ALIBABA CLOUD

Alibaba Cloud

ApsaraDB for RDS
RDS PPAS Database

Document Version: 20210924

Alibaba Cloud

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 `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Preface

This topic provides an overview of ApsaraDB RDS for PPAS and describes related terms.
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, PPAS (compatible with Oracle), 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.

If you require technical support, log on to the ApsaraDB for RDS console and in the top navigation bar choose **Tickets > Submit Ticket**. 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.

RDS PPAS

ApsaraDB RDS for PPAS is a stable, secure, and scalable enterprise-grade relational database. Based on PostgreSQL, the most advanced open source database in the world, ApsaraDB RDS for PPAS brings enhancements in terms of performance, application solutions, and compatibility. It also provides the capability of directly running Oracle applications. You can run enterprise-grade applications on ApsaraDB RDS for PPAS to implement stable and cost-effective services.

For more information about the features that ApsaraDB RDS for PPAS offers, see Features of ApsaraDB RDS for PPAS.

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.

Term	Description
ApsaraDB RDS for XX (XX represents one of the following database engines: MySQL, SQL Server, PostgreSQL, PPAS, 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

Before you use ApsaraDB RDS for PPAS, you must understand its limits and take the necessary precautions.

The following table lists the limits of ApsaraDB RDS for PPAS.

Item	Limit
Database parameter reconfiguration	Not supported.
Root permissions of databases	ApsaraDB RDS for PPAS does not provide superuser accounts.
Database backup	Data can be backed up only by using the pg_dump plug-in.
Data import	Backed up data can be restored only by using the psql plug-in.
Database replication	• The system automatically builds High-availability (HA) database systems based on PPAS streaming replication. • Secondary RDS instances are hidden and cannot be directly accessed.
Instance restart	RDS instances must be restarted by using the ApsaraDB for RDS console or API operations.

3.Features of ApsaraDB RDS for PPAS

This topic provides an overview of the features that are supported by ApsaraDB RDS for PPAS with different database engine versions, RDS editions, and storage types.

> **Note** In the following table, the check sign (√) indicates that the feature is supported, and the cross sign (×) indicates that the feature is not supported.

PPAS

Category	Feature	PPAS 10	PPAS 9.3
		High-availability Edition	High-availability Edition
		Local SSD	Local SSD
Data migration	Migrate data from Oracle to PPAS	√	√
Instance management	Create an ApsaraDB RDS for PPAS instance	√	√
	Change the configuration of an RDS PPAS instance	√	√
	Modify the parameters of an ApsaraDB RDS for PPAS instance	√	√
	Migrate an ApsaraDB RDS for PPAS instance across zones	√	√
	Switch over services between primary and secondary ApsaraDB RDS for PPAS instances	√	√
	Restart an ApsaraDB RDS for MySQL instance	√	√
	Set the maintenance window of an ApsaraDB RDS instance	√	√
	Release an RDS PPAS instance	√	√

Category	Feature	PPAS 10	PPAS 9.3
		High-availability Edition	High-availability Edition
		Local SSD	Local SSD
	Manage ApsaraDB RDS for PPAS instances in the recycle bin	√	√
Account management	Create an account on an ApsaraDB RDS for PPAS instance	√	√
	Reset the password of an account on an ApsaraDB RDS for PPAS instance	√	√
Database management	Create a database on an ApsaraDB RDS for PPAS instance	√	√
	Delete a database from an ApsaraDB RDS for PPAS instance	√	√
	Use plug-ins	√	√
Database connection	Connect to an ApsaraDB RDS for PPAS instance	√	√
	Configure endpoints for an RDS for PPAS instance	√	√
	View and modify the internal and public endpoints and ports of an ApsaraDB RDS for PPAS instance	√	√
	Apply for or release a public endpoint for an ApsaraDB RDS for PPAS instance	√	√
	View resource monitoring data	√	√
	Set the monitoring frequency	√	√

Monitoring and alerting Category	Feature	PPAS 10	PPAS 9.3
		High-availability Edition	High-availability Edition
		Local SSD	Local SSD
	Configure alert rules for an ApsaraDB RDS for PPAS instance	√	√
Network management	Change the network type of an ApsaraDB RDS for PPAS instance	√	√
Read-only instance	Create a read-only ApsaraDB RDS for PPAS instance	√	×
Security management	Control access to an ApsaraDB RDS for PPAS instance	√	√
	Switch an ApsaraDB RDS for PPAS instance to the enhanced whitelist mode	√	√
Audit	Enable and disable SQL Audit (database audit) on an ApsaraDB RDS for PPAS instance	√	√
	View the logs of an ApsaraDB RDS for PPAS instance	√	√
Backup	Back up an ApsaraDB RDS for PPAS instance	√	√
	View the free quota for backup storage of an ApsaraDB RDS for PPAS instance	√	√
	Download the backup files of an RDS PPAS instance	√	√
Restoration	Restore the data of an ApsaraDB RDS for PPAS instance	√	√
	Create tags	√	√

Category Tag management	Feature	PPAS 10	PPAS 9.3
		High-availability Edition	High-availability Edition
		Local SSD	Local SSD
	Unbind tags from an ApsaraDB RDS for MySQL instance	√	√
	Filter RDS instances by tag	√	√

4.Specifications

4.1. Primary ApsaraDB RDS for PPAS instance type

This topic provides an overview of primary ApsaraDB RDS for PPAS instance types. This overview includes the most recent instance types, the earlier instance types, and the specifications for each instance type.

ApsaraDB RDS for PPAS instances

RDS edition	PPAS version	Instance family	Instance type	CPU and memory	Maximum connections	Maximum IOPS	Storage capacity
High-availability Edition	10	General-purpose instance	rds.ppas.t1.small	1 core, 1 GB	100	1,200	150 GB
		Dedicated instance	ppas.x4.small.2	1 core, 4 GB	200	5,000	250 GB
			ppas.x4.medium.2	2 cores, 8 GB	400	10,000	
			ppas.x8.medium.2	2 cores, 16 GB	2,500	15,000	
			ppas.x4.large.2	4 cores, 16 GB	2,500	20,000	250 GB or 500 GB
			ppas.x8.large.2	4 cores, 32 GB	5,000	30,000	
			ppas.x4.xlarge.2	8 cores, 32 GB	5,000	40,000	500 GB or 1,000 GB
			ppas.x8.xlarge.2	8 cores, 64 GB	10,000	60,000	
			ppas.x4.2xlarge.2	16 cores, 64 GB	10,000	80,000	1,000 GB or 2,000 GB
			ppas.x8.2xlarge.2	16 cores, 128 GB	12,000	120,000	
			ppas.x4.4xlarge.2	32 cores, 128 GB	12,000	160,000	2,000 GB or 3,000
			ppas.x8.4xlarge.2	32 cores, 256 GB	12,000	240,000	

RDS edition	PPAS version	Instance family	Instance type	CPU and memory	Maximum connections	Maximum IOPS	GB Storage capacity
		Dedicated host	rds.ppas.st.h43	60 cores, 470 GB	12,000	450,000	3,000 GB, 4,000 GB, 5,000 GB, or 6,000 GB

Phased-out ApsaraDB RDS for PPAS instance types

The following table lists phased-out ApsaraDB RDS for PPAS instance types. These instance types are no longer available to new instances.

Instance type	CPU cores	Memory capacity	Maximum connections	Maximum IOPS
rds.ppas.s1.small	1	2 GB	200	1,000
rds.ppas.s2.large	2	4 GB	400	2,000
rds.ppas.s3.large	4	8 GB	800	5,000
rds.ppas.m1.medium	4	16 GB	1,500	8,000
rds.ppas.c1.xlarge	8	32 GB	2,000	12,000
rds.ppas.c2.xlarge	16	64 GB	2,000	14,000
rds.pg.c2.2xlarge	16	128 GB	3,000	16,000

4.2. Read-only ApsaraDB RDS for PPAS instance type

This topic provides an overview of read-only ApsaraDB RDS for PPAS instance types, which include the most recent instance types. The overview includes the specifications for each instance type.

Read-only ApsaraDB RDS for PPAS instances

Role	Database engine version	Instance family	Instance type	CPU and memory specifications	Maximum number of connections	Maximum IOPS	Storage capacity
Read-only instance	10	General-purpose instance family	rds.ppas.t1.small	1 core, 1 GB	100	1200	150GB
		Dedicated instance family	ppas.x4.small.2	1 core, 4 GB	200	5000	250GB
			ppas.x4.medium.2	2 cores, 8 GB	400	10000	
			ppas.x8.medium.2	2 cores, 16 GB	2500	15000	
			ppas.x4.large.2	4 cores, 16 GB	2500	20000	250GB/500GB
			ppas.x8.large.2	4 cores, 32 GB	5000	30000	
			ppas.x4.xlarge.2	8 cores, 32 GB	5000	40000	500GB/1000GB
			ppas.x8.xlarge.2	8 cores, 64 GB	10000	60000	
			ppas.x4.2xlarge.2	16 cores, 64 GB	10000	80000	1000GB/2000GB
			ppas.x8.2xlarge.2	16 cores, 128 GB	12000	120000	
			ppas.x4.4xlarge.2	32 cores, 128 GB	12000	160000	2000GB/3000GB
			ppas.x8.4xlarge.2	32 cores, 256 GB	12000	240000	
		Dedicated host instance family	rds.ppas.st.h43	60 cores, 470 GB	12000	450000	3000GB/4000GB/5000GB/6000GB

5.Quick start

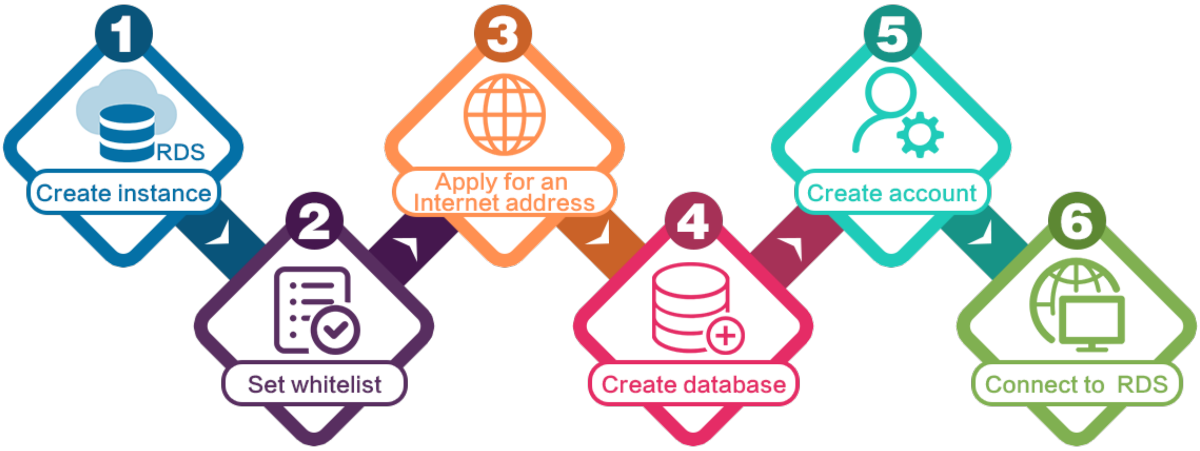
5.1. General workflow to use RDS PPAS

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

Quick start flowchart

If this is the first time that you use RDS PPAS, read Limits before you purchase an RDS PPAS instance.

The following flowchart shows the general workflow.



1. Create an ApsaraDB RDS for PPAS instance
2. Configure a whitelist for an ApsaraDB RDS for PPAS instance
3. Apply for or release a public endpoint for an ApsaraDB RDS for PPAS instance
4. Create databases and accounts for an ApsaraDB RDS for PPAS instance
5. Connect to an ApsaraDB RDS for PPAS instance

5.2. Create an ApsaraDB RDS for PPAS instance

This topic describes how to create an ApsaraDB RDS for PPAS instance by using the ApsaraDB RDS console. You can also call an API operation to create an ApsaraDB RDS for PPAS instance.

Prerequisites

You have an Alibaba Cloud account. For more information, see Sign up with Alibaba Cloud.

Procedure

1.
2. Configure the following parameters.

Parameter	Description

Parameter	Description
Billing Method	○ **Subscription**: A subscription instance is an instance that you can subscribe to for a specified period of time 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 require your pay-as-you-go instance, you can release the instance to reduce costs. **Note**
Region	The region where the RDS instance resides. ○ If your application is deployed on an Elastic Compute Service (ECS) instance, the RDS instance must reside in the same region as the ECS instance. For example, the RDS instance and the ECS instance can both reside in the China (Hangzhou) region. If the RDS instance and the ECS instance reside in different regions, they cannot communicate over an internal network and therefore they cannot deliver optimal performance. ○ If your application is deployed on an on-premises server or computer, we recommend that you select a region that is in close proximity to the on-premises server or computer.
Database Engine	The database engine and version that the RDS instance runs. Select **PPAS (Compatible with Oracle)**. Supported PPAS versions are 9.3 and 10. **Note** The available database engines and versions vary based on the region that you select.
Edition	**High-availability**: The database system consists of one primary RDS instance and one secondary RDS instance. These instances run in the classic high-availability architecture. **Note** The available RDS editions vary based on the region and database engine version that you select. For more information about RDS editions, see Overview of ApsaraDB RDS editions.

Parameter	Description
Storage Type	○ **Local SSD**: A local SSD resides on the same host as the database engine. You can store data on local SSDs to reduce I/O latency. ○ **ESSD**: Enhanced SSDs (ESSDs) come in three performance levels (PLs). ■ ESSD PL1: An ESSD of PL1 is a regular ESSD. ■ ESSD PL2: An ESSD of PL2 delivers IOPS and throughput that are approximately twice higher than the IOPS and throughput delivered by an ESSD of PL1. ■ ESSD PL3: An ESSD of PL3 delivers IOPS that is up to 20 times higher than the IOPS delivered by an ESSD of PL1. An ESSD of PL3 also delivers throughput that is up to 11 times higher than the throughput delivered by an ESSD of PL1. ESSDs of PL3 are suitable for business scenarios in which highly concurrent requests must be processed with high I/O performance and at low read and write latencies. ○ **Standard SSD**: A standard SSD is an elastic block storage device that is built on top of the distributed storage architecture. You can store data on standard SSDs to separate computing from storage.
Zone	The zone where the RDS instance resides. Each zone is an independent physical location within a region. For example, the China (Hangzhou) region contains Zone H, Zone I, and Zone J. ApsaraDB RDS supports the following two deployment methods: ○ **Multi-zone Deployment**: The primary RDS instance and the secondary RDS instance reside in different zones to provide zone-disaster recovery. This is the recommended deployment method. ○ **Single-zone Deployment**: The primary RDS instance and the secondary RDS instance reside in the same zone. **Note** If you select the RDS Basic Edition, you can select only the **Single-zone Deployment** method.
Instance Type	○ **Entry-level**: belongs to the general-purpose instance family. A general-purpose instance exclusively occupies the allocated memory and I/O resources, but shares CPU and storage resources with the other general-purpose instances that are deployed on the same server. ○ **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 highest configuration of the dedicated instance family. A dedicated host instance occupies all the CPU, memory, storage, and I/O resources on the server where the instance is deployed. **Note** For more information, see Primary ApsaraDB RDS instance types.

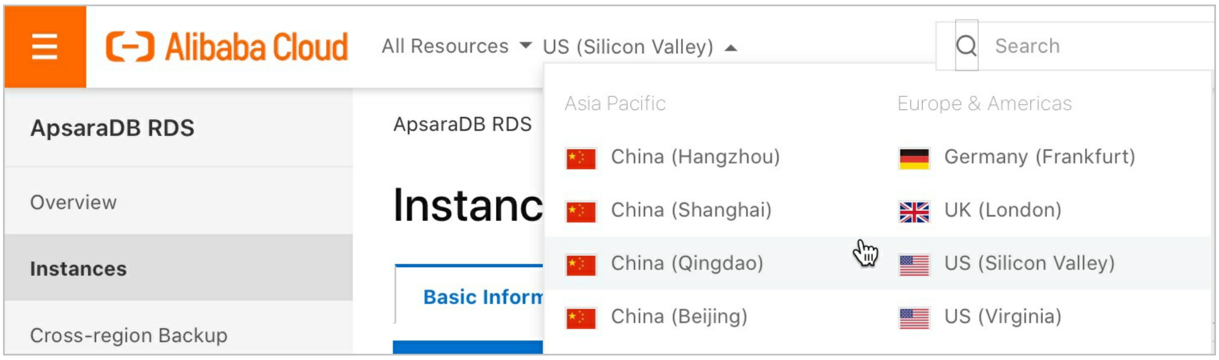
Parameter	Description
Capacity	The size of the storage space that is provided for the RDS instance to store data files, system files, binary log files, and transaction files. You can increase the storage capacity in increments of 5 GB. ⓘ **Note** The dedicated instance family used with local SSDs supports the exclusive allocations of resources. In this case, the storage capacity for each instance type is immutable. For more information about this issue, see Primary ApsaraDB RDS instance types.

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

Parameter	Description
Network Type	
Resource Group	The resource group to which the RDS instance belongs. You can retain the default resource group or select a custom resource group based on your business requirements.

5. In the lower-right corner of the page, click **Next: Confirm Order**.
6. Confirm the configuration of the RDS instance in the Parameters section, specify the **Purchase Plan** and **Duration** parameters, read and select **Terms of Service**, and then click **Pay Now**. You need to specify the Duration parameter only when you select the subscription billing method for the RDS instance.

> ⓘ **Note** If you select the subscription billing method for the RDS instance, we recommend that you select **Auto-Renew Enabled**. This prevents interruptions to your workloads even if you forget to review the RDS instance.



What to do next

- Configure a whitelist for an ApsaraDB RDS for PPAS instance
- Create databases and accounts for an ApsaraDB RDS for PPAS instance
- Apply for or release a public endpoint for an ApsaraDB RDS for PPAS instance
- Connect to an ApsaraDB RDS for PPAS instance

FAQ

- After I create an RDS instance, why does the ApsaraDB RDS console not respond and why am I unable to find the RDS instance?
  This issue may occur due to the following reasons:
  - The region that you selected is not the region where the RDS instance resides.
    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 are dynamically allocated within zones. After you submit the purchase order, the zone that you selected may run out of 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 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.
- If my RDS instance resides in a VPC, how many private IP addresses does it have?
  The number of private IP addresses that your RDS instance has varies based on the database engine and RDS edition that are used.
  - MySQL 5.5, 5.6, 5.7, and 8.0 on RDS High-availability Edition with local SSDs: 1
  - MySQL 5.6, 5.7, and 8.0 on RDS Enterprise Edition with local SSDs: 1
  - MySQL 5.7 on RDS Basic Edition with standard SSDs: 1
  - MySQL 8.0 on RDS Basic Edition with standard SSDs: 2
  - MySQL 5.7 and 8.0 on RDS High-availability Edition with standard SSDs or ESSDs: 3
  - MySQL 5.7 and 8.0 on RDS Enterprise Edition with standard SSDs or ESSDs: 1

References

- For more information about how to create an RDS instance by using the ApsaraDB RDS API, see Create an instance.
- For more information about how to create an RDS instance that runs a different database engine, see the following topics:
  - Create an ApsaraDB RDS for SQL Server instance
  - Create an ApsaraDB RDS for PostgreSQL instance
  - Create an ApsaraDB RDS for MariaDB TX instance

5.3. Configure a whitelist for an ApsaraDB RDS for PPAS instance

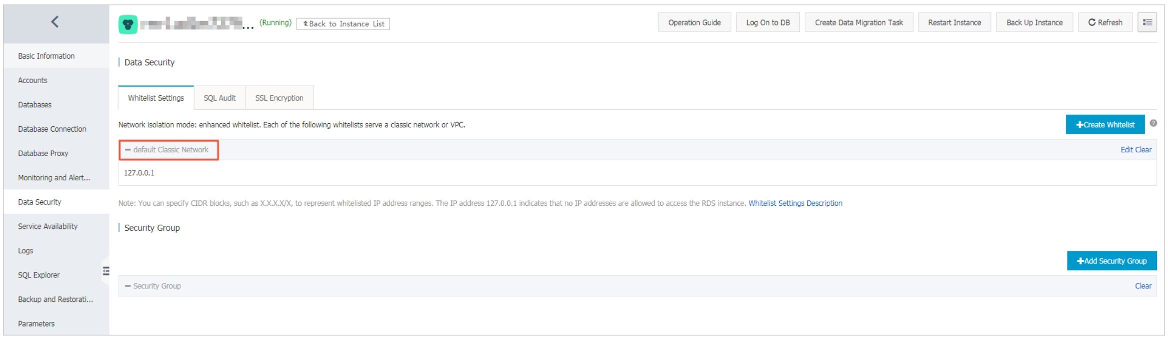
Context

Note

Configure an IP address whitelist in enhanced whitelist mode

1.

2.
3.
4.
5. Confirm your connection scenario and perform its required operations.



[redacted]... (Running) Back to Instance List

Data Security

Network isolation mode: enhanced whitelist. Each of the following whitelists serve a classic network or VPC.

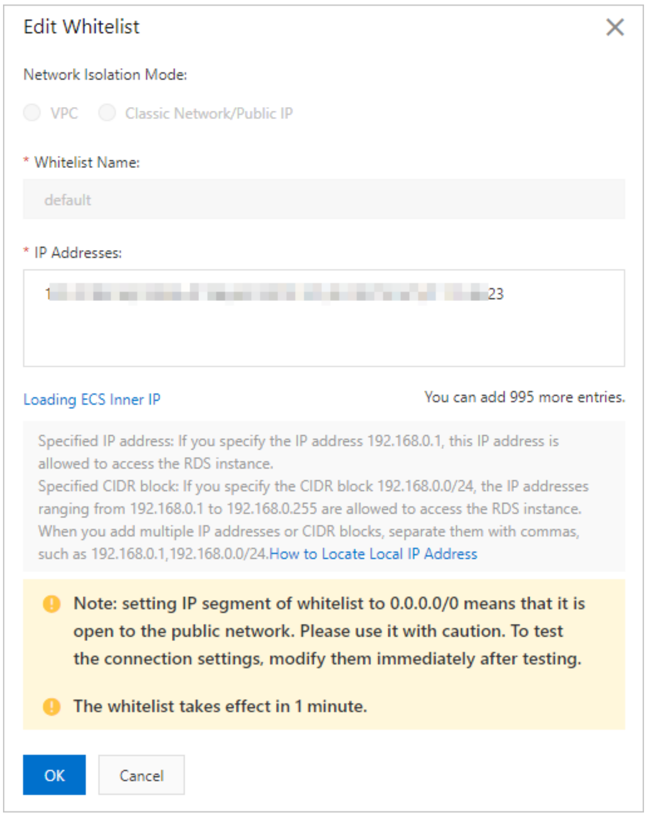
default Classic Network

127.0.0.1

Note: You can specify CIDR blocks, such as X.X.X.X/X, to represent whitelisted IP address ranges. The IP address 127.0.0.1 indicates that no IP addresses are allowed to access the RDS instance. Whitelist Settings Description

Security Group

Security Group



Edit Whitelist

Network Isolation Mode:

○ VPC ○ Classic Network/Public IP

* Whitelist Name:

default

* IP Addresses:

[redacted]

Loading ECS Inner IP

You can add 995 more entries.

Specified IP address: If you specify the IP address 192.168.0.1, this IP address is allowed to access the RDS instance.
Specified CIDR block: If you specify the CIDR block 192.168.0.0/24, the IP addresses ranging from 192.168.0.1 to 192.168.0.255 are allowed to access the RDS instance.
When you add multiple IP addresses or CIDR blocks, separate them with commas, such as 192.168.0.1,192.168.0.0/24.How to Locate Local IP Address

Note: setting IP segment of whitelist to 0.0.0.0/0 means that it is open to the public network. Please use it with caution. To test the connection settings, modify them immediately after testing.

The whitelist takes effect in 1 minute.

Connection scenario	Operation
(Recommended) Your ECS and RDS instances reside in the same VPC.	
Your ECS and RDS instances reside in different VPCs.	
Your ECS and RDS instances both reside in the classic network.	

Connection scenario	Operation
Your ECS instance resides in the classic network. Your RDS instance resides in a VPC.	
Your ECS instance resides in a VPC. Your RDS instance resides in the classic network.	
The host that requires access to your RDS instance resides outside the cloud.	i. Navigate to the **Whitelist Settings** tab of the Data Security page, and click **Edit** to the right of the IP address whitelist labeled **default Classic Network**. ii. In the dialog box that appears, enter the public IP address of your host in the IP Addresses field and click **OK**. Note ■ Applications running on your host connect to the public endpoint of your RDS instance. ■ For more information, see How do I locate the IP address connected to an RDS for PostgreSQL or RDS for PPAS instance?

Note

Configure an IP address whitelist in standard whitelist mode

1.
2.
3.
4.
5. Click **Create Whitelist** and in the Create Whitelist dialog box set the **Whitelist Name** parameter. This allows you to create an IP address whitelist. Otherwise, click **Modify** to the right of an existing IP address whitelist. This allows you to modify the IP address whitelist.
6. Enter the specified IP addresses or CIDR blocks. Then, click **ok**.

Note

- If you enter more than one IP address or CIDR block, you must separate these IP addresses or CIDR blocks with commas (,). Do not add spaces preceding or following the commas. Example: `192.168.0.1,172.16.213.9` .
- A maximum of 1,000 IP addresses and CIDR blocks can be configured for each RDS instance. If you want to enter a large number of IP addresses, we recommend that you merge discontinuous IP addresses into CIDR blocks, for example, 10.10.10.0/24.
- After you add IP addresses or CIDR blocks to the IP address whitelist labeled **default** , ApsaraDB RDS deletes the default IP address 127.0.0.1.

Common whitelist configuration errors

-
-
-
-

Related operations

API	Description
DescribeDBInstanceIPArrayList	Queries the IP address whitelists of an ApsaraDB RDS instance.
ModifySecurityIps	Modifies an IP address whitelist of an ApsaraDB RDS instance.

5.4. Create databases and accounts for an ApsaraDB RDS for PPAS instance

This topic describes how to create databases and accounts for an ApsaraDB RDS for PPAS instance. After you create an RDS instance, you must create databases and accounts for the RDS instance. If the RDS instance runs PPAS, you must create a privileged account in the ApsaraDB for RDS console. Then, you can create and manage databases by using a client. The pgAdmin 4 client is used in the example in this topic.

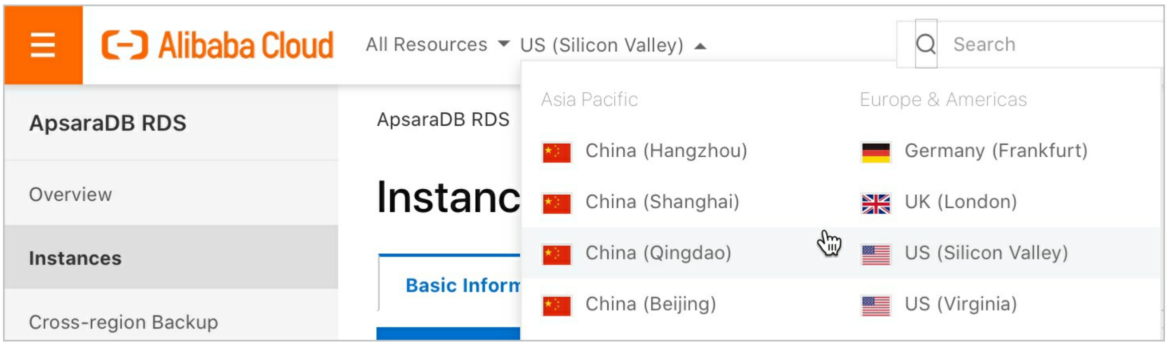
Precautions

- Databases on the same instance share all of the resources that belong to the instance. Each ApsaraDB RDS for PPAS instance supports one privileged account, countless standard accounts, and countless databases. You can create and manage standard accounts and databases by using SQL statements.
- To migrate an on-premises database to an RDS instance, you must create a database and an account with the same names on the RDS instance.

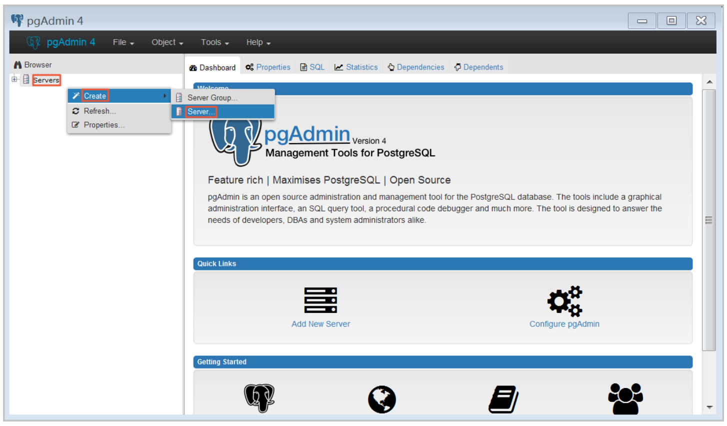
- Use service roles to create accounts and follow the principle of least privilege to assign appropriate read-only and read/write permissions to the accounts. When necessary, you can create more than one account and allow each account to access only the data within its authorized workloads. If an account does not need to write data to a database, assign read-only permissions to the account.
- For security purposes, we recommend that you configure strong passwords for the accounts that you created and change the passwords on a regular basis.

Procedure

1. Log on to the ApsaraDB for RDS console.
2. In the top navigation bar, select the region where the target RDS instance resides.

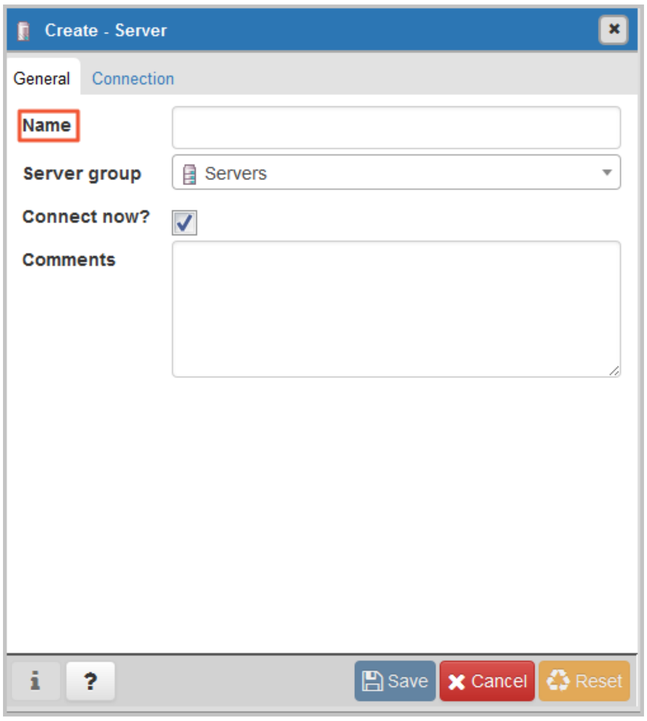


3. Find the target RDS instance and click its ID.
4. In the left-side navigation pane, click **Accounts**.
5. Click **Create Initial Account**.
6. Enter the information of the account that you want to create.
   Parameter description:
   - Database Account: Enter the username of the account. The username 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.
   - Password: Enter the password of the account.
     - 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.
     - Special characters include ! @ # $ % ^ & * ( ) _ + - =
   - Confirm Password: Enter the password again to make sure that you enter the correct password.
7. Click **OK**.
8. Add the IP address that is used to access the RDS instance to the RDS whitelist. For more information, see Configure a whitelist for an ApsaraDB RDS for PPAS instance.
9. Start the pgAdmin 4 client.
10. Right-click **Servers** and select **Create** > **Server**.



pgAdmin is an open source administration and management tool for the PostgreSQL database. The tools include a graphical administration interface, an SQL query tool, a procedural code debugger and much more. The tool is designed to answer the needs of developers, DBAs and system administrators alike.

11. On the **General** tab of the **Create - Server** dialog box, enter the name of the server.



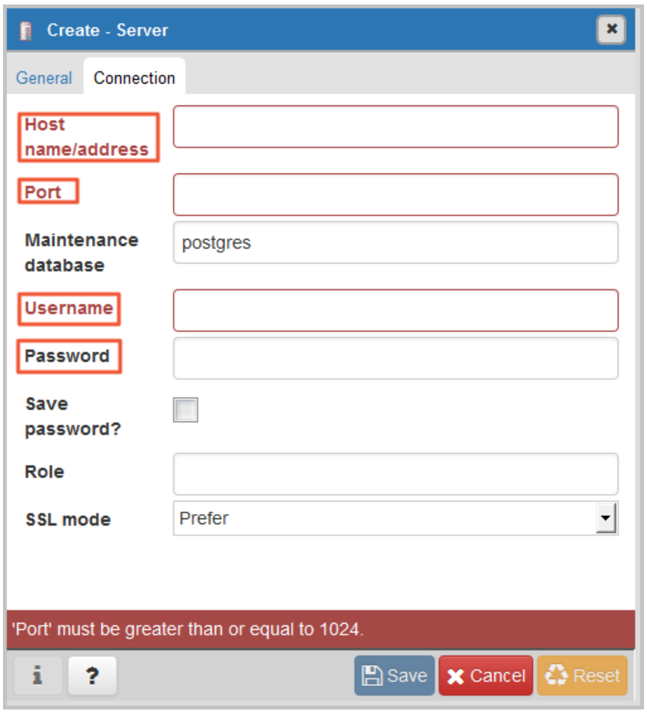
Name

Server group: Servers

Connect now? ☑

Comments

12. Click the **Connection** tab and enter the information of your RDS instance.



Create - Server

Host name/address:

Port:

Maintenance database: postgres

Username:

Password:

Save password? □

Role:

SSL mode: Prefer

'Port' must be greater than or equal to 1024.

Parameter description:

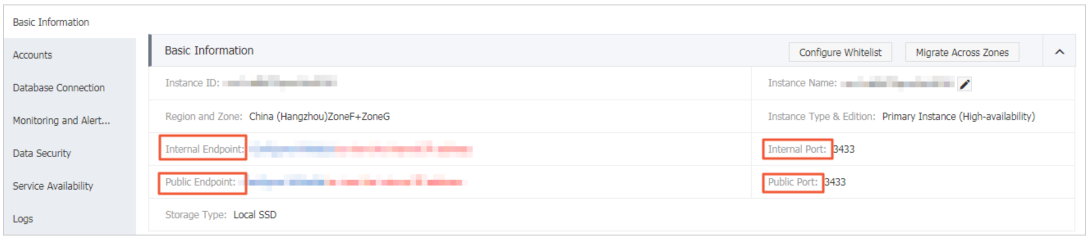
- Host name/address: Enter the endpoint of the RDS instance. If you connect to the RDS instance over the internal network, enter the internal endpoint of the RDS instance. If you connect to the RDS instance over the Internet, enter the public endpoint of the RDS instance. To view the internal and public endpoints and port numbers of the RDS instance, follow these steps:

  a. Log on to the ApsaraDB for RDS console.

  b. In the top navigation bar, select the region where your RDS instance resides.

  c. Find your RDS instance and click its ID.

  d. On the Basic Information page, find the internal and public endpoints and their port numbers.

  Basic Information

  Instance ID: [redacted]

  Instance Name: [redacted]

  Region and Zone: China (Hangzhou)ZoneF+ZoneG

  Instance Type & Edition: Primary Instance (High-availability)

  Internal Endpoint: [redacted]

  Internal Port: 3433

  Public Endpoint: [redacted]

  Public Port: 3433

  Storage Type: Local SSD

- Port: Enter the port number of your RDS instance. If you connect to your RDS instance over an internal network, enter the internal port number of your RDS instance. If you connect to your RDS instance over the Internet, enter the public port number of your RDS instance.

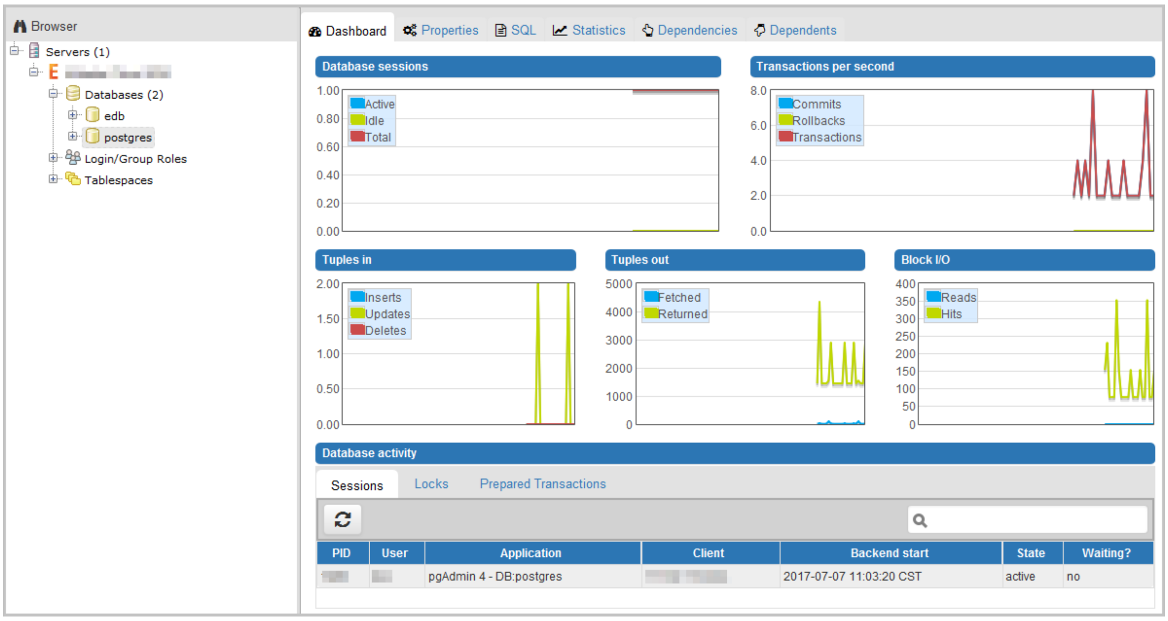
- Username: Enter the username of the privileged account that is used to log on to your RDS instance.

- Password: Enter the password of the account that is used to log on to your RDS instance.

13. Click **Save**.

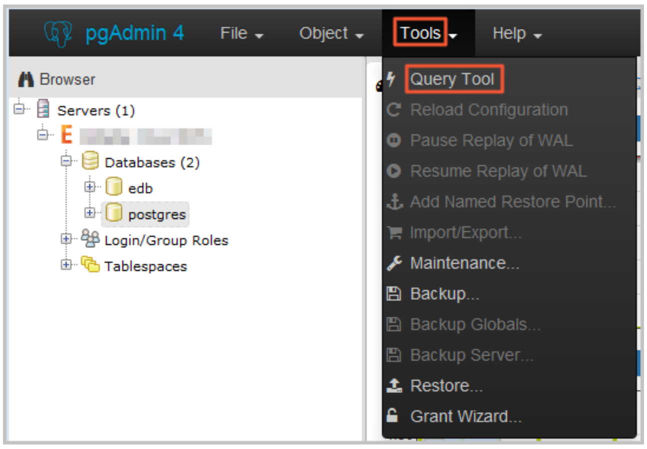
14. If the connection information is correct, choose **Servers > Server Name > Databases > postgres**. The connection is successful if the following interface is displayed.

> ⓘ **Note** postgres is the default system database of the RDS instance. Do not perform operations on this database.



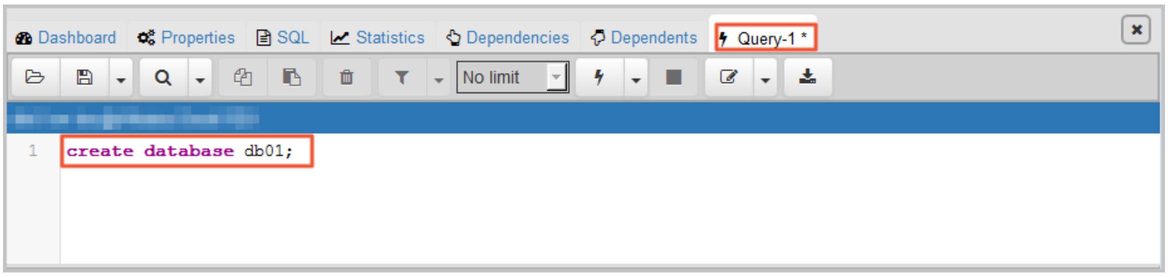
PID	User	Application	Client	Backend start	State	Waiting?
[redacted]	[redacted]	pgAdmin 4 - DB:postgres	[redacted]	2017-07-07 11:03:20 CST	active	no

15. Click **postgres** and select **Tools** > **Query Tool**.



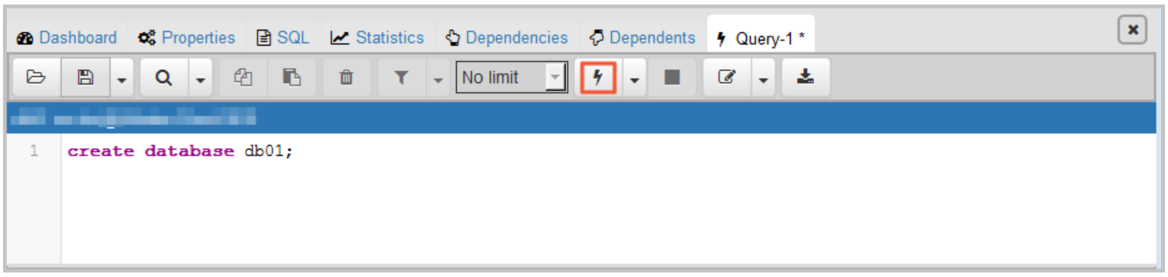
16. On the **Query-1** tab, enter the following command to create a database:

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



```
create database db01;
```

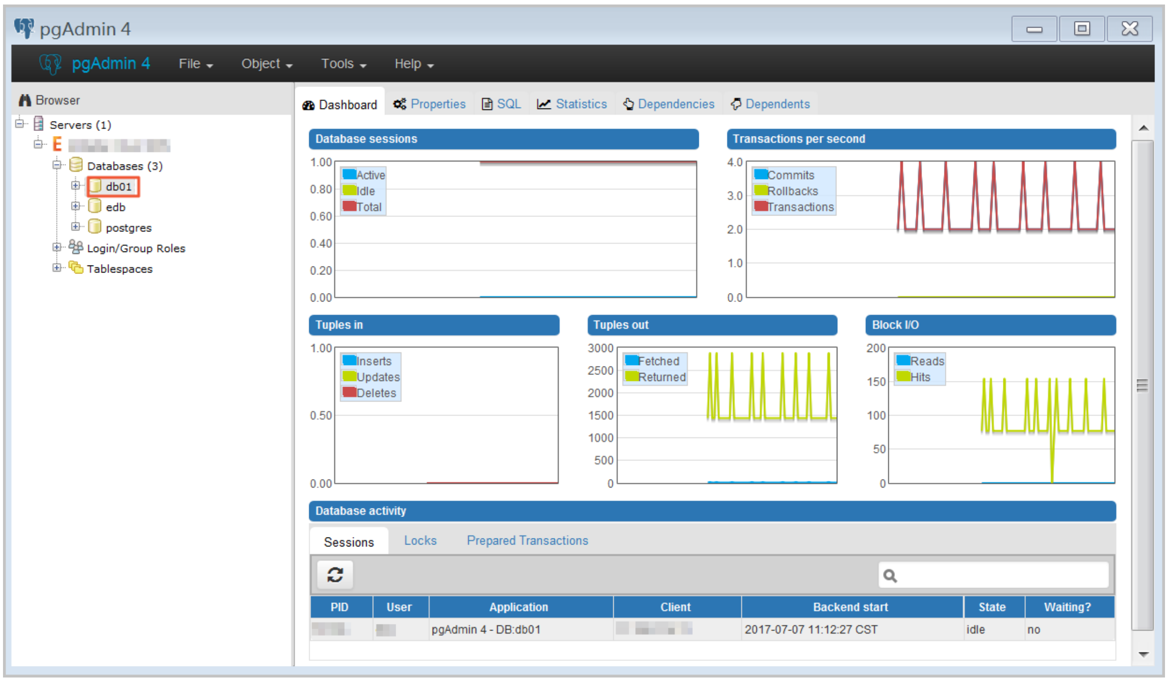
17. Click the **Execute/Refresh** icon.



[redacted]

```
create database db01;
```

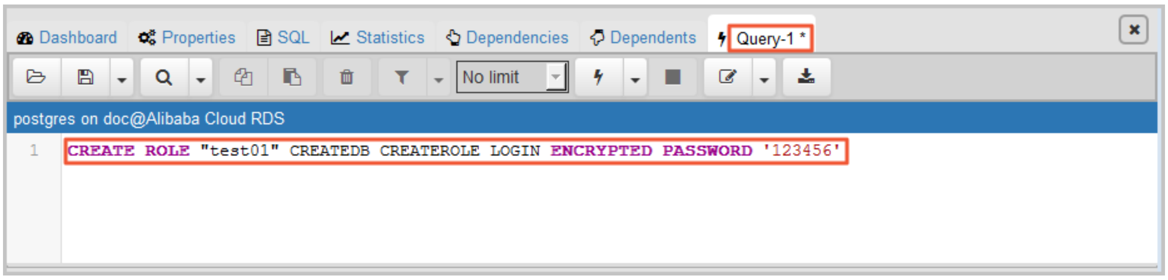
18. If the execution is successful, the database is created. Right-click **Databases** and select **Refresh**. Then you can find the new database.



PID	User	Application	Client	Backend start	State	Waiting?
[redacted]	[redacted]	pgAdmin 4 - DB:db01	[redacted]	2017-07-07 11:12:27 CST	idle	no

19. On the **Query-1** tab, enter the following command to create an account:

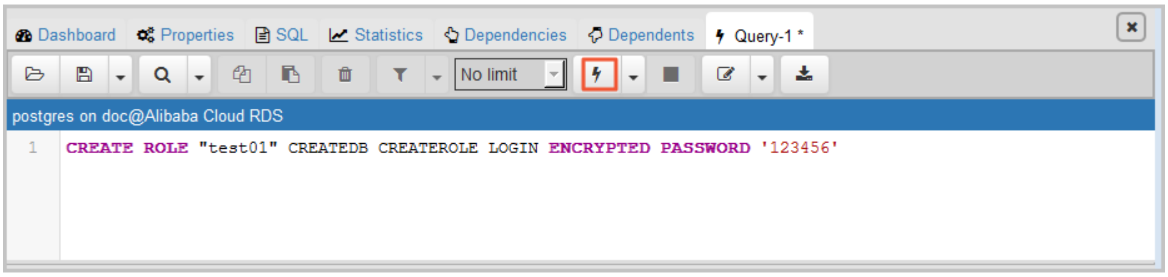
```
CREATE ROLE "username" CREATEDB CREATEROLE LOGIN ENCRYPTED PASSWORD 'password';
```



postgres on doc@Alibaba Cloud RDS

```
CREATE ROLE "test01" CREATEDB CREATEROLE LOGIN ENCRYPTED PASSWORD '123456'
```

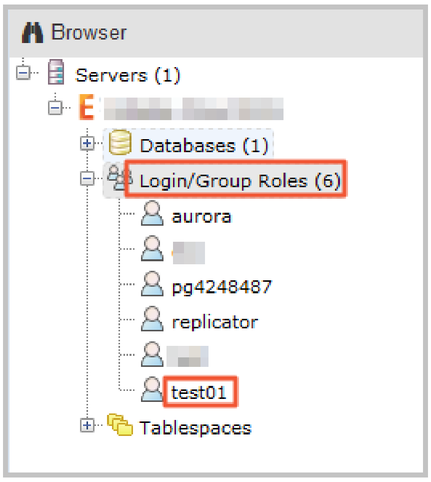
20. Click the **Execute/Refresh** icon.



postgres on doc@Alibaba Cloud RDS

```
CREATE ROLE "test01" CREATEDB CREATEROLE LOGIN ENCRYPTED PASSWORD '123456'
```

21. If the execution is successful, the account is created. Right-click **Login/Group Roles** and select **Refresh**. Then you can find the new account.



FAQ

Can I manage the accounts created on my primary RDS instance from its read-only instances?

No, although accounts created on the primary instance are replicated to its read-only instances, you cannot manage the accounts on the read-only instances. Read-only instances only allow accounts to read data.

Related operations

Operation	Description
Create an account	Creates an account on an ApsaraDB for RDS instance.

5.5. Connect to an ApsaraDB RDS for PPAS instance

After you complete the initial configurations, you can use an Elastic Compute Service (ECS) instance or a database client to connect to an ApsaraDB RDS for PPAS instance.
You can use a database client or Alibaba Cloud Data Management (DMS) to connect to an RDS instance. This topic describes how to connect to an ApsaraDB RDS for PPAS instance by using DMS and the pgAdmin 4 client.

Background information

You can log on to DMS from the ApsaraDB for RDS console and then connect to an RDS instance. DMS provides an integrated solution for data management. DMS supports data management, schema management, access control, BI charts, trend analysis, data tracking, performance optimization, and server management. DMS can be used to manage NoSQL databases and relational databases, such as MySQL, SQL Server, PostgreSQL, MongoDB, and Redis. It can also be used to manage Linux servers.

You can also use a database client to connect to an RDS instance. ApsaraDB RDS for PPAS is fully compatible with PPAS. You can connect to RDS in the similar way you connect to an on-premises PPAS server. This topic describes how to use the pgAdmin 4 client to connect to an RDS instance. This topic also serves as a reference if you choose to use other database clients. When you use a client to connect to an RDS instance, you must select the internal and public endpoints based on your network environment:

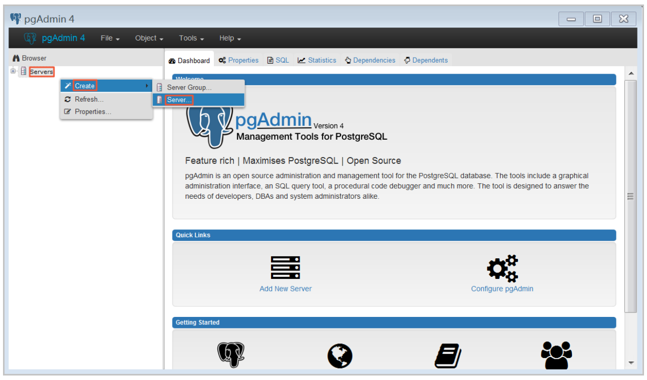
- If the client is deployed on an ECS instance that resides in the same region and has the same network type as the RDS instance, you can use the internal endpoint. For example, if the ECS and RDS instances both reside in VPCs in the China (Hangzhou) region, use the internal endpoint to establish a secure connection.
- In other situations, use the public endpoint.

Use DMS to connect to an RDS instance

For more information, see Use DMS to log on to an ApsaraDB RDS for PPAS instance.

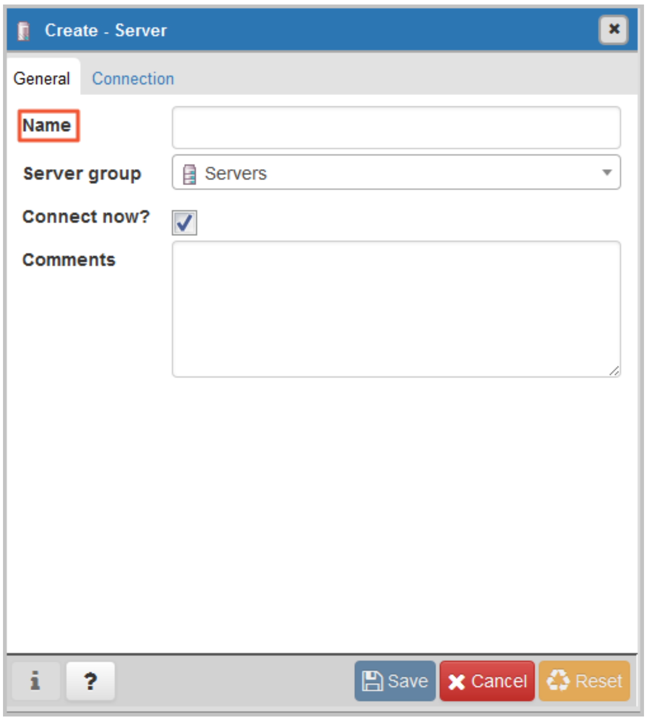
Use a client to connect to an RDS instance

1. Add the IP address that is used to access your RDS instance to an IP address whitelist. For more information about how to configure an IP address whitelist, see Configure a whitelist for an ApsaraDB RDS for PPAS instance.
2. Start the pgAdmin 4 client.
3. Right-click **Servers** and choose **Create** > **Server**.



pgAdmin is an open source administration and management tool for the PostgreSQL database. The tools include a graphical administration interface, an SQL query tool, a procedural code debugger and much more. The tool is designed to answer the needs of developers, DBAs and system administrators alike.

4. On the **General** tab of the **Create - Server** dialog box, enter the name of the server.



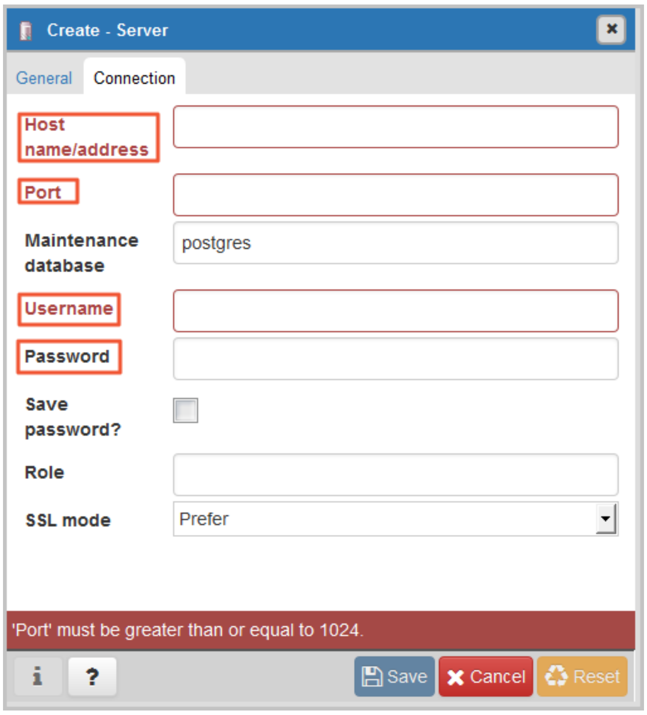
Name

Server group: Servers

Connect now? ☑

Comments

5. Click the **Connection** tab and enter the information of the target RDS instance.



Host name/address

Port

Maintenance database: postgres

Username

Password

Save password? □

Role

SSL mode: Prefer

'Port' must be greater than or equal to 1024.

Parameter description:

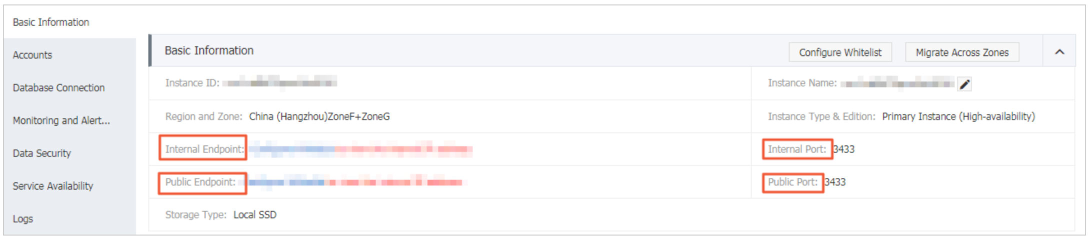
- Host name/address: Enter the endpoint of the RDS instance. If you connect to the RDS instance over the internal network, enter the internal endpoint of the RDS instance. If you connect to the RDS instance over the Internet, enter the public endpoint of the RDS instance. To view the internal and public endpoints and port numbers of the RDS instance, follow these steps:

  a. Log on to the ApsaraDB for RDS console.

  b. In the top navigation bar, select the region where your RDS instance resides.

c. Find your RDS instance and click its ID.

d. On the Basic Information page, find the internal and public endpoints and their port numbers.



Basic Information

Basic Information

Instance ID: [redacted]

Instance Name: [redacted]

Region and Zone: China (Hangzhou)ZoneF+ZoneG

Instance Type & Edition: Primary Instance (High-availability)

Internal Endpoint: [redacted]

Internal Port: 3433

Public Endpoint: [redacted]

Public Port: 3433

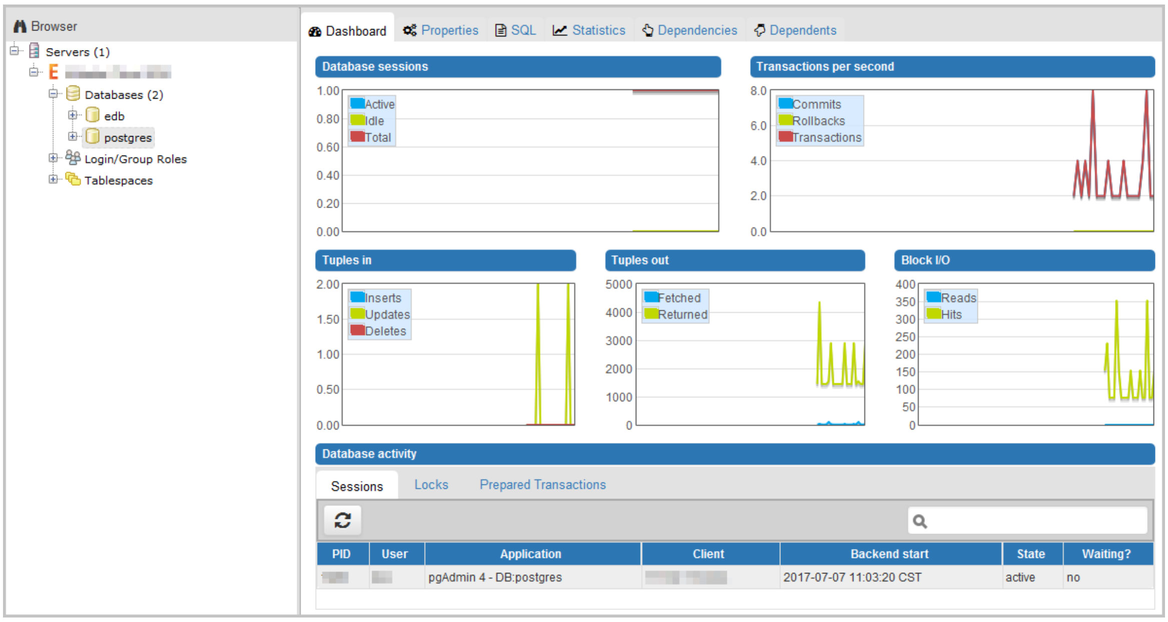
Storage Type: Local SSD

- Port: Enter the port number of your RDS instance. If you connect to your RDS instance over an internal network, enter the internal port number of your RDS instance. If you connect to your RDS instance over the Internet, enter the public port number of your RDS instance.
- Username: Enter the username of the privileged account that is used to log on to your RDS instance.
- Password: Enter the password of the account that is used to log on to your RDS instance.

6. Click **Save**.

7. If the connection information is correct, choose **Servers > Server Name > Databases > edb** or **postgres**. The connection is successful if the following interface is displayed.

> **Note** edb and postgres are default system databases of your RDS instance. Do not perform any operation in these databases.



PID	User	Application	Client	Backend start	State	Waiting?
[redacted]	[redacted]	pgAdmin 4 - DB:postgres	[redacted]	2017-07-07 11:03:20 CST	active	no

FAQ

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

You can install third-party dependencies for your functions in Function Compute and use built-in modules to obtain the data of an RDS instance. For more information, see Install third-party dependencies.

5.6. Read-only instances

5.6.1. Overview of read-only ApsaraDB RDS for PPAS instances

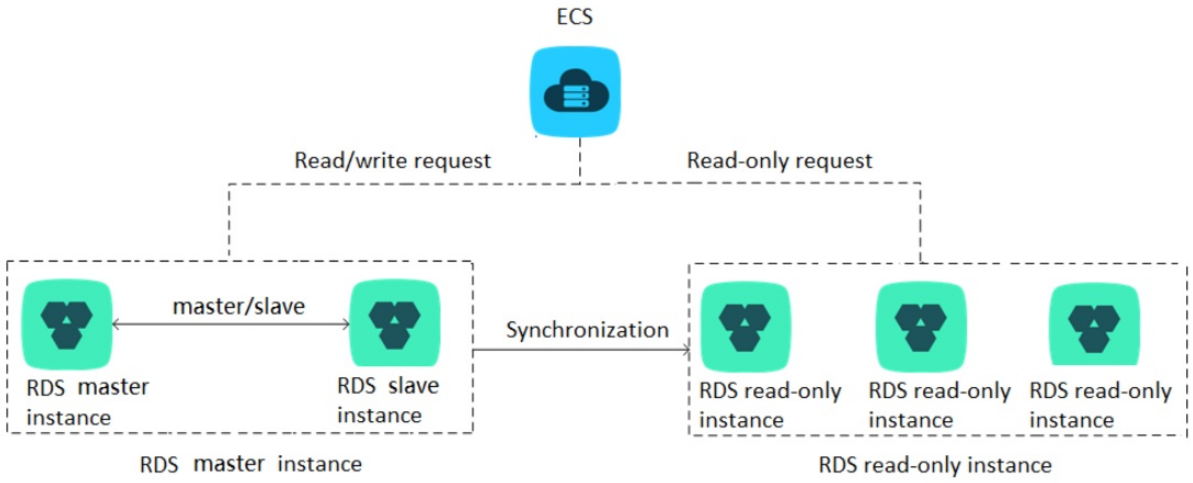
This topic provides an overview of read-only ApsaraDB RDS for PPAS instances. If a large number of read requests overwhelm your primary instance, your business may be interrupted. In this situation, you can create one or more read-only instances to offload read requests from the primary instance and increase the throughput of your application.

Overview

While a read-only instance is being created, the data is replicated from the secondary instance. The data on the secondary instance is consistent with that on the primary instance. After an update to the data on the primary instance is complete, this update is immediately synchronized to all of the read-only instances.

> Note
>
> - The primary instance must belong to the dedicated instance family and provide at least 8 CPU cores and 32 GB of memory.
> - Each read-only instance works in a single-node architecture, where no instances are provided as backups.

The following figure shows the topology of read-only instances in a database system.



Billing

You are charged an hourly rate for each read-only instance based on pay-as-you-go billing.

Features

- Billing method: Read-only instances use pay-as-you-go billing to reduce costs.
- Region and zone: Read-only instances reside in the same region as the primary instance, but possibly in different zones.
- Specifications and storage capacity: The specifications and storage capacity of read-only instances

cannot be lower than those of the primary instance.

- Change the network type of an ApsaraDB RDS for PPAS instance: The network type of read-only instances can be different from that of the primary instance.
- Account and database management: Read-only instances do not require database or account maintenance, because their database and account information is synchronized with the primary instance.
- IP address whitelist: While read-only instances are being created, they automatically replicate the IP address whitelists of the primary instance. However, the IP address whitelists on read-only instances are independent of the IP address whitelists that are configured on the primary instance. For more information about how to modify the whitelists of a read-only instance, see Configure a whitelist for an ApsaraDB RDS for PPAS instance.
- Monitoring and alerting: You can monitor system performance metrics, such as the disk usage, input/output operations per second (IOPS), maximum number of connections, and CPU utilization.

Limits

- A maximum of five read-only instances are allowed for a primary instance.
- Read-only instances do not support backup settings or manual backups.
- You cannot migrate data to read-only instances.
- You cannot create or delete databases on read-only instances.
- You cannot create or delete accounts, authorize accounts, or change the passwords of accounts on read-only instances.

FAQ

Can I manage accounts created in the primary instance from its read-only instances?

No, although accounts created on the primary instance are replicated to its read-only instances, you cannot manage the accounts on the read-only instances. Read-only instances only allow accounts to read data.

5.6.2. Create an RDS PPAS read-only instance

This topic describes how to create an RDS PPAS read-only instance. You can create read-only instances to process massive read requests sent to the database and increase the application throughput. A read-only instance is a read-only copy of the master instance. Changes to the master instance are also automatically synchronized to all relevant read-only instances.
For more information, see Overview of read-only ApsaraDB RDS for PPAS instances.

Prerequisites

- The master instance is an RDS PPAS 10.0 instance.
- The configuration of the master instance must be at least 8-core 32 GB (dedicated or dedicated-host instance).

Precautions

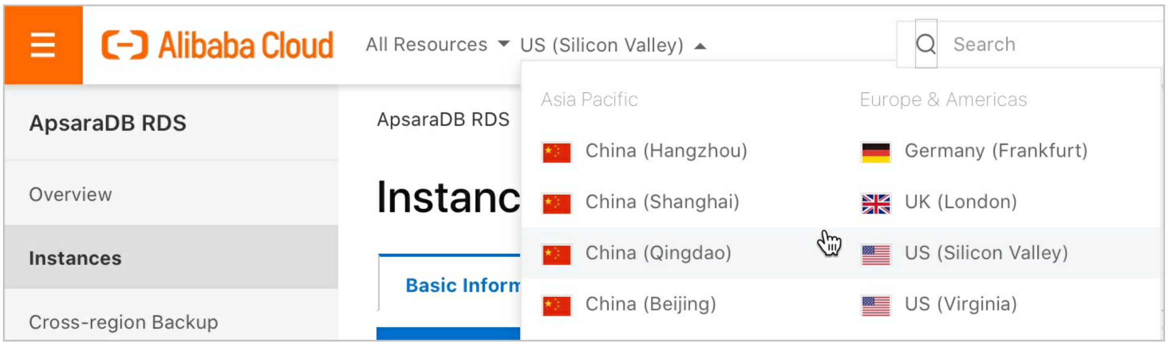
- You can create read-only instances under a master instance but cannot switch an existing instance to a read-only instance.
- Creating a read-only instance does not affect the master instance because the read-only instance copies data from the slave instance.
- Read-only instances do not inherit parameter settings of the master instance, but use default

parameter settings. You can modify the parameter settings on the console.

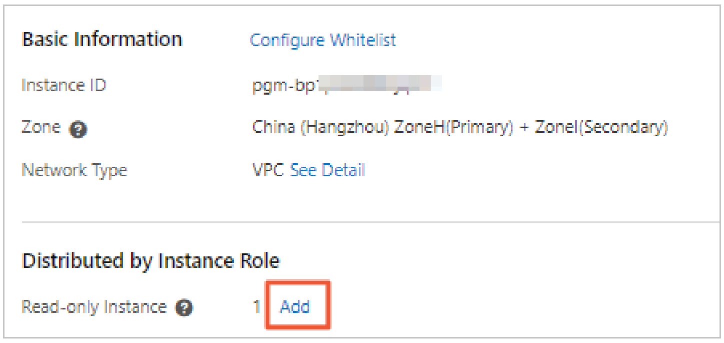
- Specifications and storage capacity of each read-only instance cannot be lower than those of the master instance.
- Each master instance can have up to five read-only instances.
- A read-only instance is charged according to the Pay-As-You-Go billing method. That is, fees are deducted for a read-only instance once every hour.

Create a read-only instance

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



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



Basic Information Configure Whitelist

Instance ID pgm-bp[redacted]

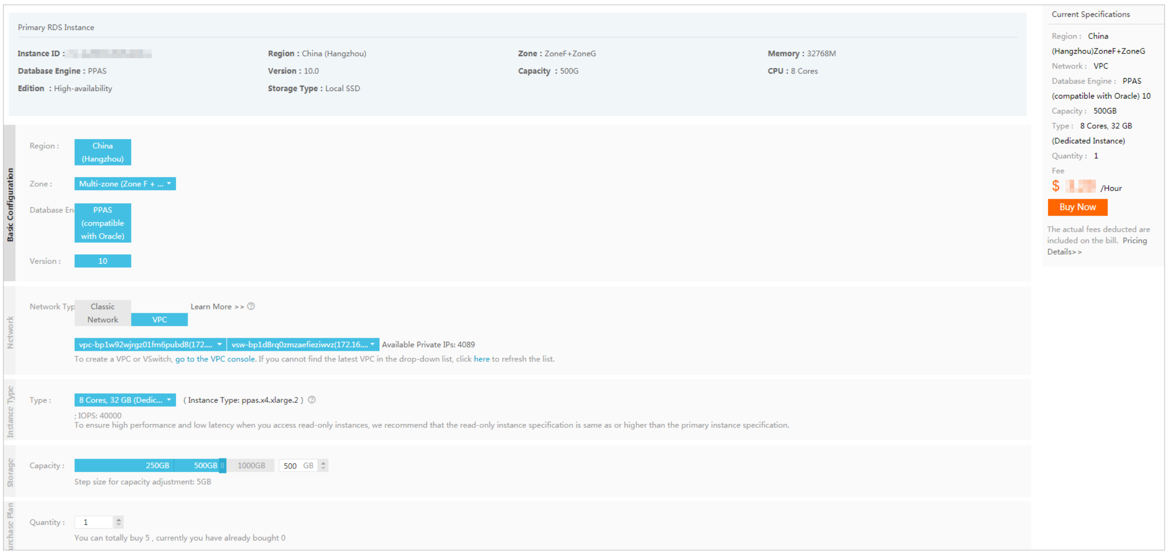
Zone China (Hangzhou) ZoneH(Primary) + ZoneI(Secondary)

Network Type VPC See Detail

Distributed by Instance Role

Read-only Instance 1 Add

5. On the purchase page, select the instance configuration and click **Buy Now**.



Primary RDS Instance

Instance ID : [redacted]
Region : China (Hangzhou)
Zone : ZoneF+ZoneG
Memory : 32768M
Database Engine : PPAS
Version : 10.0
Capacity : 500G
CPU : 8 Cores
Edition : High-availability
Storage Type : Local SSD

Basic Configuration

Region : China (Hangzhou)

Zone : Multi-zone (Zone F + ...

Database En PPAS (compatible with Oracle)

Version : 10

Network

Network Typ Classic Network VPC Learn More >>

vpc-bp1w92wjrgz01fm6pubd8(172.... vsw-bp1d8rq0zmzaefieziwvz(172.16.... Available Private IPs: 4089

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.

Instance Type

Type : 8 Cores, 32 GB (Dedic... (Instance Type: ppas.x4.xlarge.2)

; IOPS: 40000

To ensure high performance and low latency when you access read-only instances, we recommend that the read-only instance specification is same as or higher than the primary instance specification.

Storage

Capacity : 250GB 500GB 1000GB 500 GB

Step size for capacity adjustment: 5GB

Purchase Plan

Quantity : 1

You can totally buy 5 , currently you have already bought 0

Current Specifications

Region : China (Hangzhou)ZoneF+ZoneG

Network : VPC

Database Engine : PPAS (compatible with Oracle) 10

Capacity : 500GB

Type : 8 Cores, 32 GB (Dedicated Instance)

Quantity : 1

Fee

$ [redacted] /Hour

Buy Now

The actual fees deducted are included on the bill. Pricing Details>>

> Note
>
> - We recommend that you deploy read-only instances and the master instance in the same VPC.
> - The configuration (memory and storage) of each read-only instance must be equal to or higher than that of the master instance.
> - You can deploy up to five read-only instances to improve availability and horizontally scale performance.

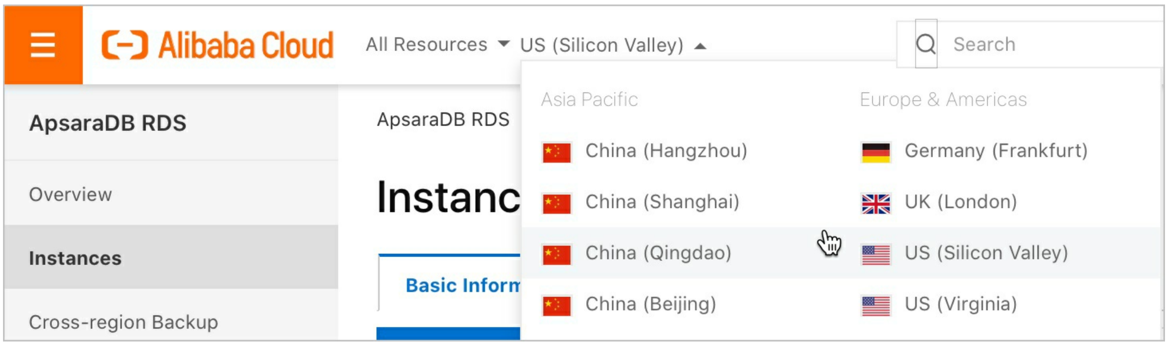
6. On the **Order Confirmation** page, review the order information, select **Terms of Service, Service Level Agreement, and Terms of Use**, click Pay Now, and complete the payment.

The instance creation takes a few minutes.

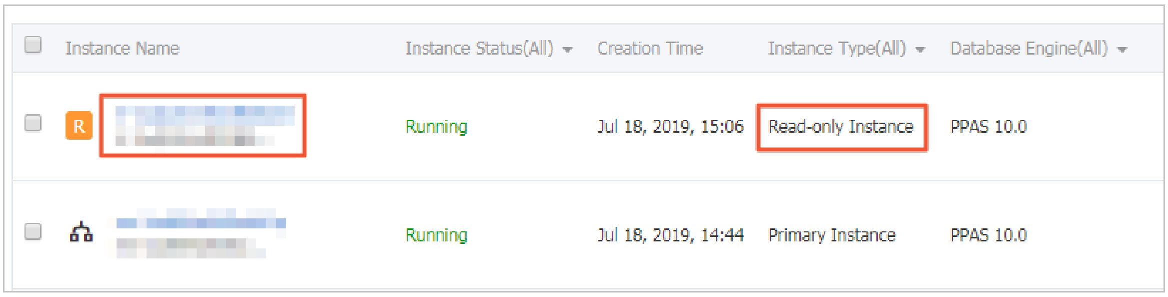
View a read-only instance

To view a read-only instance in the instance list, follow these steps:

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



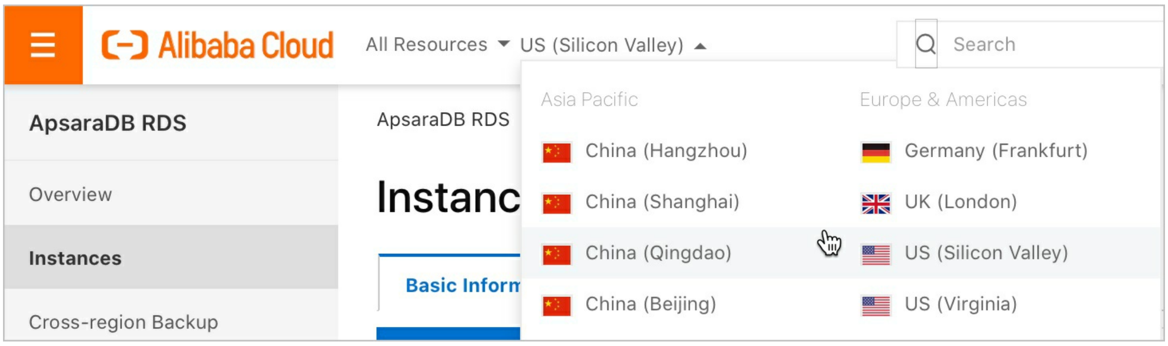
3. In the instance list, find the read-only instance and click its ID.



☐	Instance Name	Instance Status(All)	Creation Time	Instance Type(All)	Database Engine(All)
☐	R [redacted]	Running	Jul 18, 2019, 15:06	Read-only Instance	PPAS 10.0
☐	[redacted]	Running	Jul 18, 2019, 14:44	Primary Instance	PPAS 10.0

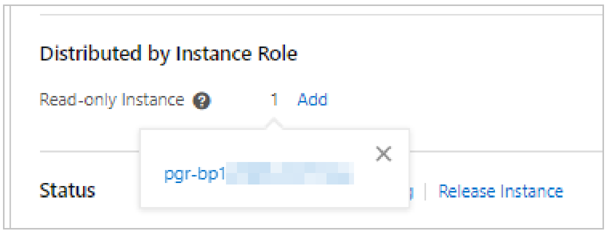
To view a read-only instance on the **Basic Information** page of the master instance, follow these steps:

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



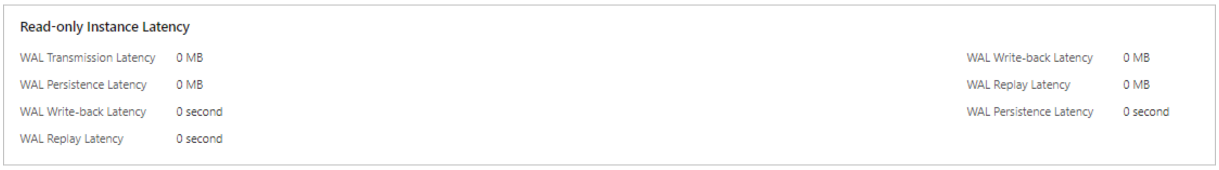
3. Find the master instance and click its ID.

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



View the delay of a read-only instance

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



Read-only Instance Latency

WAL Transmission Latency	0 MB	WAL Write-back Latency	0 MB
WAL Persistence Latency	0 MB	WAL Replay Latency	0 MB
WAL Write-back Latency	0 second	WAL Persistence Latency	0 second
WAL Replay Latency	0 second		

APIs

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

6.Data migration

6.1. Use DTS to migrate PPAS data

You can use data transmission service (DTS) to migrate data from a local database to apsaradb RDS for PPAS without stopping services. The migration process has no impact on the local Oracle database.

Background information

DTS Data Migration supports structural migration and full migration of PPAS.

- Schema migration
  DTS migrates the schemas of the required objects to the destination database. Currently DTS supports structural migration of objects such: tables, views, synonyms, triggers, stored procedure, stored functions, packages, custom types.
- Full data migration
  DTS migrates all data of the migration objects in a local database to the target instance. If data is written to the local Oracle database during migration, the incremental data may not be migrated to the RDS instance. Therefore, to ensure data consistency, we recommend that you full migration data during off-peak hours.

Limits

Migrating a PPAS local database to an RDS has the following restrictions.

- DDL operations that are performed during incremental data migration cannot be synchronized to the destination database.
- Migration of materialized views is not supported.
- When the structure is migrated, the reverse index is migrated to a normal index.
- When the structure is migrated, The Bitmap index is migrated to a normal index.
- When the structure is migrated, the partitioned index is migrated to an index that is created separately on each partition.

Prerequisites

You have prepared the RDS instance. For more information, see Configure endpoints for an RDS for PPAS instance and Create databases and accounts for an ApsaraDB RDS for PPAS instance.

Preparations

Before you migrate, create a migration account respectively in the local database and the RDS instance. Create the database to be migrated in the RDS instance. Grant the migration account the read and write permissions on the database to be migrated. The following table lists the permissions required for database accounts when different migration types are used.

Database type	Schema migration	Full data migration
Local Oracle instance	Schema owner	Schema owner
PPAS instance on RDS	Schema owner	Schema owner

1. Create a migration account in the on-premises database through the PostgreSQL client.

```
CREATE USER username IDENTIFIED BY password
```

The following table lists the parameters of the function.

- username: the account to be created.
- password: the password for logging on to this account.

Example:

```
CREATE USER myuser IDENTIFIED BY mypassword
```

2. Grant permissions to the migration account in the local database. The required permissions are described in the table above.

```
GRANT privileges ON tablename TO username;
```

The following table lists the parameters of the function.

- privileges: the permissions granted to the account, such as SELECT, INSERT, and UPDATE. To grant ALL permissions to the account, use ALL.
- tablename: the table name. To grant the permissions for all tables to the account, use the wildcard (*).
- username: the account to which you want to grant permissions.

The scenarios are as follows:

```
GRANT ALL ON* TO myuser
```

Official migration

1. In RDS console click **migrate databases**, enter DTS from the shortcut menu.
2. In the left-side navigation pane, click **data Migration**.
3. In **migration tasks** right click **create a migration task**.
4. Enter the task name, local database information, and target database information, and click **authorize the whitelist and go to the next step**. From the shortcut menu.
   - Task name: enter a default value for the task name.
   - Source Database
     - **Instance type**: The instance type of the local database. Select **user-created database with a public IP address**.
     - **Instance region**: The region where the local database is located.
     - **Database Engine**: the type of local database. Select **Oracle**.
     - **Hostname or IP address**: The public endpoint of the on-premises database.
     - **Port**: The public port of the local database.
     - **Instance type**: indicates whether the local database is a RAC cluster.
     - **SID**: The SID of the local database.
     - **Database account**: The Migration account of the local database.
     - **Database password**: the password of the migration account of the local database.
   - Destination Database
     - **Instance type**: The instance type of the cloud database, Select **RDS instance**.
     - **Instance region**: The region where the cloud database is located.

    - **RDS instance ID**: the ID of the destination RDS instance. Click the drop-down menu to automatically associate the RDS instance of the account currently logged in to the management console, click to select the required instance.
    - **Database name**: the name of the target database.
    - **Database account**: The Migration account of the RDS Database.
    - **Database password**: the password of the RDS Database Migration account.

5. Select migration type, and in objects to be migrated select the objects to be migrated, and then click>put the object you want to migrate into selected click **pre-Check and start** from the shortcut menu.

   > **Note**
   >
   > - When you select a structure migration, if the target RDS instance is in the database mydatabase, there is no Schema with the same name as the local database migration account, then DTS automatically creates a Schema with the same name, and the Owner of the Schema is the migration account.
   > - -In data migration, the data (structure) of the local database is copied to the target database without affecting the data (structure) of the local database.
   > - -During data migration, DDL operations are not supported and they may cause migration failures.

   If you want to modify the name of the migrated object on the target database, you can **selected** to the right of the list, click **edit** to modify the name of the selected object.

6. This step shows an example of a failed pre-check. If the pre-check is successful, see step 8.
   The system displays the pre-check results.

7. Click detection result for failure after

   ⓘ

   to view the failure Details. You can troubleshoot the failure based on the failure details.

8. After troubleshooting, in **migration tasks** page, select the current migration task, click **start** from the shortcut menu.

9. After pre-check is passed, click **confirm**. The Migration Task is automatically executed.

What to do next

Since the migration accounts have the read-write privileges, you need to delete the migration accounts in the local database and the RDS instance after data migration to ensure the security of the local database.

6.2. Migrate data between ApsaraDB RDS for PPAS 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
ApsaraDB RDS for PPAS	ApsaraDB RDS for PPAS

Precautions

- Data migration does not affect the data of the source database. During data migration, DTS reads the data of the source database and copies the data to the destination database. DTS does not delete the data of the source database. 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.
- To ensure data consistency, we recommend that you do not write data to the source RDS instance during full data migration.
- If a data migration task fails, DTS automatically resumes the task. Before you switch your workloads to the destination instance, stop or release the data migration task. Otherwise, the data in the source instance will overwrite the data in the destination instance after the task is resumed.
- DTS automatically creates a database in the destination RDS instance. However, if the name of the source database is invalid, you must manually create a database in the destination RDS instance before you configure the data migration task.

  > ? **Note** For more information about the naming conventions of ApsaraDB RDS and how to create a database, see Create accounts and databases for an ApsaraDB RDS for MySQL instance.

- If you migrate data between ApsaraDB RDS for PostgreSQL instances, take note of the following limits: After your workloads are switched to the destination database, newly written sequences do not increment from the maximum value of the sequences in the source database. Therefore, you must query the maximum value of the sequences in the source database before you switch your workloads to the destination database. Then, you must specify the queried maximum value as the starting value of the sequences in the destination database. You can run the following statements to query the maximum value of the sequences in the source database:

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

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 complete, 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

Migration scenario	Operation type	SQL statements
- 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	- 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	- 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. - 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
	DDL	- ALTER TABLE and ADD INDEX - 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. - DROP TABLE - RENAME TABLE

Permissions required for database accounts

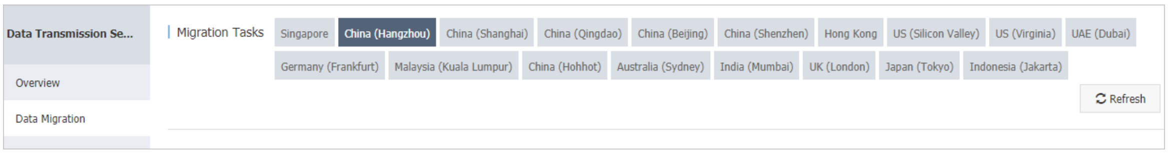
Migration scenario	Database	Schema migration	Full data migration	Incremental data migration
- Migrate data between ApsaraDB RDS for MySQL instances - Migrate data between ApsaraDB RDS for MariaDB TX instances - Migrate data from an ApsaraDB RDS for MariaDB TX instance to an ApsaraDB RDS for MySQL instance	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 ⓘ **Note** A privileged account has the required permissions.
	Destination instance	The read and write permissions	The read and write permissions	The read and write permissions

Migration 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 Note • 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.

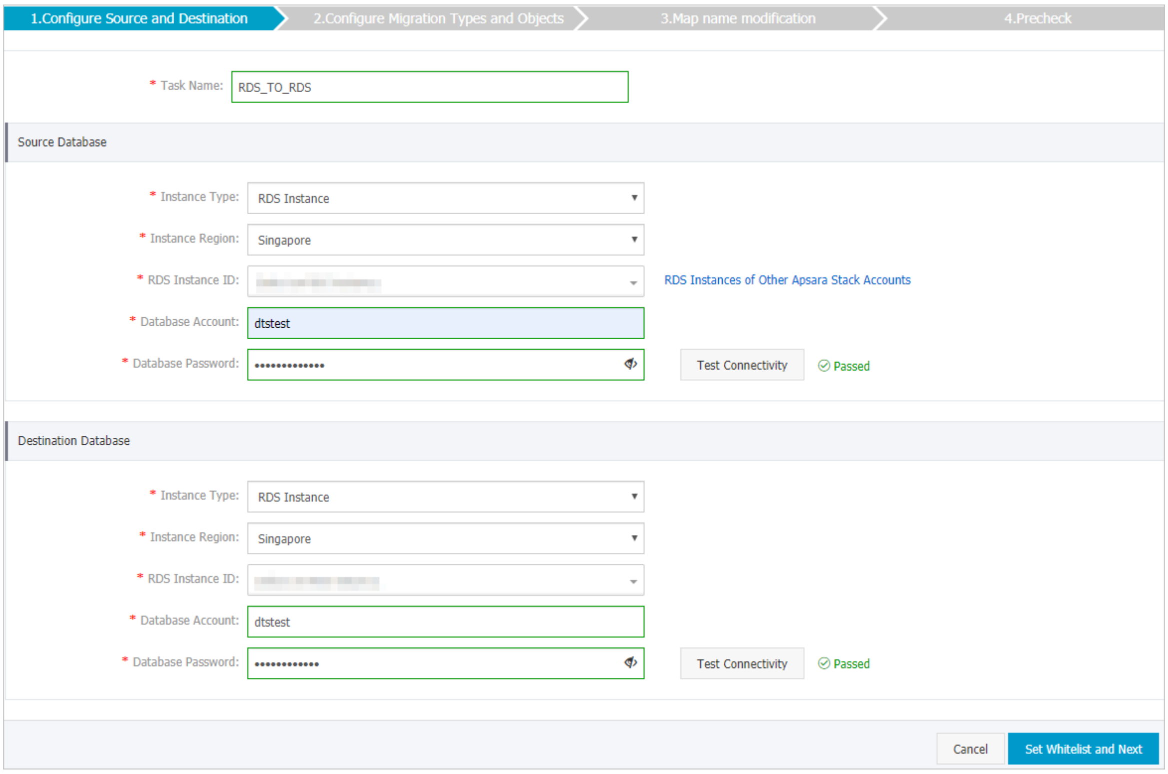
Migration scenario	Database	Schema migration	Full data migration	Incremental data migration
	Destination instance	The CREATE and USAGE permissions on the objects to be migrated	The permissions of the database owner, including the permissions to perform the INSERT, UPDATE, and DELETE operations Note A standard account of an ApsaraDB RDS for PostgreSQL instance has the required permissions.	The permissions of the database owner, including the permissions to perform the INSERT, UPDATE, and DELETE operations Note A standard account of an ApsaraDB RDS for PostgreSQL instance has the required permissions.
Migrate data between ApsaraDB RDS for PPAS instances	Source instance	The USAGE permission on pg_catalog	The SELECT permission on the objects to be migrated	The permissions of the superuser role
	Destination instance	The CREATE and USAGE permissions on the objects to be migrated	The permissions of the schema owner	The permissions of the schema owner

Procedure

1. Log on to the DTS console.
2. In the left-side navigation pane, click **Data Migration**.
3. At the top of the **Migration Tasks** page, select the region where the destination instance resides.



4. In the upper-right corner of the page, click **Create Migration Task**.
5. Configure the source and destination databases.



1.Configure Source and Destination > 2.Configure Migration Types and Objects > 3.Map name modification > 4.Precheck

* Task Name: RDS_TO_RDS

Source Database

* Instance Type: RDS Instance

* Instance Region: Singapore

* RDS Instance ID: [redacted] RDS Instances of Other Apsara Stack Accounts

* Database Account: dtstest

* Database Password: •••••••••••••• Test Connectivity ✓ Passed

Destination Database

* Instance Type: RDS Instance

* Instance Region: Singapore

* RDS Instance ID: [redacted]

* Database Account: dtstest

* Database Password: ••••••••••••• Test Connectivity ✓ Passed

Cancel | Set Whitelist and Next

Section	Parameter	Description
N/A	Task Name	DTS automatically generates a task name. We recommend that you specify an informative name for easy identification. You do not need to use a unique task 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. **Note** The source and destination RDS instances can be the same or different. You can use DTS to migrate data within an RDS instance or between two RDS instances.
	Database Name	Enter the name of the source database in the ApsaraDB RDS for PostgreSQL instance. **Note** This parameter is required only if the database engine of the RDS instance is **PostgreSQL**.
	Database Account	Enter the database account of the source RDS instance. For information about the permissions that are required for the account, see Permissions required for database accounts.

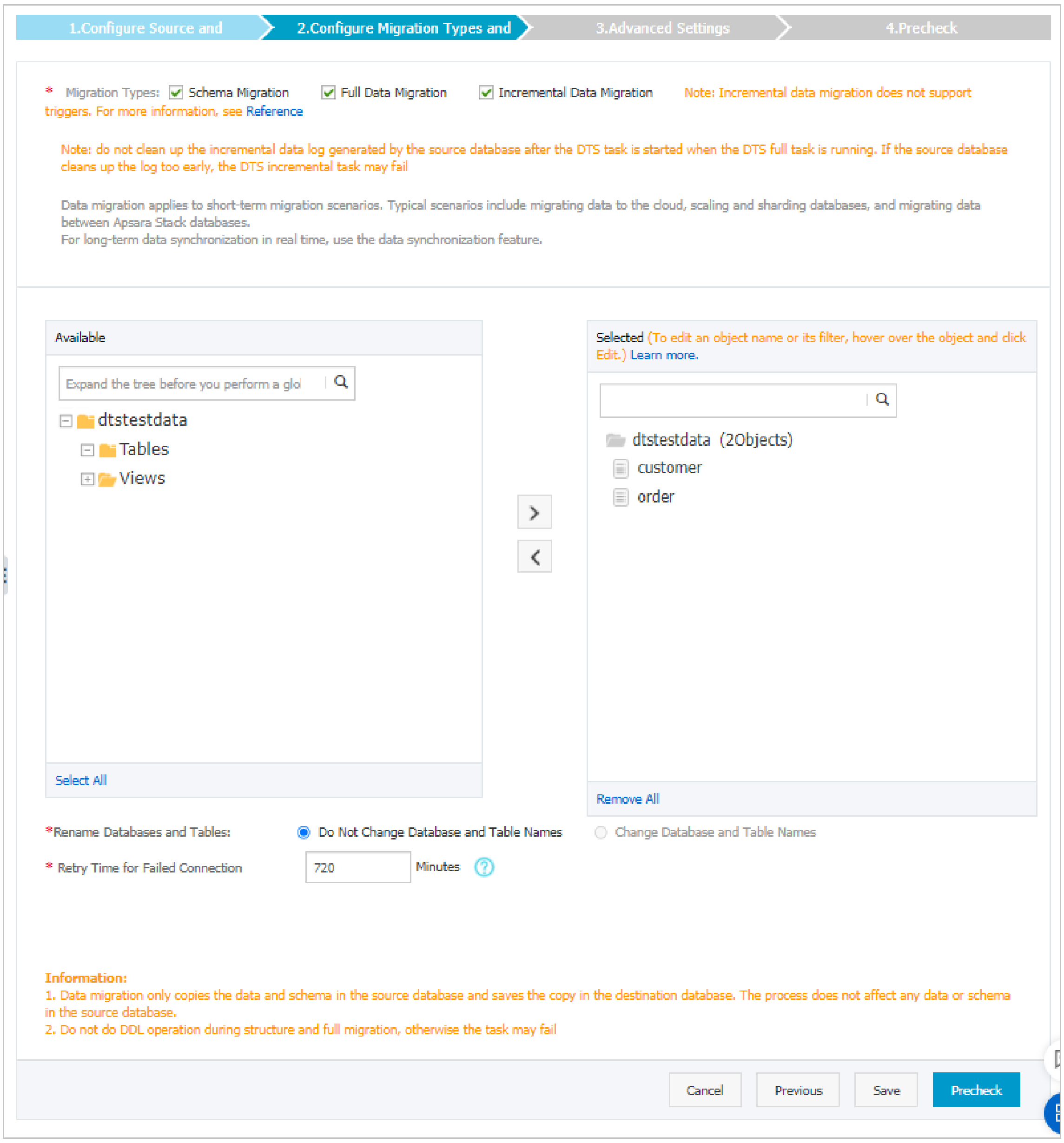
Section	Parameter	Description
	Database Password	Enter the password of the database account. **Note** After you specify the source database parameters, click **Test Connectivity** next to **Database Password** to verify whether the specified parameters are valid. If the specified parameters are valid, the **Passed** message appears. If the **Failed** message appears, click **Check** next to **Failed**. Modify the source database parameters based on the check results.
	Encryption	Select **Non-encrypted** or **SSL-encrypted**. If you want to select **SSL-encrypted**, you must enable SSL encryption for the RDS instance before you configure the data migration task. For more information, see Configure SSL encryption on an ApsaraDB RDS for MySQL instance. **Note** This parameter is required only if the database engine of the RDS instance is **MySQL**. The **Encryption** parameter is available only for regions in mainland China and the China (Hong Kong) region.
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. **Note** The source and destination RDS instances can be the same or different. You can use DTS to migrate data within an RDS instance or between two RDS instances.
	Database Name	Enter the name of the destination database in the ApsaraDB RDS for PostgreSQL instance. The name of the destination database can be different from the name of the source database. **Note** This parameter is required only if the database engine of the RDS instance is **PostgreSQL**.
	Database Account	Enter the database account of the destination RDS instance. For information about the permissions that are required for the account, see Permissions required for database accounts.

Section	Parameter	Description
	Database Password	Enter the password of the database account. Note After you specify the destination database parameters, click **Test Connectivity** next to **Database Password** to verify whether the parameters are valid. If the specified parameters are valid, the **Passed** message appears. If the **Failed** message appears, click **Check** next to **Failed**. Modify the destination database parameters based on the check results.
	Encryption	Select **Non-encrypted** or **SSL-encrypted**. If you want to select **SSL-encrypted**, you must enable SSL encryption for the RDS instance before you configure the data migration task. For more information, see Configure SSL encryption on an ApsaraDB RDS for MySQL instance. Note This parameter is required only if the database engine of the RDS instance is **MySQL**. The **Encryption** parameter is available only for regions in mainland China and the China (Hong Kong) region.

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

> **Note** DTS adds the CIDR blocks of DTS servers to the whitelists of the source and destination RDS instances. This ensures that DTS servers can connect to the source and destination RDS instances.

7. Select the migration types and the objects to be migrated.



* Migration Types: ☑ Schema Migration ☑ Full Data Migration ☑ Incremental Data Migration Note: Incremental data migration does not support triggers. For more information, see Reference

Note: do not clean up the incremental data log generated by the source database after the DTS task is started when the DTS full task is running. If the source database cleans up the log too early, the DTS incremental task may fail

Data migration applies to short-term migration scenarios. Typical scenarios include migrating data to the cloud, scaling and sharding databases, and migrating data between Apsara Stack databases.
For long-term data synchronization in real time, use the data synchronization feature.

Selected (To edit an object name or its filter, hover over the object and click Edit.) Learn more.

*Rename Databases and Tables: ● Do Not Change Database and Table Names ○ Change Database and Table Names

* Retry Time for Failed Connection 720 Minutes

Information:
1. Data migration only copies the data and schema in the source database and saves the copy in the destination database. The process does not affect any data or schema in the source database.
2. Do not do DDL operation during structure and full migration, otherwise the task may fail

Setting	Description
Select the migration types	Select the migration types based on your business requirements. The migration types must be supported by the database engine. ○ To perform only full data migration, select **Schema Migration** and **Full Data Migration**. ○ To ensure service continuity during data migration, select **Schema Migration**, **Full Data Migration**, and **Incremental Data Migration**. Note If **Incremental Data Migration** is not selected, we recommend that you do not write data to the source RDS instance during data migration. This ensures data consistency between the source and destination instances.

Setting	Description
Select the objects to be migrated	Select one or more objects from the **Available** section and click the > icon to move the objects to the **Selected** section. Note ◦ 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 change the names of the objects that are migrated to the destination database. For more information, see Object name mapping. ◦ If you use the object name mapping feature on an object, other objects that are dependent on the object may fail to be migrated.
Specify whether to rename objects	You can use the object name mapping feature to rename the objects that are migrated to the destination instance. For more information, see Object name mapping.
Specify the retry time for failed connections to the source or destination database	By default, if DTS fails to connect to the source or destination database, DTS retries within the next 720 minutes (12 hours). You can specify the retry time based on your needs. If DTS reconnects to the source and destination databases within the specified time, DTS resumes the data migration task. Otherwise, the data migration task fails. Note When DTS retries a connection, you are charged for the DTS instance. We recommend that you specify the retry time based on your business needs. You can also release the DTS instance at your earliest opportunity after the source and destination instances are released.

8. Click **Precheck**.

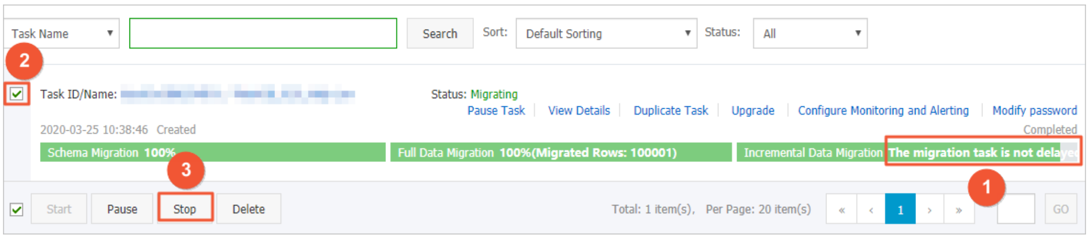
> Note
>
> - A precheck is performed before the migration task starts. The migration task only starts after the precheck succeeds.
> - If the precheck fails, click the
>
>   ⓘ
>
>   icon next to each failed check item to view the related details. Fix the issues as instructed and run the precheck again.

9. After the task passes the precheck, click **Next**.
10. In the **Confirm Settings** dialog box, specify the **Channel Specification** parameter 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
      We recommend that you do not manually stop the task during full data migration. Otherwise, the data migrated to the destination instance will be incomplete. You can wait until the data migration task automatically stops.
    - Incremental data migration
      The task does not automatically stop during incremental data migration. You must manually stop the task.

      > **Note** We recommend that you select an appropriate time to manually stop the data migration task. For example, you can stop the task during off-peak hours or before you switch your workloads to the destination instance.

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

    b. After the status of **incremental data migration** changes to **The migration task is not delayed** again, manually stop the migration task.



6.3. Migrate data from the on-premises databases to the ApsaraDB for RDS instances

You can migrate data from the on-premises databases to ApsaraDB for RDS instances to achieve smooth business migration. The migration methods are various and depend on the types of cloud databases. You can follow the guide by clicking one of the links based on your actual scenario.
For more information, see Migrate data from a self-managed Oracle database to an ApsaraDB RDS for PPAS instance.

6.4. Migrate data from an ApsaraDB RDS PPAS instance to an on-premises Oracle database

This topic describes how to migrate data from an ApsaraDB RDS PPAS instance to an on-premises Oracle database.

Limits

Currently, only files of common data types can be exported. Binary data types such as BLOB are not supported.

Prerequisites

- A server that has an Oracle database installed is available.
- The IP address of the Oracle database server is added to the whitelist of the ApsaraDB RDS PPAS instance. For more information, see Configure an IP address whitelist on an ApsaraDB RDS for PPAS instance.
- A table that has the same schema as ApsaraDB RDS PPAS database tables is created in the Oracle database.
- The PostgreSQL client is uploaded to the Oracle database server.

Procedure

> **Note** The following example demonstrates how to migrate data from an ApsaraDB RDS PPAS instance to an Oracle database installed in an ECS instance. In this example, the operating system of the ECS instance is CentOS 6.5.

1. Install the PostgreSQL client on the Oracle database server.

```
[root@oraclexe ~]# yum install postgresql.x86_64
[root@oraclexe ~]# /usr/bin/psql --version
psql (PostgreSQL) 8.4.20
```

2. Configure password-free logon for the ApsaraDB RDS PPAS instance in the ECS instance.

```
[root@oraclexe ~]# vim ~/.pgpass
[root@oraclexe ~]# cat ~/.pgpass
rm-2ze466l5u1k657yyn.ppas.rds.aliyuncs.com:3433:ora:myadmin:xxxxxxx
//The parameter must be in the HOSTNAME:PORT:DATABASE:USERNAME:PASSWORD format.
[root@oraclexe ~]# chmod 0600 ~/.pgpass
```

> **Note** The .pgpass configuration file is located in the HOME directory.

3. Test the connectivity between the ECS instance and the ApsaraDB RDS PPAS instance.

```
[root@oraclexe ~]# psql -h rm-2ze466l5u1k657yyn.ppas.rds.aliyuncs.com -p 3433 -U myadmin ora
psql.bin (9.3.1.3, server 9.3.13.37)
Enter "help" to obtain help information.
ora=>
```

If you can log on to the ApsaraDB RDS PPAS instance as the ora user, the connection has been established. After the test is complete, switch back to the root user.

```
ora=> \q
[root@oraclexe ~]#
```

4. Create a data export script in the ECS instance.

i. Create the ppas_exp_all_tables_to_csv.sh file.

```
vi ppas_exp_all_tables_to_csv.sh
```

ii. Insert the following text into the ppas_exp_all_tables_to_csv.sh script:

```
# ppas_exp_all_tables_to_csv.sh <hostname> <port> <username> <database>
 # Author: Xiao Shaocong (Scott Siu)
 # E-Mail: shaocong.xsc@alibaba-inc.com
 TMP_PATH="/tmp/ppas_tables_$1_$2_$3_$4"
 mkdir $TMP_PATH
 if [ $? -ne 0 ]
 then
   exit 1;
 fi
 echo "select '$1 $2 $3 $4 ' || tablename || ' $TMP_PATH ' || tablename from pg_tables where tableow
ner='$3' and (schemaname='$3' or schemaname='public');" > /tmp/ppas_tables_$1_$2_$3_$4.sql
 psql -h $1 -p $2 -U $3 $4 -f /tmp/ppas_tables_$1_$2_$3_$4.sql | head -n -2 | tail -n +3 | awk -F " " '{pri
ntf ("psql -h %s -p %s -U %s %s -c \"\\copy %s TO '\''%s/%s'\'' CSV HEADER\"\n",$1,$2,$3,$4,$5,$6,$7
)}' | sh
```

5. Grant execution permission to the ppas_exp_all_tables_to_csv.sh script.

```
[root@oraclexe ~]# chmod 0755 ppas_exp_all_tables_to_csv.sh
```

6. Execute the data export script in the ECS instance.

```
[root@oraclexe ~]# ./ppas_exp_all_tables_to_csv.sh rm-2ze466l5u1k657yyn.ppas.rds.aliyuncs.com 343
3 myadmin ora
```

7. Verify the data exported to a CSV file.

```
[root@oraclexe ~]# cat /tmp/ppas_tables_rm-2ze466l5u1k657yyn.ppas.rds.aliyuncs.com_3433_myadm
in_ora/*
deptno,dname,loc
10,ACCOUNTING,NEW YORK
20,RESEARCH,DALLAS
30,SALES,CHICAGO
40,OPERATIONS,BOSTON
empno,ename,job,mgr,hiredate,sal,comm,deptno
7369,SMITH,CLERK,7902,17-DEC-80 00:00:00,800.00,,20
7499,ALLEN,SALESMAN,7698,20-FEB-81 00:00:00,1600.00,300.00,30
7521,WARD,SALESMAN,7698,22-FEB-81 00:00:00,1250.00,500.00,30
7566,JONES,MANAGER,7839,02-APR-81 00:00:00,2975.00,,20
7654,MARTIN,SALESMAN,7698,28-SEP-81 00:00:00,1250.00,1400.00,30
7698,BLAKE,MANAGER,7839,01-MAY-81 00:00:00,2850.00,,30
7782,CLARK,MANAGER,7839,09-JUN-81 00:00:00,2450.00,,10
7788,SCOTT,ANALYST,7566,19-APR-87 00:00:00,3000.00,,20
7839,KING,PRESIDENT,,17-NOV-81 00:00:00,5000.00,,10
7844,TURNER,SALESMAN,7698,08-SEP-81 00:00:00,1500.00,0.00,30
7876,ADAMS,CLERK,7788,23-MAY-87 00:00:00,1100.00,,20
7900,JAMES,CLERK,7698,03-DEC-81 00:00:00,950.00,,30
7902,FORD,ANALYST,7566,03-DEC-81 00:00:00,3000.00,,20
7934,MILLER,CLERK,7782,23-JAN-82 00:00:00,1300.00,,10
empno,startdate,enddate,job,sal,comm,deptno,chgdesc
7369,17-DEC-80 00:00:00,,CLERK,800.00,,20,New Hire
7499,20-FEB-81 00:00:00,,SALESMAN,1600.00,300.00,30,New Hire
7521,22-FEB-81 00:00:00,,SALESMAN,1250.00,500.00,30,New Hire
7566,02-APR-81 00:00:00,,MANAGER,2975.00,,20,New Hire
7654,28-SEP-81 00:00:00,,SALESMAN,1250.00,1400.00,30,New Hire
7698,01-MAY-81 00:00:00,,MANAGER,2850.00,,30,New Hire
7782,09-JUN-81 00:00:00,,MANAGER,2450.00,,10,New Hire
7788,19-APR-87 00:00:00,12-APR-88 00:00:00,CLERK,1000.00,,20,New Hire
7788,13-APR-88 00:00:00,04-MAY-89 00:00:00,CLERK,1040.00,,20,Raise
7788,05-MAY-90 00:00:00,,ANALYST,3000.00,,20,Promoted to Analyst
7839,17-NOV-81 00:00:00,,PRESIDENT,5000.00,,10,New Hire
7844,08-SEP-81 00:00:00,,SALESMAN,1500.00,0.00,30,New Hire
7876,23-MAY-87 00:00:00,,CLERK,1100.00,,20,New Hire
7900,03-DEC-81 00:00:00,14-JAN-83 00:00:00,CLERK,950.00,,10,New Hire
7900,15-JAN-83 00:00:00,,CLERK,950.00,,30,Changed to Dept 30
7902,03-DEC-81 00:00:00,,ANALYST,3000.00,,20,New Hire
7934,23-JAN-82 00:00:00,,CLERK,1300.00,,10,New Hire
```

8. Import the CSV file to the Oracle database.
   - Solution 1: Use the Oracle SQL*Loader utility to import data. For more information, see Oracle SQL Loader Overview.
   - Solution 2: Use Oracle SQL Developer to import data. For more information, see SQL Developer Concepts and Usage.

Troubleshooting

Error

When you execute the data export script, the system prompts that a directory cannot be created, as shown below.

```
[root@oraclexe ~]# ./ppas_exp_all_tables_to_csv.sh rm-2ze466l5u1k657yyn.ppas.rds.aliyuncs.com 3433 myadmin ora
mkdir: Unable to create directory"/tmp/ppas_tables_rm-2ze466l5u1k657yyn.ppas.rds.aliyuncs.com_3433_myadmin_ora": The file already exists.
```

Troubleshooting procedure

Delete the existing directory.

```
[root@oraclexe ~]# rm -rf /tmp/ppas_tables_rm-2ze466l5u1k657yyn.ppas.rds.aliyuncs.com_3433_myadmin_ora
```

6.5. Migrate data from an ApsaraDB RDS PPAS instance to an on-premises PPAS database

You can use logical backup files to migrate data from an ApsaraDB RDS PPAS instance to an on-premises PPAS database.

Procedure

1. Connect the PostgreSQL client to ApsaraDB RDS PPAS.
2. Run the following command to back up data:

   ```
   pg_dump -U username -h hostname -p port databasename -f filename
   ```

   The parameters are described as follows:

   - username: the username that is used to log on to the ApsaraDB RDS PPAS database.
   - hostname: the hostname of the ApsaraDB RDS PPAS database.
   - port: the port number of the ApsaraDB RDS PPAS database.
   - databasename: the name of the ApsaraDB RDS PPAS database that you want to back up.
   - filename: the name of the backup file to be generated. Example:

     ```
     pg_dump -U ppas_user -h rdsv07z563m7o25cj550public.ppas.rds.aliyuncs.com -p 3433 edb -f ppas.sql
     ```

3. Save the *ppas.sql* backup file to the destination server.
4. Run the following command to restore data to the on-premises database:

   ```
   psql -U username -h hostname -d desintationdb -p port -f dumpfilename.sql
   ```

   The parameters are described as follows:

   - username: the username that is used to log on to the on-premises database.
   - hostname: the hostname of the on-premises database.
   - port: the port number of the on-premises database.
   - databasename: the name of the on-premises database.

- filename: the name of the backup file. Example:

  ```
  psql -U ppas_user -h localhost -d edb -p 5444 -f ppas.sql
  ```

  Permission settings of the ApsaraDB RDS PPAS database are different from those of the on-premises database. Therefore, some permission-related warnings or errors may occur during data import. Examples of warnings or errors that can be ignored are as follows:

  ```
  WARNING:  no privileges could be revoked for "xxxxx"
  ERROR:  role "xxxxx" does not exist
  ```

7.Billing

7.1. Switch an ApsaraDB RDS for PPAS instance from pay-as-you-go to subscription

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

Impacts

Switching the billing method of an instance does not affect its performance.

Precautions

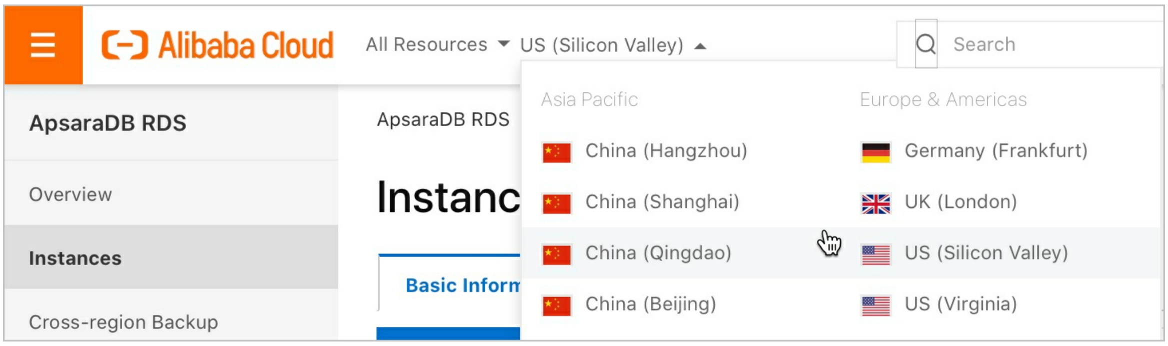
If you upgrade the specifications of an RDS instance before you pay for the subscription order, the order becomes invalid. You must cancel this order on the Billing Management page and switch the billing method of the RDS instance to subscription again.

Prerequisites

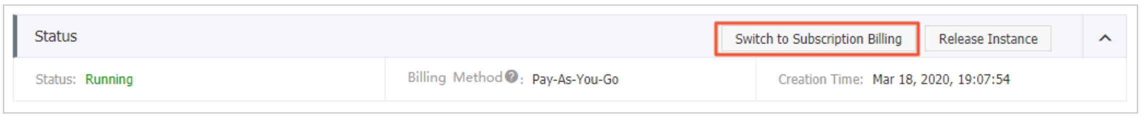
- The type of the RDS instance is not phased out. For more information, see Phased-out instance types. If you need to switch an RDS instance of a phased-out type to subscription, first change the instance type. For more information, see Change the configuration of an RDS PPAS instance.
- The billing method of the RDS instance is pay-as-you-go.
- The RDS instance is in the Running state.
- The RDS instance does not have unpaid subscription orders.

Procedure

1. Log on to the ApsaraDB for RDS console.
2. In the top navigation bar, select the region where the target RDS instance resides.



3. Find the target RDS instance and use one of the following methods to go to the **Switch to Subscription Billing** page:
   - In the Actions column, click **Switch to Subscription Billing**.
   - Click the instance ID. In the **Status** section of the Basic Information page that appears, click **Switch to Subscription Billing**.



Status

Switch to Subscription Billing

Release Instance

Status: Running

Billing Method: Pay-As-You-Go

Creation Time: Mar 18, 2020, 19:07:54

4. Specify the subscription duration.
5. Click **Pay Now**.

> **Note** You must complete the subscription order generated for the instance. You cannot purchase a new instance or switch the billing method of another instance until you complete or cancel this order. You can pay for or cancel the order on the Billing Management page.

6. Complete the order as prompted.

Related operations

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

7.2. 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.

Prerequisites

- Your RDS instance uses the subscription billing method. For more information about the billing methods, see Pricing, billable items, and billing methods.
- 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 perform this operation. For more information, see Change the specifications of an ApsaraDB RDS for MySQL instance.

Billing

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

This operation does not have impacts on the running of your RDS instance.

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

Procedure

1.
2.
3.
4. In the Status section of the **Basic Information** page, click **Switch to Pay-as-you-go Billing**.
5. Confirm the instance configuration, read and select Terms of Service, click **Pay Now**, and then complete the payment.

Related operations

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

7.3. Manually renew an ApsaraDB RDS for PPAS instance

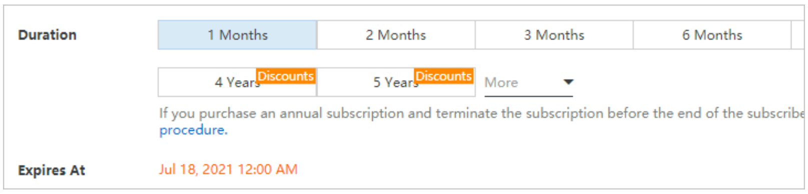
This topic describes how to manually renew an ApsaraDB RDS for PPAS instance. If your RDS instance uses subscription billing, you must renew it before it expires. This allows you to prevent service interruptions and data loss.
For more information about the impacts caused by subscription expiration, 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

1. Visit the RDS instance list , select a region above, and click the target instance ID.
2. In the **Status** section of the page that appears, click **Renew** on the right.
3. On the **Renew Subscription** page, specify the Duration parameter. A longer subscription period indicates more discounts.



Duration: 1 Months | 2 Months | 3 Months | 6 Months | 4 Years Discounts | 5 Years Discounts | More

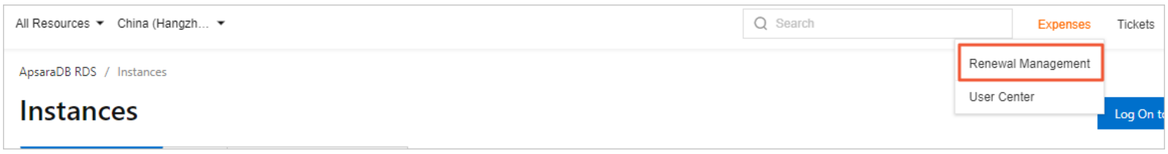
If you purchase an annual subscription and terminate the subscription before the end of the subscribe procedure.

Expires At: Jul 18, 2021 12:00 AM

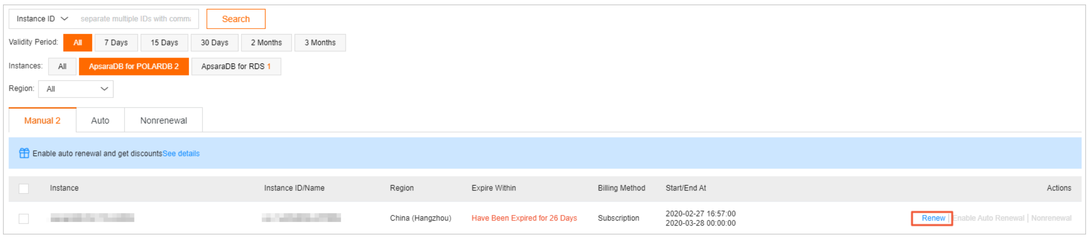
4. Read and select Terms of Service, Service Level Agreement, and Terms of Use, click **Pay Now**, and then complete the payment.

Method 2: Renew one or more RDS instances in the Billing Management console

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



3. 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.
   - To renew a single RDS instance, perform the following steps:
     a. Find the RDS instance and click **Renew** in the Actions column.



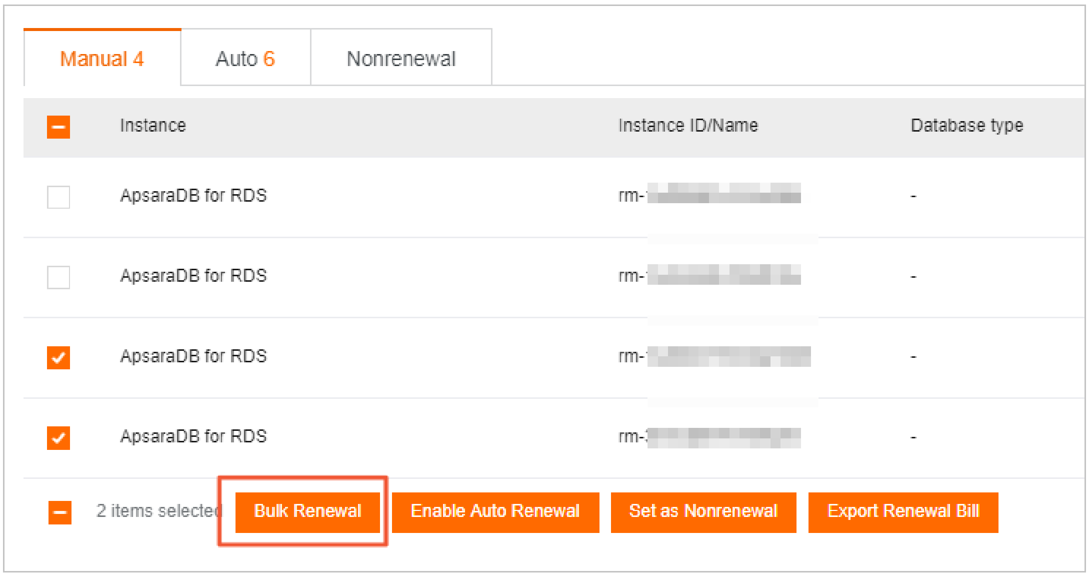
Instance ID
separate multiple IDs with comm
Search
Validity Period: All | 7 Days | 15 Days | 30 Days | 2 Months | 3 Months
Instances: All | ApsaraDB for POLARDB 2 | ApsaraDB for RDS 1
Region: All
Manual 2 | Auto | Nonrenewal
Enable auto renewal and get discounts See details

Instance	Instance ID/Name	Region	Expire Within	Billing Method	Start/End At	Actions
[redacted]	[redacted]	China (Hangzhou)	Have Been Expired for 26 Days	Subscription	2020-02-27 16:57:00 2020-03-28 00:00:00	Renew | Enable Auto Renewal | Nonrenewal

> **Note** If the RDS instance resides 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.

     b. On the page that appears, specify the Duration parameter and click **Pay Now**. Then, complete the payment.
   - To renew more than one RDS instance, perform the following steps:

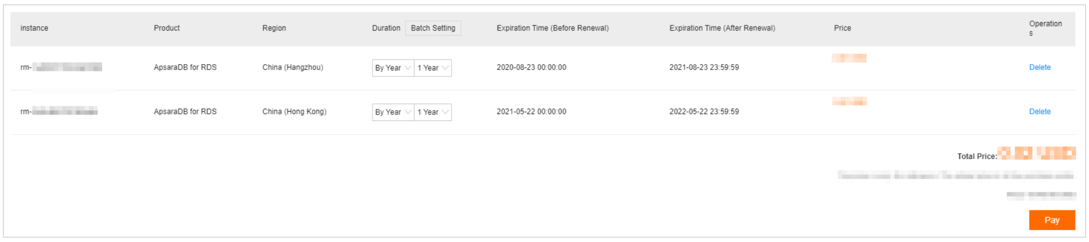
a. Select the RDS instances and click **Batch Renewal** below the instance list.



Manual 4 | Auto 6 | Nonrenewal

☐	Instance	Instance ID/Name	Database type
☐	ApsaraDB for RDS	rm-[redacted]	-
☐	ApsaraDB for RDS	rm-[redacted]	-
☑	ApsaraDB for RDS	rm-[redacted]	-
☑	ApsaraDB for RDS	rm-[redacted]	-

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



instance	Product	Region	Duration Batch Setting	Expiration Time (Before Renewal)	Expiration Time (After Renewal)	Price	Operations
rm-[redacted]	ApsaraDB for RDS	China (Hangzhou)	By Year 1 Year	2020-08-23 00:00:00	2021-08-23 23:59:59	[redacted]	Delete
rm-[redacted]	ApsaraDB for RDS	China (Hong Kong)	By Year 1 Year	2021-05-22 00:00:00	2022-05-22 23:59:59	[redacted]	Delete

Total Price: [redacted]

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 Configure auto-renewal for an ApsaraDB RDS for PPAS instance.

7.4. Configure auto-renewal for an ApsaraDB RDS for PPAS instance

If you enable auto-renewal for your ApsaraDB RDS for PPAS instance, you do not need to manually renew your subscription or be concerned about business interruptions caused by subscription expiration.

If your RDS instance uses the subscription billing method, the subscription will expire. If you do not renew your subscription before the expiration, your business is interrupted and data may be lost. For more information, see Impact of expiration and overdue payment.

> **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 on the third day before your RDS instance expires. If the deduction fails, the system will attempt to deduct the fee every day in the next two days.

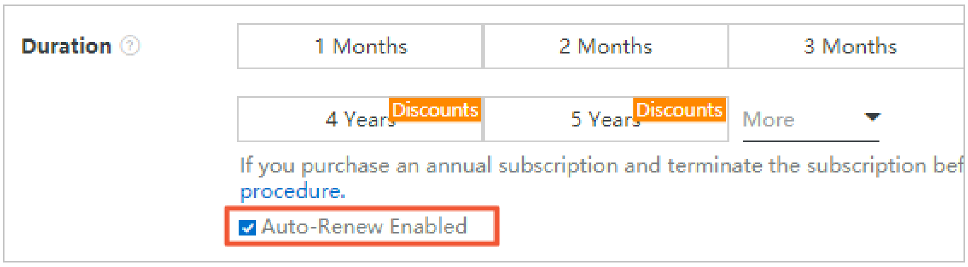
> **Note** Make sure that the balance of your Alibaba Cloud account is sufficient. Otherwise, the renewal fails. If the automatic fee deduction fails all three times, you must manually renew your RDS instance in time to avoid business interruption and data loss.

- 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 business interruption. For more information, see Manually renew an ApsaraDB RDS for PPAS 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**.



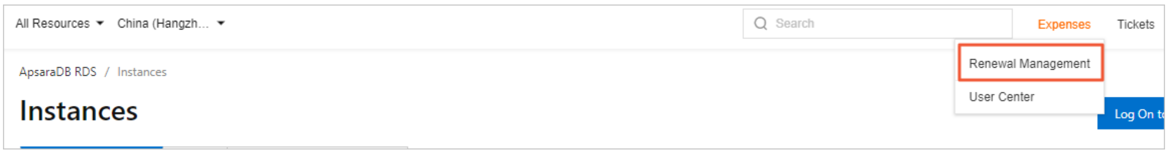
If you purchase an annual subscription and terminate the subscription bef
procedure.

☑ Auto-Renew Enabled

Enable auto-renewal after you purchase an RDS instance

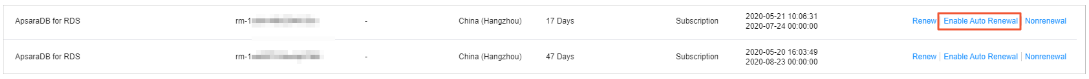
> **Note** After you enable auto-renewal for a created RDS instance, the system automatically renews the RDS instance based on the selected renewal cycle. For example, if you select a three-month renewal cycle, you are charged for a three-month subscription in each renewal cycle.

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



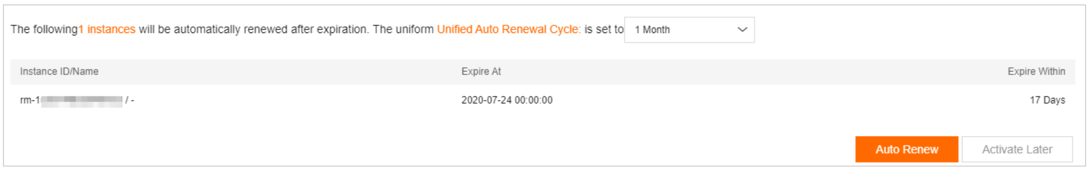
3. On the **Manual** or **Nonrenewal** tab, specify the filter conditions to find the RDS instance for which you want to enable auto-renewal. You can enable auto-renewal for one or more RDS instances at a time.
   - Enable auto-renewal for a single RDS instance.

a. Find the RDS instance and in the Actions column click **Enable Auto Renewal**.



ApsaraDB for RDS	rm-1[redacted]	-	China (Hangzhou)	17 Days	Subscription	2020-05-21 10:06:31 2020-07-24 00:00:00	Renew | Enable Auto Renewal | Nonrenewal
ApsaraDB for RDS	rm-1[redacted]	-	China (Hangzhou)	47 Days	Subscription	2020-05-20 16:03:49 2020-08-23 00:00:00	Renew | Enable Auto Renewal | Nonrenewal

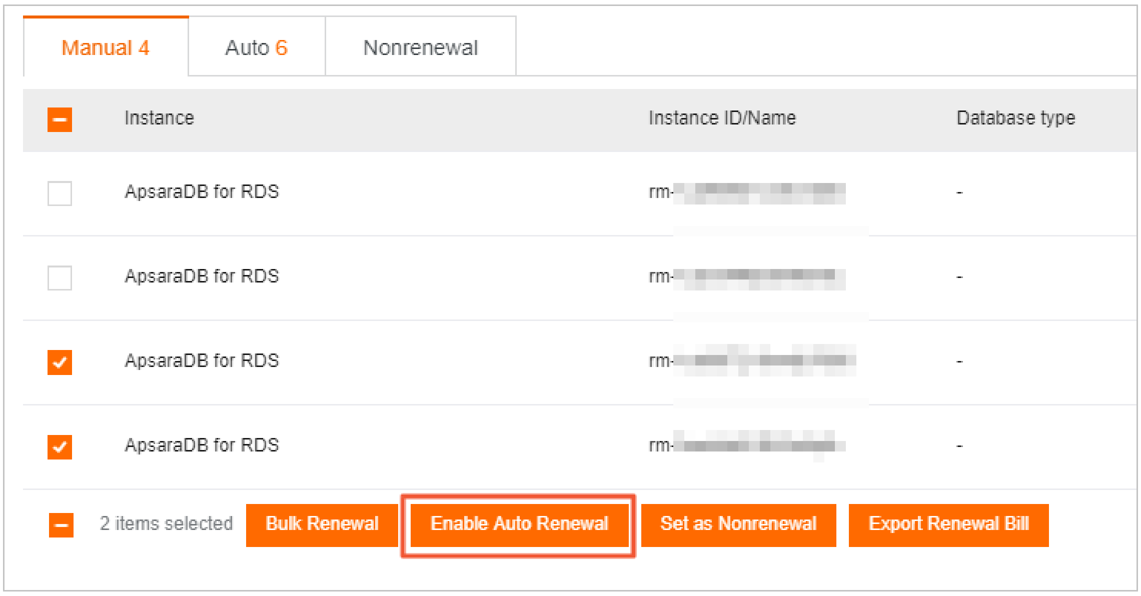
b. In the dialog box that appears, specify the **Unified Auto Renewal Cycle** parameter and click **Auto Renew**.



The following1 instances will be automatically renewed after expiration. The uniform Unified Auto Renewal Cycle: is set to 1 Month

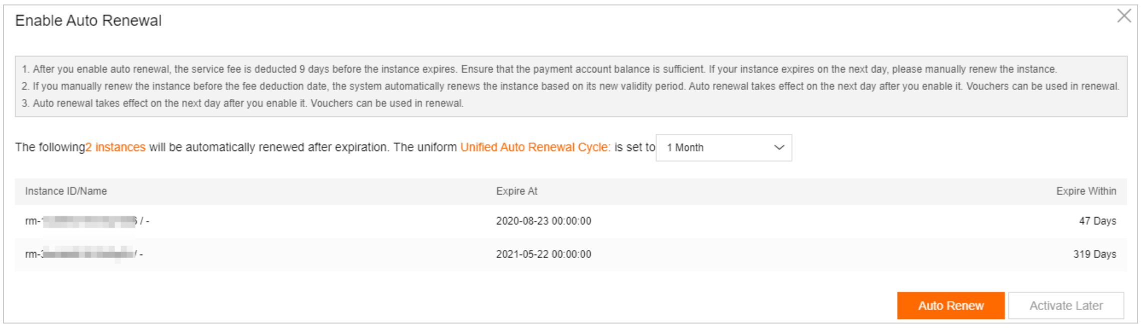
Instance ID/Name	Expire At	Expire Within
rm-1[redacted] / -	2020-07-24 00:00:00	17 Days

- Enable auto-renewal for multiple RDS instances.
  Select the RDS instances and click **Enable Auto Renewal** below the instance list.



	Instance	Instance ID/Name	Database type
□	ApsaraDB for RDS	rm-[redacted]	-
□	ApsaraDB for RDS	rm-[redacted]	-
☑	ApsaraDB for RDS	rm-[redacted]	-
☑	ApsaraDB for RDS	rm-[redacted]	-

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



Enable Auto Renewal

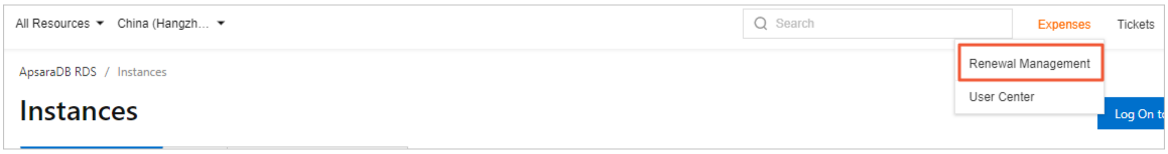
1. After you enable auto renewal, the service fee is deducted 9 days before the instance expires. Ensure that the payment account balance is sufficient. If your instance expires on the next day, please manually renew the instance.
2. If you manually renew the instance before the fee deduction date, the 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 following2 instances will be automatically renewed after expiration. The uniform Unified Auto Renewal Cycle: is set to 1 Month

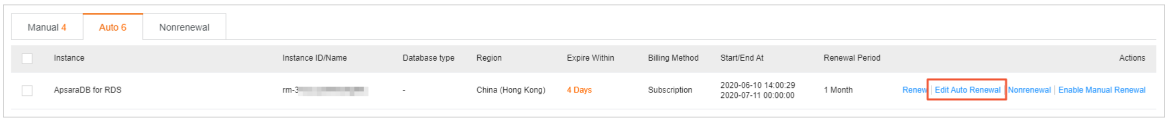
Instance ID/Name	Expire At	Expire Within
rm-[redacted] / -	2020-08-23 00:00:00	47 Days
rm-[redacted] / -	2021-05-22 00:00:00	319 Days

Change the auto-renewal cycle

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



3. 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.

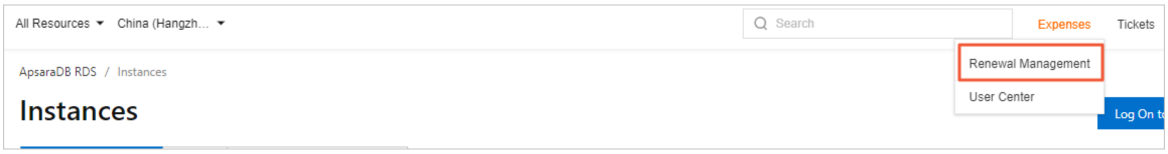


□	Instance	Instance ID/Name	Database type	Region	Expire Within	Billing Method	Start/End At	Renewal Period	Actions
□	ApsaraDB for RDS	rm-3[redacted]	-	China (Hong Kong)	4 Days	Subscription	2020-06-10 14:00:29 2020-07-11 00:00:00	1 Month	Renew | Edit Auto Renewal | Nonrenewal | Enable Manual Renewal

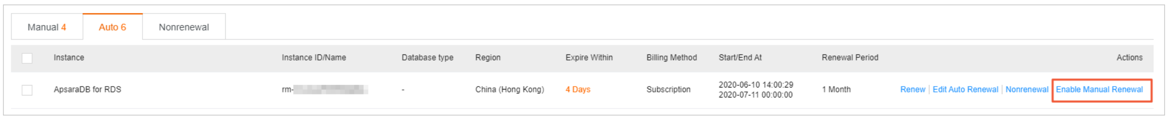
4. In the dialog box that appears, change the auto-renewal cycle and click **OK**.

Disable auto-renewal

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



3. 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.



□	Instance	Instance ID/Name	Database type	Region	Expire Within	Billing Method	Start/End At	Renewal Period	Actions
□	ApsaraDB for RDS	rm-[redacted]	-	China (Hong Kong)	4 Days	Subscription	2020-06-10 14:00:29 2020-07-11 00:00:00	1 Month	Renew | Edit Auto Renewal | Nonrenewal | Enable Manual Renewal

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

Related operations

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

8.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

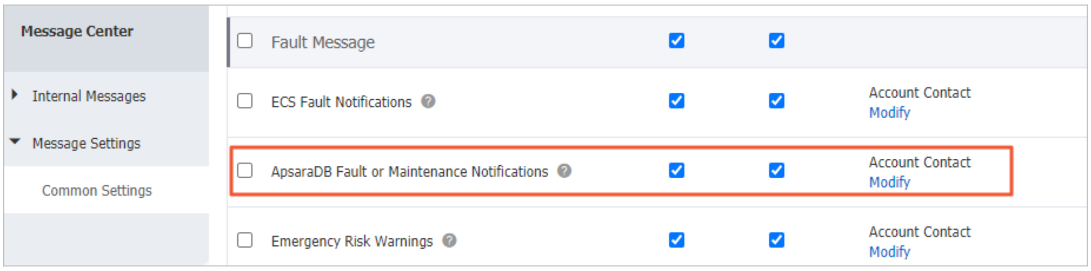
A pending event is found, which is an O&M event.

> ⓘ **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. Event notifications are sent by usingphone calls, emails, internal messages, or the ApsaraDB for Redis console. To use this feature, log on to theMessage 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



□ Fault Message	☑	☑	
□ ECS Fault Notifications	☑	☑	Account Contact Modify
□ ApsaraDB Fault or Maintenance Notifications	☑	☑	Account Contact Modify
□ Emergency Risk Warnings	☑	☑	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 Disconnection Time**, select an RDS instance and click **Specify Disconnection 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 Disconnection 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 Primary/secondary switchover SSL certificate update Backup mode change	Transient connections	From the time specified by the RDS instance is subject to the following impacts: ● 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. Scheduled Disconnection Time
Minor engine version update	Transient connections	From the time specified by the RDS instance is subject to the following impacts: ● 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	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. ● 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. ● Release notes of the PolarDB kernel, Release notes and Release notes.

Cause	Impact type	Impact description
Proxy version upgrade	Transient connections	From the time specified by the RDS instance is subject to the following impacts: • 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	From the time specified by the RDS instance is subject to the following impacts: • 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	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. **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.

9.Instance

9.1. Create an ApsaraDB RDS for PPAS instance

This topic describes how to create an ApsaraDB RDS for PPAS instance by using the ApsaraDB RDS console. You can also call an API operation to create an ApsaraDB RDS for PPAS instance.

Prerequisites

You have an Alibaba Cloud account. For more information, see Sign up with Alibaba Cloud.

Procedure

1.
2. Configure the following parameters.

Parameter	Description
Billing Method	○ **Subscription**: A subscription instance is an instance that you can subscribe to for a specified period of time 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 require your pay-as-you-go instance, you can release the instance to reduce costs. Note
Region	The region where the RDS instance resides. ○ If your application is deployed on an Elastic Compute Service (ECS) instance, the RDS instance must reside in the same region as the ECS instance. For example, the RDS instance and the ECS instance can both reside in the China (Hangzhou) region. If the RDS instance and the ECS instance reside in different regions, they cannot communicate over an internal network and therefore they cannot deliver optimal performance. ○ If your application is deployed on an on-premises server or computer, we recommend that you select a region that is in close proximity to the on-premises server or computer.
Database Engine	The database engine and version that the RDS instance runs. Select **PPAS (Compatible with Oracle)**. Supported PPAS versions are 9.3 and 10. Note The available database engines and versions vary based on the region that you select.

Parameter	Description
Edition	**High-availability**: The database system consists of one primary RDS instance and one secondary RDS instance. These instances run in the classic high-availability architecture. ⓘ **Note** The available RDS editions vary based on the region and database engine version that you select. For more information about RDS editions, see Overview of ApsaraDB RDS editions.
Storage Type	○ **Local SSD**: A local SSD resides on the same host as the database engine. You can store data on local SSDs to reduce I/O latency. ○ **ESSD**: Enhanced SSDs (ESSDs) come in three performance levels (PLs). ■ ESSD PL1: An ESSD of PL1 is a regular ESSD. ■ ESSD PL2: An ESSD of PL2 delivers IOPS and throughput that are approximately twice higher than the IOPS and throughput delivered by an ESSD of PL1. ■ ESSD PL3: An ESSD of PL3 delivers IOPS that is up to 20 times higher than the IOPS delivered by an ESSD of PL1. An ESSD of PL3 also delivers throughput that is up to 11 times higher than the throughput delivered by an ESSD of PL1. ESSDs of PL3 are suitable for business scenarios in which highly concurrent requests must be processed with high I/O performance and at low read and write latencies. ○ **Standard SSD**: A standard SSD is an elastic block storage device that is built on top of the distributed storage architecture. You can store data on standard SSDs to separate computing from storage.
Zone	The zone where the RDS instance resides. Each zone is an independent physical location within a region. For example, the China (Hangzhou) region contains Zone H, Zone I, and Zone J. ApsaraDB RDS supports the following two deployment methods: ○ **Multi-zone Deployment**: The primary RDS instance and the secondary RDS instance reside in different zones to provide zone-disaster recovery. This is the recommended deployment method. ○ **Single-zone Deployment**: The primary RDS instance and the secondary RDS instance reside in the same zone. ⓘ **Note** If you select the RDS Basic Edition, you can select only the **Single-zone Deployment** method.

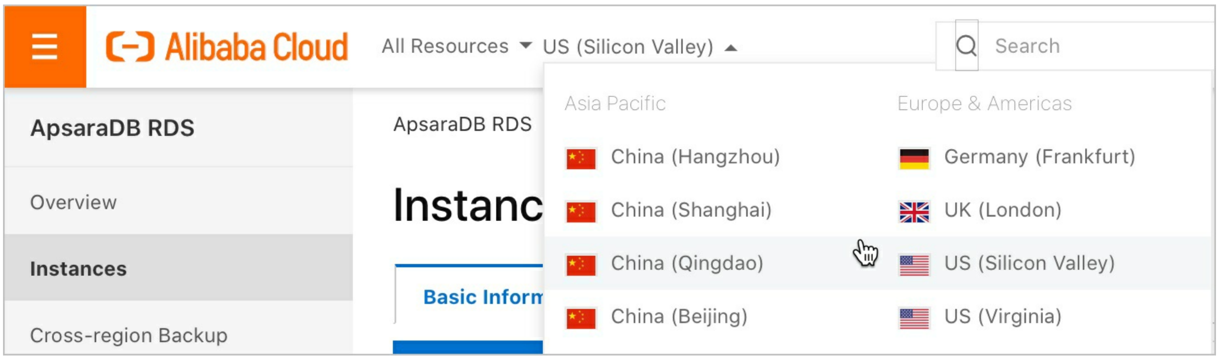
Parameter	Description
Instance Type	○ **Entry-level**: belongs to the general-purpose instance family. A general-purpose instance exclusively occupies the allocated memory and I/O resources, but shares CPU and storage resources with the other general-purpose instances that are deployed on the same server. ○ **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 highest configuration of the dedicated instance family. A dedicated host instance occupies all the CPU, memory, storage, and I/O resources on the server where the instance is deployed. **Note** For more information, see Primary ApsaraDB RDS instance types.
Capacity	The size of the storage space that is provided for the RDS instance to store data files, system files, binary log files, and transaction files. You can increase the storage capacity in increments of 5 GB. **Note** The dedicated instance family used with local SSDs supports the exclusive allocations of resources. In this case, the storage capacity for each instance type is immutable. For more information about this issue, see Primary ApsaraDB RDS instance types.

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

Parameter	Description
Network Type	
Resource Group	The resource group to which the RDS instance belongs. You can retain the default resource group or select a custom resource group based on your business requirements.

5. In the lower-right corner of the page, click **Next: Confirm Order**.
6. Confirm the configuration of the RDS instance in the Parameters section, specify the **Purchase Plan** and **Duration** parameters, read and select **Terms of Service**, and then click **Pay Now**. You need to specify the Duration parameter only when you select the subscription billing method for the RDS instance.

Note If you select the subscription billing method for the RDS instance, we recommend that you select **Auto-Renew Enabled**. This prevents interruptions to your workloads even if you forget to review the RDS instance.



What to do next

- Configure a whitelist for an ApsaraDB RDS for PPAS instance
- Create databases and accounts for an ApsaraDB RDS for PPAS instance
- Apply for or release a public endpoint for an ApsaraDB RDS for PPAS instance
- Connect to an ApsaraDB RDS for PPAS instance

FAQ

- After I create an RDS instance, why does the ApsaraDB RDS console not respond and why am I unable to find the RDS instance?
  This issue may occur due to the following reasons:
  - The region that you selected is not the region where the RDS instance resides.
    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 are dynamically allocated within zones. After you submit the purchase order, the zone that you selected may run out of 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 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.
- If my RDS instance resides in a VPC, how many private IP addresses does it have?
  The number of private IP addresses that your RDS instance has varies based on the database engine and RDS edition that are used.
  - MySQL 5.5, 5.6, 5.7, and 8.0 on RDS High-availability Edition with local SSDs: 1
  - MySQL 5.6, 5.7, and 8.0 on RDS Enterprise Edition with local SSDs: 1
  - MySQL 5.7 on RDS Basic Edition with standard SSDs: 1
  - MySQL 8.0 on RDS Basic Edition with standard SSDs: 2
  - MySQL 5.7 and 8.0 on RDS High-availability Edition with standard SSDs or ESSDs: 3
  - MySQL 5.7 and 8.0 on RDS Enterprise Edition with standard SSDs or ESSDs: 1

References

- For more information about how to create an RDS instance by using the ApsaraDB RDS API, see Create an instance.
- For more information about how to create an RDS instance that runs a different database engine,

see the following topics:

- Create an ApsaraDB RDS for SQL Server instance
- Create an ApsaraDB RDS for PostgreSQL instance
- Create an ApsaraDB RDS for MariaDB TX instance

9.2. Restart an ApsaraDB RDS for MySQL instance

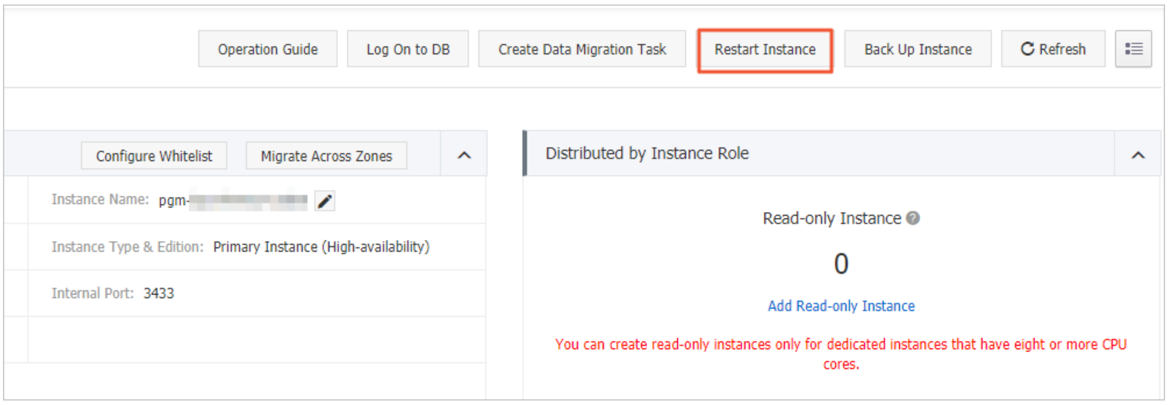
This topic describes how to manually restart an ApsaraDB RDS for MySQL instance. This applies if the number of connections exceeds the specified threshold or a performance issue occurs.

Precautions

When you restart an RDS instance, a brief disconnection with the RDS instance will occur. Before you perform a restart, make appropriate arrangements for your workloads. Proceed with caution.

Procedure

1.
2.
3.
4. In the upper-right corner of the page, click **Restart Instance**.



Instance Name: pgm-[redacted]

Instance Type & Edition: Primary Instance (High-availability)

Internal Port: 3433

You can create read-only instances only for dedicated instances that have eight or more CPU cores.

5. In the message that appears, click **Confirm**.

Related operations

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

9.3. Set the maintenance window of an ApsaraDB RDS instance

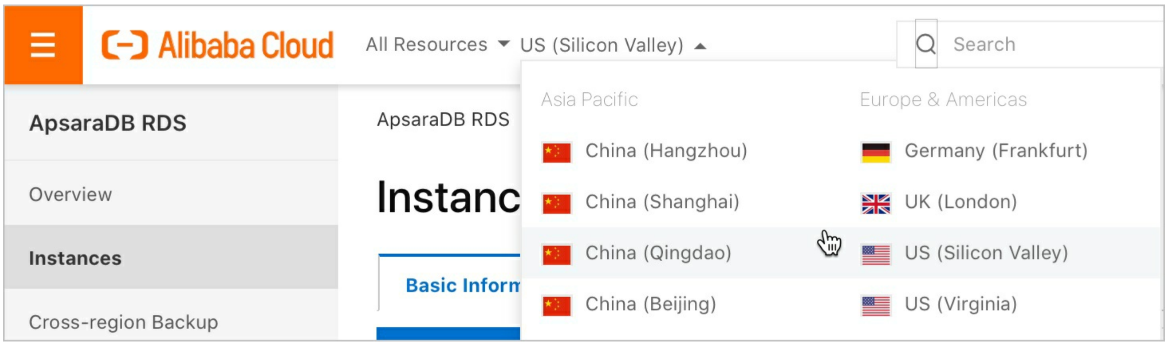
This topic describes how to set the maintenance window of an ApsaraDB RDS instance. To ensure database stability, the backend system performs maintenance operations on your RDS instance every day during the maintenance window you specify. The default maintenance window spans from 02:00 to 06:00 UTC+8. We recommend that you set the maintenance window to off-peak hours to avoid interference to your business.

Precautions

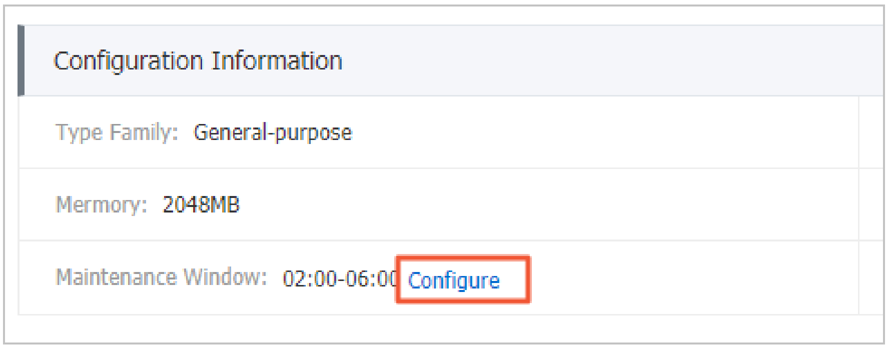
- Before the backend system starts maintenance, ApsaraDB for RDS sends notification emails to the contacts listed in your Alibaba Cloud account.
- To ensure smooth maintenance, your RDS instance enters the Instance Maintaining state prior to the maintenance window. While your RDS instance stays in Instance Maintaining state, database access and query operations such as performance monitoring are still available. However, apart from account and database management and IP address whitelist configuration, all other modify operations such as upgrade, downgrade, and restart are temporarily unavailable.
- During the maintenance window, one or two transient disconnections may occur. Make sure that your application is configured to automatically reconnect to your RDS instance.

Procedure

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



3. Find the target RDS instance. Then, click its ID, or click **Manage** in the **Actions** column.
4. In the **Configuration Information** section of the Basic Information page, click **Configure** next to **Maintenance Window**.



Configuration Information

Type Family: General-purpose

Mermory: 2048MB

Maintenance Window: 02:00-06:00 Configure

5. Select a maintenance window and click **Save**.

> **Note** The maintenance window is in UTC+8.

Related operations

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

9.4. Migrate an ApsaraDB RDS for PPAS instance across zones

You can migrate an ApsaraDB RDS for PPAS instance across zones within the same region. After the migration, the attributes, configuration, and endpoints of the instance remain unchanged. The migration may take several hours, depending on the volume of data to be migrated.

Migration scenarios

Migration scenario	Description
Migration from one zone to another	The original zone where the RDS instance resides cannot ensure service performance due to heavy workloads or other issues.
Migration from one zone to multiple zones	You want to achieve disaster recovery across data centers for the RDS instance. After the migration, the RDS instance and its secondary instance reside in different zones. Multi-zone deployment delivers higher disaster recovery capabilities than single-zone deployment. For example, RDS instances deployed in a single zone can withstand server and rack faults, whereas RDS instances deployed in multiple zones can withstand data center faults.
Migration from multiple zones to one zone	You can perform this type of migration to meet specific business requirements.

Billing

The migration is free of charge even if you migrate the RDS instance from one zone to multiple zones.

Prerequisites

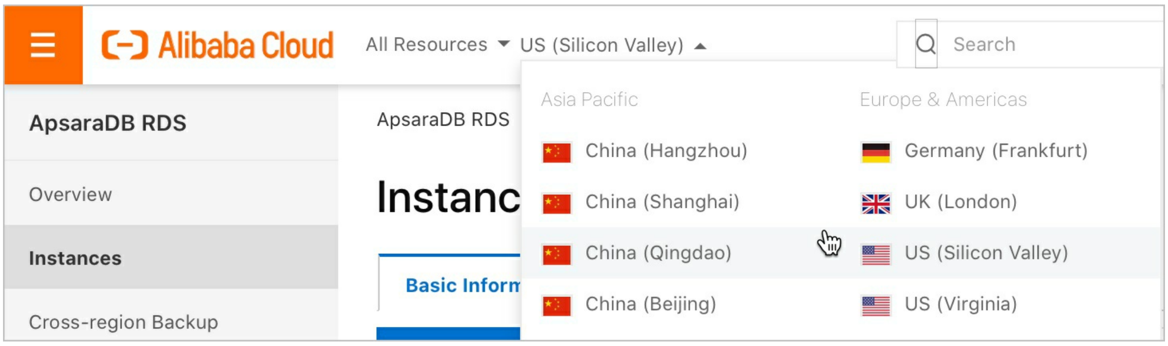
Cross-zone migration is available only when the region where the RDS instance resides has multiple zones. For more information about regions and zones, see Regions and zones.

Precautions

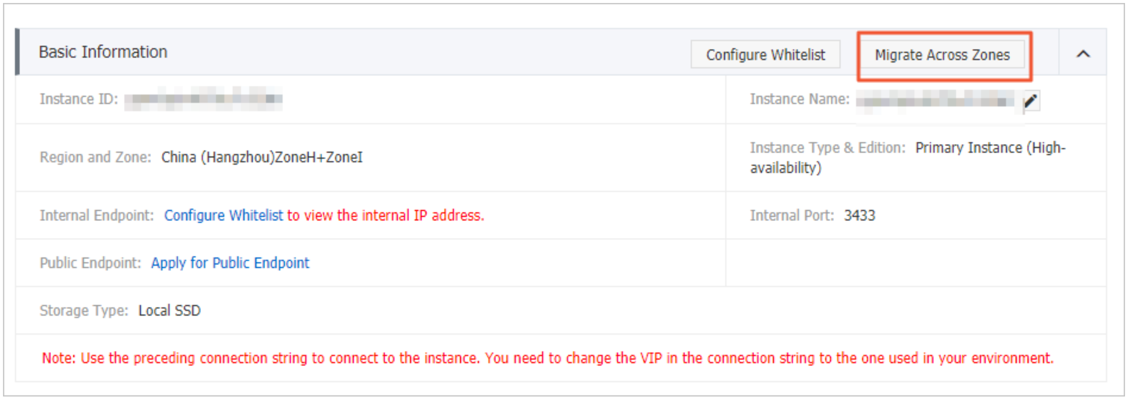
During cross-zone migration, a 30-second brief disconnection may occur, and most database, account, and network operations cannot be performed. Make sure that your application is configured to automatically reconnect to the RDS instance. We recommend that you migrate the RDS instance during off-peak hours.

Procedure

1. Log on to the ApsaraDB for RDS console.
2. In the top navigation bar, select the region where the target RDS instance resides.



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



Basic Information — Configure Whitelist — Migrate Across Zones

Instance ID: [redacted]

Instance Name: [redacted]

Region and Zone: China (Hangzhou)ZoneH+ZoneI

Instance Type & Edition: Primary Instance (High-availability)

Internal Endpoint: Configure Whitelist to view the internal IP address.

Internal Port: 3433

Public Endpoint: Apply for Public Endpoint

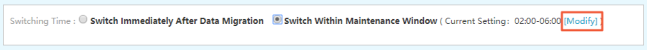
Storage Type: Local SSD

Note: Use the preceding connection string to connect to the instance. You need to change the VIP in the connection string to the one used in your environment.

5. In the Migrate Instance Across Zones dialog box, select the destination zone, VSwitch, and migration time. Then, click **OK**.
   After you click **OK**, the system starts to copy data to the destination zone. This does not affect the workloads on the RDS instance. After the data is copied, the workloads are switched over to the destination zone at the specified time (**Switch Now** or **Switch Within Maintenance Window**).

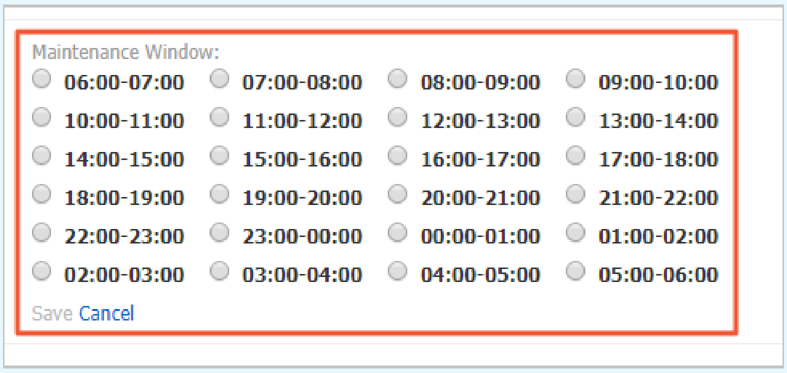
Note

- During the switchover, a 30-second brief disconnection may occur. Make sure that your application is configured to automatically reconnect to the RDS instance. Otherwise, you must manually reconnect the application to the RDS instance.
- If the Domain Name System (DNS) cache on the client is not flushed in a timely manner, some workloads may be switched over to the destination zone 10 minutes later. This causes another brief disconnection.
- If you want to change the maintenance window, follow these steps:
  a. Click **Change**.



Switching Time : ○ **Switch Immediately After Data Migration** ● **Switch Within Maintenance Window** (Current Setting: 02:00-06:00 [Modify])

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



Maintenance Window:

○ 06:00-07:00 ○ 07:00-08:00 ○ 08:00-09:00 ○ 09:00-10:00
○ 10:00-11:00 ○ 11:00-12:00 ○ 12:00-13:00 ○ 13:00-14:00
○ 14:00-15:00 ○ 15:00-16:00 ○ 16:00-17:00 ○ 17:00-18:00
○ 18:00-19:00 ○ 19:00-20:00 ○ 20:00-21:00 ○ 21:00-22:00
○ 22:00-23:00 ○ 23:00-00:00 ○ 00:00-01:00 ○ 01:00-02:00
○ 02:00-03:00 ○ 03:00-04:00 ○ 04:00-05:00 ○ 05:00-06:00

Save Cancel

  c. Refresh the page and perform Step 5 again.

Related operations

Operation	Description
Migration zone	Migrates an ApsaraDB for RDS instance across zones.

9.5. Switch over services between the RDS PPAS master and slave instances

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

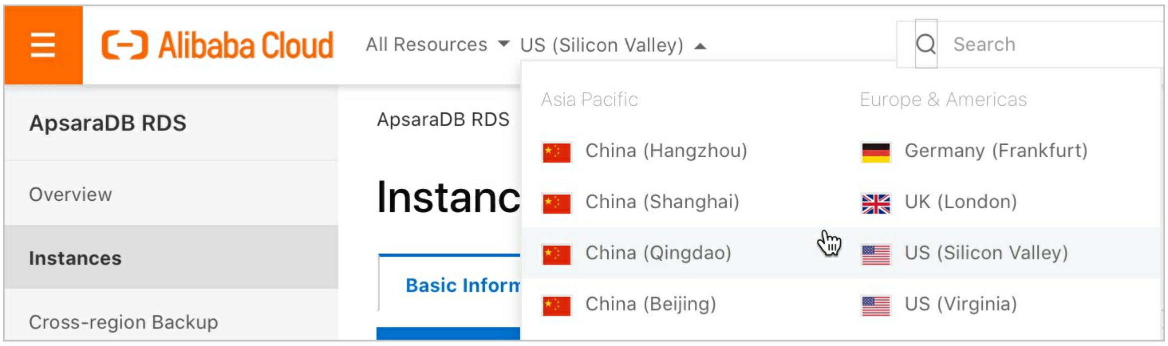
If the master instance cannot be accessed, your business is automatically switched to the slave instance.

Precautions

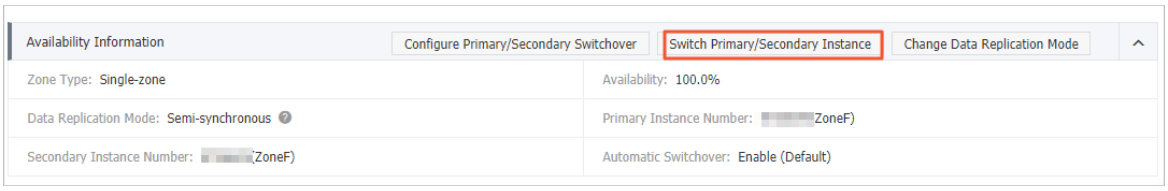
During the switchover, your RDS instance may be disconnected. Make sure that your application can automatically reconnect to your RDS instance after the switchover.

Procedure

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



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


Availability Information
Configure Primary/Secondary Switchover
Switch Primary/Secondary Instance
Change Data Replication Mode

Zone Type: Single-zone

Availability: 100.0%

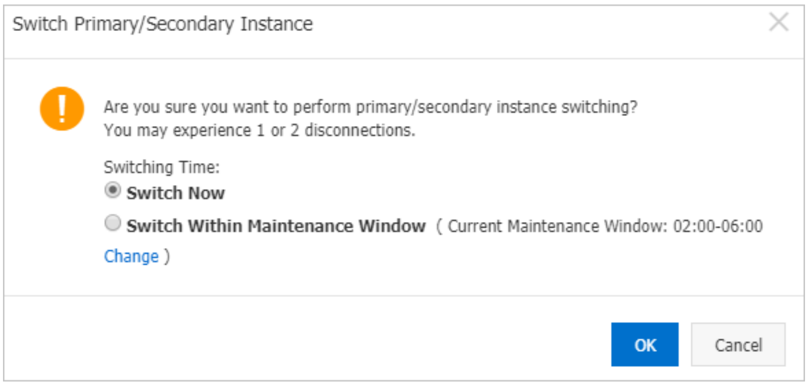
Data Replication Mode: Semi-synchronous

Primary Instance Number: [redacted]ZoneF)

Secondary Instance Number: [redacted]ZoneF)

Automatic Switchover: Enable (Default)

6. Select an appropriate time to perform the switch, and click **OK**.
   During the switch, operations such as managing the databases and accounts and switchover the network types cannot be performed. Therefore, we recommend that you select **Switch Within Maintenance Window**.



Switch Primary/Secondary Instance

Are you sure you want to perform primary/secondary instance switching?
You may experience 1 or 2 disconnections.

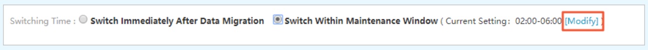
Switching Time:

● Switch Now

○ Switch Within Maintenance Window （Current Maintenance Window: 02:00-06:00 Change)

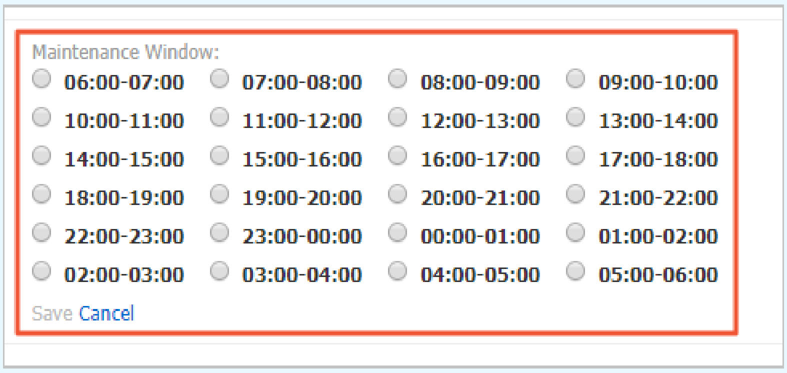
Note If you want to change the maintenance window, follow these steps:

i. Click **Change**.



Switching Time : ○ Switch Immediately After Data Migration ● Switch Within Maintenance Window (Current Setting: 02:00-06:00 [Modify])

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



Maintenance Window:

○ 06:00-07:00 ○ 07:00-08:00 ○ 08:00-09:00 ○ 09:00-10:00
○ 10:00-11:00 ○ 11:00-12:00 ○ 12:00-13:00 ○ 13:00-14:00
○ 14:00-15:00 ○ 15:00-16:00 ○ 16:00-17:00 ○ 17:00-18:00
○ 18:00-19:00 ○ 19:00-20:00 ○ 20:00-21:00 ○ 21:00-22:00
○ 22:00-23:00 ○ 23:00-00:00 ○ 00:00-01:00 ○ 01:00-02:00
○ 02:00-03:00 ○ 03:00-04:00 ○ 04:00-05:00 ○ 05:00-06:00

Save Cancel

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

APIs

Operation	Description
SwitchDBInstanceHA	Switches between the master and slave instances.

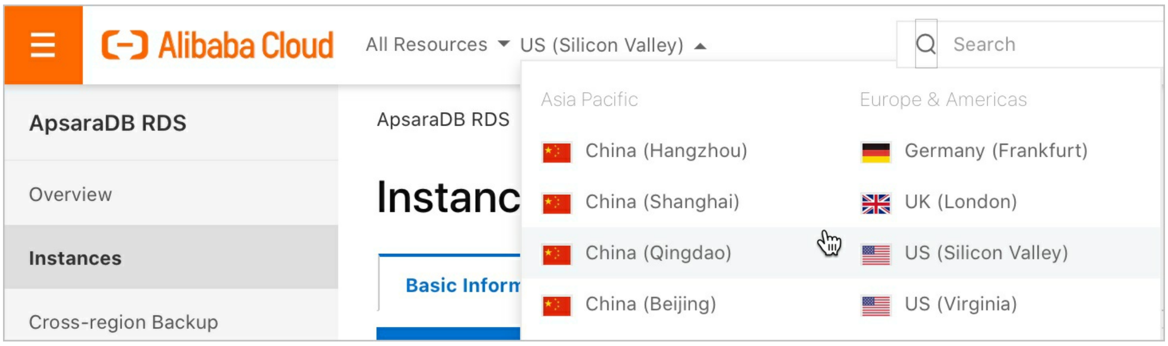
9.6. Release an RDS PPAS instance

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

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

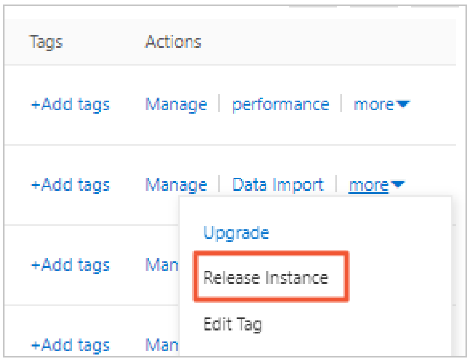
Release a pay-as-you-go-based RDS instance

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

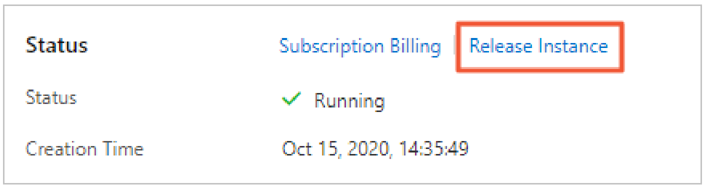


3. Use one of the following two methods to open the **Release Instance** dialog box:

- Method 1:
  Find the target RDS instance and in the **Actions** column choose **More > Release Instance**.



- Method 2:
  a. Find the target RDS instance and click the instance ID.
  b. On the **Basic Information** page, find the **Status** section and click **Release Instance**.



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

Unsubscribe from a subscription RDS instance

If you want to unsubscribe from an RDS instance, submit a ticket.

APIs

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

9.7. Change the configuration of an RDS PPAS instance

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

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

Configuration items

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

Configuration item	Description
CPU and Memory	All PPAS DB engine versions and editions support the CPU and memory change.
Capacity	All PPAS DB engine versions and editions allow you to increase storage capacity. Note • For information about the capacity range, see Primary ApsaraDB RDS instance types. • You cannot decrease the storage capacity if the RDS instance uses cloud SSDs. • If the storage capacity range of the current specifications cannot meet your requirements, you can change the specifications.

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

Billing

For more information, see Specification change fees.

Prerequisites

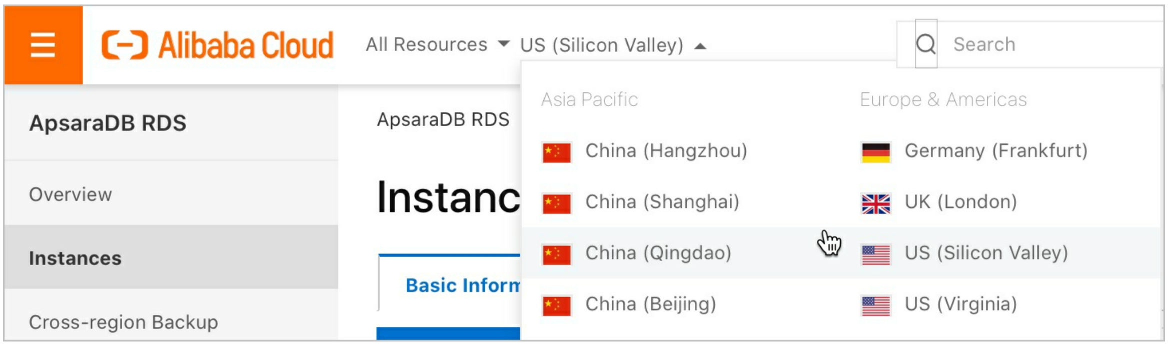
Your Alibaba Cloud account does not have an unpaid renewal order.

Precautions

When the new configuration is taking effect, the RDS instance may be disconnected for about 30 seconds and most operations related to databases, accounts, and networks cannot be performed. Therefore, we recommend that you change the configuration during off-peak hours or make sure that your application can automatically reconnect to the RDS instance.

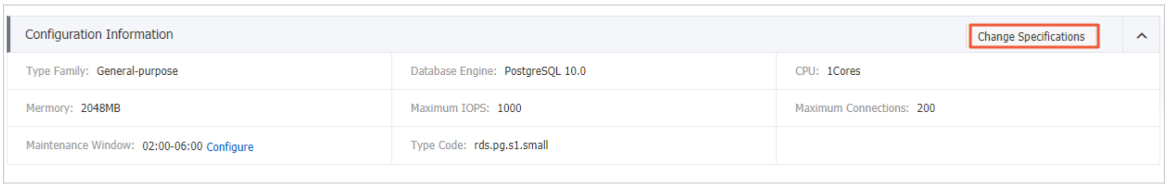
Procedure

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



3. Find the target RDS instance and click the instance ID.
4. On the **Basic information** page, find the **Configuration Information** section and click **Change**

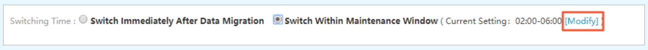
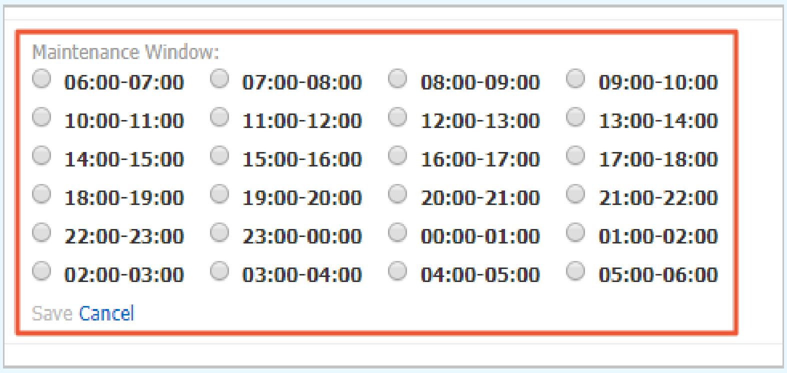
Specifications.



Configuration Information | Change Specifications

Type Family: General-purpose	Database Engine: PostgreSQL 10.0	CPU: 1Cores
Mermory: 2048MB	Maximum IOPS: 1000	Maximum Connections: 200
Maintenance Window: 02:00-06:00 Configure	Type Code: rds.pg.s1.small	

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

> **Note** To change the maintenance window, follow these steps:
>
> i. Click **Modify**.
>
> 
>
> Switching Time : ○ Switch Immediately After Data Migration ● Switch Within Maintenance Window (Current Setting: 02:00-06:00 [Modify])
>
> ii. In the **Configuration Information** section, select a maintenance window and click **Save**.
>
> 
>
> Maintenance Window:
>
> | | | | |
> |---|---|---|---|
> | ○ 06:00-07:00 | ○ 07:00-08:00 | ○ 08:00-09:00 | ○ 09:00-10:00 |
> | ○ 10:00-11:00 | ○ 11:00-12:00 | ○ 12:00-13:00 | ○ 13:00-14:00 |
> | ○ 14:00-15:00 | ○ 15:00-16:00 | ○ 16:00-17:00 | ○ 17:00-18:00 |
> | ○ 18:00-19:00 | ○ 19:00-20:00 | ○ 20:00-21:00 | ○ 21:00-22:00 |
> | ○ 22:00-23:00 | ○ 23:00-00:00 | ○ 00:00-01:00 | ○ 01:00-02:00 |
> | ○ 02:00-03:00 | ○ 03:00-04:00 | ○ 04:00-05:00 | ○ 05:00-06:00 |
>
> Save Cancel
>
> iii. Go back to the **Change Specifications** page, refresh the page, and change the configuration again.

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

FAQ

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

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

9.8. Modify the parameters of an ApsaraDB RDS for PPAS instance

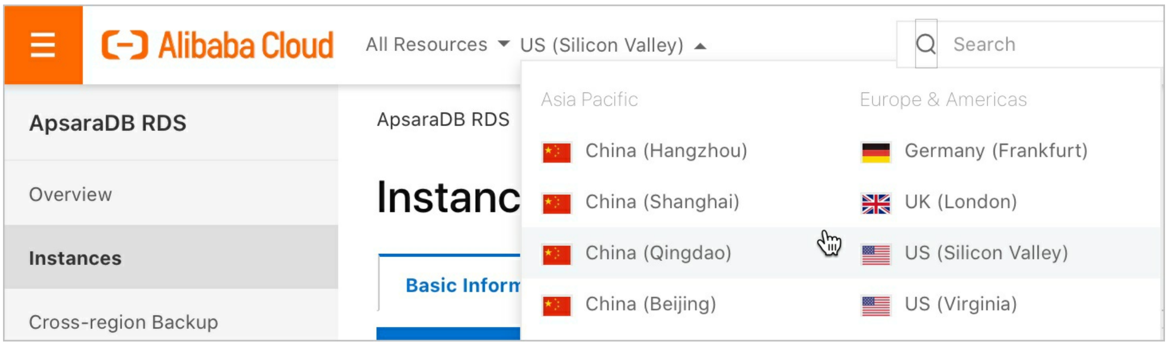
This topic describes how to view and modify the parameters of an ApsaraDB RDS for PPAS instance by using the ApsaraDB for RDS console or the API. You can also view the parameter modification history in the ApsaraDB for RDS console.

Precautions

- For instance stability purposes, you are allowed to modify only some parameters in the ApsaraDB for RDS console. If you want to modify more parameters, submit a ticket.
- When you modify parameters on the **Editable Parameters** tab, refer to the **Value Range** column that corresponds to each parameter.
- The new values of some parameters can take effect only after an instance restart. For more information, refer to the **Force Restart** column on the **Editable Parameters** tab in the ApsaraDB for RDS console. We recommend that you modify these parameters during off-peak hours and make sure that your application is configured to automatically reconnect to your RDS instance.

Modify parameters

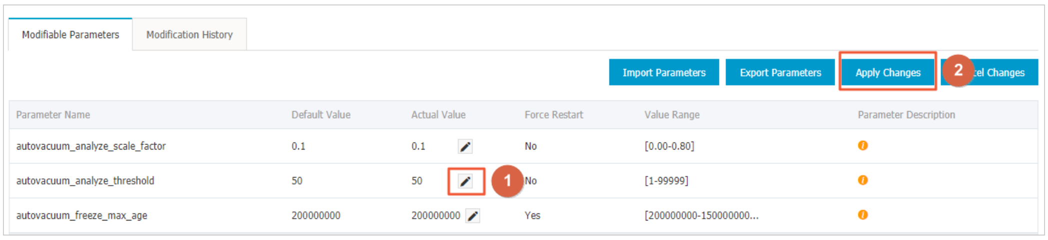
1. Log on to the ApsaraDB for RDS console.
2. In the top navigation bar, select the region where the target RDS instance resides.



3. Find the target RDS instance and click its ID.
4. In the left-side navigation pane, click **Parameters**.
5. On the **Editable Parameters** tab, reconfigure one or more parameters. You can modify one or more parameters at a time.
   - To modify a single parameter, follow these steps:
     a. Find the parameter and click the

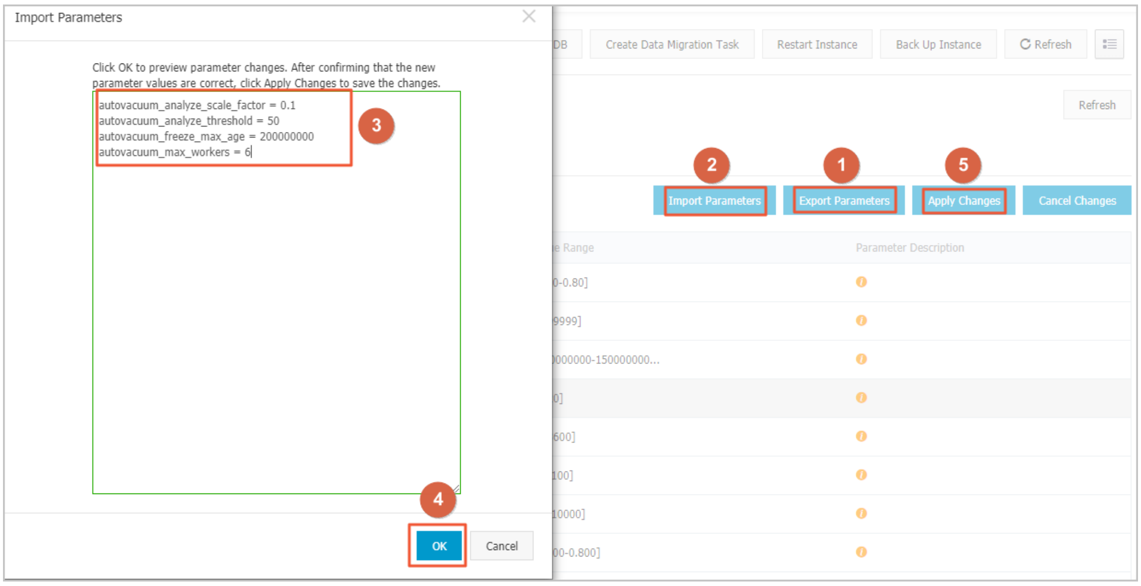
        ✎

        icon in the Actual Value column.
     b. In the dialog box that appears, enter a new value within the value range and click **Confirm**.
     c. In the upper-right corner of the page, click **Apply Changes**.
     d. In the dialog box that appears, click **OK**.



Parameter Name	Default Value	Actual Value	Force Restart	Value Range	Parameter Description
autovacuum_analyze_scale_factor	0.1	0.1	No	[0.00-0.80]	●
autovacuum_analyze_threshold	50	50	No	[1-99999]	●
autovacuum_freeze_max_age	200000000	200000000	Yes	[200000000-150000000...	●

- To modify more than one parameter at a time, follow these steps:
  a. In the upper-right corner, click **Export Parameters** to download the parameters and their values as a file to your computer.
  b. Open the file and modify parameters.
  c. In the upper-right corner, 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**.

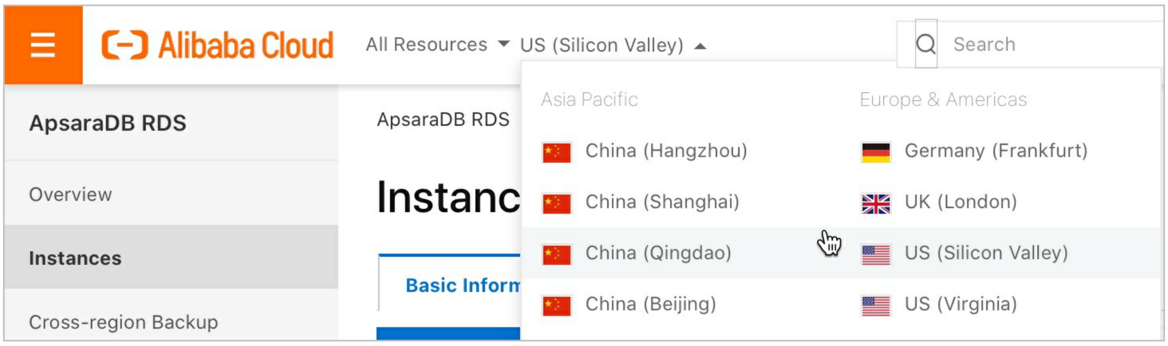


Click OK to preview parameter changes. After confirming that the new parameter values are correct, click Apply Changes to save the changes.

```
autovacuum_analyze_scale_factor = 0.1
autovacuum_analyze_threshold = 50
autovacuum_freeze_max_age = 200000000
autovacuum_max_workers = 6
```

View the parameter modification history

1. Log on to the ApsaraDB for RDS console.
2. In the top navigation bar, select the region where the target RDS instance resides.



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

5. Click the **Edit History** tab.
6. Select a time range and click **Search**.

Parameter description

For more information, see PPAS parameters in official PPAS documentation.

Related operations

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

9.9. Manage ApsaraDB RDS for PPAS instances in the recycle bin

This topic describes how to manage expired and overdue ApsaraDB RDS for PPAS instances in the recycle bin. You can unlock or destroy these instances in the recycle bin.

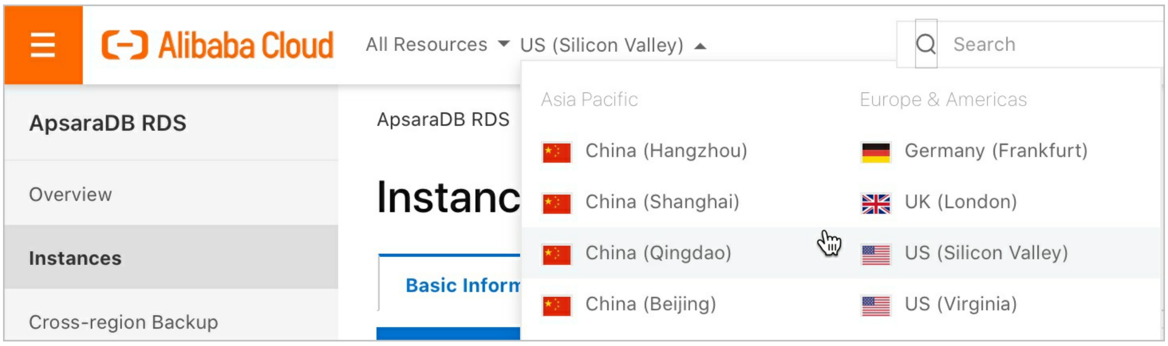
Unlock an overdue RDS instance

If a pay-as-you-go RDS instance is locked due to overdue payments, check the billing method of your Alibaba Cloud account in the Billing Management console.

Unlock an expired RDS instance

If a subscription RDS instance is locked due to expiration, you can go to the recycle bin and renew the RDS instance.

1. Log on to the recycle bin.
2. In the top navigation bar, select the region where the RDS instance resides.

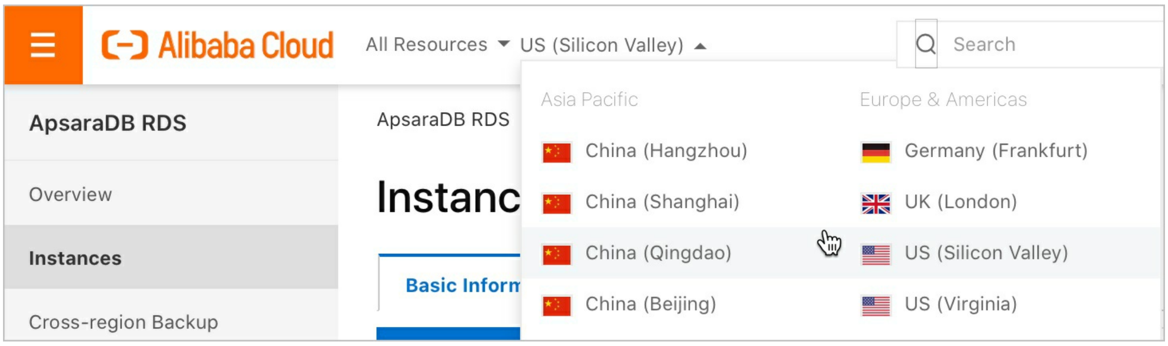


3. Find the RDS instance and click **Unlock**.
   The RDS instance is immediately unlocked after the renewal is complete.

Rebuild an RDS instance

After a subscription RDS instance expires, it will be retained for a specified period of time. After the specified retention period elapses, the RDS instance will be released. However, the backups of the RDS instance can still be retained for eight more days. During the eight-day retention period, you can restore the data of the RDS instance from a backup to a new RDS instance by using the instance rebuild function. For more information, see Unlock or rebuild an expired or overdue ApsaraDB RDS instance.

1. Log on to the recycle bin.
2. In the top navigation bar, select the region where the RDS instance resides.



3. Find the RDS instance and click **Recreate Instance**.
   By default, the system creates an RDS instance with the same specifications in the same zone. You can also create an RDS instance with different specifications in a different zone.

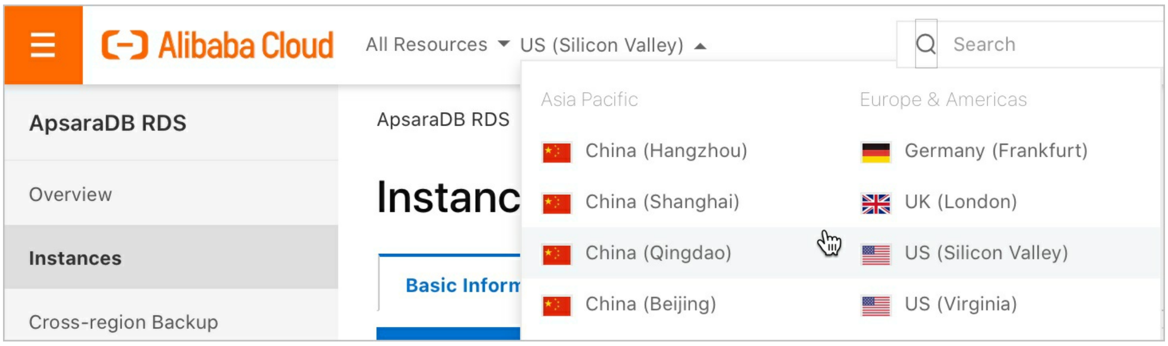
Destroy an RDS instance

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

Warning After you destroy an RDS instance, all of the backups are destroyed. Proceed with caution.

Procedure

1. Log on to the recycle bin.
2. In the top navigation bar, select the region where the RDS instance resides.



3. Find the RDS instance and click **Destroy**.

References

Unlock or rebuild an expired or overdue ApsaraDB RDS instance

10.Database connection

10.1. Connect to an ApsaraDB RDS for PPAS instance

After you complete the initial configurations, you can use an Elastic Compute Service (ECS) instance or a database client to connect to an ApsaraDB RDS for PPAS instance.
You can use a database client or Alibaba Cloud Data Management (DMS) to connect to an RDS instance. This topic describes how to connect to an ApsaraDB RDS for PPAS instance by using DMS and the pgAdmin 4 client.

Background information

You can log on to DMS from the ApsaraDB for RDS console and then connect to an RDS instance. DMS provides an integrated solution for data management. DMS supports data management, schema management, access control, BI charts, trend analysis, data tracking, performance optimization, and server management. DMS can be used to manage NoSQL databases and relational databases, such as MySQL, SQL Server, PostgreSQL, MongoDB, and Redis. It can also be used to manage Linux servers.

You can also use a database client to connect to an RDS instance. ApsaraDB RDS for PPAS is fully compatible with PPAS. You can connect to RDS in the similar way you connect to an on-premises PPAS server. This topic describes how to use the pgAdmin 4 client to connect to an RDS instance. This topic also serves as a reference if you choose to use other database clients. When you use a client to connect to an RDS instance, you must select the internal and public endpoints based on your network environment:

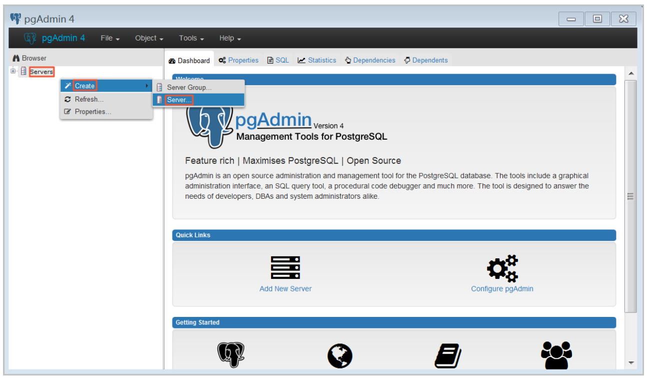
- If the client is deployed on an ECS instance that resides in the same region and has the same network type as the RDS instance, you can use the internal endpoint. For example, if the ECS and RDS instances both reside in VPCs in the China (Hangzhou) region, use the internal endpoint to establish a secure connection.
- In other situations, use the public endpoint.

Use DMS to connect to an RDS instance

For more information, see Use DMS to log on to an ApsaraDB RDS for PPAS instance.

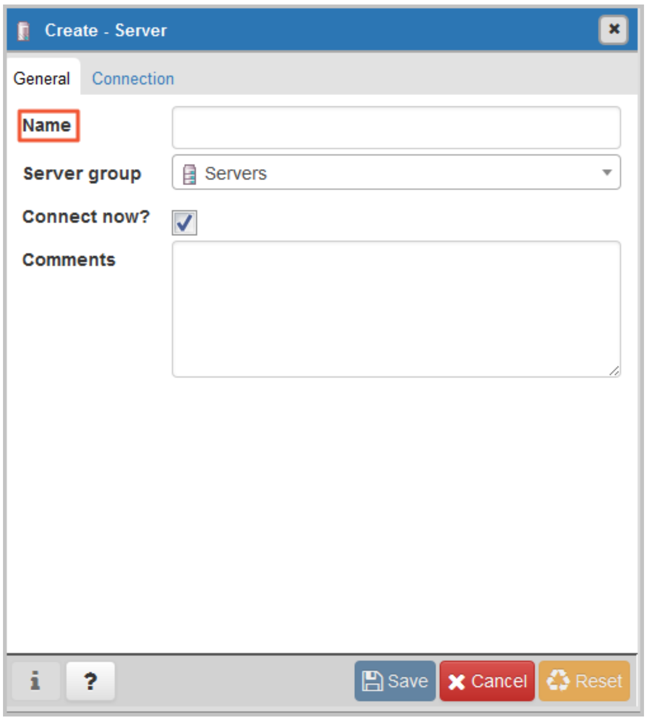
Use a client to connect to an RDS instance

1. Add the IP address that is used to access your RDS instance to an IP address whitelist. For more information about how to configure an IP address whitelist, see Configure a whitelist for an ApsaraDB RDS for PPAS instance.
2. Start the pgAdmin 4 client.
3. Right-click **Servers** and choose **Create > Server**.



pgAdmin is an open source administration and management tool for the PostgreSQL database. The tools include a graphical administration interface, an SQL query tool, a procedural code debugger and much more. The tool is designed to answer the needs of developers, DBAs and system administrators alike.

4. On the **General** tab of the **Create - Server** dialog box, enter the name of the server.



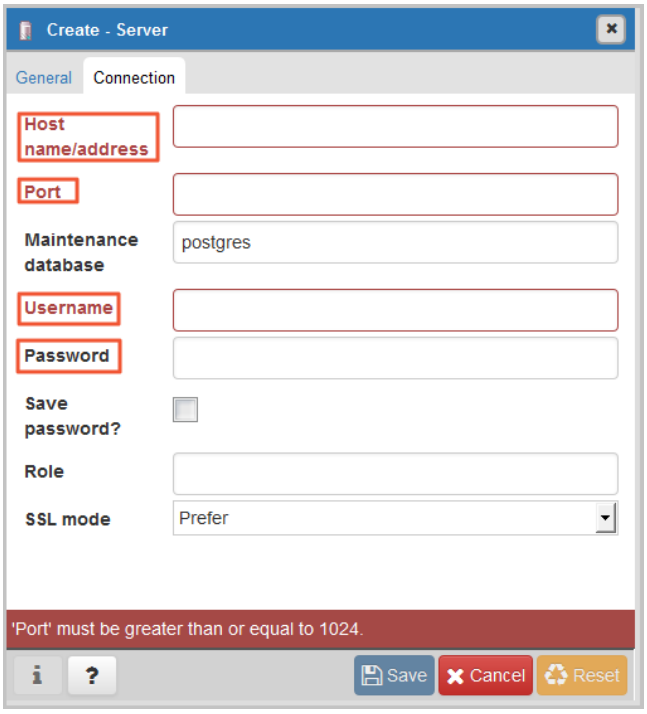
Name

Server group: Servers

Connect now? ☑

Comments

5. Click the **Connection** tab and enter the information of the target RDS instance.



Host name/address:

Port:

Maintenance database: postgres

Username:

Password:

Save password? □

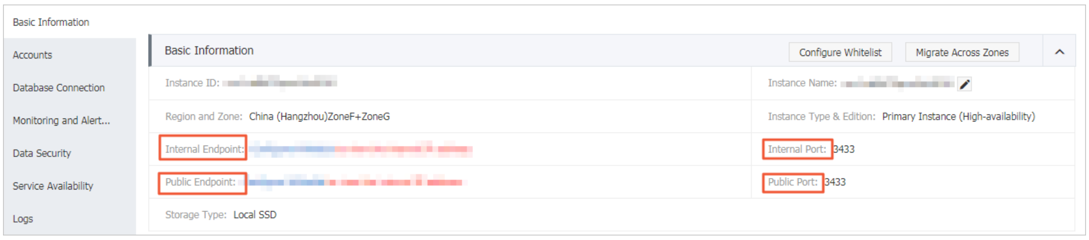
Role:

SSL mode: Prefer

'Port' must be greater than or equal to 1024.

Parameter description:

- Host name/address: Enter the endpoint of the RDS instance. If you connect to the RDS instance over the internal network, enter the internal endpoint of the RDS instance. If you connect to the RDS instance over the Internet, enter the public endpoint of the RDS instance. To view the internal and public endpoints and port numbers of the RDS instance, follow these steps:
  a. Log on to the ApsaraDB for RDS console.
  b. In the top navigation bar, select the region where your RDS instance resides.
  c. Find your RDS instance and click its ID.
  d. On the Basic Information page, find the internal and public endpoints and their port numbers.



Instance ID: [redacted]

Instance Name: [redacted]

Region and Zone: China (Hangzhou)ZoneF+ZoneG

Instance Type & Edition: Primary Instance (High-availability)

Internal Endpoint: [redacted]

Internal Port: 3433

Public Endpoint: [redacted]

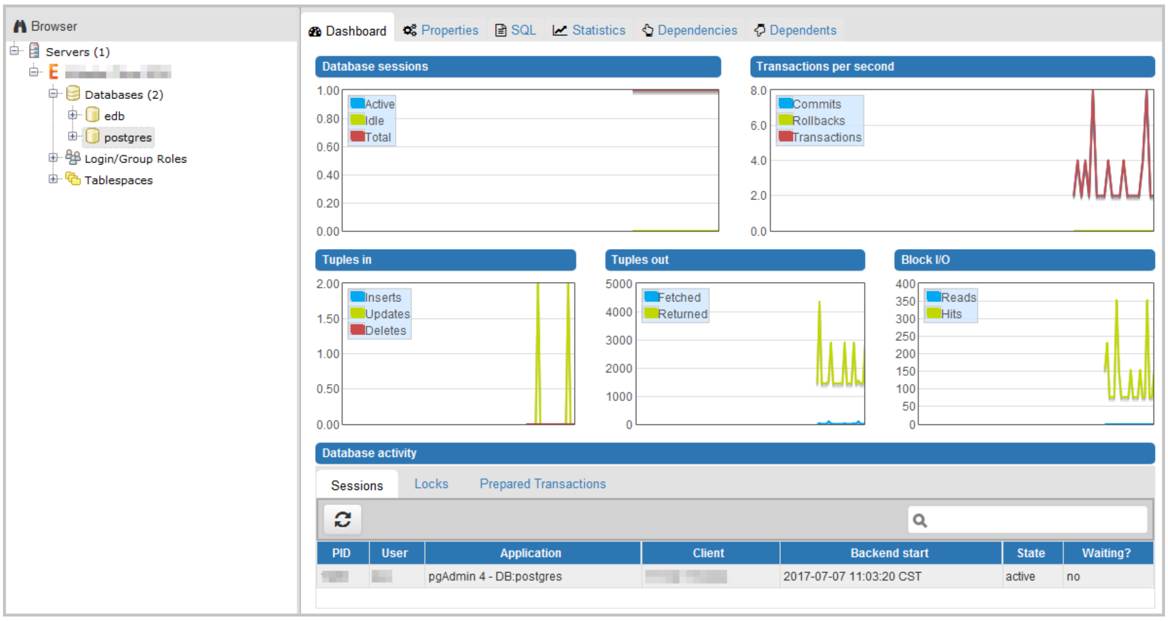
Public Port: 3433

Storage Type: Local SSD

- Port: Enter the port number of your RDS instance. If you connect to your RDS instance over an internal network, enter the internal port number of your RDS instance. If you connect to your RDS instance over the Internet, enter the public port number of your RDS instance.
- Username: Enter the username of the privileged account that is used to log on to your RDS instance.
- Password: Enter the password of the account that is used to log on to your RDS instance.

6. Click **Save**.
7. If the connection information is correct, choose **Servers** > **Server Name** > **Databases** > **edb** or **postgres**. The connection is successful if the following interface is displayed.

? Note edb and postgres are default system databases of your RDS instance. Do not perform any operation in these databases.



PID	User	Application	Client	Backend start	State	Waiting?
[redacted]	[redacted]	pgAdmin 4 - DB:postgres	[redacted]	2017-07-07 11:03:20 CST	active	no

FAQ

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

You can install third-party dependencies for your functions in Function Compute and use built-in modules to obtain the data of an RDS instance. For more information, see Install third-party dependencies.

10.2. Apply for or release a public endpoint for an ApsaraDB RDS for PPAS instance

ApsaraDB RDS for PPAS 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 the RDS instance over an internal network. If you want to connect to the RDS instance over the Internet, you must apply for a public endpoint.

Internal and public endpoints

Endpoint type	Description

Endpoint type	Description
Internal endpoint	• An internal endpoint is provided by default. You do not need to apply for this endpoint. In addition, you cannot release this endpoint. You can change the network type of the RDS instance. • If your application is deployed on an Elastic Compute Service (ECS) instance that resides in the same region and has the same network type as the RDS instance, the ECS and RDS instances can communicate over an internal network. You do not need to apply for a public endpoint for the RDS instance. • For security and performance purposes, we recommend that you connect to the RDS instance by using the internal endpoint.
Public endpoint	• You must manually apply for a public endpoint. You can release this endpoint if it is no longer required. • If you cannot connect to the RDS instance by using the internal endpoint, you must apply for a public endpoint. This includes the following scenarios: ◦ Connect to the RDS instance from an ECS instance that resides in a different region or has a different network type from the RDS instance. ◦ Connect to the RDS instance from a device outside Alibaba Cloud. **Note** • 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.

Procedure

1. Visit the RDS instance list, select a region above, and click the target instance ID.
2. In the left-side navigation pane, click **Database Connection**.
3. Apply for or release a public endpoint for your RDS instance:
   - If you have not applied for a public endpoint, you can click **Apply for Public Endpoint**.
   - 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 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.

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

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

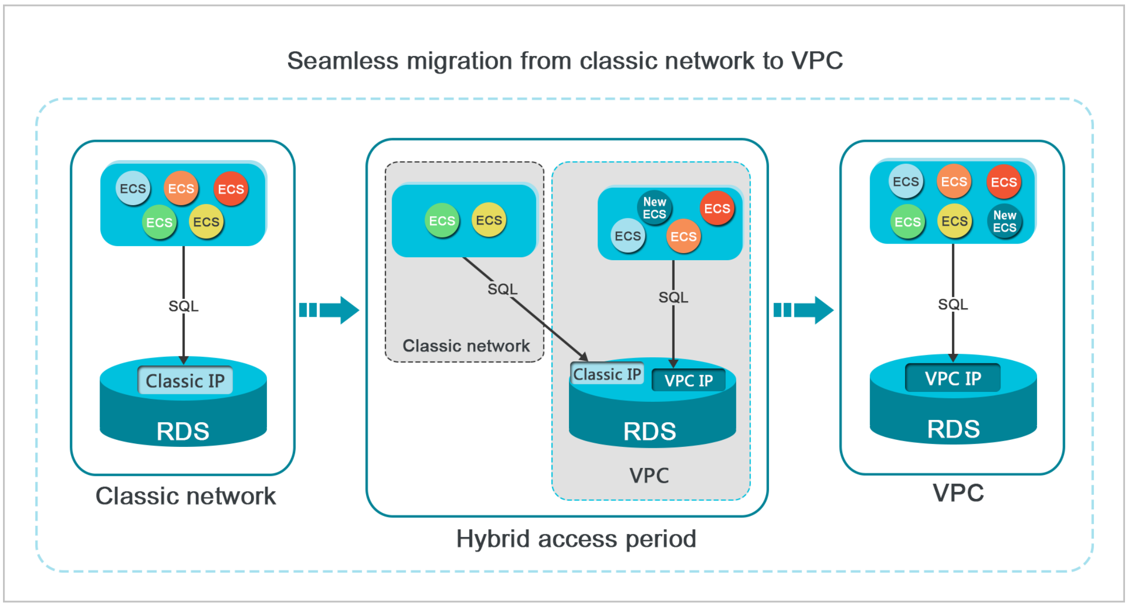
Background information

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

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

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

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



Limits

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

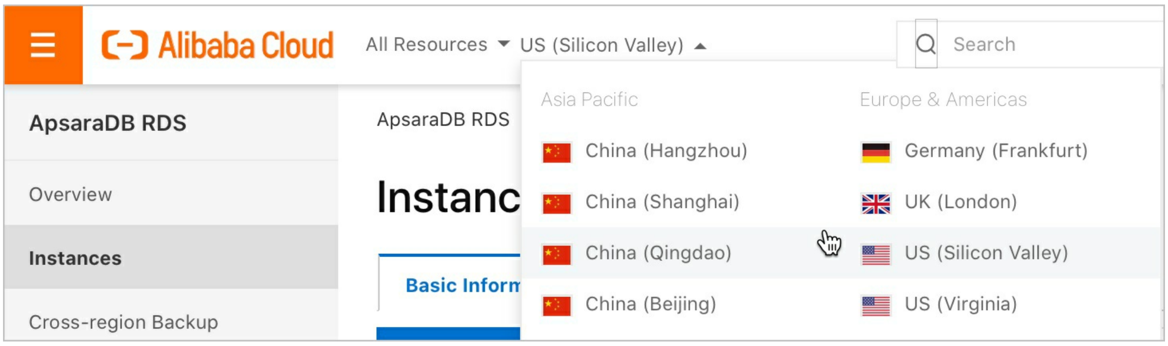
- Switching to the classic network is not supported.
- Migrating the RDS instance to another zone is not supported.

Prerequisites

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

Migrate the RDS instance from the classic network to a VPC

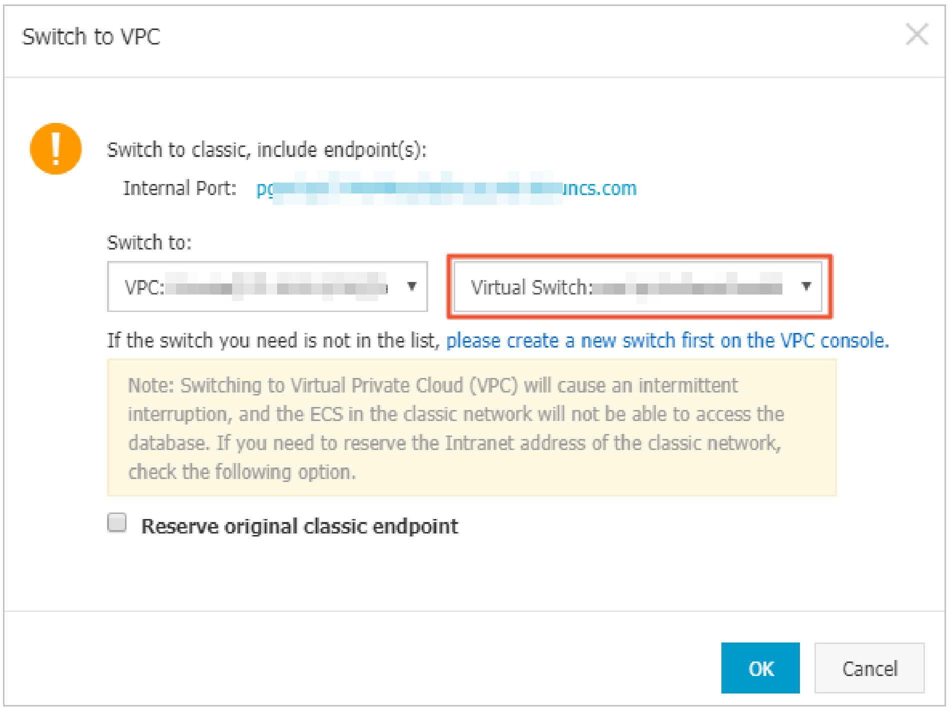
1. Log on to the ApsaraDB for RDS console.
2. In the upper-left corner of the page, select the region where the instance is located.



3. Find the instance and click the instance ID.
4. In the left-side navigation pane, click **Database Connections**.
5. Click **Switch to VPC**.
6. In the dialog box that appears, select a VPC and VSwitch, and select whether to retain the internal and public endpoints of the classic network.
   - Select a VPC. We recommend that you select the VPC where your ECS instance is located.

Otherwise, the ECS instance and RDS instance cannot communicate through the internal connections unless you create an express connection or gateway. For more information, see Alibaba Cloud CEN tutorials and VPN gateway.

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



Switch to classic, include endpoint(s):

Internal Port: pg[redacted]ncs.com

Switch to:

VPC: [redacted]

Virtual Switch: [redacted]

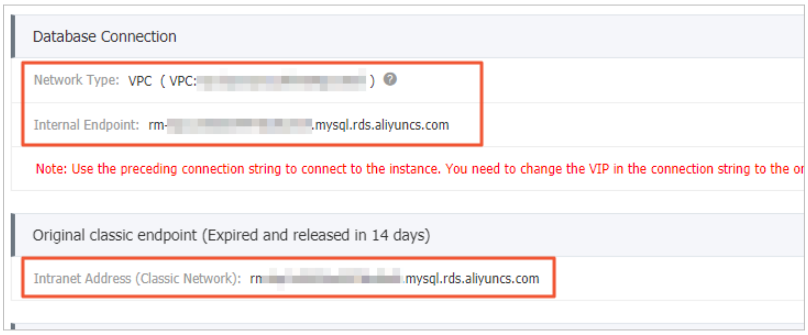
If the switch you need is not in the list, please create a new switch first on the VPC console.

Note: Switching to Virtual Private Cloud (VPC) will cause an intermittent interruption, and the ECS in the classic network will not be able to access the database. If you need to reserve the Intranet address of the classic network, check the following option.

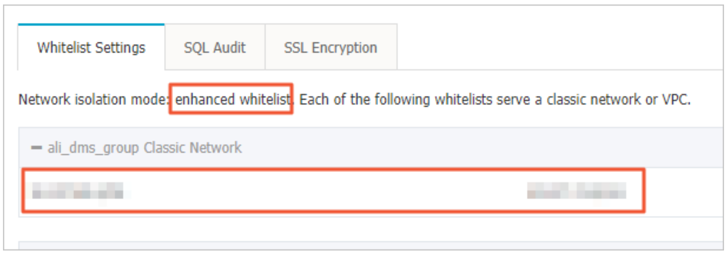
□ Reserve original classic endpoint

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

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

Action	Description
Select	The endpoint of the classic network is retained, and a new endpoint of the VPC is added. Indicates that the hybrid access mode is used and RDS can be simultaneously accessed by ECS instances both in the classic network and VPC through the internal endpoints. If the endpoint of the classic network is retained, the RDS instance will not be immediately disconnected when the network type is changed. The ECS instances in the classic network will not be disconnected from the internal access to the RDS instance until the internal endpoint of the classic network expires. Before the endpoint of the classic network expires, add the endpoint of the VPC to the ECS instance that is located in the same VPC. This makes sure that your business is smoothly migrated to the VPC. Within seven days before the endpoints of the classic network expire, the system will send a text message to the mobile phone bound to your account every day.  Database Connection Network Type: VPC (VPC:[redacted]) Internal Endpoint: rm-[redacted].mysql.rds.aliyuncs.com Note: Use the preceding connection string to connect to the instance. You need to change the VIP in the connection string to the or Original classic endpoint (Expired and released in 14 days) Intranet Address (Classic Network): rn[redacted]mysql.rds.aliyuncs.com

7. Add the internal IP address of the ECS instance in the VPC to the **VPC whitelist group** of the RDS instance. This makes sure that the ECS instance can access the RDS instance through the internal network. If no VPC whitelist group exists, create a new group.



Network isolation mode: enhanced whitelist Each of the following whitelists serve a classic network or VPC.

− ali_dms_group Classic Network

[redacted] [redacted]

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

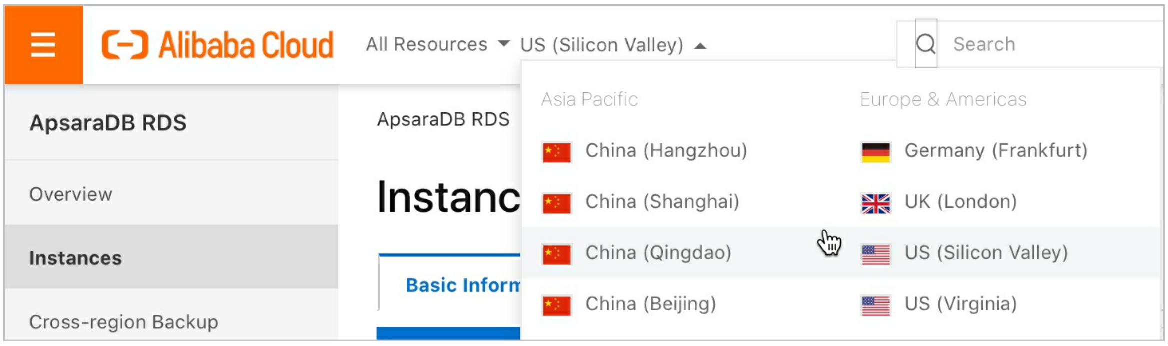
> **Note** To connect an ECS instance in the classic network to an RDS instance in a VPC through the internal network, you can use ClassicLink or switch the network type to VPC.

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

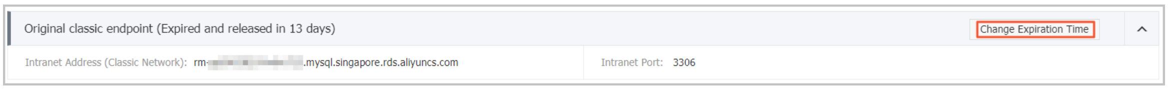
During the hybrid access period, you can change the retention period for the original internal endpoint of the classic network at any time as needed. The system will update the expiration date based on the modified date. For example, if the original internal endpoint of the classic network is set to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

Follow these steps to change the expiration time:

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



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



Original classic endpoint (Expired and released in 13 days)

Change Expiration Time

Intranet Address (Classic Network): rm-[redacted].mysql.singapore.rds.aliyuncs.com

Intranet Port: 3306

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

10.4. Use DMS to log on to an ApsaraDB RDS for PPAS instance

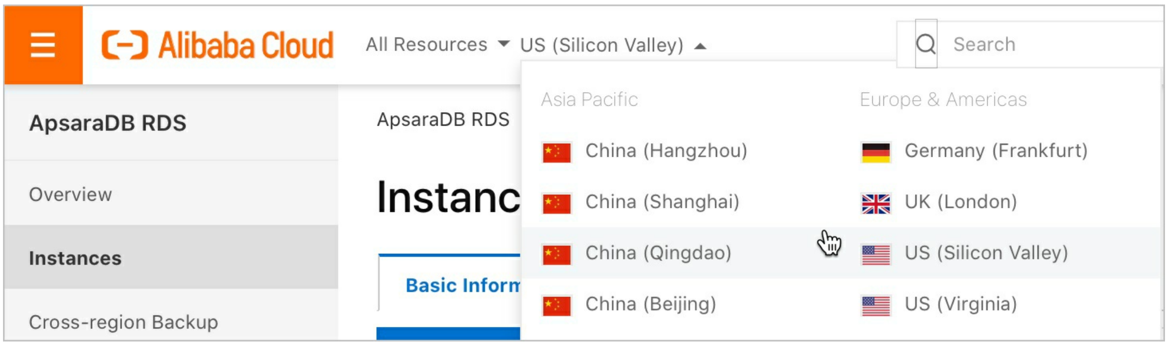
This topic describes how to log on to an ApsaraDB RDS for PPAS instance by using Alibaba Cloud Data Management (DMS).

Precautions

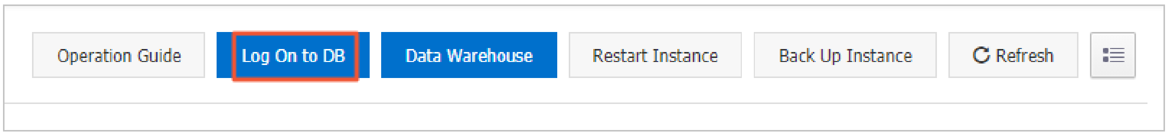
You can use only an internal endpoint to log on to the RDS instance by using DMS.

Procedure

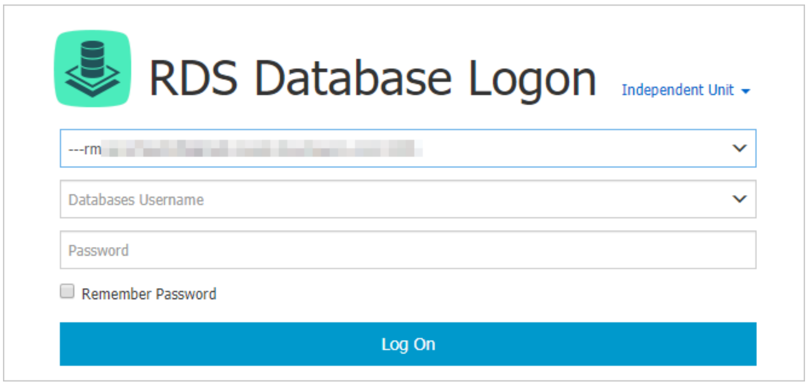
1. Log on to the ApsaraDB RDS console.
2. In the left-side navigation pane, click **Instances**. In the top navigation bar, select the region where your RDS instance resides.



3. Find your RDS instance and click its ID. The **Basic Information** page appears.
4. In the upper-right corner of the page, click **Log On to DB** to open the RDS Database Logon page.



5. On the **RDS Database Logon** page, configure the following parameters:
   - Endpoint:Port number: Enter the endpoint and port number that are used to log on to your RDS instance in the `<Internal endpoint>:<Internal port number>` format. Example: `rm-bpxxxxxxx.rds.aliyuncs.com:3433`. For more information about how to view the endpoint and port number of an RDS instance, see View and modify the internal and public endpoints and ports of an ApsaraDB RDS for PPAS instance.
   - Database Username: Enter the username of the account that is used to log on to your RDS instance.
   - Password: Enter the password of the account that is used to log on to your RDS instance.



6. Click **Log On**.

> **Note** If you want the browser to remember the password, select **Remember Password** before you click **Log On**.

7. If the system prompts you to add the classless inter-domain routing (CIDR) block of the DMS server to an IP address whitelist of your RDS instance, click **Specify for All Instances** or **Specify for Current Instance**.
8. Click **Log On**.

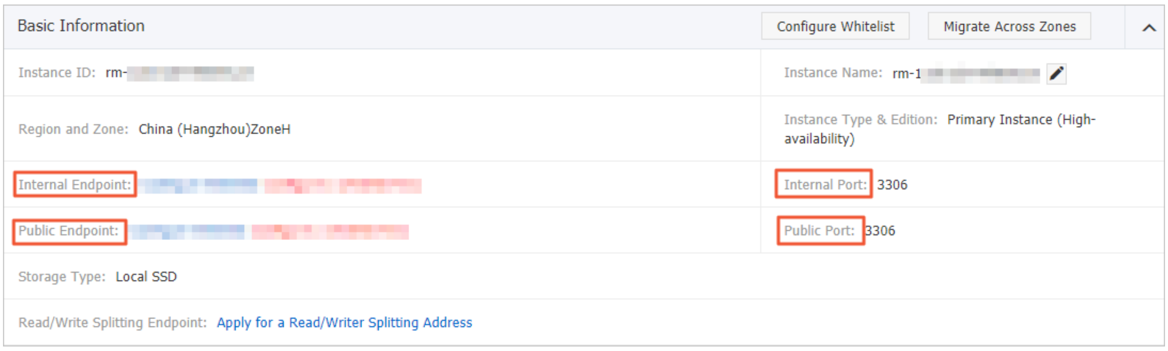
10.5. View and modify the internal and public endpoints and ports of an ApsaraDB RDS for PPAS instance

You must use the internal or public endpoint and port to connect to an ApsaraDB RDS for PPAS instance. This topic describes how to view and modify the internal and public endpoints and ports of an ApsaraDB RDS for PPAS instance in the ApsaraDB for RDS console.

View the internal and public endpoints and port numbers of an RDS instance in the original ApsaraDB RDS console

1. Visit the RDS instance list, select a region above, and click the target instance ID.
2. In the **Basic Information** section of the Basic Information page, view the internal and public endpoints and port numbers of the RDS instance.

> Note
>
> - The internal and public endpoints of an RDS instance are displayed only after you configure IP address whitelists for the instance. For more information, see Configure an IP address whitelist for an ApsaraDB RDS for MySQL instance.
> - The public endpoint of an RDS instance is displayed only after you apply for a public endpoint for the instance. For more information, see Apply for or release a public endpoint on an ApsaraDB RDS for MySQL instance.



Basic Information

Instance ID: rm-[redacted]

Instance Name: rm-1[redacted]

Region and Zone: China (Hangzhou)ZoneH

Instance Type & Edition: Primary Instance (High-availability)

Internal Endpoint: [redacted]

Internal Port: 3306

Public Endpoint: [redacted]

Public Port: 3306

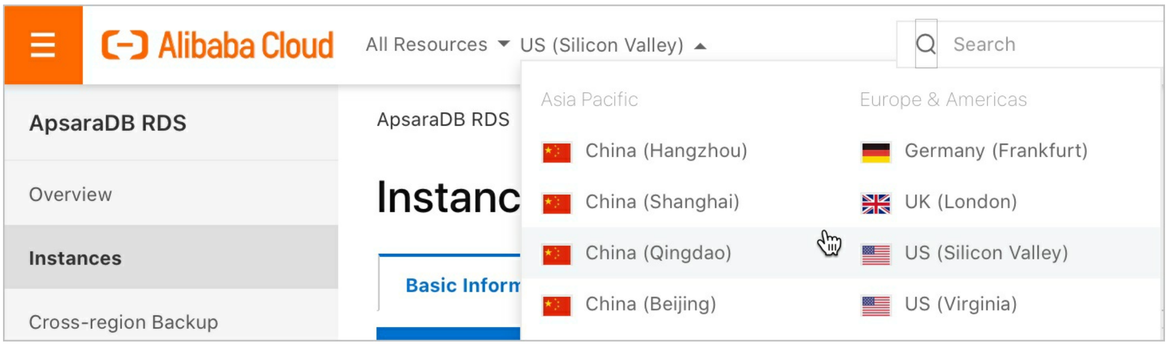
Storage Type: Local SSD

Read/Write Splitting Endpoint: Apply for a Read/Writer Splitting Address

Modify the internal and public endpoints

> Note You cannot modify the ports of an RDS instance.

1. Log on to the ApsaraDB for RDS console.
2. In the top navigation bar, select the region where the target RDS instance resides.



3. Find the target RDS instance and click its ID.
4. In the left-side navigation pane, select **Database Connection**.
5. In the upper-right corner of the Database Connection section, click **Change Endpoint**.
6. In the dialog box that appears, specify the internal or public endpoints, and click **OK**.

> ⓘ **Note** The prefix of the endpoint must be 8 to 64 characters in length and can contain letters, digits, and hyphens (-). It must start with a lowercase letter.

10.6. Change the network type of an ApsaraDB RDS for PPAS instance

This topic describes how to change the network type of an ApsaraDB RDS for PPAS instance between classic network and VPC.

Network type

- Classic network: RDS instances in the classic network are not isolated. You can only use whitelists to block unauthorized access to the instances.
- VPC: Each Virtual Private Cloud (VPC) is an isolated network. We recommend that you select the VPC network type because it is more secure.
  You can customize the routing table, Classless Inter-Domain Routing (CIDR) blocks, and gateway in a VPC. To smoothly migrate applications to the cloud, you can use leased lines or VPNs to connect your own data center to a VPC to make a virtual data center on the cloud.

> ⓘ **Note**
>
> - You can select the classic network or VPC network type and switch between them free of charge.
> - Before you change the network type of an ApsaraDB RDS for PPAS instance, you must switch its network isolation mode to enhanced whitelist. For more information, see Switch an ApsaraDB RDS for PPAS instance to the enhanced whitelist mode.

Change the network type from VPC to classic network

Precautions

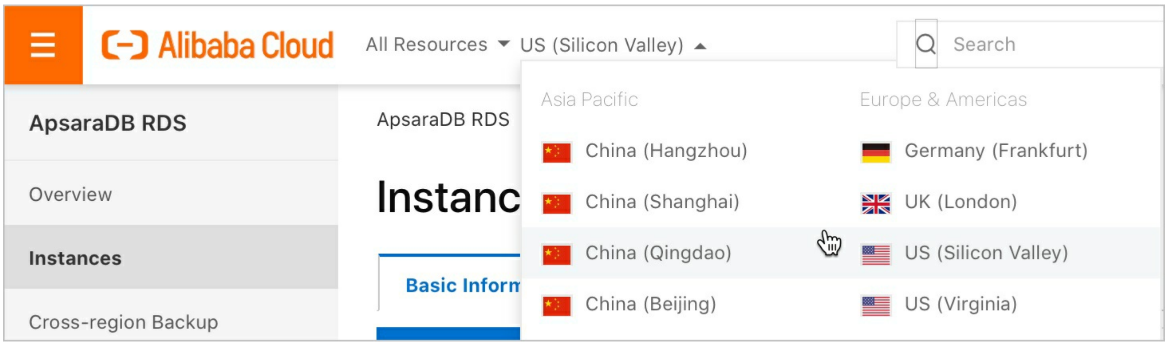
- After the network type is changed, the internal endpoint of your RDS instance remains unchanged, but the IP address associated with the internal endpoint changes.
- After the network type of an RDS instance is changed to classic network, the Elastic Compute Service

(ECS) instances that used to reside in the same VPC as your RDS instance cannot access your RDS instance by using the internal endpoint. Make sure that you update the endpoint in the application that needs to connect to the RDS instance.

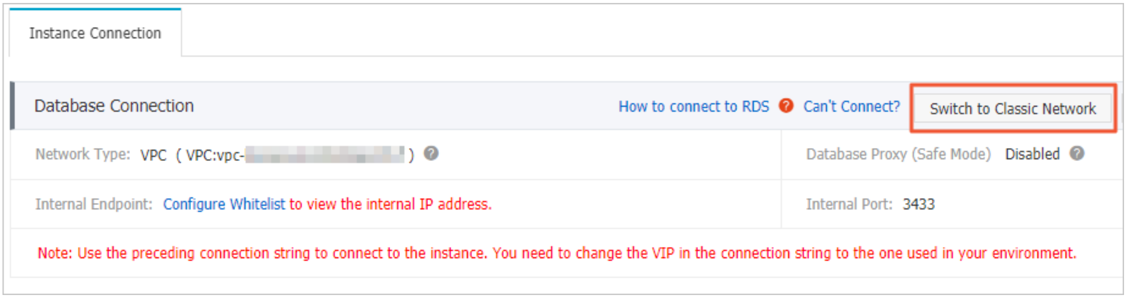
- When you change the network type, a 30-second brief disconnection may occur. To avoid interference to your business, change the network type during off-peak hours or make sure that your application is configured to automatically reconnect to the RDS instance.

Procedure

1. Log on to the ApsaraDB for RDS console.
2. In the top navigation bar, select the region where the target RDS instance resides.



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



Network Type: VPC (VPC:vpc-[redacted])

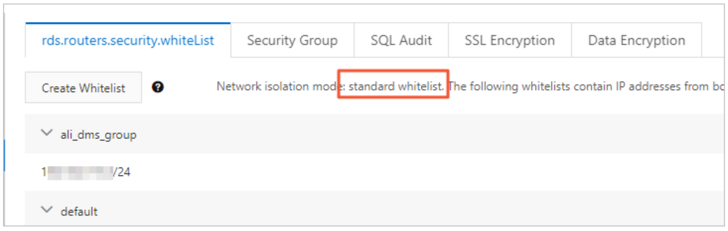
Database Proxy (Safe Mode) Disabled

Internal Endpoint: Configure Whitelist to view the internal IP address.

Internal Port: 3433

Note: Use the preceding connection string to connect to the instance. You need to change the VIP in the connection string to the one used in your environment.

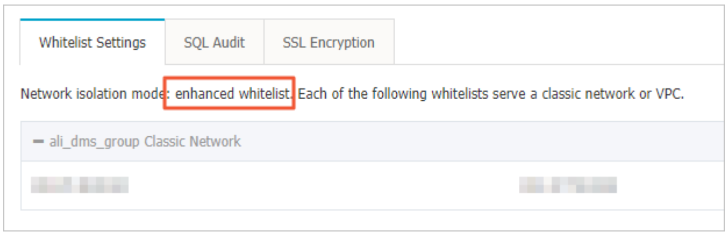
6. In the dialog box that appears, click **OK**.
   After the network type is changed, only ECS instances in the classic network can access your RDS instance over an internal network. Configure the internal endpoint for these ECS instances.
7. Configure a whitelist of your RDS instance to allow access from the ECS instances over the internal network.
   - If the network isolation mode of the RDS instance is standard whitelist, add the internal IP addresses of the ECS instances to any whitelist.



Network isolation mode: standard whitelist. The following whitelists contain IP addresses from bo

1[redacted]/24

   - If the network isolation mode of the RDS instance is enhanced whitelist, add the internal IP addresses of the ECS instances to a classic network whitelist. If no classic network whitelist is available, create a whitelist.



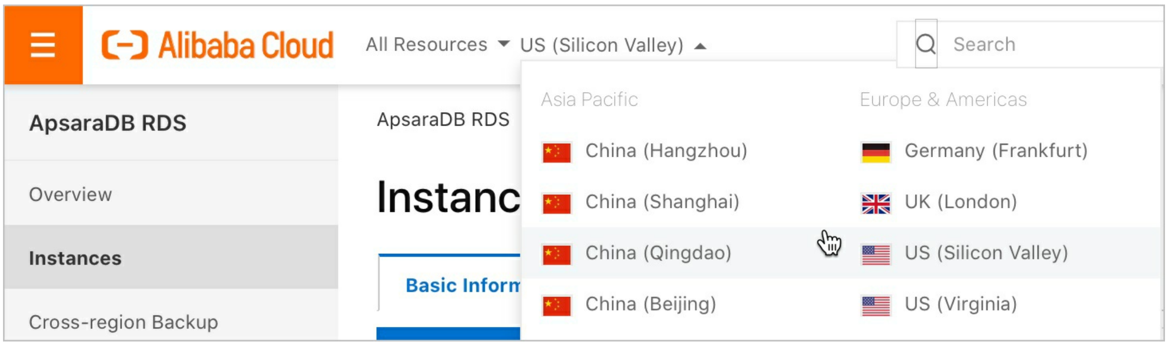
Network isolation mode: enhanced whitelist. Each of the following whitelists serve a classic network or VPC.

ali_dms_group Classic Network

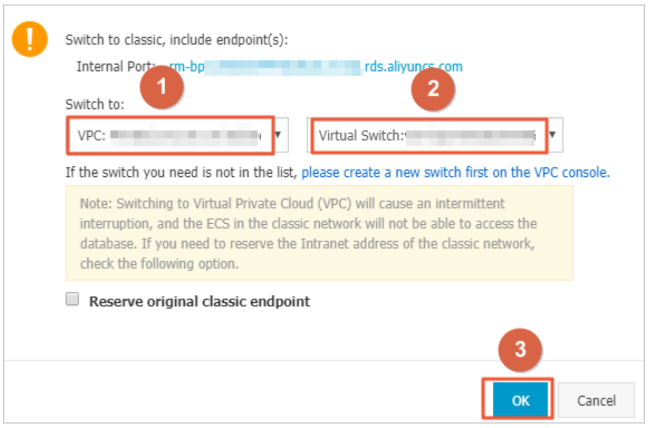
Change the network type from classic network to VPC

Procedure

1. Log on to the ApsaraDB for RDS console.
2. In the top navigation bar, select the region where the target RDS instance resides.



3. Find the target RDS instance and click its ID.
4. In the left-side navigation pane, click **Database Connection**.
5. Click **Switch to VPC**.
6. In the Switch to VPC dialog box, select a VPC and VSwitch and specify whether to retain the classic network endpoint.
   - Select a VPC. We recommend that you select the VPC where your ECS instances reside. Otherwise, the ECS instances cannot communicate with the RDS instance over the internal network unless you enable communication by using Cloud Enterprise Network or VPN Gateway.
   - Select a VSwitch. If no VSwitches are available in the selected VPC, create one in the same zone where the RDS instance resides. For more information, see Create a VSwitch.



Switch to classic, include endpoint(s):

Internal Port: rm-bp rds.aliyuncs.com

Switch to:

VPC:

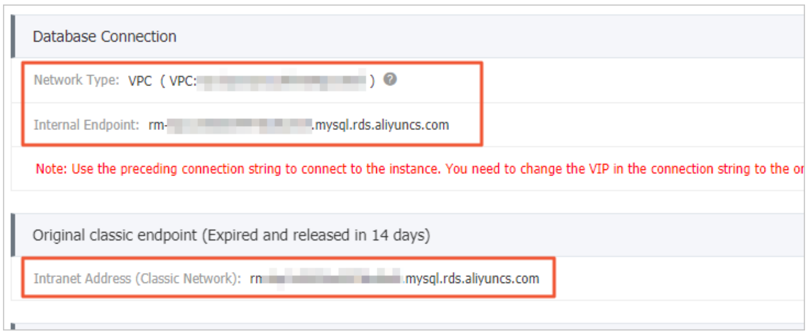
Virtual Switch:

If the switch you need is not in the list, please create a new switch first on the VPC console.

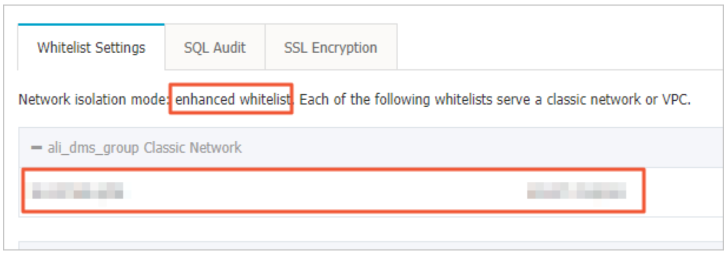
Note: Switching to Virtual Private Cloud (VPC) will cause an intermittent interruption, and the ECS in the classic network will not be able to access the database. If you need to reserve the Intranet address of the classic network, check the following option.

□ Reserve original classic endpoint

   - Determine whether to select **Reserve Original Classic Network Endpoint** based on the following table.

Action	Description
Clear	The classic network endpoint is not retained and will become a VPC endpoint. When you change the network type, a 30-second brief disconnection may occur, and connections between ECS instances in the classic network and the RDS instance are interrupted.
Select	The classic network endpoint is retained, and a new VPC endpoint is generated. In such cases, the RDS instance runs in hybrid access mode. Specifically, ECS instances both in the classic network and a VPC can access the RDS instance over the internal network. When you change the network type, no brief disconnection occurs. Connections between ECS instances in the classic network and the RDS instance remain available until the classic network endpoint expires. Before the classic network endpoint expires, you must add the new VPC endpoint to the ECS instances. This allows you to migrate your business to the VPC without interruption. The system will send a text message to the phone number bound to your Alibaba Cloud account every day within the seven days before the classic network endpoint expires.  Database Connection Network Type: VPC (VPC:[redacted]) Internal Endpoint: rm-[redacted].mysql.rds.aliyuncs.com Note: Use the preceding connection string to connect to the instance. You need to change the VIP in the connection string to the or Original classic endpoint (Expired and released in 14 days) Intranet Address (Classic Network): rn[redacted].mysql.rds.aliyuncs.com For more information, see Configure a hybrid access solution to smoothly migrate an RDS instance from the classic network to a VPC.

7. Add the internal IP addresses of ECS instances in the selected VPC to a VPC whitelist. This allows the ECS instances to access the RDS instance over the internal network. If no VPC whitelists are available, create one.



Network isolation mode: enhanced whitelist. Each of the following whitelists serve a classic network or VPC.

ali_dms_group Classic Network

[redacted] [redacted]

8.
   - If you have retained the classic network endpoint, add the VPC endpoint to the ECS instances before the classic network endpoint expires.
   - If you have not retained the classic network endpoint, connections between ECS instances in the classic network and the RDS instance over the internal network are interrupted. You must add the new endpoint to ECS instances in the VPC immediately after the network type is changed.

> Note If you want to connect ECS instances in the classic network to an RDS instance in a VPC over the internal network, you can establish connections by using ClassicLink or migrate the ECS instances to the same VPC as the RDS instance.

FAQ

How do I change the VPC of an RDS instance?

1. You cannot directly change the VPC of an RDS instance. You can change the network type of the RDS instance from VPC to classic network .
2. Change the network type back to select a new VPC.

Related operations

Operation	Description
Change the network type of an ApsaraDB for RDS instance	Changes the network type of an ApsaraDB for RDS instance.

11.Account

11.1. Create an account on an ApsaraDB RDS for PPAS instance

After you create an ApsaraDB RDS for PPAS instance, you must create databases and accounts on the instance before you can use the instance. This topic describes how to create an account on an ApsaraDB RDS for PPAS instance.

Precautions

- The PPAS database engine requires you to create a privileged account in the ApsaraDB RDS console. Then, you can create and manage databases by using Alibaba Cloud Data Management (DMS).
- Databases on the same RDS instance share all of the resources that belong to the instance. Each RDS instance supports one privileged account and multiple standard accounts. You can create and manage standard accounts by using SQL statements.
- If you want to migrate data from an on-premises database to an RDS instance, you must log on to the RDS instance and create a database and an account with the same names as the on-premises database and its authorized account.
- Follow the least privilege principle to create accounts and grant them read-only permissions or both read and write permissions on databases based on your business requirements. If necessary, you can create more than one account and grant them only the permissions on specific databases. If an account does not need to write data to a database, grant only the read-only permissions on that database to the account.
- For security purposes, we recommend that you configure strong passwords for the accounts that are created on your RDS instance. In addition, we recommend that you change the passwords on a regular basis.
- After you create a privileged account for your RDS instance, you cannot delete the privileged account.

Create a privileged account

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

Parameter	Description

Parameter	Description
Database Account	Enter the username of the account. The username of the account must meet the following requirements: ○ The username of the account must be 2 to 16 characters in length. ○ The username of the account must start with a letter and end with a letter or digit. ○ The username of the account can contain lowercase letters, digits, and underscores (_). ○ The username of the account cannot be the same as the username of an existing account.
Password	Enter the password of the account. The password of the account must meet the following requirements: ○ 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. ○ Special characters include: ! @ # $ % ^ & * ( ) _ + - =
Confirm Password	Enter the password of the account again.

7. Click **OK**.

Create a standard account

To create a standard account, you must log on to the RDS instance by using DMS and then execute the following statement:

```
CREATE ROLE "username" CREATEDB CREATEROLE LOGIN ENCRYPTED PASSWORD 'password';
```

For more information about how to connect to an RDS instance, see Connect to an ApsaraDB RDS for PPAS instance.

Manage a schema

1. Execute the following statement to create an account that is authorized to log on to the RDS instance:

   ```
   CREATE USER newuser LOGIN PASSWORD 'password';
   ```

   Parameter description:

   - USER: the username of the account. In this example, the username is newuser.
   - PASSWORD: the password of the account.

2. Execute the following statement to create a schema for the newuser account:

   ```
   CREATE SCHEMA newuser;GRANT newuser to myuser;ALTER SCHEMA myuser OWNER TO newuser;REVO
   KE newuser FROM myuser;
   ```

> Note
>
> - If you have not granted the myuser role to the newuser account before you execute the `ALTER SCHEMA myuser OWNER TO newuser` statement, the following error is reported:
>
>   ```
>   ERROR: must be member of role "newuser"
>   ```
>
> - After you grant the OWNER permissions to the newuser account, we recommend that revoke the myuser role from the newuser account. This increases the security of the RDS instance.

3. Log on to the RDS instance by using the newuser account.

```
psql -U newuser -h intranet4example.pg.rds.aliyuncs.com -p 3433 pg001
Password for user newuser:
psql.bin (9.4.4, server 9.4.1)
Type "help" for help.
```

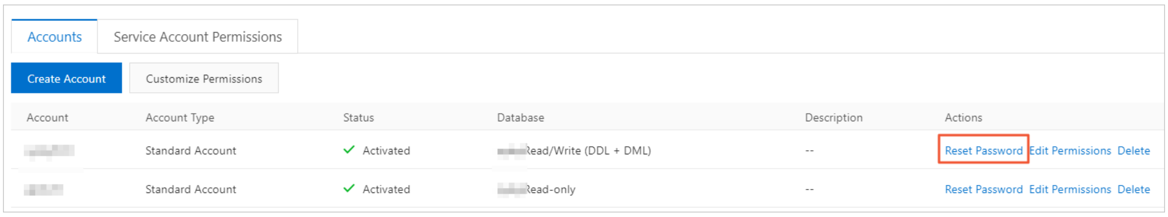
11.2. Reset the password of an account on an ApsaraDB RDS for PPAS instance

This topic describes how to reset the password of an account on your ApsaraDB RDS for PPAS instance. If the password is lost, you can reset the password in the ApsaraDB RDS console.

Procedure

> Note For data security purposes, we recommend that you change the password of each account on a regular basis.

1. Visit the RDS instance list, select a region above, and click the target instance ID.
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
[redacted]	Standard Account	✓ Activated	[redacted]Read/Write (DDL + DML)	--	Reset Password Edit Permissions Delete
[redacted]	Standard Account	✓ Activated	[redacted]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.

12.Database

12.1. Create a database on an ApsaraDB RDS for PPAS instance

Before you start to use ApsaraDB RDS, you must create databases and accounts on your RDS instance. This topic describes how to create a database on an ApsaraDB RDS for PPAS instance.

Prerequisites

Create an ApsaraDB RDS for PPAS 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.

Precautions

- Databases on the same RDS instance share all of the resources that belong to the instance. You can create and manage a number of databases on your RDS instance by using SQL statements.
- If you want to migrate data from an on-premises database to your RDS instance, you must create a database and an account on your RDS instance. The database and the account must have the same names as the on-premises database and its authorized account.

Procedure

1. Connect to your RDS instance. For more information, see Connect to an ApsaraDB RDS for PPAS instance.
2. In the SQL window, execute the following statement to create a database:

```
CREATE DATABASE name
 [ [ WITH ] [ OWNER [=] user_name ]
    [ TEMPLATE [=] template ]
    [ ENCODING [=] encoding ]
    [ LC_COLLATE [=] lc_collate ]
    [ LC_CTYPE [=] lc_ctype ]
    [ TABLESPACE [=] tablespace_name ]
    [ CONNECTION LIMIT [=] connlimit ] ]
```

For example, if you want to create a database named test, execute the following statement:

```
create database test;
```

12.2. Delete a database from an ApsaraDB RDS for PPAS instance

This topic describes how to delete a database from an ApsaraDB RDS for PPAS instance.

Procedure

1. Connect to the RDS instance to which the database belongs. For more information, see Connect to an ApsaraDB RDS for PostgreSQL instance.
2. Run the following statement to delete the database:

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

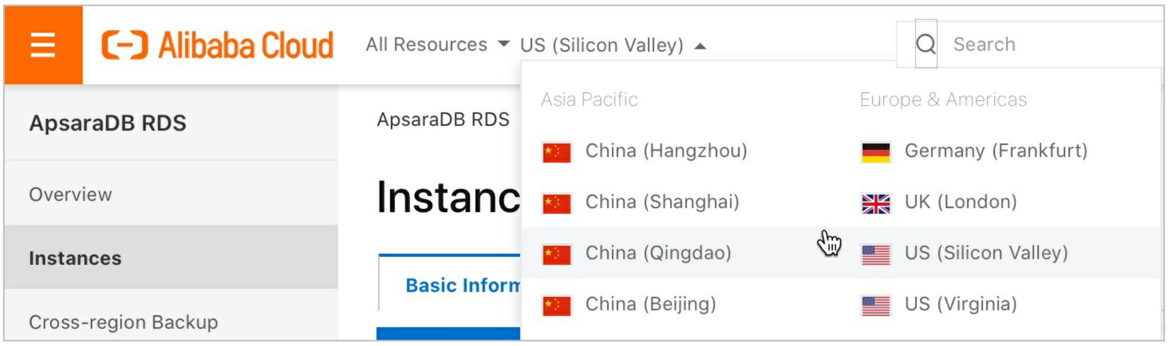
13.Monitoring and alerts

13.1. View resource monitoring data

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

Procedure

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



3. Find the target RDS instance and click the instance ID.
4. In the left-side navigation pane, click **Monitoring and Alerts**.
5. On the **Monitoring** tab, specify the time range. The following table describes the monitoring metrics.

Metric	Description
Disk Space (MB)	The disk space usage of the RDS instance. Unit: MByte.
IOPS (Input/Output Operations per Second)	The number of I/O requests to the data disk per second and the number of I/O requests to the log disk per second for the RDS instance. Unit: Number/second.
Memory Usage (%)	The memory usage of the RDS instance.
CPU Utilization (%)	The CPU usage of the RDS instance.
Total Connections	The total number of connections to the RDS instance.

13.2. Set the monitoring frequency

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

Background information

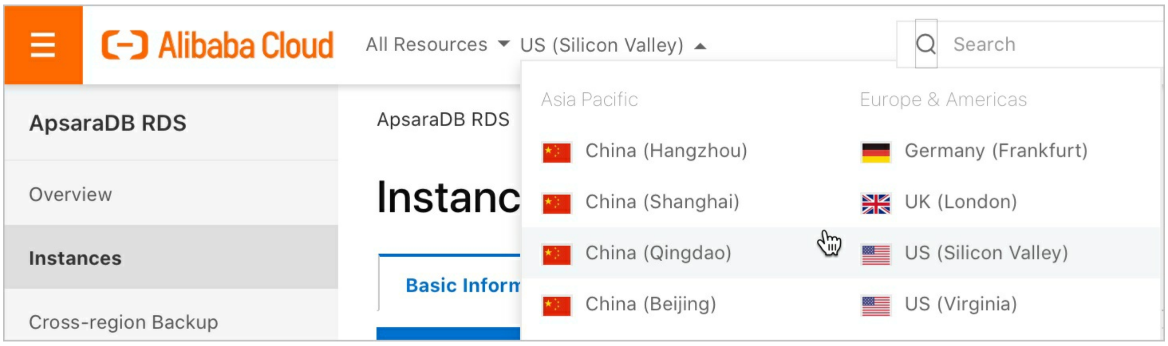
RDS PPAS supports two monitoring frequencies:

- Once per 60 seconds
- Once per 300 seconds

Note ApsaraDB RDS allows you to query the monitoring data from the last 30 days or less. You may not be able to query the monitoring data over a time range of more than 30 days.

Procedure

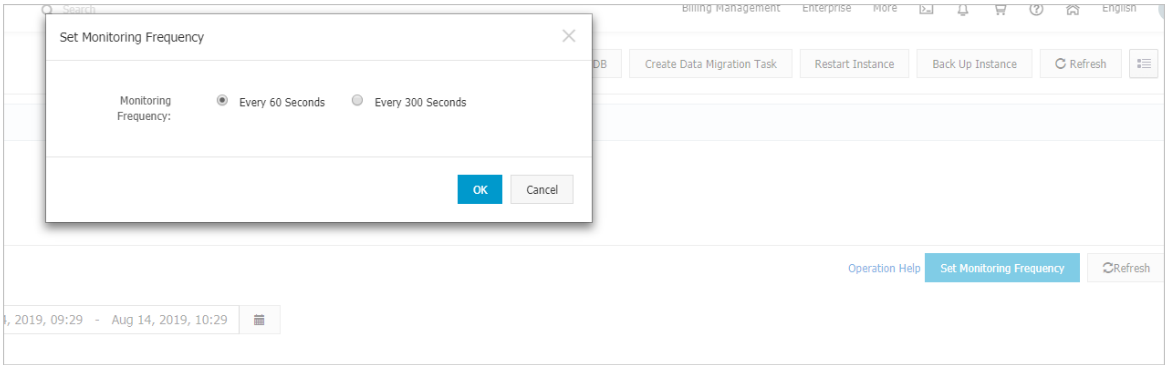
1. Log on to the RDS console.
2. In the upper-left corner, select the region where the target RDS instance is located.



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

   Note For information about the monitoring metrics supported by the instance, see View resource monitoring data.

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



Set Monitoring Frequency

Monitoring Frequency: ● Every 60 Seconds ○ Every 300 Seconds

APIs

API	Description
Query the monitoring frequency of an ApsaraDB RDS instance	Used to query the monitoring data of an RDS instance.

13.3. Configure alert rules for an ApsaraDB RDS for PPAS instance

This topic describes how to configure alert rules for an ApsaraDB RDS for PPAS instance. ApsaraDB for RDS offers the monitoring and alerting feature. If exceptions are detected in your RDS instance or if your RDS instance is locked due to low disk capacity, the system can send notifications to you.

Prerequisites

Your RDS instance resides in a region of mainland China.

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.

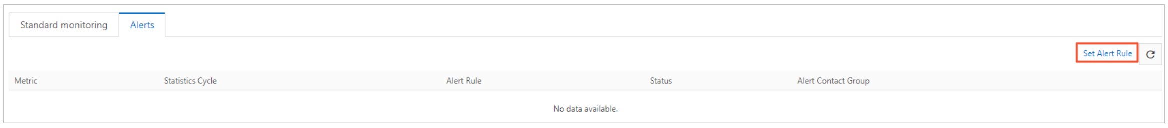
Enable the initiative alert feature

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. Visit the RDS instance list, select a region above, and click the target instance ID.
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. Visit the RDS instance list, select a region above, and click the target instance ID.
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.



Metric	Statistics Cycle	Alert Rule	Status	Alert Contact Group

No data available.

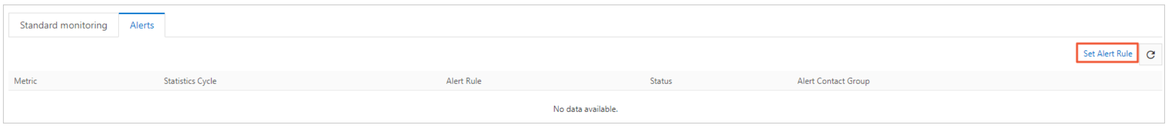
5. Create an alert group. For more information, see Create an alert contact or alert group.
6. Create an alert rule. For more information, see Create a threshold-triggered alert rule.

> **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. Visit the RDS instance list, select a region above, and click the target instance ID.
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.



Metric	Statistics Cycle	Alert Rule	Status	Alert Contact Group
No data available.				

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 a threshold-triggered 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.

14.Data security

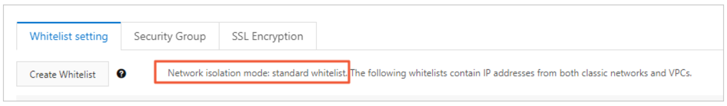
14.1. Switch an ApsaraDB RDS for PPAS instance to the enhanced whitelist mode

This topic describes how to switch an ApsaraDB RDS for PPAS instance from the standard whitelist mode to the enhanced whitelist mode. The enhanced whitelist mode offers higher security than the standard whitelist mode.

Context

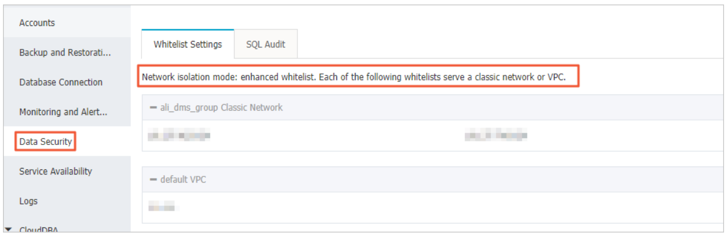
RDS instances support the following two network isolation modes:

- Standard whitelist
  IP addresses from both the classic network and virtual private clouds (VPCs) can be added to the same IP address whitelist. The standard whitelist mode is less secure than the enhanced whitelist mode. We recommend that you switch to the enhanced whitelist mode.



Network isolation mode: standard whitelist. The following whitelists contain IP addresses from both classic networks and VPCs.

- Enhanced whitelist
  IP addresses from the classic network and VPCs must be added to different IP address whitelists. When you create an IP address whitelist, you must specify its network type.



Network isolation mode: enhanced whitelist. Each of the following whitelists serve a classic network or VPC.

ali_dms_group Classic Network

[redacted] [redacted]

default VPC

[redacted]

Changes incurred

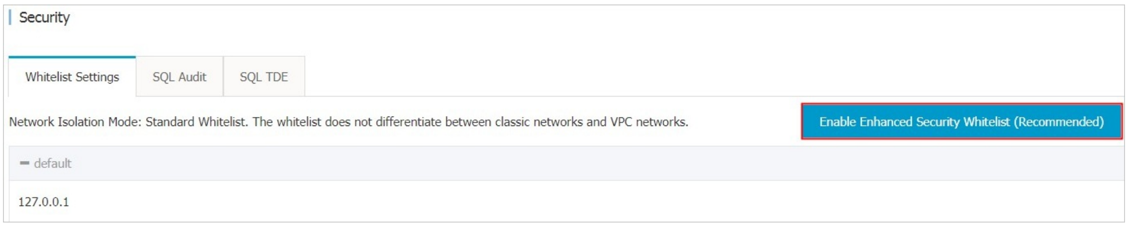
- If the RDS instance resides in a VPC, an IP address whitelist of the VPC network type is created. The new IP address whitelist contains all the IP addresses from the original IP address whitelists.
- If the RDS instance resides in the classic network, an IP address whitelist of the classic network type is created. The new IP address whitelist contains all the IP addresses from the original IP address whitelists.
- If the RDS instance runs in hybrid access mode, two IP address whitelists are created: one with the VPC network type and the other with the classic network type. Both IP address whitelists contain all the IP addresses from the original IP address whitelists.

Precautions

- After you switch to the enhanced whitelist mode, you cannot switch back to the standard whitelist mode.
- In the enhanced whitelist mode, an IP address whitelist of the classic network type can also be used to allow communication over the Internet. If you want to access the RDS instance from a host over the Internet, you can add the public IP address of the host to an IP address whitelist of the classic network type.

Procedure

1. Visit the RDS instance list, select a region above, and click the target instance ID.
2. In the left-side navigation pane, click **Data Security**.
3. On the **Whitelist Settings** tab, click **Switch to Enhanced Whitelist (Recommended)**.



Network Isolation Mode: Standard Whitelist. The whitelist does not differentiate between classic networks and VPC networks.

127.0.0.1

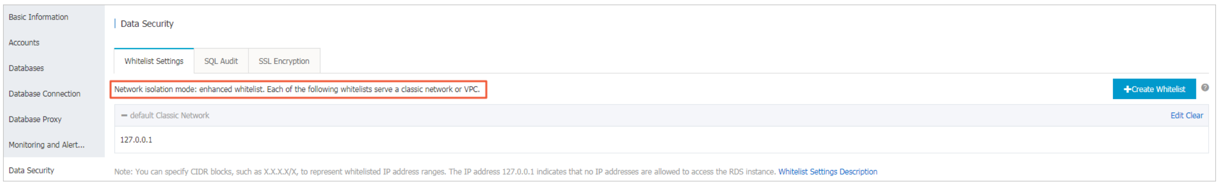
4. In the dialog box that appears, click **Confirm**.

14.2. Configure an IP address whitelist on an ApsaraDB RDS for PPAS instance

This topic describes how to configure an IP address whitelist on an ApsaraDB RDS for PPAS instance. An IP address whitelist allows only the specified external devices to access your RDS instance.
The default IP address whitelist contains only the IP address 127.0.0.1. This indicates that no devices are allowed to access the RDS instance.
The configuration of IP address whitelists provides high security for your RDS instance and does not interrupt the operation of your RDS instance. We recommend that you update the IP address whitelist regularly.

Precautions

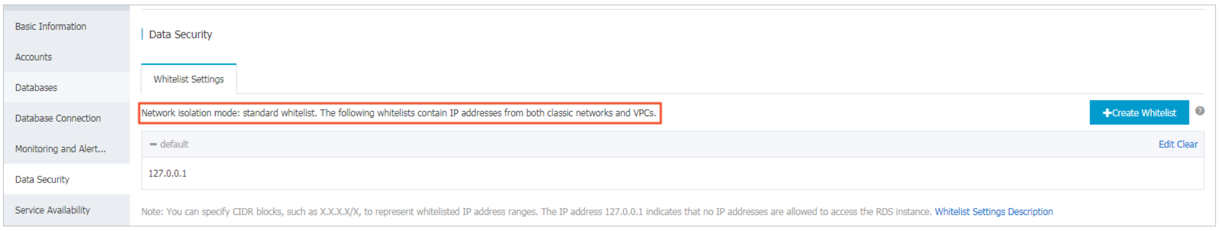
- You can edit or clear the default IP address whitelist but cannot delete it.
- You can configure up to 200 IP address whitelists per RDS instance.
- You can add up to 1,000 IP addresses and Classless Inter-Domain Routing (CIDR) blocks per IP address whitelist. If you want to add a large number of IP addresses, we recommend that you combine these IP addresses into CIDR blocks such as 192.168.1.0/24.
- If you attempt to log on to your RDS instance by using Alibaba Cloud Data Management (DMS) before you add the IP address of DMS to a whitelist of your RDS instance, DMS prompts you to add its IP address. By default, DMS creates a whitelist that contains its IP address on your RDS instance.
- You must check the network isolation mode of your RDS instance before you configure an IP address whitelist. Operations to configure an IP address whitelist vary based on the network isolation mode.



Network isolation mode: enhanced whitelist. Each of the following whitelists serve a classic network or VPC.

127.0.0.1

Note: You can specify CIDR blocks, such as X.X.X.X/X, to represent whitelisted IP address ranges. The IP address 127.0.0.1 indicates that no IP addresses are allowed to access the RDS instance. Whitelist Settings Description



Network isolation mode: standard whitelist. The following whitelists contain IP addresses from both classic networks and VPCs.

127.0.0.1

Note: You can specify CIDR blocks, such as X.X.X.X/X, to represent whitelisted IP address ranges. The IP address 127.0.0.1 indicates that no IP addresses are allowed to access the RDS instance. Whitelist Settings Description

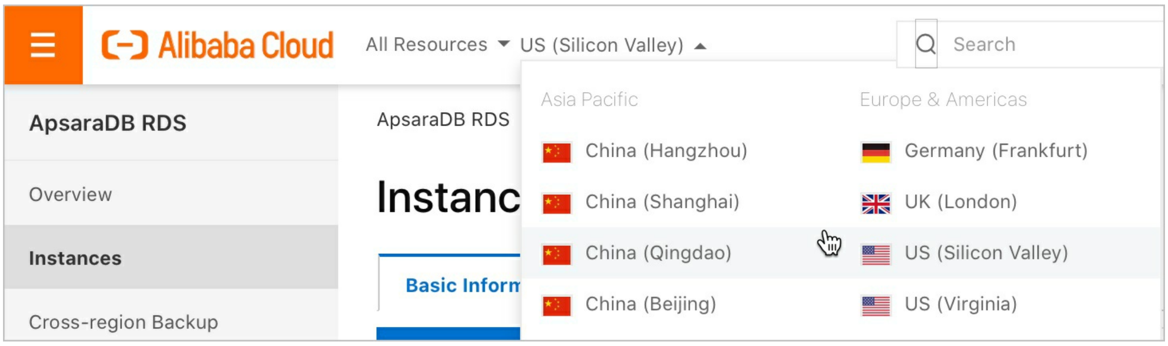
Note The internal networks to which RDS instances belong are divided into two types: classic network and VPC.

- classic network: a traditional type of network.
- VPC: A Virtual Private Cloud (VPC) is an isolated network with higher security and better performance than the classic network.

Procedure

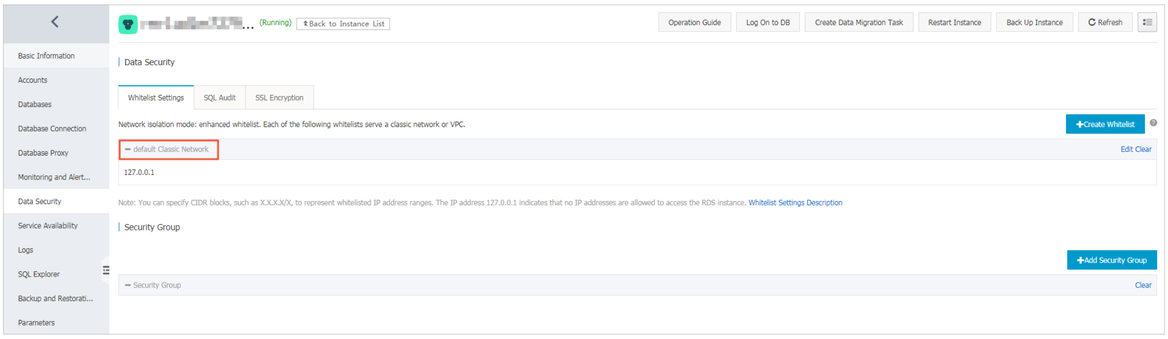
Configure an enhanced IP address whitelist

1. Log on to the ApsaraDB for RDS console.
2. In the top navigation bar, select the region where your RDS instance resides.



3. Find your RDS instance and click its ID.
4. In the left-side navigation pane, click **Data Security**.
5. On the **Whitelist Settings** tab, perform the following operations based on your access requirements:
   - Access your RDS instance from Elastic Compute Service (ECS) instances in a VPC: Click **Edit** on the right of the IP address whitelist labeled default VPC.
   - Access your RDS instance from ECS instances in the classic network: Click **Edit** on the right of the IP address whitelist labeled default Classic Network.
   - Access your RDS instance from hosts or instances over the Internet: Click **Edit** on the right of the IP address whitelist labeled default Classic Network.

   Note
   - If an ECS instance connects to your RDS instance by using the internal endpoint over a VPC or the classic network, you must make sure that the two instances are in the same region. The two instances must also have the same network type. Otherwise, the connection fails.
   - You can also click **Create Whitelist** to create an IP address whitelist. In the Create Whitelist dialog box, set Network Isolation Mode to **VPC** or **Classic Network/Public IP** based on your access requirements.



Data Security

Network isolation mode: enhanced whitelist. Each of the following whitelists serve a classic network or VPC.

default Classic Network

127.0.0.1

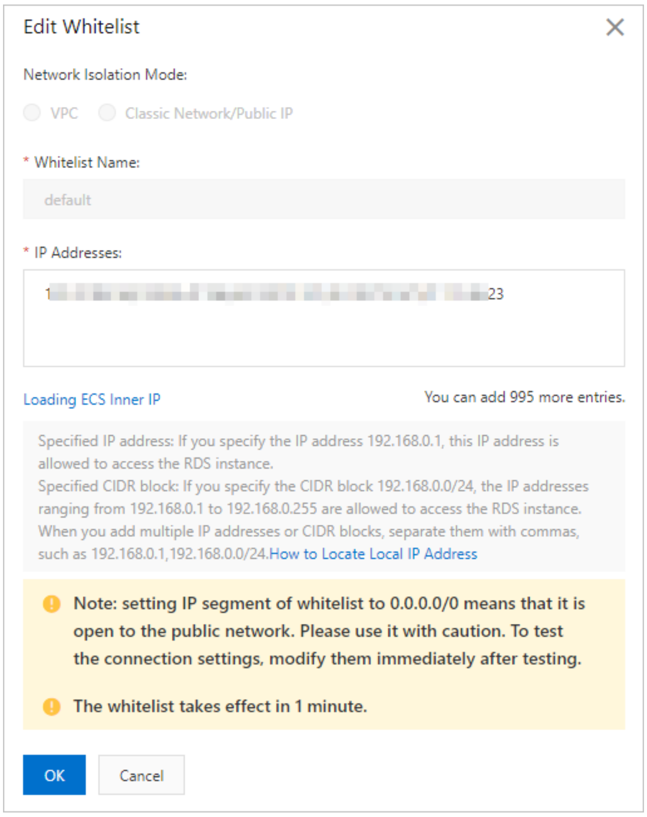
Note: You can specify CIDR blocks, such as X.X.X.X/X, to represent whitelisted IP address ranges. The IP address 127.0.0.1 indicates that no IP addresses are allowed to access the RDS instance. Whitelist Settings Description

Security Group

Security Group

6. In the Edit Whitelist dialog box, enter the IP addresses or CIDR blocks that require access to your RDS instance and click **OK**.
   - If you enter the CIDR block 10.10.10.0/24 in the IP Addresses field, all of the IP addresses in the 10.10.10.X format can access your RDS instance.
   - If you want to add more than one IP address or CIDR block, you must separate them with commas (,). Do not add spaces preceding or following the commas. Example: 192.168.0.1,172.16.213.9.
   - After you click **Add Internal IP Addresses of ECS Instances**, the IP addresses of all ECS instances under your Alibaba Cloud account are displayed. You can quickly add them to the IP address whitelist.

> **Note** After you add IP addresses or CIDR blocks to the **default** IP address whitelist, the default IP address 127.0.0.1 is automatically deleted.



Network Isolation Mode:

* Whitelist Name: default

* IP Addresses: 1[redacted]23

You can add 995 more entries.

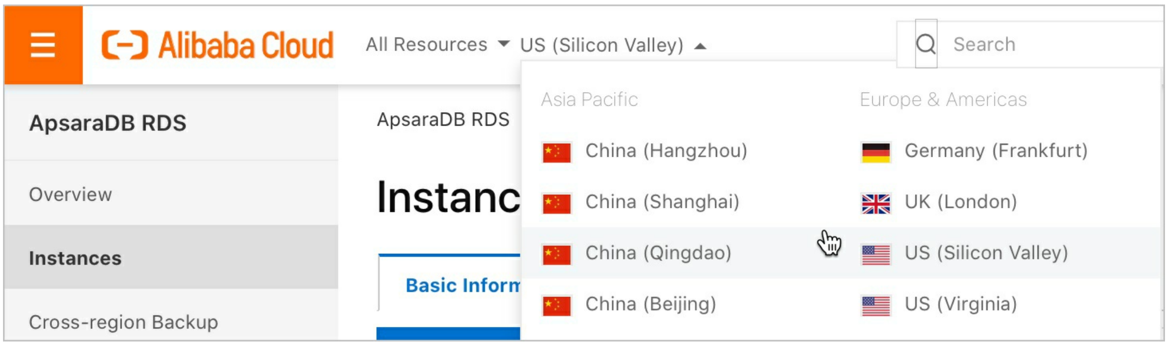
Specified IP address: If you specify the IP address 192.168.0.1, this IP address is allowed to access the RDS instance.
Specified CIDR block: If you specify the CIDR block 192.168.0.0/24, the IP addresses ranging from 192.168.0.1 to 192.168.0.255 are allowed to access the RDS instance.
When you add multiple IP addresses or CIDR blocks, separate them with commas, such as 192.168.0.1,192.168.0.0/24.How to Locate Local IP Address

Note: setting IP segment of whitelist to 0.0.0.0/0 means that it is open to the public network. Please use it with caution. To test the connection settings, modify them immediately after testing.

The whitelist takes effect in 1 minute.

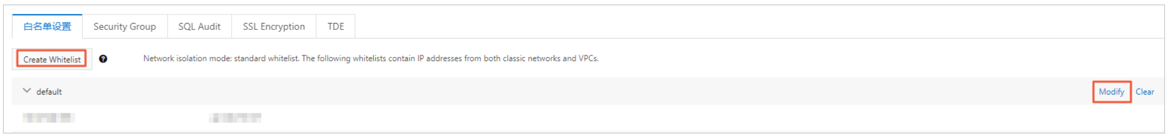
Configure a standard IP address whitelist

1. Log on to the ApsaraDB for RDS console.
2. In the top navigation bar, select the region where your RDS instance resides.



3. Find your RDS instance and click its ID.
4. In the left-side navigation pane, click **Data Security**.
5. On the **Whitelist Settings** tab of the Data Security page, click **Edit** to the right of the IP address whitelist labeled **default**.

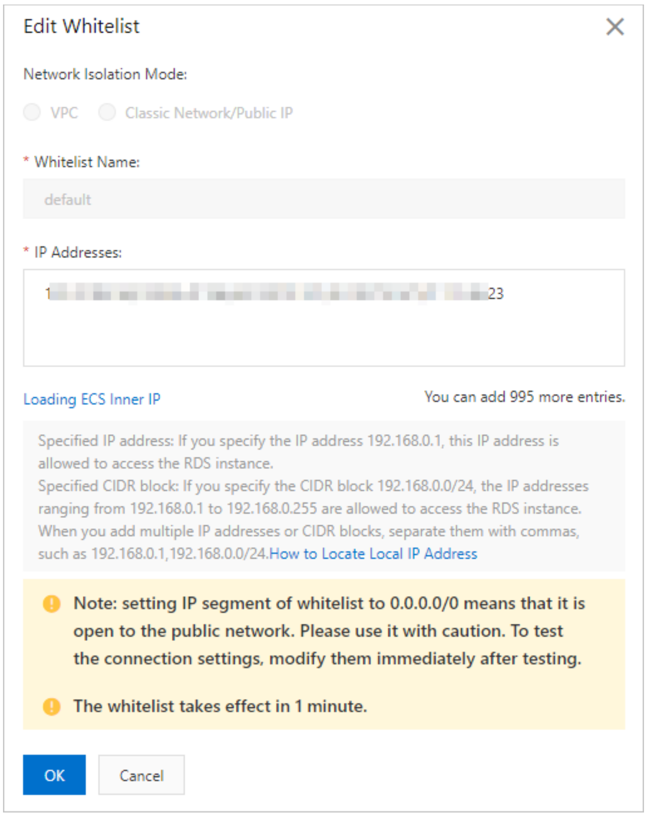
> Note You can also click **Create Whitelist** to create an IP address whitelist.



Network isolation mode: standard whitelist. The following whitelists contain IP addresses from both classic networks and VPCs.

6. In the **Edit Whitelist** dialog box, enter IP addresses or CIDR blocks in the IP Addresses field and click **OK**.
   - If you enter the CIDR block 10.10.10.0/24 in the IP Addresses field, all of the IP addresses in the 10.10.10.X format can access your RDS instance.
   - If you want to add more than one IP address or CIDR block, you must separate them with commas (,). Do not add spaces preceding or following the commas. Example: 192.168.0.1,172.16.213.9.
   - After you click **Add Internal IP Addresses of ECS Instances**, the IP addresses of all ECS instances under your Alibaba Cloud account are displayed. You can quickly add them to the IP address whitelist.

> Note After you add IP addresses or CIDR blocks to the **default** IP address whitelist, the default IP address 127.0.0.1 is automatically deleted.



Network Isolation Mode:

○ VPC ○ Classic Network/Public IP

* Whitelist Name:

default

* IP Addresses:

1[redacted]23

You can add 995 more entries.

Specified IP address: If you specify the IP address 192.168.0.1, this IP address is allowed to access the RDS instance.
Specified CIDR block: If you specify the CIDR block 192.168.0.0/24, the IP addresses ranging from 192.168.0.1 to 192.168.0.255 are allowed to access the RDS instance.
When you add multiple IP addresses or CIDR blocks, separate them with commas, such as 192.168.0.1,192.168.0.0/24.How to Locate Local IP Address

Note: setting IP segment of whitelist to 0.0.0.0/0 means that it is open to the public network. Please use it with caution. To test the connection settings, modify them immediately after testing.

The whitelist takes effect in 1 minute.

Common errors

- On the **Whitelist Settings** tab of the **Data Security** page, the IP address whitelist labeled default only contains 127.0.0.1. The default IP address 127.0.0.1 indicates that all devices are denied access. You must add the IP addresses of the devices that require access to your RDS instance to IP address whitelists.
- An IP address whitelist contains entries in the 0.0.0.0 format. However, the correct format is 0.0.0.0/0.

  > **Note** The 0.0.0.0/0 entry indicates that all devices can access your RDS instance. Exercise caution when you use this entry.

- If you use the enhanced whitelist mode, you must:
  - If your RDS instance resides in a VPC and is accessed by using its internal endpoint, make sure that the internal IP address of your ECS instance is added to the IP address whitelist labeled default VPC.
  - If your RDS instance resides in the classic network and is accessed by using its internal endpoint, make sure that the internal IP address of your ECS instance is added to the IP address whitelist labeled default Classic Network.
  - If you want to use ClassicLink to allow ECS instances to access your RDS instance, add their private IP addresses to the **default VPC** whitelist.
  - If your RDS instance resides in the classic network and is accessed over the Internet, make sure that the public IP address of your ECS instance is added to the IP address whitelist labeled default Classic Network.
- The public IP addresses that you add to an IP address whitelist are invalid. This problem may occur due to the following reasons:
  - Public IP addresses dynamically change.

- The tool or website you use to query public IP addresses returns inaccurate results.

For more information, see How do I locate the IP address connected to an RDS for PostgreSQL or RDS for PPAS instance?.

Related operations

Operation	Description
Query IP address whitelists	Queries the IP address whitelists of an ApsaraDB for RDS instance.
Modify IP address whitelist	Modifies an IP address whitelist of an ApsaraDB for RDS instance.

15.Audit

15.1. Enable and disable SQL Audit (database audit) on an ApsaraDB RDS for PPAS instance

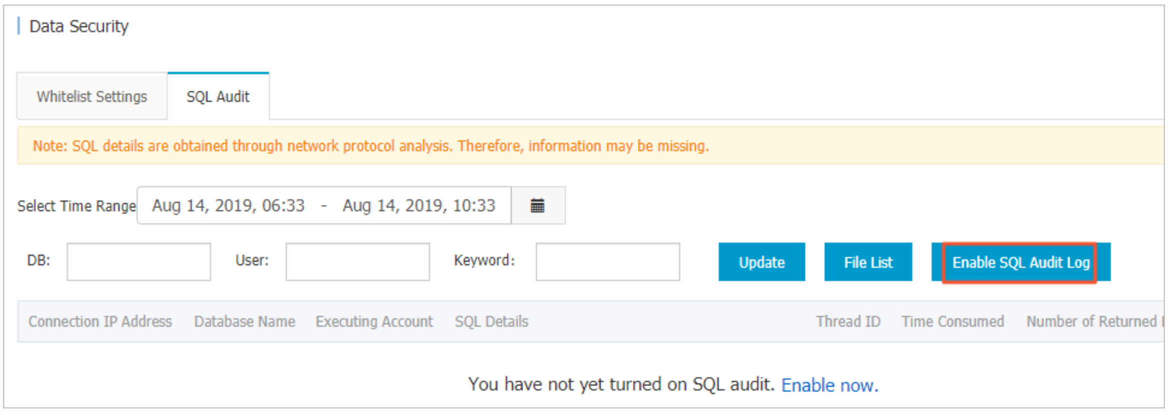
This topic describes how to enable and disable the SQL Audit feature of an ApsaraDB RDS for PPAS instance. This feature allows you to view and audit the SQL statements executed.

Precautions

- You cannot view the SQL logs that are generated before the SQL Audit feature is enabled.
- The SQL Audit feature does not compromise the performance of your RDS instance.
- The retention period of SQL logs is 30 days.
- The retention period of the SQL log files that are exported from the SQL Audit feature is two days. The system deletes the SQL log files that are stored longer than two days.
- The maximum length that the SQL Audit feature allows for an SQL statement is 2,000 bytes. The part that exceeds 2,000 bytes cannot be logged.
- The SQL Audit feature is disabled by default. After this feature is enabled, you are charged additional fees. For more information, visit the ApsaraDB for RDS product homepage.

Enable the SQL Audit feature

1.
2.
3.
4. In the left-side navigation pane, click **Data Security**.
5. On the **SQL Audit** tab, click **Enable SQL Audit**.



Note: SQL details are obtained through network protocol analysis. Therefore, information may be missing.

Select Time Range: Aug 14, 2019, 06:33 - Aug 14, 2019, 10:33

You have not yet turned on SQL audit. Enable now.

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

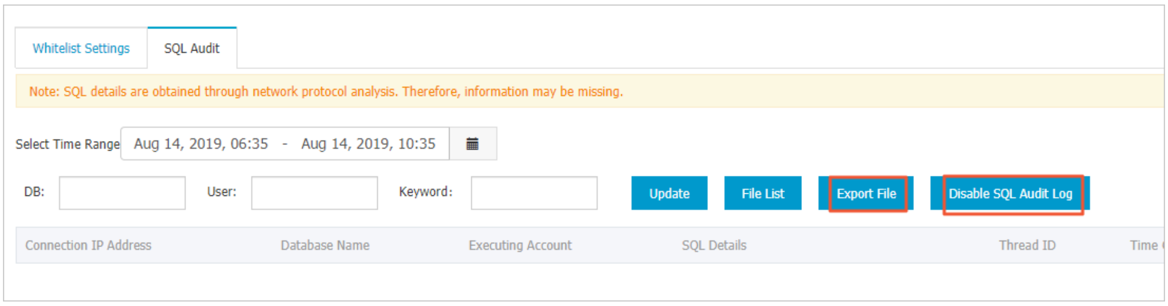
After the SQL Audit feature is enabled, you can query SQL statements based on the specified search criteria, such as the time range, databases, users, and keywords.

Disable the SQL Audit feature

If you no longer need the SQL Audit feature, you can disable it to reduce costs.

> **Note** After the SQL Audit feature is disabled, all of the SQL logs are deleted. Before you disable the SQL Audit feature, we recommend that you export the SQL logs as a file to your computer.

1.
2.
3.
4. In the left-side navigation pane, click **Data Security**.
5. On the **SQL Audit** tab, click **Export File** to export the SQL logs as a file to your computer.
6. After the file is exported, click **Disable SQL Audit**.



Note: SQL details are obtained through network protocol analysis. Therefore, information may be missing.

Select Time Range Aug 14, 2019, 06:35 - Aug 14, 2019, 10:35

7. In the message that appears, click **Confirm**.

15.2. 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 let-side navigation pane, click **Event Center**, and then select a region above.
2. Click the **Historical Events** tab.

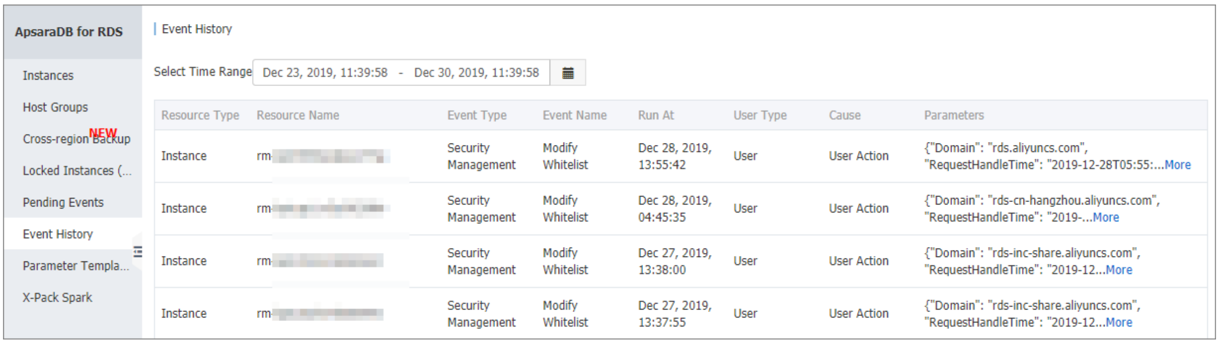
Introduction to the Historical Events page

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.
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: ● 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: ● 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 History

Select Time Range Dec 23, 2019, 11:39:58 - Dec 30, 2019, 11:39:58

Resource Type	Resource Name	Event Type	Event Name	Run At	User Type	Cause	Parameters
Instance	rm[redacted]	Security Management	Modify Whitelist	Dec 28, 2019, 13:55:42	User	User Action	{"Domain": "rds.aliyuncs.com", "RequestHandleTime": "2019-12-28T05:55:...More
Instance	rm[redacted]	Security Management	Modify Whitelist	Dec 28, 2019, 04:45:35	User	User Action	{"Domain": "rds-cn-hangzhou.aliyuncs.com", "RequestHandleTime": "2019-...More
Instance	rm[redacted]	Security Management	Modify Whitelist	Dec 27, 2019, 13:38:00	User	User Action	{"Domain": "rds-inc-share.aliyuncs.com", "RequestHandleTime": "2019-12...More
Instance	rm[redacted]	Security Management	Modify Whitelist	Dec 27, 2019, 13:37:55	User	User Action	{"Domain": "rds-inc-share.aliyuncs.com", "RequestHandleTime": "2019-12...More

Events

Event type	Operation
Instance Management	Restart Instance (RestartDBInstance)
	Renew (RenewInstance)
	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)

Event type	Operation
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)
Account Management	Create Account (CreateAccount)
	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)

Event type	Operation
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 Cloud	Restore Backup File in OSS to RDS Instance (CreateMigrateTask)
	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 events of ApsaraDB for RDS instances in a region	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.

16.Backup

16.1. Back up an ApsaraDB RDS for PPAS instance

This topic describes how to back up an ApsaraDB RDS for PPAS instance. You can specify a data and log backup cycle based on which the system automatically backs up data and logs. You can also manually back up an RDS instance.

Precautions

- Backup files occupy backup storage. Each RDS instance is allocated with a free quota for backup storage. If your backup storage usage exceeds the free quota, you must pay for the extra backup space that you use. We recommend that you specify a backup cycle based on your business requirements to maximize the usage of the free backup storage. For more information about the free quota for backup storage, see View the free quota for backup storage of an ApsaraDB RDS for PPAS instance.
- For more information about the billing methods and billing items, see Pricing, billable items, and billing methods.
- For more information about the billing standard for backup storage usage, see Pricing.
- Do not execute data definition language (DDL) statements during a backup. These statements trigger locks on tables, and the backup may fail as a result of the locks.
- We recommend that you back up your RDS instance during off-peak hours.
- If the data volume is large, backing up your RDS instance may require a long time.
- Backups are retained based on the specified retention period. We recommend that you download the backups you require to your computer before they are deleted.

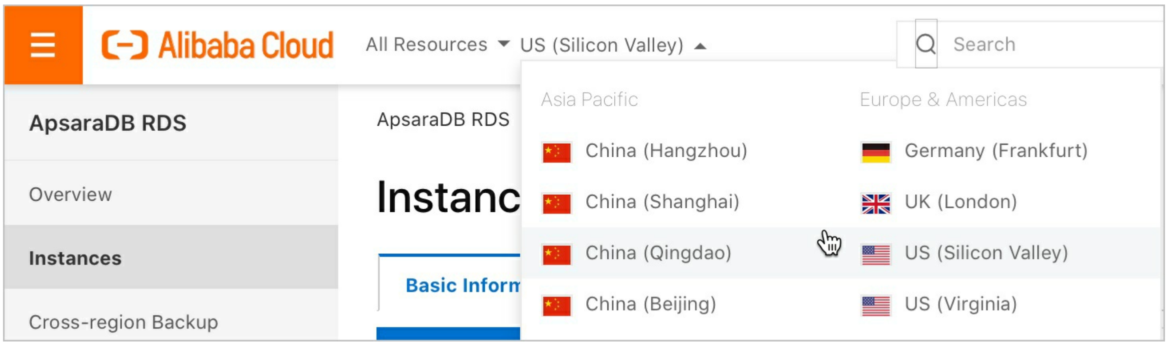
Backup types

Data backup	Log backup
You can back up the data of your RDS instance. Only physical backups are supported. The data backup files can be used to restore your RDS instance. Your RDS instance automatically perform physical backup by default. Note You can use commands to perform logical backup and restoration. For more information, see Create a logical backup and restore data from a logical backup.	You can back up the binary logs of your RDS instance. The binary log files can be used to restore your RDS instance to a point in time.

Configure a backup policy for automated backup

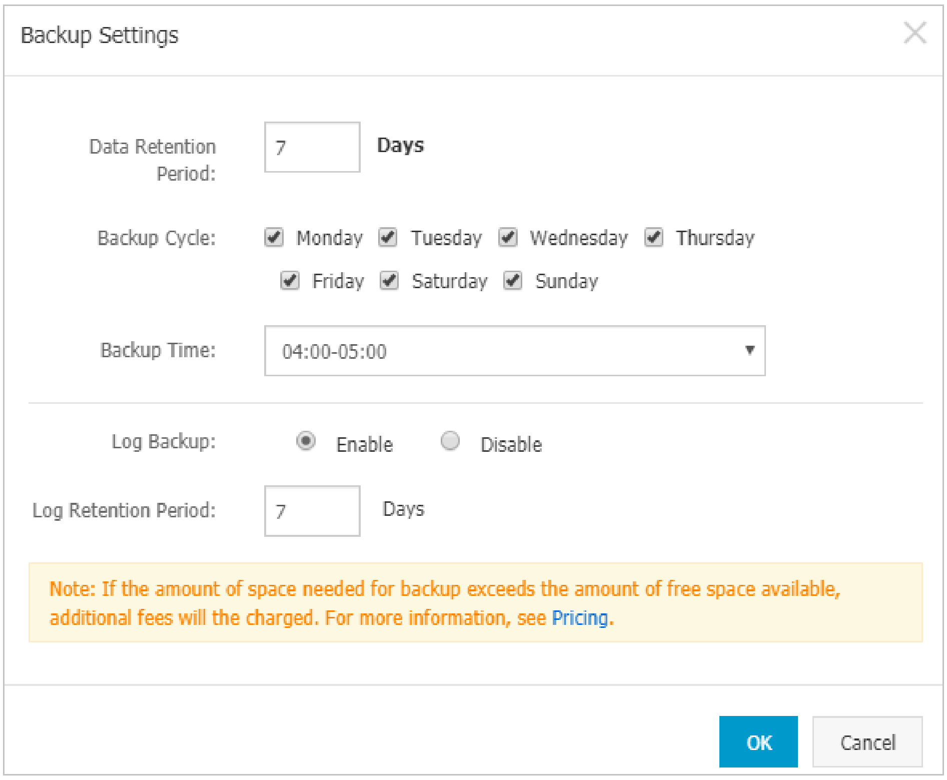
ApsaraDB for RDS automatically backs up your RDS instance based on the specified backup policy.

1. Log on to the ApsaraDB for RDS console.
2. In the top navigation bar, select the region where the target RDS instance resides.



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

Parameter	Description
Data Retention Period	You can specify 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 to create backups. You can select one or more days of a week. **Note** To ensure data security, we recommend that you back up your RDS instance at least twice a week.
Backup Time	The hour at which you want to create a backup.
Log backup	The switch to enable or disable the log backup function. **Notice** If you disable this function, all binary log files are deleted, and you cannot restore the RDS instance to a point in time.
Log Retention Period	◦ The number of days for which you want to retain binary log files. Valid values: 7 to 730. Unit: days. Default value: 7. ◦ The log retention period must be shorter than or equal to the data retention period.



Backup Settings

Data Retention Period: 7 Days

Backup Cycle: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

Backup Time: 04:00-05:00

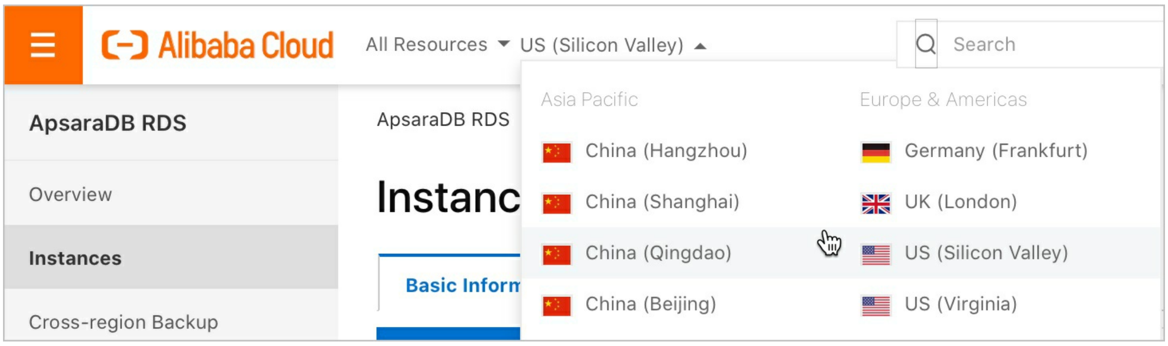
Log Backup: ● Enable ○ Disable

Log Retention Period: 7 Days

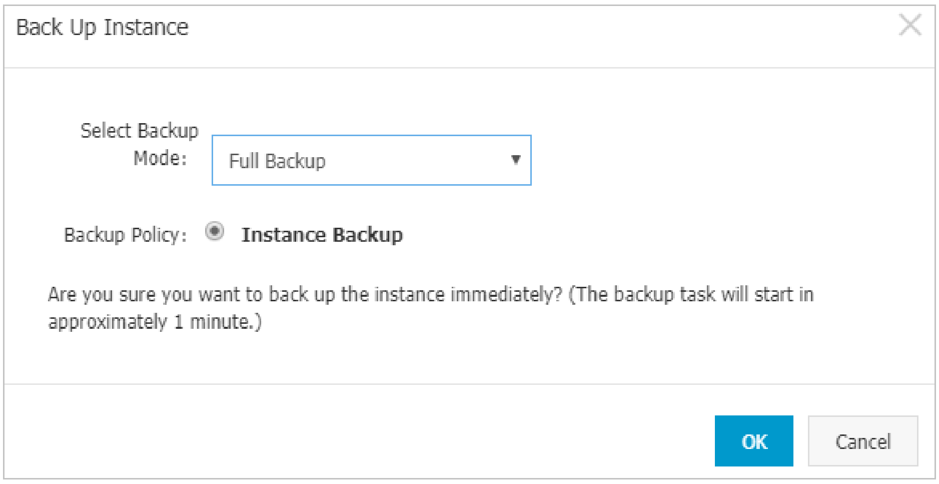
Note: If the amount of space needed for backup exceeds the amount of free space available, additional fees will the charged. For more information, see Pricing.

Back up data manually

1. Log on to the ApsaraDB for RDS console.
2. In the top navigation bar, select the region where the target RDS instance resides.



3. Find the target RDS instance and click its ID. The **Basic Information** page appears.
4. In the upper-right corner of the page, click **Back Up Instance**.



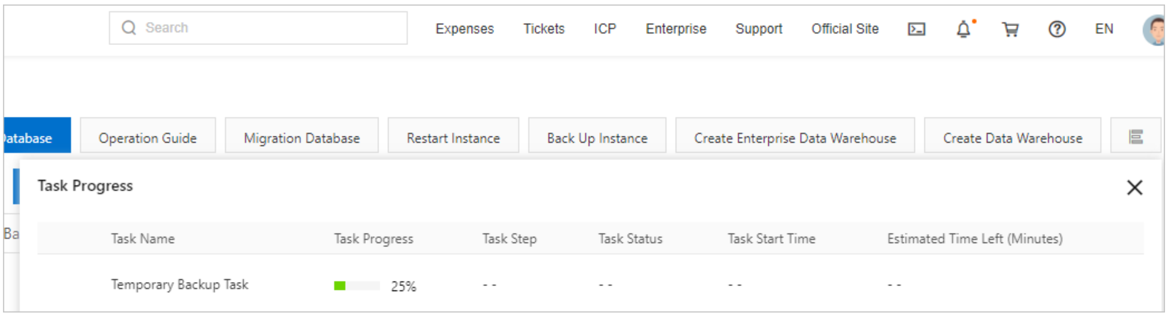
Back Up Instance

Select Backup Mode: Full Backup

Backup Policy: ● Instance Backup

Are you sure you want to back up the instance immediately? (The backup task will start in approximately 1 minute.)

5. Select a backup mode and click **Confirm**.
6. In the upper-right corner of the page, click the **Task Progress** button to view the progress of the backup task.



Task Progress

Task Name	Task Progress	Task Step	Task Status	Task Start Time	Estimated Time Left (Minutes)
Temporary Backup Task	25%	--	--	--	--

Note You cannot download backup files to your computer.

FAQ

1. Can I disable the data backup function of my RDS instance?
   No, you cannot disable the data backup function of your RDS instance. However, you can reduce the backup frequency to as low as twice a week. The data retention period must be within the range from 7 days to 730 days.
2. Can I disable the log backup function of my RDS instance?
   Yes, you can disable the data backup function of your RDS instance. You can log on to the ApsaraDB for RDS console and navigate to the Backup Settings tab to disable the log backup function of your RDS instance.

Related operations

Operation	Description
Create data backup	Creates a backup for an ApsaraDB for RDS instance.
Query data backup files	Queries the backup sets created for an ApsaraDB for RDS instance.

Operation	Description
Query backup settings	Queries the backup settings of an ApsaraDB for RDS instance.
Modify backup settings	Modifies the backup settings of an ApsaraDB for RDS instance.
Delete backup sets	Deletes one or more data backup files from an ApsaraDB for RDS instance.
Query backup tasks	Queries the backup tasks created for an ApsaraDB for RDS instance.
Query log backup files	Queries the binary log files of an ApsaraDB for RDS instance.

16.2. View the free quota for backup storage of an ApsaraDB RDS for PPAS instance

This topic describes how to view the free quota for backup storage of an ApsaraDB RDS for PPAS instance. It also provides more information about how to calculate your excess backup storage usage. The free quota can vary based on the instance configuration.

Context

Formula

The free quota that is provisioned to store backup files is calculated based on the following formula: Free quota = 50% × Storage capacity purchased during instance creation (unit: GB; rounded up to the next integer).

The excess backup storage usage for which you must pay an hourly rate is calculated based on the following formula: Excess backup storage usage = Size of data backup files + Size of log backup files - Free quota.

If the size of data backup files is 30 GB, the size of log backup files is 10 GB, and the storage capacity purchased during instance creation is 60 GB, then the excess backup storage usage for which you must pay an hourly rate is 10 GB based on the following calculation: `Excess backup storage usage = 30 + 10 - 50% × 60 = 10 (GB)` . This indicates that you must pay for an additional 10 GB of backup storage per hour.

? Note

16.3. Download the backup files of an RDS PPAS instance

This topic describes how to download the log backup files of an RDS PPAS instance. The downloaded log backup files are not encrypted.

Limits

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

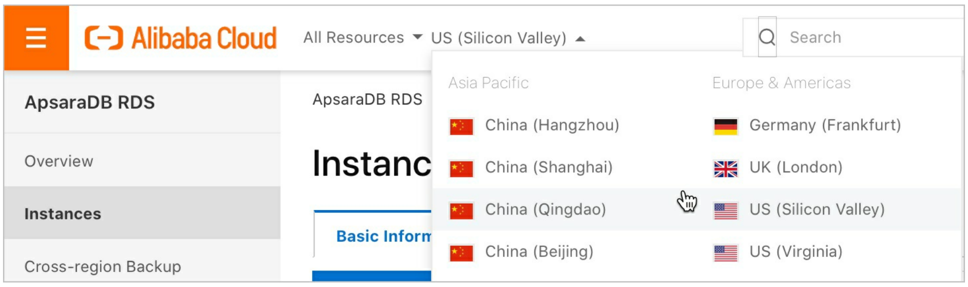
DB engine	Data backup download	Log backup download
PPAS	Not supported.	Supported by all versions.

> **Note**
> An RDS PPAS instance does not support the download of data backup files. You can restore the data of an RDS PPAS instance or migrate data from RDS PPAS to an on-premises database.

Procedure

1. Go to the **Backup and Restoration** page.

   i. Log on to the ApsaraDB for RDS console. In the left-side navigation pane, click **Instances**. In the top navigation bar, select the region where your RDS instance resides.

   ii. Find the target RDS instance and click the instance ID. In the left-side navigation pane, click **Backup and Restoration**.

2. On the **Archive List** tab, select a time range and click **Search**. In the log backup file list, find the target log backup file and in the **Actions** colum click **Download**.

   > **Note** If the log backup file is used to restore the RDS instance to an on-premises database, note the following:
   > - The Instance No. of the log backup file must the same as that of the corresponding data backup file.
   > - The start time and end time of the log backup file must be later than the selected backup time point and earlier than the time point from which you want to restore data.

3. In the **Download Instance Backup Set** or **Download Binary Log** dialog box, click .

Download method	Description
	Use a browser to download the backup file.

Download method	Description
	Copy the internal URL from which you can download the backup file. If your ECS and RDS instances reside in the same region, you can log on to the ECS instance and then use the internal URL to download the backup file. This method is faster and more secure than the other download methods.
	Copy the public URL to download the backup file. If you want to use other tools to download the backup file, select this download method.

> ? **Note** In a Linux operating system, you can run the following command to download a log backup file:
>
> ```
> wget -c '<Download URL of the log backup file>' -O <User-defined file name>.tar.gz
> ```
>
> - The -c parameter is used to enable resumable download.
> - The -O parameter is used to save the downloaded result as a file with the specified name (the file extension is .tar.gz or .xb.gz as included in the URL).
> - If you enter more than one download URL, then you must include each download URL in a pair of single quotation marks (''). Otherwise, the download fails.

16.4. Create a logical backup and restore data from a logical backup

This topic describes how to create a logical backup for your ApsaraDB RDS for PPAS instance. This topic also provides further details about how to restore data from the created logical backup.

Prerequisites

EnterpriseDB is installed on your ECS instance or on-premises server that hosts your RDS instance.

> ? **Note**
>
> - Download the EnterpriseDB software package for Windows.
> - Download the EnterpriseDB software package for Linux.

Procedure

1. Grant an account all of the permissions that are owned by the other accounts on your RDS instance. This account is used to export data.
   In this example, three accounts, User A, User B, and User C, are created on your RDS instance. Before you export data by using User A, you must run the following commands to grant the permissions of User B and User C to User A:

   ```
   -- Log on to your RDS instance by using User B and run the following command:
   grant B to A;
   -- Log on to your RDS instance by using User C and run the following command:
   grant C to A;
   ```

In this case, User A has the permissions to access all of the data tables on which User B and User C are authorized.

2. Go to the directory where pg_dump is stored and run the following command (the default directory is */usr/pgsql-10/bin/*):

```
./pg_dump -h <host> -p <port> -U <user> -f dump.sql <dbname>
```

3. To restore data, run the following commands in the directory where psql is stored (the default directory is */usr/pgsql-10/bin/*):

```
./psql  -h <host> -p <port> -U <user> -d postgres -c "drop database <dbname>"
 ./psql  -h <host> -p <port> -U <user> -d postgres -c "create database <dbname>"
 ./psql  -h <host> -p <port> -U <user> -f dump.sql -d <dbname>
```

FAQ

1. What do I do if the following permission error occurs when I export data from my RDS for PPAS instance?

```
ERROR:  permission denied for relation product_component_version
 LOCK TABLE sys.product_component_version IN ACCESS SHARE MODE
```

You are using pg_dump provided with PostgreSQL to export data from your RDS for PPAS instance. You must use PPAS binaries. For more information about how to download PPAS binaries, see the preceding steps.

2. What do I do if the following permission error occurs when I export data from my RDS for PPAS instance?

```
 ERROR:  permission denied for relation <The name of a user table>
```

The account that you use to export data does not have the permissions on the specified user table. If approved, you can grant an account all of the permissions that are owned by the other accounts on your RDS for PPAS instance. Then, run the following command by using this account:

```
GRANT ROLE <other roles>,<other roles> to <user for pg_dump>
```

3. What do I do if the following problem occurs when I run pg_dump?

```
pgdump -U xxx -h yyy -p3433 <dbname> -f my.sql
 pg_dump: A significantly large number of parameters are specified in the command line. The first para
meter is -f.
```

When you run pg_dump in a Windows operating system, you must affix the <dbname> parameter to the end of the command line.

4. What do I do if a parameter error occurs when I run pg_dump?
The parameters that you specified may be incorrect. For example, `pg_dump -Uxxx -h yyy` is not allowed. You must use a space to follow -U. This rule also applies to other parameters.

17.Restoration

17.1. Restore the data of an ApsaraDB RDS for PPAS instance

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

You can restore the data of an RDS instance from a backup set or to a point in time. You can perform the following operations to restore the data:

1. Restore data to a new RDS instance (formerly known as cloning an instance).
2. Verify the data on the new RDS instance.
3. Migrate the data to the original RDS instance.

Precautions

- The new RDS instance must have the same IP address whitelist, backup, and parameter settings as the original RDS instance.
- The data information of the new RDS instance is the same as the information indicated by the data or log backup file of the original RDS instance.
- The account information of the new RDS instance contains the data or log backup file of the original RDS instance.

Billing methods

The billing method is the same as purchasing a new RDS instance. For more information, see Pricing.

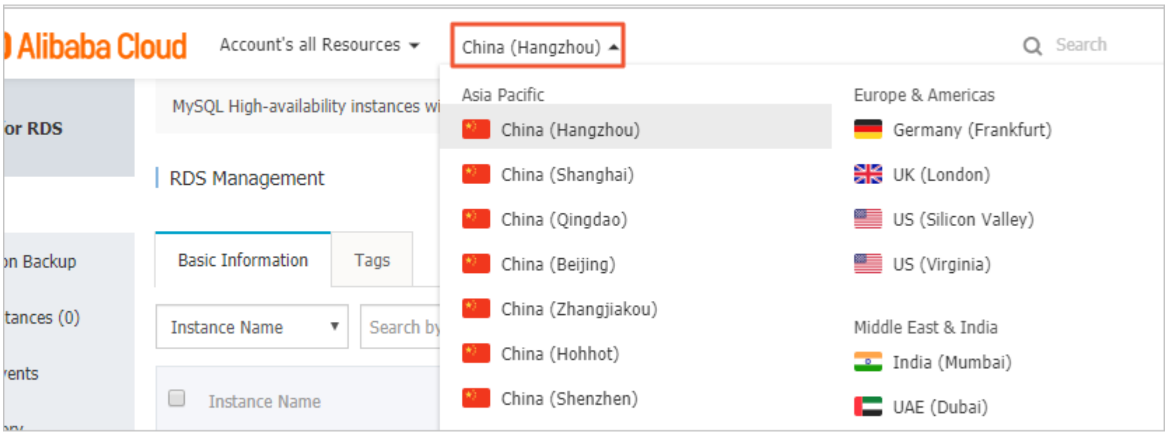
Prerequisites

The original RDS instance must meet the following requirements:

- The original RDS instance is in the Running state and is not locked.
- The original RDS instance does not have an ongoing migration task.
- If you want to restore the original RDS instance to a point in time, the log backup function is enabled for the original RDS instance.
- If you want to restore the original RDS instance from a backup set, the original RDS instance has at least one backup set.

Restore data to a new RDS instance

1. Log on to the ApsaraDB for RDS console.
2. Select the region where the original RDS instance resides.



3. Find the original RDS instance and click its ID.
4. In the left-side navigation pane, click **Backup and Restoration**.
5. In the upper-right corner of the page, click **Restore Database (Previously Clone Database)**.
6. Configure the following parameters.

Parameter	Description
Billing Method	◦ **Subscription**: You must pay the subscription fee when you create an RDS instance. We recommend that you select subscription billing for long-term use because it is more cost-effective than pay-as-you-go billing. You 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. We recommend that you select pay-as-you-go billing for short-term use. You can release your pay-as-you-go instance to reduce costs when you no longer need it.
Restore Mode	◦ **By Time**: You can restore data to a point in time within the log backup retention period. For more information about how to view or change the log backup retention period, see Back up an ApsaraDB RDS for PPAS instance. ◦ **By Backup Set** Note **By Time** is displayed only when the log backup function is enabled.
Edition	The edition of the new RDS instance. Only the **High-availability** edition is supported. In this edition, one primary instance and one secondary instance are deployed to implement high-availability. Note The RDS editions that are available vary based on the region and database engine version. For more information, see ApsaraDB for RDS edition overview.

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. Multi-zone deployment provides zone-level disaster recovery for your business. You only need to select a primary zone. The system automatically assigns a secondary zone to the new RDS instance.
Instance Type	○ **Entry-level**: belongs to the general-purpose instance family. A general-purpose instance exclusively occupies the memory and I/O resources allocated to it, but shares CPU and storage resources with other general-purpose instances that are deployed on the same server. ○ **Enterprise-level**: belongs to the dedicated instance family. A dedicated instance exclusively occupies the CPU, memory, storage, and I/O resources allocated to it. The top configuration of the dedicated instance family is the dedicated host. A dedicated host instance occupies all of the CPU, memory, storage, and I/O resources on the server where it resides. **Note** Each instance type supports a specific number of CPU cores, memory, 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 instance has available to store data files, system files, binary log files, and transaction files. The storage capacity increases in increments of 5 GB. **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.

7. Click **Next:Instance Configuration**.
8. Configure the following parameters.

Parameter	Description

Parameter	Description
Network Type	○ **Classic Network**: a traditional type of network. ○ **VPC**: A Virtual Private Cloud (VPC) is an isolated network with higher security and better performance than the classic network. If you select the VPC network type, you must also specify the **VPC** and the **VSwitch of Primary Node** parameters. **Note** The new RDS instance must have the same network type as the Elastic Compute Service (ECS) instance to which you want to connect. If both the RDS and ECS instances have the VPC network type, make sure that they reside in the same VPC. Otherwise, they cannot communicate over an internal network.
Resource Group	The resource group to which the new RDS instance belongs.

9. Click **Next: Confirm Order**.
10. Confirm the settings in the **Parameters** section, specify **Purchase Plan** and **Duration**, read and select Terms of Service, and click **Pay Now**. You only need to specify Duration when you create a subscription instance.

Verify the data on the new RDS instance

For more information, see Connect to an ApsaraDB RDS for PPAS instance.

Migrate data to the original RDS instance

After you verify data on the new RDS instance, you can migrate the data from the new RDS instance to the original RDS instance. For more information, see Migrate data between RDS instances.

Note Data migration copies data from the source RDS instance to the destination RDS instance. The migration process does not affect the source RDS instance.

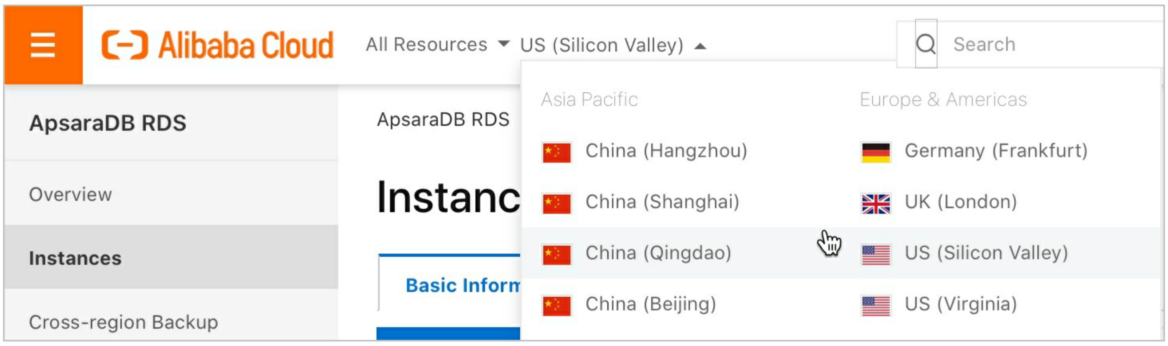
18.Manage logs

This topic describes how to manage the error logs, slow query logs, and primary/secondary instance switching logs of an ApsaraDB RDS PPAS instance through the ApsaraDB for RDS console. The logs help you locate faults. All ApsaraDB RDS PPAS instances support the log management function no matter which PPAS versions or RDS editions you choose.

Note For more information about how to archive logs, see Back up an ApsaraDB RDS for PPAS instance and Download the backup files of an RDS PPAS instance.

Procedure

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



3. Find the target RDS instance and click its ID.
4. In the left-side navigation pane, click **Logs**.
5. On the **Logs** page that appears, click the Error Log, Slow Query Log, or Primary/Secondary Instance Switching Log tab, select a time range, and click **Search**.

Tab	Description
Error Log	Records database running errors that occurred within the last month.
Slow Query Log	Records SQL statements that each took more than 1 second to run within the last month. Duplicate SQL statements are deleted.
Primary/Secondary Instance Switching Log	Records switchovers between the primary and secondary instances triggered within the last month.

Note If your ApsaraDB RDS PPAS instance resides in the China (Zhangjiakou-Beijing Winter Olympics) region, the system retains only error logs and slow query logs generated within the last nine days.

19.Tag

19.1. Create tags

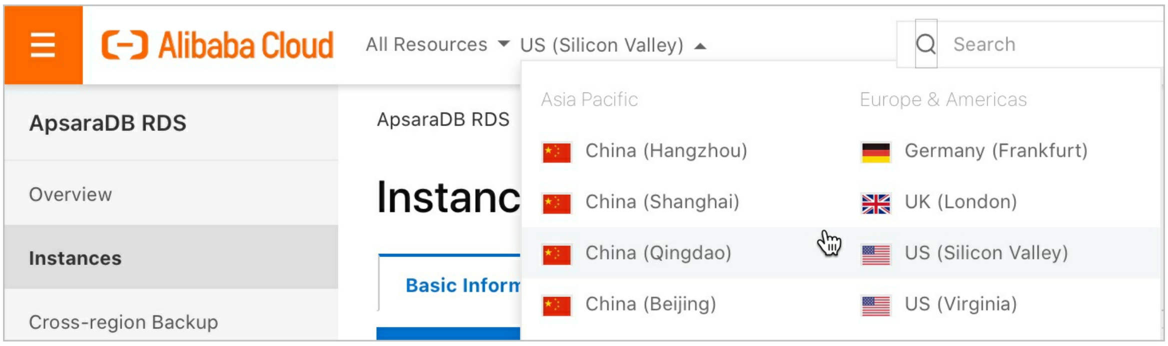
This topic describes how to create tags for one or more RDS instances. If you have a large number of RDS instances, you can create tags and then bind the tags to the instances so that you can classify and better manage the instances. Each tag consists of a key and a value.

Limits

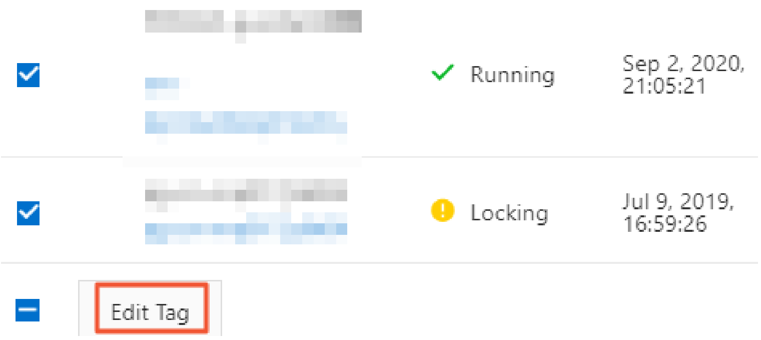
- Up to 10 tags can be bound to each RDS instance, and each tag must have a unique key. Tags with the same key are overwritten.
- You can bind up to five tags at a time.
- Tag information is independent in different regions.
- After you unbind a tag from an RDS instance, the tag is deleted if it is not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

Procedure

1. Log on to the ApsaraDB for RDS console. In the left-side navigation pane, click **Instances**. In the top navigation bar, select the region where your RDS instance resides.

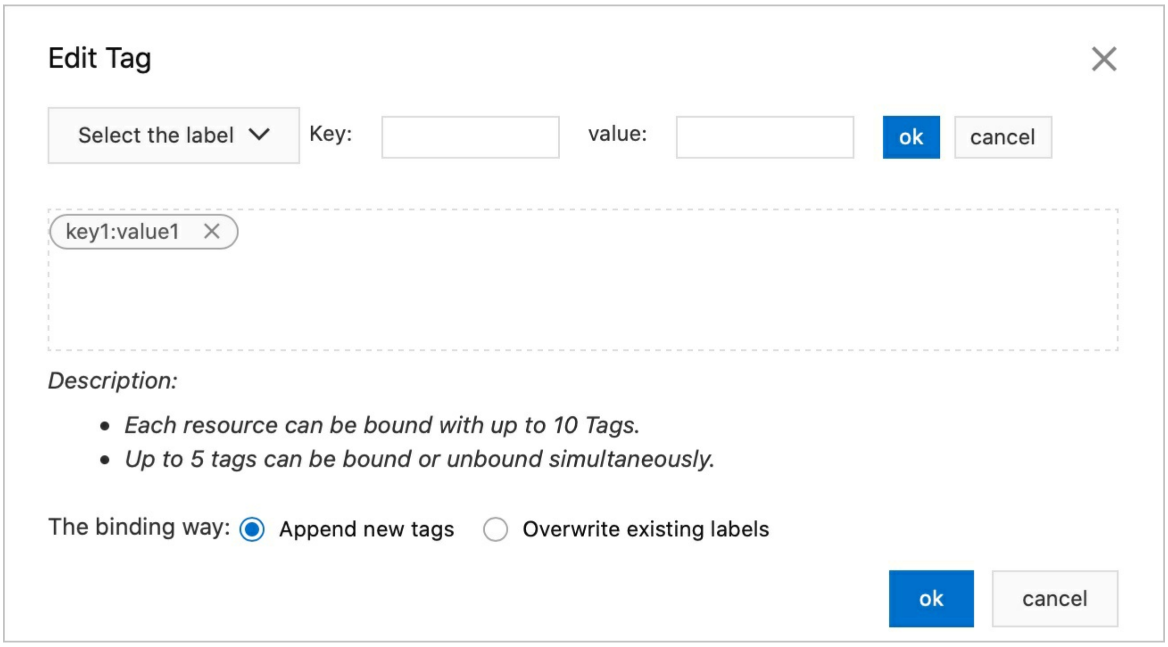


2. Specify the method of adding tags.
   - If you want to add tags to only one RDS instance, find the RDS instance and in the Actions column choose **More > Edit Tag**.
   - If you want to add tags to more than one RDS instance, select the RDS instances and click **Edit Tag**



3. Click **Add**, enter the **Key** and **Value**, and click **Confirm**.

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



Edit Tag

Select the label Key: value: ok cancel

key1:value1

Description:

- *Each resource can be bound with up to 10 Tags.*
- *Up to 5 tags can be bound or unbound simultaneously.*

The binding way: ● Append new tags ○ Overwrite existing labels

4. After you add all the tags you need, click **Confirm**.

APIs

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

19.2. Unbind tags from an ApsaraDB RDS for MySQL instance

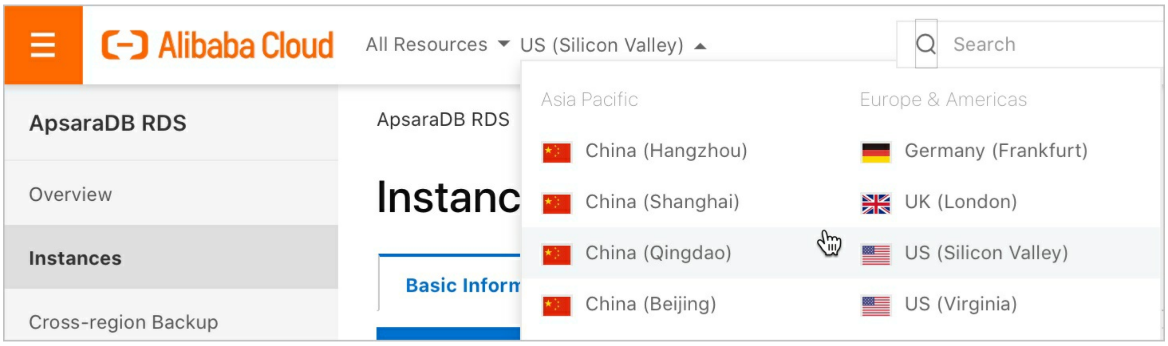
This topic describes how to unbind tags from an ApsaraDB RDS for MySQL instance. You may need to unbind tags due to instance configuration adjustments or if these tags are no longer needed.

Limits

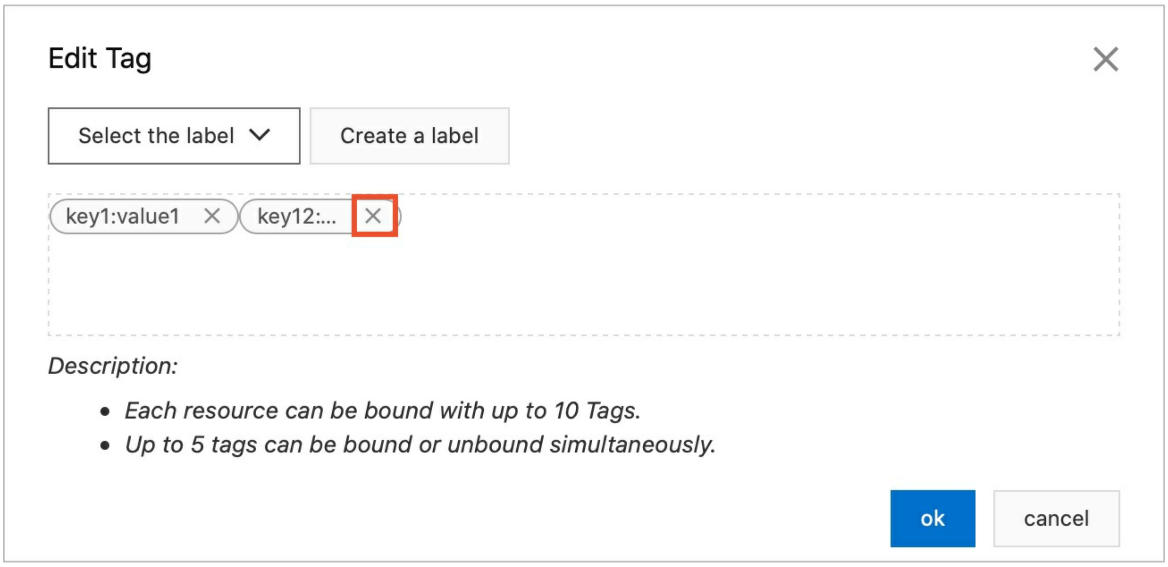
- You can unbind a maximum of 20 tags at a time.
- After you unbind a tag from an RDS instance, ApsaraDB RDS checks whether the tag is bound to any other RDS instance. If the tag is not bound to any other RDS instance, ApsaraDB RDS deletes the tag.

Procedure

1. Log on to the ApsaraDB for 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 in the Actions column choose **More > Edit Tag**.
3. In the dialog box that appears, click the **X** icon next to each tag that you want to unbind.



Description:

- *Each resource can be bound with up to 10 Tags.*
- *Up to 5 tags can be bound or unbound simultaneously.*

4. Click **OK**.

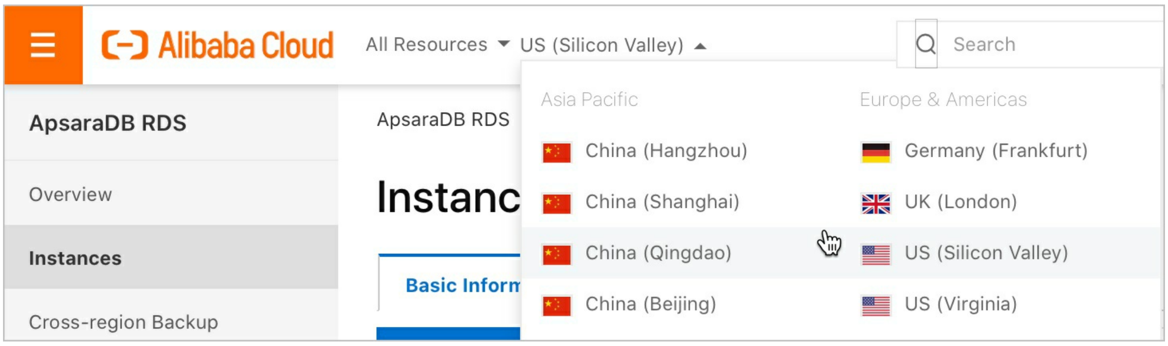
Related operations

Operation	Description
Unbind tags	Unbinds tags from one or more ApsaraDB RDS instances.

19.3. Filter RDS instances by tag

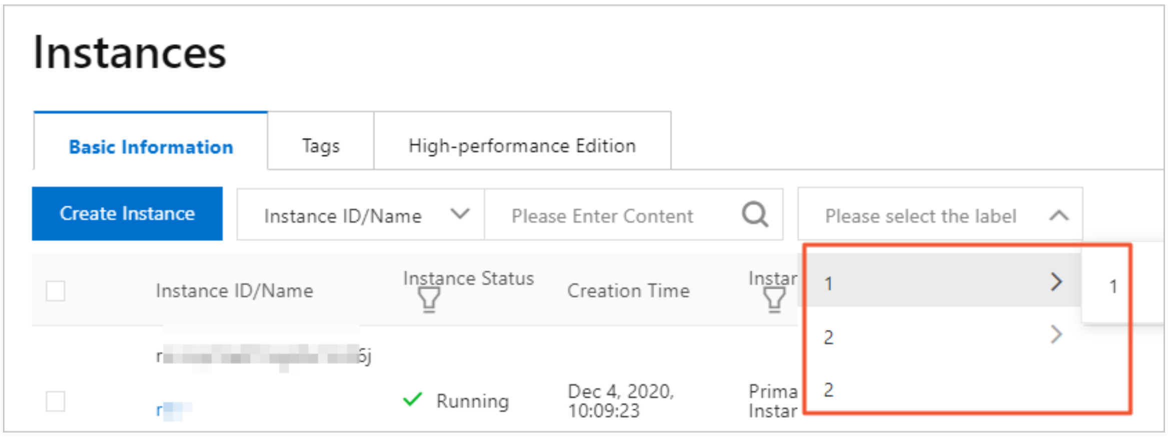
This topic describes how to filter RDS instances by tag.

1. Log on to the ApsaraDB for RDS console. In the left-side navigation pane, click **Instances**. In the top navigation bar, select the region where your RDS instance resides.



2. On the **Basic Information** tab, click the **Tag** button next to **Search** and select a tag key and a tag value.

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



APIs

API	Description
DescribeTags	Used to query tags.

20.Plug-ins

20.1. Plug-ins supported

This topic lists the plug-ins supported by ApsaraDB RDS for PPAS and their versions.

PPAS 10

Plug-in	Version
address_standardizer	2.4.1
address_standardizer_data_us	2.4.1
adminpack	1.1
ali_decoding	0.0.1
amcheck	1
autoinc	1
bloom	1
btree_gin	1.2
btree_gist	1.5
chkpass	1
citext	1.4
cube	1.2
dblink	1.2
dbms_scheduler	1
dict_int	1
dict_xsyn	1
earthdistance	1.1
edb_dblink_libpq	1
edb_dblink_oci	1
edb_sharedplancache	1
edbspl	1
file_fdw	1

Plug-in	Version
fuzzystrmatch	1.1
hstore	1.4
insert_username	1
intagg	1.1
intarray	1.2
isn	1.1
lo	1.1
ltree	1.1
moddatetime	1
oss_fdw	1.1
pageinspect	1.6
parallel_clone	1.5
pg_buffercache	1.3
pg_concurrency_control	1
pg_freespacemap	1.2
pg_jieba	1
pg_prewarm	1.2
pg_scws	1
pg_stat_statements	1.6
pg_trgm	1.3
pg_visibility	1.2
pgcrypto	1.3
pgrowlocks	1.2
pgstattuple	1.5
pldbgapi	1.1
plpgsql	1

Plug-in	Version
postgis	2.4.1
postgis_tiger_geocoder	2.4.1
postgis_topology	2.4.1
postgres_fdw	1
refint	1
seg	1.1
smlar	1
sslinfo	1.2
sslutils	1.2
tablefunc	1
tcn	1
timetravel	1
tsm_system_rows	1
tsm_system_time	1
unaccent	1.1
uuid-ossp	1.1
xml2	1.1

PPAS 9.3

Plug-in	Version
adminpack	1
autoinc	1
btree_gin	1
btree_gist	1
chkpass	1
citext	1
cube	1

Plug-in	Version
dblink	1.1
dbms_scheduler	1
dict_int	1
dict_xsyn	1
earthdistance	1
edb_dblink_libpq	1
edb_dblink_oci	1
edbspl	1
file_fdw	1
fuzzystrmatch	1
hstore	1.2
insert_username	1
intagg	1
intarray	1
isn	1
lo	1
ltree	1
moddatetime	1
oss_fdw	1
pageinspect	1.1
pg_buffercache	1
pg_freespacemap	1
pg_jieba	1
pg_reorg	1.1.13
pg_stat_statements	1.1
pg_trgm	1.1

Plug-in	Version
pgagent	1
pgcrypto	1
pgpool_recovery	1
pgpool_regclass	1
pgrowlocks	1.1
pgstattuple	1.1
pldbgapi	1.1
plpgsql	1
plpython3u	1
pltcl	1
pltclu	1
postgis	2.1.0
postgis_tiger_geocoder	2.1.4
postgis_topology	2.1.0
postgres_fdw	1
refint	1
seg	1
sslinfo	1
sslutils	1.2
tablefunc	1
tcn	1
test_parser	1
timetravel	1
tsearch2	1
unaccent	1
uuid-ossp	1

Plug-in	Version
www_fdw	0.1.8
xml2	1

20.2. Read and write external data files by using the oss_fdw plugin

This topic describes how to read and write external data files by using the oss_fdw plugin. In Alibaba Cloud, you can use this plugin to load data from OSS to an RDS PostgreSQL or RDS PPAS instance. You can also write data from an RDS PostgreSQL or RDS PPAS instance to OSS.

Prerequisites

The RDS instance runs PPAS 10.

oss_fdw example

```
# Create a plugin for apsaradb RDS for PPAS
select rds_manage_extension('create','oss_fdw');
# Create a server
CREATE SERVER ossserver FOREIGN DATA WRAPPER oss_fdw OPTIONS
   (host 'oss-cn-hangzhou.aliyuncs.com', id 'xxx', key 'xxx', bucket 'mybucket');
# Create an oss external table.
CREATE FOREIGN TABLE ossexample
   (date text, time text, open float,
   high float, low float, volume int)
   SERVER ossserver
   OPTIONS ( filepath 'osstest/example.csv', delimiter ',' ,
     format 'csv', encoding 'utf8', PARSE_ERRORS '100');
# Create a table for which data is loaded.
create table example
     (date text, time text, open float,
     high float, low float, volume int)
# Load data from ossexample to example.
insert into example select * from ossexample;
# oss_fdw estimates the file size in oss and formulates a query plan correctly.
explain insert into example select * from ossexample;
                  QUERY PLAN
---------------------------------------------------------------------
 Insert on example (cost=0.00..1.60 rows=6 width=92)
  -> Foreign Scan on ossexample (cost=0.00..1.60 rows=6 width=92)
     Foreign OssFile: osstest/example.csv.0
     Foreign OssFile Size: 728
(4 rows)
# Write the data in the example table to OSS.
insert into ossexample select * from example;
explain insert into ossexample select * from example;
                 QUERY PLAN
-----------------------------------------------------------------
 Insert on ossexample (cost=0.00..16.60 rows=660 width=92)
  -> Seq Scan on example (cost=0.00..16.60 rows=660 width=92)
(2 rows)
```

For a description of the parameters, see the following section.

oss_fdw parameters

The oss_fdw plug-in uses a method similar to other Foreign Data Wrapper (FDW) interfaces to encapsulate external data stored in OSS. You can use oss_fdw to read data stored in OSS. This process is similar to reading data tables. oss_fdw provides unique parameters to connect and parse file data in OSS.

> Note
>
> - Currently, oss_fdw can read and write files in text, csv, or gzip format.
> - The value of each parameter must be enclosed in double quotation marks (") and cannot contain any unnecessary spaces.

CREATE SERVER parameters

Parameter	Description
ossendpoint	Is the address used to access OSS from the intranet, also known as the host.
id oss	The id of the account.
key oss	The account key.
bucket	Bucket, you need to create an OSS account before configuring this parameter.

The following fault tolerance parameters can be used for data import and export. If network connectivity is poor, you can adjust these parameters to ensure successful import and export.

Parameter	Description
oss_connect_timeout	The connection timeout period. Unit: seconds. Default value: 10.
oss_dns_cache_timeout	The DNS timeout period. Unit: seconds. Default value: 60.
oss_speed_limit	The minimum allowed rate. Default value: 1024, that is, 1 kB.
oss_speed_time	The maximum time when the minimum transmission rate is tolerated. Default value: 15. Unit: seconds.

Note If the default values of oss_speed_limit and oss_speed_time are used, a timeout error occurs when the transmission rate is smaller than 1 Kbit/s for 15 consecutive seconds.

CREATE FOREIGN TABLE parameters

Parameter	Description
filepath	The name of the file that contains a path in OSS. ● A file name contains a path but not a bucket name. ● This parameter matches multiple files in the corresponding path in OSS. You can load multiple files to a database. ● You can import files named in the format of filepath or filepath.x to a database. The values of x must be consecutive numbers starting from 1. For example, among the files named filepath, filepath.1, filepath.2, filepath.3, and filepath.5, the first four files are matched and imported. The filepath.5 file is not imported.
dir	The virtual file directory in OSS. ● dir must end with (/). ● All files (excluding subfolders and files in subfolders) in the virtual file directory specified by dir will be matched and imported to a database.
Prefix	The prefix of the path name corresponding to the data file. The prefix does not support regular expressions. Only one parameter among prefix, filepath, and dir can be specified at a time because they are mutually exclusive.

Parameter	Description
format	Specifies the file format. Currently, only the csv format is supported.
encoding	The encoding format of data in the file. It supports common PostgreSQL encoding formats, such as UTF-8.
parse_errors	The fault-tolerant parsing mode ignores the errors that occur during the parsing process.
delimiter	Specifies the column delimiter.
quote	Specifies the reference character for the file.
escape	Specifies the escape character for the file.
null	Specifies that a column matching a specified string is null. For example, null 'test' indicates that the string whose column value is 'test' is null.
force_not_null	The column values are not null. For example, force_not_null 'id' is used to set the value of the 'id' column to empty strings.
compressiontype	The formats of the files to be read and written in OSS. ● none: uncompressed text files. This is the default value. ● gzip: The files to be read must be gzip compressed.
compressionlevel	The compression level of compression format written to OSS. Valid values: 1 to 9. Default value: 6.

Note

- You must specify filepath and dir in the OPTIONS parameter.
- You must specify either filepath or dir.
- The export mode only supports virtual folders, that is, only dir is supported.

Export mode parameters for CREATE FOREIGN TABLE

- oss_flush_block_size: the buffer size for the data written to OSS at a time. Default value: 32 MB. Valid values: 1 MB to 128 MB.
- oss_file_max_size: the maximum file size for the data written to OSS (subsequent data is written in another file when the maximum file size is exceeded). Default value: 1024 MB. Valid values: 8 MB to 4000 MB.
- num_parallel_worker: the number of parallel compression threads in which the OSS data is written. Valid values: 1 to 8. Default value: 3.

Auxiliary functions

FUNCTION oss_fdw_list_file (relname text, schema text DEFAULT 'public')

- Obtains the name and size of the OSS file that an external table matches.
- The unit of file size is Byte.

```
select * from oss_fdw_list_file('t_oss');
          name           |  size
--------------------------------+-----------
 oss_test/test.gz.1 | 739698350
 oss_test/test.gz.2 | 739413041
 oss_test/test.gz.3 | 739562048
(3 rows)
```

Auxiliary features

oss_fdw.rds_read_one_file: In read mode, it is used to specify a file to match the external table. If the file is specified, the external table only matches this file during data import.

Example: set oss_fdw.rds_read_one_file = 'oss_test/example16.csv.1';

```
set oss_fdw.rds_read_one_file = 'oss_test/test.gz.2';
select * from oss_fdw_list_file('t_oss');
          name           |  size
--------------------------------+-----------
  oss_test/test.gz.2 | 739413041
(1 rows)
```

oss_fdw notes

- oss_fdw is an external table plug-in developed based on the PostgreSQL FOREIGN TABLE framework.
- The data import performance is related to the CPU IO MEM MET of PPAS instances and OSS.
- To guarantee that data is correctly imported, you need to make sure that the Region of the DTS server is the same as that of the OSS server. For more information, see OSS endpoint information.
- If the SQL of the external table is read, `ERROR: oss endpoint userendpoint not in aliyun white list` , we recommend that you use the endpoint shared by Alibaba Cloud in each zone. For more information, see Regions and endpoints. If the problem persists, submit a ticket.

Error handling

When an import or export error occurs, the log displays the following error information:

- code: the HTTP status code of the request that has failed.
- error_code: the error code returned by OSS.
- error_msg: the error message returned by OSS.
- req_id: the UUID that identifies the request. If you cannot solve the problem, you can seek help from OSS development engineers by providing the req_id.

For more information about error types, see the following topics. Timeout errors can be handled by using oss_ext parameters.

- Object Storage Service
- PostgreSQL CREATE FOREIGN TABLE manual
- OSS error handling
- OSS error response

ID and key encryption

If id and key parameters for CREATE SERVER are not encrypted, executing the `select * from pg_foreign_server` statement will display the information in plaintext. Your ID and key will be exposed. The symmetric encryption can be performed on the id and key to hide the id and key. (different instances use different keys to maximize the protection of user information.) however, you cannot use methods like GP to add a data type.

The encrypted information is as follows:

```
postgres=# select * from pg_foreign_server ;
  srvname  | srvowner | srvfdw | srvtype | srvversion | srvacl |                                        srvoptions
-----------+----------+--------+---------+------------+--------+--------------------------------------------------------------------------------
----------------------------------------------------
----------------------------------
 ossserver |       10 |  16390 |         |            |        | {host=oss-cn-hangzhou-zmf.aliyuncs.com,id=MD5xxxxxxxx,key=MD
5xxxxxxxx,bucket=067862}
```

The encrypted information is preceded by MD5 (total length: len,len%8==3). Therefore, encryption is not performed again when the exported data is imported. But you cannot create the key and id preceded by MD5.

21.PPAS development driver

The RDS PPAS development driver provides diverse driver interfaces for application development:

- Linux versions: Java, OCI, and ODBC
- Windows versions: .Net, Java, OCI, and ODBC

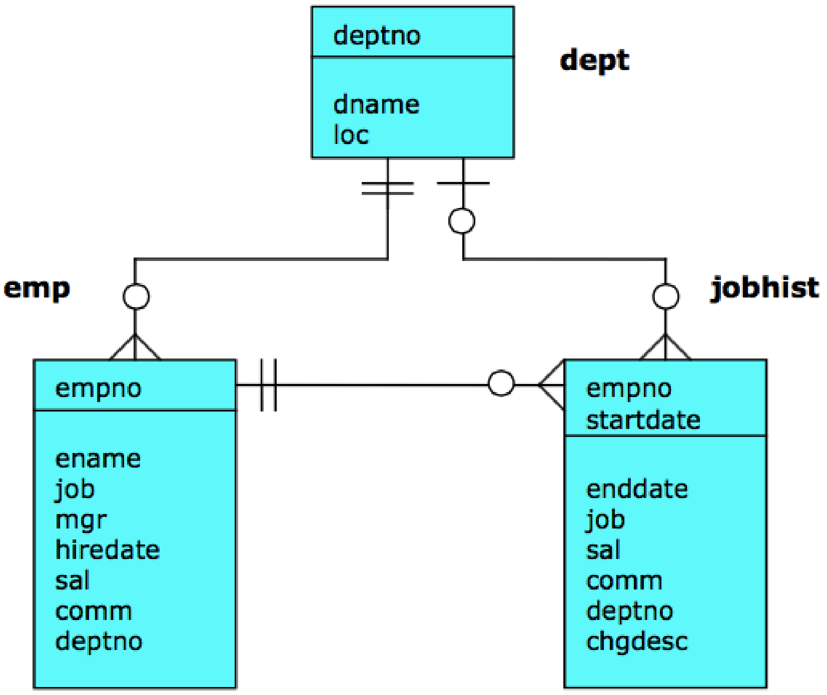
Download the PPAS development driver.

- The development driver consists of the following files:
  - edb_connectors-9.3.5.14-3-linux-x64.run
  - edb_connectors-9.3.5.14-3-linux.run
  - edb_connectors-9.3.5.14-3-windows-x64.exe
  - edb_connectors-9.3.5.14-3-windows.exe
- Default path for driver installation:
  - Linux: */opt/PostgresPlus/9.3AS/connectors*
  - Windows: *C:/Program Files/PostgresPlus/9.3AS/connectors*

22.Appendix: PPAS compatibility description

This topic provides examples to help Oracle users quickly understand the glossary and concepts used in the PPAS database and improve the efficiency of data migration and development.
The examples described in this document enable Oracle users to quickly understand glossary and concepts used in the PPAS database, and to improve the efficiency during data migration and development.

All of the following operations are based on a basic model. In this model, users can see the most basic operations used in RDS PPAS, for example, creating databases and data tables and managing accounts. The basic data model is shown as follows:



In addition, we create a database called orcl_ppas to simulate an environment similar to Oracle. In this database, we create a role named scott and a schema user space with the same name as this role.

Prerequisites

EnterpriseDB is installed on the local host or ECS.

Note

- Download EnterpriseDB for windows
- Download EnterpriseDB for Linux

Connect to database psql

```
psql -h ppasaddress.ppas.rds.aliyuncs.com -p 3433 -U myuser -d template1
 myuser password:
 psql.bin (9.4.1.3, server 9.3.5.14)
 Input "help" to obtain help information.
 template1=>
```

CREATE DATABASE

```
template1=> CREATE DATABASE orcl_ppas;
 CREATE DATABASE
 template1=> \c orcl_ppas
 psql.bin (9.4.1.3, server 9.3.5.14)
```

CREATE ROLE

```
orcl_ppas=> CREATE ROLE scott LOGIN PASSWORD 'scott123';
CREATE ROLE
```

CREATE SCHEMA

```
orcl_ppas=> CREATE SCHEMA scott;
CREATE SCHEMA
orcl_ppas=> GRANT scott TO myuser;
GRANT ROLE
orcl_ppas=> ALTER SCHEMA scott OWNER TO scott;
ALTER SCHEMA
orcl_ppas=> REVOKE scott FROM myuser;
REVOKE ROLE
```

Note

- If `cott` is not added to the `myuser` role before execution of `ALTER SCHEMA scott OWNER TO scott`, the following permission error is displayed:

  ```
  ERROR:must be member of role "scott"
  ```

- For security purpose, remove `cott` from the `myuser` role after authorization of `OWNER`.

Connect to the orcl_ppas database

Note This step is important. All of the following operations must be performed using the scott account. Otherwise, all the created data tables and various databases do not belong to the scott role and a permission error occurs.

```
[root@localhost bin]# ./psql -h ppasaddress.ppas.rds.aliyuncs.com -p 3433 -U scott -d orcl_ppas
Password of the scott role:
psql.bin (9.4.1.3, server 9.3.5.14)
Input "help" to obtain help information.
orcl_ppas=>
```

CREATE TABLE

```
CREATE TABLE dept (
   deptno NUMBER(2) NOT NULL CONSTRAINT dept_pk PRIMARY KEY,
   dname VARCHAR2(14) CONSTRAINT dept_dname_uq UNIQUE,
   lock VARCHAR2(13))
CREATE TABLE emp (
  empno NUMBER(4) NOT NULL CONSTRAINT emp_pk PRIMARY KEY,
  ename VARCHAR2(10),
  job VARCHAR2(9),
  mgr NUMBER(4),
  hiredate DATE,
  sal NUMBER(7,2) CONSTRAINT emp_sal_ck CHECK (sal > 0),
  comm NUMBER(7,2),
  deptno NUMBER(2) CONSTRAINT emp_ref_dept_fk
                REFERENCES dept(deptno))
CREATE TABLE jobhist (
  empno NUMBER(4) NOT NULL,
  startdate DATE NOT NULL,
  enddate DATE,
  job VARCHAR2(9),
  sal NUMBER(7,2),
  comm NUMBER(7,2),
  deptno NUMBER(2),
  chgdesc VARCHAR2(80),
  CONSTRAINT jobhist_pk PRIMARY KEY (empno, startdate),
  CONSTRAINT jobhist_ref_emp_fk FOREIGN KEY (empno)
      REFERENCES emp(empno) ON DELETE CASCADE,
  CONSTRAINT jobhist_ref_dept_fk FOREIGN KEY (deptno)
      REFERENCES dept (deptno) ON DELETE SET NULL,
  CONSTRAINT jobhist_date_chk CHECK (startdate <= enddate))
```

CREATE OR REPLACE VIEW

```
CREATE OR REPLACE VIEW salesemp AS
   SELECT empno, ename, hiredate, sal, comm FROM emp WHERE job = 'SALESMAN';
```

CREATE SEQUENCE

```
CREATE SEQUENCE next_empno START WITH 8000 INCREMENT BY 1;
```

INSERT INTO

```
INSERT INTO dept VALUES (10,'ACCOUNTING','NEW YORK');
INSERT INTO dept VALUES (20,'RESEARCH','DALLAS');
INSERT INTO dept VALUES (30,'SALES','CHICAGO');
INSERT INTO dept VALUES (40,'OPERATIONS','BOSTON');
INSERT INTO emp VALUES (7369,'SMITH','CLERK',7902,'17-DEC-80',800,NULL,20);
INSERT INTO emp VALUES (7499,'ALLEN','SALESMAN',7698,'20-FEB-81',1600,300,30);
INSERT INTO emp VALUES (7521,'WARD','SALESMAN',7698,'22-FEB-81',1250,500,30);
INSERT INTO emp VALUES (7566,'JONES','MANAGER',7839,'02-APR-81',2975,NULL,20);
INSERT INTO emp VALUES (7654,'MARTIN','SALESMAN',7698,'28-SEP-81',1250,1400,30);
INSERT INTO emp VALUES (7698,'BLAKE','MANAGER',7839,'01-MAY-81',2850,NULL,30);
INSERT INTO emp VALUES (7782,'CLARK','MANAGER',7839,'09-JUN-81',2450,NULL,10);
INSERT INTO emp VALUES (7788,'SCOTT','ANALYST',7566,'19-APR-87',3000,NULL,20);
INSERT INTO emp VALUES (7839,'KING','PRESIDENT',NULL,'17-NOV-81',5000,NULL,10);
INSERT INTO emp VALUES (7844,'TURNER','SALESMAN',7698,'08-SEP-81',1500,0,30);
INSERT INTO emp VALUES (7876,'ADAMS','CLERK',7788,'23-MAY-87',1100,NULL,20);
INSERT INTO emp VALUES (7900,'JAMES','CLERK',7698,'03-DEC-81',950,NULL,30);
INSERT INTO emp VALUES (7902,'FORD','ANALYST',7566,'03-DEC-81',3000,NULL,20);
INSERT INTO emp VALUES (7934,'MILLER','CLERK',7782,'23-JAN-82',1300,NULL,10);
INSERT INTO jobhist VALUES (7369,'17-DEC-80',NULL,'CLERK',800,NULL,20,'New Hire');
INSERT INTO jobhist VALUES (7499,'20-FEB-81',NULL,'SALESMAN',1600,300,30,'New Hire');
INSERT INTO jobhist VALUES (7521,'22-FEB-81',NULL,'SALESMAN',1250,500,30,'New Hire');
INSERT INTO jobhist VALUES (7566,'02-APR-81',NULL,'MANAGER',2975,NULL,20,'New Hire');
INSERT INTO jobhist VALUES (7654,'28-SEP-81',NULL,'SALESMAN',1250,1400,30,'New Hire');
INSERT INTO jobhist VALUES (7698,'01-MAY-81',NULL,'MANAGER',2850,NULL,30,'New Hire');
INSERT INTO jobhist VALUES (7782,'09-JUN-81',NULL,'MANAGER',2450,NULL,10,'New Hire');
INSERT INTO jobhist VALUES (7788,'19-APR-87','12-APR-88','CLERK',1000,NULL,20,'New Hire');
INSERT INTO jobhist VALUES (7788,'13-APR-88','04-MAY-89','CLERK',1040,NULL,20,'Raise');
INSERT INTO jobhist VALUES (7788,'05-MAY-90',NULL,'ANALYST',3000,NULL,20,'Promoted to Analyst');
INSERT INTO jobhist VALUES (7839,'17-NOV-81',NULL,'PRESIDENT',5000,NULL,10,'New Hire');
INSERT INTO jobhist VALUES (7844,'08-SEP-81',NULL,'SALESMAN',1500,0,30,'New Hire');
INSERT INTO jobhist VALUES (7876,'23-MAY-87',NULL,'CLERK',1100,NULL,20,'New Hire');
INSERT INTO jobhist VALUES (7900,'03-DEC-81','14-JAN-83','CLERK',950,NULL,10,'New Hire');
INSERT INTO jobhist VALUES (7900,'15-JAN-83',NULL,'CLERK',950,NULL,30,'Changed to Dept 30');
INSERT INTO jobhist VALUES (7902,'03-DEC-81',NULL,'ANALYST',3000,NULL,20,'New Hire');
INSERT INTO jobhist VALUES (7934,'23-JAN-82',NULL,'CLERK',1300,NULL,10,'New Hire');
```

ANALYZE

```
ANALYZE dept;
ANALYZE emp;
ANALYZE jobhist;
```

CREATE PROCEDURE

```
CREATE OR REPLACE PROCEDURE list_emp
IS
 v_empno NUMBER(4);
 v_ename VARCHAR2(10);
 CURSOR emp_cur IS
   SELECT empno, ename FROM emp ORDER BY empno;
BEGIN
 OPEN emp_cur;
 DBMS_OUTPUT.PUT_LINE('EMPNO ENAME');
 DBMS_OUTPUT.PUT_LINE('----- -------');
 LOOP
   FETCH emp_cur INTO v_empno, v_ename;
   EXIT WHEN emp_cur%NOTFOUND;
   DBMS_OUTPUT.PUT_LINE(v_empno || ' ' || v_ename);
 END LOOP;
 CLOSE emp_cur;
END;
-- Procedure that selects an employee row given the employee
-- number and displays certain columns.
CREATE OR REPLACE PROCEDURE select_emp (
 p_empno IN NUMBER)
IS
 v_ename emp.ename%TYPE;
 v_hiredate emp.hiredate%TYPE;
 v_sal emp.sal%TYPE;
 v_comm emp.comm%TYPE;
 v_dname dept.dname%TYPE;
 v_disp_date VARCHAR2(10);
BEGIN
 SELECT ename, hiredate, sal, NVL(comm, 0), dname
   INTO v_ename, v_hiredate, v_sal, v_comm, v_dname
   FROM emp e, dept d
   WHERE empno = p_empno
    AND e.deptno = d.deptno;
 v_disp_date := TO_CHAR(v_hiredate, 'MM/DD/YYYY');
 DBMS_OUTPUT.PUT_LINE('Number : ' || p_empno);
 DBMS_OUTPUT.PUT_LINE('Name : ' || v_ename);
 DBMS_OUTPUT.PUT_LINE('Hire Date : ' || v_disp_date);
 DBMS_OUTPUT.PUT_LINE('Salary : ' || v_sal);
 DBMS_OUTPUT.PUT_LINE('Commission: ' || v_comm);
 DBMS_OUTPUT.PUT_LINE('Department: ' || v_dname);
EXCEPTION
 WHEN NO_DATA_FOUND THEN
   DBMS_OUTPUT.PUT_LINE('Employee ' || p_empno || ' not found');
 WHEN OTHERS THEN
   DBMS_OUTPUT.PUT_LINE('The following is SQLERRM:');
   DBMS_OUTPUT.PUT_LINE(SQLERRM);
   DBMS_OUTPUT.PUT_LINE('The following is SQLCODE:');
   DBMS_OUTPUT.PUT_LINE(SQLCODE);
END;
-- Procedure that queries the 'emp' table based on
-- department number and employee number or name.  Returns
-- employee number and name as IN OUT parameters and job,
-- hire date, and salary as OUT parameters.
CREATE OR REPLACE PROCEDURE emp_query (
 p_deptno IN NUMBER,
 p_empno IN OUT NUMBER,
 p_ename IN OUT VARCHAR2,
 p_job OUT VARCHAR2,
 p_hiredate OUT DATE,
 p_sal OUT NUMBER)
IS
BEGIN
```

```
 SELECT empno, ename, job, hiredate, sal
   INTO p_empno, p_ename, p_job, p_hiredate, p_sal
   FROM emp
   WHERE deptno = p_deptno
    AND (empno = p_empno
     OR ename = UPPER(p_ename));
END;
-- Procedure to call 'emp_query_caller' with IN and IN OUT
-- parameters.  Displays the results received from IN OUT and
-- OUT parameters.
CREATE OR REPLACE PROCEDURE emp_query_caller
IS
 v_deptno NUMBER(2);
 v_empno NUMBER(4);
 v_ename VARCHAR2(10);
 v_job VARCHAR2(9);
 v_hiredate DATE;
 v_sal NUMBER;
BEGIN
 v_deptno := 30;
 v_empno := 0;
 v_ename := 'Martin';
 emp_query(v_deptno, v_empno, v_ename, v_job, v_hiredate, v_sal);
 DBMS_OUTPUT.PUT_LINE('Department : ' || v_deptno);
 DBMS_OUTPUT.PUT_LINE('Employee No: ' || v_empno);
 DBMS_OUTPUT.PUT_LINE('Name : ' || v_ename);
 DBMS_OUTPUT.PUT_LINE('Job : ' || v_job);
 DBMS_OUTPUT.PUT_LINE('Hire Date : ' || v_hiredate);
 DBMS_OUTPUT.PUT_LINE('Salary : ' || v_sal);
EXCEPTION
 WHEN TOO_MANY_ROWS THEN
   DBMS_OUTPUT.PUT_LINE('More than one employee was selected');
 WHEN NO_DATA_FOUND THEN
   DBMS_OUTPUT.PUT_LINE('No employees were selected');
END;
```

CREATE FUNCTION

```
CREATE OR REPLACE FUNCTION emp_comp (
 p_sal NUMBER,
 p_comm NUMBER
) RETURN NUMBER
IS
BEGIN
 RETURN (p_sal + NVL(p_comm, 0)) * 24;
END;
-- Function that gets the next number from sequence, 'next_empno',
-- and ensures it is not already in use as an employee number.
CREATE OR REPLACE FUNCTION new_empno RETURN NUMBER
IS
 v_cnt INTEGER := 1;
 v_new_empno NUMBER;
BEGIN
 WHILE v_cnt > 0 LOOP
```

```
   SELECT next_empno.nextval INTO v_new_empno FROM dual;
   SELECT COUNT(*) INTO v_cnt FROM emp WHERE empno = v_new_empno;
 END LOOP;
 RETURN v_new_empno;
END;
-- EDB-SPL function that adds a new clerk to table 'emp'.  This function
-- uses package 'emp_admin'.
CREATE OR REPLACE FUNCTION hire_clerk (
 p_ename VARCHAR2,
 p_deptno NUMBER
) RETURN NUMBER
IS
 v_empno NUMBER(4);
 v_ename VARCHAR2(10);
 v_job VARCHAR2(9);
 v_mgr NUMBER(4);
 v_hiredate DATE;
 v_sal NUMBER(7,2);
 v_comm NUMBER(7,2);
 v_deptno NUMBER(2);
BEGIN
 v_empno := new_empno;
 INSERT INTO emp VALUES (v_empno, p_ename, 'CLERK', 7782,
   TRUNC(SYSDATE), 950.00, NULL, p_deptno);
 SELECT empno, ename, job, mgr, hiredate, sal, comm, deptno INTO
   v_empno, v_ename, v_job, v_mgr, v_hiredate, v_sal, v_comm, v_deptno
   FROM emp WHERE empno = v_empno;
 DBMS_OUTPUT.PUT_LINE('Department : ' || v_deptno);
 DBMS_OUTPUT.PUT_LINE('Employee No: ' || v_empno);
 DBMS_OUTPUT.PUT_LINE('Name : ' || v_ename);
 DBMS_OUTPUT.PUT_LINE('Job : ' || v_job);
 DBMS_OUTPUT.PUT_LINE('Manager : ' || v_mgr);
 DBMS_OUTPUT.PUT_LINE('Hire Date : ' || v_hiredate);
 DBMS_OUTPUT.PUT_LINE('Salary : ' || v_sal);
 DBMS_OUTPUT.PUT_LINE('Commission : ' || v_comm);
 RETURN v_empno;
EXCEPTION
 WHEN OTHERS THEN
   DBMS_OUTPUT.PUT_LINE('The following is SQLERRM:');
   DBMS_OUTPUT.PUT_LINE(SQLERRM);
   DBMS_OUTPUT.PUT_LINE('The following is SQLCODE:');
   DBMS_OUTPUT.PUT_LINE(SQLCODE);
   RETURN -1;
END;
-- PostgreSQL PL/pgSQL function that adds a new salesman
-- to table 'emp'.
CREATE OR REPLACE FUNCTION hire_salesman (
 p_ename VARCHAR,
 p_sal NUMERIC,
 p_comm NUMERIC
) RETURNS NUMERIC
AS $$
DECLARE
 v_empno NUMERIC(4);
         VARCHAR(10)
 v_ename VARCHAR(10);
 v_job VARCHAR(9);
 v_mgr NUMERIC(4);
 v_hiredate DATE;
 v_sal NUMERIC(7,2);
 v_comm NUMERIC(7,2);
 v_deptno NUMERIC(2);
BEGIN
 Vanderbilt empno: = new_empno ();
 INSERT INTO emp VALUES (v_empno, p_ename, 'SALESMAN', 7698,
   CURRENT_DATE, p_sal, p_comm, 30);
 SELECT INTO
   Vanderbilt empno, le_ename, Vanderbilt job, Vanderbilt Mgr, glassals
   empno, ename, job, mgr, hiredate, sal, comm, deptno
   FROM emp WHERE empno = v_empno;
 RAISE INFO 'Department : %', v_deptno;
 RAISE INFO 'Employee No: %', v_empno;
 RAISE INFO 'Name : %', v_ename;
 RAISE INFO 'Job : %', v_job;
 RAISE INFO 'Manager : %', v_mgr;
 RAISE INFO 'Hire Date : %', v_hiredate;
 RAISE INFO 'Salary : %', v_sal;
 RAISE INFO 'Commission : %', v_comm;
 RETURN v_empno;
EXCEPTION
 WHEN OTHERS THEN
   RAISE INFO 'The following is SQLERRM:';
   RAISE INFO '%', SQLERRM;
   RAISE INFO 'The following is SQLSTATE:';
   RAISE INFO '%', SQLSTATE;
   RETURN -1;
END;
```

CREATE RULE

```
CREATE OR REPLACE RULE salesemp_i AS ON INSERT TO salesemp
DO INSTEAD
 INSERT INTO emp VALUES (NEW.empno, NEW.ename, 'SALESMAN', 7698,
   NEW.hiredate, NEW.sal, NEW.comm, 30);
CREATE OR REPLACE RULE salesemp_u AS ON UPDATE TO salesemp
DO INSTEAD
 UPDATE emp SET empno = NEW.empno,
          ename = NEW.ename,
          hiredate = NEW.hiredate,
          sal = NEW.sal,
          comm = NEW.comm
   WHERE empno = OLD.empno;
CREATE OR REPLACE RULE salesemp_d AS ON DELETE TO salesemp
DO INSTEAD
DELETE FROM emp WHERE empno = OLD.empno;
```

CREATE TRIGGER

```
CREATE OR REPLACE TRIGGER user_audit_trig
 AFTER INSERT OR UPDATE OR DELETE ON emp
DECLARE
 v_action VARCHAR2(24);
BEGIN
 IF INSERTING THEN
   v_action := ' added employee(s) on ';
 ELSIF UPDATING THEN
   v_action := ' updated employee(s) on ';
 ELSIF DELETING THEN
   v_action := ' deleted employee(s) on ';
 END IF;
 DBMS_OUTPUT.PUT_LINE('User ' || USER || v_action || TO_CHAR(SYSDATE,'YYYY-MM-DD'));
END;
CREATE OR REPLACE TRIGGER emp_sal_trig
 Before delete or insert or update on EMP
 FOR EACH ROW
DECLARE
 sal_diff NUMBER;
BEGIN
 IF INSERTING THEN
   DBMS_OUTPUT.PUT_LINE('Inserting employee ' || :NEW.empno);
   DBMS_OUTPUT.PUT_LINE('.. New salary: ' || :NEW.sal);
 END IF;
 IF UPDATING THEN
   sal_diff := :NEW.sal - :OLD.sal;
   DBMS_OUTPUT.PUT_LINE('Updating employee ' || :OLD.empno);
   DBMS_OUTPUT.PUT_LINE('.. Old salary: ' || :OLD.sal);
   DBMS_OUTPUT.PUT_LINE('.. New salary: ' || :NEW.sal);
   DBMS_OUTPUT.PUT_LINE('.. Raise : ' || sal_diff);
 END IF;
 IF DELETING THEN
   DBMS_OUTPUT.PUT_LINE('Deleting employee ' || :OLD.empno);
   DBMS_OUTPUT.PUT_LINE('.. Old salary: ' || :OLD.sal);
 END IF;
END;
```

CREATE PACKAGE

```
CREATE OR REPLACE PACKAGE emp_admin
IS
 FUNCTION get_dept_name (
   p_deptno NUMBER
 ) RETURN VARCHAR2;
 FUNCTION update_emp_sal (
   p_empno NUMBER,
   p_raise NUMBER
 ) RETURN NUMBER;
 PROCEDURE hire_emp (
   p_empno NUMBER,
   p_ename VARCHAR2,
   p_job VARCHAR2,
   p_sal NUMBER,
   p_hiredate DATE,
   p_comm NUMBER,
   p_mgr NUMBER,
   p_deptno NUMBER)
 PROCEDURE fire_emp (
   p_empno NUMBER)
END emp_admin;
```

CREATE PACKAGE BODY

```
-- Package body for the 'emp_admin' package.
CREATE OR REPLACE PACKAGE BODY emp_admin
IS
 -- Function that queries the 'dept' table based on the department
 -- number and returns the corresponding department name.
 FUNCTION get_dept_name (
   p_deptno IN NUMBER
 ) RETURN VARCHAR2
 IS
   v_dname VARCHAR2(14);
 BEGIN
   SELECT dname INTO v_dname FROM dept WHERE deptno = p_deptno;
   RETURN v_dname;
 EXCEPTION
   WHEN NO_DATA_FOUND THEN
     DBMS_OUTPUT.PUT_LINE('Invalid department number ' || p_deptno);
     RETURN '';
 END;
 -- Function that updates an employee's salary based on the
 -- employee number and salary increment/decrement passed
 -- as IN parameters.  Upon successful completion the function
 -- returns the new updated salary.
 FUNCTION update_emp_sal (
   p_empno IN NUMBER,
   p_raise IN NUMBER
 ) RETURN NUMBER
 IS
   v_sal NUMBER := 0;
 BEGIN
   SELECT sal INTO v_sal FROM emp WHERE empno = p_empno;
```

```
    SELECT sal INTO v_sal FROM emp WHERE empno = p_empno;
    v_sal := v_sal + p_raise;
    UPDATE emp SET sal = v_sal WHERE empno = p_empno;
    RETURN v_sal;
  EXCEPTION
    WHEN NO_DATA_FOUND THEN
      DBMS_OUTPUT.PUT_LINE('Employee ' || p_empno || ' not found');
      RETURN -1;
    WHEN OTHERS THEN
      DBMS_OUTPUT.PUT_LINE('The following is SQLERRM:');
      DBMS_OUTPUT.PUT_LINE(SQLERRM);
      DBMS_OUTPUT.PUT_LINE('The following is SQLCODE:');
      DBMS_OUTPUT.PUT_LINE(SQLCODE);
      RETURN -1;
  END;
  -- Procedure that inserts a new employee record into the 'emp' table.
  PROCEDURE hire_emp (
    p_empno NUMBER,
    p_ename VARCHAR2,
    p_job VARCHAR2,
    p_sal NUMBER,
    p_hiredate DATE,
    p_comm NUMBER,
    p_mgr NUMBER,
    p_deptno NUMBER)
  AS
  BEGIN
    INSERT INTO emp(empno, ename, job, sal, hiredate, comm, mgr, deptno)
      VALUES(p_empno, p_ename, p_job, p_sal,
          p_hiredate, p_comm, p_mgr, p_deptno);
  END;
  -- Procedure that deletes an employee record from the 'emp' table based
  -- on the employee number.
  PROCEDURE fire_emp (
    p_empno NUMBER)
  AS
  BEGIN
    DELETE FROM emp WHERE empno = p_empno;
  END;
END;
```

23.Common management functions

The superuser permissions in RDS PPAS are not released, so you cannot use the superuser account in the same way as offline usage of PPAS to manage database objects. Therefore, we provide a set of common management functions, allowing you to use various PPAS features.

Rules for using management functions

Various management functions on the cloud must be run by an RDS root account. The RDS root account is a management account specified upon instance allocation, and has the permissions such as createdb, createrole, and logon.

- **Plugin management function: rds_manage_extension**
  This function enables you to manage plugins on the cloud. You can use this function to create and delete the plugins that are currently supported by PPAS.

```
rds_manage_extension(operation text, pname text, schema text default NULL,logging bool default false)
 operation: create or drop
 pname: the name of the supported plugin
 schema: the target mode to which the plugin is created
 logging: the log information obtained upon creating the plugin
 The plugins that are currently supported include:
 pg_stat_statements
 btree_gin
 btree_gist
 chkpass
 citext
 cube
 dblink
 dict_int
 earthdistance
 hstore
 intagg
 intarray
 isn
 ltree
 pgcrypto
 pgrowlocks
 pg_prewarm
 pg_trgm
 postgres_fdw
 sslinfo
 tablefunc
 tsearch2
 unaccent
 postgis
 postgis_topology
 fuzzystrmatch
 postgis_tiger_geocoder
 plperl
 pltcl
 plv8
 "uuid-ossp"
 plpgsql
 oss_fdw
 For example:
 1. Create the plugin named dblink.
   select rds_manage_extension('create','dblink');
 2. Delete the plugin named dblink.
   select rds_manage_extension('drop','dblink');
```

- Currently connected session: rds_pg_stat_activity()
  This function is similar to the pg_stat_activity view, and returns all information about the connected sessions related to the account.
- Check slow SQL: rds_pg_stat_statements()
  This function is the encapsulation of the pg_stat_statements view. It allows you to check the slow SQL statements within your range of permission.
- Performance analysis functions

This group of functions is similar to the Oracle AWR report. It enables you to analyze the real-time performance of the current PPAS instance.

```
 1 rds_truncsnap()
 NOTE: Delete all currently stored snapshots.
 2 rds_get_snaps()
 NOTE: Get the information of all currently stored snapshots.
 3 rds_snap()
 NOTE: Generate a real-time snapshot.
 4 rds_report(beginsnap bigint, endsnap bigint)
 Produce a starting snapshot change and an ending snapshot change to generate a snapshot based performance analysis report.
 Example: The process of generating a performance analysis report through the production of snapshots is described as follows.
 SELECT * FROM rds_truncsnap(); // Delete the previously stored snapshots.
 SELECT * from rds_snap(); // Produce a snapshot.
 SELECT * from rds_snap(); // Produce a snapshot.
 SELECT * from rds_snap(); // Produce a snapshot.
 SELECT * FROM rds_get_snaps(); // Get the currently produced snapshots ID, namely, 1, 2, and 3.
 SELECT * FROM edbreport(1, 3); // Generate a performance analysis report based on the snapshots.
```

- Session termination function.

```
rds_pg_terminate_backend(upid int)
 rds_pg_cancel_backend(upid int)
 These two functions are the native pg_terminate_backend and pg_cancel_backend. The only difference between the two functions is that they cannot run the connections created by the superuser.
 Example: Terminate the session with process ID 123456.
 select rds_pg_cancel_backend(123456);
```

- VPD function

  VPD is short for Virtual Private Database. It is an encapsulation compatible with Package DBMS_RLS because their parameters are the same.

```
1 rds_drop_policy corresponding to DBMS_RLS.DROP_POLICY
 2 rds_enable_policy corresponding to DBMS_RLS.ENABLE_POLICY
 3 rds_add_policy corresponding to DBMS_RLS.ADD_POLICY
```

Learn more about VPD