TaurusDB

Service Overview

Issue 01

Date 2025-02-28

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.

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?

TaurusDB is an enterprise-grade cloud-native database fully compatible with MySQL. It decouples compute from storage and uses Huawei-developed Data Function Virtualization (DFV), which scales to up to 128 TB per instance. A failover can be complete within seconds. It provides the superior performance and high availability of a commercial database at the price of an open-source database.

For details about the DB engines and versions supported by TaurusDB, see **DB Engines and Versions**.

Progressive Knowledge

You can go to **Progressive Knowledge** to learn about the basic concepts and usage of TaurusDB.

How to Use TaurusDB

You can create and manage TaurusDB instances on the web-based **management console**.

To help you make the most of TaurusDB, see **Advantages**.

Advantages

- Performance
  - By decoupling compute from storage and using a "log as database" architecture, TaurusDB delivers seven times the performance of open-source databases.
  - Remote Direct Memory Access (RDMA) is used for data transfer in database systems to break through the I/O performance bottleneck.
  - TaurusDB supports kernel features, such as query result cache, query plan cache, and online DDL, to improve user experience.
- Scalability
  - Horizontal scaling: In addition to a primary node, you can add up to 15 read replicas for an instance to handle high-concurrency requests.
  - Vertical scaling: You can scale up or down instance specifications as needed.

- Availability
  - You can deploy an instance across AZs or regions to improve DR capabilities.
  - Three copies of the data are stored to ensure reliability.
  - TaurusDB uses shared distributed storage. If the primary node fails, one of the read replicas is promoted to primary with an RPO of zero.
  - The latency between the primary node and its read replicas is several milliseconds, ensuring high availability.
- Security
  - With shared distributed storage, TaurusDB can achieve service recovery within seconds and near-zero data loss.
  - VPCs, security groups, SSL connections, and data encryption are used to strictly control access security.
  - TaurusDB has passed over 15 security certifications, including ISO 27001, CSA, Trusted Cloud, and China's level-3 certification for information security protection. It is the first in China to obtain the highest NIST CSF certification.
- Compatibility

  TaurusDB is fully compatible with MySQL. You can easily migrate your MySQL databases to TaurusDB without refactoring existing applications.
- Backup
  - Snapshots are created in seconds and can be used to restore data quickly.
  - The storage system enables data to be restored to any point in time without replaying incremental logs.
- Storage
  - Based on Huawei-developed DFV distributed storage, TaurusDB supports up to 128 TB of storage.
  - TaurusDB automatically grows storage as needed.
- Operator pushdown

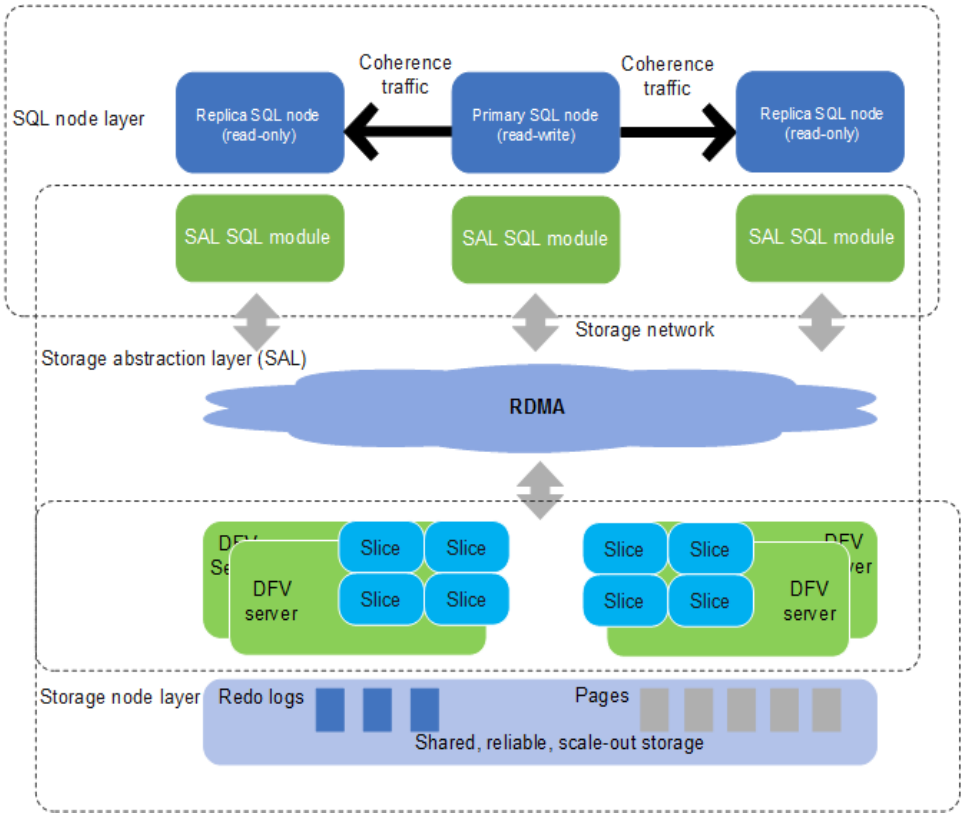
  Column projection, condition filtering, and aggregation calculation are pushed down to a distributed storage layer for parallel processing. This improves query performance and reduces network traffic and the load on computes nodes. Operator pushdown is integrated with parallel query to execute the entire process in parallel.

2 Product Architecture

The TaurusDB architecture consists of three layers. From bottom to top, they are:

1. Storage node layer: This layer is built on Huawei Data Function Virtualization (DFV) storage, which provides distributed, strong-consistency, and high-performance storage. This layer ensures data reliability and horizontal scalability, with a reliability rate of no less than 99.999999999% (11 nines). DFV is a high-performance and high-reliability distributed storage system that is vertically integrated with databases. Storage clusters are deployed in pools to improve storage utilization and build a data-centric full-stack data service architecture.
2. Storage abstraction layer: This layer is key to ensuring database performance. It connects to the DFV storage pool below it and provides semantics upward for ensuring efficient storage scheduling. Table file operations are abstracted into distributed storage.
3. SQL parsing layer: This layer is fully compatible with open-source MySQL 8.0, allowing you to easily migrate your workloads from MySQL to TaurusDB using MySQL-native syntax and tools. This saves you time and efforts. In addition to full compatibility with MySQL, TaurusDB comes with an optimized kernel and a hardened system.

Figure 2-1 Product architecture



3 Basic Concepts

Before using TaurusDB, you should be familiar with the following concepts.

Cluster Instances

TaurusDB uses a decoupled compute and storage architecture that auto-scales up to 128 TB per DB instance. A cluster DB instance contains a primary node and up to 15 read replicas which can be created in minutes.

Single-Node Instances

A single-node instance contains only one primary node and there are no read replicas. Single-node instances do not involve data synchronization between nodes and can easily ensure atomicity, consistency, isolation, and durability of transactions. Single-node instances cannot ensure high availability. If a fault occurs, the services cannot recover in a timely manner.

Instance Specifications

Each instance is configured with compute and memory resources, for example, 16 vCPUs and 64 GB.

Regions and AZs

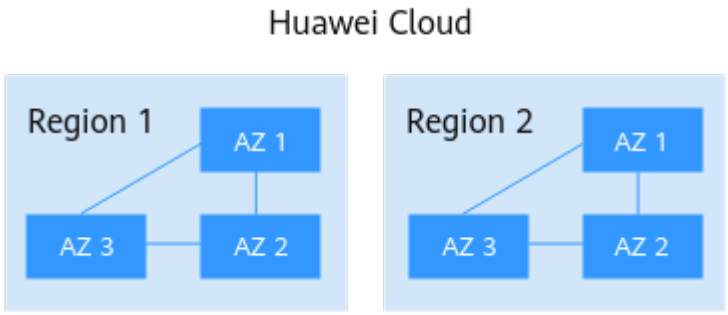
A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- 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 can be universal or dedicated. A universal region provides all sorts of cloud services for all users. A dedicated region provides only services of a given 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 3-1 shows the relationship between regions and AZs.

Figure 3-1 Regions and AZs



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

Compatibility Between TaurusDB and Browsers

For details, see **Which Browsers Are Supported?**

4 Advantages

TaurusDB is an enterprise-grade cloud database with decoupled compute and storage.

Performance

TaurusDB can deliver seven times the performance of open-source MySQL for certain workloads and achieve millions of queries per second (QPS).

Scalability

- Horizontal scaling: You can add up to 15 read replicas within minutes as required.
- Vertical scaling: You can scale up or down instance specifications to handle uncertain workload growth.
- Storage scaling: The storage automatically grows as the amount of data in your database increases. An instance supports up to 128 TB of storage.

Availability

TaurusDB supports cross-AZ and remote disaster recovery for financial-grade reliability.

There are three data copies to ensure reliability.

Compatibility

TaurusDB is fully compatible with MySQL, so there is no need to refactor applications.

Cost

Only 10% of the commercial databases

Middleware-free Architecture

When the service performance is normal, Distributed Database Middleware (DDM) is not required.

5 Instance Description

5.1 DB Engines and Versions

Table 5-1 lists the DB engines and versions supported by TaurusDB.

Table 5-1 DB engines and versions

DB Engine	Version	Minor Kernel Version
TaurusDB	MySQL 8.0	• 2.0.57.240900 • 2.0.54.240600 • 2.0.51.240300 • 2.0.48.231200 • 2.0.45.230900 • 2.0.42.230600 • 2.0.39.230300 • 2.0.28.18 • 2.0.28.17 • 2.0.28.16 • 2.0.28.15 • 2.0.28.12 • 2.0.28.10 • 2.0.28.9 • 2.0.28.7 • 2.0.28.4 • 2.0.28.1

NOTE

For details about the updates in each minor kernel version, see **TaurusDB Kernel Version Release History**.

5.2 Instance Specifications

The CPU architecture of TaurusDB instances can be x86 or Kunpeng.

- x86 instances use Intel® Xeon® Scalable processors and feature robust and stable computing performance. When working on high-performance networks, the instances provide the additional performance and stability that enterprise-class applications demand.
- Kunpeng instances use Kunpeng 920 processors and 25GE high-speed intelligent NICs for powerful compute and high-performance networks, making them an excellent choice for enterprises needing cost-effective, secure, and reliable cloud services.

Different CPU architectures support different instance specifications. The details are as follows.

x86 Instance Specifications

x86 instances support both dedicated and general-purpose specifications.

- **Dedicated**: 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.
- **General-purpose**: The vCPUs and memory are shared with other general-purpose instances on the same physical machine. vCPU usage is maximized through resource overcommitment. General-purpose instances are cost-effective and suitable for scenarios where stable performance is not critical.

Table 5-2 x86 instance specifications

Specifications	Specification Code	vCPUs	Memory (GB)	Supported Regions
Dedicated	gaussdb.mysql.large.x86.4	2	8	CN North-Beijing4, CN North-Ulanqab1
				CN East-Shanghai1
				CN South-Guangzhou
				CN Southwest-Guiyang1
				CN-Hong Kong
				AP-Singapore, AP-Jakarta
				ME-Riyadh

Specifications	Specification Code	vCPUs	Memory (GB)	Supported Regions
				AF-Johannesburg
				TR-Istanbul
	gaussdb.mysql.large.x86.8	2	16	CN North-Beijing4, CN North-Ulanqab1
				CN Southwest-Guiyang1
				AP-Singapore
				AF-Johannesburg
	gaussdb.mysql.xlarge.x86.4	4	16	CN North-Beijing4, CN North-Ulanqab1
				CN East-Shanghai1
				CN South-Guangzhou
				CN Southwest-Guiyang1
				CN-Hong Kong
				AP-Bangkok, AP-Singapore, AP-Jakarta
				ME-Riyadh
				AF-Johannesburg
				TR-Istanbul
	gaussdb.mysql.xlarge.x86.8	4	32	CN North-Beijing4, CN North-Ulanqab1
				CN Southwest-Guiyang1
				AP-Singapore
				AF-Johannesburg
	gaussdb.mysql.2xlarge.x86.4	8	32	CN North-Beijing4, CN North-Ulanqab1
				CN East-Shanghai1
				CN South-Guangzhou
				CN Southwest-Guiyang1
				CN-Hong Kong
				AP-Bangkok, AP-Singapore, AP-Jakarta
				ME-Riyadh

Specifications	Specification Code	vCPUs	Memory (GB)	Supported Regions
				AF-Johannesburg
				TR-Istanbul
	gaussdb.mysql.2xlarge.x86.8	8	64	CN North-Beijing4, CN North-Ulanqab1
				CN Southwest-Guiyang1
				AP-Singapore
				AF-Johannesburg
	gaussdb.mysql.4xlarge.x86.4	16	64	CN North-Beijing4, CN North-Ulanqab1
				CN East-Shanghai1
				CN South-Guangzhou
				CN Southwest-Guiyang1
				CN-Hong Kong
				AP-Bangkok, AP-Singapore, AP-Jakarta
				ME-Riyadh
				AF-Johannesburg
				TR-Istanbul
	gaussdb.mysql.4xlarge.x86.8	16	128	CN North-Beijing4, CN North-Ulanqab1
				CN Southwest-Guiyang1
				AP-Singapore
				AF-Johannesburg
	gaussdb.mysql.8xlarge.x86.4	32	128	CN North-Beijing4, CN North-Ulanqab1
				CN East-Shanghai1
				CN South-Guangzhou
				CN Southwest-Guiyang1
				CN-Hong Kong
				AP-Bangkok, AP-Singapore, AP-Jakarta
				ME-Riyadh

Specifications	Specification Code	vCPUs	Memory (GB)	Supported Regions
				AF-Johannesburg
				TR-Istanbul
	gaussdb.mysql.8xlarge.x86.8	32	256	CN North-Beijing4, CN North-Ulanqab1
				CN Southwest-Guiyang1
				AP-Singapore
				AF-Johannesburg
	gaussdb.mysql.16xlarge.x86.4	60	256	CN North-Beijing4, CN North-Ulanqab1
				CN East-Shanghai1
				CN South-Guangzhou
				CN Southwest-Guiyang1
				CN-Hong Kong
				AP-Bangkok, AP-Singapore, AP-Jakarta
				ME-Riyadh
				AF-Johannesburg
				TR-Istanbul
	gaussdb.mysql.16xlarge.x86.8	64	512	CN North-Beijing4, CN North-Ulanqab1
				CN Southwest-Guiyang1
				AP-Singapore
				AF-Johannesburg
General-purpose	gaussdb.mysql.large.x86.normal.2	2	4	CN North-Beijing4
				CN Southwest-Guiyang1
				CN East-Shanghai1
				CN South-Guangzhou
				CN-Hong Kong
	gaussdb.mysql.large.x86.normal.4	2	8	CN North-Beijing4
				CN Southwest-Guiyang1

Specifications	Specification Code	vCPUs	Memory (GB)	Supported Regions
	gaussdb.mysql.xlarge.x86.normal.2	4	8	CN North-Beijing4
				CN Southwest-Guiyang1
				CN East-Shanghai1
				CN South-Guangzhou
				CN-Hong Kong
	gaussdb.mysql.xlarge.x86.normal.4	4	16	CN North-Beijing4
				CN Southwest-Guiyang1
	gaussdb.mysql.2xlarge.x86.normal.2	8	16	CN North-Beijing4
				CN Southwest-Guiyang1
				CN East-Shanghai1
				CN South-Guangzhou
				CN-Hong Kong
	gaussdb.mysql.2xlarge.x86.normal.4	8	32	CN North-Beijing4
				CN Southwest-Guiyang1
	gaussdb.mysql.4xlarge.x86.normal.2	16	32	CN North-Beijing4
				CN Southwest-Guiyang1
				CN East-Shanghai1
				CN South-Guangzhou
				CN-Hong Kong
	gaussdb.mysql.4xlarge.x86.normal.4	16	64	CN North-Beijing4
				CN Southwest-Guiyang1
	gaussdb.mysql.8xlarge.x86.normal.2	32	64	CN North-Beijing4
				CN Southwest-Guiyang1
				CN East-Shanghai1
				CN South-Guangzhou
				CN-Hong Kong
	gaussdb.mysql.8xlarge.x86.normal.4	32	128	CN North-Beijing4
				CN Southwest-Guiyang1

NOTICE

- The DB instance specifications vary according to site requirements.
- For information about Transactions Per Second (TPS) and Queries Per Second (QPS), see **Performance White Paper**.

Kunpeng Instance Specifications

Kunpeng instances only support dedicated specifications.

Dedicated: CPU and memory resources are dedicated for use and performance is stable without being affected by other instances on the same physical machine. Dedicated instances are good for scenarios that require stable performance.

Table 5-3 Kunpeng instance specifications

Specifications	Specification Code	vCPUs	Memory (GB)	Supported Regions
Dedicated	gaussdb.mysql.xlarge.arm.4	4	16	CN North-Beijing4, CN North-Ulanqab1
				CN East-Shanghai1
				CN South-Guangzhou
				AP-Singapore
	gaussdb.mysql.xlarge.arm.8	4	32	CN North-Beijing4
				CN East-Shanghai1
				CN South-Guangzhou
				CN Southwest-Guiyang1
				AP-Singapore
	gaussdb.mysql.2xlarge.arm.4	8	32	CN North-Beijing4, CN North-Ulanqab1
				CN East-Shanghai1
				CN South-Guangzhou
				AP-Singapore
	gaussdb.mysql.2xlarge.arm.8	8	64	CN North-Beijing4
				CN East-Shanghai1
				CN South-Guangzhou
				CN Southwest-Guiyang1
				AP-Singapore

Specifications	Specification Code	vCPUs	Memory (GB)	Supported Regions
	gaussdb.mysql.4xlarge.arm.4	16	64	CN North-Beijing4, CN North-Ulanqab1
				CN East-Shanghai1
				CN South-Guangzhou
				AP-Singapore
	gaussdb.mysql.4xlarge.arm.8	16	128	CN North-Beijing4
				CN East-Shanghai1
				CN South-Guangzhou
				CN Southwest-Guiyang1
				AP-Singapore
	gaussdb.mysql.8xlarge.arm.4	32	128	CN North-Beijing4, CN North-Ulanqab1
				CN East-Shanghai1
				CN South-Guangzhou
				AP-Singapore
	gaussdb.mysql.8xlarge.arm.8	32	256	CN North-Beijing4
				CN Southwest-Guiyang1
				AP-Singapore
	gaussdb.mysql.12xlarge.arm.4	48	192	CN North-Beijing4, CN North-Ulanqab1
				CN East-Shanghai1
				CN South-Guangzhou
				AP-Singapore
	gaussdb.mysql.12xlarge.arm.8	48	384	CN North-Beijing4
				CN East-Shanghai1
				CN South-Guangzhou
				CN Southwest-Guiyang1
				AP-Singapore
	gaussdb.mysql.15xlarge.arm.8	60	480	CN North-Beijing4
				CN East-Shanghai1
				CN South-Guangzhou

Specifications	Specification Code	vCPUs	Memory (GB)	Supported Regions
				CN Southwest-Guiyang1
				AP-Singapore

NOTICE

- The DB instance specifications vary according to site requirements.
- For information about Transactions Per Second (TPS) and Queries Per Second (QPS), see **Performance White Paper**.

5.3 Storage Types

TaurusDB provides two storage types: Cloud Database Engine Level 6 (DL6) and Cloud Database Engine Level 5 (DL5).

This section describes the differences between the two storage types, helping you choose the one that best suits your needs.

Storage Type Description

Table 5-4 Storage type description

Storage Type	Description	Applicable Scenario
DL6	The shared storage is the default storage type for TaurusDB instances created before July 2024. DL6-based instances achieve zero RPO with a 3-AZ deployment and deliver better performance and higher peak throughput.	Core application systems that are sensitive to performance and have demanding requirements on storage I/O during peak hours, such as those in finance, e-commerce, government, and gaming

Storage Type	Description	Applicable Scenario
DL5	The new storage type uses Huawei Cloud's hardware and network infrastructure technologies, ensuring that DL5-based instances maintain the same high availability (zero RPO in the 3-AZ deployment) as DL6-based instances. Although the peak performance may decrease, the cost per unit capacity is significantly reduced.	CPU-intensive sub-core business systems or application modules that focus on minimal costs

NOTE

As the two storage types rely on different physical media, you cannot change the storage type for an existing instance. To change the storage type, you are advised to purchase a new TaurusDB instance, select the desired storage type, and migrate data from the original instance to the new instance using DRS.

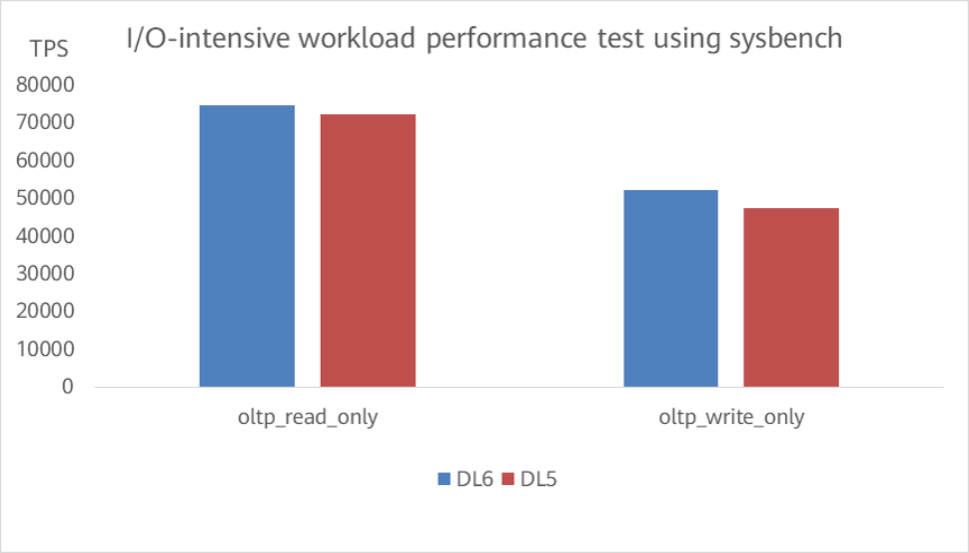
Billing

For details, see **Price Calculator**.

Performance Comparison

When DL6- and DL5-based instances with the same compute specifications and I/O-intensive workloads were compared using sysbench, there was only an about 3% difference in read performance and less than 10% difference in write performance.

Figure 5-1 Performance comparison results



5.4 Instance Statuses

The status of a DB instance indicates the health of the DB instance. You can view the status of a DB instance on the management console.

Table 5-5 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 failed to be created.
Rebooting	A DB instance is being rebooted.
Changing a DB instance name	The name of a DB instance is being changed.
Changing port	The port of a DB instance is being changed.
Changing instance specifications	The CPU or memory of a DB instance is being changed.
Adding read replicas	Read replicas are being added to a DB instance.
Deleting a read replica	A read replica is being deleted from a DB instance.

Status	Description
Promoting to primary	A read replica is being promoted to primary.
Isolating	A read replica is being isolated.
Isolated	A read replica has been isolated.
Creating	A backup is being created.
Scaling up	The storage space of a DB instance is being scaled up.
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.
Changing certificate settings	The certificate settings of a DB instance are being changed.
Changing serverless compute resources	The compute resources of a serverless DB instance are being changed.
Upgrading minor version	The kernel version of a DB instance is being upgraded.
Deleted	A DB instance has been deleted and will not be displayed in the instance list.

6 Security

6.1 Shared Responsibilities

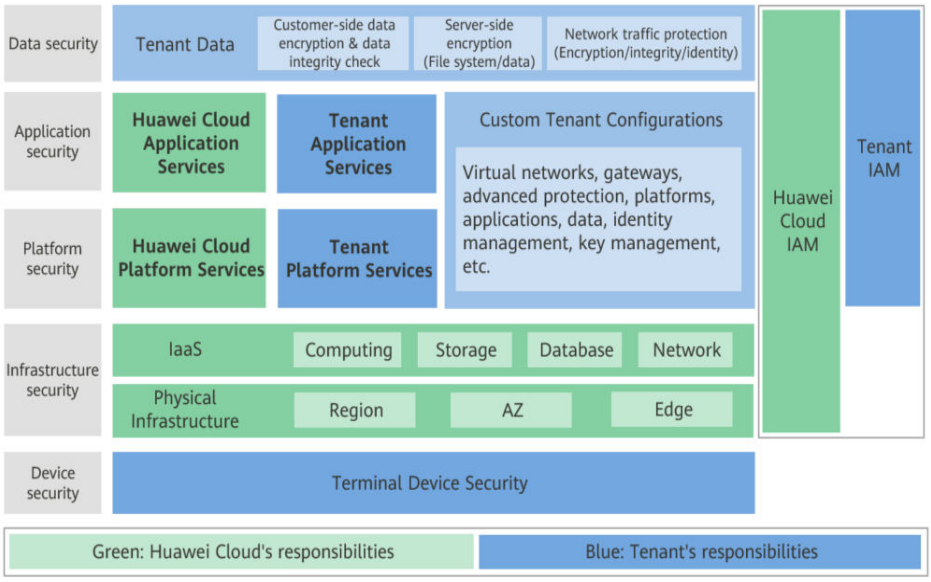
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

The shared responsibility model for Huawei Cloud and the tenants who use Huawei Cloud services is illustrated in **Figure 6-1**. Responsibilities are as follows:

- **Huawei Cloud**: Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OSs of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas behind and measures used to ensure Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 6-1 Huawei Cloud shared security responsibility model



6.2 Identity Authentication and Access Control

Identity Authentication

When you access TaurusDB, the system authenticates your identity using the password or IAM authentication.

- **Password authentication**

  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 authentication**

  You can use **Identity and Access Management (IAM)** to provide fine-grained control of TaurusDB permissions. IAM provides identity authentication, permissions management, and access control, helping you secure access to your Huawei Cloud resources. IAM users can use TaurusDB 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**.

- **VPC and subnet**

  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 network manner.

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

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

- **Security group**

  A security group is a logical group that provides access control policies for ECSs and TaurusDB 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 TaurusDB instances.

6.3 Data Protection

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

Table 6-1 Methods for data security

Method	Description
Transmission encryption (HTTPS)	HTTP and HTTPS are both supported, but HTTPS is recommended for enhanced security.
Data backup	You can back up and restore databases to ensure data reliability.
Critical operation protection	With this function enabled, the system authenticates a user's identity when they perform any risky operations like deleting an instance. This enhances the protection for your data and configuration.
SSL	You can use SSL to encrypt the connection between TaurusDB and the client. It provides privacy, authentication, and integrity to Internet communications.

6.4 Audit and Logs

Audit

- Cloud Trace Service (CTS)

  CTS 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.

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

  With CTS, you can record operations associated with TaurusDB for future query, audit, and backtracking.

- 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

TaurusDB provides a variety of log types and functions for database analysis or audit. You can view logs on the management console.

- Error logs

  TaurusDB allows you to view database-level logs, including error logs and slow SQL query logs.
- Slow query logs

  Slow query logs record statements that exceed **long_query_time** (10 seconds by default). You can view log details and statistics to identify slow statements, so you can optimize them.
- SQL Explorer

  Enabling SQL Explorer will allow TaurusDB to store all SQL statement logs for analysis.

SQL Explorer is disabled by default.

If SQL Explorer is enabled, you can use DAS to view average execution duration, total execution duration, average lock wait time, average rows scanned, and the like.

6.5 Risk Monitoring

Cloud Eye is a comprehensive monitoring platform for resources like cloud databases and cloud servers. It enables you to monitor resources, configure alarm rules, identify resource exceptions, and quickly respond to resource changes.

Metrics

You can monitor resources and operations, such as CPU usage and network throughput using Cloud Eye.

The monitoring interval can be 1 minute, 1 second, or 5 seconds. The default monitoring interval is 1 minute. To improve the accuracy of monitoring metrics, you can enable Monitoring by Seconds.

Even Monitoring

Event monitoring provides reporting, query, and alarm functions for event data. You can create alarm rules for both system events and custom events. When specific events occur, Cloud Eye generates alarms for you.

6.6 Fault Rectification

Automated backups are created during the backup window of your DB instances. TaurusDB saves automated backups based on the retention period (1 to 732 days) you specified.

Cross-Region Backups

TaurusDB can store backups in a different region from the DB instance for disaster recovery. If a DB instance in a region is faulty, you can use the backups in another region to restore data to a new DB instance.

After you enable cross-region backup, the 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 an internal network. TaurusDB supports multiple-AZ deployment for cross-AZ DR.

Failover

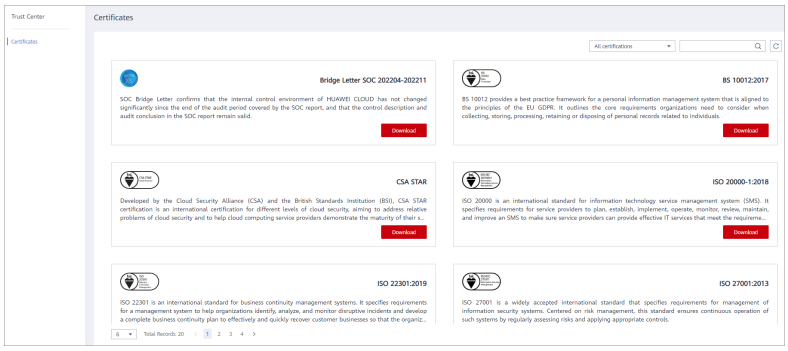
A TaurusDB instance contains one primary node and multiple read replicas. If the primary node becomes unavailable, TaurusDB automatically fails over to a read replica.

6.7 Certificates

Compliance Certificate

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. You can **download** them.

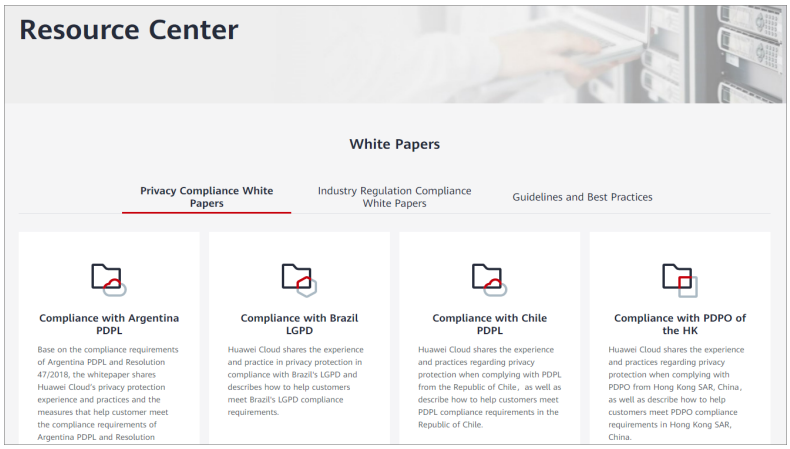
Figure 6-2 Downloading compliance certificates



Resource Center

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

Figure 6-3 Resource center



7 Permissions

If you need to assign different permissions to personnel in your enterprise to access your TaurusDB 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 resources but do not want them to delete TaurusDB 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 resources.

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

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

TaurusDB 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 is a project-level service deployed in specific physical regions. If you set **Scope** to **Region-specific projects** and select the specified projects in the specified regions, the users only have permissions for TaurusDB instances in the selected projects. If you set **Scope** to **All projects**, the users have permissions for TaurusDB instances in all region-specific projects. When accessing TaurusDB 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 permission 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 permission access. For example, you can grant users only permissions 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 TaurusDB, see **Permissions Policies and Supported Actions**.

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

Table 7-1 System-defined permissions for TaurusDB

Role/Policy Name	Description	Type
GaussDB FullAccess	Full permissions for TaurusDB	System-defined policy
GaussDB ReadOnlyAccess	Read-only permissions for TaurusDB	System-defined policy

Table 7-2 lists common operations supported by each system-defined permission of TaurusDB.

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

Operation	GaussDB FullAccess	GaussDB ReadOnlyAccess
Creating a TaurusDB instance	Supported	Not supported
Deleting a TaurusDB instance	Supported	Not supported
Querying TaurusDB instances	Supported	Supported

Table 7-3 Common operations and supported actions

Operation	Action	Description
Modifying parameters in a parameter template	gaussdb:param:modify	-
Changing DB instance specifications	gaussdb:instance:modifySpec	-

Operation	Action	Description
Creating a 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 To create an encrypted instance, configure the KMS Administrator permission for the project. To create yearly/monthly instances, configure the following CBC actions: bss:renewal:view bss:renewal:update bss:balance:view bss:order:view bss:order:update bss:order:pay To configure TDE during instance creation, configure the following action: iam:agencies:createServiceLinkedAgencyV5
Creating a manual backup	gaussdb:backup:create	-
Querying backups	gaussdb:backup:list	-
Querying error logs	gaussdb:log:list	-
Rebooting a DB instance	gaussdb:instance:restart	-
Querying DB instances	gaussdb:instance:list	-
Creating a parameter template	gaussdb:param:create	-
Deleting a parameter template	gaussdb:param:delete	-
Modifying a backup policy	gaussdb:instance:modifyBackupPolicy	-

Operation	Action	Description
Viewing parameter templates	gaussdb:param:list	-
Deleting a DB instance	gaussdb:instance:delete	To unsubscribe from a yearly/monthly instance, configure the following action: bss:unsubscribe:update
Deleting a manual backup	gaussdb:backup:delete	-
Querying project tags	gaussdb:tag:list	-
Applying a parameter template	gaussdb:param:apply	-
Adding or deleting project tags in batches	gaussdb:instance:dealTag	-
Changing quotas	gaussdb:quota:modify	-
Upgrading a DB instance version	gaussdb:instance:upgrade	-
Promoting a read replica to the primary node	gaussdb:instance:switchover	-
Changing a database port	gaussdb:instance:modifyPort	-
Changing a security group	gaussdb:instance:modifySecurityGroup	-
Changing the private IP address	gaussdb:instance:modifyIp	To select an IP address, configure the following actions: vpc:vpcs:list vpc:vpcs:get
Enabling or disabling SSL	gaussdb:instance:modifySSL	-
Changing an instance name	gaussdb:instance:rename	-
Adding read replicas	gaussdb:instance:addNodes	-
Deleting read replicas	gaussdb:instance:deleteNodes	-
Scaling storage space	gaussdb:instance:modifyStorageSize	-

Operation	Action	Description
Changing a DB instance password	gaussdb:instance:modifyPassword	-
Binding an EIP to a DB instance	gaussdb:instance:bindPublicIp	To display EIPs on the console, configure: vpc:publicIps:get vpc:publicIps:list
Unbinding an EIP from a DB instance	gaussdb:instance:unbindPublicIp	-
Modifying a monitoring policy	gaussdb:instance:modifyMonitorPolicy	-
Changing a failover priority	gaussdb:instance:modifySwitchoverPriority	-
Changing the maintenance window	gaussdb:instance:modifyMaintenanceWindow	-
Isolating nodes	gaussdb:instance:isolateNodes	-
Enabling or disabling SQL Explorer	gaussdb:instance:modifyTraceSQLPolicy	-
Querying HTAP instances	gaussdb:htapInstance:list	-
Creating an HTAP instance	gaussdb:htapInstance:create	-
Modifying a GaussDB HTAP instance.	gaussdb:htapInstance:modify	-
Deleting an HTAP instance	gaussdb:htapInstance:delete	-
Changing an HTAP instance name	gaussdb:htapInstance:rename	-
Rebooting an HTAP instance	gaussdb:htapInstance:restart	-
Upgrading an HTAP instance version	gaussdb:htapInstance:upgrade	-
Promoting a read replica of an HTAP instance to primary	gaussdb:htapInstance:switchover	-
Changing the specifications of an HTAP Instance	gaussdb:htapInstance:modifySpec	-

Operation	Action	Description
Scaling up storage of an HTAP instance	gaussdb:htapInstance:modifyStorageSize	-
Binding an EIP for an HTAP instance	gaussdb:htapInstance:bindPublicIp	-
Unbinding an EIP from an HTAP instance	gaussdb:htapInstance:unbindPublicIp	-
Changing the port of an HTAP instance	gaussdb:htapInstance:modifyPort	-
Changing the HTAP instance password	gaussdb:htapInstance:modifyPassword	-
Creating an HTAP Data Synchronization Task	gaussdb:htapInstance:createDataSync	-
Modifying an HTAP Data Synchronization Task	gaussdb:htapInstance:modifyDataSync	-
Deleting an HTAP Data Synchronization Task	gaussdb:htapInstance:deleteDataSync	-
Creating a database proxy instance	gaussdb:proxy:create	-
Changing the IP address of a proxy instance	gaussdb:proxy:modifyIp	-
Modifying the read weights of a proxy instance	gaussdb:proxy:modifyWeight	-
Changing the database proxy port	gaussdb:proxy:modifyPort	-
Modifying database proxy access control	gaussdb:proxy:modifyAccess	-
Deleting a proxy instance	gaussdb:proxy:delete	-
Querying proxy Instances	gaussdb:proxy:list	-
Upgrading a proxy instance version	gaussdb:proxy:upgrade	-
Changing a proxy instance name	gaussdb:proxy:rename	-
Adding database proxy nodes	gaussdb:proxy:addNodes	-
Deleting database proxy nodes	gaussdb:proxy:deleteNodes	-

Operation	Action	Description
Changing specifications of a proxy instance	gaussdb:proxy:modifySpec	-
Applying for a private domain name for a database proxy instance	gaussdb:proxy:createDns	-
Changing the domain name of proxy instance	gaussdb:proxy:modifyDns	-
Deleting the domain name of a proxy instance	gaussdb:proxy:deleteDns	-
Changing the routing policy of a proxy instance	gaussdb:proxy:modifyRouteMode	-
Enabling or disabling SSL for a proxy instance	gaussdb:proxy:modifySSL	-
Creating database users	gaussdb:user:create	-
Deleting database users	gaussdb:user:delete	-
Changing the password of a database user	gaussdb:user:modify	-
Querying database users	gaussdb:user:list	-
Authorizing database permissions to users	gaussdb:user:grantPrivilege	-
Revoking database permissions from users	gaussdb:user:revokePrivilege	-
Creating databases	gaussdb:database:create	-
Deleting databases	gaussdb:database:delete	-
Querying databases	gaussdb:database:list	-
Querying predefined tags	-	To query predefined tags, configure the following action: tms:resourceTags:list
Querying configured log groups	-	To query configured log groups, configure the following action: lts:groups:get
Querying configured log streams	-	To query configured log streams, configure the following action: lts:topics:get

Operation	Action	Description
Modifying auto scaling policies	gaussdb:autoscaling:createPolicy	To modify auto scaling policies, configure the following action: iam:agencies:listAgencies

8 Constraints

To improve instance stability and security, TaurusDB has certain constraints in place.

Specifications and Performance

Table 8-1 Specification and performance constraints

Resource Type	Constraint	Remarks
Storage space	• Pay-per-use instance: a maximum of 128,000 GB • Yearly/monthly instance: 40 GB to 128,000 GB • Serverless instance: a maximum of 128,000 GB • Standard HTAP instance: 50 GB to 32,000 GB for backend nodes; 50 GB to 1,000 GB for frontend nodes	-
Temporary disk space	500 GB at most	For more information, see **How Can I Use Temporary Disk of TaurusDB?**
Connections	TaurusDB does not have constraints on the number of connections. It depends on the default values and value ranges of certain parameters in your DB engine.	For more information, see **What Is the Maximum Number of Connections to a TaurusDB Instance?**

Quotas

Table 8-2 Quota constraints

Quota	Constraint	Remarks
TaurusDB instances	50 instances at most	For details about how to increase the quota, see **Increasing Quotas**.
Read replicas	• A single yearly/monthly instance: 0 to 15 read replicas • A single pay-per-use instance: 0 to 15 read replicas • A single serverless instance: 0 to 7 read replicas	For more information, see **Introducing Read Replicas**.
Tags	A maximum of 20 tags for each instance	For more information, see **Tag Management**.
Free backup space	About 100% of the purchased storage space	For more information, see **How Is TaurusDB Backup Data Billed?**
Automated backup retention period	• Same-region backup: 1 to 732 days (7 days by default) You can request to extend the retention period to 3,660 days by choosing **Service Tickets > Create Service Ticket** in the upper right corner of the management console. • Cross-region backup: 1 to 1,825 days	For more information, see **Configuring a Same-Region Backup Policy** and **Configuring a Cross-Region Backup Policy**.
Log retention period	• Error logs: 30 days • Slow query logs: 30 days • Slow query logs in plaintext: 30 days	For more information, see **Log Management**.

Naming

Table 8-3 Naming constraints

Item	Constraint	Remarks
Instance name	The name must start with a letter and consist of 4 to 64 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.	For more information, see **Changing a DB Instance Name**.
Database name	• The database name must consist of 1 to 64 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed. The total number of hyphens (-) cannot exceed 10. • To prevent errors, reserved keywords cannot be used.	For more information, see **Creating a Database**.
Username	• The username must consist of 1 to 32 characters. Only letters, digits, and underscores (_) are allowed. • To prevent errors, reserved keywords cannot be used.	For more information, see **Creating an Account**.
Parameter template name	The template name must consist of 1 to 64 characters. Only letters (case-sensitive), digits, hyphens (-), underscores (_), and periods (.) are allowed.	For more information, see **Creating a Parameter Template**.
Backup name	The name must start with a letter and consist of 4 to 64 characters. Only letters, digits, hyphens (-), and underscores (_) are allowed.	For more information, see **Creating a Manual Backup**.
Table name/ function name/ stored procedure name/view name	To prevent errors, reserved keywords cannot be used.	For more information, see **Database Table Usage**.

Security

Table 8-4 Security constraints

Item	Constraint	Remarks
Database root permissions	Only the **root** user is available on the instance creation page.	-

Item	Constraint	Remarks
Account password	• It must consist of 8 to 32 characters. • It must contain at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters (~!@#$%^*-_=+?,()&|.). • It cannot be the username or the username spelled backwards. • It must comply with the values of **validate_password** parameters. To check the password-related parameter values, click an instance name, choose **Parameters** in the navigation pane, and search for **validate_password** in the upper right corner of the page.	For more information, see **Resetting the Administrator Password**.
Port	• The default value is 3306 and can be changed manually. • The database port ranges from 1025 to 65534, excluding 5342, 5343, 5344, 5345, 12017, 20000, 20201, 20202, 33060, 33062, and 33071, which are reserved for system use.	For more information, see **Changing a Database Port**.
VPC	After a TaurusDB instance is created, the VPC cannot be changed.	-

Item	Constraint	Remarks
Security group	• By default, you can create a maximum of 100 security groups in your cloud account. • By default, you can add a maximum of 50 rules to a security group. • One TaurusDB instance can be bound to multiple security groups, and one security group can be associated with multiple TaurusDB instances. • When creating an instance, you can select multiple security groups. (For better network performance, you are advised to select at most five security groups.)	-
System accounts	To provide O&M services, the system automatically creates system accounts when you create TaurusDB instances. These system accounts are unavailable to you. • **rdsAdmin**: a management account with highest permissions, which is used to query and modify instance information, rectify faults, migrate data, and restore data. • **rdsRepl**: a replication account, which is used to synchronize data from primary nodes to standby nodes or read replicas. • **rdsBackup**: a backup account, which is used to back up data in the background. • **rdsMetric**: a metric monitoring account, which is used by watchdog to collect database status data. • **rdsProxy**: a database proxy account, which is used for authentication when the database is connected through a proxy address. This account is automatically created when you create a proxy instance.	-

Item	Constraint	Remarks
Instance parameters	Most parameters can be modified through the console or APIs. To ensure security and stability of instances, some parameters cannot be modified.	For more information, see **Modifying Parameters of a DB Instance**.

Instance Operations

Table 8-5 Function constraints

Item	Constraint	Remarks
MySQL storage engine	TaurusDB supports only the InnoDB storage engine.	-
TaurusDB access	• If TaurusDB instances do not have EIPs bound, the instances must be in the same VPC as the ECSs associated with these instances. • Security group rules must be added to allow ECSs to access TaurusDB instances. By default, a TaurusDB instance cannot be accessed by an ECS in a different security group. To enable access, you must add an inbound rule to the security group of a TaurusDB instance. When adding the rule, set the protocol and port, respectively, to TCP and to the default database port of the instance. • Port of a TaurusDB instance: The default port is **3306**. You can change it if you want to access a TaurusDB instance through another port over a private or public network. For details, see **Changing a Database Port**.	-

Item	Constraint	Remarks
Data migration	DRS or mysqldump can be used to migrate data to TaurusDB.	For more information, see **Data Migration**.
TaurusDB instance reboot	Instances can only be rebooted on the TaurusDB console.	For more information, see **Rebooting a DB Instance**.
TaurusDB backups	TaurusDB backups are stored in OBS buckets and are not visible to you.	-
Binlog function	Binlog cannot be enabled for TaurusDB read replicas.	For more information, see **How Do I Enable and View Binlog of My TaurusDB Instance?**
Partitioned tables	TaurusDB is compatible with MySQL Community Server 8.0.22. For a list-partitioned table, there are a maximum of 256 values in a partition, or an error is reported. (Workaround: Redistribute the contents of one table partition into multiple partitions.)	-
Small-scale instances	For TaurusDB instances with 2 vCPUs and 8 GB memory, there are a maximum of 300,000 tables in a single instance and a maximum of 5,000 tables in a single database.	-

9 Related Services

Table 9-1 shows the relationship between TaurusDB and other services.

Table 9-1 Related services

Service	Description
Elastic Cloud Service (ECS)	Enables you to access TaurusDB 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 instances.
Object Storage Service (OBS)	Stores automated and manual backups of your TaurusDB instances.
Cloud Eye	Monitors TaurusDB resources in real time and reports alarms and warnings promptly if any.
Cloud Trace Service (CTS)	Records operations on cloud service resources for future query, audit, and backtrack.
Data Replication Service (DRS)	Smoothly migrates databases to the cloud.
Enterprise Project Management Service (EPS)	Allows you to manage cloud resources and user groups by enterprise project.
Tag Management Service (TMS)	Makes it simple for users to implement, manage, and maintain tags on cloud resources.
Distributed Database Middleware (DDM)	Connects to multiple TaurusDB instances and allows you to access distributed databases.

10 Differences Between TaurusDB and RDS for MySQL

TaurusDB has good performance, scalability, and usability. For details, see **Table 10-1**.

Table 10-1 Differences between TaurusDB and RDS for MySQL

Item	RDS for MySQL	TaurusDB
Architecture	Traditional primary/standby architecture. Data is synchronized between the primary and standby databases through binlogs.	Decoupled storage and compute architecture. Compute nodes share the same data. Data does not need to be synchronized through binlogs.
Performance	Hundreds of thousands of QPS, three times the performance of the open-source MySQL in high concurrency.	Millions of QPS, seven times the performance of open-source MySQL for certain workloads. In complex queries, operations, such as column extraction, conditional filtering, and aggregation calculation, can be pushed down to the storage layer, improving the performance by dozens of times compared with traditional databases.

Item	RDS for MySQL	TaurusDB
Scalability	• Up to five read replicas can be added for each DB instance. The time required for adding read replicas depends on how much data there is. Adding read replicas require additional storage. • The storage grows as needed, to up to 4 TB per DB instance.	• Up to 15 read replicas can be added for each DB instance. Thanks to the shared storage, the time required for adding read replicas is not affected by how much data there is, and no additional storage is needed for read replica creation. • The storage grows as needed, to up to 128 TB per DB instance.
Availability	If the primary instance fails, the standby instance can be automatically promoted to the primary, with an RTO of less than 30s.	If the primary node is faulty, a read replica can be automatically promoted to the primary, with an RTO of less than 10s. It has less latency because no data synchronization through binlogs is required between the primary node and read replicas.
Backup and restoration	Data can be restored to a specific point in time using full backups and binlog playback.	Data can be restored to a specific point in time using full backups (snapshots) and redo log playback, which is faster.
DB engine version	MySQL 5.6, 5.7, and 8.0	MySQL 8.0

