TaurusDB for PostgreSQL

Service Overview

Issue 01

Date 2025-11-14

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 What Is TaurusDB for PostgreSQL?

TaurusDB for PostgreSQL is a cloud-native database developed by Huawei. It is fully compatible with open-source PostgreSQL. Leveraging Huawei Cloud's latest high-performance compute and storage infrastructure and Babelfish's compatibility with Microsoft SQL Server, TaurusDB for PostgreSQL provides a high-performance, highly elastic, secure, and reliable database service.

This product is in the open beta test (OBT) phase. To use it, submit a service ticket.

Why TaurusDB for PostgreSQL?

- Open-source ecosystem

  TaurusDB for PostgreSQL is fully compatible with open-source PostgreSQL and provides various extensions. You can migrate native PostgreSQL applications to TaurusDB for PostgreSQL with no refactorings.

- Heterogeneous compatibility

  With Babelfish, TaurusDB for PostgreSQL supports T-SQL statements and the Tabular Data Stream (TDS) protocol. You can migrate Microsoft SQL Server applications to TaurusDB for PostgreSQL. Only minimal code changes are needed. There is no need to change the drivers.

Using TaurusDB for PostgreSQL

You can create and manage DB instances on the management console.

To help you use TaurusDB for PostgreSQL, see **Basic Concepts**.

2 Advantages

3 Product Series

TaurusDB for PostgreSQL instances are classified into the following types:

- Single-node
- Primary/Standby

Table 3-1 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 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 synchronously 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

Comparison

- Single-node instances: Different from primary/standby instances that have two database nodes, a single-node instance has only one node, reducing the price to half of a primary/standby instance. If the node fails, the restoration will take a long time. Therefore, single-node instances are not recommended for workloads that are highly sensitive to database availability.
- Primary/Standby instances: use the standby database node only for failover and restoration. The standby database node does not provide services. If the primary node fails, the standby node can take over services immediately. Since standby nodes cause extra performance overhead, the performance of single-node instances is similar to or even higher than primary/standby instances.

4 DB Instance Description

4.1 DB Instance Types

The smallest management unit of TaurusDB for PostgreSQL is the 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 database. You can easily create or modify DB instances using the management console. TaurusDB for PostgreSQL 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 4-1 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 specifications. The primary and standby instances can be deployed in different AZs.	• When a primary instance is being created, a standby instance is provisioned synchronously to provide data redundancy. The standby instance is invisible to you after being created. • If a failover occurs due to a primary instance failure, your database client will be disconnected briefly. You need to reconnect the client to the instance. • TaurusDB for PostgreSQL uses asynchronous replication by default.

You can use TaurusDB for PostgreSQL to create and manage DB instances running various DB engines.

For details about the differences between different DB instance types, see **Product Series**.

4.2 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

TaurusDB for PostgreSQL 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 4-2 Performance comparison

Item	Cloud SSD	Extreme SSD
I/O performance	Sub-par 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

4.3 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 4-3 DB instance statuses

Status	Description
Available	A DB instance is available.
Abnormal	A DB instance is abnormal.
Creating	A DB instance is being created.
Creation failed	A DB instance has failed to be created.
Rebooting	A DB instance is being rebooted.
Changing port	A DB instance port is being changed.
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.

Status	Description
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.
Deleted	A DB instance has been deleted and will not be displayed in the instance list.
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.

5 DB Instance Specifications

5.1 x86-based Instance Specifications

TaurusDB for PostgreSQL supports the following x86-based instance specifications for the cloud SSD storage type: general-purpose (recommended) and dedicated (recommended). For details, see **Table 5-1** and **Table 5-2**.

Table 5-1 x86-based instance specifications

Instance Specifications	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. It is a cost-effective option and suitable for scenarios where stable performance is not critical.	Suitable for scenarios that have high requirements on cost-effectiveness.	These instance specifications are available in the following regions: • AP-Singapore • AP-Bangkok • TR-Istanbul • LA-Sao Paulo1 • ME-Riyadh

Instance Specifications	Description	Scenario	Constraints
Dedicated (recommended)	Your instance gets dedicated vCPUs and memory, so the performance is stable. It is not affected by other instances on the same physical machine. Dedicated instances are good for scenarios that require stable performance.	Suitable for core database scenarios such as e-commerce, gaming, finance, government, and enterprise applications.	

Details of General-Purpose and Dedicated Instance Specifications

Table 5-2 Details of general-purpose and dedicated instance specifications

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

Instance Specifications	Specification Code for Primary/Standby Instances	Specification Code for Single-Node Instances	vCPUs	Memory (GB)
	taurus.pg.x1.xlarge.2.ha	-	4	8
	taurus.pg.x1.xlarge.4.ha	-	4	16
	taurus.pg.x1.xlarge.8.ha	taurus.pg.x1.xlarge.8	4	32
	taurus.pg.x1.2xlarge.2.ha	taurus.pg.x1.2xlarge.2	8	16
	taurus.pg.x1.2xlarge.4.ha	taurus.pg.x1.2xlarge.4	8	32
	taurus.pg.x1.2xlarge.8.ha	taurus.pg.x1.2xlarge.8	8	64
	taurus.pg.x1.4xlarge.2.ha	taurus.pg.x1.4xlarge.2	16	32
	taurus.pg.x1.4xlarge.4.ha	taurus.pg.x1.4xlarge.4	16	64
	taurus.pg.x1.4xlarge.8.ha	taurus.pg.x1.4xlarge.8	16	128
	taurus.pg.x1.8xlarge.2.ha	taurus.pg.x1.8xlarge.2	32	64
	taurus.pg.x1.8xlarge.4.ha	taurus.pg.x1.8xlarge.4	32	128
	taurus.pg.x1.8xlarge.8.ha	taurus.pg.x1.8xlarge.8	32	256
	taurus.pg.x1.16xlarge.2.ha	taurus.pg.x1.16xlarge.2	64	128
	taurus.pg.x1.16xlarge.4.ha	taurus.pg.x1.16xlarge.4	64	256
	taurus.pg.x1.16xlarge.8.ha	taurus.pg.x1.16xlarge.8	64	512
	taurus.pg.x1.24xlarge.2.ha	taurus.pg.x1.24xlarge.2	96	192
	taurus.pg.x1.24xlarge.4.ha	taurus.pg.x1.24xlarge.4	96	384
	taurus.pg.x1.24xlarge.8.ha	taurus.pg.x1.24xlarge.8	96	768

Instance Specifications	Specification Code for Primary/Standby Instances	Specification Code for Single-Node Instances	vCPUs	Memory (GB)
	taurus.pg.x1.32xlarge.2.ha	taurus.pg.x1.32xlarge.2	128	256
	taurus.pg.x1.32xlarge.4.ha	taurus.pg.x1.32xlarge.4	128	512
	taurus.pg.x1.32xlarge.8.ha	taurus.pg.x1.32xlarge.8	128	1,024

The DB instance specifications vary according to site requirements.

6 Security

6.1 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 6-1**.

- **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 6-1 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 6-1**, 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.

6.2 Identity Authentication and Access Control

Identity Authentication

When you access TaurusDB for PostgreSQL, 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 TaurusDB for PostgreSQL permissions. IAM provides identity authentication, permissions management, and access control, helping you secure access to your Huawei Cloud resources. IAM users can use TaurusDB for PostgreSQL resources only after their accounts and passwords are verified. For details, see **Creating an IAM User and Logging 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 ECSs and TaurusDB for PostgreSQL instances that have the same security requirements and are mutually trusted in 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 TaurusDB for PostgreSQL instances.

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

6.3 Data Protection

TaurusDB for PostgreSQL provides a series of methods and features to ensure data security and reliability.

Table 6-1 TaurusDB for PostgreSQL data protection methods and features

Method	Description
Secure Sockets Layer (SSL)	SSL is supported to ensure data transmission security.
Cross-AZ deployment	To ensure high availability, TaurusDB for PostgreSQL allows you to deploy primary and standby DB instances across AZs. AZs are physically isolated but interconnected through an internal network.

6.4 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 TaurusDB for PostgreSQL for auditing.

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

- 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.

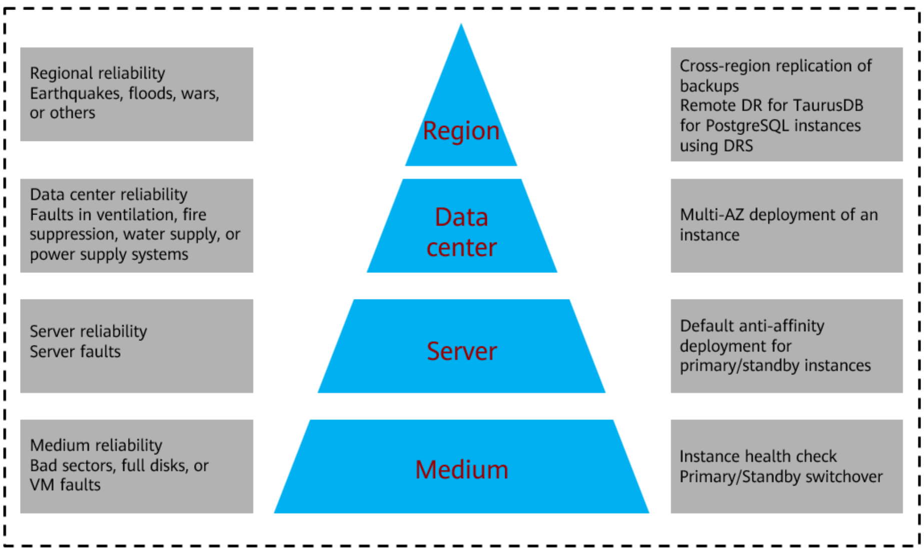
Logs

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

6.5 Resilience

TaurusDB for PostgreSQL uses EVS disks to store data, providing three-copy storage and 99.9999999% data durability. It also provides features like cross-region replication and intra-AZ anti-affinity, to guarantee reliability and availability of your instances.

Figure 6-2 Reliability architecture



6.6 Fault Recovery

TaurusDB for PostgreSQL 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).

Multiple-AZ Deployment

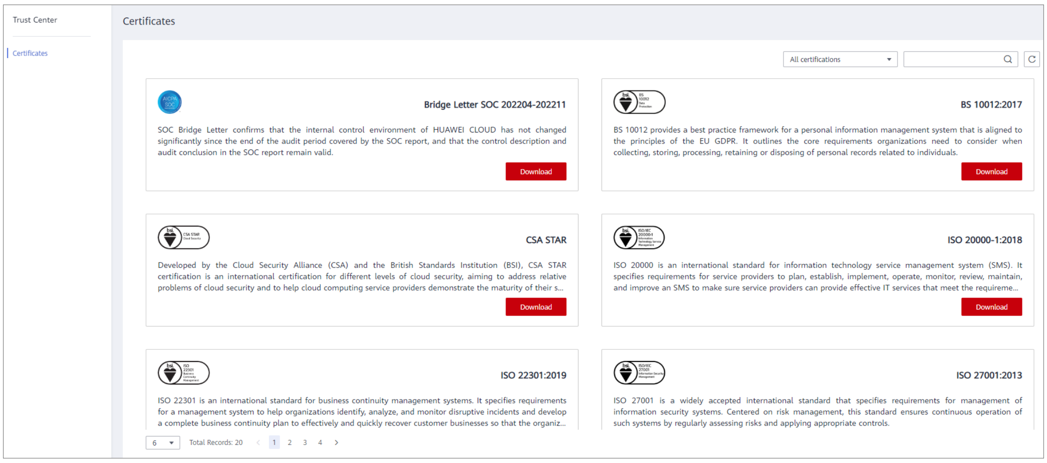
An AZ is a physical region where resources have their own independent power supply and networks. AZs are physically isolated but interconnected through a private network. You can deploy primary and standby DB instances in a single AZ or across AZs to achieve failover and high availability.

6.7 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**.

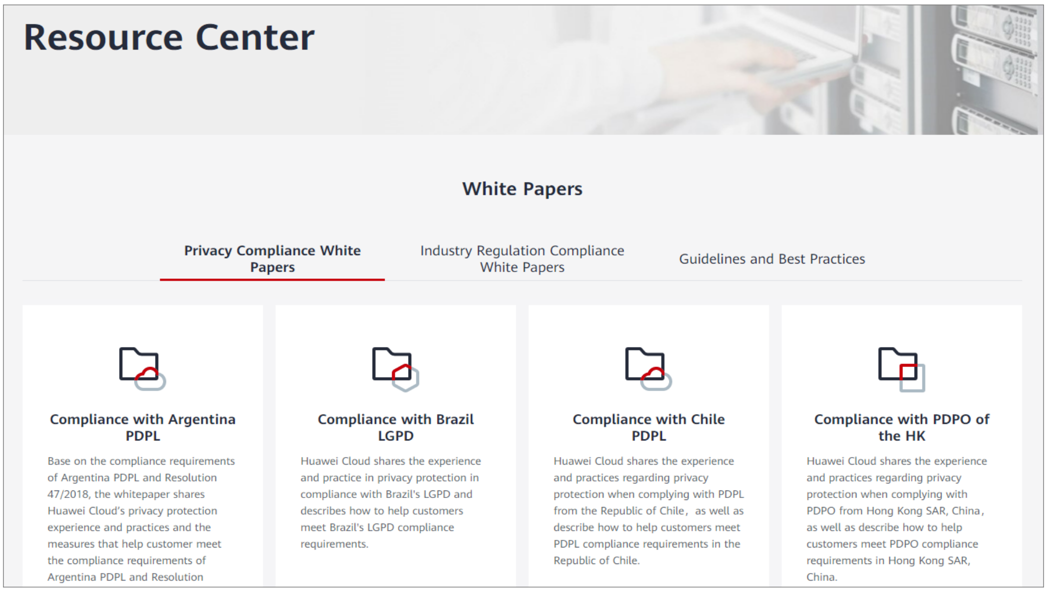
Figure 6-3 Downloading compliance certificates



Resource Center

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

Figure 6-4 Resource center



7 Permissions

If you need to assign different permissions to personnel in your enterprise to access your TaurusDB for PostgreSQL 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 secure access to your Huawei 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 TaurusDB for PostgreSQL resources but do not want them to delete TaurusDB for PostgreSQL resources or perform any other high-risk operations, you can create IAM users for the software developers and grant them only the permissions required for using TaurusDB for PostgreSQL resources.

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**.

TaurusDB for PostgreSQL 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.

TaurusDB for PostgreSQL is a project-level service deployed in specific physical regions. When you set **Scope** to **Region-specific projects** and select the specified projects in the specified regions, the users only have permissions for TaurusDB for PostgreSQL instances in the selected projects. If you set **Scope** to **All resources**, the users have permissions for TaurusDB for PostgreSQL instances in all region-specific projects. When accessing TaurusDB for PostgreSQL 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 a certain type of database resources.

Table 7-1 lists all the system-defined permissions for TaurusDB for PostgreSQL.

Table 7-1 System-defined permissions for TaurusDB for PostgreSQL

Role/Policy Name	Description	Type	Dependencies
TaurusDB FullAccess	Full permissions for TaurusDB for PostgreSQL	System-defined policy	**TaurusDB FullAccess** already contains the **iam:agencies:listAgencies**, **iam:roles:listRoles**, and **iam:agencies:pass** actions. TaurusDB for PostgreSQL is a region-level service, and IAM is a global service. If you want to grant **TaurusDB FullAccess** to a project, grant **BSS ServiceAgencyReadPolicy** (global service) to it as well. Granting **TaurusDB FullAccess** to all projects eliminates the need for additional configuration when using IAM actions. **BSS ServiceAgencyCreatePolicy** contains the following actions: **iam:agencies:createAgency** and **iam:permissions:grantRoleToAgency**.

Role/Policy Name	Description	Type	Dependencies
TaurusDB ReadOnlyAccess	Read-only permissions for TaurusDB for PostgreSQL	System-defined policy	N/A

Table 7-2 lists the common operations supported by system-defined permissions for TaurusDB for PostgreSQL.

Table 7-2 Common operations supported by system-defined permissions

Operation	TaurusDB FullAccess	TaurusDB ReadOnlyAccess
Creating a TaurusDB for PostgreSQL instance	√	x
Deleting a TaurusDB for PostgreSQL instance	√	x
Querying TaurusDB for PostgreSQL instances	√	√

Table 7-3 Common operations and supported actions

Operation	Actions	Remarks
Creating a DB instance	gaussdb:instance:create gaussdb:param:list	To select a VPC, subnet, and security group, configure the following actions: vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get vpc:securityGroupRules:get To create an encrypted instance, configure the KMS Administrator permission for the project. To purchase a yearly/monthly DB instance, configure the following actions: bss:order:update bss:order:pay
Scaling up storage space	gaussdb:instance:extendSpace	N/A
Rebooting a DB instance	gaussdb:instance:restart	N/A
Deleting a DB instance	gaussdb:instance:delete	N/A
Querying a DB instance list	gaussdb:instance:list	N/A
Querying DB instance details	gaussdb:instance:list	If the VPC, subnet, and security group are displayed in the DB instance list, you need to configure vpc:*:get and vpc:*:list.
Changing a DB instance password	gaussdb:password:update	N/A
Changing a database port	gaussdb:instance:modifyPort	N/A
Changing a DB instance name	gaussdb:instance:modify	N/A

Operation	Actions	Remarks
Changing the replication mode	gaussdb:instance:modifySynchronizeModel	N/A
Changing the failover priority	gaussdb:instance:modifyStrategy	N/A
Modifying the recycling policy	gaussdb:instance:setRecycleBin	N/A
Restoring tables to a specified point in time	gaussdb:instance:tableRestore	N/A
Obtaining a parameter template list	gaussdb:param:list	N/A
Creating a parameter template	gaussdb:param:create	N/A
Modifying parameters in a parameter template	gaussdb:param:modify	N/A
Applying a parameter template	gaussdb:param:apply	N/A
Modifying parameters of a specified DB instance	gaussdb:param:modify	N/A
Obtaining the parameter template of a specified DB instance	gaussdb:param:list	N/A
Obtaining parameters of a specified parameter template	gaussdb:param:list	N/A
Deleting a parameter template	gaussdb:param:delete	N/A
Resetting a parameter template	gaussdb:param:reset	N/A
Comparing parameter templates	gaussdb:param:list	N/A
Saving parameters in a parameter template	gaussdb:param:save	N/A

Operation	Actions	Remarks
Querying a parameter template type	gaussdb:param:list	N/A
Setting an automated backup policy	gaussdb:instance:modifyBackupPolicy	N/A
Querying an automated backup policy	gaussdb:instance:list	N/A
Creating a manual backup	gaussdb:backup:create	N/A
Obtaining a backup list	gaussdb:backup:list	N/A
Obtaining the link for downloading a backup file	gaussdb:backup:download	N/A
Querying the restoration time range	gaussdb:instance:list	N/A
Restoring data to a new DB instance	gaussdb:instance:create	To select a VPC, subnet, and security group, configure 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	gaussdb:instance:restoreInPlace	N/A
Obtaining a database backup file list	gaussdb:backup:list	N/A
Obtaining a backup database list at a specified time point	gaussdb:backup:list	N/A
Querying a database error log	gaussdb:log:list	N/A

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

Operation	Actions	Remarks
Revoking permissions of a database account	gaussdb:databasePrivilege:revoke	N/A
Viewing a task center list	gaussdb:task:list	N/A
Deleting a task from the task center	gaussdb:task:delete	N/A
Managing a tag	gaussdb:instance:modify	Tag-related operations depend on the tms:resourceTags:* permission.
Stopping an instance	gaussdb:instance:stop	N/A
Starting an instance	gaussdb:instance:start	N/A
Modifying the remarks of a database account	gaussdb:databaseUser:update	N/A

8 Constraints

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

Specifications and Performance

Table 8-1 Specifications

Item	Constraints
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**.
IOPS	• Cloud SSD: a maximum of 50,000 • Extreme SSD: a maximum of 128,000

Quotas

Table 8-2 Quotas

Item	Constraints
Tags	A maximum of 20 tags can be added for a DB instance.
Free backup space	TaurusDB for PostgreSQL provides free backup space of the same size as your purchased storage space.
Retention period of automated backups	The default value is 7 days. The value ranges from 1 to 732 days.
Log query	• Error log records: 2,000 • Slow query log records: 2,000

Naming

Table 8-3 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 TaurusDB for PostgreSQL template database names. TaurusDB for PostgreSQL template databases include **postgres**, **template0**, and **template1**.
Account name	● 1 to 128 characters long ● Only letters, digits, hyphens (-), and underscores (_) are allowed. It must be different from system accounts. System accounts include **rdsadmin**, **rdsuser**, **rdsbackup**, and **rdsmirror**.
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 8-4 Security

Item	Constraints
root permissions	Only the **root** user is available on the instance creation page. TaurusDB for PostgreSQL supports **root** privilege escalation in specific scenarios. For details, see **Privileges of the root User**.
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 (~!@#%^*-_=+?,).
Database port	2100 to 9500

Item	Constraints
Disk encryption	If you enable disk encryption during instance creation, the disk encryption status and the key cannot be changed later.
VPC	After a TaurusDB for PostgreSQL instance is created, the VPC cannot be changed.
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 TaurusDB for PostgreSQL instance can be associated with one security group, and one security group can be associated with multiple TaurusDB for PostgreSQL instances.

Item	Constraints
System account	To provide O&M services, the system automatically creates system accounts when you create TaurusDB for PostgreSQL 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 files to 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. ● **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 optimal performance of TaurusDB for PostgreSQL, you can modify parameters in the parameter template you created as needed.

Instance Operations

Table 8-5 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 TaurusDB for PostgreSQL, or from one TaurusDB for PostgreSQL instance to another. 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.
Primary/Standby replication	TaurusDB 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.
Rebooting a DB instance	TaurusDB for PostgreSQL instances cannot be rebooted through commands. They must be rebooted on the management console.
Stopping or starting a DB instance	● You can temporarily stop pay-per-use instances to save money. ● 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.
Log management	TaurusDB for PostgreSQL logging is enabled by default and cannot be disabled.

Privileges of the root User

TaurusDB for PostgreSQL provides privileges for the **root** user. To create objects on a TaurusDB 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 8-6 Privileges of the **root** user

Version	Whether to Escalate Privileges	Initial Version for Privilege Escalation
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 catalog.
- Run the **analyze** command on a system catalog.
- Create an extension.
- Grant an object permission to a user.

9 Related Services

Table 9-1 Related services

Service Name	Description
Elastic Cloud Server (ECS)	Enables you to access TaurusDB for PostgreSQL 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 TaurusDB for PostgreSQL instances.
Object Storage Service (OBS)	Stores automated and manual backups of your TaurusDB for PostgreSQL instances.
Data Replication Service (DRS)	Smoothly migrates databases to the cloud.

10 Basic Concepts

DB Instances

The smallest management unit of TaurusDB for PostgreSQL is a 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 TaurusDB 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**.

Instance Specifications

Instance specifications determine the compute (vCPUs) and memory capacity (memory size) of a DB instance. For details, see **x86-based Instance Specifications**.

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. TaurusDB for PostgreSQL will automatically create full 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.

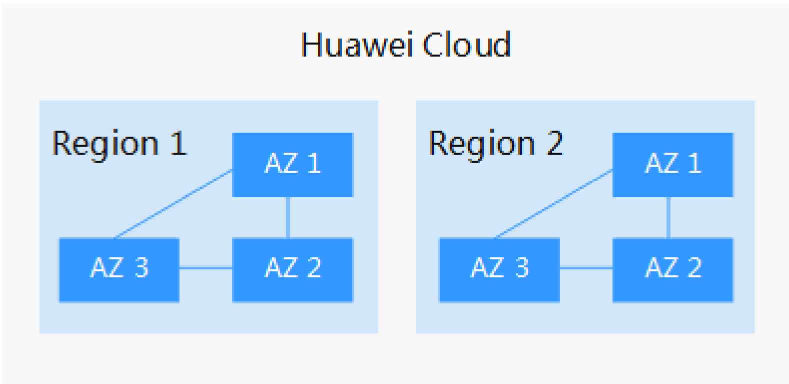
Regions and AZs

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 10-1 shows the relationship between regions and AZs.

Figure 10-1 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.

