RDS for PostgreSQL

Service Overview

Issue 01

Date 2025-09-11

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 What Is RDS for PostgreSQL?

PostgreSQL is an open-source object-relational database management system that focuses on extensibility and standards compliance. It is known as the most advanced open-source database available.

Why Is RDS for PostgreSQL Your Right Choice?

RDS for PostgreSQL excels in processing complex online transaction processing (OLTP) transactions and supports NoSQL (JSON, XML, or hstore) and geographic information system (GIS) data types. It has earned a reputation for reliability and data integrity, and is widely used for websites, location-based applications, and complex data object processing.

- RDS for PostgreSQL supports the PostGIS extension and provides excellent spatial performance.
- RDS for PostgreSQL is a good cost-effective solution for many different scenarios. You can flexibly scale resources based on your service requirements and pay for only what you use.

For details about the versions supported by RDS for PostgreSQL, see **DB Engines and Versions**.

For more information, see the official documentation at **https://www.postgresql.org/docs/**.

2 Advantages

Easy Management

- Quick Setup

  You can create a DB instance on the management console within minutes and access the DB instance from an ECS over a private network to reduce the application response time and avoid paying for the traffic that would be generated by regular public access.

- Elastic Scaling

  Cloud Eye monitors changes in the load on your database and storage capacity. You can flexibly scale resources accordingly and pay for only what you use.

- High Compatibility

  You can use RDS database engines (DB engines) the same way as you would use a native engine. RDS is compatible with existing programs and tools. With Data Replication Service (DRS), you can migrate data to RDS easily with low costs.

- Easy O&M

  Routine RDS maintenance and management operations, including hardware and software fault handling and database patching, are easy to perform. With a web-based console, you can reboot DB instances, reset passwords, modify parameters, view error or slow query logs, and restore data. Additionally, the system helps you monitor DB instances in real time and generates alarms if errors occur. You can check DB instance information at any time, including CPU usage, IOPS, database connections, and storage space usage.

High Performance

- Optimized Performance

  Combining years of experience in database R&D, setup, and maintenance with cloud-based technology, Huawei Cloud has built a database service that is highly available, reliable, secure, scalable, and easy to maintain.

- Optimized Hardware

  RDS offers stable and high-performance database services using servers that have been proven robust by customer success in a wide range of applications.

- Optimized SQL Solutions

  RDS can detect slowly-executed SQL statements, so you can optimize the code accordingly.

- High-Speed Access

  You can access RDS DB instances directly from ECSs deployed in the same region. This means applications can respond faster, and saves money as it is an intranet connection so there are no traffic charges generated.

- Performance White Paper
  - **RDS for PostgreSQL Performance White Paper**

High Security

- Network Isolation

  Virtual Private Clouds (VPCs) and network security groups are used to isolate and secure your DB instances. VPCs allow you to define which IP addresses are allowed to access your DB instance. You can configure subnets and security groups to control access to DB instances.

- Access Control

  RDS controls access through the account/IAM user and security groups. When you create an RDS DB instance, an account is automatically created. To separate out specific permissions, you can create IAM users and assign permissions to them as needed. VPC security groups have rules that govern both inbound and outbound traffic of DB instances.

- Transmission Encryption

  RDS uses Transport Layer Security (TLS) and Secure Sockets Layer (SSL) to encrypt transmission. You can download a Certificate Agency (CA) certificate from the RDS console and upload it when connecting to a database for authentication.

- Storage Encryption

  RDS encrypts data before storing it.

- Data Deletion

  When you delete an RDS DB instance, its attached disks, storage space its automated backups occupy, and all data it stores will be deleted. You can restore a deleted DB instance using a manual backup or rebuild the DB instance from the recycle bin within the retention period.

- Security Protection

  RDS is protected by multiple layers of firewalls to defend against various malicious attacks, such as DDoS attacks and SQL injections. For security reasons, you are advised to access RDS DB instances through a private network.

High Reliability

- Dual-Host Hot Standby

  RDS uses the hot standby architecture, in which failover upon fault occurrence takes only some seconds.

- Data Backup

The system automatically backs up data every day and stores backup files as packages in Object Storage Service (OBS). The backup files can be stored for 732 days and can be restored with just a few clicks. You can set a custom backup policy and create manual backups at any time.

- Data Restoration

  You can restore data from backups to any point in time during the backup retention period. In most scenarios, you can use backups to restore data to a new instance or an existing instance at any point in time within 732 days. After the data is verified, data can be migrated back to the primary DB instance.

  Deleted DB instances can be moved to the recycle bin. You can rebuild the DB instance that was deleted up to 7 days ago from the recycle bin.

- Data Durability

  RDS provides a data durability of 99.9999999%, ensuring data security and reliability and protecting your workloads from faults.

Comparison Between RDS and On-Premises Databases

Table 2-1 Comparison

Item	RDS	On-Premises Database
Service availability	For details, see **ECS Advantages**.	Requires device procurement, primary/standby relationship setup, and RAID setup.
Data reliability	For details, see **What Is EVS?**	Requires device procurement, primary/standby relationship setup, and RAID setup.
Database backup	Supports automated backups, manual backups, and custom backup retention periods.	Requires device procurement, setup, and maintenance.
Hardware and software investment	Supports on-demand pricing and scaling without requiring hardware and software investment.	Requires large investment in database servers.
System hosting	Not required.	Requires two servers for primary/standby DB instances.
Maintenance cost	Not required.	Requires large labor investment and professional database administrator (DBA) for maintenance.
Deployment and scaling	Supports elastic scaling, fast upgrade, and on-demand enabling.	Requires procurement, deployment, and coordination of hardware that matches original devices.

3 Typical Use Cases

Reducing Read Pressure with Read/Write Splitting

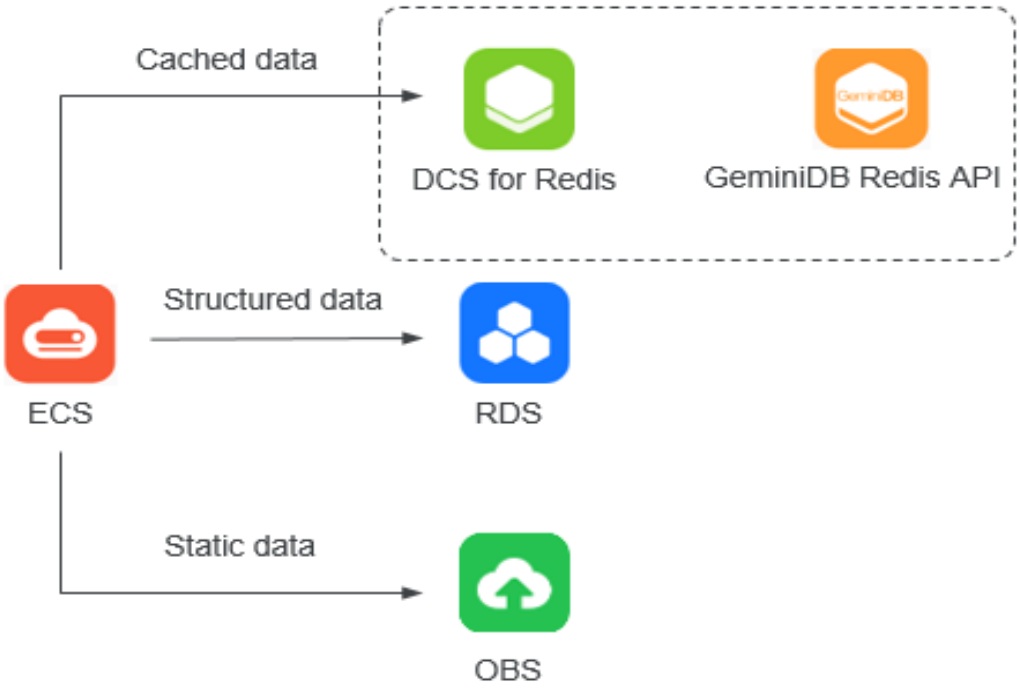
RDS for PostgreSQL supports read replicas to offload read traffic from primary DB instances.

To offload read pressure on the primary DB instance, you can create one or more read replicas in the same region as the primary instance. These read replicas can process a large number of read requests and increase application throughput.

Storing Diverse Data Types

RDS can work with Distributed Cache Service (DCS) for Redis, GeminiDB Redis API, and OBS to store different types of data.

Figure 3-1 Storing diverse data types



4 Product Series

RDS for PostgreSQL DB instances are classified into the following types:

- Single-node
- Primary/Standby

Table 4-1 DB instance types

DB Instance Type	Description	Notes	Scenarios
Single-node	A single-node architecture is more cost-effective than a primary/standby DB pair.	If a fault occurs on a single-node instance, the instance cannot recover in a timely manner.	• Personal learning • Microsites • Development and testing environment of small- and medium-sized enterprises

DB Instance Type	Description	Notes	Scenarios
Primary/Standby	An HA architecture. A pair of primary and standby DB instances shares the same IP address and can be deployed in different AZs.	• When a primary instance is being created, a standby instance is provisioned along with it to provide data redundancy. The standby instance is invisible to you after being created. • If the primary instance fails, a failover occurs, during which database connection is interrupted. If there is a replication delay between the primary and standby instances, the failover takes an extended period of time. The client needs to be able to reconnect to the instance.	• Production databases of large and medium enterprises • Applications for the Internet, Internet of Things (IoT), retail e-commerce sales, logistics, gaming, and other industries

Advantage Comparison

- Single-node DB instances: support the creation of read replicas and support the queries of error logs and slow query logs. Different from a primary/standby DB instance that has two database nodes, a single-node DB instance has only one node, reducing the price to half of a primary/standby DB instance. If the node fails, the restoration will take a long time. Therefore, single-node DB instances are not recommended for workloads that are highly sensitive to database availability.
- Primary/Standby DB instances: use the standby database node only for failover and restoration. The standby database node does not provide services. The performance of single-node DB instances is similar to or even higher than primary/standby DB instances because standby nodes cause extra performance overhead.

Table 4-2 Function comparisons

Function	Single-Node	Primary/Standby
Number of nodes	1	2
Specifications	vCPUs: a maximum of 64 Memory: a maximum of 512 GB Storage: a maximum of 4,000 GB	vCPUs: a maximum of 64 Memory: a maximum of 512 GB Storage: a maximum of 4,000 GB
Monitoring and alarms	Supported	Supported
Security group	Supported	Supported
Backup and restoration	Supported	Supported
Recycle bin	Supported	Supported
Parameter settings	Supported	Supported
SSL	Supported	Supported
Log management	Supported	Supported
Read replicas (which need to be created)	Supported	Supported
High-frequency monitoring	Supported	Supported
Failover	Not supported	Supported
Standby DB instance migration	Not supported	Supported
Manual primary/standby switchover	Not supported	Supported
Instance class change	Supported	Supported

5 DB Instance Description

5.1 DB Instance Types

The smallest management unit of RDS is DB instance. A DB instance is an isolated database environment on the cloud. Each DB instance can contain multiple user-created databases, and you can access a DB instance using the same tools and applications that you use with a stand-alone DB instance. You can easily create or modify DB instances using the management console or HTTPS-compliant application programming interfaces (APIs). RDS does not have limits on the number of running DB instances. Each DB instance has a unique identifier.

DB instances are classified into the following types.

Table 5-1 DB instance types

DB Instance Type	Description	Notes
Single-node	A single-node architecture is more cost-effective than a primary/standby DB pair.	If a fault occurs on a single-node instance, the instance cannot recover in a timely manner.

DB Instance Type	Description	Notes
Primary/ Standby	An HA architecture. In a primary/standby pair, each instance has the same instance class. The primary and standby instances can be deployed in different AZs.	• When a primary instance is being created, a standby instance is provisioned along with it to provide data redundancy. The standby instance is invisible to you after being created. • If a failover occurs due to a primary instance failure, there is a brief interruption between your database client and the instance. The client needs to be able to reconnect to the instance. • RDS for PostgreSQL uses asynchronous replication by default.

DB Instance Type	Description	Notes
Read replica	A single-node or HA architecture	• Read replicas include single-node read replicas and HA read replicas. – Single-node read replicas: If you choose single-node read replicas, you are advised to buy more than one single-node read replica and enable database proxy. That way, if one read replica fails, the database proxy can route traffic to other read replicas. – HA read replicas: If the physical server where a primary read replica is deployed fails, the standby read replica automatically takes over the workloads. When you purchase a read replica, select the same value for **Table Name** as the DB instance. • If the replication between a read replica (single-node or HA) and the DB instance is abnormal, it can take a long time to rebuild and restore the read replica (depending on the data volume).

You can use RDS to create and manage DB instances running various DB engines.

For details about differences and function comparison between different instance types, see **Product Series**.

5.2 DB Instance Storage Types

The database system is generally an important part of an IT system and has high requirements on storage I/O performance. You can select a storage type based on service demands. You cannot change the storage type after the DB instance is created.

Description

RDS supports **Cloud SSD** and **Extreme SSD** to suit different performance requirements of your workloads.

- Cloud SSD

  Stores data in cloud disks for decoupled storage and compute. The maximum throughput is 350 MB/s.

  The supported IOPS depends on the I/O performance of the Elastic Volume Service (EVS) disk. For details, see "Ultra-high I/O" in **Disk Types and Performance** of the *Elastic Volume Service Service Overview*.

- Extreme SSD

  Uses 25GE network and RDMA technologies to provide you with up to 1,000 MB/s throughput per disk and sub-millisecond latency.

  The supported IOPS depends on the I/O performance of the EVS disk. For details, see "Extreme SSD" in **Disk Types and Performance** of the *Elastic Volume Service Service Overview*.

Performance Comparison

Table 5-2 Performance comparison

Item	Cloud SSD	Extreme SSD
I/O performance	Subpar I/O performance due to additional network I/O overheads	Higher I/O performance than cloud SSDs
Elastic scalability	Scaling in seconds	Scaling in seconds
Maximum IOPS	50,000	128,000
Maximum throughput	350 MB/s	1,000 MB/s
Read/write latency	1 ms	Sub-millisecond

5.3 DB Engines and Versions

Table 5-3 lists the DB engines and versions supported by RDS for PostgreSQL.

Table 5-3 DB engines and versions

DB Engine	Single-Node	Primary/Standby
PostgreSQL	• 17 • 16 • 15 • 14 • 13 • 12 (Only for existing instances) • 11 (Only for existing instances) • 10 (Only for existing instances) • 9.6 (Only for existing instances) • 9.5 (Only for existing instances)	• 17 • 16 • 15 • 14 • 13 • 12 (Only for existing instances) • 11 (Only for existing instances) • 10 (Only for existing instances) • 9.6 (Only for existing instances)

5.4 DB Instance Statuses

DB Instance Statuses

The status of a DB instance indicates the health of the DB instance. You can use the management console or API to view the status of a DB instance.

Table 5-4 DB instance statuses

Status	Description
Available	A DB instance is available.
Abnormal	A DB instance is abnormal.
Creating	A DB instance is being created.
Cloning	A DB instance is being cloned.
Creation failed	A DB instance has failed to be created.
Switchover in progress	A standby DB instance is being switched over to the primary DB instance.
Changing type to primary/standby	A single-node DB instance is being changed to a primary/standby DB instance.
Rebooting	A DB instance is being rebooted.

Status	Description
Changing port	A DB instance port is being changed.
Changing instance class	The CPU or memory of a DB instance is being modified.
Changing proxy instance class	The CPU or memory of a DB proxy instance is being modified.
Scaling up	Storage space of a DB instance is being scaled up.
Backing up	A DB instance is being backed up.
Restoring	A DB instance is in the process of being restored from a backup.
Restore failed	A DB instance fails to be restored.
Frozen	A DB instance is frozen when your account balance is less than or equal to $0 USD. Retained frozen DB instances are unfrozen only after your account is recharged and the overdue payments are cleared.
Storage full	Storage space of a DB instance is full. Data cannot be written to databases. You need to scale up the storage space to make the instance available.
Deleted	A DB instance has been deleted and will not be displayed in the instance list.
Upgrading minor version	A DB instance minor version is being upgraded.
Upgrading	A DB engine version is being upgraded.
Migrating standby DB instance	A standby instance is being migrated to another AZ in the same region.
Promoting to primary	A read replica is being promoted to a primary DB instance.
Parameter change. Pending reboot	A modification to a database parameter is waiting for an instance reboot before it can take effect.
Stopping	A DB instance is being stopped.
Stopped	A DB instance has been stopped. It can be stopped for up to seven days. You can manually restart it or it will be automatically restarted after seven days.
Starting	A stopped DB instance is being started.

Status	Description
Changing read/write permissions of the instance	The read/write permissions of a DB instance are being changed.
Forced to read-only	A DB instance is set to read-only and operations that cause data changes, such as data writes and updates, are not allowed for the instance.

6 DB Instance Classes

6.1 x86-based Instance Classes

To learn about the DB engine versions supported by RDS for PostgreSQL, see **DB Engines and Versions**.

RDS for PostgreSQL supports the following x86-based instance classes: general-purpose (recommended), dedicated (recommended), general-enhanced (installed base operations), and general-enhanced II (installed base operations), as listed in **Table 6-1**. For details about each instance class, see **Table 6-2** and **Table 6-3**.

Table 6-1 x86-based instance classes

Instance Class	Description	Scenario	Constraints
General-purpose (recommended)	CPU resources are shared with other general-purpose DB instances on the same physical machine. CPU usage is maximized through resource overcommitment. This instance class is a cost-effective option and suitable for scenarios where performance stability is not critical.	Suitable for scenarios that have high requirements on cost-effectiveness.	These instance classes are available in the following regions: • CN North-Beijing4 and CN North-Ulanqab1 • CN East-Shanghai1 • CN South-Guangzhou and CN South-Guangzhou-InvitationOnly • CN Southwest-Guiyang1 • AP-Bangkok and AP-Singapore • CN-Hong Kong • LA-Sao Paulo1, LA-Santiago, LA-Mexico City1, and LA-Mexico City2 • AF-Johannesburg
Dedicated (recommended)	The instance has dedicated CPU and memory resources to ensure stable performance. The performance of a dedicated instance is never affected by other instances on the same physical machine. This instance class is good when performance stability is important.	Suitable for core database scenarios such as e-commerce, gaming, finance, government, and enterprise applications.	
General-enhanced and general-enhanced II	With a leading network acceleration engine and Data Plane Development Kit (DPDK) fast packet processing, this instance class provides higher network performance and computing power.	Suitable for websites and web applications that require high database computing and network performance.	These two instance classes are for installed base operations.

Details of General-Purpose and Dedicated Instance Classes

Table 6-2 Details of general-purpose and dedicated instance classes

Instance Class	Specification Code for Primary/ Standby Instances	Specification Code for Read Replicas	Specification Code for Single-Node Instances	vCPUs	Memory (GB)
General-purpose	rds.pg.n1.medium.2.ha	rds.pg.n1.medium.2.rr	rds.pg.n1.medium.2	1	2
	rds.pg.n1.large.2.ha	rds.pg.n1.large.2.rr	rds.pg.n1.large.2	2	4
	rds.pg.n1.large.4.ha	rds.pg.n1.large.4.rr	rds.pg.n1.large.4	2	8
	rds.pg.n1.xlarge.2.ha	rds.pg.n1.xlarge.2.rr	rds.pg.n1.xlarge.2	4	8
	rds.pg.n1.xlarge.4.ha	rds.pg.n1.xlarge.4.rr	rds.pg.n1.xlarge.4	4	16
	rds.pg.n1.2xlarge.2.ha	rds.pg.n1.2xlarge.2.rr	rds.pg.n1.2xlarge.2	8	16
	rds.pg.n1.2xlarge.4.ha	rds.pg.n1.2xlarge.4.rr	rds.pg.n1.2xlarge.4	8	32
Dedicated **NOTE** The specifications supported for cloud SSDs and extreme SSDs are different.	rds.pg.x1.large.2.ha	rds.pg.x1.large.2.rr	-	2	4
	rds.pg.x1.large.4.ha	rds.pg.x1.large.4.rr	-	2	8
	rds.pg.x1.large.8.ha	rds.pg.x1.large.8.rr	-	2	16
	rds.pg.x1.xlarge.2.ha	rds.pg.x1.xlarge.2.rr	-	4	8
	rds.pg.x1.xlarge.4.ha	rds.pg.x1.xlarge.4.rr	-	4	16
	rds.pg.x1.xlarge.8.ha	rds.pg.x1.xlarge.8.rr	rds.pg.x1.xlarge.8	4	32
	rds.pg.x1.2xlarge.2.ha	rds.pg.x1.2xlarge.2.rr	rds.pg.x1.2xlarge.2	8	16
	rds.pg.x1.2xlarge.4.ha	rds.pg.x1.2xlarge.4.rr	rds.pg.x1.2xlarge.4	8	32
	rds.pg.x1.2xlarge.8.ha	rds.pg.x1.2xlarge.8.rr	rds.pg.x1.2xlarge.8	8	64

Instance Class	Specification Code for Primary/ Standby Instances	Specification Code for Read Replicas	Specification Code for Single-Node Instances	vCPUs	Memory (GB)
	rds.pg.x1.2xlarge.16.ha	rds.pg.x1.2xlarge.16.rr	rds.pg.x1.2xlarge.16	8	128
	rds.pg.x1.4xlarge.2.ha	rds.pg.x1.4xlarge.2.rr	rds.pg.x1.4xlarge.2	16	32
	rds.pg.x1.4xlarge.4.ha	rds.pg.x1.4xlarge.4.rr	rds.pg.x1.4xlarge.4	16	64
	rds.pg.x1.4xlarge.8.ha	rds.pg.x1.4xlarge.8.rr	rds.pg.x1.4xlarge.8	16	128
	rds.pg.x1.8xlarge.2.ha	rds.pg.x1.8xlarge.2.rr	rds.pg.x1.8xlarge.2	32	64
	rds.pg.x1.8xlarge.4.ha	rds.pg.x1.8xlarge.4.rr	rds.pg.x1.8xlarge.4	32	128
	rds.pg.x1.8xlarge.8.ha	rds.pg.x1.8xlarge.8.rr	rds.pg.x1.8xlarge.8	32	256
	rds.pg.x1.16xlarge.2.ha	rds.pg.x1.16xlarge.2.rr	rds.pg.x1.16xlarge.2	64	128
	rds.pg.x1.16xlarge.4.ha	rds.pg.x1.16xlarge.4.rr	rds.pg.x1.16xlarge.4	64	256
	rds.pg.x1.16xlarge.8.ha	rds.pg.x1.16xlarge.8.rr	rds.pg.x1.16xlarge.8	64	512

Details of General-Enhanced and General-Enhanced II Instance Classes

Table 6-3 Details of general-enhanced and general-enhanced II instance classes

Instance Class	vCPUs	Memory (GB)
General-enhanced	1	2
	1	4
	2	4
	2	8
	2	16
	4	8
	4	16

Instance Class	vCPUs	Memory (GB)
	4	32
	8	32
	8	64
	16	64
	32	128
	60	128
	60	256
General-enhanced II	2	4
	2	8
	2	16
	4	8
	4	16
	4	32
	8	16
	8	32
	8	64
	16	32
	16	64
	16	128
	32	64
	32	128
	64	128
	64	256
	64	512

The DB instance specifications vary according to site requirements.

7 Security

7.1 Shared Responsibilities

Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Unlike traditional on-premises data centers, cloud computing separates operators from users. This approach not only enhances flexibility and control for users but also greatly reduces their operational workload. For this reason, cloud security cannot be fully ensured by one party. Cloud security requires joint efforts of Huawei Cloud and you, as shown in **Figure 7-1**.

- **Huawei Cloud**: Huawei Cloud is responsible for infrastructure security, including security and compliance, regardless of cloud service categories. The infrastructure consists of physical data centers, which house compute, storage, and network resources, virtualization platforms, and cloud services Huawei Cloud provides for you. In PaaS and SaaS scenarios, Huawei Cloud is responsible for security settings, vulnerability remediation, security controls, and detecting any intrusions into the network where your services or Huawei Cloud components are deployed.
- **Customer**: As our customer, your ownership of and control over your data assets will not be transferred under any cloud service category. Without your explicit authorization, Huawei Cloud will not use or monetize your data, but you are responsible for protecting your data and managing identities and access. This includes ensuring the legal compliance of your data on the cloud, using secure credentials (such as strong passwords and multi-factor authentication), and properly managing those credentials, as well as monitoring and managing content security, looking out for abnormal account behavior, and responding to it, when discovered, in a timely manner.

Figure 7-1 Huawei Cloud shared security responsibility model

Cloud security responsibilities are determined by control, visibility, and availability. When you migrate services to the cloud, assets, such as devices, hardware, software, media, VMs, OSs, and data, are controlled by both you and Huawei Cloud. This means that your responsibilities depend on the cloud services you select. As shown in **Figure 7-1**, customers can select different cloud service types (such as IaaS, PaaS, and SaaS services) based on their service requirements. As control over components varies across different cloud service categories, the responsibilities are shared differently.

- In on-premises scenarios, customers have full control over assets such as hardware, software, and data, so tenants are responsible for the security of all components.
- In IaaS scenarios, customers have control over all components except the underlying infrastructure. So, customers are responsible for securing these components. This includes ensuring the legal compliance of the applications, maintaining development and design security, and managing vulnerability remediation, configuration security, and security controls for related components such as middleware, databases, and operating systems.
- In PaaS scenarios, customers are responsible for the applications they deploy, as well as the security settings and policies of the middleware, database, and network access under their control.
- In SaaS scenarios, customers have control over their content, accounts, and permissions. They need to protect their content, and properly configure and protect their accounts and permissions in compliance with laws and regulations.

7.2 Identity Authentication and Access Control

Identity Authentication

When you access RDS, the system authenticates your identity using a password or IAM.

- **Password verification**

  To manage your instance, you need to use Data Admin Service (DAS) to log in to your instance. The login is successful only after your account and password are verified.

- **IAM verification**

  You can use **Identity and Access Management (IAM)** to provide fine-grained control over RDS permissions. IAM provides identity authentication, permissions management, and access control, helping you efficiently manage access to your Huawei Cloud resources. IAM users can use RDS resources only after their accounts and passwords are verified. For details, see **Step 2: Create IAM Users and Log In**.

Access Control

- **Permissions control**

  If you need to assign different permissions to different employees in your enterprise to access your instance resources, IAM is a good choice. For details, see **Permissions**.

- **VPCs and subnets**

  A VPC is a logically isolated, configurable, and manageable virtual network. It helps improve the security of cloud resources and simplifies network deployment. You can define security groups, virtual private networks (VPNs), IP address segments, and bandwidth for a VPC. This facilitates internal network configuration and management and allows you to change your network in a secure and convenient manner.

  A subnet provides dedicated network resources that are logically isolated from other networks for security.

  For details, see **Creating a VPC**.

- **Security groups**

  A security group is a logical group that provides access control policies for the ECSs and RDS instances that have the same security protection requirements and are mutually trusted within a VPC. To ensure database security and reliability, you need to configure security group rules to allow only specific IP addresses and ports to access your RDS instances.

  For details, see **Adding a Security Group Rule**.

7.3 Data Protection

RDS provides a series of methods and features to ensure data security and reliability.

Table 7-1 Methods for data security

Method	Description	Reference
Secure Sockets Layer (SSL)	SSL is supported to ensure data transmission security.	**Connecting to an RDS for PostgreSQL Instance Through the psql CLI Client**
Cross-AZ deployment	To ensure high availability, RDS allows you to deploy primary and standby DB instances across AZs. AZs are physically isolated but interconnected through an internal network.	**Buying an RDS for PostgreSQL DB Instance**
Deletion protection	RDS allows you to move unsubscribed yearly/monthly DB instances and deleted pay-per-use DB instances to the recycle bin. You can rebuild a DB instance that was deleted up to 7 days ago from the recycle bin.	**Recycling a DB Instance**

7.4 Audit and Logs

Audit

- Cloud Trace Service (CTS)

  CTS is a log audit service intended for cloud security. It records operations on the cloud resources in your account. You can use the logs generated by CTS to perform security analysis, track resource changes, audit compliance, and locate faults.

  After you enable CTS and configure a tracker, CTS can record management and data traces of RDS for auditing.

  For details about how to enable and configure CTS, see **CTS Getting Started**.

  For details about RDS for PostgreSQL management and data traces that can be tracked by CTS, see **Key Operations Supported by CTS**.

- Database Security Service (DBSS)

  DBSS is based on machine learning and big data analytics technologies. It provides functions such as database audit, SQL injection attack detection, and risky operation identification to ensure the security of databases on the cloud.

  You are advised to use DBSS to provide extended data security capabilities. For details, see **Database Security Service**.

  Advantages:

  – DBSS can help you meet security compliance requirements.

    ▪ DBSS can help you comply with DJCP (graded protection) standards for database audit.

        - DBSS can help you comply with security laws and regulations, and provide compliance reports that meet data security standards (such as Sarbanes-Oxley).
      - DBSS can back up and restore database audit logs and meet the audit data retention requirements.
      - DBSS can monitor risks, sessions, session distribution, and SQL distribution in real time.
      - DBSS can report alarms for risky behavior and attacks and respond to database attacks in real time.
      - DBSS can locate internal violations and improper operations and keep data assets secure.

    Deployed in bypass pattern, database audit can perform flexible audits on the database without affecting user services.

      - Database audit monitors database logins, operation types (data definition, operation, and control), and operation objects based on risky operations to effectively audit the database.
      - Database audit analyzes risks and sessions, and detects SQL injection attempts so you can stay apprised of your database status.
      - Database audit provides a report template library to generate daily, weekly, or monthly audit reports according to your configurations. It sends real-time alarm notifications to help you obtain audit reports in a timely manner.

Logs

- Error logs contain logs generated while the database is running. They can help you analyze database problems.

  For details, see **Viewing and Downloading Error Logs**.
- Slow query logs record statements that exceed **log_min_duration_statement**. You can view log details and statistics to identify statements that are executing slowly and optimize the statements.

  For details, see **Viewing and Downloading Slow Query Logs**.

7.5 Risk Monitoring

Monitoring Metrics

RDS works with Cloud Eye to monitor instances in your account in real time, reporting alarms and sending notifications based on your settings. You can get details about running metrics and storage usage of your instances in real time.

For details about RDS for PostgreSQL metrics and how to create alarm rules, see **Configuring Displayed Metrics**.

Protection for Critical Operations

With critical operation protection enabled, to enhance the security of your data and configurations, the system requires your identity to be authenticated before

critical operations like deleting an instance can be performed. For more information, see **Critical Operation Protection**.

7.6 Fault Recovery

RDS automatically creates backups for your DB instance during a backup window you specify. The backups are stored based on a preset retention period (1 to 732 days).

To restore instance data, you can choose one of the following methods:

- **Restoring a DB instance from backups**
- **Restoring a DB instance to a point in time**

Cross-Region Backup

RDS can store backups in a different region from the DB instance for disaster recovery. If the DB instance ever fails, you can use backups in the other region to restore data to a new DB instance.

If you enable cross-region backup, backups are automatically stored in the region you specify.

Multiple-AZ Deployment

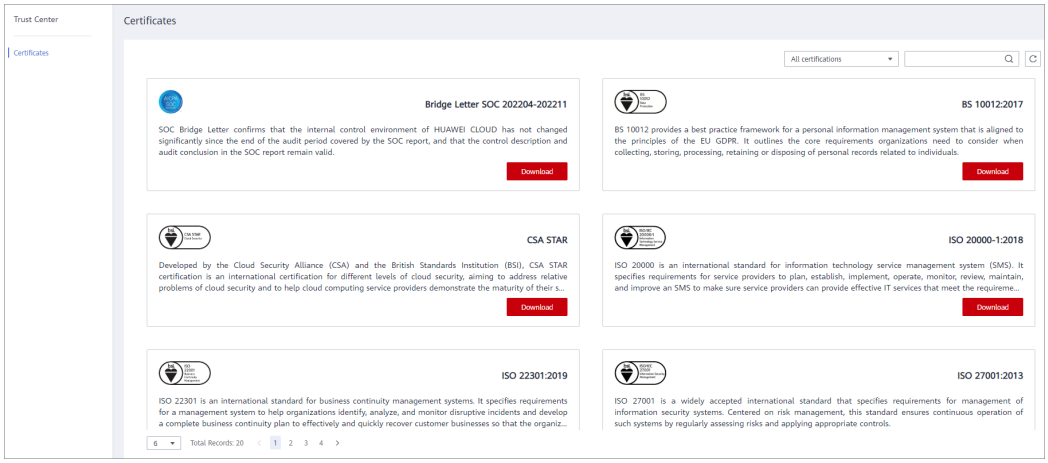
An AZ is a physical region where resources have their own independent power supply and networks. AZs are physically isolated but interconnected through a private network. You can deploy primary and standby DB instances in a single AZ or across AZs to achieve failover and high availability.

7.7 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO), system and organization controls (SOC), and Payment card industry (PCI) compliance standards. These certifications are available for **download**.

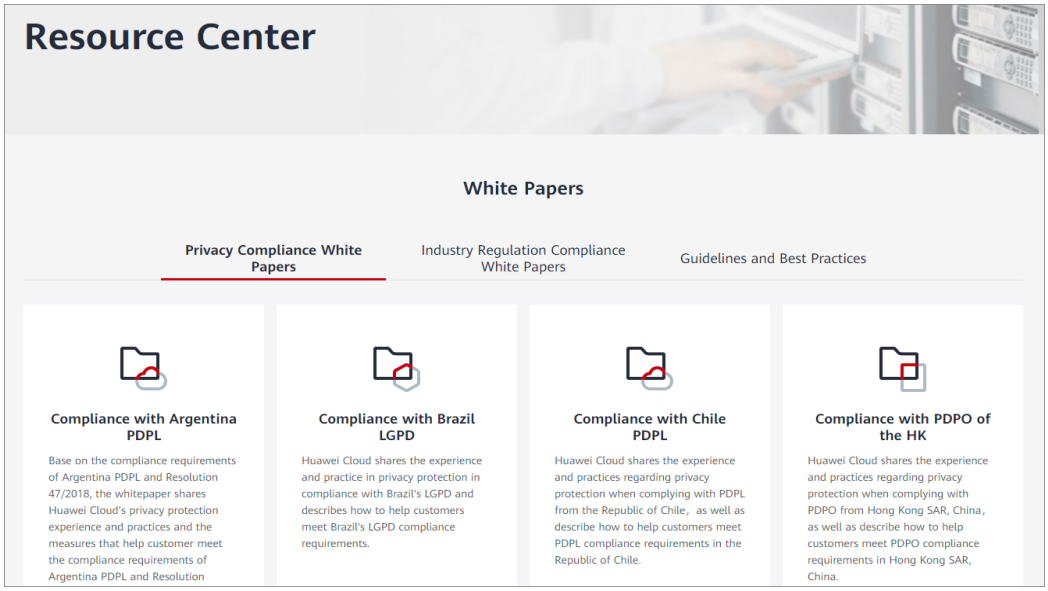
Figure 7-2 Downloading compliance certificates



Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see **Resource Center**.

Figure 7-3 Resource center



8 Permissions

If you need to assign different permissions to personnel in your enterprise to access your RDS resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you to securely access your cloud resources.

With IAM, you can create IAM users and assign permissions to control their access to specific resources. For example, if you want some software developers in your enterprise to use RDS resources but do not want them to delete RDS instances or perform any other high-risk operations, you can create IAM users and grant permission to use RDS instances but not permission to delete them.

If your Huawei account does not require individual IAM users for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account. For more information about IAM, see **IAM Service Overview**.

RDS Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

RDS is a project-level service deployed for specific regions. When you set **Scope** to **Region-specific projects** and select the specified projects in the specified regions, the users only have permissions for RDS instances in the selected projects. If you set **Scope** to **All resources**, the users have permissions for RDS instances in all region-specific projects. When accessing RDS instances, the users need to switch to the authorized region.

You can grant permissions by using roles and policies.

- Roles: A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. Only a limited number of service-level roles are available for authorization. Cloud services depend on each other. When you grant permissions using roles, you also need to attach any existing role dependencies. Roles are not ideal for fine-grained authorization and least privilege access.

- Policies: A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant users only the permission to manage database resources of a certain type. A majority of fine-grained policies contain permissions for specific APIs, and permissions are defined using API actions. For the API actions supported by RDS, see **Permissions and Supported Actions**.

Table 8-1 lists all the system-defined permissions for RDS.

Table 8-1 System-defined permissions for RDS

Role/Policy Name	Description	Type	Dependencies
RDS FullAccess	Full permissions for Relational Database Service	System-defined policy	Purchasing a yearly/monthly DB instance requires the following actions: bss:order:update bss:order:pay To use storage autoscaling, an IAM user must be granted the following actions: • iam:agencies:listAgencies • iam:agencies:createAgency • iam:permissions:listRolesForAgencyOnProject • iam:permissions:grantRoleToGroupOnProject • iam:permissions:grantRoleToAgencyOnProject • iam:roles:listRoles • iam:roles:createRole To create a yearly/monthly instance using a RAM-based shared KMS key, an IAM user must be granted the

Role/Policy Name	Description	Type	Dependencies
			following actions: • iam:agencies:listAgencies • iam:roles:listRoles • iam:agencies:pass • iam:agencies:createAgency • iam:permissions:grantRoleToAgency **RDS FullAccess** already contains the **iam:agencies:listAgencies**, **iam:roles:listRoles**, and **iam:agencies:pass** actions. RDS is a region-level service, and IAM is a global service. If you grant a user the **RDS FullAccess** policy for a specific project, grant **BSS ServiceAgency CreatePolicy** (global service) for the project as well. Granting **RDS FullAccess** for all projects eliminates the need for additional configuration

Role/Policy Name	Description	Type	Dependencies
			when using IAM actions. **BSS ServiceAgency CreatePolicy** contains the following actions: **iam:agencies:createAgency** and **iam:permissions:grantRoleToAgency**.
RDS ReadOnlyAccess	Read-only permissions for Relational Database Service	System-defined policy	N/A
RDS ManageAccess	Database administrator permissions for all operations except deleting RDS resources	System-defined policy	N/A
RDS Administrator	Administrator permissions for RDS	System-defined role	**Tenant Guest** and **Server Administrator** roles, which must be attached in the same project as the **RDS Administrator** role. If only the **RDS Administrator** role is attached, to use storage autoscaling, an IAM user must be granted the actions on storage autoscaling listed in **Table 8-3**.

Table 8-2 lists the common operations supported by system-defined permissions for RDS.

Table 8-2 Common operations supported by system-defined permissions

Operation	RDS FullAccess	RDS ReadOnlyAccess	RDS ManageAccess	RDS Administrator
Creating an RDS DB instance	√	x	√	√
Deleting an RDS DB instance	√	x	x	√
Querying an RDS DB instance list	√	√	√	√

Table 8-3 Common operations and supported actions

Operation	Actions	Remarks
Creating a DB instance	rds:instance:create rds:param:list	Selecting a VPC, subnet, and security group requires the following actions: • vpc:vpcs:list • vpc:vpcs:get • vpc:subnets:get • vpc:securityGroups:get • vpc:securityGroupRules:get Creating an encrypted instance requires the **KMS Administrator** permission for the project. Purchasing a yearly/monthly DB instance requires the following actions: bss:order:update bss:order:pay

Operation	Actions	Remarks
Changing DB instance specifications	rds:instance:modifySpec	N/A
Scaling up storage space	rds:instance:extendSpace	N/A
Changing a DB instance type from single-node to primary/standby	rds:instance:singleToHa	If the original single-node instance is encrypted, you need to configure the **KMS Administrator** permission in the project.
Rebooting a DB instance	rds:instance:restart	N/A
Deleting a DB instance	rds:instance:delete	N/A
Querying a DB instance list	rds:instance:list	N/A
Querying DB instance details	rds:instance:list	Displaying VPCs, subnets, and security groups on the instance details page requires **vpc:*:get** and **vpc:*:list**.
Changing a DB instance password	rds:password:update	N/A
Changing a database port	rds:instance:modifyPort	N/A
Changing a floating IP address	rds:instance:modifyIp	Querying unused IP addresses requires the following actions: vpc:subnets:get vpc:ports:get
Changing a DB instance name	rds:instance:modify	N/A
Changing a maintenance window	rds:instance:modify	N/A
Performing a manual switchover	rds:instance:switchover	N/A

Operation	Actions	Remarks
Changing the replication mode	rds:instance:modifySynchroni-zeModel	N/A
Changing the failover priority	rds:instance:modifyStrategy	N/A
Changing a security group	rds:instance:modifySecurityGro up	N/A
Binding or unbinding an EIP	rds:instance:modifyPublicAcces s	Querying public IP addresses requires the following actions: vpc:publicIps:get vpc:publicIps:list
Modifying the recycling policy	rds:instance:setRecycleBin	N/A
Querying the recycling policy	rds:instance:list	N/A
Enabling or disabling SSL	rds:instance:modifySSL	N/A
Enabling or disabling event scheduler	rds:instance:modifyEvent	N/A
Configuring read/ write splitting	rds:instance:modifyProxy	N/A
Applying for a private domain name	rds:instance:createDns	N/A
Migrating a standby DB instance to another AZ	rds:instance:create	Standby DB instance migration involves operations on the IP address in the subnet. For encrypted DB instances, you need to configure the **KMS Administrator** permission in the project.
Restoring tables to a specified point in time	rds:instance:tableRestore	N/A
Changing host permission	rds:instance:modifyHost	N/A

Operation	Actions	Remarks
Querying hosts of the corresponding database account	rds:instance:list	N/A
Obtaining a parameter template list	rds:param:list	N/A
Creating a parameter template	rds:param:create	N/A
Modifying parameters in a parameter template	rds:param:modify	N/A
Applying a parameter template	rds:param:apply	N/A
Modifying parameters of a specified DB instance	rds:param:modify	N/A
Obtaining the parameter template of a specified DB instance	rds:param:list	N/A
Obtaining parameters of a specified parameter template	rds:param:list	N/A
Deleting a parameter template	rds:param:delete	N/A
Resetting a parameter template	rds:param:reset	N/A
Comparing parameter templates	rds:param:list	N/A
Saving parameters in a parameter template	rds:param:save	N/A
Querying a parameter template type	rds:param:list	N/A
Setting an automated backup policy	rds:instance:modifyBackupPolicy	N/A

Operation	Actions	Remarks
Querying an automated backup policy	rds:instance:list	N/A
Creating a manual backup	rds:backup:create	N/A
Obtaining a backup list	rds:backup:list	N/A
Obtaining the link for downloading a backup file	rds:backup:download	N/A
Deleting a manual backup	rds:backup:delete	N/A
Replicating a backup	rds:backup:create	N/A
Querying the restoration time range	rds:instance:list	N/A
Restoring data to a new DB instance	rds:instance:create	Selecting a VPC, subnet, and security group requires the following actions: vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get vpc:securityGroupRules:get
Restoring data to an existing or original DB instance	rds:instance:restoreInPlace	N/A
Obtaining the binlog clearing policy	rds:binlog:get	N/A
Merging binlog files	rds:binlog:merge	N/A
Downloading a binlog file	rds:binlog:download	N/A
Deleting a binlog file	rds:binlog:delete	N/A
Configuring a binlog clearing policy	rds:binlog:setPolicy	N/A

Operation	Actions	Remarks
Obtaining a database backup file list	rds:backup:list	N/A
Obtaining a backup database list at a specified time point	rds:backup:list	N/A
Querying a database error log	rds:log:list	N/A
Querying a database slow log	rds:log:list	N/A
Downloading a database error log	rds:log:download	N/A
Downloading a database slow log	rds:log:download	N/A
Enabling or disabling the audit log function	rds:auditlog:operate	N/A
Obtaining an audit log list	rds:auditlog:list	N/A
Querying the audit log policy	rds:auditlog:list	N/A
Obtaining the link for downloading an audit log	rds:auditlog:download	N/A
Obtaining a switchover log	rds:log:list	N/A
Creating a database	rds:database:create	N/A
Querying details about databases	rds:database:list	N/A
Querying authorized databases of a specified user	rds:database:list	N/A
Dropping a database	rds:database:drop	N/A
Creating a database account	rds:databaseUser:create	N/A
Querying details about database accounts	rds:databaseUser:list	N/A

Operation	Actions	Remarks
Querying authorized accounts of a specified database	rds:databaseUser:list	N/A
Deleting a database account	rds:databaseUser:drop	N/A
Authorizing a database account	rds:databasePrivilege:grant	N/A
Revoking permissions of a database account	rds:databasePrivilege:revoke	N/A
Viewing a task center list	rds:task:list	N/A
Deleting a task from the task center	rds:task:delete	N/A
Submitting an order for a yearly/monthly DB instance	bss:order:update	Purchasing a yearly/monthly DB instance requires the following actions: bss:order:pay
Managing a tag	rds:instance:modify	Tag-related operations depend on the tms:resourceTags:* permission.

Operation	Actions	Remarks
Configuring autoscaling	rds:instance:extendSpace	To enable storage autoscaling, an IAM user (instead of your Huawei account) must be granted the following actions: • Creating a custom policy: – iam:agencies:listAgencies – iam:agencies:createAgency – iam:permissions:listRolesForAgencyOnProject – iam:permissions:grantRoleToGroupOnProject – iam:roles:listRoles – iam:roles:createRole • Adding system role **Security Administrator**: 1. Select a user group to which the user belongs. 2. Click **Authorize** in the **Operation** column. 3. Add the **Security Administrator** role.
Stopping or starting a DB instance	rds:instance:operateServer	N/A
Modifying the remarks of a database account	rds:databaseUser:update	N/A

9 Constraints

The following tables list the constraints designed to ensure the stability and security of RDS for PostgreSQL.

Specifications and Performance

Table 9-1 Specifications

Item	Constraints	Description
Storage space	• Cloud SSD: 40 GB to 4,000 GB • Extreme SSD: 40 GB to 4,000 GB	-
Maximum connections	It depends on the value of **max_connections**.	For more information, see **What Is the Maximum Number of Connections to an RDS DB Instance?**
IOPS	• Cloud SSD: a maximum of 50,000 • Extreme SSD: a maximum of 128,000	The input/output operations per second (IOPS) supported depends on the I/O performance of Elastic Volume Service (EVS) disks. For details, see the description about ultra-high I/O and extreme SSDs in **Disk Types and Performance** of *Elastic Volume Service Service Overview*.

Quotas

Table 9-2 Quotas

Item	Constraints	Description
Read replica	A maximum of five read replicas can be created for a DB instance.	For more information, see **Introduction to Read Replicas**.
Tags	A maximum of 20 tags can be added for a DB instance.	For more information, see **Managing Tags**.
Free backup space	RDS provides free backup space of the same size as your purchased storage space.	After you pay for the storage space of your DB instance, you will get a backup space of the same size for free. For more information, see **How Is RDS Backup Data Billed?**
Retention period of automated backups	The default value is 7 days. The value ranges from 1 to 732 days.	For more information, see **Configuring a Same-Region Backup Policy**.
Log query	• Error log records: 2,000 • Slow query log records: 2,000	For more information, see **Log Management**.

Naming

Table 9-3 Naming

Item	Constraints
Instance name	• 4 to 64 characters long • Must start with a letter. Only letters (case sensitive), digits, hyphens (-), and underscores (_) are allowed.
Database name	• 1 to 63 characters long • Only letters, digits, and underscores (_) are allowed. It cannot start with **pg** or a digit, and must be different from RDS for PostgreSQL template database names. RDS for PostgreSQL template databases include **postgres**, **template0**, and **template1**.

Item	Constraints
Account name	• 1 to 63 characters long • Only letters, digits, and underscores (_) are allowed. It cannot start with **pg** or a digit, and must be different from system usernames. System users include **rdsAdmin**, **rdsMetric**, **rdsBackup**, **rdsRepl**, **rdsProxy**, **rdsDdm**, and **rdsDisaster**. – **rdsAdmin**: a management account with the highest permissions. It is used to query and modify instance information, rectify faults, migrate data, and restore data. – **rdsRepl**: a replication account, used to synchronize data from the primary instance to the standby instance or read replicas. – **rdsBackup**: a backup account, used for backend backup. – **rdsMetric**: a metric monitoring account used by watchdog to collect database status data. – **rdsProxy**: the proxy account, which is automatically created when read/write splitting is enabled and is used for authentication when a database is connected through a read/write splitting address. – **rdsDdm**: a DDM account. – **rdsDisaster**: a DR account, used to set up cross-region DR.
Backup name	• 4 to 64 characters long • Must start with a letter. Only letters (case sensitive), digits, hyphens (-), and underscores (_) are allowed.
Parameter template name	• 1 to 64 characters long • Only letters (case sensitive), digits, hyphens (-), underscores (_), and periods (.) are allowed.

Security

Table 9-4 Security

Item	Constraints
root permissions	Only the **root** user is available on the instance creation page. RDS for PostgreSQL supports **root** privilege escalation in specific scenarios. For details, see **Privileges of the Root User**.

Item	Constraints
root password	• 8 to 32 characters long • Must contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters (~!@#%^*-_=+?,). For more information, see **Resetting the Administrator Password to Restore Root Access**.
Database port	2100 to 9500 For more information, see **Changing a Database Port**.
Disk encryption	If you enable disk encryption during instance creation, the disk encryption status and the key cannot be changed later. For more information, see **Performing a Server-Side Encryption**.
VPC	The VPC where a DB instance is located cannot be changed after the instance is created.
Security group	• By default, you can create a maximum of 100 security groups in your cloud account. • By default, you can add up to 50 security group rules to a security group. • One RDS DB instance can be associated with multiple security groups, and one security group can be associated with multiple RDS DB instances. • When creating a DB instance, you can select multiple security groups. For better network performance, you are advised to select no more than five security groups. For more information, see **Changing a Security Group**.

Item	Constraints
System account	To provide O&M services, the system automatically creates system accounts when you create RDS for PostgreSQL DB instances. These system accounts are unavailable to you. • **rdsAdmin**: a management account with the highest permission. It is used to query and modify instance information, rectify faults, migrate data, and restore data. • **pg_execute_server_program**: an account that allows executing programs on the database server as the user the database runs as with COPY and other functions which allow executing a server-side program. • **pg_read_all_settings**: an account that reads all configuration variables. • **pg_read_all_stats**: an account that reads all **pg_stat_*** views and uses various extension-related statistics. • **pg_stat_scan_tables**: an account that executes monitoring functions that may take **ACCESS SHARE** locks on tables, potentially for a long time. • **pg_signal_backend**: an account that signals another backend to cancel a query or terminate its session. • **pg_read_server_files**: an account that allows reading files from any location the database can access on the server with COPY and other file-access functions. • **pg_write_server_files**: an account that allows writing to files in any location the database can access on the server with COPY and other file-access functions. • **pg_monitor**: an account that reads and executes various monitoring views and functions. This role is a member of **pg_read_all_settings**, **pg_read_all_stats**, and **pg_stat_scan_tables**. • **rdsRepl**: a replication account, used to synchronize data from the primary instance to the standby instance or read replicas. • **rdsBackup**: a backup account, used for backend backup. • **rdsMetric**: a metric monitoring account used by watchdog to collect database status data.
Instance parameter	To ensure the optimal performance of RDS, you can modify parameters in the parameter template you created as needed. For more information, see **Suggestions on RDS for PostgreSQL Parameter Tuning**.

Instance Operations

Table 9-5 Instance operations

Item	Constraints
Instance deployment	ECSs where DB instances are deployed are not directly visible to you. You can only access the DB instances through IP addresses and database ports.
Data migration	You can migrate data from self-managed PostgreSQL databases, PostgreSQL databases built on other clouds, self-managed Oracle databases, RDS for MySQL, self-managed MySQL databases, or MySQL databases built on other clouds to RDS for PostgreSQL, or from one RDS for PostgreSQL instance to another RDS for PostgreSQL instance. Data migration tools include Data Replication Service (DRS), pg_dump, and Data Admin Service (DAS). You are advised to use DRS because it is easy to use and can complete a migration task in minutes. DRS facilitates data transfer between databases, helping you reduce DBA labor costs and hardware costs. For more information, see **Migration Solution Overview**.
Primary/Standby replication	RDS for PostgreSQL uses a primary/standby dual-node replication cluster. You do not need to set up replication additionally. The standby DB instance is not visible to you and therefore you cannot access it directly.
High CPU usage	If the CPU usage is high or close to 100%, data read/write and database access will become slow, and an error will be reported during data deletion. For details, see **High CPU Usage of RDS for PostgreSQL DB Instances**.
Rebooting a DB instance	DB instances cannot be rebooted through commands. They must be rebooted through the RDS console.
Stopping or starting a DB instance	• You can temporarily stop pay-per-use instances to save money. For more information, see **Stopping an Instance**. • After stopping your instance, you can restart it to begin using it again.
Viewing backups	You can download automated and manual backups for local storage. To download a backup, you can use OBS Browser+, the current browser, or the download URL. For more information, see **Downloading a Full Backup File**.
Log management	RDS for PostgreSQL logging is enabled by default and cannot be disabled.

Item	Constraints
Recycle bin	RDS allows you to move unsubscribed yearly/monthly DB instances and deleted pay-per-use DB instances to the recycle bin. You can rebuild a DB instance that was deleted up to 7 days ago from the recycle bin.

Privileges of the Root User

RDS for PostgreSQL provides permissions for the **root** user. To create objects on an RDS for PostgreSQL database without operation risks, escalate your account to root privileges when necessary.

The following table describes root privilege escalation in different versions.

Table 9-6 Privileges of the root user

Version	Whether to Escalate Privileges	Initial Version for Privilege Escalation
pgcore9	No	N/A
pgcore10	No	N/A
pgcore11	Yes	11.11
pgcore12	Yes	12.6
pgcore13	Yes	13.2
pgcore14	Yes	14.4
pgcore15	Yes	15.4
pgcore16	Yes	16.2

Escalate to root privileges when you need to:

- Create an event trigger.
- Create a wrapper.
- Create a logical replication publication.
- Create a logical replication subscription.
- Query and maintain replication sources.
- Create a replication user.
- Create a full-text index template and parser.
- Run the **vacuum** command on a system table.
- Run the **analyze** command on a system table.
- Create an extension.

- Grant an object permission to a user.

10 Related Services

The following figure shows the relationship between RDS and other services.

Figure 10-1 Relationship between RDS and other services

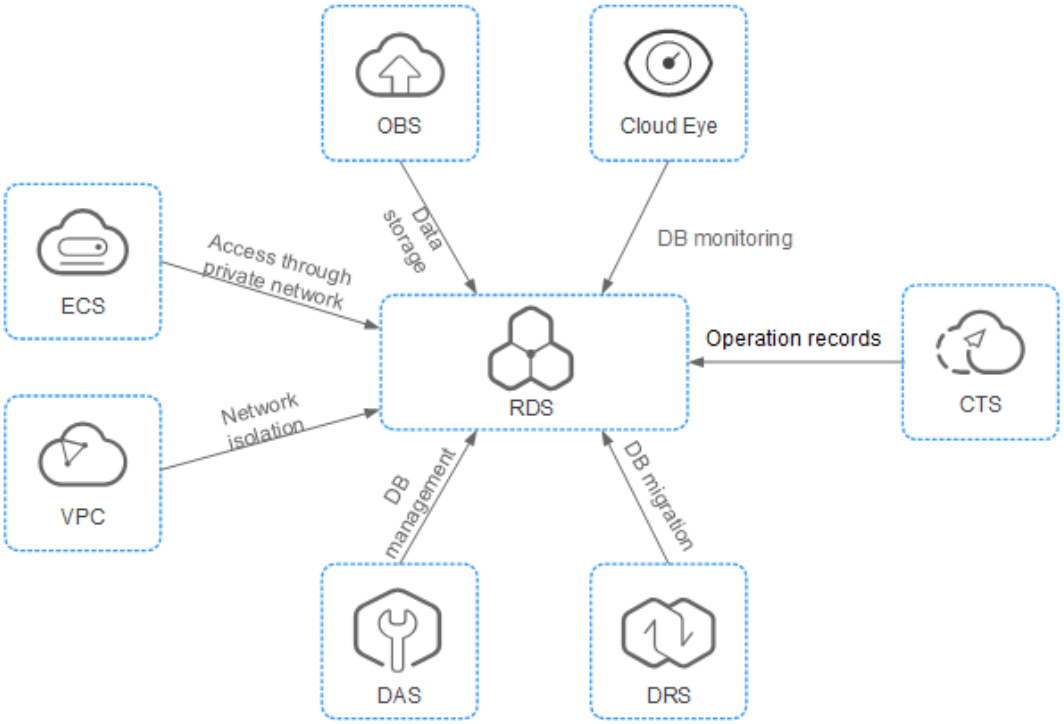


Table 10-1 Related services

Service Name	Description
Elastic Cloud Server (ECS)	Enables you to access RDS DB instances through an internal network. You can then access applications faster and you do not need to pay for public network traffic.
Virtual Private Cloud (VPC)	Isolates your networks and controls access to your RDS DB instances.

Service Name	Description
Object Storage Service (OBS)	Stores automated and manual backups of your RDS DB instances.
Cloud Eye	Monitors RDS resources in real time and reports alarms and warnings promptly.
Cloud Trace Service (CTS)	Records operations on cloud service resources for query, audit, and backtrack.
Data Replication Service (DRS)	Smoothly migrates databases to the cloud.
Data Admin Service (DAS)	Provides a visualized GUI interface for you to connect to and manage cloud databases.

11 Basic Concepts

DB Instances

The smallest management unit of RDS is DB instance. A DB instance is an isolated database environment on the cloud. An instance ID uniquely identifies a DB instance. A DB instance can contain multiple user-created databases and can be accessed using tools and applications. Each database name is unique.

A default administrator account is provided when you purchase a DB instance. You can use this account to create databases and database users and assign permissions to them. You can set the administrator password when or after purchasing a DB instance. If you forget the administrator password, you can reset it.

You can use RDS to create and manage DB instances running various DB engines. For details about DB instance types, specifications, engines, versions, and statuses, see **DB Instance Description**.

DB Instance Classes

The DB instance class determines the compute (vCPUs) and memory capacity (memory size) of a DB instance. For details, see **x86-based Instance Classes**.

Automated Backups

When you create a DB instance, an automated backup policy is enabled by default, but after the DB instance is created, you can modify the policy if needed. RDS will automatically create backups for DB instances based on your settings.

Manual Backups

Manual backups are user-initiated full backups of DB instances. They are retained until you delete them manually.

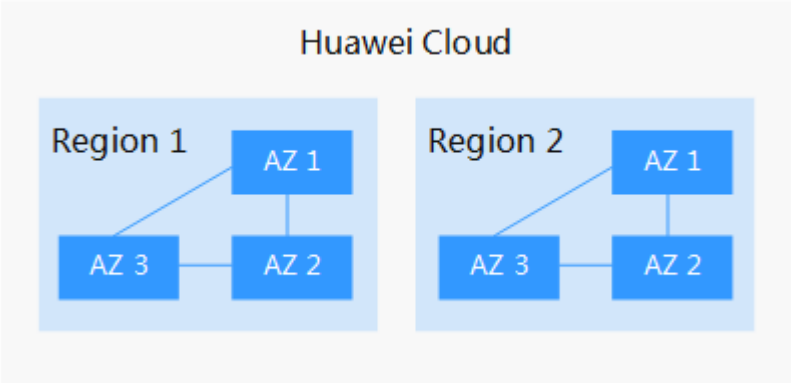
Regions and AZs

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are defined by their geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), can all be shared within a given region. Regions are classified as universal regions and dedicated regions. A universal region provides cloud services for all users. A dedicated region provides services of only a specific type or only for specific users.
- An AZ contains one or multiple physical data centers. Each AZ has its own independent cooling, fire extinguishing, moisture-proofing, and electrical facilities. Within an AZ, compute, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers so you can build cross-AZ high-availability systems.

Figure 11-1 shows the relationship between regions and AZs.

Figure 11-1 Regions and AZs



Huawei Cloud provides services in many regions around the world. You can select a region and AZ as needed. For more information, see **Global Products and Services**.

Projects

Projects are used to group and isolate OpenStack resources (compute, storage, and network resources). A project can be a department or a project team. Multiple projects can be created for a single account.

