Database Security Service

Service Overview

Issue 23

Date 2022-11-25

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions


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

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

Contents

 Copyright © Huawei Technologies Co., Ltd.

1 DBSS

Database Security Service (DBSS) is an intelligent database security service. Based on the big data analytics technologies, it can audit your databases, detect SQL injection attacks, and identify high-risk operations.

Supported Databases

Database audit provides the audit function in out-of-path disposition pattern for the following databases on Huawei Cloud:

- Relational Database Service (RDS)
- Databases built on ECS
- Databases built on BMS

Databases of some types and versions can be audited without using agents, as shown in **Table 1-1**.

Table 1-1 Agent-free relational databases

Database Type	Supported Edition
GaussDB(for MySQL)	All editions are supported by default.
RDS for SQLServer	All editions are supported by default.
RDS for MySQL	• 5.6 (5.6.51.1 or later) • 5.7 (5.7.29.2 or later) • 8.0 (8.0.20.3 or later)
GaussDB(DWS)	• 8.2.0.100 or later
PostGresql	• 14 (14.4 or later) • 13 (13.6 or later) • 12 (12.10 or later) • 11 (11.15 or later) • 9.6 (9.6.24 or later) • 9.5 (9.5.25 or later)

 Copyright © Huawei Technologies Co., Ltd.

Database audit supports the following database types and versions.

Table 1-2 Database types and versions supported by database audit

Database Type	Edition
MySQL	• 5.0, 5.1, 5.5, 5.6, 5.7 • 8.0 (8.0.11 and earlier) • 8.0.20 • 8.0.23 • 8.0.25
Oracle (The Oracle database uses closed-source protocol and has complex adaptation versions. If you need to audit the Oracle database, contact customer service.)	• 11g 11.1.0.6.0, 11.2.0.1.0, 11.2.0.2.0, 11.2.0.3.0, and 11.2.0.4.0 • 12c 12.1.0.2.0, 12.2.0.1.0 • 19c
PostgreSQL	• 7.4 • 8.0 8.0, 8.1, 8.2, 8.3, 8.4 • 9.0 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 • 10.0 10.0, 10.1, 10.2, 10.3, 10.4, 10.5 • 11.0 • 12.0 • 13.0 • 14.0
SQL Server	• 2008, 2008R2 • 2012 • 2014 • 2016 • 2017
DWS	• 1.5 • 8.1
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8

 Copyright © Huawei Technologies Co., Ltd.

Database Type	Edition
Gbase XDM Cluster	V8.0
Greenplum	V6.0
HighGo	V6.0
GaussDB(for MYSQL)	MySQL 8.0
GaussDB	1.4 Enterprise Edition
DAMENG	DM8
KINGBASE	V8
MongoDB	V5.0
DDS	4.0
Hbase (Supported by CTS instance 23.02.27.182148 and later versions)	1.3.1 2.2.3
Hive	1.2.2 2.3.9 3.1.2 3.1.3

Service Features

- Help you meet security compliance requirements.
  - Comply with DJCP (graded protection) standards for database audit.
  - Comply with security laws and regulations, and provide compliance reports that meet data security standards (such as Sarbanes-Oxley).
- Back up and restore database audit logs and meet the audit data retention requirements.
- Monitor risks, sessions, session distribution, and SQL distribution in real time.
- Report alarms for risky behaviors and attacks and responds to database attacks in real time.
- Locate internal violations and improper operations and keep data assets secure.

Deployed in out-of-path pattern, database audit can perform flexible audit on the database without affecting user services.

- Monitors database login, operation type (data definition, operation, and control), and operation object based on risky operations to effectively audit the database.
- Analyzes risks, sessions, and SQL injection to help you master the database situation in a timely manner.

 Copyright © Huawei Technologies Co., Ltd.

- Provides a report template library to generate daily, weekly, or monthly audit reports according to your configurations. Sends real-time alarm notifications to help you obtain audit reports in a timely manner.

 Copyright © Huawei Technologies Co., Ltd.

2 Functions

Database audit delivers functions such as user behavior detection and audit, multi-dimensional lead analysis, real-time alarms, and reports.

- User Behavior Detection and Audit
  - Associates access operations in the application layer with those in the database layer.
  - Uses built-in or user-defined privacy data protection rules to mask private data (such as accounts and passwords) in audit logs displayed on the console.
- Multi-dimensional Lead Analysis
  - Behavior analysis

    Supports analysis in multiple dimensions, such as audit duration, statement quantity, risk quantity, risk distribution, session statistics, and SQL distribution.
  - Session analysis

    Conducts analysis based on time, user, IP address, and client.
  - Statement analysis

    Provides multiple search criteria, such as time, risk severity, user, client IP address, database IP address, operation type, and rule.
- Real-time Alarms for Risky Operations and SQL Injection
  - Risky operation

    Defines a risky operation in fine-grained dimensions such as operation type, operation object, and risk severity.
  - SQL injection

    Provides an SQL injection library, which facilitates alarm reporting for database exceptions based on the SQL command feature or risk severity.
  - System resource

    Reports alarms when the usage of system resources (CPU, memory, and disk) reaches configured threshold.
- Fine-grained Reports for Various Abnormal Behaviors
  - Session behavior

    Provides session analysis report of the client and database users.

 Copyright © Huawei Technologies Co., Ltd.

- Risky operation

  Provides the risk distribution and analysis report.
- Compliance report

  Provides compliance reports that meet data security standards (for example, Sarbanes-Oxley).

 Copyright © Huawei Technologies Co., Ltd.

3 Advantages

Database audit provides you with the database audit function in out-of-path pattern, enabling the system to generate real-time alarms for risky operations. In addition, database audit generates compliance reports that meet data security standards. In this way, it locates internal violations and improper operations, protecting your data assets.

- Simple to set up

  Database audit is deployed in out-of-path pattern. It is simple to set up and operate.
- Comprehensive audit

  Supports audit of databases built on RDS, ECS, and BMS on HUAWEI CLOUD.
- Quick identification

  Implements 99%+ application association audit, complete SQL parsing, and accurate protocol analysis.
- Efficient analysis

  Responds quickly for data query with 10,000 requests per second from massive volumes of data saved.
- Compliance with various regulations
  - Meets the requirements of database audit for Grade III security compliance.
  - Complies with laws and regulations, such as the cybersecurity law and SOX.
- Clear permission division

  Clearly divides permissions among the system administrator, security administrator, and audit administrator, meeting audit security requirements.

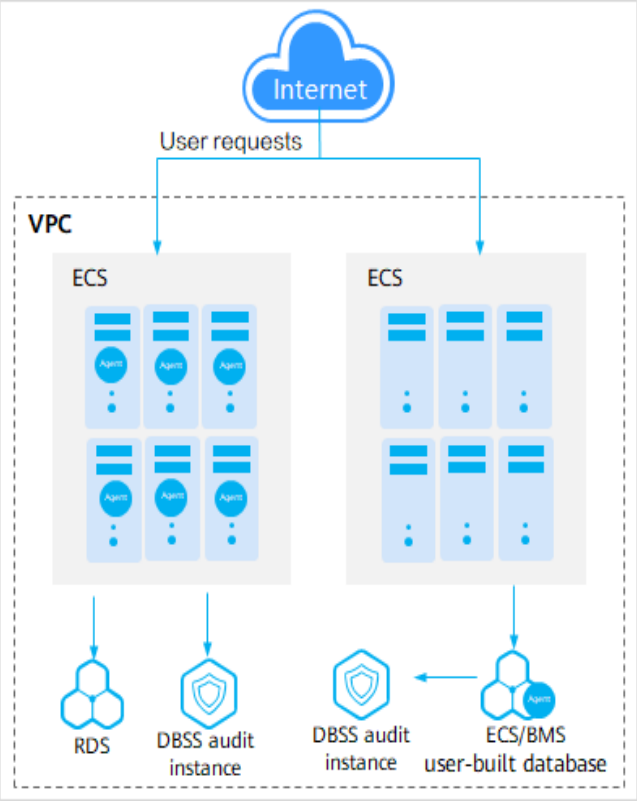
 Copyright © Huawei Technologies Co., Ltd.

4 Deployment Architecture

Database audit is deployed in out-of-path pattern. It supports audit of RDS databases and databases built on ECS and BMS on HUAWEI CLOUD.

Figure 4-1 shows the database audit deployment architecture.

Figure 4-1 Database audit deployment architecture



The agent deployment for database audit is as follows:

- For databases built on ECS or BMS, agents must be deployed on the database side.
- For relational databases, agents must be deployed on the application or proxy side.

 Copyright © Huawei Technologies Co., Ltd.

5 Editions

Database audit provides professional and advanced editions for you to choose from.

Table 5-1 describes the database audit editions.

Table 5-1 Database audit editions

Edition	Maximum Databases	System Resource	Performance
Starter	1	• CPU: 4 vCPUs • Memory: 16 GB • Disk: 500 GB	• Peak QPS: 1,000 queries/second • Database load rate: 1.2 million statements/hour • Stores 100 million online SQL statements. • Stores 5 billion archived SQL statements.
Professional	6	• CPU: 8 vCPUs • Memory: 32 GB • Hard disk: 1.084 GB	• Peak QPS: 6,000 queries/second • Database load rate: 7.2 million statements/hour • Stores 600 million online SQL statements. • Stores 10 billion archived SQL statements.
Advanced	30	• CPU: 16 vCPUs • Memory: 64 GB • Hard disk: 2.108 GB	• Peak QPS: 30,000 queries/second • Database load rate: 10.80 million statements/hour • Stores 1.5 billion online SQL statements. • Stores 60 billion archived SQL statements.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- A database instance is uniquely defined by its database IP address and port.

  The number of database instances equals the number of database ports. If a database IP address has N database ports, there are N database instances.

  Example: A user has two database IP addresses, IP_1 and IP_2. IP_1 has a database port. IP_2 has three database ports. IP_1 and IP_2 have four database instances in total. To audit all of them, select professional edition DBSS, which supports a maximum of six database instances.
- To change the edition of a DBSS instance, unsubscribe from it and purchase a new one.
- The cloud native edition can be purchased only on the RDS console.
- The table above lists the system resources consumed by a database audit instance. Ensure your system has the required configurations before purchasing database audit instances.
- Online SQL statements are counted based on the assumption that the capacity of an SQL statement is 1 KB.

 Copyright © Huawei Technologies Co., Ltd.

6 Constraints

Database audit is subject to certain constraints.

Supported Database Types

The following types of databases on HUAWEI CLOUD can be audited in out-of-path mode:

- Relational Database Service (RDS)
- Databases built on ECS
- Databases built on BMS

Databases That Do Not Need Agents

Databases of some types and versions can be audited without using agents, as shown in **Table 1-1**.

Table 6-1 Agent-free relational databases

Database Type	Supported Edition
GaussDB(for MySQL)	All editions are supported by default.
RDS for SQLServer	All editions are supported by default.
RDS for MySQL	• 5.6 (5.6.51.1 or later) • 5.7 (5.7.29.2 or later) • 8.0 (8.0.20.3 or later)
GaussDB(DWS)	• 8.2.0.100 or later

 Copyright © Huawei Technologies Co., Ltd.

Database Type	Supported Edition
PostGresql	• 14 (14.4 or later) • 13 (13.6 or later) • 12 (12.10 or later) • 11 (11.15 or later) • 9.6 (9.6.24 or later) • 9.5 (9.5.25 or later)

Databases That Need Agents

The following database versions can be audited.

Table 6-2 Database types and versions supported by database audit

Database Type	Edition
MySQL	• 5.0, 5.1, 5.5, 5.6, 5.7 • 8.0 (8.0.11 and earlier) • 8.0.20 • 8.0.23 • 8.0.25
Oracle (The Oracle database uses closed-source protocol and has complex adaptation versions. If you need to audit the Oracle database, contact customer service.)	• 11g 11.1.0.6.0, 11.2.0.1.0, 11.2.0.2.0, 11.2.0.3.0, and 11.2.0.4.0 • 12c 12.1.0.2.0, 12.2.0.1.0 • 19c
PostgreSQL	• 7.4 • 8.0 8.0, 8.1, 8.2, 8.3, 8.4 • 9.0 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 • 10.0 10.0, 10.1, 10.2, 10.3, 10.4, 10.5 • 11.0 • 12.0 • 13.0 • 14.0

Copyright © Huawei Technologies Co., Ltd.

Database Type	Edition
SQL Server	• 2008, 2008R2 • 2012 • 2014 • 2016 • 2017
DWS	• 1.5 • 8.1
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8
Gbase XDM Cluster	V8.0
Greenplum	V6.0
HighGo	V6.0
GaussDB(for MYSQL)	MySQL 8.0
GaussDB	1.4 Enterprise Edition
DAMENG	DM8
KINGBASE	V8
MongoDB	V5.0
DDS	4.0
Hbase (Supported by CTS instance 23.02.27.182148 and later versions)	1.3.1 2.2.3
Hive	1.2.2 2.3.9 3.1.2 3.1.3

Supported OSs

To use database audit, you need to install its agent on database nodes or application nodes. The database audit agent can run on the 64-bit Linux or Windows.

- For more information, see **Table 6-3**.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-3 Supported Linux OS versions

System Name	System version
CentOS	• CentOS 7.0 (64bit) • CentOS 7.1 (64bit) • CentOS 7.2 (64bit) • CentOS 7.3 (64bit) • CentOS 7.4 (64bit) • CentOS 7.5 (64bit) • CentOS 7.6 (64bit) • CentOS 7.8 (64bit) • CentOS 7.9 (64bit) • CentOS 8.0 (64bit) • CentOS 8.1 (64bit) • CentOS 8.2 (64bit)
Debian	• Debian 7.5.0 (64bit) • Debian 8.2.0 (64bit) • Debian 8.8.0 (64bit) • Debian 9.0.0 (64bit) • Debian 10.0.0 (64bit)
Fedora	• Fedora 24 (64bit) • Fedora 25 (64bit) • Fedora 29 (64bit) • Fedora 30 (64bit)
OpenSUSE	• SUSE 13 (64bit) • SUSE 15 (64bit) • SUSE 42 (64bit)
SUSE	• SUSE 11 SP4 (64bit) • SUSE 12 SP1 (64bit) • SUSE 12 SP2 (64bit)
Ubuntu	• Ubuntu 14.04 (64bit) • Ubuntu 16.04 (64bit) • Ubuntu 18.04 (64bit) • Ubuntu 20.04 (64-bit)
EulerOS	• Euler 2.2 (64bit) • Euler 2.3 (64bit) • Euler 2.5 (64bit)
OpenEuler	• OpenEuler 20.03 (64bit)

 Copyright © Huawei Technologies Co., Ltd.

System Name	System version
Oracle Linux	• Oracle Linux 6.9 (64bit) • Oracle Linux 7.4 (64bit)
Red Hat	• Red Hat Enterprise Linux 7.4 (64bit) • Red Hat Enterprise Linux 7.6 (64bit)
NeoKylin	• NeoKylin 7.0 (64bit)
Kylin	• Kylin Linux Advanced Server release V10 (64bit)
Uniontech OS	• Uniontech OS Server 20 Enterprise (64bit)
Huawei Cloud Euler	• Huawei Cloud Euler 2.0 (64bit)
KylinSec	• KylinSec 3.4 (64bit)

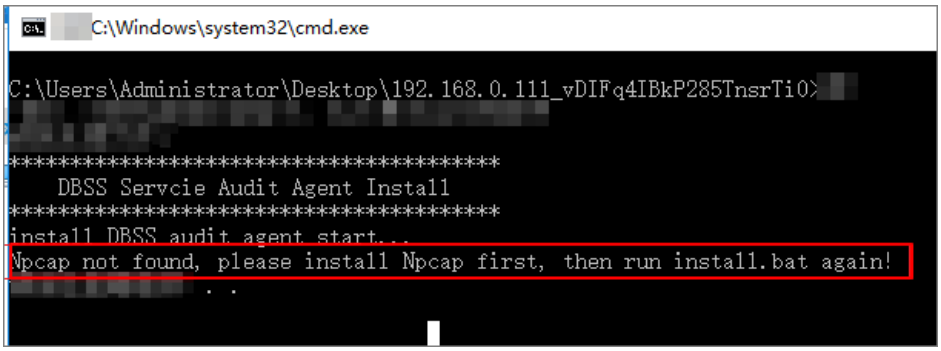
- The following Windows OSs are supported:
  - Windows Server 2008 R2 (64bit)
  - Windows Server 2012 R2 (64bit)
  - Windows Server 2016 (64bit)
  - Windows Server 2019 (64bit)
  - Windows 7 (64bit)
  - Windows 10 (64bit)

  NOTE

  The DBSS agent depends on Npcap. If the message "Npcap not found, please install Npcap first" is displayed when you install the DBSS agent, first install Npcap and then the DBSS agent.

  Npcap download link: **https://npcap.com/#download**

  Figure 6-1 Npcap not found

Other Constraints

- If SSL is enabled for a database, the database cannot be audited. To use database audit, disable SSL first. For details, see **How Do I Disable SSL for a Database?**

 Copyright © Huawei Technologies Co., Ltd.

- Ensure the VPC of the database audit instance is the same as that of the node (application side or database side) where you plan to install the database audit agent. Otherwise, the instance will be unable to connect to the agent or perform audit. For more information, see **How Do I Determine Where to Install an Agent?**
- In some SQL Server databases, complex **declare** statements, **select** functions, and symbol statements that cannot be identified by the system may fail to be parsed.

 Copyright © Huawei Technologies Co., Ltd.

7 Security

7.1 Shared Responsibilities

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

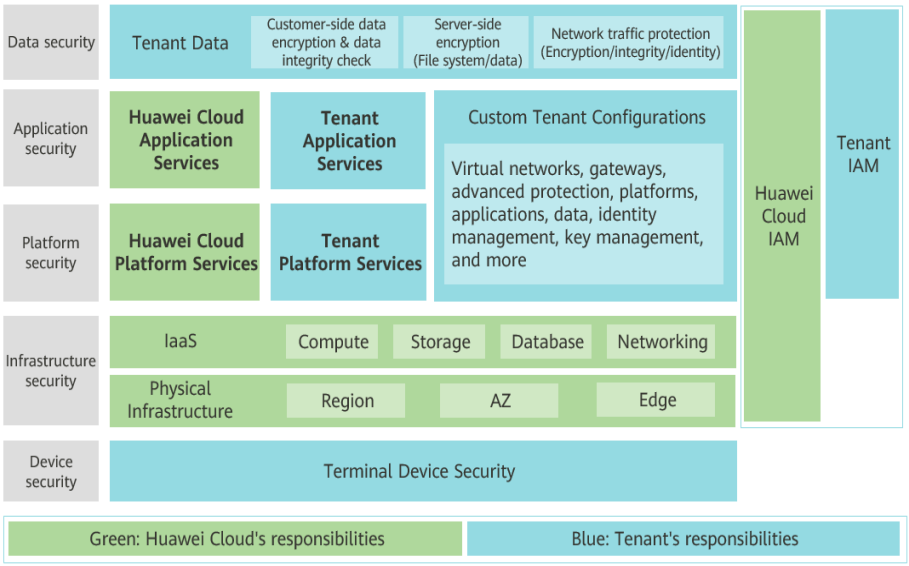
Figure 7-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **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 OS 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 and measures for building 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.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-1 Huawei Cloud shared security responsibility model



7.2 Asset Identification and Management

DBSS instances are created on ECSs. You can use DBSS instances to protect and audit the databases built on RDS, ECS, and BMS. DBSS works with Resource Management Service (RMS) and Tag Management Service (TMS). You can view DBSS instance information on the platform of these services.

7.3 Identity Authentication and Access Control

- **Credential Authentication**

  You can access DBSS through the DBSS console, APIs, or SDK. Regardless of the access method, requests are sent through the REST APIs provided by DBSS.

  DBSS APIs can be accessed only after requests are authenticated. DBSS supports the following authentication methods:

  - Token-based authentication: Requests are authenticated using tokens. By default, token authentication is required for access to the DBSS console.
  - AK/SK authentication: Requests are encrypted using AK/SK pairs. This method is recommended because it provides higher security than token-based authentication.

- **Access Control**

  DBSS supports access control through IAM permissions.

 Copyright © Huawei Technologies Co., Ltd.

Table 7-1 DBSS access control

Method		Description	Reference
Permission management	IAM permission	IAM permissions define which actions on your cloud resources are allowed or denied. After creating an IAM user, the administrator adds the user to one or more groups, and assigns permission policies or roles to these groups. The user will inherit permissions from its groups.	**IAM Permissions** **Permission Management** **Permission Control (Fine-grained)**

7.4 Data Protection

DBSS takes different measures to ensure the security and reliability of data audited and stored in DBSS.

Table 7-2 Data protection methods and features

Measure	Description	Reference
Transmission encryption (HTTPS)	DBSS supports HTTP and HTTPS. HTTPS is recommended to enhance the security of data transmission.	**Making an API Request**
Personal data protection	DBSS controls the data access and records all operations performed on the data.	**Personal Data Protection Mechanism**
Privacy protection	DBSS can mask the sensitive data of the audited data.	**Manage Privacy Data Protection Rules**
Data backup	You can manually or automatically back up audit logs to OBS.	**Backing Up and Restoring Database Audit Logs**
Data destruction	If you delete your DBSS instance or deregister your account, DBSS will delete the audit instance.	-

7.5 Audit and Logs

- **Audit**

Copyright © Huawei Technologies Co., Ltd.

DBSS can audit all operations performed by database common users and administrators and generate compliance reports. DBSS can record traffic, intrusion, anomaly monitoring, data masking, and remote work, locate the operators of abnormal actions, generate alarms for specific events in real time, and display statistics graphs for top operations. DBSS meets the database audit requirements from ISO 27001 and DJCP compliance standards.

Table 7-3 DBSS audit function

Function	Description
System operation audit	DBSS records all system operations and reports alarms for high-, medium-, and low-risks operations as configured. • **SQL Injection Detection**: You can add SQL injection rules to audit your databases. • **Adding Risky Operations**: DBSS has built-in rules for detecting data reduction and slow SQL statements. You can also add risky operations and customize detection rules. • **Alarm Notification**: You can configure different alarm reporting methods and alarm severity levels for system operations and your application environment. Once a system exception or abnormal user operation occurs, the system will send you alarm notifications by email or system messages in a timely manner.

Cloud Trace Service (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.

After you enable CTS and configure a tracker, CTS records the management traces of DBSS for auditing.

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

For details about DBSS operations that can be tracked, see **Auditable Operations**.

- **Logs**

After you enable CTS, the system starts recording operations on DBSS. You can view the operation records of the last 7 days on the CTS console.

For details on how to view CTS logs, see **How Do I View CTS Logs?**

7.6 Resilience

DBSS uses a four-level reliability architecture. It provides inspection, resistance, recovery, and adaptation capabilities to help you manually or automatically recover services, enhancing data durability and reliability.

 Copyright © Huawei Technologies Co., Ltd.

Table 7-4 DBSS reliability architecture

Capability	Item	Objective	Category
Inspection	Intrusion detection	DBSS can work with HSS to detect server exceptions. The detection accuracy is higher than 98%. The detection takes 1 minute.	Security
	Monitoring	DBSS generates alarms for microservice exception logs.	System
Resistance	Data backup	All key data can be backed up. Even if a database is completely damaged, its services can be restored using the backup data. User service logs will be backed up to OBS.	System
	Rapid response	DBSS can quickly detect and rectify AZ- or region-level service faults. DBSS is deployed in out-of-path mode and system services will not be affected.	System
	Service decoupling	Microservices can be separately deployed, started, and stopped.	System
Recovery	VM-level recovery	A faulty VM can be automatically or manually recovered.	System
	System-level recovery	The system can be automatically or manually recovered.	System
Adaptation	Automatic key rotation	Dynamic SCC key rotation	Security
	Automatic certificate rotation	Dynamic rotation of internal microservice communication certificates	Security
	Automatic rotation of accounts and passwords	Dynamic rotation of service accounts and passwords	Security

7.7 Risk Monitoring

DBSS works with Cloud Eye to monitor instances in your account. You can check database security status and DBSS metrics in real time, including CPU usage, memory usage, and disk usage.

 Copyright © Huawei Technologies Co., Ltd.

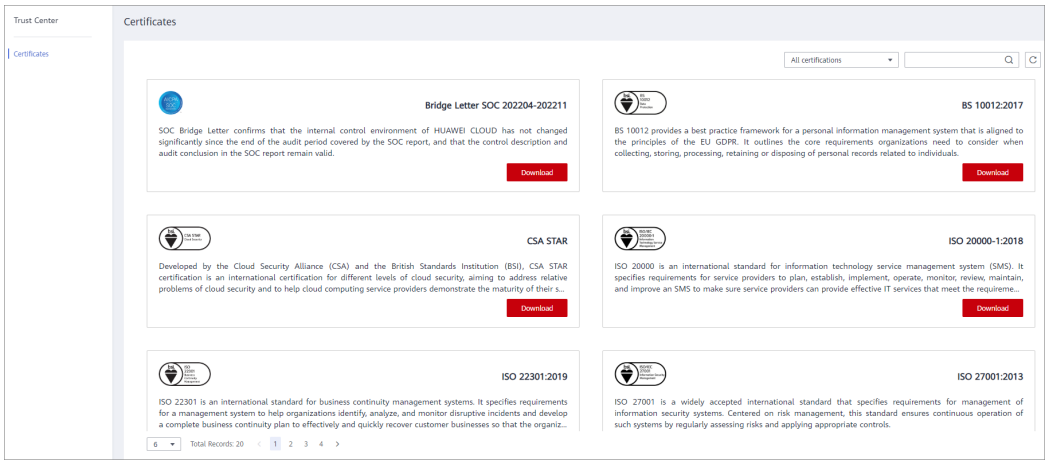
For details about the DBSS monitoring metrics, how to create alarm rules, and how to view DBSS metrics, see **Monitoring**.

7.8 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). You can **download** them from the console.

Figure 7-2 Downloading compliance certificates

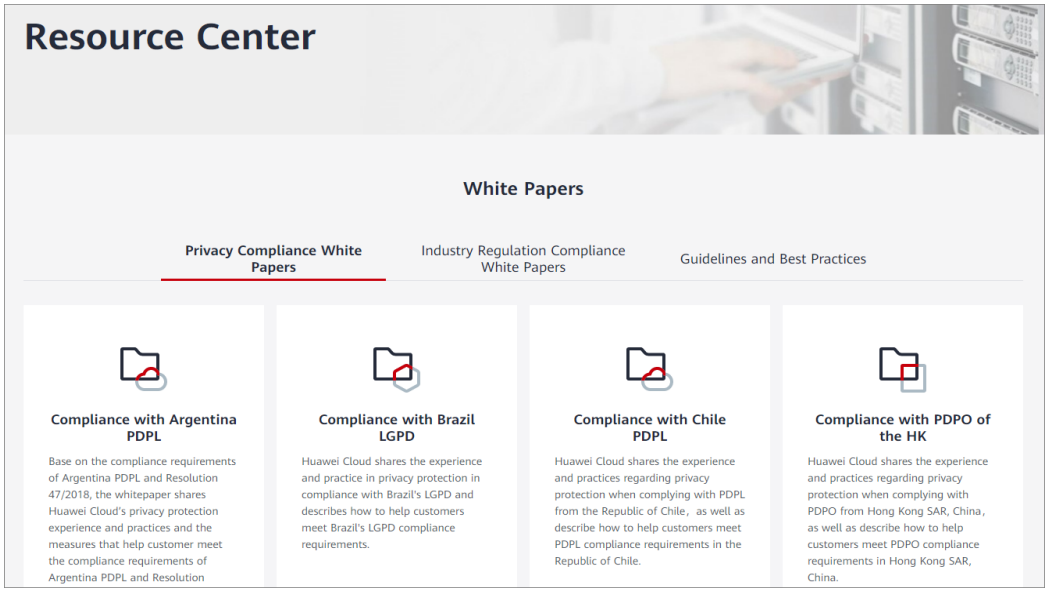


Resource Center

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

Copyright © Huawei Technologies Co., Ltd.

Figure 7-3 Resource center



 Copyright © Huawei Technologies Co., Ltd.

8 Billing

This section describes the DBSS billing items, billing modes, and renewal.

Billing Item

You are charged based on the edition and duration your select. The total cost will be automatically calculated and displayed on the purchase page.

Table 8-1 DBSS billing

Billing Item	Description
Edition	Professional or advanced
Duration	Yearly or monthly

Billing Modes

For now, DBSS only supports yearly/monthly billing and cannot be billed per use. For pricing details, see **Product Pricing Details**.

Changing Billing Mode

- To change the edition of a DBSS instance, unsubscribe from it and purchase a new one.
- Unsubscription: To stop using DBSS, go to the Billing Center to **unsubscribe** from it.

Renewal

If you do not renew a DBSS instance that is billed in yearly/monthly mode upon its expiration, a retention period will be granted.

A DBSS instance stops providing services when it expires. To avoid loss caused by security issues, you are advised to renew it in a timely manner. DBSS expiration does not affect your other services.

 Copyright © Huawei Technologies Co., Ltd.

You can renew your resources on the **Renewals** page of the management console. For details, see **Renewal Management**.

Expiration and Overdue Payment

- Service expiration

  If you do not renew an instance upon its expiration, a retention period will be granted. For details, see **Retention Period**.

- Overdue payment

  For database and asset security purposes, you are advised to top up your account and repay arrears in a timely manner. For details, see **Repaying Arrears**.

FAQ

For more charging FAQs, see **DBSS FAQs**.

Copyright © Huawei Technologies Co., Ltd.

9 Personal Data Protection Mechanism

To ensure that website visitors' personal data, such as the username, password, and mobile phone number, will not be obtained by unauthorized or unauthenticated entities or people and to prevent data leakage, DBSS controls access to the data and records logs for operations performed on the data.

Personal Data

Table 9-1 lists the personal data generated or collected by DBSS.

Table 9-1 Personal data

Type	Collection Method	Can Be Modified	Mandatory
Username	Entered by users on the console login page.	No	Yes Usernames are used to identify users.
Email	Entered by users when configuring email notifications for database audit.	Yes	No

Storage Mode

- Usernames are not sensitive data and stored in plaintext.
- Emails are encrypted before storage.

Access Control

Only users having the **DBSS System Administrator** permission can configure email notifications. Users can view only their own emails.

 Copyright © Huawei Technologies Co., Ltd.

Logging

All non-query operations on users' personal data, including creating and deleting instances, are recorded in audit logs by DBSS and uploaded to CTS. Users can only view their own audit logs.

 Copyright © Huawei Technologies Co., Ltd.

10 Permissions Management

If you need to assign different permissions to employees in your enterprise to access your DBSS resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides functions such as identity authentication, permissions management, and access control.

With IAM, you can create IAM users and assign permissions to control their access to specific resources. For example, some software developers in your enterprise need to use DBSS resources but should not be allowed to delete them or perform any high-risk operations. In this scenario, you can create IAM users for the software developers and grant them only the permissions required for using DBSS resources.

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

IAM can be used free of charge. You pay only for the resources in your account.

For details about IAM, see **What is IAM?**

DBSS Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. After authorization, the user can perform specified operations on BMS based on the permissions.

DBSS is a project-level service deployed and accessed in specific physical regions. When you set **Scope** to **Region-specific projects** and select the specified projects (for example, **ap-southeast-2**) in the specified regions (for example, **AP-Bangkok**), the users only have permissions for ECSs in the selected projects. If you set **Scope** to **All resources**, the users have permissions for ECSs in all region-specific projects. When accessing DBSS, the users need to switch to a region where they have been authorized to use cloud services.

You can grant permissions by using roles and policies.

- Roles: A coarse-grained authorization strategy that defines permissions by job responsibility. Only a limited number of service-level roles are available for authorization. When using roles to grant permissions, you also need to assign dependency roles. However, roles are not an ideal choice for fine-grained authorization and secure access control.

 Copyright © Huawei Technologies Co., Ltd.

- 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 permission to manage a certain type of *ECSs*. A majority of fine-grained policies contain permissions for specific APIs, and permissions are defined using API actions. For details about the API actions supported by DBSS, see section "Permissions and Supported Actions".

Table 10-1 describes all the system-defined DBSS roles.

Table 10-1 System roles supported by DBSS

Role Name	Description	Dependency
DBSS System Administrator	Users with this set of permissions can perform the following operations on database audit: • Purchasing an instance • Starting, disabling, and restarting an instance • Obtaining the instance list • Obtaining the basic information of an instance • Obtaining the audit statistics • Obtaining the monitoring information • Obtaining the operation logs • Managing databases • Managing agents • Configuring email notifications • Backup and restoration	To purchase an instance, users must have the **VPC Administrator**, **ECS Administrator**, and **BSS Administrator** roles. • **VPC Administrator**: Users with this set of permissions can perform all execution permission for Virtual Private Cloud (VPC). It is a project-level role, which must be assigned in the same project. • **ECS Administrator**: Users with this set of permissions can perform any operations on an ECS. It is a project-level role, which must be assigned in the same project. • **BSS Administrator**: Users with this set of permissions can perform any operation on menu items on pages **My Account**, **Billing Center**, and **Resource Center**. It is a project-level role, which must be assigned in the same project.

 Copyright © Huawei Technologies Co., Ltd.

Role Name	Description	Dependency
DBSS Audit Administrator	Users with this set of permissions can perform the following operations on database audit: • Obtaining the instance list • Obtaining the basic information of an instance • Obtaining the audit statistics • Obtaining the report results • Obtaining the rule information • Obtaining the statement information • Obtaining the session information • Obtaining the monitoring information • Obtaining the operation logs • Obtaining the database list • Managing reports	None

 Copyright © Huawei Technologies Co., Ltd.

Role Name	Description	Dependency
DBSS Security Administrator	Users with this set of permissions can perform the following operations on database audit: • Obtaining the instance list • Obtaining the basic information of an instance • Obtaining the audit statistics • Obtaining the report results • Obtaining the rule information • Obtaining the statement information • Obtaining the session information • Obtaining the monitoring information • Obtaining the operation logs • Obtaining the database list • Configuring audit rules • Configuring alarm notifications • Managing reports	None

Table 10-2 lists the common operations supported by each system-defined permission of DBSS. Select the permissions as needed.

Table 10-2 Common operations supported by each system-defined permission

Operation	DBSS System Administrator	DBSS Audit Administrator	DBSS Security Administrator
Purchasing an instance	√	×	√

 Copyright © Huawei Technologies Co., Ltd.

Operation	DBSS System Administrator	DBSS Audit Administrator	DBSS Security Administrator
Starting, disabling, and restarting an instance	√	×	×
Obtaining the instance list	√	×	×
Obtaining the basic information of an instance	√	√	√
Obtaining the audit statistics	√	√	√
Obtaining the monitoring information	√	√	√
Obtaining the operation logs	√	√	√
Managing databases	√	×	×
Managing agents	√	×	×
Configuring email notifications	√	×	×
Backup and restoration	√	√	×
Obtaining the report results	√	√	√
Obtaining the rule information	√	√	√
Obtaining the statement information	√	√	√
Obtaining the session information	√	√	√
Obtaining the database list	√	√	√

 Copyright © Huawei Technologies Co., Ltd.

Operation	DBSS System Administrator	DBSS Audit Administrator	DBSS Security Administrator
Managing reports	×	√	×
Configuring audit rules	×	×	√
Configuring alarm notifications	×	×	×

Helpful Links

- **What Is IAM?**
- **Creating a User Group, a User, and Granting DBSS Permissions**

 Copyright © Huawei Technologies Co., Ltd.

11 Related Services

ECS

DBSS instances are created on ECSs. You can use the DBSS instances to audit databases built on ECS.

RDS

DBSS can audit RDS instances.

BMS

DBSS can audit databases built on BMSs.

CTS

Cloud Trace Service (CTS) provides you with a history of DBSS operations. After enabling CTS, you can view all generated traces to review and audit performed DBSS operations. For details, see the *Cloud Trace Service User Guide*.

Table 11-1 DBSS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating an instance	dbss	createInstance
Deleting an Instance	dbss	deleteInstance
Starting an Instance	dbss	startInstance
Stopping an Instance	dbss	stopInstance
Restarting an Instance	dbss	rebootInstance

OBS

Object Storage Service (OBS) is an object-based cloud storage service. It provides massive, secure, highly reliable, and low-cost data storage capabilities. Database

 Copyright © Huawei Technologies Co., Ltd.

audit logs can be backed up to OBS buckets to achieve high availability for disaster recovery.

SMN

SMN is an extensible, high-performance message processing service.

- To enable notifications, you must configure SMN first.
- After enabling notifications, you can receive an email when an alarm is triggered or an audit report is generated.
- You can enable or disable alarm notifications on the **Alarm Notifications** tab of the **Settings** page.
- You can enable or disable report notifications on the **Reports** page.

For details about SMN, see *Simple Message Notification User Guide*.

Cloud Eye

Cloud Eye is a multi-dimensional monitoring platform for resources such as ECSs and bandwidth. With Cloud Eye, you can understand the resource usage and running status of services running on the cloud platform, receive alarm notifications in a timely manner, and react to changes to keep your services running smoothly. For details about the alarm function, see *Cloud Eye User Guide*.

Table 11-2 DBSS metrics supported by Cloud Eye

Metric Name	Description	Value Range	Monitored Object	
SQL Injection Alarms	Collects the number of SQL injection alarms of a monitored object.	≥0 count	ECS	4 min
XSS Vulnerability Alarms	Collects the number of XSS vulnerability alarms of a monitored object.	≥0 count	ECS	4 min
Webshell Upload Alarms	Collects the number of webshell upload alarms of a monitored object.	≥0 count	ECS	4 min

 Copyright © Huawei Technologies Co., Ltd.

Metric Name	Description	Value Range	Monitored Object	
Link Theft Alarms	Collects the number of link theft alarms of a monitored object.	≥0 count	ECS	4 min
Blacklisted IP address alarms	Collects the number of alarms on blacklisted IP addresses of a monitored object.	≥0 count	ECS	4 min
IP Address Whitelist Alarms	Collects the number of alarms on whitelisted IP addresses of a monitored object.	≥0 count	ECS	4 min

IAM

Identity and Access Management (IAM) provides you with permission management for DBSS.

Only users who have the DBSS System Administrator permissions can use DBSS.

To obtain the permissions, contact users who have the Security Administrator permissions. For details, see the *Identity and Access Management User Guide*.

 Copyright © Huawei Technologies Co., Ltd.