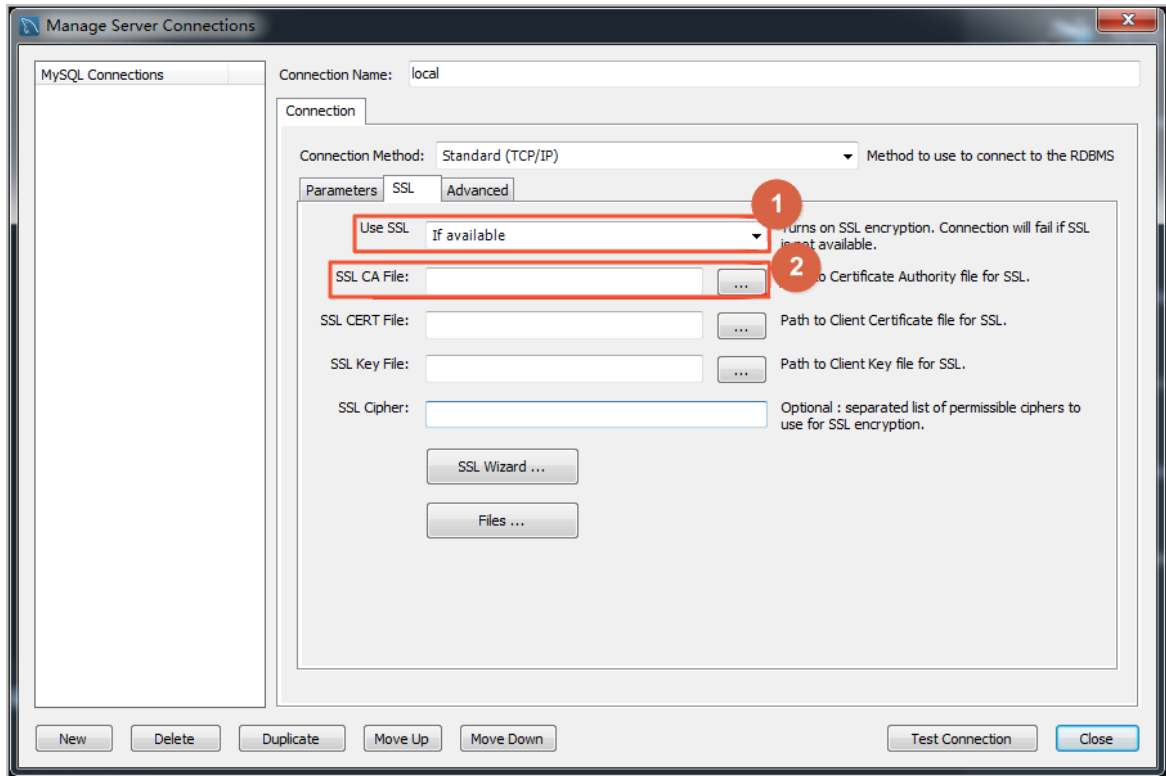
If you do not modify these configurations, the following error is returned. In most cases, similar errors are caused by invalid Java security configurations.

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

Configure an SSL certificate

Before your application or client can connect to your RDS instance, you must configure an SSL certificate on your application or client after you enable SSL encryption. In this section, MySQL Workbench is used as an example. If you use other applications or clients, see the related instructions.

1. Start MySQL Workbench.
2. Choose **Database > Manage Connections**.
3. Enable **Use SSL** and import the required SSL certificate file.

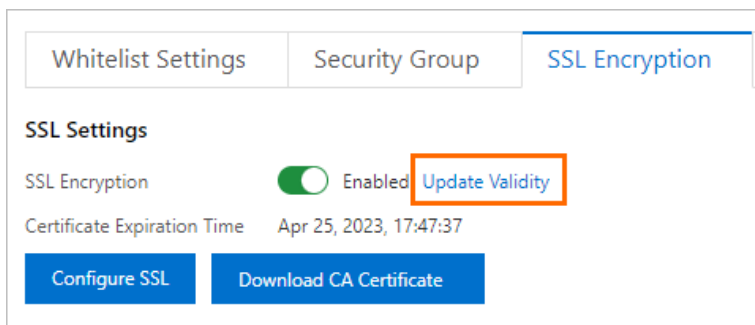


Update the validity period of an SSL certificate

Note

- The **Update Validity** operation causes your RDS instance to restart. Proceed with caution.
- After you perform the **Update Validity** operation, you must download the SSL certificate file and configure the SSL certificate again.

- 1.
2. In the left-side navigation pane, click **Data Security**.
3. On the page that appears, click the **SSL Encryption** tab. Then, click **Update Validity**.



Notice The Update Validity operation causes your RDS instance to restart. We recommend that you update the validity period during off-peak hours.

18.3. Configure TDE for an ApsaraDB RDS for SQL Server instance


This topic describes how to configure Transparent Data Encryption (TDE) for an ApsaraDB RDS for SQL Server instance. TDE can perform real-time I/O encryption and decryption on data files. Data is encrypted before it is written to a disk. Data is also decrypted when it is read from a disk and written to the memory. After TDE is enabled, the size of data files does not increase. You can use TDE without the need to modify the connected application.

Prerequisites

- Your RDS instance runs SQL Server 2019 SE or an Enterprise Edition of SQL Server.
- Your RDS instance is not a read-only instance. For more information, see [Create a read-only ApsaraDB RDS for SQL Server instance](#).
- If you want to use Bring Your Own Keys (BYOKs), the certificate, private key, and password that are used for encryption and decryption are obtained.

Precautions


- TDE cannot be disabled after it is enabled for an RDS instance. TDE can be disabled after it is enabled for a database.
- If you use Key Management Service (KMS) to generate a key after you enable TDE on an RDS instance, you must disable TDE for the RDS instance before you can restore the data of the RDS instance to a self-managed database. For more information, see the "[Disable TDE](#)" section of this topic.

 **Note** After you disable TDE, some transaction logs are still encrypted. The backup files that are downloaded cannot be used to restore the data of the RDS instance. You can wait until three log backups and one full backup are complete on the RDS instance. Then, you can download the most recent full backup file that is generated. This full backup file contains the decrypted data of the RDS instance. For more information, see [Database Encryption in SQL Server 2008 Enterprise Edition](#). For more information about how to configure a backup policy, see [Back up an ApsaraDB RDS for SQL Server instance](#).

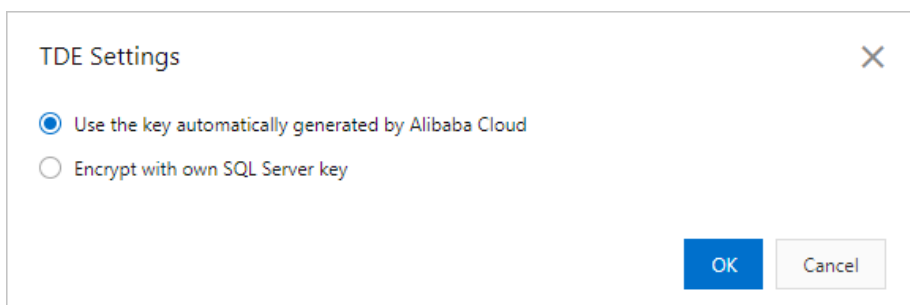
- After you enable TDE for an RDS instance, the CPU utilization of the RDS instance significantly increases.

Enable TDE

- 1.
2. In the left-side navigation pane, click **Data Security**.
3. On the **TDE** tab, turn on the switch next to **TDE Status**.

 **Note** You can enable TDE only when the RDS instance meets the requirements that are described in the "Prerequisites" section of this topic.

4. Select a key.

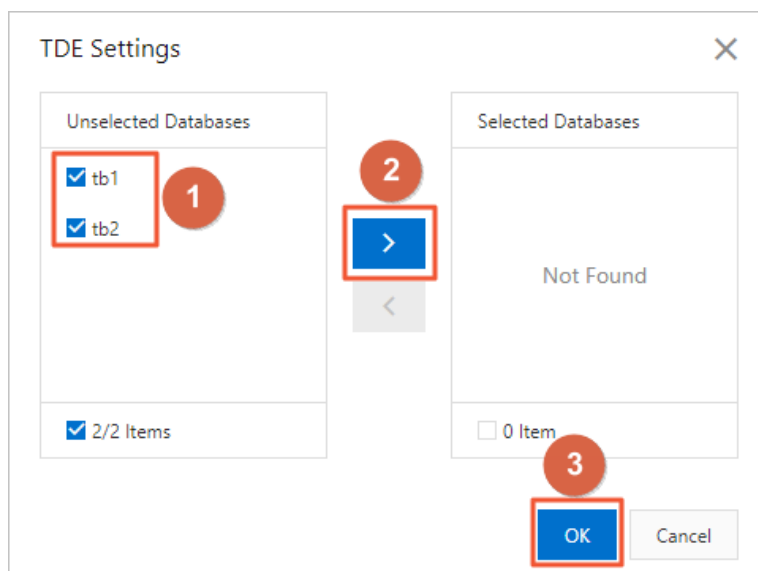


- o If you select the Use a key automatically generated by Alibaba Cloud option, perform the following operations:

In the TDE Settings dialog box, select databases from the Unselected Databases section, click the

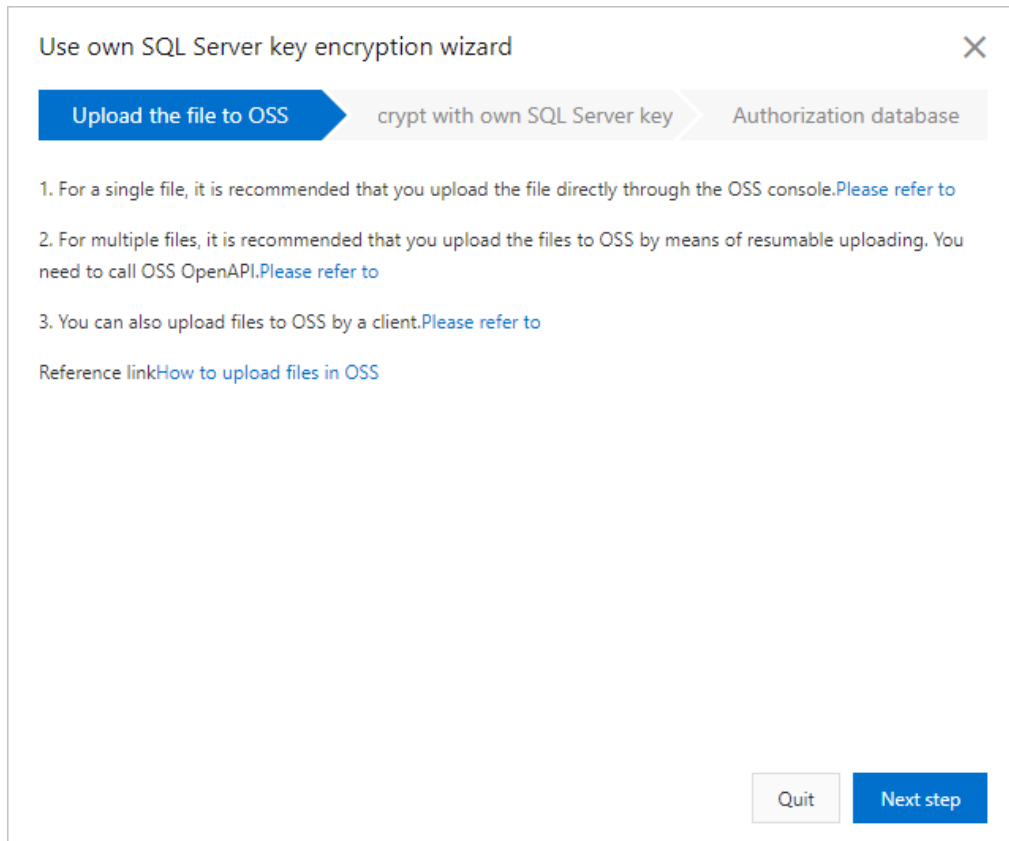


icon to move the selected databases to the Selected Databases section, and then click **OK**.



- o If you select the Encrypt with own SQL Server key option, perform the following operations:

- a. Upload the certificate file and the private key file to your OSS bucket. For more information, see [Upload objects](#).



b. Click **Next** and configure the parameters related to the key.

✕

Use own SQL Server key encryption wizard

Upload the file to OSS
crypt with own SQL Server key
Authorization database

* OSS Bucket

* Certificate

* Private key

* Password

You have authorized the RDS service account to access your OSS permissions.

Quit
Previous
Next step

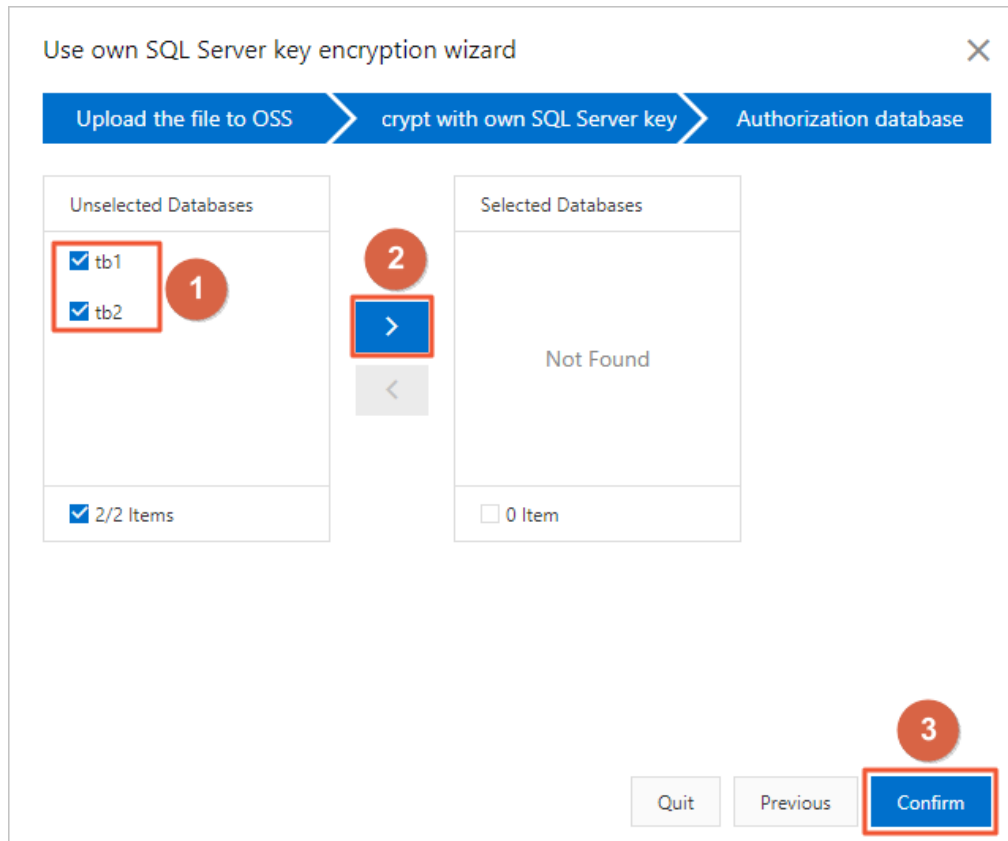
Parameter	Description
OSS Bucket	The OSS bucket in which the certificate file and the private key file are stored.
Certificate	The certificate file that you uploaded to the OSS bucket.
Private key	The private key file that you uploaded to the OSS bucket.
Password	The password of your own SQL Server key.

- c. Click **Next** to go to the **Authorization Database** page.

Select databases from the **Unselected Databases** section, click the




icon to move the selected databases to the **Selected Databases** section, and then click **OK**.



Disable TDE

After TDE is enabled for an RDS instance, TDE cannot be disabled. To disable TDE for a database, you can remove the database from the **Selected Databases** section.

- 1.
2. In the left-side navigation pane, click **Data Security**.
3. Click the **TDE** tab in the upper section of the page. Then, click **TDE Settings** on the TDE tab.
4. In the TDE Settings dialog box, select databases from the **Selected Databases** section, click the  icon to move the selected databases to the **Unselected Databases** section, and then click **OK**.

Note After you disable TDE, some transaction logs are still encrypted. The backup files that are downloaded cannot be used to restore the data of the RDS instance. You can wait until three log backups and one full backup are complete on the RDS instance. Then, you can download the most recent full backup file that is generated. This full backup file contains the decrypted data of the RDS instance. For more information, see [Database Encryption in SQL Server 2008 Enterprise Edition](#). For more information about how to configure a backup policy, see [Back up an ApsaraDB RDS for SQL Server instance](#).

18.4. Configure a distributed transaction whitelist for an ApsaraDB RDS for SQL Server instance

Distributed transaction whitelists allow for distributed transactions between an Elastic Compute Service (ECS) instance and an ApsaraDB RDS for SQL Server instance.


For more information about the related best practices, see [Connect Kingdee K/3 WISE to ApsaraDB RDS for SQL Server](#).

Prerequisites

The RDS instance runs one of the following SQL Server versions on RDS High-Availability Edition: 2012 SE, 2012 EE, 2014 SE, 2016 SE, 2016 EE, and 2017 SE.

Configure the RDS instance

- 1.
2. In the left-side navigation pane, click **Data Security**.
3. On the **Whitelist Settings** tab, select a whitelist and click **Edit** to the right. In the dialog box that appears, enter the IP address of the ECS instance.

 **Note**

- If the ECS and RDS instances reside in the same VPC, you must enter the private IP address of the ECS instance. You can view the private IP address of the ECS instance on the **Instance Details** page of the ECS instance in the ECS console.
- If the ECS and RDS instances reside in different VPCs, you must enter the public IP address of the ECS instance. In addition, you must apply for a public endpoint for the RDS instance. For more information, see [Apply for a public endpoint for an RDS SQL Server instance](#).

4. Click **Add**.
5. Click the **Whitelist for Distributed Transaction** tab.
6. Click **Create Whitelist**.
7. Configure the following parameters.

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

Parameter	Description
Whitelist	<p>Enter the IP address of the ECS instance and the name of the Windows-based computer where the ECS instance resides. Make sure that you separate the IP address and the computer name with a comma (,). Example: 192.168.1.100,k3ecstest.</p> <p>If you want to enter more than one entry, make sure that each entry is in a different line.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p>? Note You can view the computer name by choosing Control Panel > System and Security > System on your computer.</p> </div>

✕

Create ECS Whitelist for Distributed Transaction

Group Name:

Whitelist:

192.168.1.100,k3ecstest

You can add 30 more entries.

8. Click **OK**.

Configure the ECS instance

1. Log on to the [ECS console](#).
2. In the left-side navigation pane, choose **Instances & Images > Instances**.
3. In the top navigation bar, select the region where the target ECS instance resides.
4. Find the target ECS instance and click its instance ID.
5. In the left-side navigation pane, click **Security Groups**.
6. Find the target security group and in the Actions column and click **Add Rules**.
7. On the **Inbound** tab, click **Add Security Group Rule**.
8. Configure the following parameters.

Parameter	Description
Action	Select Allow .
Priority	Retain the default value 1.

Parameter	Description
Protocol Type	Select Custom TCP .
Port Range	Enter 135. <div style="border: 1px solid #ccc; background-color: #e0f2f1; padding: 5px; margin: 5px 0;"> ? Note Port 135 is the fixed port for the RPC service. </div>
Authorization Object	<p>The two IP addresses of the RDS instance. To obtain these IP addresses, perform the following steps: Log on to the ApsaraDB for RDS console and navigate to the Whitelist for Distributed Transaction tab of the Data Security page for the RDS instance.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <div style="display: flex; justify-content: space-between; border-bottom: 1px solid #ccc; margin-bottom: 5px;"> Whitelist Settings SQL Audit SSL Encryption Whitelist for Distributed Transaction </div> <p>RDS Instance Details:</p> <p>172.17.0.10:3306</p> <p>172.17.0.11:3306</p> </div>
Description	Enter the description of the security group rule. The description must be 2 to 256 characters in length and cannot start with <code>http://</code> or <code>https://</code> .

9. Click **OK**.
10. Add another security group rule. This rule has the same parameter settings as the previous rule except the **Port Range** parameter that is set to 1024/65535.

18.5. Enable or disable the release protection feature for an ApsaraDB RDS for SQL Server instance

If your ApsaraDB RDS for SQL Server instance uses the pay-as-you-go billing method and runs critical workloads, you can enable the release protection feature for the instance. This feature prevents your RDS instance from being manually released due to unintended operations or lack of communication among team members. This topic describes how to enable or disable the release protection feature for an ApsaraDB RDS for SQL Server instance.

Prerequisites

The RDS instance uses the pay-as-you-go billing method.

Precautions

The release protection feature cannot prevent the automatic release of RDS instances in normal scenarios such as the following scenarios:

- A payment in your account is overdue for more than 15 days.
- The RDS instance does not comply with the applicable security compliance policies.

Benefits of release protection


If you release an RDS instance for which the release protection feature is enabled, the following result is returned:

- If you release the RDS instance in the ApsaraDB RDS console, the "The instance cannot be released because release protection has been enabled. Disable release protection first" message is displayed.
- If you call the `DeleteDBInstance` operation to release the RDS instance, the error code `OperationDenied.DeletionProtection` is returned.

Enable the release protection feature when you create an RDS instance

This section describes how to configure the release protection feature when you create an RDS instance. For more information, see [Create an ApsaraDB RDS for SQL Server instance](#).


- 1.
2. On the **Instances** page, click **Create Instance**.
3. In the **Basic Configurations** step, set **Billing Method** to **Pay-As-You-Go** and complete the remaining configurations. Click **Next: Instance Configuration**.
4. In the **Instance Configurations** step, select **Prevent release through the console or API by mistake** and complete the remaining configurations. Click **Next: Confirm Order**.
5. Complete the remaining configurations until the RDS instance is created.

 **Note** When you can call the `CreateDBInstance` or `CloneDBInstance` operation to create an RDS instance, you can enable or disable the release protection feature for the RDS instance by setting the `DeletionProtection` parameter.

Modify release protection settings

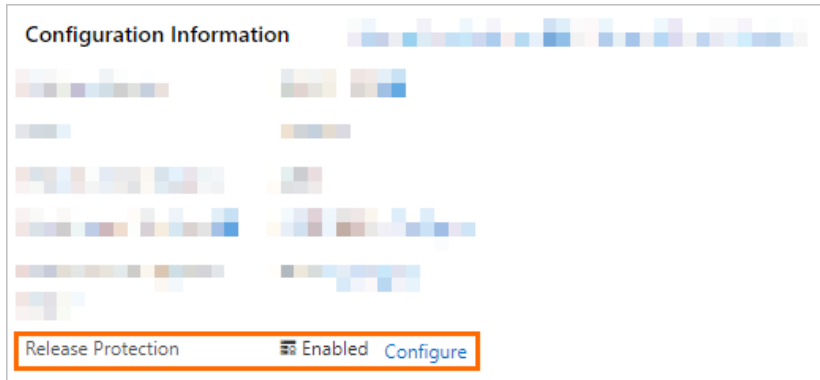
You can also enable or disable the release protection feature for an RDS instance by modifying the settings of the RDS instance.

- 1.
2. On the **Instances** page, find the RDS instance whose release protection settings you want to modify. In the **Actions** column, click **More** and select **Change Instance Release Protection Settings**.
3. In the **Change Release Protection Setting** dialog box, turn on or turn off **Release Protection**.
4. Click **OK**.

 **Note** You can also call the `ModifyDBInstanceDeletionProtection` operation to enable or disable the release protection feature for an RDS instance.

Check whether the release protection feature is enabled

- 1.
2. On the **Basic Information** page, view the **Release Protection** section of the **Configuration Information** section.



Related operations

Operation	Description
Create an instance	Creates an ApsaraDB RDS instance.
Restore data to a new ApsaraDB RDS instance	Restores the data of an ApsaraDB RDS instance to a new instance. The new instance is also called a cloned instance.
Enable or disable the release protection feature	Enables or disables the release protection feature for an ApsaraDB RDS instance.

18.6. Configure disk encryption for an ApsaraDB RDS for SQL Server instance

This topic describes how to configure disk encryption for an ApsaraDB RDS for SQL Server instance that uses standard SSDs or enhanced SSDs (ESSDs). The disk encryption feature provides maximum protection for your data and relieves the need to modify business or application configurations.

Introduction

ApsaraDB RDS provides the disk encryption feature for free for RDS instances that use standard SSDs or ESSDs. After you enable this feature for your RDS instance, this feature encrypts the entire data disks of your RDS instance based on block storage. This way, your data cannot be deciphered even if it is leaked. Disk encryption does not interrupt your workloads. In addition, you do not need to modify your application configurations.

Prerequisites

- Your RDS instance does not belong to the shared instance family. For more information, see [ApsaraDB RDS instance families](#).
- Your RDS instance is being created. After your RDS instance is created, you cannot enable the disk encryption feature.
- The Standard SSD or Enhanced SSD storage type is selected when you are creating your RDS instance. For more information, see [Storage types](#).

Billing rules

The disk encryption feature is free of charge. You are not charged for the read and write operations that you perform on the encrypted disks.

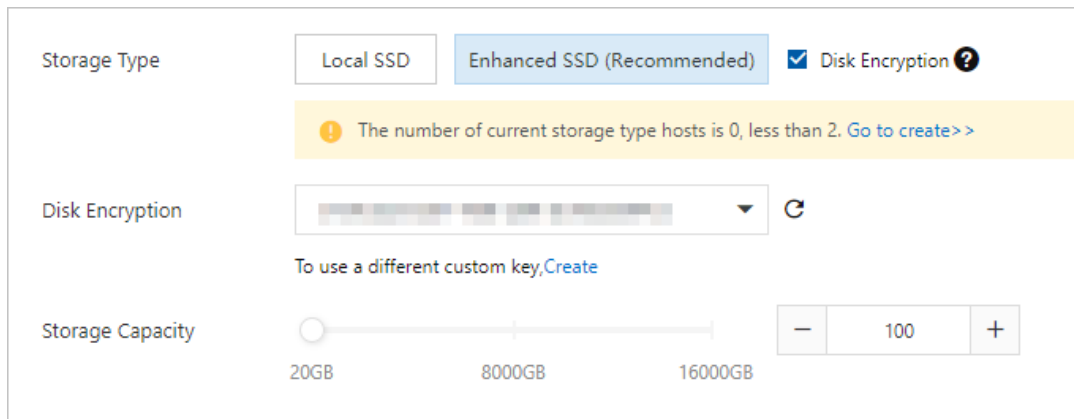
Precautions

- The disk encryption feature cannot be disabled after it is enabled.
- If you enable the disk encryption feature for your RDS instance, your RDS instance does not support cross-region backups. For more information, see [Enable cross-region backups for an ApsaraDB RDS for SQL Server instance](#).
- Disk encryption does not interrupt your workloads. In addition, you do not need to modify your application configurations.
- If you enable the disk encryption feature for your RDS instance, the snapshots that are created for the instance are automatically encrypted. In addition, if you use the encrypted snapshots to create an RDS instance that uses standard SSDs or ESSDs, the disk encryption feature is automatically enabled for the new RDS instance.
- If your Key Management Service (KMS) is overdue, the standard SSDs or ESSDs of your RDS instance become unavailable. Make sure that your KMS is normal. For more information, see [What is KMS?](#)
- If you disable or delete the CMK that is used for disk encryption, your RDS instance cannot run as normal. For example, you cannot create snapshots, restore data from snapshots, or rebuild the secondary RDS instance of your RDS instance.

Procedure

When you create an RDS instance, select the **Standard SSD** or **Enhanced SSD** storage type, select the **Disk Encryption** option to the right of the selected storage type, and then select a key that is used for encryption. For more information, see [Create an ApsaraDB RDS for SQL Server instance](#).

Note For information about how to create a key, see [Create a CMK](#).



19.Audit

19.1. Use the SQL Audit feature on an ApsaraDB RDS for SQL Server instance

This topic describes how to use the SQL Audit feature on an ApsaraDB RDS for SQL Server instance. You can use the SQL Audit feature to view the details about the SQL statements that are executed on your RDS instance and audit the SQL statements on a regular basis. After you enable the SQL Audit feature, the performance of your RDS instance is not affected.

Precautions

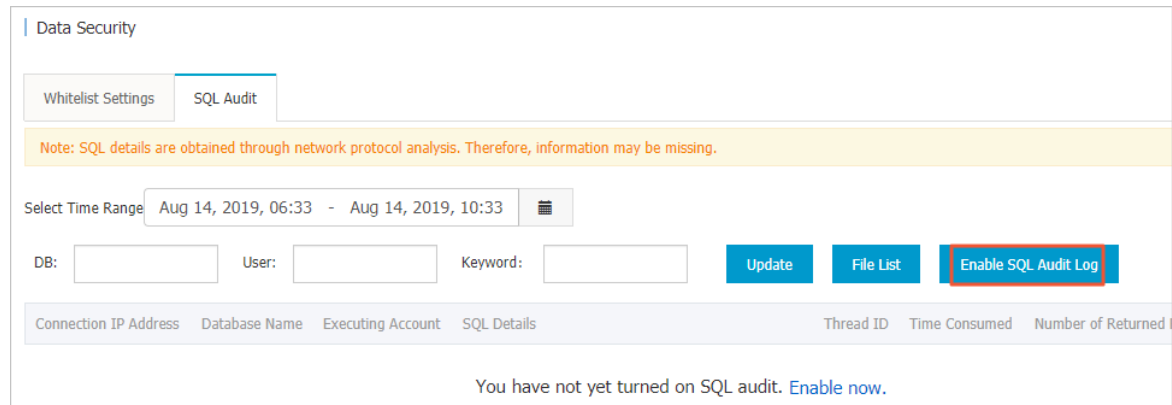
- You cannot view the SQL audit logs that are generated before you enable the SQL Audit feature.
- After you enable the SQL Audit feature, the performance of your RDS instance is not affected.
- The retention period of SQL audit logs is 30 days.
- The retention period of SQL audit log files that are exported is two days. ApsaraDB RDS automatically deletes the SQL audit log files that are stored for longer than two days.
- The maximum length that the SQL Audit feature allows for each SQL statement is 2,000 bytes. The part that exceeds 2,000 bytes cannot be logged.
- The SQL Audit feature is disabled by default. The SQL Audit feature is charged per hour.

The fee that is charged per hour for the SQL Audit feature varies based on the region where your RDS instance resides:

- USD 0.15 per GB-hour: China (Hong Kong), US (Silicon Valley), and US (Virginia).
 - USD 0.18 per GB-hour: Singapore (Singapore), Japan (Tokyo), Germany (Frankfurt), UAE (Dubai), Australia (Sydney), Malaysia (Kuala Lumpur), India (Mumbai), Indonesia (Jakarta), and UK (London).
 - USD 0.12 per GB-hour: all regions except the preceding regions.
- The SQL Audit feature on an ApsaraDB RDS for SQL Server instance is provided by the minor engine of SQL Server and the maximum number of SQL audit logs that can be buffered in memory is 4 MB. If a large number of SQL statements are executed to query data, a small amount of SQL audit logs may be lost. If you want to allow SQL audit logs to be buffered in the storage of your RDS instance to keep all the SQL audit logs, you must submit a to modify the default configuration.

Enable the SQL Audit feature

- 1.
2. In the left-side navigation pane, click **Data Security**.
3. On the **SQL Audit** tab, click **Enable SQL Audit**.



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

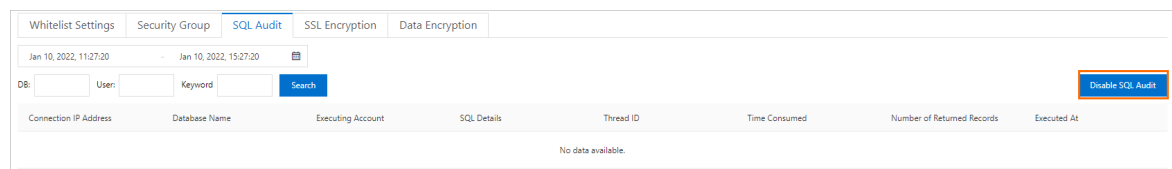
After you enable the SQL Audit feature, you can query SQL statements based on filter criteria such as the time, database, user, and keyword.

Disable the SQL Audit feature

If you no longer require the SQL Audit feature, you can disable the feature to reduce costs.

Note After the SQL Audit feature is disabled, all SQL audit logs including historical SQL audit logs are deleted. Before you disable the SQL Audit feature, we recommend that you export the SQL audit logs to your computer.

- 1.
2. In the left-side navigation pane, click **Data Security**.
3. On the **SQL Audit** tab, click **Export File** to export the SQL audit logs to your computer.
4. After you export the SQL audit logs to your computer, click **Disable SQL Audit**.



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

19.2. View the error logs of an ApsaraDB RDS for SQL Server instance

This topic describes how to view the error logs of an ApsaraDB RDS for SQL Server instance in the ApsaraDB RDS console or by using SQL statements. You can use the error logs to troubleshoot issues. After a primary/secondary switchover is complete, you can view the primary/secondary switchover logs of an RDS instance in the ApsaraDB RDS console.

Prerequisites

Your RDS instance runs RDS High-availability Edition or RDS Cluster Edition. For more information about how to switch workloads over between primary and secondary RDS instances, see [Switch workloads over between primary and secondary ApsaraDB RDS for SQL Server instances](#).

Precautions

The first logs in this topic refer to error logs. For more information about how to view transaction logs, see [Back up an ApsaraDB RDS for SQL Server instance](#) and [Download the data backup files and log backup files of an ApsaraDB RDS for SQL Server instance](#).

Limits

If your RDS instance runs SQL Server 2008 R2 with standard SSDs or enhanced SSDs (ESSDs), you cannot view primary/secondary switchover logs on the **Logs** page of the ApsaraDB RDS console.

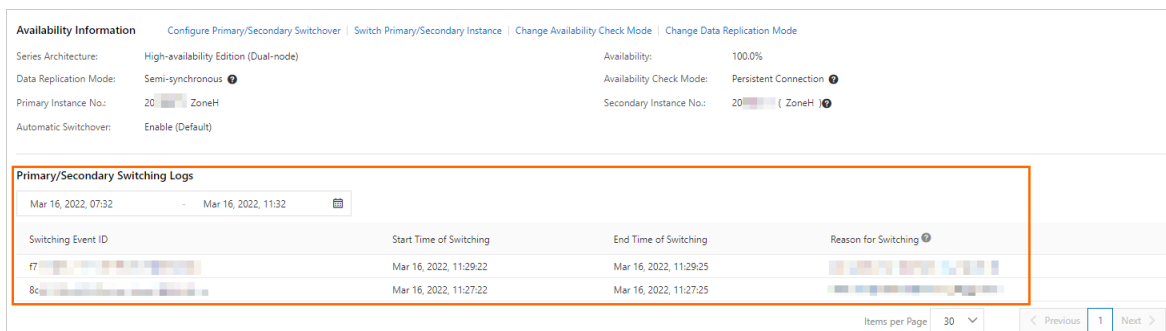
View error logs in the ApsaraDB RDS console

- 1.
2. In the left-side navigation pane, click **Logs**.
3. On the **Logs** page, click the **Error Logs** tab, select a time range, and then click **OK**.

Tab	Description
Error Logs	Provides logs on events that occurred over the last month. The events include custom events and specific system events.

View primary/secondary switchover logs in the ApsaraDB RDS console

- 1.
2. In the left-side navigation pane, click **Service Availability**.
3. In the **Primary/Secondary Switching Logs** section of the page that appears, select a time range and view the primary/secondary switchover logs that are generated over the selected time range.



View error logs by using SQL statements

- If your RDS instance runs SQL Server 2016 or an earlier version, run the `sp_rds_read_error_logs` stored procedure to read error logs. The method that is used to run this stored procedure is similar to the method that is used to run the `sp_readerrorlog` stored procedure.

o Example 1:

```
EXEC sp_rds_read_error_logs
```

o Example 2:

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

- If your RDS instance runs SQL Server 2017 or SQL Server 2019, run the `sp_readerrorlog` stored

procedure to read error logs.

Example:

```
EXEC sp_readerrorlog
```

19.3. View the event history of an ApsaraDB RDS instance

This topic describes how to view the operation and maintenance (O&M) events that are performed by users and Alibaba Cloud on an ApsaraDB RDS for SQL Server instance. These events include instance creation and parameter reconfiguration.

Billing

The event history feature is free of charge in the public preview phase, but starts to be charged after the public preview phase ends.

Scenarios

- Track instance management operations.
- Audit the security of instance management operations.
- Audit the compliance of the instance management operations that are performed by Alibaba Cloud. This applies to security-demanding sectors, such as finance and government affairs.

View the event history feature

1. Log on to the [RDS management console](#), in the left-side navigation pane, click **Event Center**, and then select a region above.
2. Click the **Historical Events** tab.

Introduction to the Historical Events page

The Historical Events page shows details about historical events in the selected region. These details include the resource types, resource names, and event types. The following table describes the parameters of a historical event.

Parameter	Description
Resource Type	The type of the RDS resource managed in the event. Only the Instance resource type is supported.
Resource Name	The name of the RDS resource managed in the event. If the value of the Resource Type parameter is Instance , the Resource Name column displays the ID of the involved RDS instance.
Event Type	The type of the event, for example, Instance Management , Database Management , Read-write Splitting , and Network Management . For more information, see Events .

Parameter	Description
Event Name	The operation executed in the event. For example, if the event type is Instance Management , supported operations include Create Instance , Delete Instance , Change Specifications , and Restart Instance . For more information, see Events .
Run At	The time when the event was executed.
User Type	The initiator of the event. Valid values: <ul style="list-style-type: none"> User: initiates operations by using the ApsaraDB RDS console or the API. System: initiates automatic O&M operations or periodic tasks. O&M Administrator: initiates manual O&M operations.
Cause	The cause of the event. Valid values: <ul style="list-style-type: none"> User Action: The event was initiated from a user by using the ApsaraDB RDS console or the API. System Action or O&M Action: The event was initiated from the system or an O&M administrator.
The user information	The ID of the account that is used by a user to perform the event.
Parameters	The request parameters used by a user to initiate the event in the ApsaraDB RDS console.

Note

- The Historical Events page shows the historical events that were generated about 5 minutes earlier.
- Historical Events are presented specific to regions. You can select a region in the top navigation bar and then view the historical events in the selected region.

Event Center

Scheduled Events | **Historical Events** | Resource Requests

Dec 2, 2021, 10:51:44 - Dec 2, 2021, 15:51:44

Resource Type	Resource Name	Event Type	Event Name	Run At	User Type	Cause	The User Information	Parameters
instance	rm-bp-...	Instance Management	Modify Instance Description	Dec 2, 2021, 14:55:10	User	User Action	28...	{"Domain": "rds-inc-share.aliyunco...
instance	rm-bp-...	Instance Management	Modify Instance Description	Dec 2, 2021, 14:28:07	User	User Action	28...	{"Domain": "rds-inc-share.aliyunco...
instance	pgm-bp-...	Security Management	Modify Whitelist	Dec 2, 2021, 14:28:07	User	User Action	14...	{"Domain": "rds.aliyunco...", "Req...
instance	pgm-bp-...	Security Management	Modify Whitelist	Dec 2, 2021, 13:41:42	User	User Action	14...	{"Domain": "rds.aliyunco...", "Req...

Events

Event type	Operation
	Restart Instance (RestartDBInstance)
	Renew (RenewInstance)

Event type	Operation
Instance Management	Change Specifications (ModifyDBInstanceSpec)
	Migrate Across Zones (MigrateToOtherZone)
	Shrink Log (PurgeDBInstanceLog)
	Upgrade Kernel Version (UpgradeDBInstanceEngineVersion)
	Modify Instance Description (ModifyDBInstanceDescription)
	Modify Maintenance Window (ModifyDBInstanceMaintainTime)
	Create Read-only Instance (CreateReadOnlyDBInstance)
	Destroy Instance (DestroyDBInstance)
	Modify Upgrade Mode of Kernel Version (ModifyDBInstanceAutoUpgradeMinorVersion)
	Edit Parameters (ModifyParameter)
CloudDBA	Create Diagnostics Report (CreateDiagnosticReport)
Database Management	Create Database (CreateDatabase)
	Delete Database (DeleteDatabase)
	Modify Database Description (ModifyDBDescription)
	Replicate Database Between Instances (CopyDatabaseBetweenInstances)
	Modify System Collation and Time Zone (ModifyCollationTimeZone)
Read-write Splitting	Create Read-write Splitting Endpoint (AllocateReadWriteSplittingConnection)
	Query System-assigned Weight (CalculateDBInstanceWeight)
	Modify Read-write Splitting Policy (ModifyReadWriteSplittingConnection)
	Release Read-write Splitting Endpoint (ReleaseReadWriteSplittingConnection)
Security Management	Enable Enhanced Whitelist (MigrateSecurityIPMode)
	Enable SSL (ModifyDBInstanceSSL)
	Enable TDE (ModifyDBInstanceTDE)
	Modify Whitelist (ModifySecurityIps)
	Create Account (CreateAccount)

Event type	Operation
Account Management	Delete Account (DeleteAccount)
	Authorize Account to Access Database (GrantAccountPrivilege)
	Revoke Database Permissions from Account (RevokeAccountPrivilege)
	Modify Description of Database Account (ModifyAccountDescription)
	Reset Account Password (ResetAccountPassword)
	Reset Permissions of Superuser Account (ResetAccount)
High Availability (HA)	Trigger Switchover Between Primary and Secondary Instances (SwitchDBInstanceHA)
	Modify HA Mode (ModifyDBInstanceHAConfig)
Network Management	Apply for Public Endpoint (AllocateInstancePublicConnection)
	Modify Expiry Time of Endpoint (ModifyDBInstanceNetworkExpireTime)
	Modify Endpoint and Port (ModifyDBInstanceConnectionString)
	Switch Network Type (ModifyDBInstanceNetworkType)
	Release Public Endpoint (ReleaseInstancePublicConnection)
	Switch Between Internal and Public Endpoints (SwitchDBInstanceNetType)
Log Management	Enable/disable Log Audit (ModifySQLCollectorPolicy)
Backup Restoration	Create Data Backup (CreateBackup)
	Clone Instance (CloneDBInstance)
	Create Temporary Instance (CreateTempDBInstance)
	Modify Backup Policy (ModifyBackupPolicy)
	Restore Backup Set to Original Instance (RestoreDBInstance)
	Delete Data Backup (DeleteBackup)
	Restore Database (RecoveryDBInstance)
Cross-region Backup Restoration	Restore Data to New Instance Across Regions (CreateDdrInstance)
	Modify Cross-region Backup Settings (ModifyInstanceCrossBackupPolicy)
SQL Server Backup Migration to	Restore Backup File in OSS to RDS Instance (CreateMigrateTask)

Event type	Operation
	Make Database Available While Migrating Backup Data to Cloud (CreateOnlineDatabaseTask)
Monitoring	Set Monitoring Frequency (ModifyDBInstanceMonitor)
Data Migration	Create Upload Path for SQL Server (CreateUploadPathForSQLServer)
	Import Data from Other RDS (ImportDatabaseBetweenInstances)
	Cancel Migration Task (CancelImport)
Tag Management	Bind Tags to Instance (AddTagsToResource)
	Remove Tag (RemoveTagsFromResource)

Related operations

Operation	Description
Query historical events	Queries the events of an ApsaraDB RDS instance.
Query status of the event history feature	Queries the status of the historical events feature of an ApsaraDB RDS instance.
Enable or disable the event history feature	Enables or disables the historical events feature of an ApsaraDB RDS instance.

20.Backup

20.1. Enable snapshot backups for an ApsaraDB RDS for SQL Server instance


This topic describes how to enable snapshot backups for an ApsaraDB RDS for SQL Server instance. Compared with physical backups, snapshot backups support a higher backup speed and a larger amount of data.

Prerequisites

- Your RDS instance uses standard SSDs or enhanced SSDs (ESSDs).
- The cross-region backup feature is not enabled for your RDS instance. If this feature is enabled, you must disable this feature before you enable snapshot backups. For more information, see [Disable cross-region backups for an RDS instance](#).
- Your RDS instance does not belong to the shared instance family or a dedicated cluster. For more information, see [ApsaraDB RDS instance families](#)
- Your RDS instance is created after January 1, 2021.

Comparison between snapshot backups and physical backups

Item	Physical backup	Snapshot backup
Backup speed	The backup speed is fast. However, the restoration speed varies based on the specifications of your RDS instance.	The backup speed is extremely fast. The speed of creating a snapshot backup is approximately twice the speed of creating a physical backup. Note When you create a snapshot backup for the first time, ApsaraDB RDS backs up all the data of your RDS instance. The backup process may require a long period of time.
Backup frequency	Physical backups support the following two backup frequencies: <ul style="list-style-type: none"> • Same as Data Backup • Every 30 minutes 	The Backup Frequency is fixed to Every 30 minutes and cannot be changed.

Item	Physical backup	Snapshot backup
Restoration speed	The restoration speed is fast. However, the restoration speed varies based on the specifications of your RDS instance.	<p>The restoration speed is extremely fast. The restoration speed is not affected by the amount of data. The speed of restoring data from a snapshot backup is higher than the speed of restoring data from a physical backup.</p> <ul style="list-style-type: none"> • Restore data to a new RDS instance <ul style="list-style-type: none"> ◦ The time that is required to restore data from a data backup file is approximately 30 minutes. This includes the time that is required to create an RDS instance and the time that is required to restore the data from the data backup file. ◦ The time that is required to restore data to a point in time varies based on the log backup file that is used. This includes the time that is required to create an RDS instance and the time that is required to restore the data from the log backup file. • Restore data to an existing RDS instance <ul style="list-style-type: none"> ◦ The time that is required to restore data from a data backup file is approximately 10 minutes. ◦ The time that is required to restore data to a point in time varies based on the log backup file that is used. <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note The logs that are restored are generated between the point in time at which the closest snapshot backup file is generated and the point in time to which you want to restore data.</p> </div>
Amount of data supported	Up to 4 TB of data is supported.	Up to 16 TB of data is supported.
Impact on instance performance	A large number of resources are occupied. This has a significant impact on the performance of your RDS instance. We recommend that you perform a physical backup during off-peak hours.	Only a small number of I/O resources are occupied. This does not significantly affect the performance of your RDS instance. You can perform a snapshot backup at any time.
Download of backup files	Physical backup files can be downloaded.	Snapshot backup files cannot be downloaded.

Benefits

The data from physical backup files can be restored at a speed of only up to 20 MB per second. Each physical backup supports up to 4 TB of data. If you want to restore a large amount of data, the restoration process may require a long period of time. The snapshot backups of ApsaraDB RDS for SQL Server are developed based on Volume Shadow Copy Service, which is provided by Microsoft. ApsaraDB RDS can complete a snapshot backup within a short period of time. Snapshot backups help ensure data consistency and integrity. For more information, see [Volume Shadow Copy Service](#).

Snapshot backups have the following benefits:

- Each snapshot backup supports up to 16 TB of data.
- Snapshot backups support a higher backup speed than **physical backups**.
- Snapshot backups do not occupy CPU or memory resources. Compared with **physical backups**, snapshot backups occupy less I/O resources. When snapshot backups are being created, the performance of your RDS instance is not significantly affected.
- Compared with **physical backups**, **snapshot backups** support a higher restoration speed, reduced recovery time objective (RTO), and improved fault resistance for your database service.
- After you enable **snapshot backups**, you can still perform **physical backups** to back up your RDS instance. For more information, see [Manually back up your RDS instance](#).

Billing

Each RDS instance is allocated a free quota for backup storage. If your usage exceeds the free quota, you are charged for the excess storage. For more information, see [Backup storage fees for an ApsaraDB RDS for SQL Server instance](#).


Limits

- Snapshot backup files cannot be stored in a region that is different from the region where your RDS resides. For more information, see [Enable cross-region backups for an ApsaraDB RDS for SQL Server instance](#).
- You can change the backup method of your RDS instance from **Physical Backup** to **Snapshot Backup**. However, you cannot change the backup method of your RDS instance from **Snapshot Backup** to **Physical Backup**.
- Snapshot backups support only **full backups**. Snapshot backups do not support **individual databases or tables**.
- Snapshot backup files cannot be downloaded.

Procedure

By default, the **Physical Backup** method is enabled for new RDS instances. You can manually change the backup method of an RDS instance to **Snapshot Backup**.

- 1.
2. In the left-side navigation pane, click **Backup and Restoration**.
3. On the **Backup and Restoration** page, click the **Backup Settings** tab and click **Edit** next to **Backup Settings**.
4. Set the **Backup Method** parameter to **Snapshot Backup** and click **Save**.

 Notice

- After you change the backup method of the RDS instance to **Snapshot Backup**, you cannot change the billing method of the RDS instance back to **Physical Backup**.
- After you change the backup method of the RDS instance to **Snapshot Backup**, you can still perform **Physical Backup** to back up your RDS instance. For more information, see [Manually back up your RDS instance](#).
- If you select the **Snapshot Backup** method, the backup frequency is fixed to **Every 30 Minutes** and cannot be changed.

What to do next

[Back up an ApsaraDB RDS for SQL Server instance](#)

Related operations

Operation	Description
Create data backup	Creates a data backup for an ApsaraDB RDS instance.
Query the data backup files	Queries the data backup files of an ApsaraDB RDS instance.
查询备份设置	Queries the backup settings of an ApsaraDB RDS instance.
Modify backup settings	Modifies the backup settings of an ApsaraDB RDS instance.
Query backup tasks	Queries the backup tasks of an ApsaraDB RDS instance.
Query log backup files	Queries the log backup files of an ApsaraDB RDS instance.

20.2. Backup storage fees for an ApsaraDB RDS for SQL Server instance

This topic describes the fees that are required to store the backup files of an ApsaraDB RDS for SQL Server instance.

Overview

A free quota is provided to store the backup files of each RDS instance. If the total size of your backup files does not exceed the free quota, you are not charged backup storage fees. If the total size of your backup files exceeds the free quota, you are charged an hourly fee for the excess backup storage that you use. The hourly fee is calculated by using the following formula: **Hourly fee for backup storage = (Total size of backup files - Free quota) × Unit price**.

Backup method	Total size of backup files	Free quota (unit: GB; rounded only up to the next integer)	Unit price (USD/GB)
Snapshot backup	Total size of backup files = Size of data backup files + Size of log backup files	Free quota = 200% × Purchased storage capacity	0.00004
Physical backup	You can log on to the ApsaraDB RDS console and go to the Basic Information page of your RDS instance. In the lower-right corner of the page, you can view the total size of backup files.	Free quota = 50% × Purchased storage capacity	<ul style="list-style-type: none"> RDS instances that use standard SSDs or enhanced SSDs (ESSDs): 0.00004 RDS instances that use local SSDs: 0.00020

How to reduce backup storage fees

- Reduce the size of backup files. To achieve this, you can delete backup files, reduce the backup frequency, or shorten the backup retention period. For more information, see [Back up an ApsaraDB RDS for SQL Server instance](#).
- Increase the free quota for backup storage. To achieve this, you can expand the storage capacity of your RDS instance. For more information, see [Change the specifications of an ApsaraDB RDS for SQL Server instance](#).

The free quota varies based on the storage capacity of your RDS instance. For example, if you back up your RDS instance by using the physical backup method and expand the storage capacity of your RDS instance from 150 GB to 300 GB, the free quota increases from 75 GB to 150 GB.

20.3. Back up an ApsaraDB RDS for SQL Server instance

This topic describes how to back up an ApsaraDB RDS for SQL Server instance. You can configure a backup policy that allows ApsaraDB RDS to automatically back up your RDS instance. You can also manually back up your RDS instance.

Precautions

- Backup files do not occupy the storage capacity that you purchased for your RDS instance. Each RDS instance is allocated a free quota for backup storage. If your usage exceeds the free quota, you are charged for the excess usage. We recommend that you specify a backup cycle based on your business requirements to make the best use of the free quota. For more information, see [View the free quota for backup storage of an ApsaraDB RDS for SQL Server instance](#).
- You must familiarize yourself with the billing methods and billable items of backup storage. For more information, see [Billable items, billing methods, and pricing](#).
- You must familiarize yourself with the billing standards of backup storage. For more information, see [Backup storage fees for an ApsaraDB RDS for SQL Server instance](#).
- We recommend that you back up your RDS instance during off-peak hours and do not execute DDL statements during a backup. DDL statements trigger locks on tables, and the backup may fail as a result of the locks.
- If your RDS instance contains a large amount of data, a backup may require a long period of time.

- Backup files are retained based on the retention period that you specify. Before the specified retention period elapses, we recommend that you download the backup files that you require to your computer.
- If your RDS instance runs the RDS Basic Edition, High-availability Edition, or Cluster Edition, your RDS instance collects traffic statistics from the network interface controllers of the operating system that is used. In this case, the volume of traffic on your RDS instance surges during a backup.

Overview of data backups and log backups

Database engine	Data backup	Log backup
-----------------	-------------	------------




Database engine	Data backup	Log backup
SQL Server	<ul style="list-style-type: none"> • Physical backups <ul style="list-style-type: none"> ◦ Full physical backups and incremental physical backups are supported. Logical backups are not supported. ◦ Automatic backups are performed based on the backup cycle that you specify. The backup cycle consists of three phases: a full backup, an incremental backup, and another incremental backup. For example, if a full backup is performed on Monday, an incremental backup is separately performed on Tuesday and Wednesday. Then, a full backup is performed again on Thursday, and an incremental backup is separately performed again on Friday and Saturday. The backup cycle continues until you modify the backup policy of your RDS instance. <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin: 10px 0;"> <p>Note If a manual full backup is performed within a backup cycle, two consecutive incremental backups are automatically performed within the next two days following the manual full backup.</p> </div> <ul style="list-style-type: none"> ◦ Backups on individual databases are supported. You can back up one or more databases of your RDS instance at a time. ◦ SQL Server shrinks transaction logs during each backup. You can log on to the ApsaraDB RDS console and go to the Backup and Restoration page of your RDS instance. Then, you can click Shrink Transaction Log to manually shrink transaction logs. <ul style="list-style-type: none"> • Snapshot backups Full snapshot backups are performed based on the backup cycle that you specify. 	<ul style="list-style-type: none"> • ApsaraDB RDS automatically backs up the binary logs of your RDS instance based on the backup frequency that you specify. ApsaraDB RDS supports the following two backup frequencies: <ul style="list-style-type: none"> ◦ Same as Data Backup ◦ Every 30 Minutes <p>The total size of log backup files does not vary based on the backup frequency that you specify.</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin: 10px 0;"> <p>Note The backup frequency for snapshot backups is fixed to Every 30 Minutes and cannot be changed.</p> </div> <ul style="list-style-type: none"> • The log backup feature cannot be disabled. • You can specify a log backup retention period. The log backup retention period that you specify must be within the range of 7 days to 730 days. • You can download log backup files. <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin: 10px 0;"> <p>Note If the Backup Frequency parameter is set to Every 30 Minutes, you can restore the data of your RDS instance to a specific point in time within the last 30 minutes in the event of SSD damage or other unexpected failures. This is supported when your RDS instance runs the RDS Basic Edition.</p> </div>

Configure a backup policy for automatic backups

ApsaraDB RDS can automatically back up your instance based on the backup policy that you specify.

- 1.

- In the left-side navigation pane, click **Backup and Restoration**.
- On the **Backup and Restoration** page, click the **Backup Settings** tab. In the Data Backup Settings section, click **Edit**.
- Configure the following parameters and click **Save**.


Parameter	Description
Data Backup Retention	The number of days for which you want to retain data backup files. Valid values: 7 to 730. Unit: days. Default value: 7.
Backup Cycle	The cycle based on which you want to create backups. You can select one or more days of the week.  Note For data security purposes, we recommend that you back up your RDS instance at least twice a week.
	The backup method that you want to use. Valid values: <ul style="list-style-type: none"> Snapshot Backup: ApsaraDB RDS backs up the data from standard SSDs or enhanced SSDs (ESSDs) at a specific point in time. The backup speed is fast. For more information, see Enable snapshot backups for an ApsaraDB RDS for SQL Server instance. Physical Backup: This is the default backup method. ApsaraDB RDS produces replicas for the data of your RDS instance. The backup speed is slow.  Note
Backup Time	The hour at which you want to create a backup.
Backup Frequency	<ul style="list-style-type: none"> Same as Data Backup Every 30 Minutes The total size of log backup files does not vary based on the backup frequency that you specify.  Note If you select the Snapshot Backup method, the backup frequency is fixed to Every 30 Minutes and cannot be changed.
Log Retention Period (Days)	The number of days for which you want to retain log backup files. The log backup retention period is the same as the period that is specified by the Data Backup Retention parameter.

Manually back up your RDS instance

-
- In the upper-right corner of the page, click **Back Up Instance** to open the **Back Up Instance** dialog box.

3. Configure the following parameters and click **OK**.

Parameter	Description
Backup Policy	<ul style="list-style-type: none"> ◦ Snapshot Backup: ApsaraDB RDS backs up the data from standard SSDs or enhanced SSDs (ESSDs) at a specific point in time. The backup speed is fast. For more information, see Enable snapshot backups for an ApsaraDB RDS for SQL Server instance. ◦ Physical Backup: This is the default backup method. ApsaraDB RDS produces replicas for the data of your RDS instance. The backup speed is slow. <p>Note Snapshot Backup is available only when the snapshot backup feature is enabled. For more information, see Enable snapshot backups for an ApsaraDB RDS for SQL Server instance.</p>
Select Backup Mode	<ul style="list-style-type: none"> ◦ Full Backup: ApsaraDB RDS immediately performs a full backup. ◦ Automatic Backup: ApsaraDB RDS immediately performs a full backup or an incremental backup. <p>Note Automatic Backup is available only when you set the Backup Policy parameter to Physical Backup.</p>
Backup Policy	<p>This parameter is available only when you set the Select Backup Mode parameter to Full Backup.</p> <ul style="list-style-type: none"> ◦ Instance Backup: ApsaraDB RDS backs up all the data of your RDS instance. ◦ Database/Table Backup: ApsaraDB RDS backs up only the databases that you specify. This option is available only when you set the Backup Policy parameter to Physical Backup. <p>Note If you select Database/Table Backup, you must select databases from the left-side list and click the > icon to move the selected databases to the right-side list. If no databases are created on your RDS instance, you must create databases before you back up your RDS instance. For more information, see Create a database on an ApsaraDB RDS for SQL Server instance.</p>

4. Click the  icon in the upper-right corner of the page to view the progress of the backup task that you created.

Note After the backup task is completed, you can go to the **Backup and Restoration** page to download the backup file that is generated from the backup task. Some RDS instances do not support the download of backup files. For more information, see [Download the data backup files and log backup files of an ApsaraDB RDS for SQL Server instance](#).

FAQ

1. Can I disable the data backup feature for my RDS instance?

No, you cannot disable the data backup feature for your RDS instance. However, you can reduce the backup frequency to at least twice a week. The data backup retention period must be within the range of 7 days to 730 days.

2. Can I disable the log backup feature for my RDS instance?

No, you cannot disable the log backup feature for your RDS instance.

Operations

Operation	Description
Create data backup	Creates a data backup for an ApsaraDB RDS instance.
Query the data backup files	Queries the data backup files of an ApsaraDB RDS instance.
查询备份设置	Queries the backup settings of an ApsaraDB RDS instance.
Modify backup settings	Modifies the backup settings of an ApsaraDB RDS instance.
Query backup tasks	Queries the backup tasks of an ApsaraDB RDS instance.
Query log backup files	Queries the log backup files of an ApsaraDB RDS instance.

20.4. Enable cross-region backups for an ApsaraDB RDS for SQL Server instance

This topic describes how to enable cross-region backups for an ApsaraDB RDS for SQL Server instance. After you enable cross-region backups, the backup files of the original RDS instance are automatically replicated from the source region to the specified destination region. You can use the backup files in the destination region to manage and restore the data of the original RDS instance.

Prerequisites

- The original RDS instance uses standard SSDs or enhanced SSDs (ESSDs).
- The original RDS instance does not run SQL Server 2019 EE.
- Disk encryption and Transparent Data Encryption (TDE) are not enabled for the original RDS instance. For more information, see [Configure disk encryption for an ApsaraDB RDS for SQL Server instance](#) and [Configure TDE for an ApsaraDB RDS for SQL Server instance](#).

Note

- For more information about how to enable cross-region backups for an ApsaraDB RDS for MySQL instance, see [Enable cross-region backups for an ApsaraDB RDS for MySQL instance](#).
- For more information about how to enable cross-region backups for an ApsaraDB RDS for PostgreSQL instance, see [Enable cross-region backups for an ApsaraDB RDS for PostgreSQL instance](#).

Context

Cross-region backups are different from default backups. For more information about default backups, see [Back up an ApsaraDB RDS for SQL Server instance](#).

If a cross-region backup is complete, you can restore the data of the original RDS instance from the cross-region backup file that is generated to a new RDS instance that resides in the destination region. For more information, see [Restore the data of an ApsaraDB RDS for SQL Server instance across regions](#).

Differences between cross-region backups and default backups

Comparison item	Cross-region backup	Default backup
Default status	By default, cross-region backups are disabled. If you want to perform cross-region backups, you must manually enable cross-region backups.	By default, default backups are enabled.
Storage	Cross-region backup files are stored in a different region rather than the source region.	Default backup files are stored in the source region.
Restoration	The data of a cross-region backup file can be restored only to a new RDS instance that resides in the destination region.	The data of a default backup file can be restored to one of the following RDS instances: <ul style="list-style-type: none"> • New RDS instance in the source region • Original RDS instance
Retention period	After the original RDS instance is released, its cross-region backup files are still retained based on the cross-region backup retention period that you specify.	By default, after the original RDS instance is released, its default backup files are retained for seven days.

Billing

You are charged an hourly fee for cross-region backups. The hourly fee consists of the following parts:

- Remote storage fee: USD 0.0002/GB.
- Network traffic fee: For more information, see [Network traffic fees](#).


Precautions

- Cross-region backups do not affect default backups. These types of backups can exist at the same time.
- After a default backup is complete, a cross-region backup is triggered. During the cross-region backup

process, the original RDS instance replicates the default backup file that is generated to the destination region.


- After you enable cross-region backups, the original RDS instance checks whether valid data backup files are generated over the most recent 24 hours. If no valid data backup files are generated over the most recent 24 hours, the original RDS instance triggers a full backup.
- After you enable cross-region log backups, the original RDS instance checks the valid data backup files that are generated over the most recent 24 hours.
 - If continuous binary log files are archived following the valid data backup files, the original RDS instance replicates the archived binary log files to the destination region.
 - If no continuous binary log files are archived following the valid data backup files, the original RDS instance triggers a backup on its secondary RDS instance.
- Cross-region backups are not supported in a few Alibaba Cloud regions due to network reasons. The following table lists the Alibaba Cloud regions where cross-region backups are supported.

Source region	Destination region
China (Hangzhou), China (Shanghai), China (Qingdao), China (Beijing), China (Zhangjiakou), China (Hohhot), China (Shenzhen), China (Hong Kong), China (Ulanqab), China (Chengdu), China (Guangzhou), and China (Heyuan)	China (Hong Kong), China (Hangzhou), China (Shanghai), China (Qingdao), China (Shenzhen), China (Zhangjiakou), China (Hohhot), China (Beijing), China (Ulanqab), China (Chengdu), China (Guangzhou), and China (Heyuan)

 **Note** The backup files from the source region can be replicated to a different region rather than the source region. The available destination regions vary based on your network environment.

Enable cross-region backups for a single RDS instance in the ApsaraDB RDS console

- 1.
2. Find the RDS instance for which you want to enable cross-region backups. In the Actions column, choose **More > Cross-region Backup Settings**.

 **Note**

- You can also click **Edit** on the **Cross-region Backup** tab of the **Backup and Restoration** page.
- If the **Cross-region Backup Settings** option or the **Cross-region Backup** tab cannot be found, you must check whether the RDS instance meets all prerequisites.

3. Configure the following parameters.

Cross-region Backup Settings
✕

Cross-region Enable Disabled

Backup Status

Backup Region China (Hohhot) ▼

Cross-region 90 days

Retention Period Enter an integer from 7 to 1825.

Cross-region Log Enable Disabled

Backup Status

i Note: You will be charged for additional fees if you enable cross-region backup. [Learn More](#)

OK
Cancel

Parameter	Description
Cross-region Backup Status	Specify whether to enable or disable cross-region backups. Select Enable .
Backup Region	Select the destination region to which the backup files of the RDS instance are automatically replicated.
Cross-region Retention Period	Specify the number of days for which cross-region backup files are retained. Valid values: 7 to 1825. The value 1825 is equivalent to five years. <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #ccc;"> <p>? Note After the RDS instance expires or is released, its cross-region backup files are still retained based on the cross-region backup retention period that you specify. You can log on to the ApsaraDB RDS console, click Backups in the left-side navigation pane, and then click the Cross-region Backup tab to view the cross-region backup files that are retained.</p> </div>
Cross-region Log Backup Status:	Specify whether to enable or disable cross-region log backups. After you enable cross-region log backups, the log backup files of the RDS instance are automatically replicated to the specified Object Storage Service (OSS) bucket in the destination region.

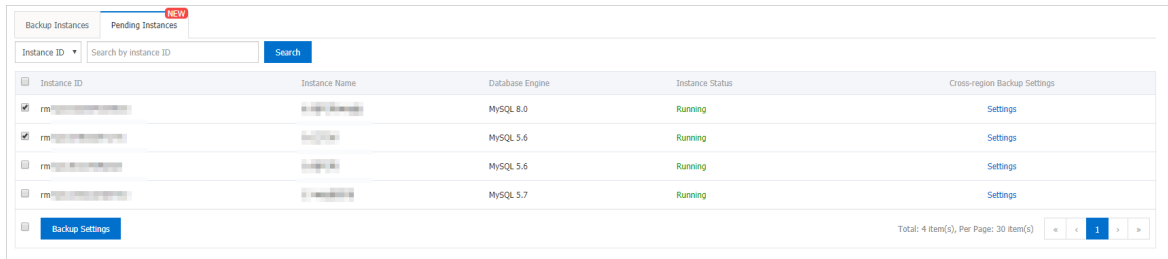
4. Click **OK**.

Enable cross-region backups for multiple RDS instances at a time

1. Log on to the [RDS management console](#) , in the left-side navigation pane, click **Backups** , and then select a region above.
2. On the **Cross-region Backup** tab, click the **Pending Instances** tab.

3. Select the RDS instances for which you want to enable cross-region backups. Then, click **Backup Settings**.

Note You can also click **Settings** in the Cross-region Backup Settings column of an RDS instance to enable cross-region backups only for the RDS instance.



4. Configure the following parameters.

Parameter	Description
Cross-region Backup Status	Specify whether to enable or disable cross-region backups. Select Enable .
Backup Region	Select the destination region to which the backup files of the RDS instance are automatically replicated.
Cross-region Retention Period	Specify the number of days for which cross-region backup files are retained. Valid values: 7 to 1825. The value 1825 is equivalent to five years. <div style="background-color: #e1f5fe; padding: 5px; border: 1px solid #cfe2f3;"> <p>Note After the RDS instance expires or is released, its cross-region backup files are still retained based on the cross-region backup retention period that you specify. You can log on to the ApsaraDB RDS console, click Backups in the left-side navigation pane, and then click the Cross-region Backup tab to view the cross-region backup files that are retained.</p> </div>
Cross-region Log Backup Status:	Specify whether to enable or disable cross-region log backups. After you enable cross-region log backups, the log backup files of the RDS instance are automatically replicated to the specified Object Storage Service (OSS) bucket in the destination region.

5. Click **OK**.

Modify the cross-region backup settings of an RDS instance

The Cross-region Backup tab is added to the Backups page in the ApsaraDB RDS console. On the Cross-region Backup tab, you can modify the cross-region backup settings of an RDS instance even after the RDS instance is released.

1. Log on to the [RDS management console](#), in the left-side navigation pane, click **Backups**, and then select a region above.
2. On the Backups page, click the **Cross-region Backup** tab. Click the **Backup Instances** tab and find the RDS instance whose cross-region backup settings you want to modify. Then, click **Settings** in the Cross-region Backup Settings column to modify the cross-region backup settings of the RDS instance.

Note If the RDS instance is released, you can only change the cross-region backup retention period.

Disable cross-region backups for an RDS instance

If you no longer require cross-region backups, you can perform the following steps to disable cross-region backups:

1. Log on to the [RDS management console](#), in the left-side navigation pane, click **Backups**, and then select a region above.
2. On the Backups page, click the **Cross-region Backup** tab. Click the **Backup Instances** tab and find the RDS instance for which you want to disable cross-region backups. Then, click **Settings** in the Cross-region Backup Settings column.
3. In the dialog box that appears, set the **Cross-region Backup Status** parameter to **Disabled** and set the **Cross-region Retention Period** parameter to 7.

Note After you disable cross-region backups, no new cross-region backup files are generated. The existing cross-region backup files must be retained for at least seven days. Therefore, you must set the cross-region backup retention period to seven days. After the seven-day retention period elapses, all existing cross-region backup files are deleted and you are no longer charged for the storage of cross-region backup files.

4. Click **OK**.

View and download the cross-region backup files of an RDS instance

1. Log on to the [RDS management console](#), in the left-side navigation pane, click **Backups**, and then select a region above.
2. On the Backups page, click the **Cross-region Backup** tab. Then, click the **Backup Instances** tab to view the cross-region backup files of the RDS instance.

Instance ID	Instance Name	Database Engine	Instance Status	Cross-region Backup Status	Latest Backup Region	Latest Backup Start Time	Cross-region Retention Period	Cross-region Backup Settings
rm-xxxxxxx	xxxxxxx	MySQL 5.7	Running	Enable	China (Hohhot)	Dec 16, 2019, 10:14	7 Days	Settings
rm-xxxxxxx	xxxxxxx	MySQL 8.0	Running	Enable	China (Qingdao)	Dec 16, 2019, 10:03	7 Days	Settings

3. Click the ID of the RDS instance. On the page that appears, click the **Data Backup** or **Log Backup** tab. Then, find the backup file that you want to download, and click **Download** in the Actions column.
4. Click **Download**.

Note You are not charged for the traffic that you consume to download backup files over an internal network. However, you are charged for the traffic that you consume to download backup files over the Internet. For more information, see [Network traffic fees](#).

FAQ

After I disable cross-region backups for my RDS instance, why am I still charged for the storage of cross-region backup files?

After you disable cross-region backups for your RDS instance, no new cross-region backup files are generated and you are no longer charged for the traffic that is consumed to transmit cross-region backup files. However, you are still charged for the storage of the existing cross-region backup files within the cross-region backup retention period that you specify. The existing cross-region backup files must be retained for at least seven days. Therefore, you must set the cross-region backup retention period to seven days. For more information, see the "[Modify the cross-region backup settings of an RDS instance](#)" section of this topic. After the cross-region backup retention period that you specify elapses, all existing cross-region backup files are deleted and you are no longer charged for the storage of cross-region backup files.

Related operations


Operation	Description
Check cross-region backup	Checks whether an ApsaraDB RDS instance has a cross-region data backup file that can be used to restore data across regions.
Restore data to a new instance across regions	Restores the data of an ApsaraDB RDS instance to a new ApsaraDB RDS instance.
Modify cross-region backup settings	Modifies the cross-region backup settings of an RDS instance.
Query cross-region backup settings	Queries the cross-region backup settings of an ApsaraDB RDS instance.
Query cross-region data backup files	Queries the cross-region data backup files of an ApsaraDB RDS instance.
Query cross-region log backup files	Queries the cross-region log backup files of an ApsaraDB RDS instance.
Query regions that support cross-region backup	Queries the available destination regions to which the cross-region backup files from a specified source region can be replicated.
Query the time range to which you can restore data by using a cross-region backup set	Queries the restorable time range that is supported by a specified cross-region backup file.
Query ApsaraDB for RDS instances on which cross-region backup is enabled	Queries the ApsaraDB RDS instances for which cross-region backups are enabled in a region and the cross-region backup settings of the instances.


20.5. Download the data backup files and log backup files of an ApsaraDB RDS for SQL Server instance

This topic describes how to download the unencrypted data backup files and log backup files of an ApsaraDB RDS for SQL Server instance. You can archive the backup files that you download. You can also restore data from these backup files to on-premises databases.

Limits

If the **AliyunRDSReadOnlyAccess** policy is attached to a RAM user, the RAM user has only the read permissions and cannot download data backup files or log backup files. You must attach the **AliyunRDSFullAccess** policy to your RAM user in the RAM console.


Database engine	Download data backup files	Download log backup files
SQL Server	<ul style="list-style-type: none"> You can download full physical backup files and incremental physical backup files. For more information, see the "Download full or incremental physical backup files" section of this topic. You can also download the physical backup files of individual databases. For more information, see the "Download the physical backup files of individual databases" section of this topic. <div style="background-color: #e1f5fe; padding: 5px; border: 1px solid #ccc;"> <p> Note You cannot download snapshot backup files. For more information, see Enable snapshot backups for an ApsaraDB RDS for SQL Server instance.</p> </div>	<p>You can download log backup files regardless of the instance configuration. For more information, see the "Download log backup files" section of this topic.</p>

 **Note**

- You can use Database Backup (DBS) to implement automated backups and automated downloads. For more information, see [Back up databases](#).
- For more information about data backups and log backups, see [Overview of data backups and log backups](#).

Download full or incremental physical backup files

- 1.
2. In the left-side navigation pane, click **Backup and Restoration**.
3. Click the **Data Backup** tab.
4. Specify the time range that you want to query.
5. Find the data backup file that you want to download. In the **Actions** column, click **Download Instance Backup**.


 **Note**

- If Download Instance Backup cannot be found in the Actions column, see the "Limits" section of this topic.
- If you want to download a data backup file and use the file to restore data, we recommend that you select the data backup file that is created at the point in time closest to the point in time at which the required data exists.
- If you want to download a log backup file and use the file to restore data to an on-premises database, the start time of the log backup file must be within a specific time range. The time range starts after the point in time at which the selected data backup file is generated and ends before the point in time to which you want to restore data.

6.

Download the physical backup files of individual databases

- 1.
2. In the left-side navigation pane, click **Backup and Restoration**.
3. Click the **Data Backup** tab.
4. Specify the time range that you want to query.
5. Find the data backup file that you want to download. In the **Actions** column, click **Download Database Backup**.
6. On the **Download Backup Files of Individual Database** page, find the data backup file that you want to download, and click **Download** in the **Actions** column.


 **Note**

- If Download Instance Backup cannot be found in the Actions column, see the "Limits" section of this topic.
- If you want to download a data backup file and use the file to restore data, we recommend that you select the data backup file that is created at the point in time closest to the point in time at which the required data exists.
- If you want to download a log backup file and use the file to restore data to an on-premises database, the start time of the log backup file must be within a specific time range. The time range starts after the point in time at which the selected data backup file is generated and ends before the point in time to which you want to restore data.

7.

Download log backup files

- 1.
2. In the left-side navigation pane, click **Backup and Restoration**.
3. Click the **Log Backup** tab.
4. Specify the time range that you want to query.
5. Find the log backup file that you want to download. In the **Actions** column, click **Download**.

 **Note**

- If Download Instance Backup cannot be found in the Actions column, see the "Limits" section of this topic.
- If you want to download a data backup file and use the file to restore data, we recommend that you select the data backup file that is created at the point in time closest to the point in time at which the required data exists.
- If you want to download a log backup file and use the file to restore data to an on-premises database, the start time of the log backup file must be within a specific time range. The time range starts after the point in time at which the selected data backup file is generated and ends before the point in time to which you want to restore data.

6.

21. Restoration

21.1. Restore the data of an ApsaraDB RDS for SQL Server instance

This topic describes how to restore the data of an ApsaraDB RDS for SQL Server instance.

Context

You can use one of the following methods to restore the data of your RDS instance:

- [Restore the data to an existing RDS instance](#)
- [Restore the data to a new RDS instance](#)
- [Restore the data to the original RDS instance by using a temporary RDS instance](#)

Restore the data to an existing instance

You can restore the data of your RDS instance to the original RDS instance or to a different existing RDS instance. During this process, you can restore some or all of the databases that are created on your RDS instance. In addition, you can restore the data from a data backup file or to a specific point in time.

 **Note** This method is supported for RDS instances that run SQL Server 2008 R2 with standard or enhanced SSDs (ESSDs), SQL Server 2012, SQL Server 2016, SQL Server 2017, or SQL Server 2019.

- 1.
2. In the left-side navigation pane, click **Backup and Restoration**.
3. Click **Restore**.
4. In the **Select Restore Method** dialog box, select **Restore to Existing Instance** and click **OK**.
5. Configure the following parameters and click **OK**.

Parameter	Description
Restore Method	<ul style="list-style-type: none"> ◦ By Time: allows you to restore the data to a point in time within the specified log retention period. For information about how to view or change the log backup retention period, see Back up an ApsaraDB RDS for SQL Server instance. ◦ By Backup Set: allows you to restore the data from a full or incremental data backup file.
Restore Time	This parameter appears only when you set the Restore Method parameter to By Time . Select the point in time to which you want to restore the data.
Backup Set	This parameter appears only when you set the Restore Method parameter to By Backup Set . Select the data backup file from which you want to restore the data.
More Backup Sets	This parameter displays the latest 1,000 data backup files. If you cannot find the required data backup file from the Backup Set drop-down list, you can select this check box. Then, ApsaraDB RDS displays more data backup files for you to search.

Parameter	Description
Destination Instance Name	<p>Select the destination RDS instance to which you want to restore the data.</p> <p>By default, ApsaraDB RDS displays all the RDS instances that are created within your Alibaba Cloud account and reside in the selected region. These displayed RDS instances include the original RDS instance whose data you want to restore.</p> <div style="background-color: #e6f2ff; padding: 10px;"> <p>Note</p> <ul style="list-style-type: none"> ○ If you use a snapshot backup file, you can restore the data only to an RDS instance on which the snapshot backup feature is enabled. For more information, see Enable snapshot backups for an ApsaraDB RDS for SQL Server instance. ○ The destination RDS instance can run a higher SQL Server version than the original RDS instance. ○ If the original RDS instance belongs to the shared instance family, you cannot restore the data of the instance to a general-purpose or dedicated RDS instance. Similarly, if the original RDS instance belongs to the general-purpose or dedicated instance family, you cannot restore the data of the instance to a shared RDS instance. ○ If ApsaraDB RDS displays a large number of RDS instances, you can enter a keyword in the Destination Instance Name field to search for the required destination RDS instance. </div>
Databases to Restore	<ol style="list-style-type: none"> i. Select the databases that you want to restore. By default, ApsaraDB RDS displays and selects all the databases that are created on the original RDS instance. <ul style="list-style-type: none"> ■ If you want to restore all the data of the original RDS instance, select all the databases. ■ If you want to restore one or more databases, select only the required databases. ii. Specify the names that you want to use for the selected databases on the destination RDS instance. By default, the original names of the selected databases are retained. <div style="background-color: #e6f2ff; padding: 10px;"> <p>Note The names of the selected databases on the original RDS instance cannot be the same as those of the existing databases on the destination RDS instance.</p> </div>

Note

- If a selected database on the original RDS instance has the same name as an existing database on the destination RDS instance, you must specify **New Database Name** for the selected database.
- The value of **New Database Name** can contain only lowercase letters, digits, underscores (_), and hyphens (-).


Restore data to a new RDS instance

You can restore the data of your RDS instance to a new RDS instance. This process was previously known as instance cloning. During this process, you can specify to restore the data from a data backup file or to a specific point in time. If you restore the data from a data backup file, you can restore some or all of the databases whose data is included in the file.

You must pay for the new RDS instance. The required fee is the same as the amount you pay when you purchase the RDS instance. If you no longer require the original RDS instance after the restoration, we recommend that you immediately release or unsubscribe from the instance. For more information, see [Release or unsubscribe from an ApsaraDB RDS for SQL Server instance](#).

 **Note** This method is supported for RDS instances that run SQL Server 2008 R2 with standard or ESSDs, SQL Server 2012, SQL Server 2016, SQL Server 2017, or SQL Server 2019.

- 1.
2. In the left-side navigation pane, click **Backup and Restoration**.
3. Click **Restore**.
4. In the dialog box that appears, select **Restore to New Instance** and click **OK**.
5. On the **Restore Database (Previously Clone Instance)** page, configure the following parameters.

Parameter	Description
Billing Method	<ul style="list-style-type: none"> ◦ Subscription: A subscription instance is an instance for which you pay an upfront fee. For long-term use, the subscription billing method is more cost-effective than the pay-as-you-go billing method. You are offered lower prices for longer subscription periods. ◦ Pay-As-You-Go: A pay-as-you-go instance is charged per hour based on your actual resource usage. For short-term use, we recommend that you select the pay-as-you-go billing method. If you no longer need a pay-as-you-go instance, you can release the instance to reduce costs.
Restore Mode	<ul style="list-style-type: none"> ◦ By Time: allows you to restore data to a point in time within the specified log retention period. For more information about how to view or change the log backup retention period, see Back up an ApsaraDB RDS for SQL Server instance. ◦ By Backup Set: allows you to restore the data from a data backup file. <div style="background-color: #e6f2ff; padding: 10px; margin-top: 10px;"> <p> Note</p> <ul style="list-style-type: none"> ◦ The By Time option is available only after the log backup feature is enabled. ◦ You can restore some or all of the databases that are created on the original RDS instance. </div>

Parameter	Description
Database	<p>Specify whether to restore some or all of the databases that are created on the original RDS instance. If you select Part, you must manually enter the names of the databases that you want to restore. In addition, you must separate the database names with commas (,).</p> <p>Note If you have enabled the snapshot backup feature for the original RDS instance, you can select only All Instances but not Part. For more information, see Enable snapshot backups for an ApsaraDB RDS for SQL Server instance.</p>
Edition	<ul style="list-style-type: none"> ◦ Basic: The database system consists of only a primary RDS instance. Computing is separated from storage to increase cost-effectiveness. ◦ High-availability: The database system consists of a primary RDS instance and a secondary RDS instance. These instances work in the high-availability architecture. ◦ Cluster: The database system consists of a primary RDS instance, a secondary RDS instance, and up to seven read-only RDS instances. The read capability of the database system improves with the number of read-only RDS instances. <p>Note The available RDS editions vary based on the region and database engine version that you select. For more information, see Overview of ApsaraDB RDS editions.</p>
Zone of Primary Node	
Instance Type	<ul style="list-style-type: none"> ◦ General-purpose (Entry-level): specifies the general-purpose instance family. A general-purpose instance exclusively occupies the allocated memory and I/O resources. However, it shares CPU and storage resources with the other general-purpose instances that are deployed on the same server. ◦ Dedicated (Enterprise-level): specifies the dedicated instance family or the dedicated host instance family. A dedicated instance exclusively occupies the allocated CPU, memory, storage, and I/O resources. The dedicated host instance family is the highest configuration of the dedicated instance family. A dedicated host instance exclusively occupies all the CPU, memory, storage, and I/O resources of the server on which the instance is deployed. ◦ Dedicated: A dedicated cluster exclusively occupies all the resources on a VM or physical host. The permissions to manage hosts in a dedicated cluster can be authorized to you. This allows you to create multiple database instances on a host. For more information, see Add hosts. <p>Note Each instance type supports a specific number of CPU cores, memory capacity, maximum number of connections, and maximum IOPS. For more information, see Primary instance types.</p>

Parameter	Description
Capacity	<p>The storage capacity that is provided for the RDS instance to store data files, system files, binary log files, and transaction files. You can adjust the storage capacity in increments of 5 GB.</p> <p>Note Dedicated instances are allocated exclusive resources. Therefore, the storage capacity of a dedicated instance that is equipped with local SSDs varies based on the instance type. For more information, see Primary ApsaraDB RDS instance types.</p>

6. Click **Next: Instance Configuration**.

7. Configure the following parameters.

Parameter	Description
Network Type	
Resource Group	The resource group to which the new RDS instance belongs.

8. Click **Next: Confirm Order**.

9. Confirm the settings in the **Parameters** section, configure the **Purchase Plan** and **Duration** parameters, read and select Terms of Service, click **Pay Now**, and then complete the payment. You must configure the Duration parameter only when the new RDS instance uses the subscription billing method.

Restore the data to the original RDS instance by using a temporary RDS instance

This method is supported for RDS instances that run SQL Server 2008 R2 with local SSDs. For more information, see [Restore the data of an ApsaraDB RDS for SQL Server instance by using a temporary RDS instance](#).

Related operations

Operation	Description
Restore databases	Restores the data of an ApsaraDB RDS instance.

21.2. Restore the data of an ApsaraDB RDS for SQL Server instance across regions

This topic describes how to restore the data of an ApsaraDB RDS for SQL Server instance from a cross-region backup file to a new RDS instance. The new RDS instance must reside in the same region as the cross-region backup file.

Prerequisites



A cross-region backup file is generated. For more information, see [Enable cross-region backups for an ApsaraDB RDS for SQL Server instance](#).

Note


- For more information about how to restore the data of an ApsaraDB RDS for MySQL instance across regions, see [Restore the data of an ApsaraDB RDS for MySQL instance across regions](#).
- For more information about how to restore the data of an ApsaraDB RDS for PostgreSQL instance across regions, see [Restore the data of an ApsaraDB RDS for PostgreSQL instance across regions](#).

Restore data to a new RDS instance

1. Log on to the [RDS management console](#), in the left-side navigation pane, click **Backups**, and then select a region above.
2. On the **Backup Instances** tab of the **Cross-region Backup** tab, find your RDS instance and click the ID of the instance. On the page that appears, find the backup file that you want to use, and click **Restore** in the **Actions** column.
3. Select **Restore to New Instance** and click **OK**.
4. On the **Restore Database** page, click the **Subscription** or **Pay-As-You-Go** tab and configure the following parameters.

Parameter	Description
Restore Mode	<ul style="list-style-type: none"> ◦ By Backup Set: allows you to restore the data of your RDS instance from a data backup file. ◦ By Time: allows you to restore the data of your RDS instance to a specific point in time. The point in time must be within the specified log backup retention period.
Backup Set	The data backup file from which you want to restore the data of your RDS instance. This parameter appears only when you set the Restore Mode parameter to By Backup Set .
Restore Point	<p>The point in time to which you want to restore the data of your RDS instance. This parameter appears only when you set the Restore Mode parameter to By Time.</p> <div data-bbox="552 1615 1385 1727" style="background-color: #e6f2ff; padding: 5px;"> <p> Note Both local and cross-region log backup files can be used to restore the data of your RDS instance to a specific point in time.</p> </div>
Region	<p>The region to which the new RDS instance belongs.</p> <div data-bbox="552 1839 1385 1939" style="background-color: #e6f2ff; padding: 5px;"> <p> Note You can select only the region to which the cross-region backup files of your RDS instance are stored.</p> </div>

Parameter	Description
Zone	The zone where the new RDS instance resides. Each zone is an independent physical location within a region. Zones in the same region provide the same services. You can create the new RDS instance in the same zone as the Elastic Compute Service (ECS) instance to which you want to connect. You can also create the new RDS instance in a different zone than the ECS instance to which you want to connect.
CPU and Memory	The specifications of the new RDS instance. Each instance type supports a specific number of CPU cores, memory capacity, maximum number of connections, and maximum input/output operations per second (IOPS). For more information, see Primary ApsaraDB RDS instance types .
Capacity	The storage capacity that the new RDS instance has available to store data files, system files, archived log files, and transaction files.
Network Type	<ul style="list-style-type: none"> ◦ Classic Network: the traditional type of network. ◦ VPC: the recommended type of network. A virtual private cloud (VPC) is an isolated virtual network that provides higher security and higher performance than the classic network. If you select the VPC network type, you must also select a vSwitch that is associated with the specified VPC.

 **Note** The settings of some parameters cannot be modified. These parameters include Database Engine, Version, and Edition. The same settings of these parameters must be specified for both your RDS instance and the new RDS instance.

5. Specify the **Duration** and **Quantity** parameters. Then, click **Buy Now**. You must specify the Duration parameter when the new RDS instance is billed on a subscription basis.
6. On the **Order Confirmation** page, read and select Terms of Service, Service Level Agreement, and Terms of Use. Then, click Pay Now and complete the payment.

References

After you create an RDS instance, you must configure IP address whitelists or security groups and create accounts. For more information, see [Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance](#) and [Create an account on an ApsaraDB RDS for SQL Server instance](#). If you want to connect to the RDS instance over the Internet, you must also apply for a public endpoint. For more information, see [Apply for or release a public endpoint on an ApsaraDB RDS for SQL Server instance](#). After you complete these operations, you can connect to the RDS instance. For more information, see [Connect to an ApsaraDB RDS for SQL Server instance](#).

Related operations

Operation	Description
Check cross-region backup	Checks whether an ApsaraDB RDS instance has a cross-region data backup file that can be used to restore data across regions.

Operation	Description
Restore data to a new instance across regions	Restores the data of an ApsaraDB RDS instance to a new RDS instance that resides in a different region than the original RDS instance.
Modify cross-region backup settings	Modifies the cross-region backup settings of an ApsaraDB RDS instance.
Query cross-region backup settings	Queries the cross-region backup settings of an ApsaraDB RDS instance.
Query cross-region data backup files	Queries the cross-region data backup files of an ApsaraDB RDS instance.
Query cross-region log backup files	Queries the cross-region log backup files of an ApsaraDB RDS instance.
Query regions that support cross-region backup	Queries the regions to which the cross-region backup files from the current region can be restored.
Query the time range to which you can restore data by using a cross-region backup set	Queries the restorable time range that is supported by a cross-region backup file.
Query ApsaraDB for RDS instances on which cross-region backup is enabled	Queries the ApsaraDB RDS instances for which the cross-region backup feature is enabled in a region and the cross-region backup settings of these instances.

21.3. Restore the data of an ApsaraDB RDS for SQL Server instance by using a temporary RDS instance

This topic describes how to restore the data of a primary ApsaraDB RDS for SQL Server instance by using a temporary RDS instance. The data restoration feature minimizes the losses that are caused by unintentional operations.

After you create a temporary RDS instance for the primary RDS instance, the primary RDS instance still runs as normal. The temporary RDS instance serves only as an intermediary for data restoration. After data is restored to the temporary RDS instance, verify that the restored data is correct. Then, migrate the restored data to the primary RDS instance. This minimizes the impact of data restoration on your workloads.

Prerequisites

- The primary RDS instance runs one of the following SQL Server versions:
 - SQL Server 2012 EE Basic
 - SQL Server 2012 Web
 - SQL Server 2016 Web
 - SQL Server 2008 R2 (with local SSDs)

- The primary RDS instance has data backup files. If you want to restore data to a point in time, log backup files are required.

Precautions

- The temporary RDS instance inherits the account and password settings of the primary RDS instance.
- The temporary RDS instance uses the classic network type.
- Only one temporary RDS instance can be created. If you want to create a temporary RDS instance, you must delete the existing temporary RDS instance.
- A temporary RDS instance is free of charge. After a temporary RDS instance is created, it remains valid within 48 hours. After 48 hours, ApsaraDB RDS deletes the temporary RDS instance.

Procedure

- 1.
2. In the left-side navigation pane, click **Backup and Restoration**.
3. Click the **Temporary Instance** tab.
4. Select the period that is the closest to the point in time to which you want to restore data. ApsaraDB RDS restores data based on the last backup before the point in time. Then, click **Create Temporary Instance**.
5. In the message that appears, click **OK**.
6. After the temporary RDS instance is created, go to the Instances page.
7. Click the ID of the primary RDS instance.
8. In the upper-right corner of the page, click **Import Database** to go to the **Data Transmission Service (DTS)** console.
9. In the left-side navigation pane, click **Data Migration**.
10. Click **Create Migration Task**. On the page that appears, specify Task Name, Source Database, and Destination Database.

Parameter description:

- Task Name: 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: Select **RDS Instance** from the drop-down list.
 - Instance Region: Select a region from the drop-down list. This region is the same as that of the primary RDS instance.
 - RDS Instance ID: Select the ID of the temporary RDS instance from the drop-down list.
 - Database Account: Enter the username of the account that has read and write permissions on the data that you want to migrate. You must specify the same username for the temporary and primary RDS instances.
 - Database Password: Enter the password of the account. You must specify the same password for the temporary and primary RDS instances.
- Destination Database
 - Instance Type: Select **RDS Instance** from the drop-down list.

- Instance Region: Select the region where the primary RDS instance resides from the drop-down list.
 - RDS instance ID: Select the ID of the primary RDS instance from the drop-down list.
 - Database Account: Enter the username of the account that has read and write permissions on the data that you want to migrate.
 - Database Password: Enter the password of the account.
11. Click **Set Whitelist and Next** to go to the **Configure Migration Types and Objects** step.
 12. Specify Migration Type. Select the objects that you want to migrate in the Available section and click the > icon to add the selected objects to the Selected section. To modify the name of an object that you want to migrate in the destination database, move the pointer over the destination database in the Selected section. The **Edit** button appears.
 13. Click **Precheck**.
 14. If the precheck fails, perform this step. If the precheck succeeds, go to Step 18.

If the precheck fails, click the



icon next to each **Failed** check item to view the failure details. After all the errors are fixed, select the current migration task on the **Migration Tasks** page and perform a precheck again.

Pre-check
✕

Pre-check failed 90%

Check item	Check content	Check result
Check database availability	Check whether the database for target database to be migrated in is available	Success
Check source database permission	Check whether account permissions for the source database meet the requirements for migration	Success
Check target database permission	Check whether account permissions for the target database meet the requirements for migration	Success
Check objects with the same name	Check whether there are any structure objects having the same names with objects to be migrated in the target database	Failed i

Cancel

15. After all the errors are fixed, select the new migration task and click **Start** on the **Migration Tasks** page.
16. After the precheck succeeds, click **OK**.
17. In the **Confirm Settings** dialog box, specify the Channel Specification parameter, select **Data Transmission Service (Pay-As-You-Go) Service Terms**, and then click **Buy and Start** to start the migration task.

Related operations

Operation	Description
Create a temporary instance	Creates a temporary ApsaraDB RDS instance.

21.4. Log on to a temporary ApsaraDB RDS for SQL Server instance

This topic describes how to log on to a temporary ApsaraDB RDS for SQL Server instance. After you create a temporary RDS instance for a primary RDS instance, ApsaraDB RDS restores data from the specified backup file to the temporary RDS instance. You can log on to the temporary RDS instance, verify that the restored data is correct, and then migrate the restored data from the temporary RDS instance to the primary RDS instance.

Prerequisites

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

- SQL Server 2012 on RDS Basic Edition
- SQL Server 2016 on RDS Basic Edition
- SQL Server 2008 R2 (with local SSDs)

Procedure

You can log on to a temporary RDS instance over an internal network, which is fast, secure, and free of traffic charges.

To log on to a temporary RDS instance by using an Elastic Compute Service (ECS)-based client, perform the following steps:

1. Create an ECS instance that is used to access the temporary RDS instance. The ECS instance must meet the following requirements:
 - The ECS instance resides in the same region as the temporary RDS instance.
 - The ECS instance uses the classic network type. This is because ECS and RDS instances must have the same network type to communicate over an internal network and all temporary RDS instances use the classic network type.
2. Add the private IP address of the ECS instance to an IP address whitelist of the temporary RDS instance.
3. Log on to the ECS instance. For more information, see [Overview](#).
4. Access the temporary RDS instance from the ECS instance. For more information, see the "Use a database client to connect to your RDS instance" section in [Connect to an ApsaraDB RDS for SQL Server instance](#).

22. Disable the database proxy mode on an ApsaraDB RDS for SQL Server instance

This topic describes how to disable the database proxy mode on an ApsaraDB RDS for SQL Server instance. After you disable the database proxy mode, the RDS instance runs in standard mode. This improves the performance of the RDS instance.

Precautions

In the database proxy mode, the multi-statement function is enabled by default at the protocol layer. After you disable the database proxy mode, the multi-statement function is also disabled. In this case, if you run multi-statements, the system reports errors. Before you disable the database proxy mode, we recommend that you check and add the connection parameters of your RDS instance. For example, add the allowMultiQueries parameter in the JDBC API.

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

Access modes

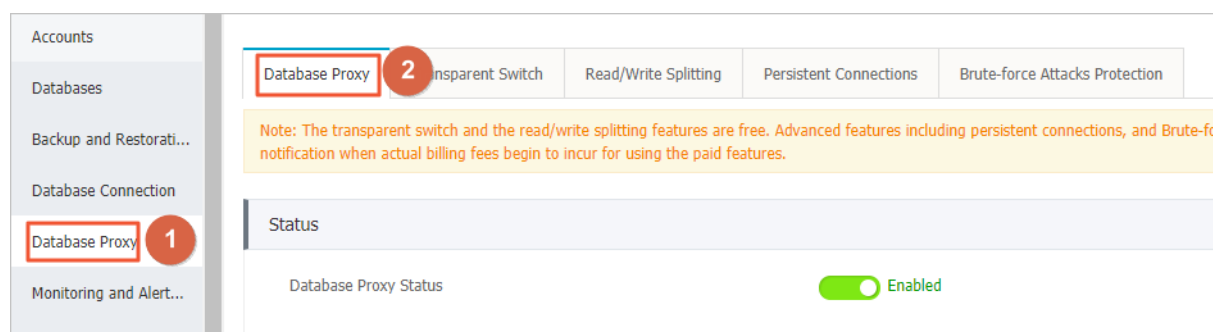
Database engine version	Access mode
SQL Server 2012, SQL Server 2016, and SQL Server 2017	Only the standard mode is supported.
SQL Server 2008 R2	Both the standard mode and the database proxy mode are supported.

Prerequisites

The database proxy mode is enabled for your RDS instance.

Note

- If the Database Proxy tab appears, the database proxy mode is enabled. Perform the following steps to disable the database proxy mode.
- If the Database Proxy tab does not appear, the database proxy mode is disabled. You do not need to perform the operations that are described in this topic.



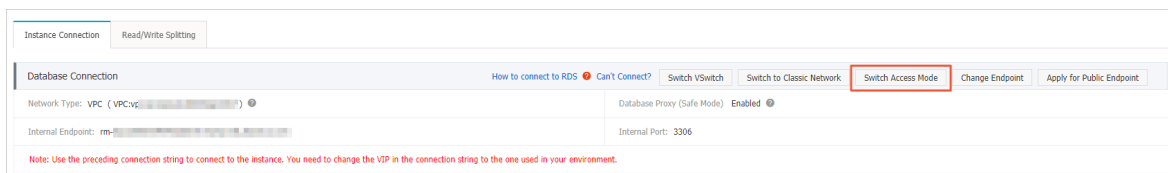
Procedure

Precautions

- You can only disable the database proxy mode. However, you cannot enable the database proxy mode.
- When you disable the database proxy mode, a transient connection error of about 30 seconds will occur. We recommend that you disable the database proxy mode during off-peak hours. Alternatively, make sure that you configure your application to automatically reconnect to your RDS instance.
- If your RDS instance runs SQL Server 2008 R2 in a virtual private cloud (VPC), the database proxy mode is selected by default. You cannot disable the database proxy mode.
- If your RDS instance runs SQL Server 2008 R2 in the classic network, the standard mode is selected by default. You cannot disable the standard mode or change the network type to VPC.

Method 1

- 1.
2. In the left-side navigation pane, click **Database Connection**.
3. In the upper-right corner of the Instance Connection tab, click **Switch Access Mode**. In the message that appears, click **OK**.



Method 2

- 1.
2. In the left-side navigation pane, click **Database Proxy**.
3. On the **Database Proxy** tab, turn off **Database Proxy Status**. In the dialog box that appears, click **Confirm**.

23. Performance optimization and diagnosis

23.1. Troubleshoot the issues of high CPU utilization on an ApsaraDB RDS for SQL Server instance

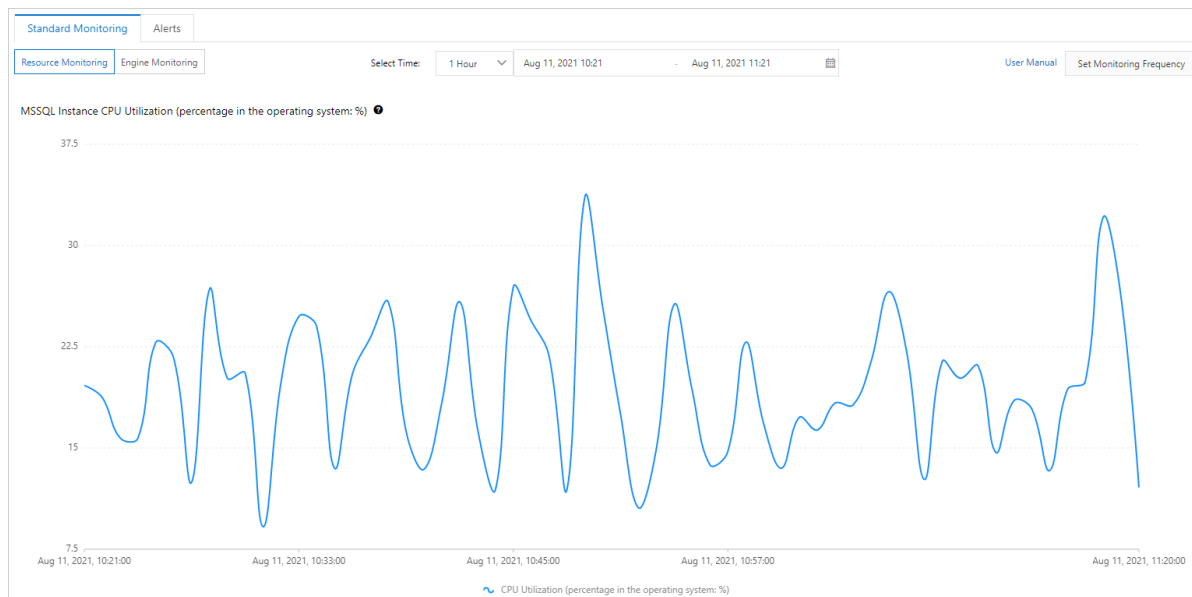
This topic describes how to troubleshoot the issues that cause the high CPU utilization of an ApsaraDB RDS for SQL Server instance. High CPU utilization may affect query performance.

View CPU utilization

You can use one of the following features to view the CPU utilization of your RDS instance in the [ApsaraDB RDS console](#):

- Monitoring and alerting

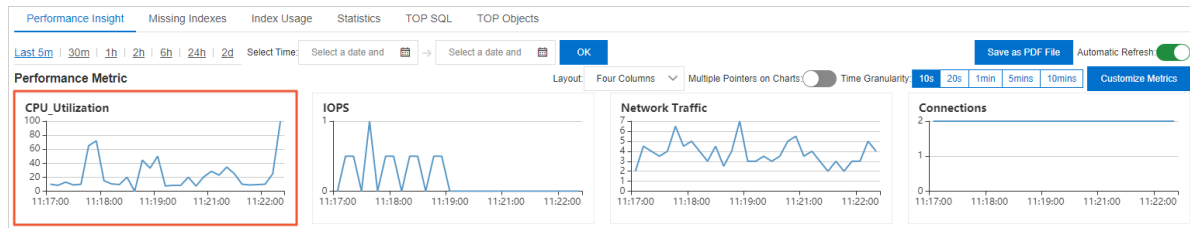
Go to the **Monitoring and Alerts** page. Click the **Standard Monitoring** tab. Then, click **Resource Monitoring** to view the CPU utilization of your RDS instance.



- CloudDBA

The RDS instance does not run SQL Server 2008 R2 with standard SSDs or enhanced SSDs (ESSDs).

In the left-side navigation pane, choose **CloudDBA > Performance Optimization**. On the **Performance Insight** tab of the page that appears, view the CPU utilization of your RDS instance.



Note The shared instance family supports the reuse of CPU resources. When you select the shared instance family, the performance of your RDS instance may be limited due to the reuse of CPU resources even if the CPU utilization of the instance is not high. Therefore, we recommend that you select the dedicated instance family or the dedicated host instance family. This way, you can ensure the stable, high performance of your RDS instance. For more information about the shared instance family, see [Instance families](#).

Analyze CPU metrics

- Cause

In most cases, a sudden increase in CPU utilization is caused by the following issues:

- The number of query requests suddenly increases. For example, the number of query requests increases due to a sudden increase in workloads or due to the cache penetration at the data caching layer.
- The CPU overhead for query requests suddenly increases. For example, if new query requests are processed by using an inefficient method or if the execution plans of some query statements change, the CPU overhead increases.
- The frequency at which ApsaraDB RDS compiles execution plans for query statements significantly increases. For example, if the pressure on the cache increases, the number of execution plans that are cached and the cache hit ratio significantly decrease. In this case, the frequency at which ApsaraDB RDS compiles execution plans for SQL statements significantly increases. As a result, the overall CPU overhead of your RDS instance significantly increases.

- Analysis

Analyze the following metrics to troubleshoot an increase in CPU utilization.

- QPS

If the value of the QPS metric increases at the same rate as CPU utilization, the increase in CPU utilization is caused by an increase in the number of query requests. This means that the reason for the increase in CPU utilization does not lie in your RDS instance. You must analyze your application to troubleshoot the increase in CPU utilization.

- Page_Lookups/sec

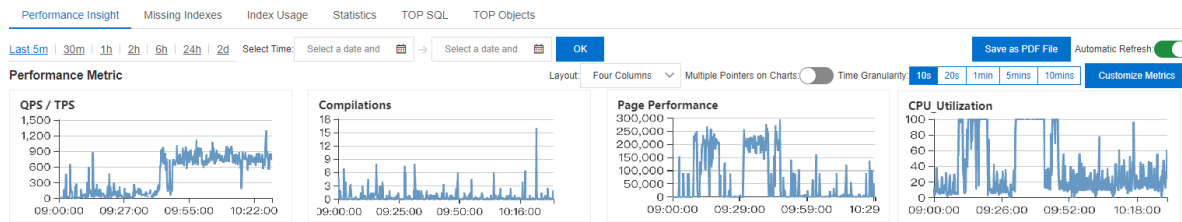
The Page_Lookups/sec metric indicates the cumulative number of pages that are logically read per second to process query requests. In most cases, the value of this metric becomes high because ApsaraDB RDS uses an inefficient method to execute query statements. If the value of this metric is high, the CPU overhead for query requests is high. If the value of the Page_Lookups/sec metric increases at the same rate as CPU utilization but the value of the QPS metric remains relatively stable, the CPU overhead for query statements increases. In this case, you must identify the types of query statements that contribute to the increase in CPU utilization. Then, you can optimize these types of query statements to reduce CPU utilization.

o **Sqlcompliations**

The **Sqlcompliations** metric indicates the number of compile operations per second for query requests. If the value of this metric increases at the same rate as CPU utilization but the value of the **QPS** metric remains relatively stable, the increase in CPU utilization may be caused by the CPU overhead that is required to compile execution plans for query requests. You can further check the **Cache_Object_Counts** and **Cache_Pages** metrics, which are related to the number of execution plans that are cached. If the values of these metrics significantly decrease, the increase in CPU utilization may be caused by significantly high pressure on the cache. In these cases, an effective solution is to increase the memory capacity of your RDS instance.

● **Case**

The following figure shows a sample case.



The CPU utilization statistics show that the increase in CPU utilization occurs from 09:10 to 09:20 and from 09:30 to 09:40. However, the value of the **QPS** metric does not increase during these periods of time. The value of the **QPS** metric increases after 09:40. Therefore, the increase in CPU utilization is not caused by an increase in the number of query requests.

The value of the **Sqlcompliations** metric does not increase during these periods of time, and the absolute value of this metric is low. Therefore, the increase in CPU utilization is not caused by the CPU overhead that is required to compile execution plans for query statements.

The value of the **Page_Lookups/sec** metric increases at the same rate as CPU utilization during these periods of time. Therefore, the increase in CPU utilization may be caused by the high CPU overhead that is required to process some query requests during these periods of time.

You must identify the query statements that require high CPU overhead during these periods of time. In addition, if the value of the **Page_Lookups/sec** metric increases, CPU utilization increases. The execution of some query statements may require high CPU overhead. However, some of these query statements may require medium CPU overhead for logical read operations. Therefore, you must analyze the query statements that are executed during these periods of time to troubleshoot the increase in CPU utilization.

Analyze active sessions

● **Cause**

The most common cause of a sudden increase in CPU utilization is the inefficiency of the method that is used to execute query statements. You can use the Average Active Sessions (AAS) metric of CloudDBA to identify and analyze the query statements that are executed by using an inefficient method.

● **Analysis**

ApsaraDB RDS checks active sessions every 10 seconds and records the SQL statements, query hash values, execution plans, and wait events of active query requests. In most cases, when a query statement that requires high CPU overhead is running, the value in the Wait Category column of the query statement on the Waits tab is CPU.

The **SQL Hash** column on the **SQL** tab displays the hash values that are generated after SQL statements are structured based on parameters. The hash values are used to mark SQL statements that have identical structures. This way, ApsaraDB RDS can classify and aggregate SQL statements based on the structures of the SQL statements. You can query the latest statistics of an SQL statement from the `sys.dm_exec_query_stats` system view based on the value in the `query_hash` column of the SQL statement.

We recommend that you perform the following operations:

- Click the hyperlink in the **SQL Hash** column on the **SQL** tab to view the AAS statistics of the SQL statement.
- Click **Analyze** in the **Execution Plan** column on the **SQL** tab to view the execution plan of the SQL statement. You can also view the optimization suggestions that are generated by CloudDBA.

The preceding optimization suggestions are suitable for SQL statements with simple structures. If the SQL statements on your RDS instance have complex structures, we recommend that you further analyze and test the execution plans of these SQL statements based on the preceding optimization suggestions.

For more information about the AAS metric, see [性能洞察](#).


Analyze top N SQL statements

- Cause

You can use the TOP SQL feature of CloudDBA to identify the SQL statements that cause an increase in CPU utilization during a specific period of time. This feature does not provide information such as the execution frequency, average CPU overhead, and overall CPU overhead of various SQL statements. If you want to optimize the overall CPU resource efficiency of your RDS instance, we recommend that you obtain the details about the SQL statements that consume the most CPU resources.

- Analysis

SQL Server can automatically aggregate information about different objects, such as SQL statements and stored procedures. SQL Server also provides system views such as `sys.dm_exec_query_stats` and `sys.dm_exec_procedure_stats`. You can query the information about different objects from the system views. Then, you can identify the SQL statements that consume the most resources. The resources can be of various types.

 **Note** The TOP SQL report and TOP Objects report in CloudDBA and the top N query reports in SQL Server Management Studio (SSMS) are also based on system views. These reports are easy to use but are less flexible than system views.

Optimize parameter settings

The maximum degree of parallelism (MAXDOP) is used to limit the maximum number of active threads that can be simultaneously used by a single query request. The number of active threads represents the number of cores. If execution plans with high degrees of parallelism are compiled for SQL statements that require high CPU overhead, the time that is required to execute these SQL statements may significantly decrease. However, the CPU overhead per unit of time significantly increases. Therefore, we recommend that you specify a proper MAXDOP to balance the query speed and the CPU utilization based on the following suggestions:

- If the concurrency of query requests is high and the CPU overhead of most of the supported SQL statements is low, set the MAXDOP to a small value. The MAXDOP can be as low as 1, which specifies a zero degree of parallelism.

- If the concurrency of query requests is low and the CPU overhead of some of the supported SQL statements is high, set the MAXDOP to a large value. We recommend that the MAXDOP do not exceed 50% or 25% of the maximum number of cores that are available for your RDS instance.

The default MAXDOP is 2, which is a medium value that balances the query speed and the CPU overhead. You can invoke the `sp_rds_configure` stored procedure to reconfigure the MAXDOP. After you reconfigure the MAXDOP, the new setting immediately takes effect. You do not need to restart your RDS instance.

23.2. Troubleshoot the issues of high I/O on an ApsaraDB RDS for SQL Server instance

This topic describes how to troubleshoot the issues that cause high I/O on an ApsaraDB RDS for SQL Server instance. High I/O affects query performance.

Context

I/O performance varies based on two major factors: IOPS and I/O throughput. In most cases, IOPS is unlikely to become the source of a performance bottleneck. However, I/O throughput may cause a performance bottleneck after it reaches the specified upper limit.

Limits on I/O throughput

- RDS instances equipped with local SSDs

Local SSD-equipped RDS instances share the local SSDs of the physical host on which these instances are deployed. The maximum IOPS per RDS instance is limited, but the I/O throughput per RDS instance is not limited. Therefore, the maximum I/O throughput of an RDS instance can reach more than 1 GB per second. However, these RDS instances may compete for I/O resources. If you require an exclusive allocation of I/O resources, we recommend that you select the dedicated host instance family. For more information, see [Primary instance types](#).

- Cloud SSD-equipped RDS instances

Each cloud SSD-equipped RDS instance is equipped with dedicated standard SSDs or enhanced SSDs (ESSDs). Therefore, each cloud SSD-equipped RDS instance has an exclusive allocation of I/O resources. The maximum I/O throughput of a cloud SSD-equipped RDS instance varies based on the following factors:

- The computing specifications of the RDS instance. The computing specifications vary based on the specifications of the Elastic Compute Service (ECS) g6 instance families. For more information, see [Instance families](#).
- The storage type and storage capacity of the RDS instance. For more information, see [EBS performance](#).

View the I/O throughput of an RDS instance

Prerequisites

The RDS instance does not run SQL Server 2008 R2 with standard SSDs or enhanced SSDs (ESSDs).

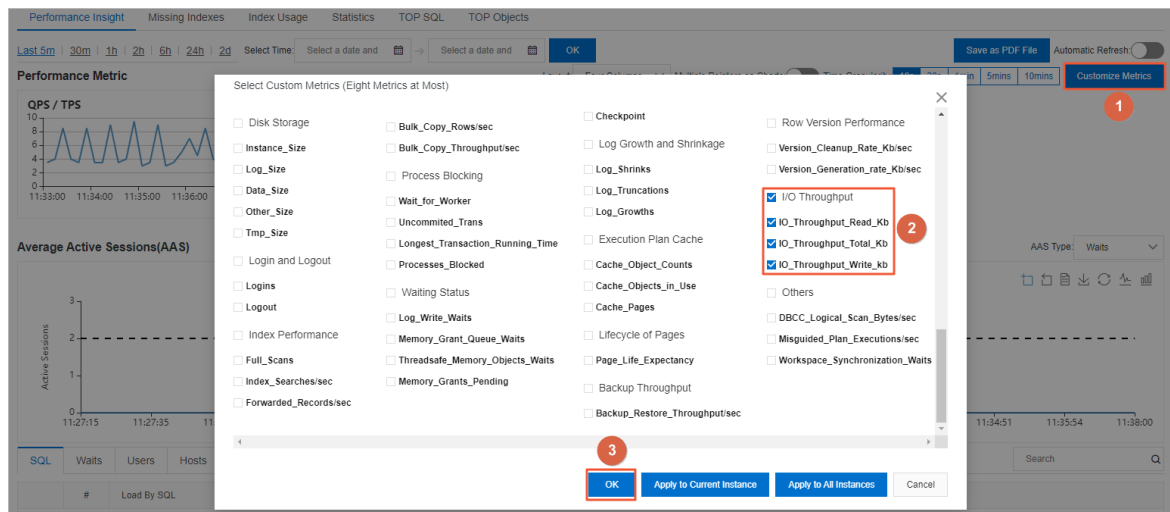
- 1.
2. Find the RDS instance and click the ID of the instance. In the left-side navigation pane, choose **CloudDBA > Performance Optimization**. On the Performance Optimization page, click the

Performance Insight tab.

- In the upper-right corner of the tab, click **Customize Metrics**. In the dialog box that appears, select **I/O Throughput** and click **OK**.

Note After you select **I/O Throughput**, the following metrics are selected:

- IO_Throughput_Read_Kb**: the I/O throughput per second for read operations on the disk
- IO_Throughput_Write_Kb**: the I/O throughput per second for write operations on the disk
- IO_Throughput_Total_Kb**: the total I/O throughput per second for read and write operations on the disk



Analyze and optimize the I/O throughput of an RDS instance

The I/O load on an RDS instance includes two major parts: the read operations on data files and the read and write operations on transaction log files. The read operations on data files include the read operations on data pages during queries and backups. For transaction log files, a majority of the read operations are derived from backups, and the write operations are derived from the other related scenarios rather than backups.

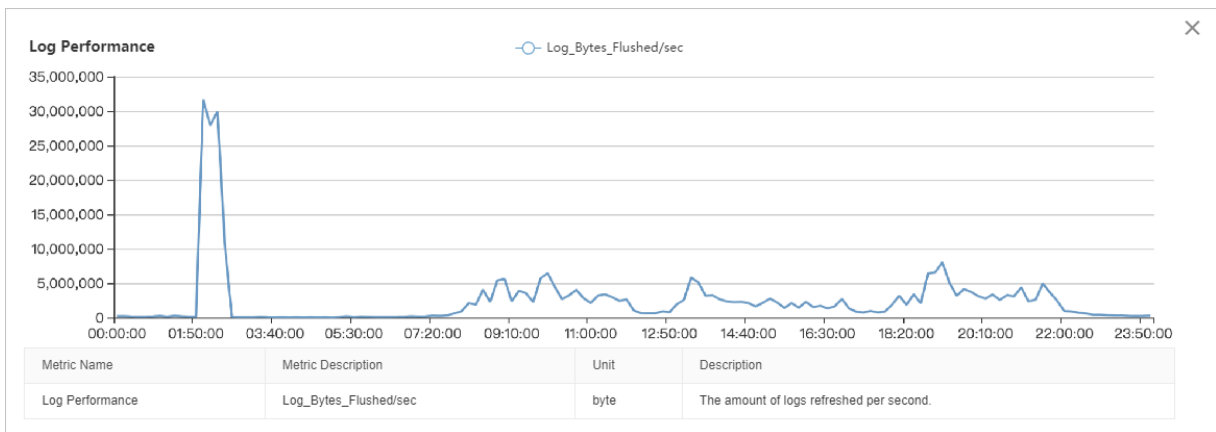
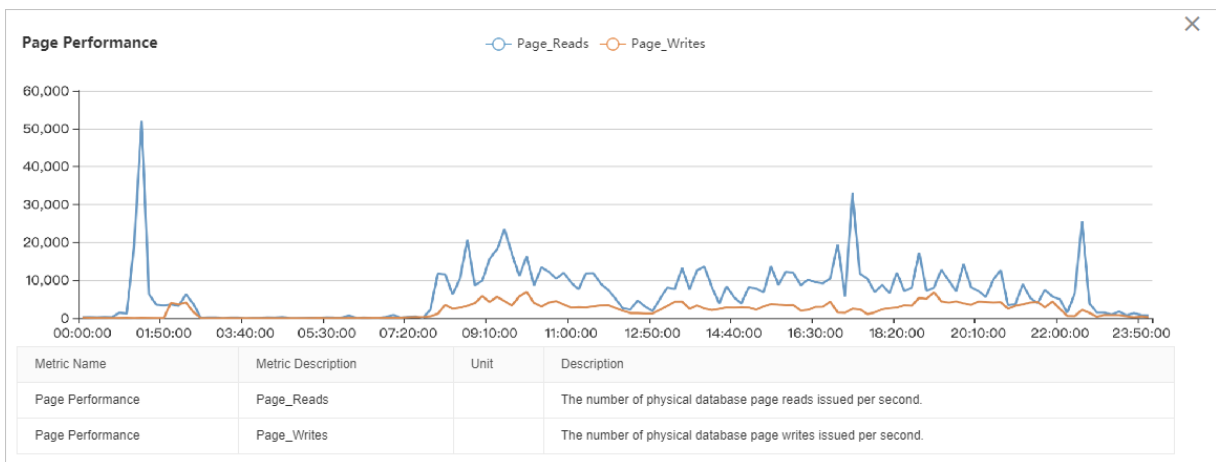
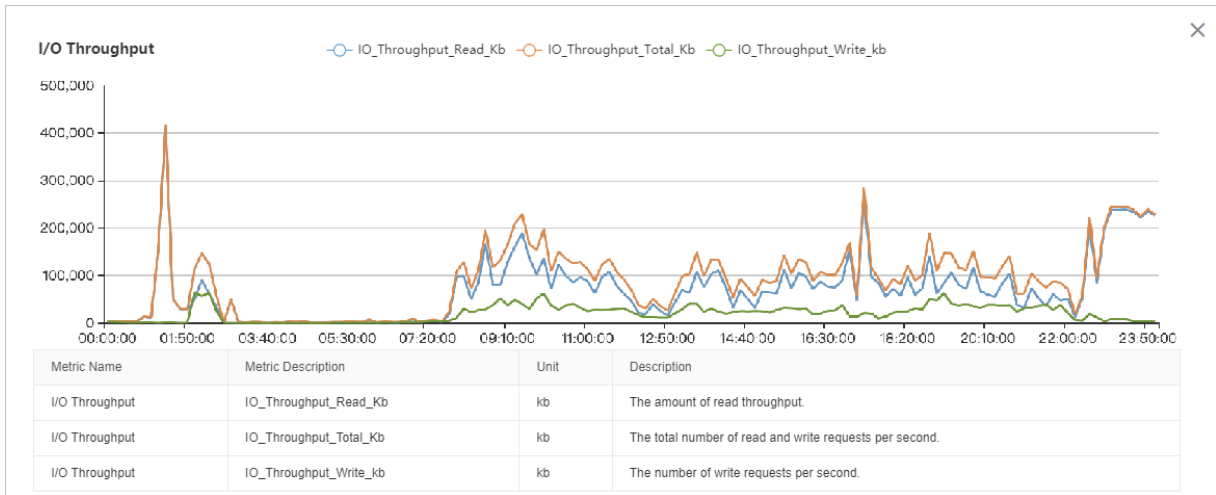
If the I/O throughput of an RDS instance is high, you can click **Customize Metrics**. In the dialog box that appears, you can select the following metrics, which are used to identify the type of load that causes an increase in I/O throughput.

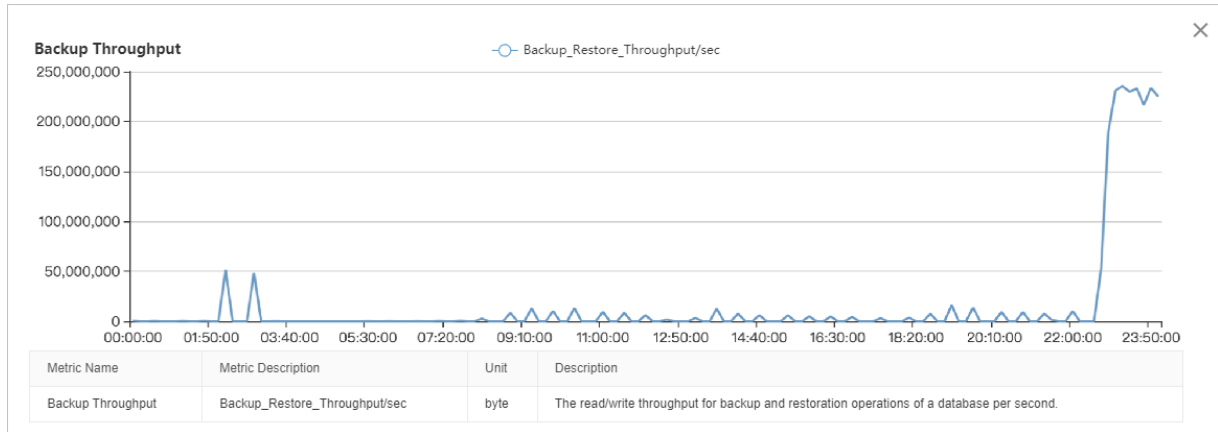
Metric	I/O type	Description
Page_Reads	Read	The number of data pages that are read from data files per second. These data pages cannot be hit in the cache.
Page_Write	Write	The number of data pages that are written to data files per second.
Log_Bytes_Flushed/sec	Write	The number of bytes that are written to transaction log files per second.

Metric	I/O type	Description
Backup_Restore_Throughput / sec	Read	The number of bytes that are read and written to data files and transaction log files per second. This metric is valid for backup and restore operations.

Note The size per data page is 8 KB.

The following figures show analysis cases.





The overall I/O throughput statistics show that the read load is higher than the write load. From 08:00 to 22:00, the I/O throughput is relatively stable. From 01:00 to 03:00 and from 22:00 to 24:00, the I/O throughput shows peak values. To further analyze the I/O throughput statistics during these peak hours, you must obtain more performance data.

- The I/O throughput statistics of data pages show that the I/O throughput suddenly increases at around 01:00 due to read operations on data pages. The peak read speed reaches approximately 50,000 data pages per second, which is equal to approximately 400 MB per second.
- The I/O throughput statistics of data pages, logs, and backups show that the I/O throughput peak during the period of time from 02:00 to 03:00 is derived from four sources. These sources are read operations on data pages, write operations on data pages, write operations on transaction log files, and log backups. I/O throughput peaks at approximately 40 MB per second for both read and write operations on data pages, approximately 30 MB per second for write operations on transaction log files, and approximately 50 MB per second for log backups. The cumulative I/O throughput peaks at approximately 150 MB per second.
- The I/O throughput statistics of data pages and logs show that the I/O load during the period of time from 08:00 to 22:00 is derived from three sources in descending order based on their proportions. These sources are read operations on data pages, write operations on data pages, and write operations on transaction log files. I/O throughput reaches 80 MB to 100 MB per second for read operations on data pages, approximately 30 MB per second for write operations on data pages, and approximately 5 MB per second for write operations on transaction log files.
- The I/O throughput statistics of backups show that the I/O throughput peak during the period of time from 22:00 to 24:00 is derived only from backups. The I/O throughput for backups remains higher than 220 MB per second.

Troubleshoot high I/O throughput caused by read operations on data pages

The high I/O throughput issue that is caused by read operations on data pages is one of the most common high I/O throughput issues in ApsaraDB RDS for SQL Server. In most cases, this issue occurs if the cache size is insufficient. If the cache size of the RDS instance is insufficient, a large number of data pages that are requested by queries cannot be hit in the cache. As a result, ApsaraDB RDS needs to read these data pages from the disk.

Page Life Expectancy (PLE) is a common metric that is used to diagnose the performance of the cache. This metric indicates the average amount of time that each cached data page is retained in the cache. The time is measured in seconds. A shorter period of time indicates higher pressure on the cache.

In normal cases, we recommend that you set the threshold of the PLE metric to a value that is greater than or equal to 300 seconds. Higher memory specifications indicate a larger recommended threshold. You can use the following formula to calculate the recommended threshold:

Recommended threshold = (The memory size of the buffer pool/4) × 300

For example, if the RDS instance provides 16 GB of memory, the amount of memory that can be allocated to the buffer pool cannot exceed 12 GB. In this case, we recommend that you set the threshold to 900 seconds based on the following calculation: $(12/4) \times 300 = 900$.

 **Note** For more information, see [Page Life Expectancy \(PLE\) in SQL Server](#).

If the high I/O throughput issue is caused by read operations on data pages, we recommend that you upgrade the memory specifications of your RDS instance. We recommend that you do not upgrade the performance level (PL) of the disk.

In addition, you can reduce the total number of data pages to mitigate the read load on the RDS instance. For example, you can archive or delete historical data files, enable the data compression feature on tables, delete low-value indexes, and defragment indexes.

Troubleshoot high I/O throughput caused by write operations on data pages and transaction log files

You can use CloudDBA to check whether data manipulation language (DML) or data definition language (DDL) operations are frequently performed during the period of time that shows high I/O throughput. The supported DML operations include INSERT, DELETE, UPDATE, and MERGE. The supported DDL operations include CREATE INDEX and ALTER INDEX.

- High I/O throughput caused by DML operations

Check whether these DML operations are routine workloads. If these DML operations are not routine workloads, we recommend that you perform these DML operations during off-peak hours. For example, temporary data processing and archiving operations are not routine workloads. If these DDL operations are routine workloads, we recommend that you upgrade the PL of the disk. For example, you can upgrade the PL of an ESSD from PL1 to PL2.

We also recommend that you optimize the index structure and delete the nonclustered indexes that are no longer required.

- High I/O throughput caused by DDL operations

In most cases, DDL operations are maintenance or temporary workloads. We recommend that you perform DDL operations during off-peak hours.

In addition, when you perform operations, such as creating and rebuilding indexes, we recommend that you specify the maximum degree of parallelism (MAXDOP) in the SQL statements that are used. This reduces the peak I/O throughput during the running time of the SQL statements. However, this increases the time that is required for DDL operations.

Troubleshoot high I/O throughput caused by backups

ApsaraDB RDS for SQL Server supports backups only on primary RDS instances. This increases the I/O throughput of primary RDS instances. Among all types of backups, full backups have the largest impact on I/O throughput, and log backups have the smallest impact on I/O throughput.

Backups are important to ensure the security and reliability of your data. We recommend that you specify suitable backup settings to reduce the impact of backups on your workloads. For more information, see [Back up an ApsaraDB RDS for SQL Server instance](#).

You can log on to the ApsaraDB RDS console and go to the **Backup and Restoration** page. On this page, you can view the time that is required for each data backup. Then, you can set the backup time to an off-peak hour and specify a proper backup cycle.

- In this example, a full backup requires approximately 6 hours, and your business peak hours start from 09:00 to 21:00 every day. In addition, the background system runs data processing tasks from 22:00 on the current day to 01:00 on the next day. In this case, you can set the backup time to 01:00 to 02:00. This way, each full backup can be finished before 08:00. You can also set the backup cycle to every day of the week. This expedites the restoration process.
- In this example, a full backup requires approximately 15 hours, and your workloads are interrupted by every backup on weekdays. We recommend that you set the backup cycle to Saturday and Sunday. However, if you want to restore data to a specific point in time, the restoration process may be time-consuming.

If you cannot prevent the conflicts between your workloads and full backups by adjusting the backup settings, we recommend that you upgrade the PL of the disk or split your data. Data splitting reduces the amount of data on individual RDS instances. Data splitting also reduces the time that is required for each full backup.

23.3. Troubleshoot the issues of insufficient storage space on an ApsaraDB RDS for SQL Server instance

This topic describes how to troubleshoot the issues that cause insufficient storage space on an ApsaraDB RDS for SQL Server instance. Storage usage is an important metric that is used to measure the performance of your RDS instance. If the amount of available storage space is insufficient, your RDS instance may encounter serious issues. For example, data writes or backups fail, and the time that is required for a storage scaling task is abnormally long.

View storage usage

- Log on to the ApsaraDB RDS console and go to the **Basic Information** page. In the Usage Statistics section of the page, view the overall storage usage of your RDS instance. The Usage Statistics section does not provide the current or historical storage usage for various data types.

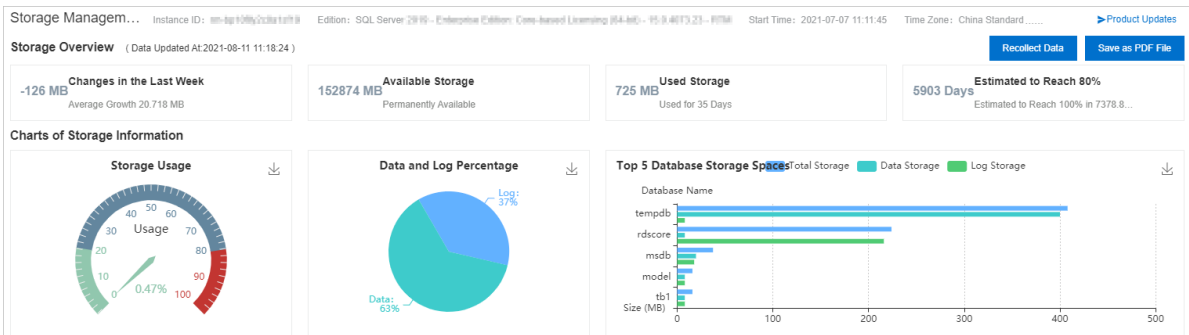
- Log on to the ApsaraDB RDS console and go to the **Monitoring and Alerts** page. On the **Standard Monitoring** tab of the page, click **Resource Monitoring**. Then, view the current and historical storage usage for various data types.

Note The **Other System File Size** metric indicates the amount of storage space that is used by some system files and all the data files and log files in the master, msdb, and model system databases. These system files include error log files, default trace files, and system extended event files.





- Log on to the ApsaraDB RDS console and choose **CloudDBA > Storage Management**. Then, view the storage usage of your RDS instance. The storage usage includes the percentages of used data storage space and used log storage space, the storage consumption trends, and the storage consumption for each of the top 10 databases and top 20 data tables that consume the most storage space. For more information, see [View the storage information of an ApsaraDB RDS for SQL Server instance](#).

Note The RDS instance does not run SQL Server 2008 R2 with standard SSDs or enhanced SSDs (ESSDs).



- Use a client tool, such as SQL Server Management Studio (SSMS), to view the storage usage of your RDS instance.

The following table describes the system views and commands that can be used to query the storage usage of your RDS instance.

System view or command	Description
<code>sp_helpdb</code>	Used to query the total storage space of each database. The total storage space of a database is equal to the total size of data files and log files in the database.
<code>sp_spaceused</code>	Used to query the name, used storage space, and unallocated storage space of the database to which you have logged on.
<code>DBCC SQLPERF (LOGSPACE)</code>	Used to query the total log storage space and used log storage space of each database.
<code>DBCC SHOWFILESTATS</code>	Used to query the total data storage space and used data storage space of the database to which you have logged on.
<code>select * from sys.master_files</code>	Used to query the total size of data files and the total size of log files in each database.
<code>select * from sys.dm_db_log_space_usage</code>	Used to query the total log storage space and used log storage space of the database to which you have logged on.  Note This command is supported only when your RDS instance runs SQL Server 2012 or later.
<code>select * from sys.dm_db_file_space_usage</code>	Used to query the total data storage space and used data storage space of the database to which you have logged on.  Note This command is supported only when your RDS instance runs SQL Server 2012 or later.

If the storage usage of your RDS instance is abnormally high, log on to the [ApsaraDB RDS console](#) and go to the **Monitoring and Alerts** page. View the storage usage for data files, log files, temporary files, and system files to identify the type of file that consumes an abnormally increased amount of storage space. Then, evaluate whether you can use the suggested solutions to release storage space or prevent an abnormal increase in storage consumption.

For more information about the storage analysis and solutions, see the following sections.

Reclaim data storage space

- Analysis

The total data storage space, which is equal to the total size of data files, consists of allocated data storage space and unallocated data storage:

- The allocated data storage space consists of used data storage space and unused data storage space. The unused data storage space can be allocated only to new records in the same table or index. The unused data storage space cannot be directly allocated to the other database objects.
- The unallocated data storage space consists of extents that are not completely allocated. Each extent provides 64 KB of contiguous storage space. The unallocated data storage space is not associated with database objects. You can compress data files to release the unallocated data storage space.

- Solution

In most cases, if the amount of your data continues to increase, the unallocated data storage space is small. In this case, you cannot reclaim a large amount of unallocated data storage space by compressing data files. Before you compress data files, we recommend that you optimize and reclaim the allocated data storage space.

You can use one of the following methods to reclaim the data storage space:

- Archive data files


Delete historical data files that are not frequently queried, migrate these data files to other RDS instances, or archive these data files. This reduces the amount of data that is stored on your RDS instance.

This method is effective to mitigate the increases in data storage consumption. However, this method has requirements for the database object structure and the logic of your application. In addition, this method requires cooperation with application designers and developers.

- Compress data files

If your RDS instance runs SQL Server 2016 or later or runs an Enterprise Edition of an SQL Server version earlier than 2016, the data compression feature is provided. This feature supports row compression and page compression. You can enable this feature on individual tables, indexes, or extents. For more information, see [Data Compression](#).

The data compression ratio ranges from 10% to 90% and varies based on the schema, column data types, and distribution of numerical values. SQL Server provides a dedicated stored procedure, [sp_estimate_data_compression_savings](#). This dedicated stored procedure is used to evaluate the amount of data storage space that you can save by enabling the data compression feature on a specified table or index.

 Note

- To modify the compression option settings of tables or indexes, you must run data definition language (DDL) operations. If you run these operations on large tables, the tables may be locked for a long period of time. The locking of the tables may interrupt your workloads. We recommend that you modify the compression option settings during off-peak hours.
- If your RDS instance runs an Enterprise Edition of SQL Server, you can set the ONLINE parameter to ON. Then, you can run DDL operations to modify the compression option settings. These DDL operations do not interrupt your workloads.
- Data compression increases CPU overhead. Therefore, you must evaluate the feasibility of data compression on your RDS instance based on your business requirements. We recommend that you enable the data compression feature only on large tables.

- Defragment indexes

If the degree of fragmentation in an index is high, the underlying data of the index consumes an abnormally large amount of storage space. In this case, you can defragment the index to reduce the amount of used data storage space.

Log on to the ApsaraDB RDS console and choose **CloudDBA > Performance Optimization**. Then, click the **Index Usage** tab. On this tab, you can view the index fragmentation in various tables. In addition, you can view the suggestions that are proposed by CloudDBA to rebuild or reorganize indexes.

- Rebuild an index


This method is suitable if the degree of fragmentation is high. By default, when you rebuild an index, the table on which the index is created is locked during the rebuild process. If your RDS instance runs an Enterprise Edition of SQL Server, you can set the **ONLINE** parameter to **ON**. This allows you to prevent a long-term lock on the table.

- Reorganize an index

This method is suitable if the degree of fragmentation is low. However, the optimization effect is not as good as the optimization effect of the index rebuilding method.

The degree of fragmentation in an index represents the percentage of pages whose logical ordering does not match the physical ordering inside the index. This percentage is different from the percentage of idle storage space in index pages. In normal cases, an index with a high degree of fragmentation is likely to be defragmented to reclaim storage space.

If you want to analyze the average percentage of idle storage space per page in an index, you can query the `sys.dm_db_index_physical_stats` system view in **SAMPLED** or **DETAILED** mode. Then, you can view the values in the `avg_page_space_used_in_percent` column of the return result. For more information, see [sys.dm_db_index_physical_stats \(Transact-SQL\)](#).

 **Note** ApsaraDB RDS needs to read a large number of index pages during queries. If you defragment indexes during queries, the performance of your RDS instance may decrease. We recommend that you defragment indexes during off-peak hours.

Index defragmentation is suitable only for archived data tables that are updated at a low frequency. If frequent insert and update operations are performed on a data table, the degrees of fragmentation in the indexes on the data table significantly increase. In addition, if you rebuild or reorganize the indexes on the data table, a large number of transaction logs are generated. This increases the amount of used log storage.

If the available storage space is still insufficient after you have tried all the suggested solutions, you can run the `DBCC SHRINKFILE` command to compress data files. This way, the unallocated data storage space is released to the operating system.

Fileid	FileGroup	TotalExtents	UsedExtents	Name	FileName
1	1	1673344	1313432	db02	E:\SQLDATA\DATA\

In the preceding figure, the size per extent is 64 KB. Therefore, the total data storage space is 104,584 MB, and the allocated data storage space is 82,089 MB. This means that the total size of the compressed data files is greater than or equal to 82,089 MB. If you want to reduce the total data storage space to 90,000 MB, run the following command:

```
DBCC SHRINKFILE(1, 90000)
```

For more information, see [Shrink a Database](#) and [DBCC SHRINKFILE \(Transact-SQL\)](#).

Reclaim log storage space

Run the `DBCC SQLPERF (LOGSPACE)` command or use CloudDBA to view the percentage of used log storage space. If the percentage is high, the amount of storage space that you can release by compressing log files is small. In this case, you can query the `sys.databases` system view. Then, you can view the values in the `log_reuse_wait` and `log_reuse_wait_desc` columns of the return result. This provides further details about why you cannot reclaim log storage space.

Note For more information about the values in the `log_reuse_wait` and `log_reuse_wait_desc` columns, see [sys.databases \(Transact-SQL\)](#).

In most cases, you do not need to manually compress log files. ApsaraDB RDS compresses log files every time when an automatic backup is complete. If you need to reduce the amount of used log storage space by compressing log files at your earliest opportunity, you can perform the following steps: Log on to the ApsaraDB RDS console and go to the **Backup and Restoration** page. In the upper-right corner of the page, click **Shrink Transaction Log**. Then, ApsaraDB RDS starts to back up all transaction logs and compress log files. For example, if the available storage space of your RDS instance is abnormally low due to an increase in log storage consumption and you cannot wait until the next automatic backup, you can perform these steps.

Note The compression of log files starts only after the backup of transaction logs is complete. If ApsaraDB RDS needs to back up a large number of transaction logs, you must wait for a long period of time before ApsaraDB RDS can complete the compression.

Reclaim temporary file storage space

- Analysis

The temporary file storage space is the amount of storage space that is used by the tempdb system database. The tempdb system database uses only the SIMPLE recovery model. In normal cases, the total size of log files in the tempdb system database is small. However, the total size of data files in the tempdb system database can significantly increase within a short period of time. For example, if you create a large number of temporary tables, join large tables, or sort data, the total size of data files in the tempdb system database increases.

- Solution

- Try to prevent storage consumption increases at the application level. For example, reduce unnecessary temporary tables, reduce queries that require the joins of large tables, and do not run large transactions.
- Restart your RDS instance during off-peak hours. After the restart, the amount of storage space that is used by the tempdb system database decreases to the size at the time when the instance was created.

Reclaim system file storage space

- Analysis

The system file storage space is the total amount of storage space that is used by the files in the master, msdb, and model system databases and some files in the system directories. In most cases, these files are small. However, these files can consume a large amount of storage space in the following scenarios:

- A large number of error logs are generated. In this case, the total size of error log files increases to a few GB or more.
- Memory dump files are generated in the event of severe exceptions.

- Solution

You cannot obtain the storage space that is used by various system files. If an abnormally large amount of storage space is used by system files, you can submit a to contact after-sales technical support.

Expand storage capacity

If the storage usage of your RDS instance is still abnormally high after you have tried all the suggested solutions, you can expand the storage capacity of the instance. For more information, see [Change the specifications of an ApsaraDB RDS for SQL Server instance](#).

23.4. Introduction to CloudDBA in ApsaraDB RDS for SQL Server

This topic describes CloudDBA in ApsaraDB RDS for SQL Server. CloudDBA is used to identify and diagnose issues on your RDS instance. CloudDBA uses AI algorithms to fix these issues and optimize your RDS instance.

Limits

CloudDBA is supported only in the following regions: China (Hangzhou), China (Shanghai), China (Qingdao), China (Beijing), China (Zhangjiakou), China (Hohhot), China (Ulanqab), China (Shenzhen), China (Heyuan), China (Chengdu), China (Hong Kong), and Singapore (Singapore).

Features

CloudDBA provides the following features:

- **View the storage information of an ApsaraDB RDS for SQL Server instance**

This feature allows you to monitor and analyze your storage at the instance level, database level, and table level. The storage monitoring and analysis data help you identify and troubleshoot storage issues. The Storage Management page in the ApsaraDB RDS console includes the following sections:

- **Storage Overview:** This section provides an overview of the storage information. The storage information includes the changes in storage space over the last week, the available storage space, the used storage space, and the estimated increase in storage consumption.
- **Charts of Storage Information:** This section displays the storage consumption of your RDS instance in charts. The storage consumption includes the storage usage, the percentages of used data storage space and used log storage space, and the top 5 databases that consume the most storage space.
- **Storage Trend:** This section displays the storage trends of your RDS instance in a chart.
- **Top 10 Databases:** This section displays the details about the top 10 databases that consume the most storage space. These details are displayed in a table.
- **Top 20 Data Tables:** This section displays the details about the top 20 data tables that consume the most storage space. These details are displayed in a table.

- **Performance Optimization**

This feature provides various important performance data about your RDS instance. The Performance Optimization page in the ApsaraDB RDS console includes the following tabs:

- **Performance Insight:** This tab displays the performance metrics of your RDS instance. You can use the metrics to find the sources of performance issues and improve the stability of your RDS instance.
- **Missing Indexes:** This tab displays the details about the missing indexes in charts and tables. This tab also displays the SQL statements that are used to create these indexes.
- **Index Usage:** This tab displays the details about the created indexes in charts and tables. This tab also displays the SQL statements that are used to create these indexes.
- **Statistics:** This tab displays the performance statistics of your RDS instance in charts and tables.
- **TOP SQL:** This tab displays the details about the SQL statements that are executed on your RDS instance. The SQL statements are sorted based on different metrics, and the SQL statement statistics are displayed in charts and tables. You can query real-time SQL statement statistics.
- **TOP Objects:** This tab displays the real-time performance drains that are caused by various objects, such as stored procedures, functions, and triggers. You can identify the top N objects that cause the highest performance drain and the SQL statements in these objects.

- **Lock optimization**

This feature provides various important performance data about your RDS instance. The Lock Optimization page in the ApsaraDB RDS console includes the following tabs:

- **DeadLock:** This tab displays the details about the deadlocks that are detected in your RDS instance. The details are displayed in charts and tables.

- **Blocking**: This tab displays the details about the blocking problems that are detected in your RDS instance. The details are displayed in charts and tables.
- **Slow SQL**: This tab displays and analyzes the SQL statements with high CPU utilization. This tab also displays the slow SQL query statistics and the slow SQL query details.

23.5. View the storage information of an ApsaraDB RDS for SQL Server instance

This topic describes how to view the storage information of an ApsaraDB RDS for SQL Server instance by using CloudDBA. CloudDBA provides the storage management feature. This feature allows you to monitor and analyze your storage consumption at three levels: instance, database, and table. You can identify and troubleshoot storage issues based on the storage monitoring and analysis data.

The storage management feature provides the basic information, storage overview, storage details, and storage trends of your RDS instance from various dimensions.

Prerequisites

The RDS instance does not run SQL Server 2008 R2 with standard SSDs or enhanced SSDs (ESSDs).

Procedure

- 1.
2. In the left-side navigation pane, choose **CloudDBA > Storage Management**. Then, you can view the following sections:
 - **Basic information**: This section displays the basic information about your RDS instance. The basic information includes the ID, edition, and start time of your RDS instance. The following table describes the parameters in the basic information section. Parameters in the basic information section

Parameter	Description
Instance ID	The unique identifier of your RDS instance.
Edition	The SQL Server major version, edition, minor version, and patch number of your RDS instance. These four parts are separated by hyphens (-).
Start Time	The last time when your RDS instance was started.
Product Updates	The entry point to the official ApsaraDB RDS documentation.

Storage Man... Instance ID: rm-4p4t5gk4rby77 Edition: SQL Server 2017 - Enterprise Edition: Case-based Licensing (CAL) - 14.0.3333.3 - RTM Start Time: 2024-09-09 10:00:00 > Product Updates

- **Storage Overview**: This section provides an overview of the storage information about your RDS instance. The storage information includes storage changes over the last week, the available storage, the used storage, and the estimated increase in storage consumption. The following table describes the parameters in the Storage Overview section. Parameters in the Storage Overview section

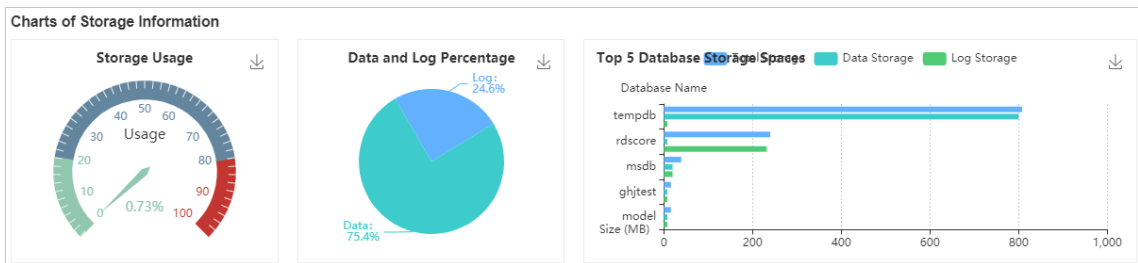
Parameter	Description
Changes in the Last Week	<p>The storage change and average daily storage consumption increase of your RDS instance over the last week.</p> <p>Note A negative value indicates a decrease in storage consumption.</p>
Available Storage	The amount of storage that is available and the number of days for which the storage remains available on your RDS instance.
Used Storage	The amount of storage that is used and the number of days for which the storage is used on your RDS instance.
Estimated to Reach	The estimated number of days for the storage usage of your RDS instance to reach 80% and 100%. The estimate is based on your storage consumption history.
Data Updated At	The time when the storage information of your RDS instance was generated.
Recollect Data	<p>If the storage information is outdated, click Recollect Data. In the message that appears, click OK. ApsaraDB RDS starts to collect the storage information again.</p> <p>Note After a few minutes, you can refresh the Storage Management page to view the new storage information.</p>
Save as PDF File	If you want to save the storage information to your computer as a file, click Save as PDF File .



- o **Charts of Storage Information:** This section displays the information about the storage consumption of your RDS instance in charts. The storage consumption information includes the storage usage, the percentages of used data storage and used log storage, and the top 5 databases that consume the most storage. The following table describes the parameters in the Charts of Storage Information section. Parameters in the Charts of Storage Information section

Parameter	Description
Storage Usage	The storage usage of your RDS instance. ApsaraDB RDS displays the storage usage in a dashboard. If the storage usage exceeds 80%, you can expand the storage capacity of your RDS instance or delete the data that is no longer required. For more information, see Change the specifications of an ApsaraDB RDS for SQL Server instance .

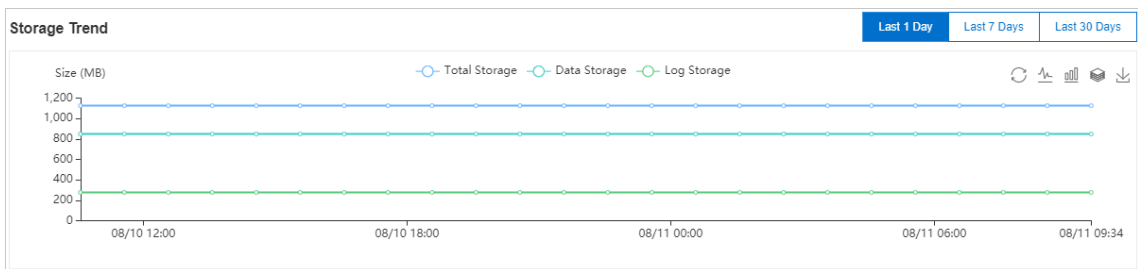
Parameter	Description
Data and Log Percentage	The percentage of the used data storage and the percentage of the used log storage in your RDS instance. ApsaraDB RDS displays the percentages in a pie chart. If the percentage of the used storage space is abnormally high, you may need to compress logs or enable the 30-minute log backup feature in the ApsaraDB RDS console. For more information, see Enable snapshot backups for an ApsaraDB RDS for SQL Server instance .
Top 5 Database Storage Spaces	<p>The amount of storage used by each of the top 5 databases that consume the most storage. ApsaraDB RDS displays the following information about the used storage in a column chart:</p> <ul style="list-style-type: none"> ■ Total Storage (Unit: MB) ■ Data Storage (Unit: MB) ■ Log Storage (Unit: MB)



o Storage Trend

This section displays the storage trends of your RDS instance over the last day, the last week, or the last month in a line chart. The storage information includes the total storage, the data storage, and the log storage.

Note This feature is new. It cannot be used to collect the storage information that was generated before this feature is released.



o Top 10 Databases: This section displays the details about the top 10 databases that consume the most storage. These details are displayed in a table. The following table describes the parameters in the Top 10 Databases section. Parameters in the Top 10 Databases section

Parameter	Description
Database Name	The name of the database.
Status	The status of the database.

Parameter	Description
Total Storage (MB)	The total amount of storage that is allocated to the database.
Used Storage (MB)	The amount of storage that is used by the database and the percentage of the used storage in the total storage for the database.
Available Storage (MB)	The amount of storage that is available to the database and the percentage of the available storage in the total storage for the database.
Restoration Mode	The mode that is used to restore the database. <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p>? Note In most cases, if the database is not a system database, the FULL recovery model is used.</p> </div>
Collation	The character set collation that is used for the database.
Log Reuse Wait	The description of the Log Reuse Wait event in the database.
Creation Time	The time when the database was created.
System Database	Indicates whether the database is a system database.

Top 10 Databases								Search <input type="text" value=""/>
	#	Database Name (Click to View Database Changes)	Status	Total Storage (MB)	Used Storage (MB)	Available Storage (MB)	Restoration Mode	Collation
+	1	tempdb	ONLINE	<div style="width: 100%;"><div style="width: 61.93%;"></div></div> 608	500.36 61.93%	307.64 38.07%	SIMPLE	Chinese_PRC_CI_AS
+	2	rdscore	ONLINE	<div style="width: 100%;"><div style="width: 82.22%;"></div></div> 240	197.33 82.22%	42.67 17.78%	FULL	Chinese_PRC_CI_AS
+	3	msdb	ONLINE	<div style="width: 100%;"><div style="width: 54.97%;"></div></div> 39.26	21.58 54.97%	17.68 45.03%	SIMPLE	Chinese_PRC_CI_AS

You can find a database and click the plus sign (+) on the left to view the details about the files in the database. The following table describes the parameters of the files in a database.

Parameters of the files

Parameter	Description
Database Name	The name of the database to which the file belongs.
File Group	The name of the file group to which the file belongs. <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p>? Note If the file is a log file, it does not belong to a file group. In this case, this parameter is empty.</p> </div>
File Type	The type of the file. Valid values: Data and Log.
File Name	The name of the file.
Total Storage (MB)	The total amount of storage that is allocated to the file.
Used Storage (MB)	The amount of storage that is used by the file and the percentage of the used storage in the total storage for the file.

Parameter	Description
Available Storage (MB)	The amount of storage that is available to the file and the percentage of the available storage in the total storage for the file.
Maximum File Size	The maximum size of the file. Unit: MB. <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;"> ? Note The value 0 indicates that the size of the file is not limited. </div>
Automatic File Growth	The increment at which the storage that is allocated to the file increases. In most cases, the storage increases based on a percentage or a fixed size.

Top 10 Databases Search Q

#	Database Name (Click to View Database Changes)	Status	Total Storage (MB)	Used Storage (MB)	Available Storage (MB)	Restoration Mode	Collation	Lo
1	tempdb	ONLINE	808	500.36 61.93%	307.54 38.07%	SIMPLE	Chinese_PRC_CLAS	NC

Database Name	File Group	File Type	File Name	Total Storage (MB)	Used Storage (MB)
tempdb		Log	templog	8	1.66 20.7%
tempdb	PRIMARY	Data	tempdev2	100	61.06 61.06%
tempdb	PRIMARY	Data	tempdev4	100	57.75 57.75%
tempdb	PRIMARY	Data	tempdev5	100	65.44 65.44%
tempdb	PRIMARY	Data	tempdev3	100	65.63 65.63%
tempdb	PRIMARY	Data	tempdev1	100	63.38 63.38%
tempdb	PRIMARY	Data	tempdev6	100	62.25 62.25%
tempdb	PRIMARY	Data	tempdev	100	61.75 61.75%
tempdb	PRIMARY	Data	tempdev7	100	61.44 61.44%

- o Top 20 Data Tables: This section displays details about the top 20 data tables that consume the most storage. These details are displayed in a table. The following table describes the parameters in the Top 20 Data Tables section. Parameters in the Top 20 Data Tables section

Parameter	Description
Table Name	The name of the data table. The value of this parameter consists of the following parts: <ul style="list-style-type: none"> ■ Database name ■ Schema name ■ Object name
Retained Size (MB)	The total amount of storage that is allocated to the data table.
Data Storage (MB)	The amount of storage that is used by the data in the data table and the percentage of the used storage in the total storage for the data table.
Index Storage (MB)	The amount of storage that is used by the indexes on the data table and the percentage of the used storage in the total storage for the data table.
Unused Storage (MB)	The amount of storage that is available to the data table and the percentage of the available storage in the total storage for the data table.
Rows	The total number of rows in the data table.
Indexes	The number of indexes in the data table.

Parameter	Description
Creation Time	The time when the data table was created.

23.6. Performance optimization

23.6.1. View the index usage statistics of an ApsaraDB RDS for SQL Server instance

This topic describes how to view the index usage statistics of an ApsaraDB RDS for SQL Server instance by using CloudDBA in the ApsaraDB RDS console. The index statistics include the usage of indexes and the degrees of fragmentation in indexes.

Prerequisites

The RDS instance does not run SQL Server 2008 R2 with standard SSDs or enhanced SSDs (ESSDs).


Procedure

- 1.
2. In the left-side navigation pane, choose **CloudDBA > Performance Optimization**.
3. Click the **Index Usage** tab.

Introduction to the Index Usage tab

- **Index Overview:** This section provides an overview of the index usage statistics of the RDS instance. The following table describes the parameters in the Index Overview section

Parameter	Description
Total Indexes	The total number of indexes that are created in the RDS instance.
Total Index Storage	The amount of storage space that is used by all indexes in the RDS instance.
Fragmentation Percentage Exceeds 30%	The number of indexes whose degrees of fragmentation exceed 30%.
Index Seeks Less Than 100	The number of indexes on which the number of search operations is smaller than 100.
Data Updated At	The time at which the index usage statistics of the RDS instance were generated.

Parameter	Description
Recollect Data	<p>If the index usage statistics are outdated, click Recollect Data. In the message that appears, click OK. ApsaraDB RDS starts to collect the index usage statistics of the RDS instance again.</p> <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;"> <p> Note After a few minutes, you can refresh the Performance Optimization page to view the updated index usage statistics.</p> </div>
Save as PDF File	If you want to save the index usage statistics of the RDS instance to your computer as a file, click Save as PDF File .

- **Charts of Index Information:** This section displays the index usage statistics of the RDS instance in charts. The following table describes the parameters in the Charts of Index Information section. Parameters in the Charts of Index Information section

Parameter	Description
Fragmentation Percentage	The distribution of the degrees of fragmentation in all indexes.
Usage	The distribution of the usage of all indexes.
Storage Changes	The changes to the amount of storage space that is used by all indexes.
Top Fragmentation Percentage	The degrees of fragmentation in the top 10 clustered indexes and nonclustered indexes that have the highest degree of fragmentation.

- **Index Information:** This section displays the details about the usage of all indexes in the RDS instance. The following table describes the parameters in the Index Information section. Parameters in the Index Information section

Parameter	Description
Table Name	<p>The name of the table on which the index is created. The value of this parameter consists of the following three parts:</p> <ul style="list-style-type: none"> ◦ Database name ◦ Schema name ◦ Object name
Index Name	The name of the index.
Fragmentation Percentage	The degree of fragmentation in the index.
Size (MB)	The amount of storage space that is used by the index.
Maintenance Operation	The maintenance operation that is recommended for the index.
Reason	The reason why the maintenance operation is recommended for the index.

Parameter	Description
Priority	The priority of the maintenance operation.
Pages	The number of pages that are occupied by the index.
Seeks	The number and percentage of search operations that are performed based on the index.
Scans	The number and percentage of scan operations that are performed based on the index.
Bookmark Lookups	The number and percentage of key lookup operations that are performed based on the index.
Update	The number and percentage of update operations that are performed on the index.
Primary Key	Indicates whether the index is a primary key index.
Disable	Indicates whether the index is disabled.
Column	The columns on which the index is created.
Fill Factor	The fill factor of the index.
Creation Time	The time at which the index was created.
Statistics Update Time	The most recent time at which the statistics of the index were updated.
Export Script	The button that is used to export the SQL statements that were used to create the index.
Export File	The button that is used to export the usage of the index as an Excel, CSV, or TXT file.

23.6.2. View the performance statistics of an ApsaraDB RDS for SQL Server instance

This topic describes how to view the performance statistics of an ApsaraDB RDS for SQL Server instance by using CloudDBA in the ApsaraDB RDS console. CloudDBA allows you to query the performance statistics over a specific time range, view the performance statistics in histograms, and update the performance statistics. You can identify and resolve the performance issues of the RDS instance based on the performance statistics to ensure the high performance of the instance.

Prerequisites

The RDS instance does not run SQL Server 2008 R2 with standard SSDs or enhanced SSDs (ESSDs).


Procedure

- 1.

2. In the left-side navigation pane, choose **CloudDBA > Performance Optimization**.
3. Click the **Statistics** tab.

Introduction to the Statistics tab

- **Statistics Overview:** This section provides an overview of the performance statistics of the RDS instance. The following table describes the parameters in the Statistics Overview section. Parameters in the Statistics Overview section

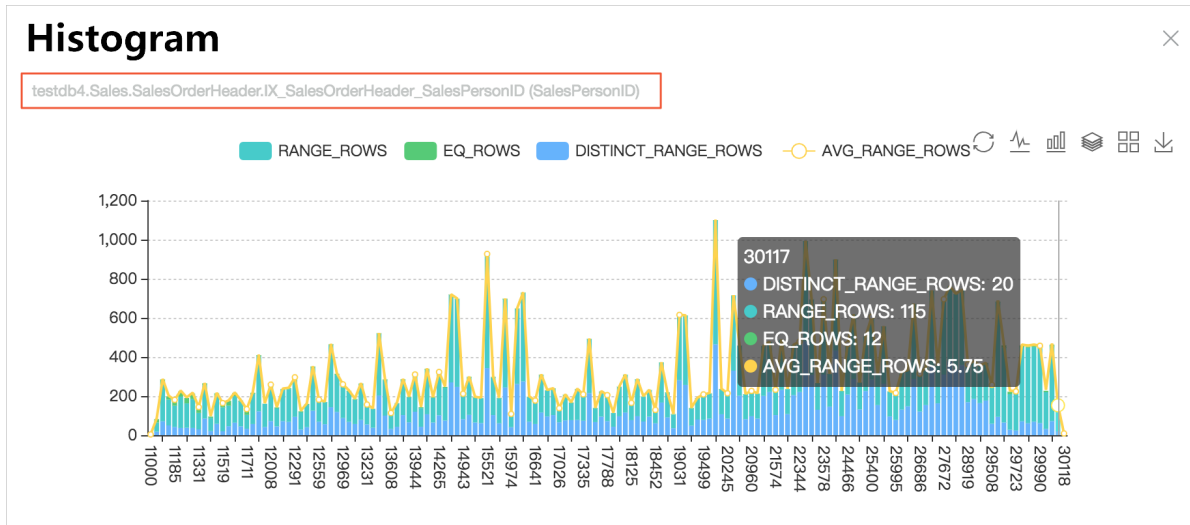
Parameter	Description
Total Statistics	The total number of statistical items that are collected from the RDS instance.
Not Updated for More Than 7 Days	The number of statistical items that are not updated for more than seven days in the RDS instance.
Not Updated for More Than 14 Days	The number of statistical items that are not updated for more than 14 days in the RDS instance.
Not Updated for More Than 30 Days	The number of statistical items that are not updated for more than 30 days in the RDS instance.
Data Updated At	The time at which the performance statistics of the RDS instance were generated.
Recollect Data	<p>If the performance statistics are outdated, click Recollect Data. In the message that appears, click OK. ApsaraDB RDS starts to collect the performance statistics of the RDS instance again.</p> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #d9e1f2;"> <p> Note After a few minutes, you can refresh the Performance Optimization page to view the updated performance statistics.</p> </div>
Save as PDF File	If you want to save the performance statistics of the RDS instance to your computer as a file, click Save as PDF File .

- **Statistics Not Updated:** This section uses charts to display the number of statistical items that are not updated in the RDS instance. The following table describes the parameters in the Statistics Not Updated section. Parameters in the Statistics Not Updated section

Parameter	Description
Statistics Not Updated	This column chart displays the numbers of the statistical items that are not updated for more than 1 day, 7 days, 14 days, and 30 days.
Statistics Not Updated in Percentages	This pie chart shows the percentages of the statistical items that are not updated for more than 1 day, 7 days, 14 days, and 30 days.

- **Statistics table:** This table displays the details about all statistical items that are collected from the RDS instance. The following table describes the parameters for a statistical item in the statistics table. Parameters in the statistics table

Parameter	Description
Table Name	The name of the table from which the statistical item is collected. The value of this parameter consists of the following three parts: <ul style="list-style-type: none"> Database name Schema name Object name
Statistics Name	The name of the statistical item.
Column Name	The name of the column from which the statistical item is collected.
Last Update Time.	The most recent time at which the statistical item was updated. If the statistical item is not updated for more than 14 days, we recommend that you manually update the statistical item.
Actions	Includes two operations: Obtain Histogram and Update. <ul style="list-style-type: none"> Obtain Histogram: You can click Obtain Histogram in the Actions column to view the distribution of the statistics about the statistical item. Update: You can click Update in the Actions column to view the updated statistics about the statistical item.



The following conclusions can be made from the histogram that is shown in the preceding figure:

The statistics about the IX_SalesOrderHeader_SalesPersonID index, which is created on the SalesPersonID column of the testdb4.Sales.SalesOrderHeader table, are unevenly distributed. The value of the AVG_RANG_ROWS metric of the index abruptly increases and decreases possibly due to data skew issues. You must update the statistics about the index. To do so, you need only to click **Update** in the Actions column of the index.

23.6.3. View the SQL statement statistics of an ApsaraDB RDS for SQL Server instance

This topic describes how to view the SQL statement statistics of an ApsaraDB RDS for SQL Server instance by using CloudDBA in the ApsaraDB RDS console. CloudDBA allows you to view real-time SQL statement statistics. You can identify the performance issues of the RDS instance based on the statistics.

Prerequisites

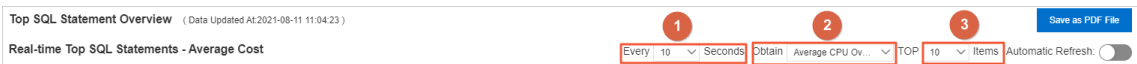
The RDS instance does not run SQL Server 2008 R2 with standard SSDs or enhanced SSDs (ESSDs).

Procedure

- 1.
2. In the left-side navigation pane, choose **CloudDBA > Performance Optimization**.
3. Click the **TOP SQL** tab.
 - o Query real-time SQL statements based on different metrics. Specify the criteria based on which you want to sort SQL statements. Then, turn on **Automatic Refresh**.

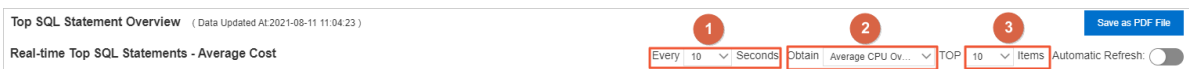
Note

- The statistics of real-time top SQL statements for the RDS instance are based on the data in the cache after the RDS instance is started. When a new SQL statement or an existing SQL statement is executed, the data in the cache is simultaneously updated. You can check the last execution time of the SQL statement in the **Last Execution Time** column of the table that is displayed in the **Real-time Top SQL Statements - List** section.
- In the table that is displayed in the **Real-time Top SQL Statements - List** section, you can click an SQL statement in the **Statement** or **SQL Block** column. In the dialog box that appears, you can click **Copy** to copy the SQL statement.

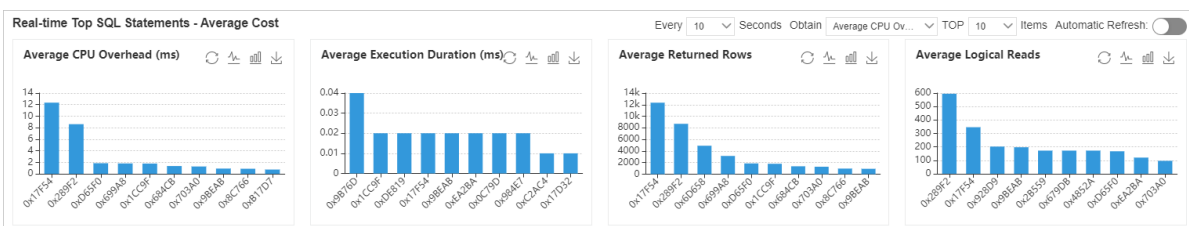


Introduction to the Top SQL tab

- **Top SQL Statement Overview:** This section displays the most recent time at which the SQL statement statistics were updated and allows you to specify the SQL statement statistics that you want to view.



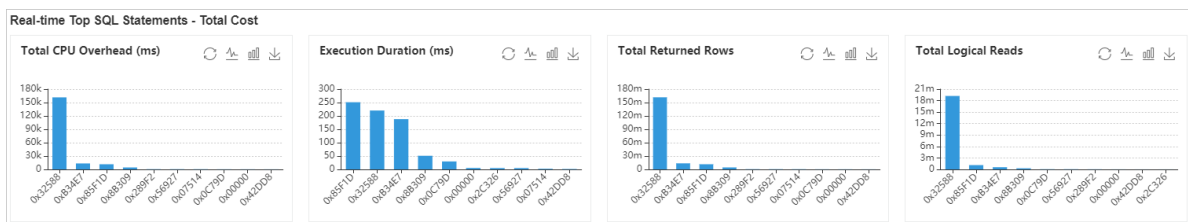
- **Real-time Top SQL Statements - Average Cost:** This section displays the SQL statements that consume the most resources on average based on the following six metrics: Average CPU Overhead, Average Execution Duration, Average Returned Rows, Average Logical Reads, Average Physical Reads, and Average Logical Writes. The following table describes the parameters in the Real-time Top SQL Statements - Average Cost section.



Parameters in the Real-time Top SQL Statements - Average Cost section

Parameter	Description
Average CPU Overhead	Sorts SQL statements based on the average CPU overhead per execution of each SQL statement. Unit: milliseconds.
Average Execution Duration	Sorts SQL statements based on the average running time per execution of each SQL statement. Unit: milliseconds.
Average Returned Rows	Sorts SQL statements based on the average number of rows that were returned per execution of each SQL statement.
Average Logical Reads	Sorts SQL statements based on the average number of logical read operations that were performed per execution of each SQL statement.
Average Physical Reads	Sorts SQL statements based on the average number of physical read operations that were performed per execution of each SQL statement.
Average Logical Writes	Sorts SQL statements based on the average number of logical write operations that were performed per execution of each SQL statement.

- Real-time Top SQL Statements - Total Cost:** This section displays the SQL statements that consume the most resources in total based on the following six metrics: Total CPU Overhead, Execution Duration, Total Returned Rows, Total Logical Reads, Total Physical Reads, and Total Executions. The following table describes the parameters in the Real-time Top SQL Statements - Total Cost section.



Parameters in the Real-time Top SQL Statements - Total Cost section

Parameter	Description
Total CPU Overhead	Sorts SQL statements based on the total CPU overhead of each SQL statement. Unit: milliseconds.
Execution Duration	Sorts SQL statements based on the total running time of each SQL statement. Unit: milliseconds.
Total Returned Rows	Sorts SQL statements based on the total number of rows that were returned for each SQL statement.
Total Logical Reads	Sorts SQL statements based on the total number of logical read operations that were performed for each SQL statement.
Total Physical Reads	Sorts SQL statements based on the total number of physical read operations that were performed for each SQL statement.
Total Executions	Sorts SQL statements based on the total number of times that each SQL statement was executed.

- Real-time Top SQL Statements - List:** This section displays the real-time SQL statements that consume

the most resources based on different metrics. The following table describes the parameters in the Real-time Top SQL Statements - List section.

Real-time Top SQL Statements - List										Search	Q
#	ID	Statement (Click to View Details)	SQL Block (Click to View Details)	Databases	Executions	Total CPU Time	Average CPU Time	Execution Duration	Average Execution		
1	0x17F5419F21BE1ECA	DELETE FROM msdb.d...	CREATE PROCEDURE...	msdb	1 1.03%	12 1.79%	12 39.05%	12 1.76%	12 37.2i		
2	0x289F236C4B451333	select db * from sys.dat...	select db * from sys.dat...	master	75 77.32%	645 95.98%	8 27.25%	651 95.74%	8 26.25f		
3	0xD65F053D3B11BC67	INSERT INTO @subsys...	CREATE PROCEDURE...	msdb	1 1.03%	1 0.15%	1 5.85%	1 0.15%	1 5.62%		
4	0x699A8F1165C31FA5	INSERT INTO @SELE...	-- Returns the V2 instan...	msdb	1 1.03%	1 0.15%	1 5.73%	3 0.44%	3 9.49%		
5	0x1CC9F7A6EEF1E313	INSERT INTO @media...	CREATE PROCEDURE...	msdb	1 1.03%	1 0.15%	1 5.66%	1 0.15%	1 5.44%		
6	0x684CB45F72C831F2	INSERT INTO @SELE...	-- Returns the V1 instan...	msdb	1 1.03%	1 0.15%	1 4.30%	1 0.15%	1 4.11%		
7	0x703A03D095D24F23	insert into [SS_u_SS_la...	use rdscore.truncate ta...	rdscore	1 1.03%	1 0.15%	1 4.05%	1 0.15%	1 3.87%		
8	0x9BEAB026E8B027B	DELETE msdb.dbo.bac...	CREATE PROCEDURE...	msdb	1 1.03%	0 0.00%	0 2.91%	0 0.00%	0 2.78%		
9	0x8C76E05FCD8C2B9	INSERT #! EXEC xp_fi...	CREATE PROCEDURE...	msdb	1 1.03%	0 0.00%	0 2.82%	0 0.00%	0 2.90%		
10	0xB17D7DD0414B6DCB	select name from sys.d...	use master;select name...	master	14 14.43%	10 1.49%	0 2.37%	10 1.47%	0 2.27%		

Parameters in the Real-time Top SQL Statements - List section

Parameter	Description
Databases	The name of the database on which the SQL statement was executed.
Statement	The SQL statement that was executed. You can click the SQL statement to view the details about the SQL statement.
SQL Block	The text content of the SQL statement. You can click the SQL statement to view the text content of the SQL statement.
Executions	The total number of times that the SQL statement was executed.
Total CPU Time	The total CPU overhead of the SQL statement.
Average CPU Time	The average CPU overhead per execution of the SQL statement.
Execution Duration	The total running time of the SQL statement.
Average Execution Duration	The average running time per execution of the SQL statement.
Total Returned Rows	The total number of rows that were returned for the SQL statement.
Average Returned Rows	The average number of rows that were returned per execution of the SQL statement.
Total Logical Reads	The total number of logical read operations that were performed for the SQL statement.
Average Logical Reads	The average number of logical read operations that were performed per execution of the SQL statement.
Total Physical Reads	The total number of physical read operations that were performed for the SQL statement.
Average Physical Reads	The average number of physical read operations that were performed per execution of the SQL statement.

Parameter	Description
Total Logical Writes	The total number of logical write operations that were performed for the SQL statement.
Average Logical Writes	The average number of logical write operations that were performed per execution of the SQL statement.
Last Execution Time	The most recent time at which the SQL statement was executed.

23.6.4. View the top N objects of an ApsaraDB RDS for SQL Server instance

This topic describes how to view the top N objects of an ApsaraDB RDS for SQL Server instance. These objects include stored procedures, functions, and triggers. You can identify and troubleshoot performance issues based on the object information.

Prerequisites

The RDS instance does not run SQL Server 2008 R2 with standard SSDs or enhanced SSDs (ESSDs).

Procedure

- 1.
2. In the left-side navigation pane, choose **CloudDBA > Performance Optimization**.
3. Click the **TOP Objects** tab.
4. In the upper-right corner of the tab, specify the **Database**, **Every XX Seconds**, **Obtain**, and **TOP XX Items** parameters. Then, turn on the **Automatic Refresh** switch.



Introduction to the TOP Objects tab

- **Top Object Overview:** This section displays the last update time of the object information and allows you to specify the object information that you want to view. The following table describes the parameters in the Top Object Overview section. Parameters in the Top Object Overview section

Parameter	Description
Database	The database whose objects you want to view. You can select more than one database.
Every XX Seconds	The interval at which ApsaraDB RDS updates the object information. This parameter takes effect only when you turn on the Automatic Refresh switch. Valid values: 5, 10, 30, and 60. Unit: seconds.
Obtain	The metric based on which ApsaraDB RDS sorts the objects of the selected database in real time. Valid values include Average CPU Overhead, Average Execution Duration, Total CPU Overhead, Total Logical Reads, and Total Physical Reads.

Parameter	Description
TOP XX Items	The number of objects that you want to view. Valid values: 5, 10, and 15.
Automatic Refresh	The switch that is used to control the automatic refresh feature.
Data Updated At	The time when the object information of your RDS instance was generated.
Save as PDF File	If you want to save the object information to your computer as a file, click Save as PDF File .

- **Real-time Top Objects - Average Cost:** This section displays the top N objects of your RDS instance based on four metrics. These metrics are Average CPU Overhead, Average Execution Duration, Average Logical Reads, and Average Returned Rows. The following table describes the parameters in the Real-time Top Objects - Average Cost section. Parameters in the Real-time Top Objects - Average Cost section

Parameter	Description
Average CPU Overhead	The average CPU overhead per statement execution for each object. Unit: milliseconds.
Average Execution Duration	The average running time per statement execution for each object. Unit: milliseconds.
Average Logical Reads	The average number of logical reads per statement execution for each object.
Average Returned Rows	The average number of rows that are returned per statement execution for each object.

- **Real-time Top Objects - Total Cost:** This section displays the top N objects of your RDS instance based on four metrics. These metrics are Total CPU Overhead Percentage, Total Execution Duration Percentage, Total Logical I/O Percentage, and Total Returned Rows Percentage. The following table describes the parameters in the Real-time Top Objects - Total Cost section. Parameters in the Real-time Top Objects - Total Cost section

Parameter	Description
Total CPU Overhead Percentage	The percentage of the total CPU overhead that is produced by statement executions on each object.
Total Execution Duration Percentage	The percentage of the total running time that is required by statement executions on each object.
Total Logical I/O Percentage	The percentage of the total logical I/O that is required by statement executions on each object.
Total Returned Rows Percentage	The percentage of the total number of rows that are returned by statement executions on each object.

- **Real-time Top Objects - List**

- This section provides an overview of the real-time performance drains for objects in the RDS instance. The following table describes the parameters for the overview of an object. Parameters for the overview of an object

Parameter	Description
Object Name	The name of the object. The value of this parameter consists of three parts: database name, schema name, and object name.
Object Type	The type of the object. Valid values: Stored Procedure, Function, and Trigger.
Total Executions	The total number of statement executions on the object after you restart your RDS instance or clear the cache.
Total CPU Overhead	The total CPU overhead for all statement executions on the object after you restart your RDS instance or clear the cache. Unit: milliseconds.
Average CPU Overhead	The average CPU overhead per statement execution on the object. Unit: milliseconds.
Total Execution Duration	The total running time of all statement executions on the object after you restart your RDS instance or clear the cache. Unit: milliseconds.
Average Execution Duration	The average running time per statement execution on the object. Unit: milliseconds.
Total Returned Rows	The total number of rows that are returned for all statement executions on the object after you restart your RDS instance or clear the cache.
Average Returned Rows	The average number of rows that are returned per statement execution on the object.
Total Logical Reads	The total number of logical reads on the object after you restart your RDS instance or clear the cache.
Average Logical Reads	The average number of logical reads per statement execution on the object.
Total Physical Reads	The total number of physical reads on the object after you restart your RDS instance or clear the cache.
Average Physical Reads	The average number of physical reads per statement execution on the object.
Total Logical Writes	The total number of logical writes on the object after you restart your RDS instance or clear the cache.
Average Logical Writes	The average number of logical writes per statement execution on the object.
Total Logical I/O	The total logical I/O for the object after you restart your RDS instance or clear the cache.
Average Logical I/O	The average logical I/O per statement execution on the object.

- This section also provides the details about the performance drain for each SQL statement on an

object. To view the details, you need to find the object on which the SQL statement is executed. Then, you need to click the plus sign (+) on the left. The following table describes the parameters for the details about an object. Parameters for the details about an object

Parameter	Description
Object Name	The name of the object on which the SQL statement is executed. The value of this parameter consists of three parts: database name, schema name, and object name.
Statement (View Details)	The details about the SQL statement. You can click this button to view the complete SQL statement.
Executions	The total number of times that the SQL statement is executed.
Obtain Query Plan	The number of times that ApsaraDB RDS obtains the execution plan of the SQL statement.
Total CPU Overhead	The total CPU overhead of the SQL statement. Unit: milliseconds.
Average CPU Overhead	The average CPU overhead per execution of the SQL statement. Unit: milliseconds.
Minimum CPU Overhead	The minimum CPU overhead among all executions of the SQL statement. Unit: milliseconds.
Maximum CPU Overhead	The maximum CPU overhead among all executions of the SQL statement. Unit: milliseconds.
Last CPU Overhead	The CPU overhead for the last execution of the SQL statement. Unit: milliseconds.
Total Execution Duration	The total running time of the SQL statement. Unit: milliseconds.
Average Execution Duration	The average running time per execution of the SQL statement. Unit: milliseconds.
Minimum Execution Duration	The minimum running time among all executions of the SQL statement. Unit: milliseconds.
Maximum Execution Duration	The maximum running time among all executions of the SQL statement. Unit: milliseconds.
Last Execution Duration	The running time for the last execution of the SQL statement. Unit: milliseconds.
Total Returned Rows	The total number of rows that are returned for the SQL statement.
Average Returned Rows	The average number of rows that are returned per execution of the SQL statement.
Minimum Returned Rows	The minimum number of rows that are returned among all executions of the SQL statement.

Parameter	Description
Maximum Returned Rows	The maximum number of rows that are returned among all executions of the SQL statement.
Last Returned Rows	The number of rows that are returned for the last execution of the SQL statement.
Total Logical Reads	The total number of logical reads that are run for the SQL statement.
Average Logical Reads	The average number of logical reads that are run per execution of the SQL statement.
Minimum Logical Reads	The minimum number of logical reads that are run among all executions of the SQL statement.
Maximum Logical Reads	The maximum number of logical reads that are run among all executions of the SQL statement.
Last Logical Reads	The number of logical reads that are run for the last execution of the SQL statement.
Total Physical Reads	The total number of physical reads that are run for the SQL statement.
Average Physical Reads	The average number of physical reads that are run per execution of the SQL statement.
Minimum Physical Reads	The minimum number of physical reads that are run among all executions of the SQL statement.
Maximum Physical Reads	The maximum number of physical reads that are run among all executions of the SQL statement.
Last Physical Read	The number of physical reads that are run for the last execution of the SQL statement.
Total Logical Writes	The total number of logical writes that are run for the SQL statement.
Average Logical Writes	The average number of logical writes that are run per execution of the SQL statement.
Minimum Logical Writes	The minimum number of logical writes that are run among all executions of the SQL statement.
Maximum Logical Writes	The maximum number of logical writes that are run among all executions of the SQL statement.
Last Logical Writes	The total number of logical writes that are run for the last execution of the SQL statement.
Total Logical I/O	The total logical I/O for the SQL statement.
Average Logical I/O	The average logical I/O per execution for the SQL statement.
Minimum Logical I/O	The minimum logical I/O among all executions of the SQL statement.

Parameter	Description
Maximum Logical I/O	The maximum logical I/O among all executions of the SQL statement.
Last Logical I/O	The logical I/O for the last execution of the SQL statement.
Last Execution Duration	The running time for the last execution of the SQL statement.

23.7. Lock optimization

23.7.1. View the deadlock statistics of an ApsaraDB RDS for SQL Server instance

This topic describes how to view the deadlock statistics of an ApsaraDB RDS for SQL Server instance by using CloudDBA in the ApsaraDB RDS console.

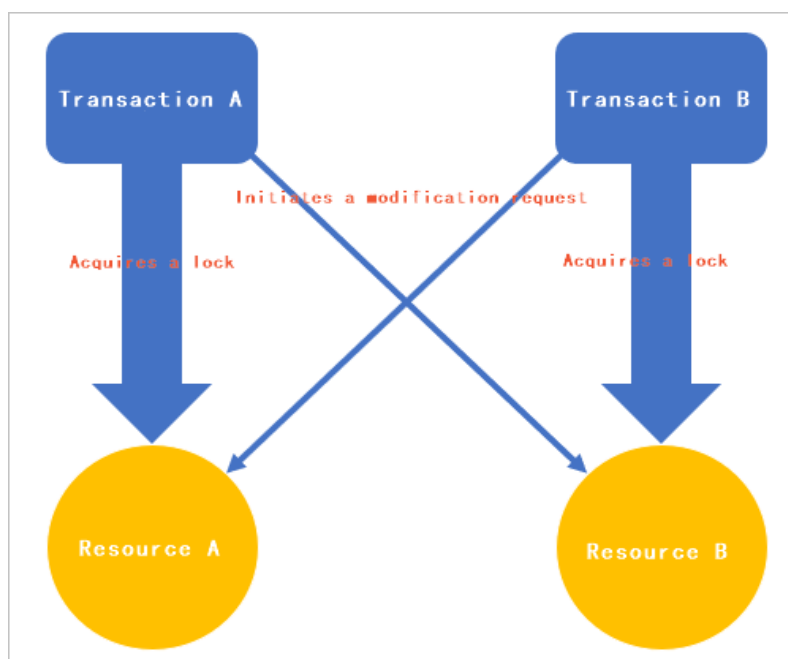
Prerequisites

The RDS instance does not run SQL Server 2008 R2 with standard SSDs or enhanced SSDs (ESSDs).

Context

When you run a transaction to modify a specific resource, the resource is locked to prevent modifications from other concurrent transactions. This ensures data consistency.

In most cases, a deadlock occurs when multiple transactions compete for the same resource. In the following example, when Transaction A is modifying Resource A, it also initiates a request to modify Resource B, which is being modified by Transaction B. This situation triggers a deadlock.



To resolve the deadlock, SQL Server terminates the transaction that can be rolled back at a lower cost than the other transaction. If you want to complete the task in the terminated transaction, you must run the transaction again.

ApsaraDB RDS provides the statistics of various deadlocks in the ApsaraDB RDS console. The deadlock statistics include the details about the start time of the blocking and blocked transactions, the IDs of the blocking and blocked sessions, the locked resources, and the types of deadlocks that occur. You can identify the problem SQL statements and other exceptions that cause the deadlocks and optimize your RDS instance to resolve the deadlocks.

Deadlock types

ApsaraDB RDS can analyze the following types of deadlocks:

- KeyDeadlock
- ObjectDeadLock
- RIDDeadlock
- PageDeadlock
- ComplieDeadlock

For more information about each type of deadlock, see [Lock Granularity and Hierarchies](#).

Lock modes

ApsaraDB RDS for SQL Server locks resources by using different lock modes that determine how the resources are accessed by concurrent transactions. The lock mode that is used to lock the resource accessed by a transaction varies based on the type of operation required by the transaction. ApsaraDB RDS for SQL Server supports the following lock modes:

- Shared (S): After a transaction acquires a shared lock on a resource, the resource can only be read but cannot be modified until the transaction releases the shared lock.
- Update (U): After a transaction acquires an update lock on a resource, the resource cannot be modified by another transaction until the transaction acquires an exclusive lock on the resource.
- Exclusive (X): After a transaction acquires an exclusive lock on a resource, the resource cannot be accessed by another transaction until the transaction releases the exclusive lock.

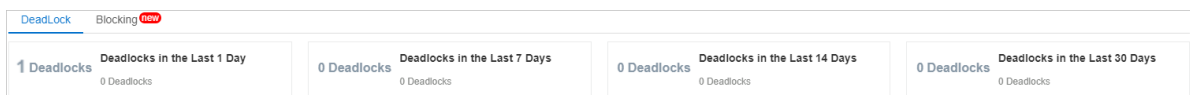
For more information about lock modes, see [Lock Modes](#).

Procedure

- 1.
2. In the left-side navigation pane, choose **CloudDBA > Lock Optimization**.

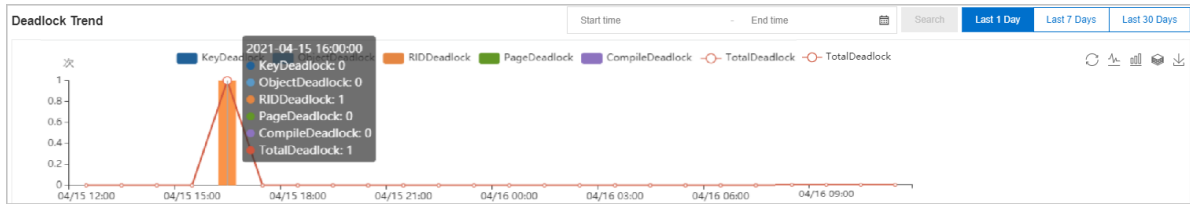
Introduction to the Deadlock tab

- Number of deadlocks



This section displays the number of deadlocks over recent time ranges.

- Deadlock Trend




This section displays different types of deadlocks that occurred over a specific time range. You can perform the following operations:

- Specify the **Start time** and **End time**. Then, click **Search** to view the trend of deadlocks that occurred over the specified time range.

Note The interval between the start time and end time cannot exceed 30 days.

- Click **Last 1 Day**, **Last 7 Days**, or **Last 30 Days** to view the trend of deadlocks that occurred over the last 1 day, last 7 days, or last 30 days.
- Move the pointer over a specific point in time to view the types and numbers of deadlocks that occurred at that point in time.

- In the upper-right corner of the trend chart, click one of the  icons. These icons allow you to change the display style of the trend chart and download the trend chart as an image.

Deadlock Details

Deadlock Details (Click each row to view the corresponding deadlock diagram.)

	LastTranStarted	SPID	IsVictim	LogUsed	LockMode	WaitResourceDesc	ObjectOwned	ObjectRequested	WaitResource	HostName
+	2021-04-15 16:04:34	53	●	444	U	RID DeadLock:DeadLock...	DeadLock dbo12	DeadLock dbo11	RID: 8:1208:0	L-PC1H39C-J-0956

< Previous 1 Next >
Items per Page 5


This section displays the details about deadlocks. You can click the **+** icon to the left of a deadlock record to view the details about the blocking and blocked sessions. The details include the following information:

- LastTranStarted**: indicates the time when the transaction was started in the session.
- SPID**: indicates the ID of the session.
- IsVictim**: indicates whether the session was terminated.

Note SQL Server comes with a deadlock monitor thread that periodically checks for deadlocks. If a deadlock is detected, SQL Server evaluates the blocking and blocked sessions and terminates the session in which the transaction can be rolled back at a lower cost than the other session. For example, a deadlock occurs between a session that executes the SELECT statement and a session that executes the UPDATE statement. In this case, SQL Server terminates the session that executes the SELECT statement, because the SELECT statement can be rolled back at a lower cost than the UPDATE statement.

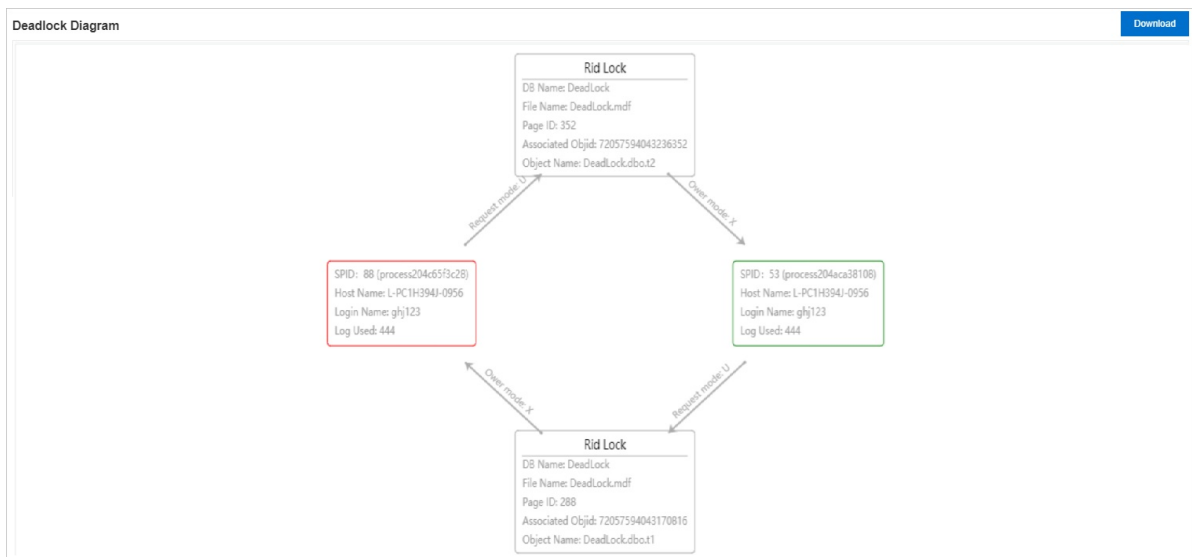
- LogUsed**: indicates the size of logs that were generated in the session. Unit: bytes.
- LockMode**: indicates the lock mode of the deadlock. For more information, see [Lock modes](#).
- WaitResourceDesc**: indicates the details about the resource for which the transaction is waiting in the session.
- Object Owned**: indicates the object that is locked in the session.

- **Object Requested**: indicates the object that the transaction requests to lock in the session.
- **Wait Resource**: indicates the name of the resource for which the transaction is waiting in the session.
- **Host Name**: indicates the name of the host on which the transaction in the session is run.
- **Login Name**: indicates the username of the account that is used to run the transaction in the session.
- **Status**: indicates the status of the transaction in the session.
- **Client App**: indicates the name of the client that initiates the transaction in the session.
- **SQL text**: indicates the details about the SQL statement that is executed in the session.

 **Note** You can click the SQL statement to copy and further analyze the SQL statement.

Click a deadlock record. Then, view the diagram of the deadlock in the Deadlock Diagram section.

● **Deadlock Diagram**



This section displays the relationships between the blocking and blocked sessions. This section also displays the details about the locked resources. You can click **Download** to download the diagram as an XDL file. This file contains the details about the deadlock. You can open and view this file by using SQL Server Management Studio (SSMS). For more information, see [SQL Server Management Studio \(SSMS\)](#).

23.7.2. View the blocking statistics of an ApsaraDB RDS for SQL Server instance

This topic describes how to view the blocking statistics of an ApsaraDB RDS for SQL Server instance by using CloudDBA in the ApsaraDB RDS console. You can identify and resolve the blocking problems of the RDS instance based on the blocking statistics.

Prerequisites

- The RDS instance is equipped with standard SSDs or enhanced SSDs (ESSDs).
- The RDS instance does not run SQL Server 2008 R2 with standard SSDs or enhanced SSDs (ESSDs).

Context

When a session is modifying a specific resource, SQL Server locks the resource to prevent access and modifications from other concurrent sessions. This enables SQL Server to ensure data consistency. In most cases, SQL Server holds the lock for a short period of time. After the session finishes modifying the resource, SQL Server immediately releases the resource and grants approval for the next session to access the resource. However, the resource can stay locked for a long period of time due to slow SQL statements or other exceptions in the session. This significantly reduces the performance of the RDS instance.

To help you resolve the preceding blocking problem, ApsaraDB RDS provides blocking statistics in the ApsaraDB RDS console. The blocking statistics include the ID of the blocking session, the time at which the blocking problem occurred, and the SQL statement that caused the blocking problem.

Sampling

In most cases, if a session causes a blocking problem that lasts approximately 2 seconds, the performance of the RDS instance does not significantly decrease. However, if multiple consecutive sessions cause blocking problems that each last approximately 2 seconds, the performance of the RDS instance significantly decreases.

ApsaraDB RDS samples blocking problems once every 10 seconds. At each point in time when ApsaraDB RDS samples blocking statistics, the sessions that require more than 2 seconds to execute an SQL statement and block other sessions are recorded.

Procedure

- 1.
2. In the left-side navigation pane, choose **CloudDBA > Lock Optimization**.
3. Click the **Blocking** tab. Then, view the details about the blocking problems that are detected in the RDS instance.

Introduction to the Blocking tab

- Number of blocking sessions


This section displays the number of blocking sessions over recent time ranges.

- Blocking Trend

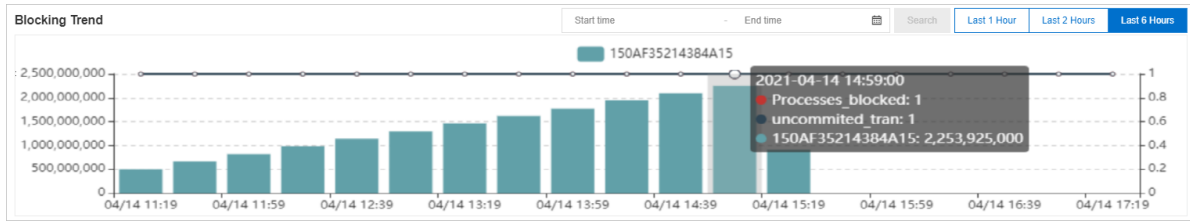
This section displays the trend of blocking durations over a specific time range.

Move the pointer over a specific point in time to query the details about the blocking problem that occurred at that point in time. The details include the following information:

- The time at which the blocking problem occurred.
- The number of blocked sessions. This number is indicated by the value of the **Processes_blocked** parameter.
- The number of transactions that are not committed. This number is indicated by the value of the **Uncommitted_tran** parameter.

 **Note** The lock that causes the blocking problem cannot be released because transactions are not committed.


- The hash value of the executed SQL statement and the length of time during which the SQL statement is blocked.



● Blocking Source Details

This section displays the details about each blocking session. The details include the following information:

- **Spid**: indicates the ID of the session.
- **QueryHash**: indicates the hash value of the requested statement in the session. The hash value of the same type of SQL statement is the same.
- **Wait Type**: indicates the reason why the session blocks another session that is in the waiting state. For more information about wait types, see [sys.dm_os_wait_stats \(Transact-SQL\)](#).
- **Execution Duration (ms)**: indicates the length of time that is required by the session to execute the requested SQL statement. Unit: milliseconds.
- **SQL**: indicates the SQL statement that causes the blocking problem.

Note You can move the pointer over an SQL statement. Then, you can click the  icon that appears to the right of the SQL statement to copy the SQL statement.

- **Time**: indicates the time at which the blocking problem occurred.
- **Database Name**: indicates the name of the database in which the blocking problem occurred.

You can click anywhere in a blocking record to view the diagram of the blocking problem.

● Blocking Diagram

This section displays the ID of the blocking session, the ID of the blocked session, the type of lock, and the blocking duration. In the following example, the blocking session is marked in red, and the blocked session is marked in blue. For more information about lock types, see [Transaction Locking and Row Versioning Guide](#).



You can move the pointer over the ID of a session to view the details about the blocking problem in the session. The details include the following information:

- **SPID**: indicates the ID of the blocking session.

- **BlockedBySpid**: indicates the ID of the blocked session.
 - **WaitType**: indicates the type of wait in the session.
 - **WaitTimeMs**: indicates the duration of blocking in the session. Unit: milliseconds.
 - **CMD**: indicates the type of SQL statement that is executed in the session.
 - **CPU**: indicates the length of time during which CPU resources are used by the session. Unit: milliseconds.
 - **DBName**: indicates the name of the database on which the session runs.
 - **ClientAppName**: indicates the name of the client from which the session is initiated.
 - **HostName**: indicates the hostname of the client from which the session is initiated.
 - **LoginId**: indicates the username that is used to log on to the session.
 - **PhysicalIO**: indicates the I/O resources that are consumed by the session to execute the requested SQL statement. Each physical I/O is equal to 8 KB.
 - **QueryHash**: indicates the hash value of the requested statement in the session. The hash value of the same type of SQL statement is the same.
 - **StartTime**: indicates the time at which the system started to execute the batch of SQL statements that contain the requested SQL statement in the session. Each batch can contain multiple SQL statements and share resources such as the values of variables.
 - **Status**: indicates the status of the RDS instance.
 - **SQL**: If you click the ID of the blocking session or blocked session, the details about the requested SQL statement in the session are displayed in the **Blocking Diagram** section.
- SQL details

In the blocking diagram, click the ID of the blocking session or blocked session to view the details about the requested SQL statement in the session. You can also copy and further analyze the statement.

23.8. Analyze the slow SQL statements on an ApsaraDB RDS for SQL Server instance

This topic describes how to analyze the slow SQL statements on an ApsaraDB RDS for SQL Server instance in the ApsaraDB RDS console.

Prerequisites

- The RDS instance is equipped with standard SSDs or enhanced SSDs (ESSDs).
- The RDS instance does not run SQL Server 2008 R2 with standard SSDs or enhanced SSDs (ESSDs).

Context

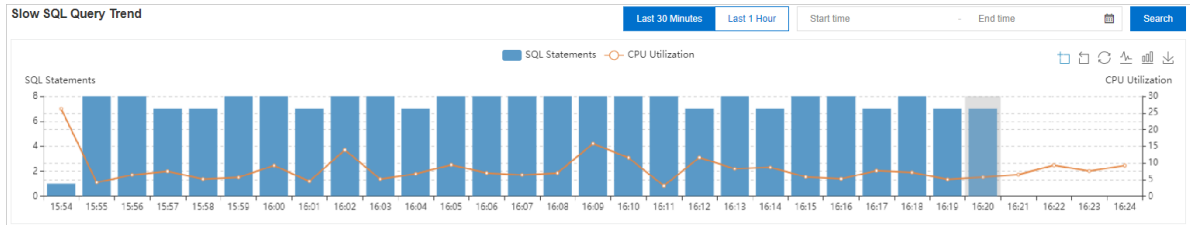
You can analyze **slow SQL statements** to troubleshoot the performance issues of an ApsaraDB RDS for SQL Server instance. This method is common and effective. SQL statements that consume a large number of CPU resources or I/O resources, require a long period of time to run, or affect a large number of rows may be slow SQL statements. The CloudDBA feature of ApsaraDB RDS records and analyzes these SQL statements and displays the analysis results on the Slow SQL page. The analysis results can be used to identify the SQL statements that affect the performance of the instance. The analysis results also help simplify the performance optimization process.

Procedure

- 1.
2. In the left-side navigation pane, choose **CloudDBA > Slow SQL**.

Introduction to the Slow SQL page

- Slow SQL Query Trend section










This section displays the CPU utilization and number of slow SQL statements over a specific time range. You can also perform the following operations:

- Specify the **Start time** and **End time**. Then, click **Search** to view the trend of slow SQL statements over the time range that you specify.

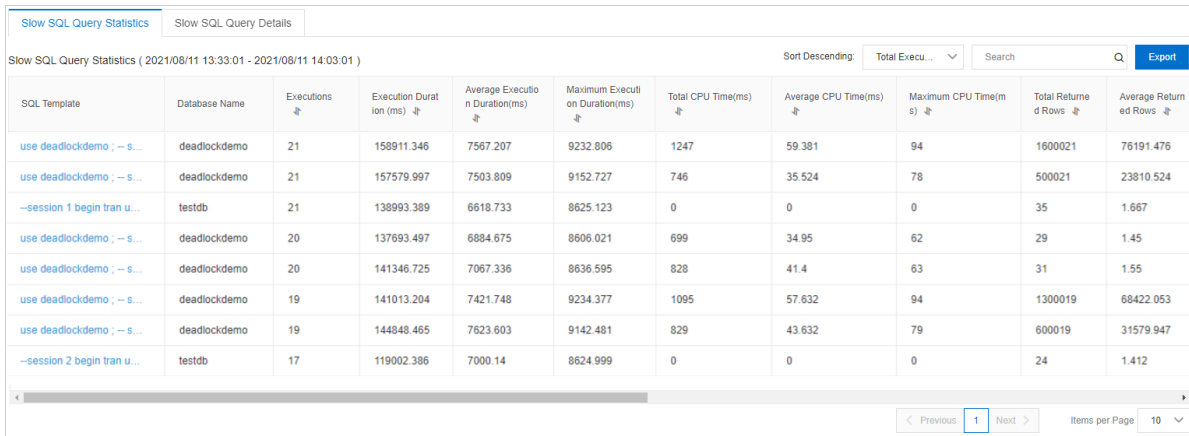
Note The interval between the start time and end time cannot exceed one day.

- Click **Last 30 Minutes** to view the trend of slow SQL statements over the last 30 minutes or click **Last 1 Hour** to view the trend of slow SQL statements over the last 1 hour.
- Move the pointer over a specific point in time to view the CPU utilization and number of slow SQL statements at the selected point in time. Click the selected point in time. In the lower section of the page, view the statistics and details about the slow SQL statements at the selected point in time.

- o In the upper-right corner, click one of the  icons to perform the operations that are supported. The following table describes the icons.

Icon	Name	Description
	Zoom	Allows you to enable or disable the zooming feature. After you enable the zooming feature, you can click a specific point in time and drag the pointer in the trend chart to select a time range. Then, the Slow SQL Query Trend section displays only the trend of slow SQL statements over the selected time range. By default, the zooming feature is enabled.
	Cancel Zoom	Allows you to disable the zooming feature.
	Restore	Allows you to restore the trend chart to the initial status.
	Switch to Line Chart	Allows you to view the trend in a line chart.
	Switch to Bar Chart	Allows you to view the trend in a column chart.
	Save as Image	Allows you to save the trend chart as an image to your computer.

● Slow SQL Query Statistics



SQL Template	Database Name	Executions	Execution Duration (ms)	Average Execution Duration (ms)	Maximum Execution Duration (ms)	Total CPU Time (ms)	Average CPU Time (ms)	Maximum CPU Time (ms)	Total Returned Rows	Average Returned Rows
use deadlockdemo; -- s...	deadlockdemo	21	158911.346	7567.207	9232.806	1247	59.381	94	1600021	76191.476
use deadlockdemo; -- s...	deadlockdemo	21	157579.997	7503.809	9152.727	746	35.524	78	500021	23810.524
--session 1 begin tran u...	testdb	21	138993.389	6618.733	8625.123	0	0	0	35	1.667
use deadlockdemo; -- s...	deadlockdemo	20	137693.497	6884.675	8606.021	699	34.95	62	29	1.45
use deadlockdemo; -- s...	deadlockdemo	20	141346.725	7067.336	8636.595	828	41.4	63	31	1.55
use deadlockdemo; -- s...	deadlockdemo	19	141013.204	7421.748	9234.377	1095	57.632	94	1300019	68422.053
use deadlockdemo; -- s...	deadlockdemo	19	144848.465	7623.603	9142.481	829	43.632	79	600019	31579.947
--session 2 begin tran u...	testdb	17	119002.386	7000.14	8624.999	0	0	0	24	1.412

This section displays the statistics of slow SQL statements over a specific time range. The statistics of a slow SQL statement include the number of times that the slow SQL statement is executed, the average length of time that is required to run the slow SQL statement, and the total CPU utilization of the slow SQL statement.

● Slow SQL Query Details

Execution Completion Time	SQL Statement	Database Name	Client	Application Name	User	CPU Time(ms)	Execution Duration (ms)	Affected Rows	I/O Logical Reads	I/O Physical Reads
2021-04-19 17:03:00	--session 2 BEGIN TRA...	testdb	sd32261003B	SQLAgent - TSQL JobStep (Jo...	testdbo	0	6211.147	1	5	0
2021-04-19 17:03:00	--session 1 BEGIN TRA...	testdb	sd32261003B	SQLAgent - TSQL JobStep (Jo...	testdbo	0	6211.351	2	8	0
2021-04-19 17:03:15	use DeadlockDemo; --...	deadlockdemo	sd32261003B	SQLAgent - TSQL JobStep (Jo...	testdbo	0	8705.98	1	460	0
2021-04-19 17:03:15	use DeadlockDemo; --...	deadlockdemo	sd32261003B	SQLAgent - TSQL JobStep (Jo...	testdbo	0	8780.845	100001	921	0
2021-04-19 17:03:30	use DeadlockDemo; --...	deadlockdemo	sd32261003B	SQLAgent - TSQL JobStep (Jo...	testdbo	0	6197.745	1	465	0
2021-04-19 17:03:30	use DeadlockDemo; --...	deadlockdemo	sd32261003B	SQLAgent - TSQL JobStep (Jo...	testdbo	0	6206.078	2	921	0
2021-04-19 17:03:45	use DeadlockDemo; --...	deadlockdemo	sd32261003B	SQLAgent - TSQL JobStep (Jo...	testdbo	0	8695.355	1	465	0
2021-04-19 17:03:45	use DeadlockDemo; --...	deadlockdemo	sd32261003B	SQLAgent - TSQL JobStep (Jo...	testdbo	0	8771.301	100001	921	0
2021-04-19 17:04:00	--session 2 BEGIN TRA...	testdb	sd32261003B	SQLAgent - TSQL JobStep (Jo...	testdbo	0	6182.156	1	5	0
2021-04-19 17:04:00	--session 1 BEGIN TRA...	testdb	sd32261003B	SQLAgent - TSQL JobStep (Jo...	testdbo	0	6183.983	2	8	0

This section displays the details about slow SQL statements over a specific time range. The details about a slow SQL statement include the name of the SQL statement, the name of the application that requests to execute the SQL statement, and the username of the account within which the SQL statement is executed.

Related information

- [View the deadlock statistics of an ApsaraDB RDS for SQL Server instance](#)
- [View the blocking statistics of an ApsaraDB RDS for SQL Server instance](#)


23.9. Use the monitoring dashboard feature

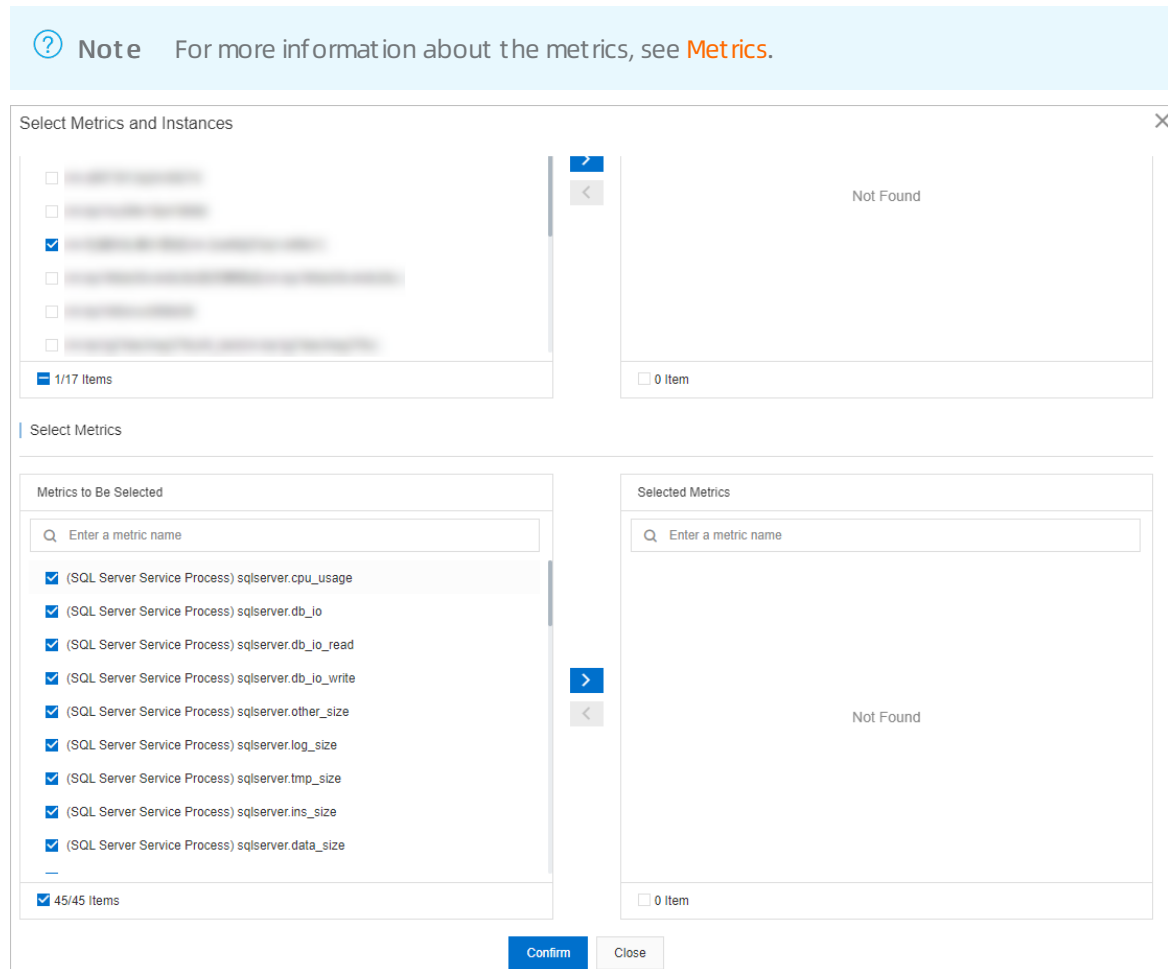
Database Autonomy Service (DAS) provides the monitoring dashboard feature for ApsaraDB RDS for SQL Server. DAS allows you to specify RDS instances and metrics to monitor and compare the metrics of the RDS instances. You can also configure metric linkage. This helps you understand the status of ApsaraDB RDS for SQL Server instances.

Context

DAS provides the monitoring dashboard feature for ApsaraDB RDS for SQL Server from May 20, 2022.

Create a monitoring dashboard

1. Log on to the [ApsaraDB RDS console](#).
2. In the left-side navigation pane, click **Performance Center**.
3. On the **Performance Center** page, click the **Monitoring Dashboard** tab.
4. Click the tab for the database engine. Then, click **Add Monitoring Dashboard**.
5. In the dialog box that appears, configure the **Dashboard Name** parameter and click **OK**.
6. Click **Select Instances and Metrics**. In the dialog box that appears, select the RDS instances and the metrics that you want to monitor. Then, click the  icon to add the selected RDS instances to the Selected Instances section and the selected metrics to the Selected Metrics section.



7. Click **Confirm**.

Note To modify the RDS instances or metrics in the monitoring dashboard, click **Add Instances and Metrics**.

View the metric trends of an RDS instance in the monitoring dashboard

1. Log on to the [ApsaraDB RDS console](#).
2. In the left-side navigation pane, click **Performance Center**.
3. On the **Performance Center** page, click the **Monitoring Dashboard** tab.
4. Click the tab for the database engine, select the monitoring dashboard that you want to view, and then specify a time range to view the trend charts of the metrics during the specified time range.

Note When you specify a time range, the end time must be later than the start time, and the interval between the start time and the end time cannot exceed seven days.

- o You can configure the **Instance filtering** parameter to filter for multiple RDS instances and then view and compare the metrics of the RDS instances.
- o You can turn on **Auto Refresh (Every 5 Seconds)** for the system to refresh the trend charts of the metrics every 5 seconds.



- You can turn on **Linkage Chart** to view the values of different metrics at the same point in time.
- You can configure the **Chart Layout** parameter to specify the number of trend charts of metrics in each row.
- You can click **Add Instances and Metrics** to modify the RDS instances or metrics in the dashboard.
- You can click **Details** in the trend chart of a metric to expand the chart. You can also change the time range to view the changes in the trend of the metric at the specified time range.
- You can click **Delete** in the trend chart of a metric to delete the chart from the dashboard.

Metrics

Category	Metric	Description
SQL Server process	cpu_usage	The CPU utilization of the RDS instance within the operating system.
	db_io	The number of I/O requests per second.
	db_io_read	The number of read I/O requests per second.
	db_io_write	The number of write I/O requests per second.
	other_size	The amount of disk space occupied by system files
	log_size	The amount of disk space occupied by log files.
	tmp_size	The amount of disk space occupied by temporary files.
	ins_size	The total amount of disk space occupied by the RDS instance.
	data_size	The amount of disk space occupied by data files.
Database	qps	The average number of times that SQL statements are executed per second.
	connection_reset	The total number of logon attempts from the connection pool per second.
	active_temp_tables	The number of active temporary tables.
	active_session	The number of active threads.
	active_cursors	The number of active cursors.
	sessions	The total number of connections.
	active_transactions	The number of active transactions.
	transactions	The average number of transactions per second.

Category	Metric	Description
	write_transactions	The average number of write transactions per second.
	read_kb	The outbound traffic per second of the RDS instance.
	write_kb	The inbound traffic per second of the RDS instance.
Basic monitoring	cache_hit_ratio	The hit ratio of the high-speed cache.
	bufferpool	The percentage of pages that are found in the high-speed cache to all pages that are read from disks.
	fullscans	The average number of full table scans per second.
	autoparam_attempts_per_sec	The number of auto parameterization attempts per second.
	forced_parameterizations_per_sec	The number of successful forced parameterizations per second.
	sql_compilations	The number of SQL compilations per second.
	unsafe_autoparams_per_sec	The number of unsafe auto parameterization attempts per second.
	failed_autoparams_per_sec	The number of auto parameterization failures per second.
	safe_autoparams_per_sec	The number of safe auto parameterization attempts per second.
	resqlcompilations	The number of SQL statement recompilations per second.
	lazy_writes	The number of times that dirty pages are written to disks per second.
	checkpoint	The number of dirty pages that the checkpoint operation must write per second.
	logout	The number of logouts per second.
	logins	The number of logons per second.
	locktimeout	The number of lock requests that time out per second, including requests for NOWAIT locks.
	deadlock	The number of lock requests that resulted in a deadlock per second.
lock_requests_per_sec	The number of new locks and lock conversions per second.	

Category	Metric	Description
	lockwaits	The number of lock requests that the client waits for per second.
	lock_waits	The statistics of processes waiting for locks.
	latchwaits	The number of latch requests that are not immediately granted per second.
	lock_wait_time_ms	The average amount of wait time for each lock request that resulted in a wait.
	average_latch_wait_time	The average waiting time to request a latch resource.
	table_lock_escalations_per_sec	The number of times that a lock on a table is escalated to the HoBT level or the table level.
	average_lock_wait_time	The average waiting time of the requested lock resource.
	total_latch_wait_time	The total waiting time for locks in the last second.

 **Note** You can click the  icon on the right of a metric in a dashboard to view the description of the metric.

24.Tag


24.1. Create tags

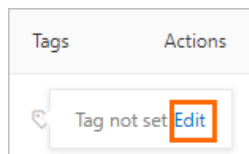
This section describes how to create tags for one or more RDS instances. If you have a large number of RDS instances, you can create tags and then bind the tags to the instances so that you can classify and better manage the instances. Each tag consists of a key and a value.

Limits

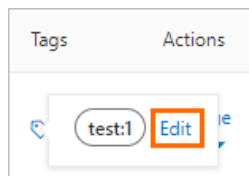
- You can add up to 20 tags to each RDS instance. Each tag must have a unique key. If two tags have the same key, the tag that is created later overwrites the earlier tag.
- You can add tags to up to 50 RDS instances at a time.
- RDS instances in different regions do not share the same tag namespace.
- After you remove a tag from an RDS instance, ApsaraDB RDS checks whether the tag is added to other RDS instances. If the tag is not added to other RDS instances, ApsaraDB RDS deletes the tag.

Add tags to an RDS instance

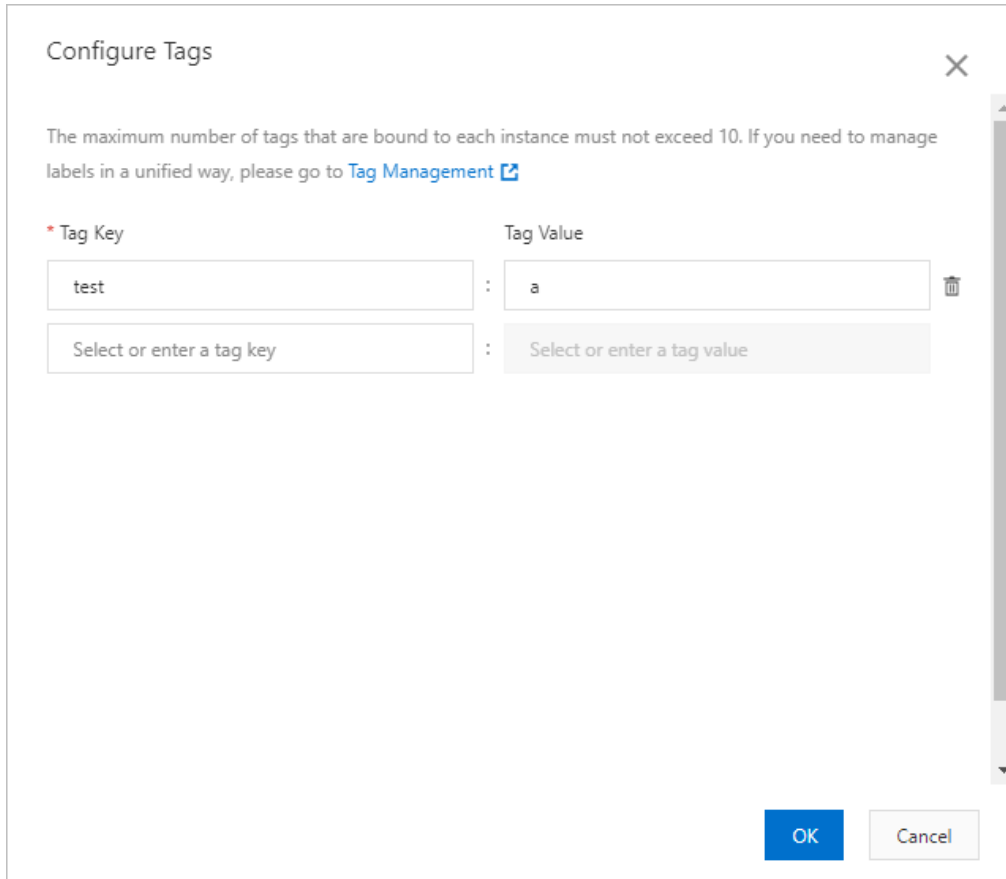
- 1.
2. Click the  icon in the **Tags** column of the required RDS instance and then click **Edit**.



If you have added a tag to the RDS instance, you can click **Edit** to edit the tag.



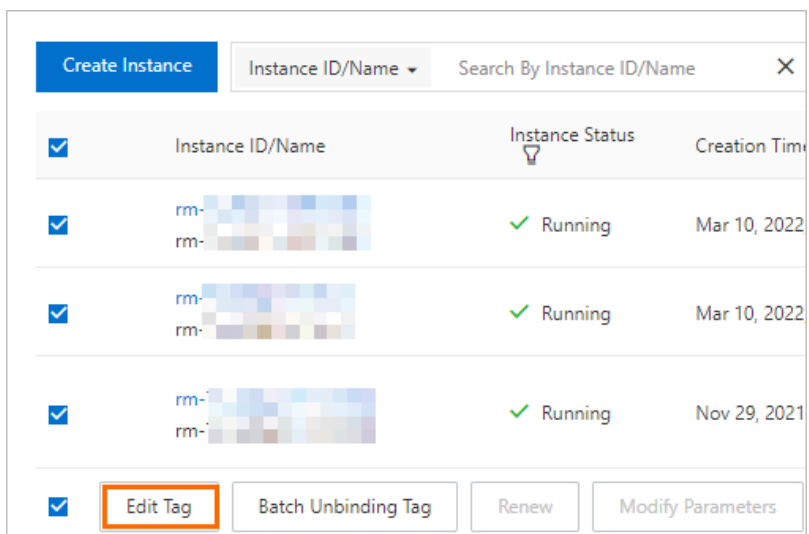
3. In the **Configure Tags** dialog box, configure the **Tag Key** and **Tag Value** parameters and click **OK**.



Add tags to multiple RDS instances at a time

- 1.
2. Select the RDS instances to which you want to add tags and click **Edit Tag** below the instance list.

Note The Edit Tag button is displayed in the lower part of the page.



3. In the **Configure Tags** dialog box, configure the **Tag Key** and **Tag Value** parameters and click **OK**.

Configure Tags ✕

The maximum number of tags that are bound to each instance must not exceed 10. If you need to manage labels in a unified way, please go to [Tag Management](#) ↗

* Tag Key	:	Tag Value	
test	:	a	✕
Select or enter a tag key	:	Select or enter a tag value	

OK
Cancel

Related operations

Operation	Description
Create and bind tags	Adds tags to one or more ApsaraDB RDS instances.


24.2. 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 remove a maximum of 20 tags at a time.
- After you remove a tag from your RDS instance, ApsaraDB RDS checks whether the tag is added to other RDS instances. If the tag is not added to other RDS instances, ApsaraDB RDS deletes the tag.

Procedure

- 1.
2. Use one of the following methods to remove tags:
 - Remove a tag from an RDS instance
 - a. Move the pointer over the  icon on the right of the instance. In the dialog box that appears, click **Edit**.

- b. Click the  icon on the right of the tag that you want to remove.
- c. Click **OK**.
- o Remove tags from multiple RDS instances at a time
 - a. Select the RDS instances from which you want to remove tags.
 - b. Click **Batch Unbinding Tag** below the instance list.
 - c. In the dialog box that appears, select the tags that you want to remove.
 - d. Click **Unbind X tags**. You can query operation details in the **Configure Tags successfully** message.


Related operations

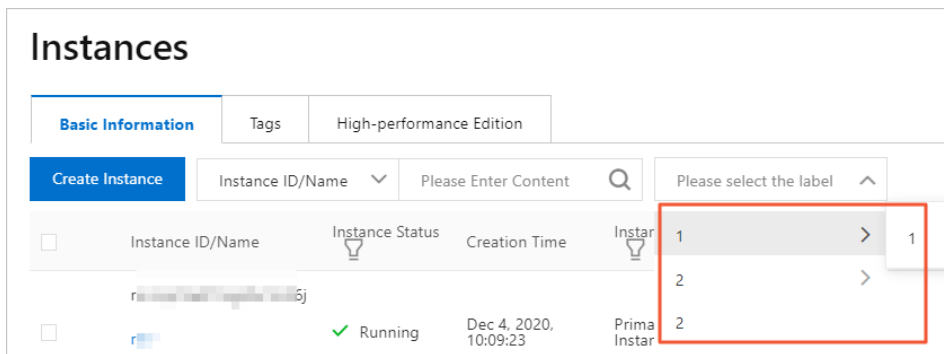
Operation	Description
Unbind tags	Removes tags from ApsaraDB RDS instances.

24.3. Use tags to filter ApsaraDB RDS for SQL Server instances

This topic describes how to filter ApsaraDB RDS for SQL Server instances based on tags after you bind tags to them.

- 1.
2. Select a **key** and a **value**. Then, ApsaraDB RDS filters your RDS instances based on the specified tag.

 **Note** To cancel the filter condition that is specified by the tag, you can click the X icon to the right of the tag.



Related operations

Operation	Description
Query the tags of ApsaraDB RDS instances	Queries the tags that are added to one or more RDS instances.


25. Best practices

25.1. Connect an ApsaraDB RDS for SQL Server instance to a self-managed domain

This topic describes how to deploy a domain controller server on an Elastic Compute Service (ECS) instance and connect an ApsaraDB RDS for SQL Server instance to a self-managed domain.

Prerequisites

- The RDS instance is not a shared instance and runs one of the following SQL Server versions:
 - SQL Server 2019 SE or EE
 - SQL Server 2017 SE or EE
 - SQL Server 2016 SE or EE
 - SQL Server 2012 SE or EE
- The RDS instance and the ECS instance that hosts your domain controller server reside in the same virtual private cloud (VPC).
- The security group of the ECS instance is configured to allow access from the private IP address of the RDS instance. For more information, see [Add a security group rule](#).
- The private IP address of the RDS instance is allowed by the firewall of the ECS instance. The firewall is disabled by default. If you have enabled the firewall, you must configure the firewall to allow the private IP address of the RDS instance.
- The domain account that is used belongs to the Domain Admins group because high permissions are required for a client to add a domain.
- The domain controller server uses the same IP address as the Domain Name System (DNS) server.
- You have logged on to the console by using an Alibaba Cloud account.

 **Note** This feature is available only to specific customers. If you want to use this feature, you must submit a or submit an application to your customer manager.

Context

Microsoft Active Directory (AD) is a directory service that is provided for specific Microsoft products, such as Windows Server Standard, Windows Server Enterprise, and Microsoft SQL Server. A directory is a hierarchical structure that stores information about the objects on the same LAN. For example, AD stores information about accounts and allows authorized users on the same LAN to query the account information. The account information includes usernames, passwords, and phone numbers.

AD is an important component in the Windows ecosystem. A number of large enterprises rely on the domain control mechanism that is provided by Windows to plan and implement centralized access management. If you migrate all your workloads from an on-premises environment to the cloud or use a hybrid cloud architecture, make sure that the cloud supports AD for global management. AD support is a key factor to determine whether you can migrate on-premises SQL Server databases to the cloud.

ApsaraDB RDS for SQL Server enables you to connect an RDS instance to a self-managed domain.

Precautions

Null.

Select a Windows version

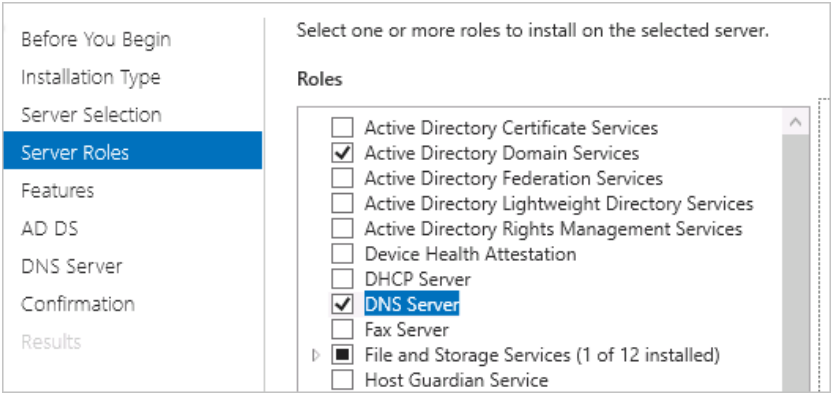
You must deploy a domain controller server on an ECS instance that runs Windows Server. The minimum requirement for the operating system of the ECS instance is Windows Server 2012 R2. We recommend that you use Windows Server 2016 or later and select English. In the following sections, Windows Server 2016 is used as an example to describe how to deploy a domain controller server for an RDS instance.

Procedure

1. [Deploy a domain controller server on an ECS instance](#)
2. [Configure a security group for the ECS instance](#)
3. [Configure the RDS instance](#)

Deploy a domain controller server on an ECS instance

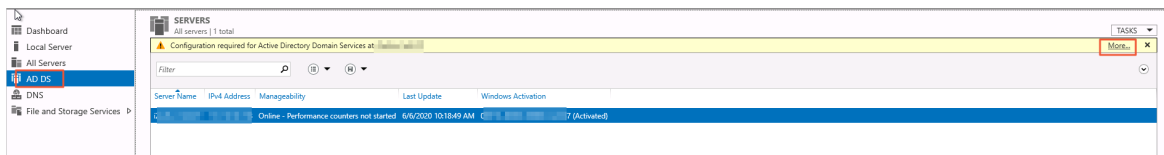
- 1.
- 2.
- 3.
4. On the **Instances** page, find the specific ECS instance that runs Windows Server 2016 and click its ID.
5. Log on to the ECS instance.
6. Search for and open **Server Manager**.
7. Click **Add roles and features** and configure the following parameters.

Parameter	Description
Installation Type	Retain default settings.
Server Selection	Retain default settings.
Server Roles	<ul style="list-style-type: none"> ◦ Select Active Directory Domain Services. In the dialog box that appears, click Add Features. ◦ Select DNS Server. In the dialog box that appears, click Add Features. Make sure that your computer uses a fixed IP address. If the IP address dynamically changes, the DNS server becomes unavailable. 

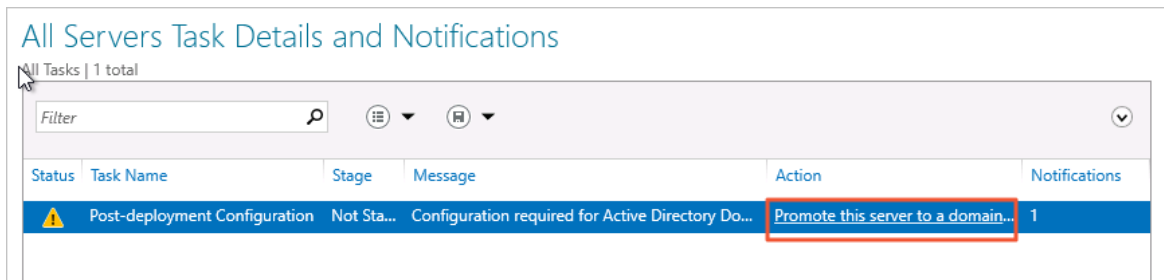
Parameter	Description
Features	Retain default settings.
AD DS	Retain default settings.
DNS Server	Retain default settings.
Confirmation	Click Inst all .

8. After the installation is complete, click **Close**.

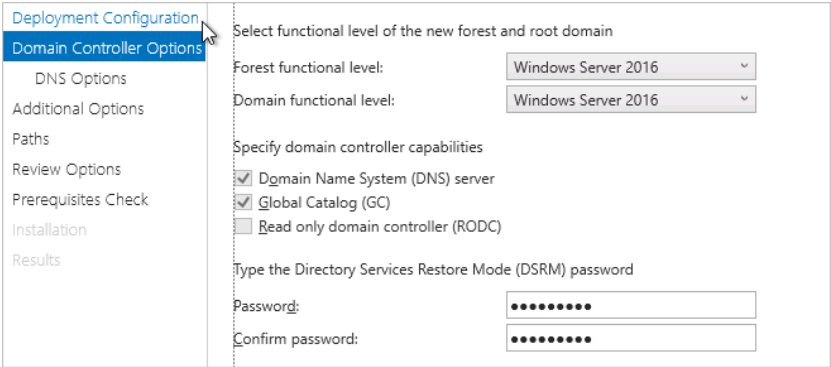
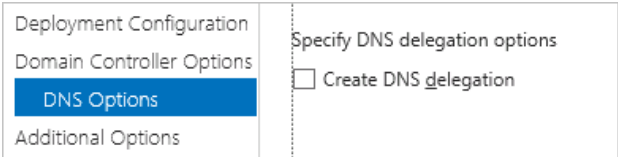
9. In the left-side navigation pane, click **AD DS**. In the upper-right corner of the page, click **More**.



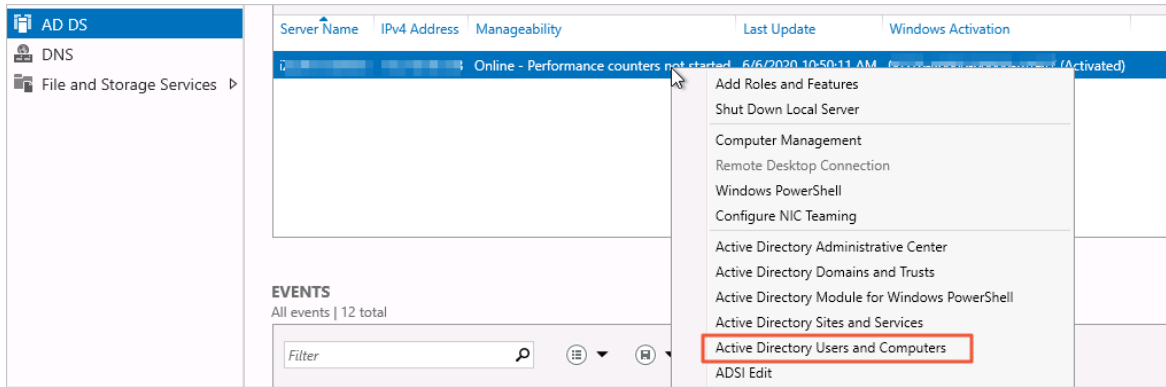
10. Click **Promote this server to a domain** and configure parameters on the following pages.



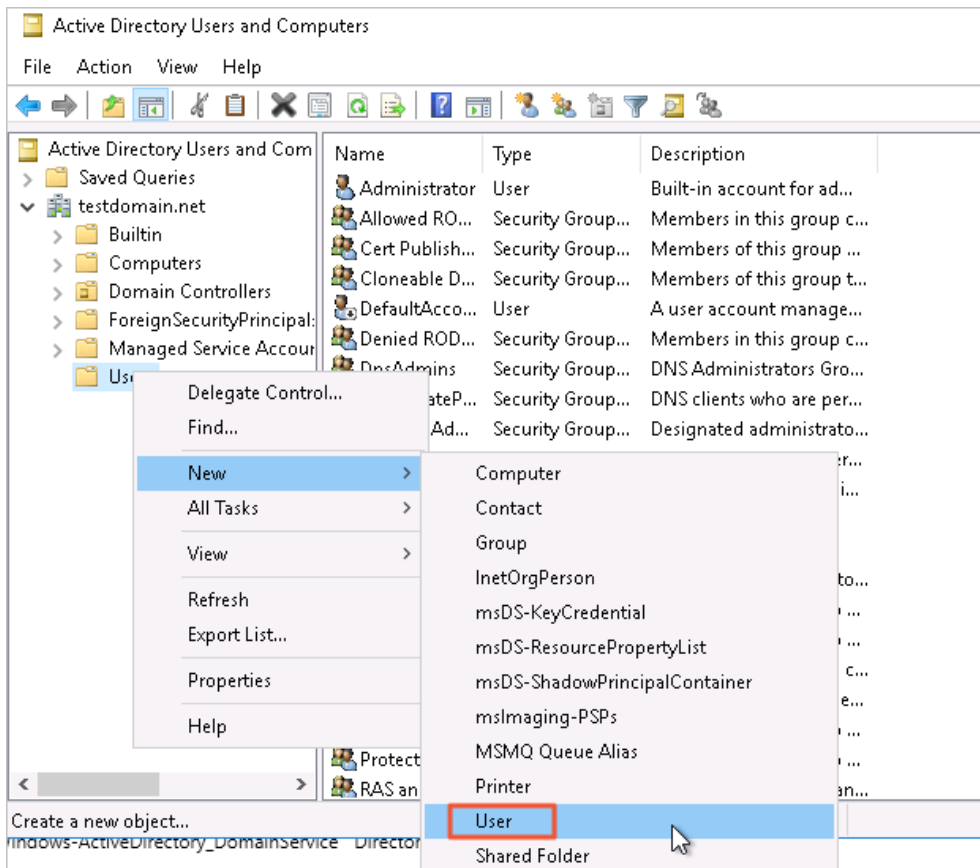
Page	Description
Deployment Configuration	<p>Select Add a new forest and set the domain name.</p> <div style="border: 1px solid #ccc; padding: 5px;"> <div style="display: flex; border-bottom: 1px solid #ccc;"> <div style="width: 30%; padding: 2px;">Deployment Configuration</div> <div style="padding: 2px;"> Select the deployment operation <input type="radio"/> Add a domain controller to an existing domain <input type="radio"/> Add a new domain to an existing forest <input checked="" type="radio"/> Add a new forest </div> </div> <div style="padding: 2px;"> Specify the domain information for this operation Root domain name: <input type="text" value="testdomain.net"/> </div> </div>

Page	Description
Domain Controller Options	<p>Set the password for the Directory Services Restore Mode (DSRM) mode.</p> 
DNS Options	<p>Clear Create DNS delegation.</p> 
Additional Options	Retain default settings.
Paths	Retain default settings.
Review Options	Retain default settings.
Prerequisites Check	<p>Click Inst all.</p> <p>Note After the installation is complete, the system restarts.</p>

11. After the system restarts, search for and open **Server Manager** again.
12. In the left-side navigation pane, click **AD DS**. Right-click the specific domain controller server and select **Active Directory Users and Computers** to go to the AD user management module.



13. Choose testdomain.net > Users. Right-click Users and choose New > User.



14. Set a username and click Next.

New Object - User

Create in: testdomain.net/Users

First name: [] Initials: []

Last name: []

Full name: testuser

User logon name: testuser @testdomain.net

User logon name (pre-Windows 2000): TESTDOMAIN\ testuser

< Back Next > Cancel

15. Set a password, select Password never expires, and click Next . Then, click Finish.

New Object - User

Create in: testdomain.net/Users

Password: []

Confirm password: []

User must change password at next logon

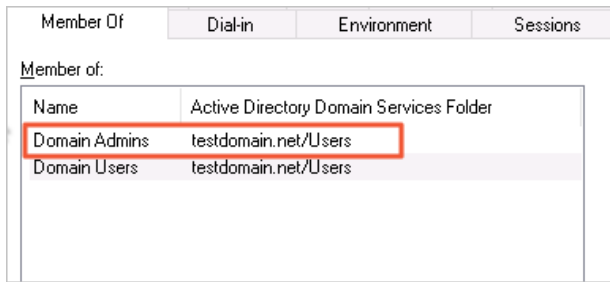
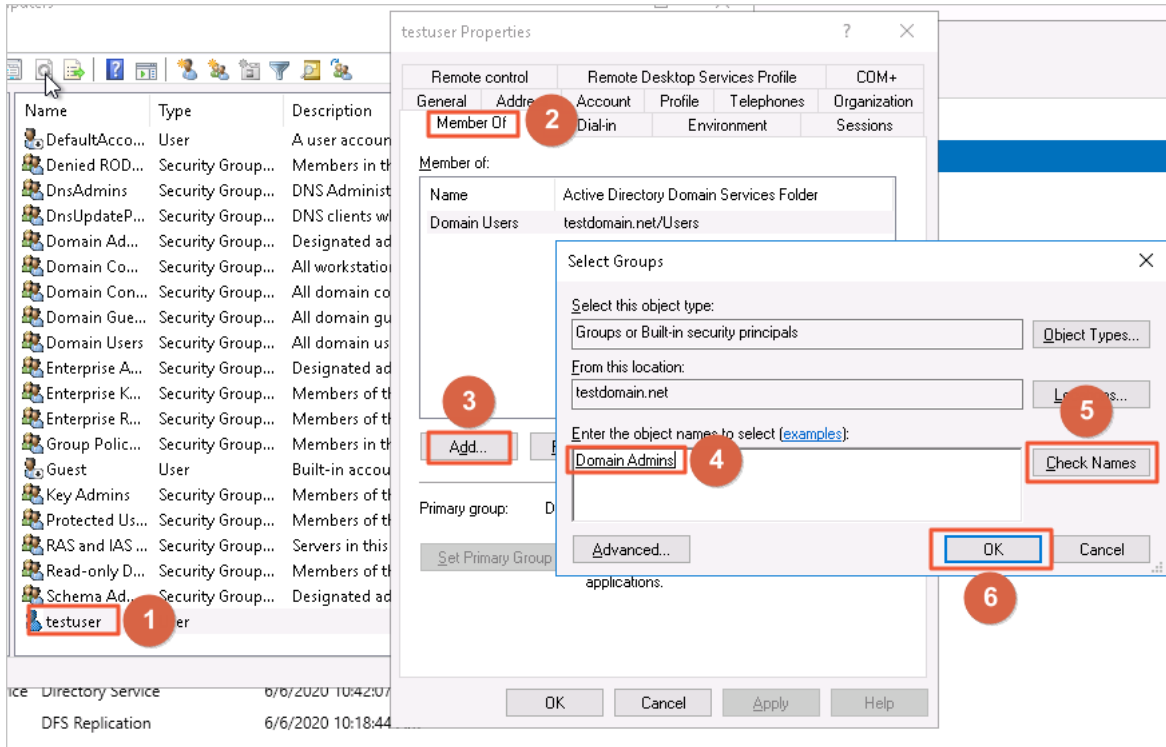
User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

16. Double-click the created user and add the user to the Domain Admins group.

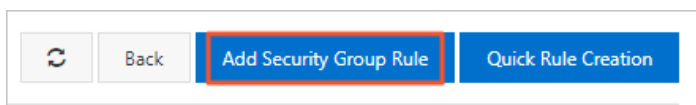


Configure a security group for the ECS instance

- 1.
- 2.
- 3.
4. On the **Instances** page, find the specific ECS instance and click its ID.
5. In the left-side navigation pane, click **Security Groups**. On the page that appears, click **Add Rules**.

Note A number of ports need to be enabled for a domain controller server. We recommend that you configure a separate security group for the domain controller server instead of configuring the domain controller server in the same security group as other ECS instances.

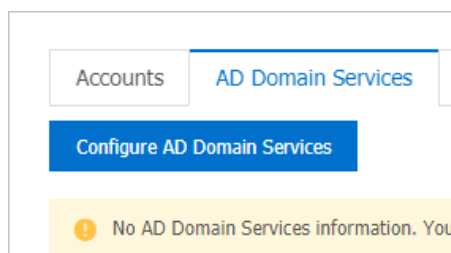
6. On the **Inbound** tab, click **Add Security Group Rule** to allow the RDS instance to access the ECS instance over the following ports.



Protocol	Port	Description
TCP	88	The port for the Kerberos authentication protocol.
TCP	135	The port for the Remote Procedure Call (RPC) protocol.
TCP/UDP	389	The port for the Lightweight Directory Access Protocol (LDAP).
TCP	445	The port for the Common Internet File System (CIFS) protocol.
TCP	3268	The port for Global Catalog.
TCP/UDP	53	The port for the DNS service.
TCP	49152~65535	The default dynamic port range for connections. Enter a value in the following format: 49152/65535.

Configure the RDS instance

- 1.
2. In the left-side navigation pane, click **Accounts**.
3. Click the **AD Domain Services** tab and click **Configure AD Domain Services**.



4. Configure the following parameters and select **I have read and understand the impact of AD Domain Services on the RDS Service Level Agreement**.

 **Warning** After the AD domain feature is enabled, **SLA** is not guaranteed.

Configure AD Domain Services
✕

*** Domain Name**

*** Directory IP Address**

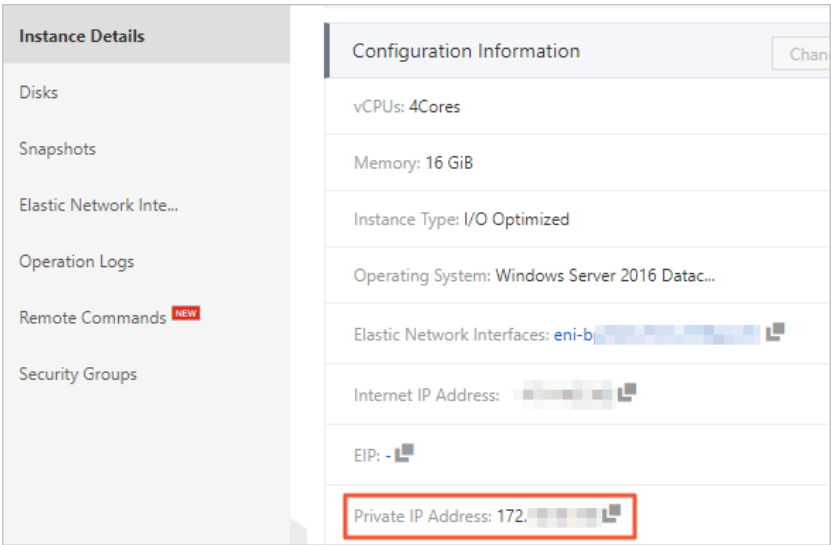
*** Domain Account**

*** Domain Password**

AD Domain Services has permissions on the operating system. After configuration, proceed with caution by following the [RDS AD Domain Services Configuration Instructions](#).

I have read and understand the impact of AD Domain Services on the [RDS Service Level Agreement](#).

OK
Cancel

Parameter	Description
Domain Name	The domain name that you specified when you created an AD on the Deployment Configuration page. In this example, enter testdomian.net.
Directory IP Address	<p>The IP address of the ECS instance on which the domain controller server is deployed. You can obtain the IP address by running the <code>ipconfig</code> command on the ECS instance or by using the ECS console.</p> 
Domain Account	The username of the user that you created.

Parameter	Description
Domain Password	The password of the preceding user.

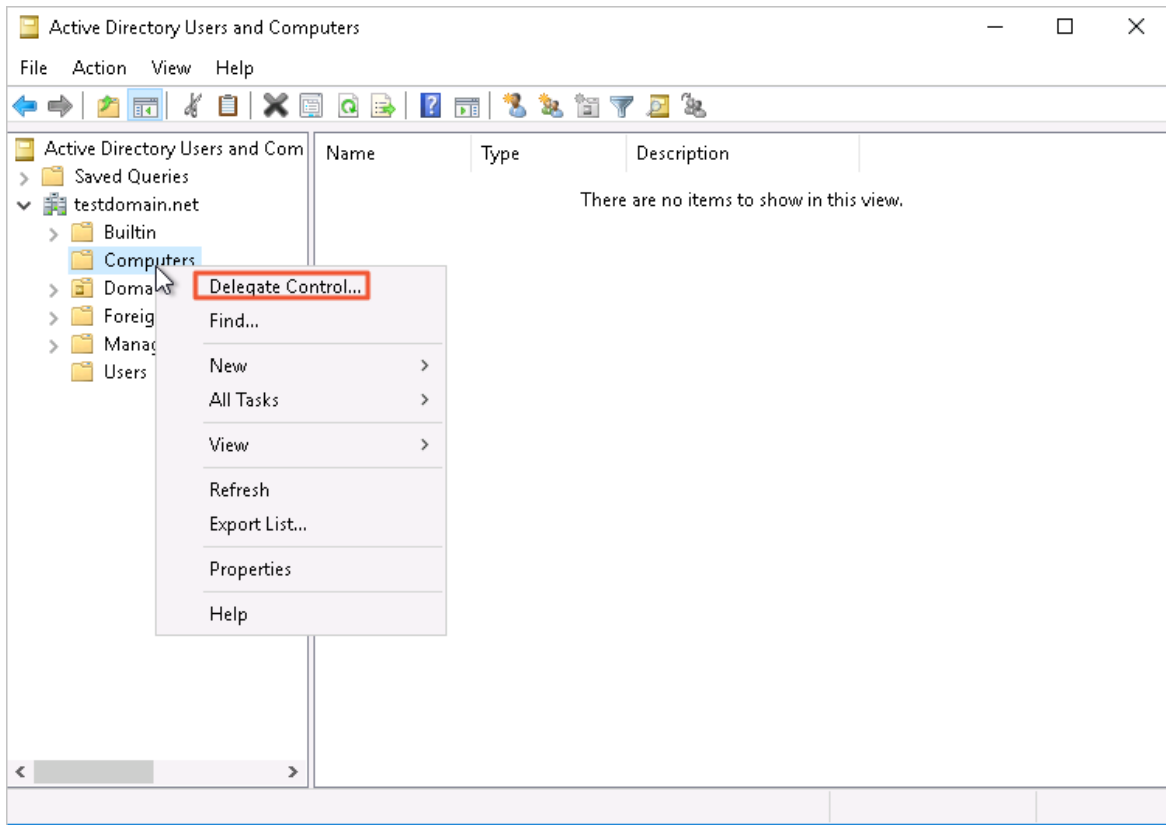
5. Click **OK** and wait until the domain is added.

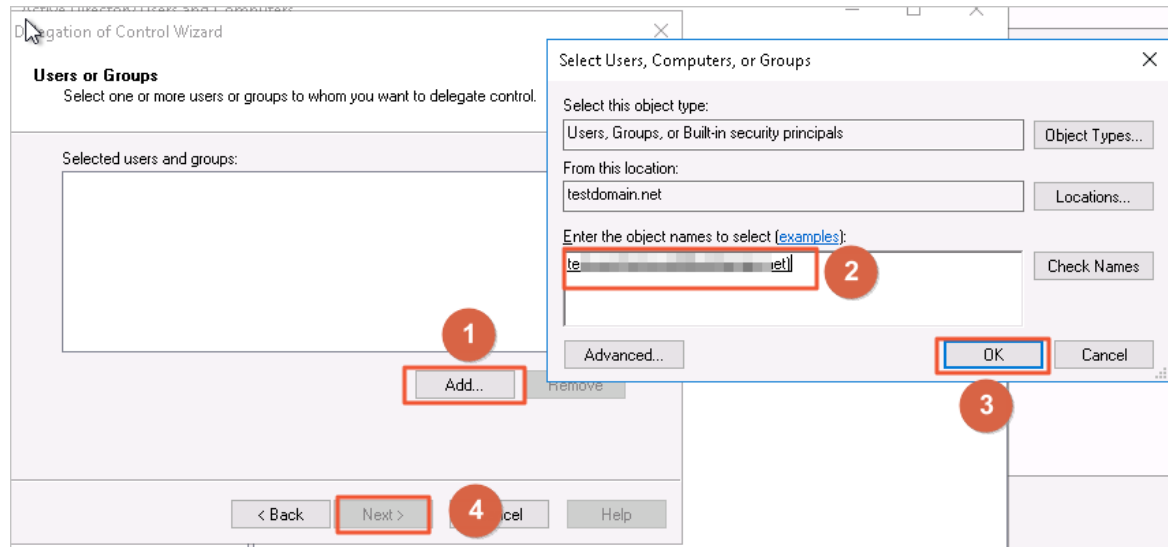
FAQ

Which account can I use to connect my RDS instance to a domain? How do I control the permissions of the account?

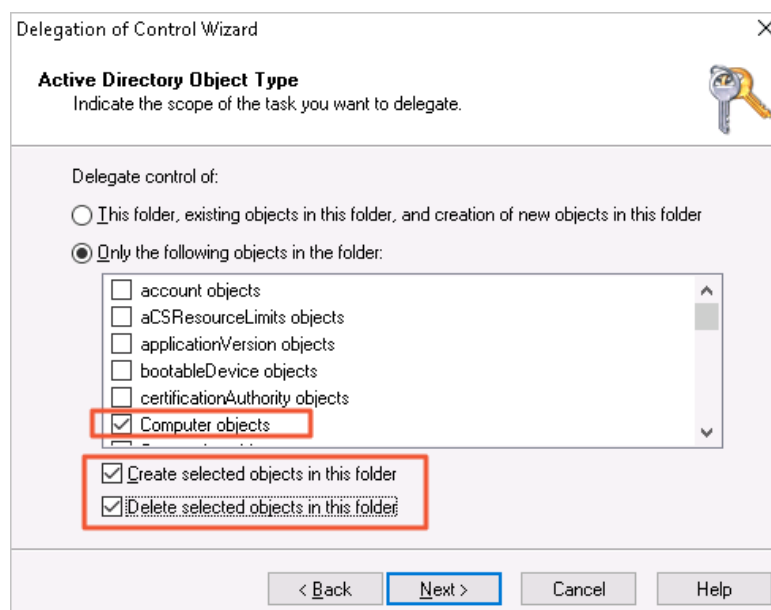
We recommend that you use an account that has the administrator rights on the domain. If you do not want to enable the administrator rights, you can use the least permissions by performing the following operations. However, if you use the least permissions, you must manually remove your computer from the domain controller server when you exit the domain. Otherwise, an error is reported when you reconnect your RDS instance to this domain.

1. After you create a user and confirm that the user belongs to the Domain Admins group, choose **Computers > Delegate Control** to add the user that you created.

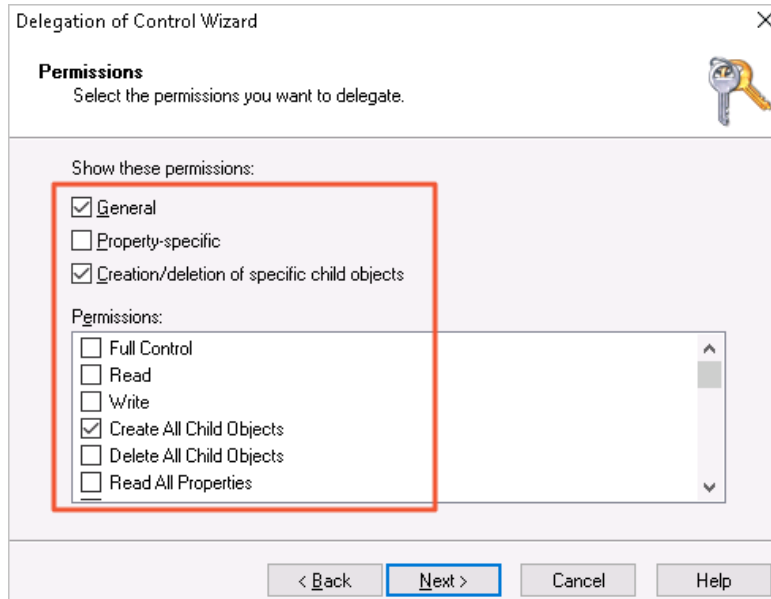




2. Right-click the user and select **Create a custom task to delegate**. Then, click **Next**.
3. Select **Only the following objects in the folder** and the red highlighted items that are shown in the following figure. Then, click **Next**.



4. Select the items that are shown in the following figure. Then, click **Next** until the procedure is complete.



25.2. Connect Kingdee K/3 WISE to ApsaraDB RDS for SQL Server

This topic describes how to connect an Elastic Cloud Service (ECS) instance that runs Kingdee K/3 WISE 15.0 or 15.1 to an ApsaraDB RDS for SQL Server instance. After the connection is established, you can run distributed transactions between the RDS instance and the ECS instance.

Solution

This solution consists of three steps:

1. Upload a full backup file of the specified Kingdee K/3 WISE set of books to an Object Storage Service (OSS) bucket. Then, restore the data from the full backup file to the RDS instance. For more information, see [Restore data to the RDS instance](#).
2. Modify the access settings of the RDS instance, ECS instance, and Windows operating system. This allows you to smoothly run distributed transactions between the RDS instance and the ECS instance. For more information, see [Enable distributed transactions](#).
3. Replace the old accounting data management tool with a new one that is compatible with ApsaraDB RDS for SQL Server. For more information, see [Initialize the new accounting data management tool](#).

Before you begin

- Install Kingdee K/3 WISE on an ECS instance that runs Windows Server 2016.
- Create an RDS instance. For more information, see [Create an ApsaraDB RDS for SQL Server instance](#).
- Obtain the full backup data of the Kingdee K/3 WISE set of books.

Note

- The ECS instance on which Kingdee K/3 WISE is installed must reside in the same region and virtual private cloud (VPC) as the RDS instance. For more information, see [VPC](#).
- The RDS instance must run one of the following SQL Server versions and RDS editions:
 - SQL Server 2019 SE on RDS High-availability Edition
 - SQL Server 2017 SE on RDS High-availability Edition
 - SQL Server 2012 or 2016 EE on RDS High-availability Edition
 - SQL Server 2012 or 2016 SE on RDS High-availability Edition

Restore data to the RDS instance

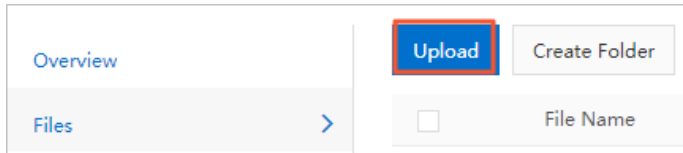
Perform the following steps to upload a full backup file of the set of books to an OSS bucket:

1. Log on to the [OSS console](#).
2. In the right-side pane, click **Create Bucket**.
3. Configure the following parameters.

Parameter	Description
Bucket Name	Enter the name for the bucket.
Region	Select the region where the bucket resides. Make sure that the bucket resides in the same region as the ECS and RDS instances.
Storage Class	Select IA .
Zone-redundant Storage	Select Not Activated .
Versioning	Select Not Activated .
Access Control List (ACL)	Select Private .
Encryption Method	Select None .
Real-time Log Query	Select Not Activated .

Note For more information about parameters, see [Create buckets](#).

4. Click **OK**.
5. In the left-side navigation pane, click **Buckets**. On the page that appears, click the bucket that you created.
6. In the left-side navigation pane of the page, click **Files**. On the page that appears, click **Upload**.



7. Drag the full backup file to upload to the **Files to Upload** section. Alternatively, click **Select Files** in the Files to Upload section and select the backup file.

Note For more information about parameters, see [Upload objects](#).

Upload To: **Current** | Specified
 oss://alicdn-log-delivery-1406926474064770-ap-southeast-1/

File ACL: **Inherited from Bucket** | Private | Public Read | Public Read/Write
 Inherited from Bucket: The ACLs of each file are the same as those of the bucket.

Files to Upload

Drag and drop one or more files or folders here

File naming conventions: 1. The file name must be UTF-8-encoded. 2. The file name must range from 1 to 1,023 bytes in length. 3. The file name cannot contain a forward slash (/). 4. The file name cannot start with a forward slash (/).

Note: If the name of the file to upload is the same as that of an existing file, the upload will fail.

Select Files | **Select Folders**

Name	Folder	Storage Class
------	--------	---------------

Perform the following steps to create a privileged account for the RDS instance:

- 1.
2. In the left-side navigation pane, click **Accounts**.
3. Click **Create Account**.
4. Configure the following parameters.


Parameter	Description
Database Account	Enter the username of the account. The username 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 lowercase letter or digit.
Account Type	Specify the type of the account. Select Privileged Account .

Parameter	Description
Password	Enter a password for the account. The password must meet the following requirements: <ul style="list-style-type: none"> ◦ The password of the account must be 8 to 32 characters in length. ◦ The password of the account must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. ◦ The password can contain any of the following characters: ! @ # \$ % ^ & * () _ + - =
Confirm Password	Enter the password of the account again.
Description	Enter a description that helps identify the account.

5. Click **OK**.

Perform the following steps to migrate the full backup file from the OSS bucket to the RDS instance:

- 1.
2. In the left-side navigation pane, click **Backup and Restoration**.
3. In the upper-right corner of the page, click **Migrate OSS Backup Data to RDS**.

 **Note** If this button does not exist, check whether the SQL Server version and edition of the RDS instance meet requirements. For more information, see the "[Before you begin](#)" section of this topic.

4. Click **Next** twice to go to the **Import Data** step.
5. Configure the following parameters.

Parameter	Description
Database Name	Enter the name of the destination database on the RDS instance.
OSS Bucket	Select the OSS bucket where the full backup file is stored.
OSS Subfolder Name	Enter the name of the subfolder where the full backup file is stored.
OSS File	Specify the full backup file that you want to import. You can enter a prefix in the search box and click the search icon to search for the full backup file by using a fuzzy match. ApsaraDB RDS displays the name, size, and update time of each full backup file that is returned. Select the full backup file that you want to migrate to the RDS instance.
Cloud Migration Method	Select Immediate Access (Full Backup) .
Consistency Check Mode	Select Synchronous DBCC .

Note If you are migrating backup data from OSS to ApsaraDB RDS for the first time, the system prompts you to authorize the OSS access permission to your Alibaba Cloud account. In this case, you only need to click **Authorize** and configure **Confirm Authorization Policy**.

Import Guide

1. Back Up Source Database 2. Upload Backup Files to OSS 3. Import Data

*Database Name

*OSS Bucket

OSS Subfolder Name

OSS File

File Name	File Size	Update Time
-----------	-----------	-------------

Cloud Migration Method Immediate Access (Full Backup) Access Pending (Incremental Backup)

Consistency Check Mode Synchronous DBCC Asynchronous DBCC

You have authorized RDS official service account to access your OSS.


6. Click **OK**.

Note Wait until the full backup file is imported into the destination database on the RDS instance. You can click **Databases** in the left-side navigation pane to view the status of the destination database.

Enable distributed transactions

Perform the following steps to configure the RDS instance:

- 1.
2. In the left-side navigation pane, click **Data Security**.
3. Find the specified IP address whitelist and 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 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 for the ECS instance in the ECS console.
- If the ECS and RDS instances reside in different VPCs, you must enter the public IP address of the ECS instance. In addition, you must apply for a public endpoint for the RDS instance. For more information, see [Apply for a public endpoint for an RDS SQL Server instance](#).

The screenshot displays the 'Instance Details' page for an RDS instance. The 'Basic Information' section includes:

- Instance ID: i-`...`
- EIP: `...` (highlighted with a red box)
- Security Group: sg-`...`
- Tags: -
- Description: -

The 'CPU and Memory' section shows 1 Cores and 2 GiB. The 'Operating System' is CentOS 8.1 64-bit. The 'Type' is ecs.t5-lc1m2.small(Standard). The 'Instance Family' is ecs.t5.

The 'Network Information' section shows:

- Network Type: VPC
- ENIs: eni-`...`
- Primary Private IP Address: `...` (highlighted with a red box)

4. Click **OK**.
5. Click the **Whitelist for Distributed Transaction** tab.
6. Click **Create Whitelist**.
7. Configure the following parameters.

Parameter	Description
-----------	-------------

Parameter	Description
Whitelist Name	Enter the name of the whitelist. The 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.
IP Addresses	Enter the IP address of the ECS instance and the name of the Windows-based computer where the ECS instance resides. Make sure that you separate the IP address and the computer name with a comma (,). Example: 192.168.1.100,k3ecstest. Enter multiple entries in different lines. Note You can view the computer name by choosing Control Panel > System and Security > System .

✕

Create ECS Whitelist for Distributed Transaction

Group Name:

Whitelist:


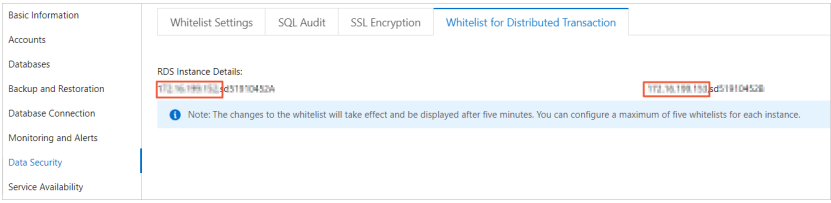
You can add 30 more entries.

8. Click **OK**.

Perform the following steps to configure the ECS instance:

1. Log on to the [ECS console](#).
2. In the top navigation bar, select the region where the ECS instance resides.
3. Find the ECS instance and click its ID.
4. Click the **Security Groups** tab.
5. Find the security group and in the Actions column click **Add Rules**.
6. On the **Inbound** tab, click **Add Rule**.
7. Configure the following parameters.

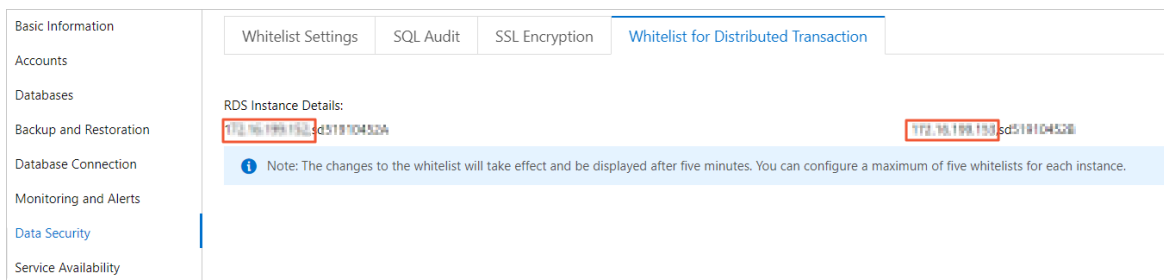
Parameter	Description
Action	Select Allow .
Priority	Enter 1 .

Parameter	Description
Protocol Type	Select Custom TCP.
Port Range	Enter 135.  Note Port 135 is the fixed port for the RPC service.
Authorization Object	Enter the two IP addresses of the RDS instance in the Authorization Objects field. You can view these IP addresses on the Whitelist for Distributed Transaction tab of the Data Security page in the ApsaraDB RDS console. 
Description	Enter a description that helps identify the rule. The description must be 2 to 256 characters in length and cannot start with http:// or https://.

8. Click **Save**.
9. Add another security group rule. This rule has the same parameter settings as the previous rule except the **Port Range** parameter that is set to 1024/65535.

Perform the following steps to configure your Windows operating system:

1. Log on to the Windows Server 2016 operating system.
2. Open the hosts file in the *C:\Windows\System32\drivers\etc\hosts* path.
3. Enter the two IP addresses of the RDS instance at the end of the hosts file. You can view these IP addresses on the **Whitelist for Distributed Transaction** tab of the **Data Security** page in the ApsaraDB RDS console.

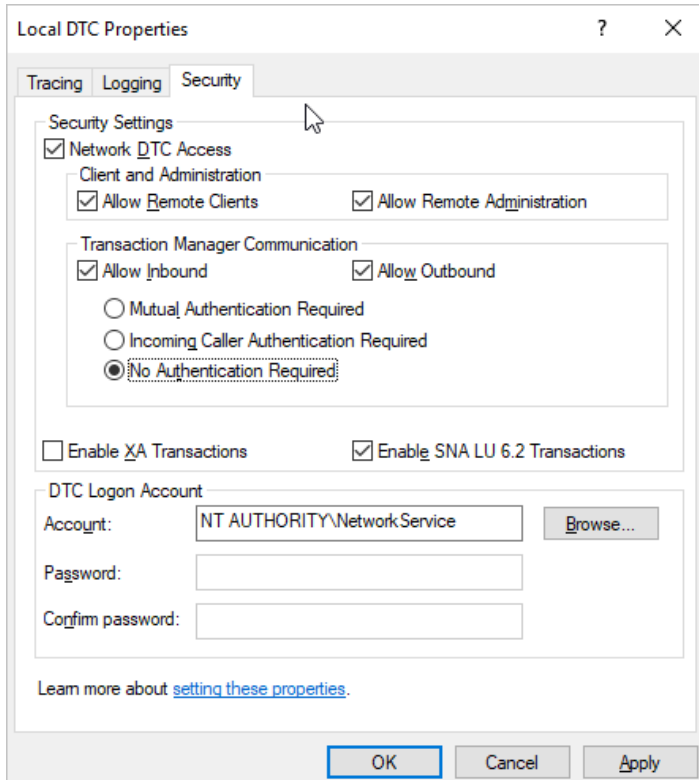


```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#|
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10      x.acme.com         # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1             localhost

192.168.1.40 sd155800007A
192.168.1.40 sd155800007B
```

4. Save the hosts file.
5. Choose **Control Panel > System and Security > Administrative Tools** and double-click **Component Services**.
6. Choose **Component Services > Computer > My Computer > Distributed Transaction Coordinator**.
7. Right-click **Local DTC** and select **Properties**.
8. Click the **Security** tab and configure the parameters.



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

Initialize the new accounting data management tool

1. Download the software package of the accounting data management tool that is used with Kingdee K/3 WISE 15.1 or 15.0.
 - o Kingdee K/3 WISE 15.1
 - o Kingdee K/3 WISE 15.0

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

2. Decompress the package and save it to the following installation directory of Kingdee K/3 WISE: *K3ERP\KDSYSTEM\KDCOM*.
3. Open Kingdee K/3 WISE.
4. In the dialog box that appears, configure the identity verification and data server information.

Note Configure the internal endpoint of the RDS instance for the data server.

5. Configure the preset connection.
6. Register the set of books.
7. Select the specified database.

Log on to Kingdee K/3 WISE


After all the settings are complete, you can run distributed transactions between the ECS and RDS instances. In addition, you can then log on to and use Kingdee K/3 WISE.

25.3. 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** You cannot create the SSRS configuration database in an ApsaraDB RDS SQL Server instance.


Prerequisites

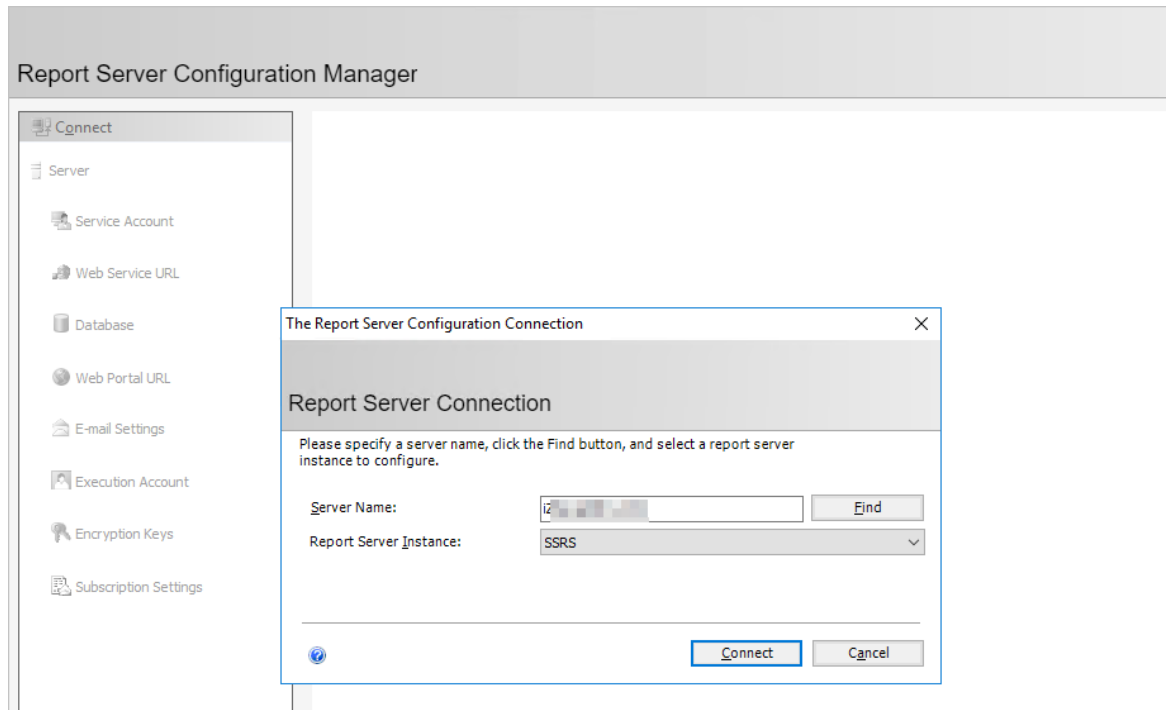
- You have created an ApsaraDB RDS SQL Server instance. For more information, see [Create an ApsaraDB RDS for SQL Server instance](#).
- You have [Create an instance by using the wizard](#).
- You have [installed SQL Server](#) on the ECS instance.

 **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.
2. Start the Report Server Configuration Manager. Configure Server Name and Report Server Instance. Click **Connect**.

 **Note** Report Server Configuration Manager automatically displays all the Report Server instances that are in the ECS instance. Select an instance as needed.

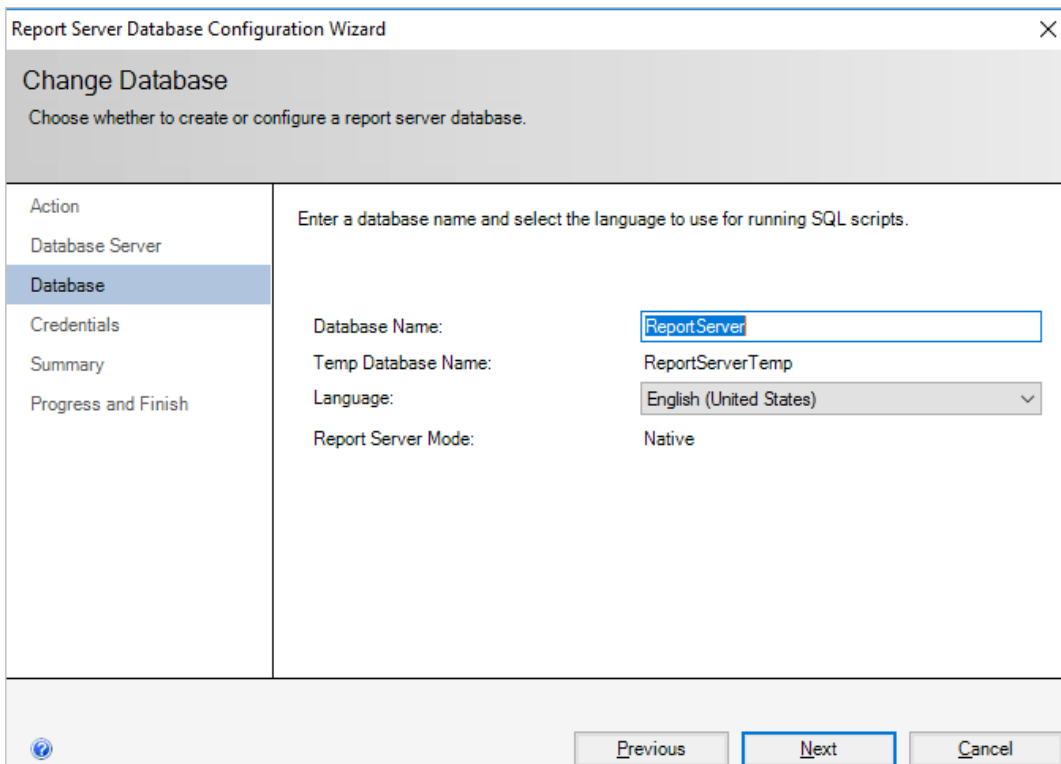


3. In the left-side navigation pane, click **Service Account** and **Web Service URL** and configure parameters based on your business needs.

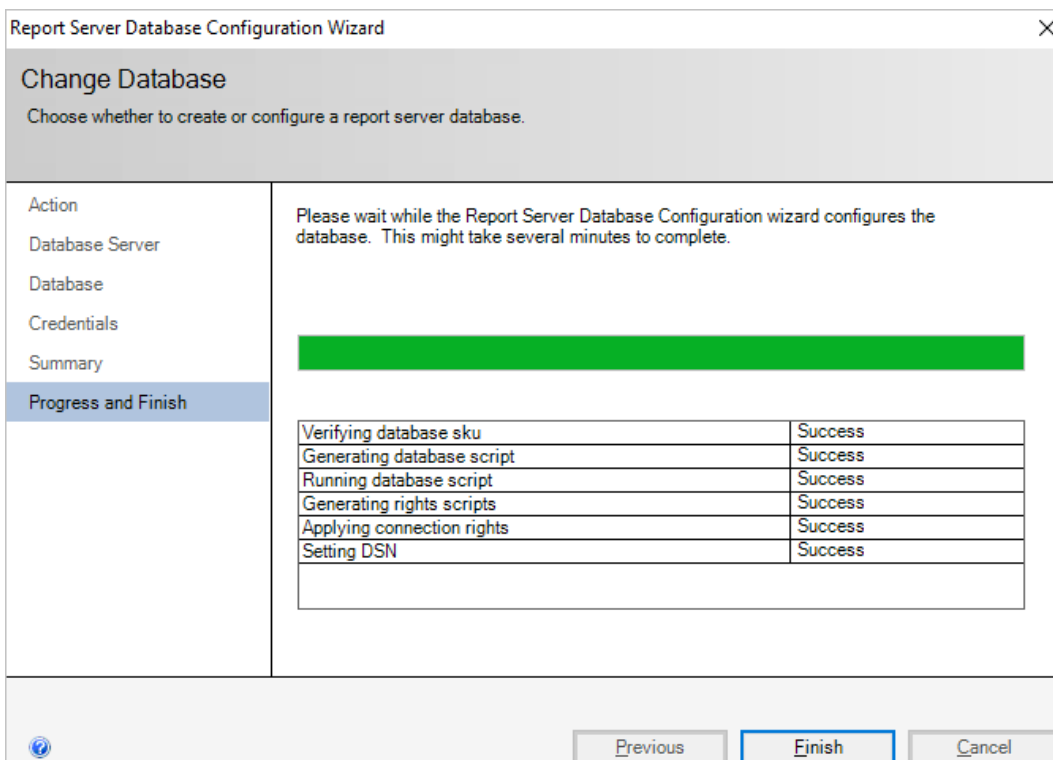
 **Note** For more information, see [Install SQL Server Reporting Services \(2017 and later\)](#).

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.
 - i. Select **Create a new report server database** and click **Next**.
 - ii. Enter the server name and click **Next**.

- iii. Enter the database name and select a language for the script. Click **Next**.



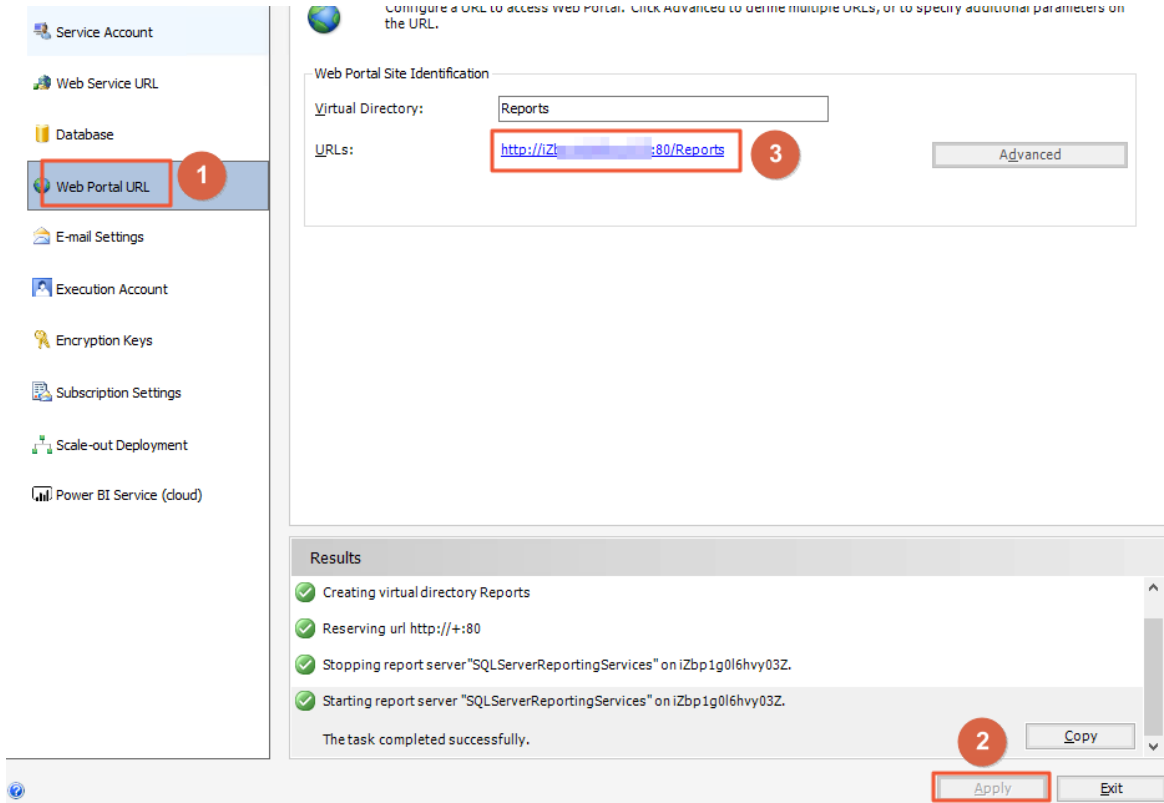
- iv. Configure the credentials for the account to connect to the report server and click **Next**.
- v. Confirm the information on the Summary page and click **Next**. Wait for the database to be created.



- vi. 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:

Section	Parameter	Description
Properties	Name	Enter the name of the data source. The name cannot contain special characters. Special characters include / @ \$ & * + = < > : ' , ? \
	Description	Specify the description of the data source to identify different data sources.
	Hide	Click to hide the data source.
	Enable	Click to enable the data source.
	Type	Select a type of the data source. Select Microsoft SQL Server .

Section	Parameter	Description
Connections	Connection String	<p>Specify the endpoint and the database name of the ApsaraDB RDS SQL Server instance in the <code>Data Source=<RDS SQL Server instance endpoint>; Initial Catalog=<database name></code> format.</p> <p>Note Make sure the IP address of the ECS instance is added to the IP whitelist of the RDS instance. For more information, see Configure an IP address whitelist for an ApsaraDB RDS for SQL Server instance.</p> <p>Connection string Learn more</p> <pre>Data Source=m-aliyun.com; Initial Catalog=alitest</pre>
Credential	Data Source Login	Select Use the following credentials .
	Credential Type	Select Database username and password .
	Username	Enter the database account of the ApsaraDB RDS SQL Server instance.
	Password	Enter the password of the database account.

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](#).