Database Security Service

User Guide

Issue	04
Date	2022-10-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

1 Overview

1.1 DBSS

Database Security Service (DBSS) is an intelligent database security service. Based on the machine learning mechanism and 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 mode for the following databases on the management console:

- RDS instances
- Databases built on ECS
- Databases built on BMS

Database audit supports the following database types and versions.

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

Database Type	Version
MySQL	• 5.0, 5.1, 5.5, 5.6, 5.7 • 8.0 (8.0.11 and earlier)
Oracle	• 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

Database Type	Version
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
SQL Server	● 2008, 2008R2 ● 2012 ● 2014 ● 2016 ● 2017
DWS	● 1.5
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8
Gbase XDM Cluster	V8.0
GaussDB for MYSQL	MySQL 8.0
GaussDB	1.4 Enterprise Edition
DAMENG	DM8
KINGBASE	V8

Service Features

- 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.
- 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.

1.2 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.
  - Risky operation

    Provides the risk distribution and analysis report.

1.3 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 the management console.

- 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.

- Clear permission division

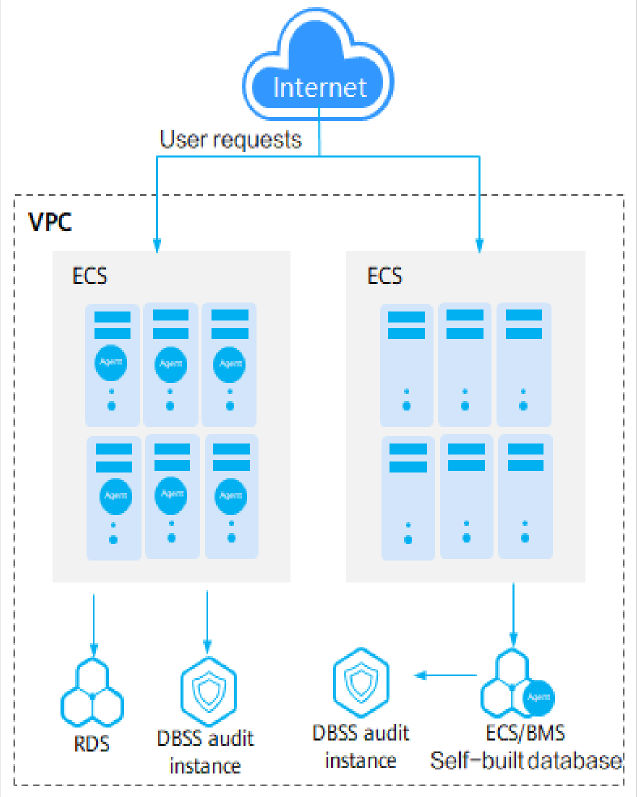
  Clearly divides permissions among the system administrator, security administrator, and audit administrator, meeting audit security requirements.

1.4 Deployment Architecture

Database audit is deployed in out-of-path pattern. It can audit databases built on ECS, BMS and RDS on the management console.

Figure 1-1 shows the database audit deployment architecture.

Figure 1-1 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.

1.5 Editions

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

Table 1-2 describes the database audit editions.

Table 1-2 Database audit editions

Version	Maximum Databases	System Resource	Performance
Basic	3	• CPU: 4 vCPUs • Memory: 16 GB • Disk: 500 GB	• Peak QPS: 3,000 queries/second • Database load rate: 3.6 million statements/hour • Stores 400 million online SQL statements. • Stores 5 billion archived SQL statements.

Version	Maximum Databases	System Resource	Performance
Professional	6	- CPU: 8 vCPUs - Memory: 32 GB - Disk: 1 TB	- 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.

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 apply for a new one.
- Online SQL statements are counted based on the assumption that the capacity of an SQL statement is 1 KB.

1.6 Constraints

Database audit is subject to certain constraints.

Supported Database Types

The following types of databases on the management console can be audited in out-of-path mode:

- RDS instances
- Databases built on ECS
- Databases built on BMS

Supported Database Versions

The following database versions can be audited.

Table 1-3 Database types and versions supported by database audit

Database Type	Version
MySQL	- 5.0, 5.1, 5.5, 5.6, 5.7 - 8.0 (8.0.11 and earlier)

Database Type	Version
Oracle	● 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
SQL Server	● 2008, 2008R2 ● 2012 ● 2014 ● 2016 ● 2017
DWS	● 1.5
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8
Gbase XDM Cluster	V8.0
GaussDB for MYSQL	MySQL 8.0
GaussDB	1.4 Enterprise Edition
DAMENG	DM8
KINGBASE	V8

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.

- For more information, see **Table 1-4**.

Table 1-4 Supported Linux OS versions

System Name	System version
CentOS	● CentOS 6.3 (64bit) ● CentOS 6.5 (64bit) ● CentOS 6.8 (64bit) ● CentOS 6.9 (64bit) ● 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)
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)
EulerOS	● Euler 2.2 (64bit) ● Euler 2.3 (64bit)
Oracle Linux	● Oracle Linux 6.9 (64bit) ● Oracle Linux 7.4 (64bit)

Other Constraints

- If SSL is enabled for a database, the database cannot be audited. To use database audit, disable SSL first.
- 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.

1.7 Security

1.7.1 Shared Responsibilities

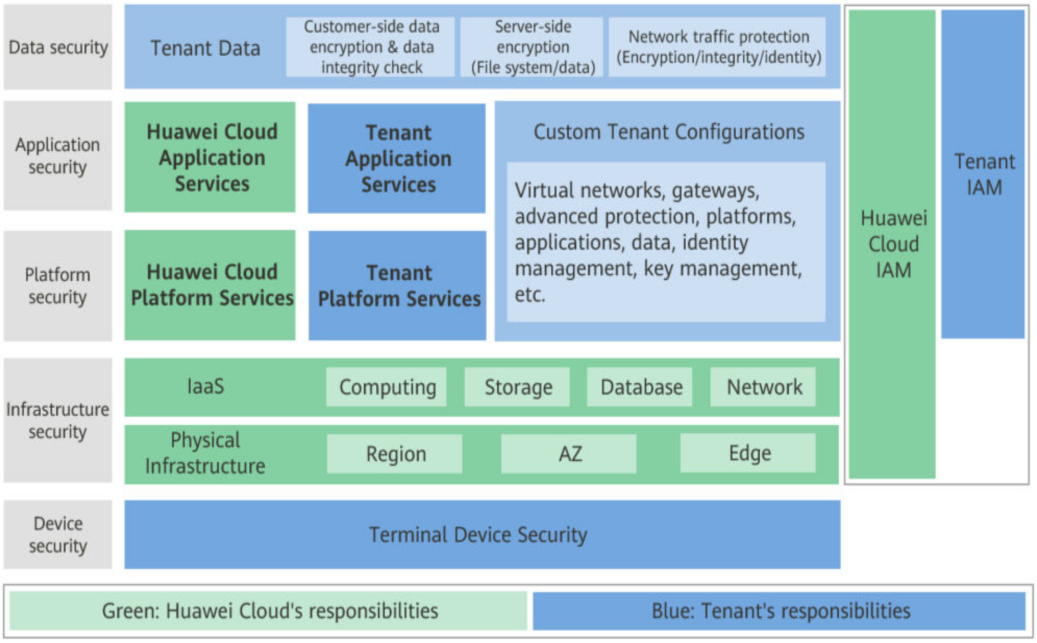
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 1-2 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 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.

Figure 1-2 Huawei Cloud shared security responsibility model


Data security
Tenant Data
Customer-side data encryption & data integrity check
Server-side encryption (File system/data)
Network traffic protection (Encryption/integrity/identity)
Application security
Huawei Cloud Application Services
Tenant Application Services
Custom Tenant Configurations
Virtual networks, gateways, advanced protection, platforms, applications, data, identity management, key management, etc.
Platform security
Huawei Cloud Platform Services
Tenant Platform Services
Infrastructure security
IaaS
Computing
Storage
Database
Network
Physical Infrastructure
Region
AZ
Edge
Huawei Cloud IAM
Tenant IAM
Device security
Terminal Device Security
Green: Huawei Cloud's responsibilities
Blue: Tenant's responsibilities

1.7.2 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.

1.7.3 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.

Table 1-5 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.	

1.7.4 Data Protection

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

Table 1-6 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.	
Personal data protection	DBSS controls the data access and records all operations performed on the data.	
Privacy protection	DBSS can mask the sensitive data of the audited data.	
Data backup	You can manually or automatically back up audit logs to OBS.	
Data destruction	If you delete your DBSS instance or deregister your account, DBSS will delete the audit instance.	-

1.7.5 Audit and Logs

- **Audit**

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 1-7 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. ● : You can add SQL injection rules to audit your databases. ● : DBSS has built-in rules for detecting data reduction and slow SQL statements. You can also add risky operations and customize detection rules. ● : 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 .

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

- **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

1.7.6 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.

Table 1-8 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

1.7.7 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.

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

1.7.8 Certificates

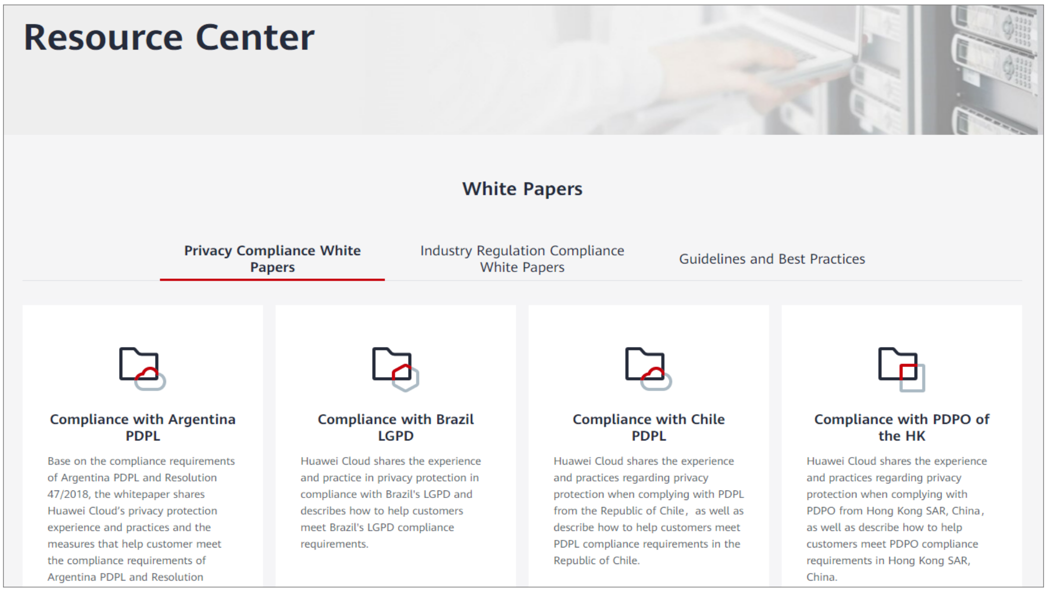
Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can them from the console.

Resource Center

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

Figure 1-3 Resource center



Resource Center

White Papers

Privacy Compliance White Papers

Industry Regulation Compliance White Papers

Guidelines and Best Practices

Compliance with Argentina PDPL

Base on the compliance requirements of Argentina PDPL and Resolution 47/2018, the whitepaper shares Huawei Cloud's privacy protection experience and practices and the measures that help customer meet the compliance requirements of Argentina PDPL and Resolution

Compliance with Brazil LGPD

Huawei Cloud shares the experience and practice in privacy protection in compliance with Brazil's LGPD and describes how to help customers meet Brazil's LGPD compliance requirements.

Compliance with Chile PDPL

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPL from the Republic of Chile, as well as describe how to help customers meet PDPL compliance requirements in the Republic of Chile.

Compliance with PDPO of the HK

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPO from Hong Kong SAR, China, as well as describe how to help customers meet PDPO compliance requirements in Hong Kong SAR, China.

1.8 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 1-9 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 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*.

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*.

1.9 User Permissions

Two permission policies are provided by default: default policies and custom policies. Default policies are pre-defined by IAM and cannot be modified. If default policies do not meet your requirements, you can create custom policies for fine-grained permission control.

Configure permission policies for a user group and add users to the group so that these users can obtain operation permissions defined in the policies.

2 Applying for a Database Audit Instance

Before using the database audit function, you need to apply for a database audit instance.

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.

Impact on the System

Database audit works in out-of-path mode, which neither affects user services nor conflicts with the local audit tools.

Procedure

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the upper right corner, click **Apply for Database Audit**.

Step 4 On the **Apply for Database Audit** page, select an **AZ** and a **Type**.

> **NOTE**
>
> If resources are sold out in an AZ, **Sold out in this AZ** will be displayed for the AZ. In this case, select another AZ.

Database audit comes in the following editions:

- **Basic**: supports up to three database instances.
- **Professional**: supports up to six database instances.

Step 5 Set database audit parameters. See **Table 2-1**.

Table 2-1 Parameters

Parameter	Description	Example Value
VPC	You can select an existing VPC, or click **View VPC** to create one. **NOTE** ● Select the VPC of the node (application or database side) where you plan to install the agent. ● To change the VPC of a DBSS instance, unsubscribe from it and apply for a new one. For more information about VPC, see *Virtual Private Cloud User Guide*.	vpc-sec
Security Group	The security group configured for the instance is displayed on the page. Once a security group is selected for an instance, the instance is protected by the access rules of this security group. For more information about security groups, see *Virtual Private Cloud User Guide*.	sg
Subnet	The **Subnet** drop-down list displays all available subnets. For more information about subnets, see *Virtual Private Cloud User Guide*.	public_sunnet
Instance Name	Custom name of the instance	DBSS-test

Step 6 Confirm the configuration and click **Try Now**.

Step 7 On the details confirmation page, you can click **Submit**.

On the **Database Audit** page, you can view the created database audit instances.

If the **Status** is **Running**, you have successfully applied for the database audit instance.

----End

3 Quick Start

After applying for a database audit instance, add the database to be audited to the instance and install an agent on the database or application side. Database audit works only when the database to be audited is connected to the database audit instance.

Background

Database audit supports auditing databases built on ECS, BMS, and RDS on the management console.

NOTICE

- Ensure the VPC, security group, and subnet of the database audit instance are the same as those 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.
- If SSL is enabled for a database, the database cannot be audited. To use database audit, disable SSL first.

Quick Configuration Procedure

After purchasing database audit, you can quickly get started by following the configuration procedure shown in **Figure 3-1**. For details, see **Table 3-1**.

Figure 3-1 Procedure for quickly configuring database audit

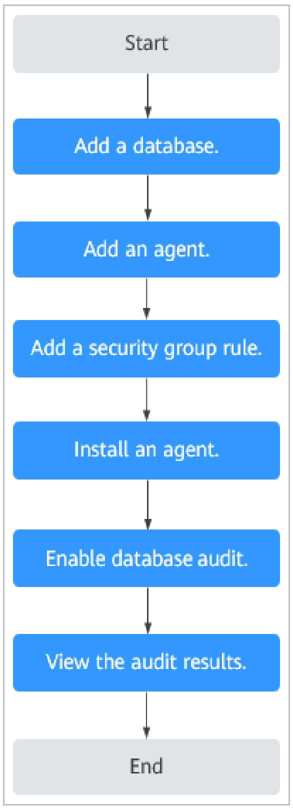


Table 3-1 Procedure for quickly configuring database audit

Step	Configuration	Description
1	**Adding a Database**	Apply for database audit. Add a database to the database audit instance and enable audit for the database.
2	**Adding an Agent**	Select an agent add mode. Database audit supports auditing databases built on ECS, BMS, and RDS on the cloud. Select an agent add mode based on your database deployed on the management console.
3	**Adding Security Group Rules**	Configure TCP (port 8000) and UDP (ports 7000 to 7100) in the security group inbound rule of the database audit instance to allow the agent to communicate with the audit instance.
4	**Installing an Agent (Linux OS)**	Download and then install the agent on the database or application based on the add mode you chose.
5	**Enabling Database Audit**	Enable database audit and connect the added database to the database audit instance.

Step	Configuration	Description
6	Viewing the Audit Results	By default, database audit complies with a **full audit rule**, which is used to audit all databases that are connected to the database audit instance. You can view the audit result on the database audit page.

Verifying the Result

When you connect the added database to the database audit instance, database audit records all operations performed on the database. You can view the audit result on the database audit page.

4 Step 1: Add a Database

Database audit supports databases built on ECS, BMS, and RDS on the console. After applying for a database audit instance, you need to add the database to be audited to the instance.

Prerequisites

You have applied for a database audit instance and the **Status** is **Running**.

Adding a Database

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Databases**.

Step 4 In the **Instance** drop-down list, select the instance whose database is to be added.

Step 5 Click **Add Database**.

Step 6 In the dialog box displayed, set the database information.

Table 4-1 Parameters

Parameter	Description	Example Value
Name	Custom name of the database to be added	test1
IP Address	IP address of the database to be added. The IP address must be an internal IP address in IPv4 or IPv6 format.	IPv4: 192.168.1.1 IPv6: fe80:0000:0000:0000:0000:0000:0000:0000

Parameter	Description	Example Value
Type	Supported database type. The options are as follows: ● MYSQL ● ORACLE ● POSTGRESQL ● SQLSERVER ● DWS ● GaussDB for MYSOL ● GaussDB ● DAMENG ● KINGBASE **NOTE** If **ORACLE** is selected, to make the audit settings take effect, restart the applications to be audited and log in to the database again.	MYSQL
Port	Port number of the database to be added	3306

Parameter	Description	Example Value
Version	Supported database versions ● When **Type** is set to **MYSQL**, the following versions are available: – 5.0, 5.1, 5.5, 5.6, 5.7 – 8.0 (8.0.11 and earlier) ● When **Type** is set to **ORACLE**, the following versions are available: – 11g – 12c – 19c ● When **Type** is set to **POSTGRESQL**, the following versions are available: – 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 ● When **Type** is set to **SQLSERVER**, the following versions are available: – 2008 – 2012 – 2014 – 2016 – 2017 ● When **Type** is set to **DWS**, the following versions are available: – 1.5 ● When **Type** is set to **GaussDB for MySQL**, the following version is available: – MySQL 8.0 ● If **Type** is set to **GaussDB**, the following version is available: – 1.4 Enterprise Edition ● When **Type** is set to **DAMENG**, the following version is available:	5.0

Parameter	Description	Example Value
	– DM8 ● When **Type** is set to **KINGBASE**, the following version is available: – V8	
Instance	Instance name of the database to be audited **NOTE** ● If you do not configure the **Instance** field, database audit will audit all instances in the database. ● If you enter an instance name, database audit will audit the entered instance. Enter a maximum of five instance names and use semicolons (;) to separate instance names.	-
Character Set	Encoding format of the database character set. The options are as follows: ● UTF-8 ● GBK	UTF-8
OS	OS of the added database. The options are as follows: ● LINUX64	LINUX64
Database Type	Type of the database to be added. Its value can be **RDS database** or **Self-built database**.	RDS database

Step 7 Click **OK**. Then a database in the **Disabled** state has been added to the database list.

NOTE

- After adding the database, confirm that the database information is correct. If the database information is incorrect, locate the target database and click **Delete** in the **Operation** column, and add the database again.

----End

5 Step 2: Add an Agent

Add a new agent or choose an existing agent for the database to be audited, depending on your database type. The agent will obtain database access traffic, upload traffic statistics to the audit system, receive audit system configuration commands, and report database monitoring data.

After adding an agent, configure TCP (port 8000) and UDP (ports 7000 to 7100) in the security group inbound rule of the agent node to allow the agent to communicate with the audit instance.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- A database has been added.

Scenarios

Determine where to add the agent based on how your database is deployed. Common database deployment modes are as follows:

- Deploy DBSS for databases built on ECS/BMS. For details, see **Figure 5-1** and **Figure 5-2**.

Figure 5-1 One application connecting to multiple databases built on ECS/BMS

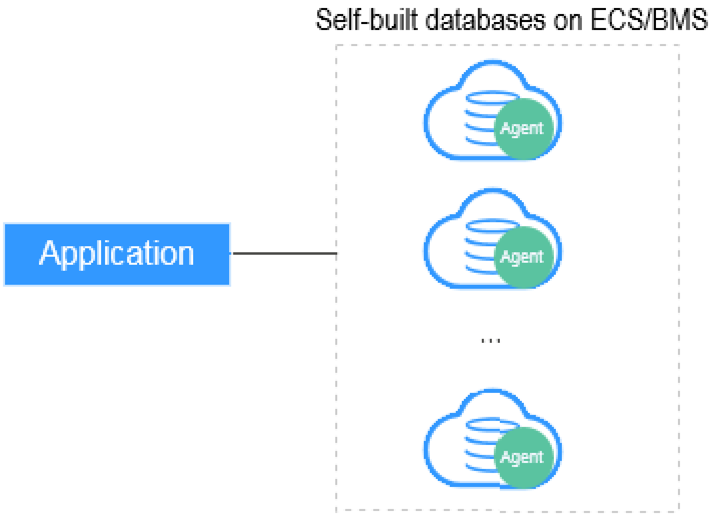
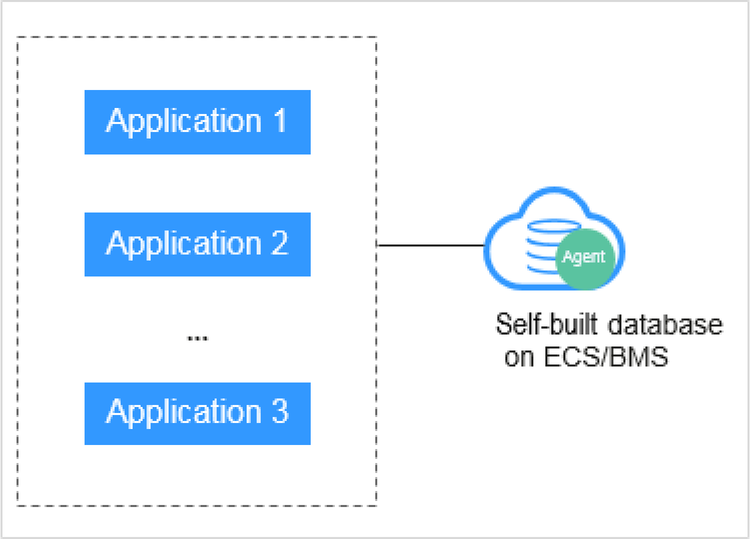


Figure 5-2 Multiple applications connecting to one database built on ECS/BMS



- Deploy DBSS for RDS databases. For details, see **Figure 5-3** and **Figure 5-4**.

Figure 5-3 One application connecting to multiple RDS databases

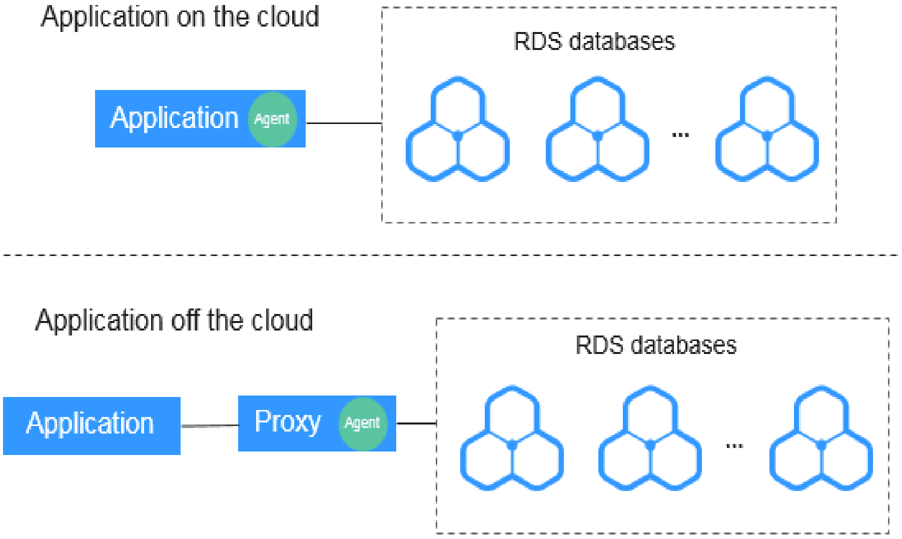


Figure 5-4 Multiple applications connecting to one RDS database

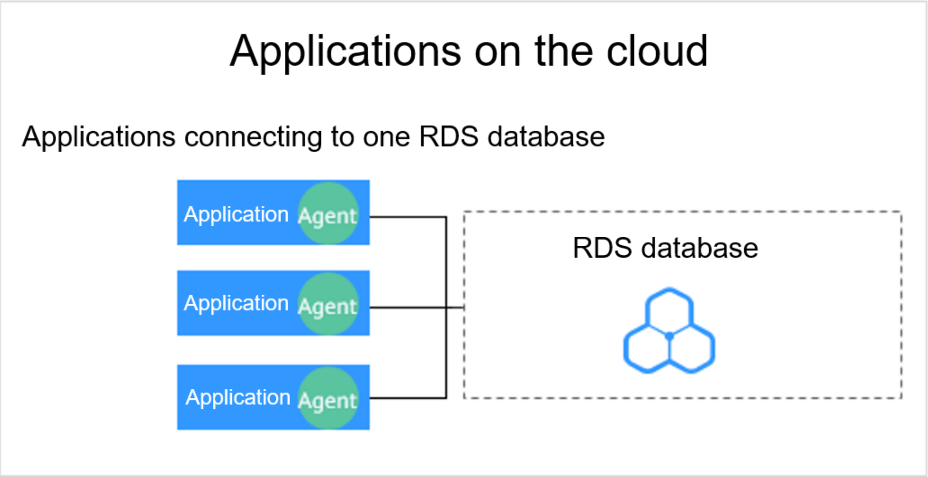

Applications on the cloud
Applications connecting to one RDS database
Application
Agent
Application
Agent
Application
Agent
RDS database

Table 5-1 provides more details.

NOTICE

- If your applications and databases (databases built on ECS/BMS) are deployed on the same node, add the agent on the database side.

Table 5-1 Agent locations

Scenario	Where to Add the Agent	Audit Scope	Description
Databases built on ECS/BMS	Database	All access records of applications that have accessed the database	● Add the agent on the database side. ● If an application connects to multiple databases built on ECS/BMS, the agent must be added on all these databases.
RDS database	Application (if applications are deployed on the cloud)	Access records of all the databases connected to the application	● Add the agent on the application side. ● If an application connects to multiple RDS databases, add an agent on each of the databases. Set **Installation Node Type** for one of them and select **Select an existing agent** for the rest of them. For details, see **Selecting an existing agent**. ● If multiple applications connect to the same RDS database, add the agent must on all these applications.
	Proxy side (if applications are deployed off the cloud)	Only the access records between the proxy and database. Those between the applications and database cannot be audited.	● Add the agent on the application side. ● **Installing Node IP Address** must be set to the IP address of the proxy.

Adding an Agent (Self-built Databases on ECS/BMS)

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Databases**.

Step 4 In the **Instance** drop-down list, select the instance whose agent is to be added.

Step 5 In the **Agent** column of the desired database, click **Add**.

Step 6 In the dialog box displayed, select an add mode. For details about related parameters, see **Table 5-2**.

Table 5-2 Parameters for adding an agent (databases built on ECS/BMS)

Parameter	Description	Example Value
Add Mode	Mode for adding an agent ● **Select an existing agent** If an agent has been installed on a database connected to the same application as the desired database, select **Select an existing agent**. ● **Create an agent** If no agent is available, select **Create an agent** to create one.	Create an agent
Installing Node Type	This parameter is mandatory when **Add Mode** is set to **Create an agent**. When auditing user-installed databases on ECS/BMS, select **Database** for **Installing Node Type**.	Database
OS	OS of the database to be audited. Its value can be **LINUX64**.	LINUX64

Step 7 Click **OK**.

Step 8 Click ⌄ next to the database to view its details and information about the added agent.

NOTE

After adding the agent, confirm that the agent information is correct. If the agent is incorrectly added, click **Delete** in the **Operation** column of the row to delete it, and add an agent again.

----End

Adding an Agent (RDS Databases)

NOTE

After you add a MySQL or GaussDB(for MySQL) database, you can start configuring security group rules. You do not need to install an agent on the database.

If an application connects to multiple RDS databases, be sure to:

- Add an agent to each of the RDS databases.
- Select **Select an existing agent** if one of the databases already has an agent. Add that agent for the rest of the databases.

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Databases**.

Step 4 In the **Instance** drop-down list, select the instance whose agent is to be added.

Step 5 In the **Agent** column of the desired database, click **Add**.

Step 6 In the displayed dialog box, select an add mode. For details about related parameters, see **Table 5-3**.

- Select **Select an existing agent** for **Add Mode**.

  NOTE

  If an agent has been installed on the application, you can select it to audit the desired database.

- Set **Add Mode** to **Create an agent**.

  If no agent is available, select **Create an agent** to create one.

  Select **Installing Node Type** to **Application**, and set **Installing Node IP Address** to the intranet IP address of the application.

Table 5-3 Parameters for adding an agent (RDS databases)

Parameter	Description	Example Value
Add Mode	Mode for adding an agent ● **Selecting an existing agent** If an agent has been installed on a database connected to the same application as the desired database, select **Select an existing agent**. ● **Create an agent** If no agent is available, select **Create an agent** to create one.	Create an agent
Installing Node Type	This parameter is mandatory when **Add Mode** is set to **Create an agent**. To audit the RDS databases, select **Application**.	Application

Parameter	Description	Example Value
Installing Node IP Address	This parameter is mandatory if **Installing Node Type** is set to **Application**. You can enter only one installation node IP address. The IP address of an agent must be unique. The IP address is the intranet IP address of the application. The IP address must be an internal IP address in IPv4 or IPv6 format. **NOTICE** To audit an RDS database connected to an off-cloud application, set this parameter to the IP address of the proxy.	192.168.1.1
Audited NIC Name	Optional. This parameter is configurable if **Installing Node Type** is set to **Application**. Name of the network interface card (NIC) of the application node to be audited	-
CPU Threshold (%)	Optional. This parameter is configurable if **Installing Node Type** is set to **Application**. CPU threshold of the application node to be audited. The default value is **80**. **NOTICE** If the CPU usage of a server exceeds the threshold, the agent on the server will stop running.	80
Memory Threshold (%)	Optional. This parameter is configurable if **Installing Node Type** is set to **Application**. Memory threshold of the application node to be audited. The default value is **80**. **NOTICE** If the memory usage of your server exceeds the threshold, the agent will stop running.	80
OS	OS of the application node to be audited. The value can be **LINUX64**. This parameter is configurable if **Installing Node Type** is set to **Application**.	LINUX64

Step 7 Click **OK**.

----End

Follow-Up Procedure

Configure TCP (port 8000) and UDP (ports 7000 to 7100) in the security group inbound rule of the agent node to allow the agent to communicate with the audit instance. For details about how to add a security group rule, see **Adding a Security Group Rule**.

6 Step 3: Add a Security Group Rule

Configure TCP (port 8000) and UDP (ports 7000 to 7100) in the security group inbound rule of the database audit instance to allow the agent to communicate with the audit instance.

This section describes how to configure TCP (port 8000) and UDP (ports 7000 to 7100) for a security group.

NOTE

You can configure security group rules before or after installing an agent.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- You have added an agent to your database.

Adding a Security Group Rule

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Database Audit** > **Databases**.

Step 4 In the **Instance** drop-down list, select the instance whose security group rule is to be added.

Step 5 Record the IP address of the agent node.

Click ⌄ next to the database to view the information of its agent, and record **Installing Node IP Address**.

Step 6 Click **Add Security Group Rule**.

Step 7 In the displayed dialog box, record the security group name (for example, **default**) of the database audit instance.

Step 8 Click **Go to VPC**.

Step 9 In the security group list, enter the group name **default** in the search box in the upper right corner of the list, and click 🔍 or press **Enter**. The group information is displayed in the list.

Step 10 Click the group name **default**.

Step 11 Click the **Inbound Rules** tab.

Check whether TCP (port number **8000**) and UDP protocols (port number from **7000** to **7100**) are configured in the inbound rules of the security group for the IP address of the installing node in **Step 5**.

- If the inbound rules of the security group have been configured for the installing node, go to **Downloading an Agent**.
- If no inbound rules of the security group have been configured for the installing node, go to **Step 12**.

Step 12 Add an inbound rule for the installing node.

1. On the **Inbound Rules** tab, click **Add Rule**.
2. In the **Add Inbound Rule** dialog box, add **TCP** (port number **8000**) and **UDP** protocols (port number from **7000** to **7100**) for the installing node IP address.
3. Click **OK**.

   After adding a security group rule, download and install the agent on a database or application, depending on the add mode you chose. Database audit can be enabled only if the audited object is connected to the database audit instance.

----End

7 Step 4: Download and Install the Agent

7.1 Downloading an Agent

Download and then install the agent on the database or application based on the add mode you chose.

NOTE

Each agent has a unique ID, which is used as the key for connecting to a database audit instance. If you delete an agent and add it back, you need to download the agent again.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- You have added an agent to the database.

Procedure

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Databases**.

Step 4 In the **Instance** drop-down list, select the instance whose agent is to be downloaded.

Step 5 Click ⌄ next to the database to view details of its agent. In the **Operation** column of the agent, click **Download Agent**, to download an agent installation package.

Download the agent installation package suitable for your OS.

- Linux OS

  Download the agent whose OS is **LINUX64**.

----End

7.2 Installing an Agent (Linux OS)

You can enable database audit only after the agent is installed. This topic describes how to install the agent on a node running a Linux OS.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- You have added an agent to your database.
- You have obtained the agent installation package for the Linux OS.
- The Linux OS version of the target node is supported by the agent.

Scenarios

You can install the agent on the database or application side, depending on your database type and deployment scenario. Common database scenarios are as follows:

- Deploy DBSS for databases built on ECS/BMS. For details, see **Figure 7-1** and **Figure 7-2**.

Figure 7-1 One application connecting to multiple databases built on ECS/BMS

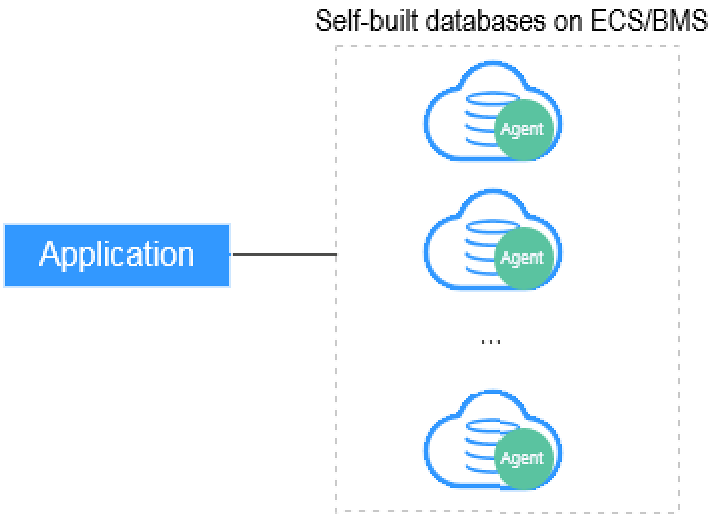
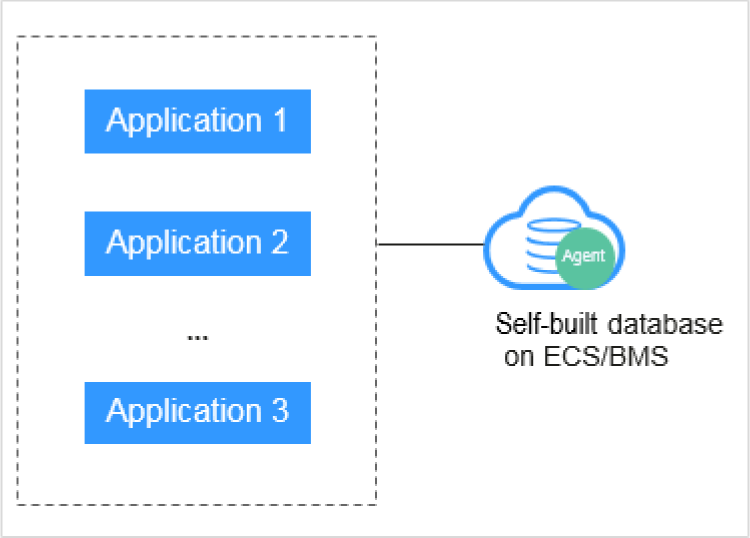


Figure 7-2 Multiple applications connecting to one database built on ECS/BMS



- Deploy DBSS for RDS databases. For details, see **Figure 7-3** and **Figure 7-4**.

Figure 7-3 One application connecting to multiple RDS databases

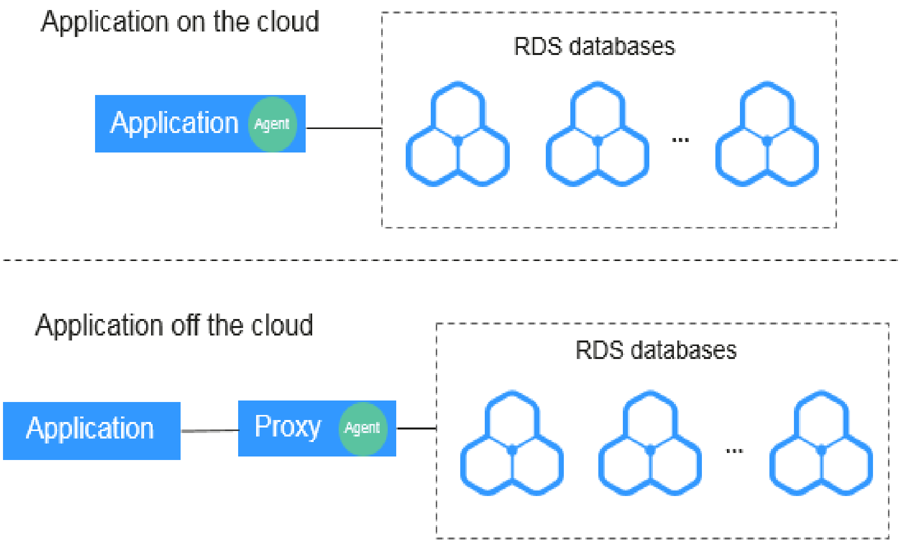


Figure 7-4 Multiple applications connecting to one RDS database

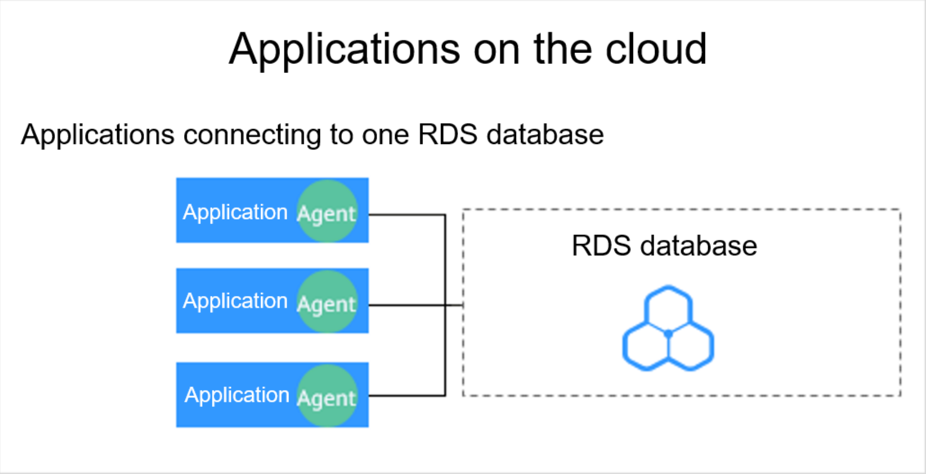

Applications on the cloud
Applications connecting to one RDS database
Application
Agent
Application
Agent
Application
Agent
RDS database

Table 7-1 describes where to install the agent in the preceding scenarios.

NOTICE

If your applications and databases (databases built on ECS/BMS) are deployed on the same node, install the agent on the database side.

Table 7-1 Agent installation scenarios

Scenario	Where to Install Agent	Audit Scope	Description
Self-built database on ECS/BMS	Database	All access records of applications that have accessed the database	• Install the agent on the database side. • If an application connects to multiple databases built on ECS/BMS, the agent must be installed on all these databases.
RDS database	Application side (if applications are deployed on the cloud)	Access records of all the databases connected to the application	• Install the agent on the application side. • If multiple applications are connected to the same RDS database, the agent must be installed on all these applications.

Scenario	Where to Install Agent	Audit Scope	Description
RDS database	Proxy side (if applications are deployed off the cloud)	Only the access records between the proxy and database. Those between the applications and database cannot be audited.	Install the agent on the proxy side.

Installing an Agent

Install the agent on the node suitable for your service scenario.

Step 1 Upload the downloaded agent installation package **xxx.tar.gz** to the node (for example, using WinSCP).

Step 2 Log in to the node as user **root** using SSH through a cross-platform remote access tool (for example, PuTTY).

Step 3 Run the following command to access the directory where the agent installation package **xxx.tar.gz** is stored:

cd *Directory_containing_agent_installation_package*

Step 4 Run the following command to decompress the installation package **xxx.tar.gz**:

tar -xvf *xxx.tar.gz*

Step 5 Run the following command to switch to the directory containing the decompressed files:

cd *Decompressed_package_directory*

Step 6 Run the following command to check whether you have the permission for executing the **install.sh** script:

ll

- If you do, go to **Step 7**.
- If you do not, perform the following operations:
  a. Run the following command to get the script execution permission:
     chmod +x install.sh
  b. Verify you have the required permissions.

Step 7 Run the following command to install the agent:

sh install.sh

NOTE

In Ubantu, run the following command to install the agent:

bash install.sh

If the following information is displayed, the agent has been installed. Otherwise, the installation fails.

```
start agent
starting audit agent
audit agent started
start success
install dbss audit agent done!
```

NOTICE

If the agent installation failed, ensure the OS version of the target node is supported and try again.

Step 8 Run the following command to view the running status of the agent program:

service audit_agent status

If the following information is displayed, the agent is running properly:

```
audit agent is running.
```

----End

8 Step 5: Enable Database Audit

By default, database audit complies with a **full audit rule**, which is used to audit all databases that are connected to the database audit instance. You can enable audit and check audit results. For details, see **Viewing the Audit Dashboard**.

Prerequisites

- You have added and installed an agent, and the agent status is **Running**.
- A security group rule has been configured for the database audit instance.

Enabling Database Audit

Step 1 Log in to the management console.

Step 2 Select a region, click ≡, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Databases**.

Step 4 Select a database audit instance from the **Instance** drop-down list.

Step 5 In the database list, click **Enable** in the **Operation** column of the database to be audited.

The **Audit Status** of the database is **Enabled**. You do not need to restart the database.

----End

Verifying Audit Results

Step 1 Run an SQL statement (for example, **show databases**) in the target database.

Step 2 Log in to the management console.

Step 3 Select a region, click ≡, and choose **Security** > **Database Security Service**. The database audit service page is displayed.

Step 4 In the left navigation pane, choose **Dashboard**.

Step 5 In the **Instance** drop-down list, select the instance that audits the target database.

Step 6 Click the **Statements** tab.

Step 7 Click 📅 next to **Time** to set the start and end time, and click **Submit**. The SQL statements entered in **Step 1** will be displayed.

----End

9 Step 6: View Audit Results

9.1 Viewing the Audit Dashboard

After connecting the database to the database audit instance, view the audit statistics, including the overall audit statistics, risk distribution, session statistics, and SQL distribution.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.
- A security group rule has been configured for the database audit instance.

Procedure

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the **Instance** drop-down list, select the instance whose audit information you want to view.

Step 4 View the overall audit statistics, risk distribution, session statistics, and SQL distribution.

- Select **All databases** or a specified database from the **Database** drop-down list to view the statistics about all databases in the instance or a specified database.
- Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days**, or click 📅 to customize start time and end time to view the statistics of the specified time range.

----End

9.2 Viewing SQL Statement Details

After connecting the database to the database audit instance, view SQL statements of the database.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.
- A security group rule has been configured for the database audit instance.

Procedure

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the **Instance** drop-down list, select the instance whose SQL statement information you want to view.

Step 4 Click the **Statements** tab.

Step 5 Query SQL statement information.

To query a specified SQL statement, perform the following steps:

- Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days**, or click 📅 to set start time and end time, and click **Search** to view SQL statements of the specified time range.
- Select **All**, **High**, **Moderate**, **Low**, or **Trusted** for **Risk Severity** and click **Search**. SQL statements of specified severity are displayed in the list.
- Click ⌄ next to **Advanced Settings**, enter the information, and click **Submit**. The specified SQL statements are displayed in the list.

NOTE

A maximum of 10,000 records can be retrieved in a query.

Step 6 In the row containing the desired SQL statement, click **Details** in the **Operation** column.

Step 7 View the SQL statement information in the **Details** dialog box. For details about related parameters, see **Table 9-1**.

NOTICE

The maximum length of an audit statement or result set is 10,240 bytes. Excessive parts are not recorded in audit logs.

Table 9-1 Parameters for details of SQL statements

Parameter	Description
Session ID	ID of an SQL statement, which is automatically generated
Database Instance	Database where an SQL statement is executed
Database Type	Type of the database where an SQL statement is executed
Database User	Database user for executing an SQL statement
Client MAC Address	MAC address of the client where an SQL statement is executed
Database MAC Address	MAC address of the database where an SQL statement is executed
Client IP Address	IP address of the client where an SQL statement is executed
Database IP Address	IP address of the database where an SQL statement is executed
Client Port	Port of the client where an SQL statement is executed
Database Port	Port of the database where the SQL statement is executed
Client Name	Name of the client where an SQL statement is executed
Operation Type	Type of an SQL statement operation
Operation Object Type	Type of an SQL statement operation object
Response Result	Response by executing an SQL statement
Affected Rows	Number of rows affected by executing an SQL statement
Started	Time when an SQL statement starts to be executed
Ended	Time when the SQL statement execution ends
SQL Statement	Name of an SQL statement
Request Result	Result of requesting for executing an SQL statement

----End

9.3 Viewing Session Distribution

After connecting the database to the database audit instance, view session distribution of the database.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.

- Database audit has been enabled.
- A security group rule has been configured for the database audit instance.

Procedure

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the **Instance** drop-down list, select the instance whose session information you want to view.

Step 4 Click the **Sessions** tab.

Step 5 View the session distribution chart.

- Select **All databases** or a specified database from the **Database** drop-down list to view the sessions about all databases in the instance or a specified database.
- Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days**, or click 📅 to set start time and end time to view the sessions of the specified time range.

----End

9.4 Viewing Audit Reports

By default, database audit complies with a full audit rule, which is used to audit all databases that are successfully connected to the database audit instance. After connecting the database to the database audit instance, generate an audit report and preview online or download it.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.
- A security group rule has been configured for the database audit instance.

Report Types

Database audit provides eight types of report templates. **Table 9-2** lists the report names. You can generate reports and set report tasks as needed.

Table 9-2 Description

Template Name	Report Types	Description
Database Security General Report	Overview report	Provides the overall audit status of the database, including risks, sessions, and login status to better manage databases.

Template Name	Report Types	Description
Database Security Compliance Report	Compliance report	This report helps database administrators and auditors detect abnormal behaviors, locate problems, and manage information.
SOX Report	Compliance report	Complies with the Sarbanes-Oxley Act (SOX) to provide statics on and evaluate database operations. This report helps database administrators and auditors detect abnormal behaviors, locate problems, and manage information.
Database Server Analysis Report	Database report	Provides statistics and analysis on active users, user IP addresses, database logins and requests, database usage duration, and database performance.
Client IP Address Analysis Report	Client report	Provides statistics on client applications, database users, and SQL statements collected from user IP addresses.
DML Command Report	Database operation report	Analyzes user and privileged operations based on DML commands.
DDL Command Report	Database operation report	Analyzes user and privileged operations based on DDL commands.
DCL Command Report	Database operation report	Analyzes user and privileged operations based on DCL commands.

Generating an Audit Report Immediately

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Reports**.

Step 4 In the **Instance** drop-down list, select the instance whose instance report you want to generate.

Step 5 Click the **Report Management** tab.

Step 6 Locate the target template, and click **Generate Report** in the **Operation** column.

Step 7 In the displayed dialog box, click 📅 to set the start time and end time of the report, and select the database for which you want to generate a report.

Step 8 Click **OK**.

The **Reports** page is displayed. You can view the report status on this page. After a report is generated, preview or download the report.

----End

Previewing or Downloading an Audit Report

Before previewing or downloading an audit report, ensure that its **Status** is **100%**.

NOTICE

To preview a report online, use Google Chrome or Mozilla FireFox.

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Reports**.

Step 4 In the **Instance** drop-down list, select the instance whose report you want to preview or download.

Step 5 Locate the target template, and click **Preview** or **Download** in the **Operation** column to preview or download the report..

----End

Setting a Report Task

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Reports**.

Step 4 In the **Instance** drop-down list, select the instance for which you want to set a report task.

Step 5 Click the **Report Management** tab.

Step 6 Locate the target template and click **Schedule Task** in the **Operation** column.

Step 7 In the displayed dialog box, set the parameters of the scheduled task.

Table 9-3 Parameters for setting a task

Parameter	Description	Example Value
Enable Task	Status of a scheduled task - ●: enabled - ○: disabled	●
Message Notifications	Enables or disables notifications. - ●: enabled - ○: disabled	●
SMN Topic	Select an existing topic from the drop-down list or click **View Topic** and create an SMN topic on the displayed page for configuring the terminals for receiving alarm notifications. For details about topics and subscriptions, see *Simple Message Notification User Guide*.	-
Report Type	Type of a report. The options are as follows: - **Daily** - **Weekly** - **Monthly**	Weekly
Execution Mode	Execution mode of the report. The options are as follows: - **Once** - **Periodically**	Periodically
Time	Time when the report is executed	10:00
Format	Only the PDF format is supported.	PDF
Database	Database for which you want to execute the report task	-

Step 8 Click **OK**.

----End

10 Configuring Audit Rules

10.1 Adding Audit Scope

By default, database audit complies with a full audit rule, which is used to audit all databases that are successfully connected to database audit. You can also add audit scope and specify the databases to be audited.

NOTICE

By default, the full audit rule takes effect even if other rules exist. To make another audit rule take effect, disable the full audit rule first.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.

Procedure

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree, choose **Rules**.

Step 4 In the **Instance** drop-down list, select an instance to add audit scope.

Step 5 **Add Audit Scope** above the audit scope list.

NOTE

- By default, database audit complies with a **full audit rule**, which is used to audit all databases that are connected to the database audit instance. This audit rule is enabled by default. You can disable it but cannot delete it.
- To make a custom rule take effect, disable the full audit rule first.

Step 6 In the displayed dialog box, set the audit scope.

Table 10-1 Parameters

Parameter	Description	Example Value
Name	Name of the custom audit scope	audit00
Database Name	Select a database or **ALL**.	db03
Operations	Audited operation type. It can be **Login** or **Operation**. When you select the **Operation** check box, you can select **All operations** or the operations in **DDL**, **DML**, and **DCL**.	Login
Database Account	(Optional) Database username. You can specify multiple accounts, separated by commas (,).	-
Exception IP Address	(Optional) IP addresses that do not need to be audited. **NOTE** If an IP address is set as both a source and an exception IP address, the IP address will not be audited.	-
Source IP Address	(Optional) IP address or IP address range used for accessing the database to be audited The IP address must be an internal IP address in IPv4 or IPv6 format.	-
Source Port	(Optional) Port number used for accessing the database to be audited	-

Step 7 Click **OK**.

When the audit scope is added successfully, it is displayed in the audit scope list in the state of **Enabled**.

----End

Related Operations

In addition to adding the audit scope, you can enable or disable SQL injection detection and add risky operations to set audit rules for database audit.

10.2 Enabling or Disabling SQL Injection Detection

SQL injection detection is enabled by default. You can disable or enable the detection rules.

NOTICE

One piece of audited data can match only one SQL injection detection rule.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- You can enable SQL injection detection when the status is **Disabled**.
- You can disable SQL injection detection when the status is **Enabled**.

Enabling SQL Injection Detection

SQL injection detection is enabled by default. You can disable the detection rules as required. When an SQL injection detection rule is disabled, the audit rule does not take effect.

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree, choose **Rules**.

Step 4 In the **Instance** drop-down list, select the instance for which you want to disable SQL injection detection.

Step 5 Click the **SQL Injection** tab.

Step 6 Locate the target rule, and click **Disable** in the **Operation** column.

When the status of an SQL injection detection rule is **Disabled**, SQL injection detection is disabled successfully.

----End

Follow-Up Procedure

To restart an SQL injection detection rule, click **Enable** in the **Operation** column of the target rule.

When the status of an SQL injection detection rule is **Enabled**, SQL injection detection is enabled successfully.

10.3 Adding Risky Operations

Database audit has built-in rules for detecting data reduction and slow SQL statements. You can also add risky operations and customize detection rules.

After enabling database audit, add and configure risky operations for audit.

NOTICE

One piece of audited data can match only one risky operation rule.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.

Procedure

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree, choose **Rules**.

Step 4 In the **Instance** drop-down list, select an instance to add risky operations. Click the **Risky Operations** tab. Click **Add** above the risky operation list.

Step 5 On the **Add Risky Operation** page, set the basic information and client IP address. .

Table 10-2 Parameters

Parameter	Description	Example Value
Name	Custom name of a risky operation	test
Risk Severity	Severity of a risky operation. The options are as follows: - **High** - **Moderate** - **Low** - **No risks**	High
Status	Status of a risky operation - ◉: enabled - ○: disabled	
Select Database	Database that the risky operation will be applied to You can select **ALL** or a specific database.	-
Client IP Address or IP Range	IP address or IP address range of the client The IP address can be an IPv4 address (for example, 192.168.1.1) or an IPv6 address (for example, fe80:0000:0000:0000:0000:0000:0000:0000).	192.168.0.0

Step 6 Set the operation type, operation object, and execution result. For details about related parameters, see **Table 10-3**.

Table 10-3 Parameters

Parameter	Description	Example Value
Operations	Type of a risky operation, including **Login** and **Operation** When you select the **Operation** check box, you can select **All operations** or the operations in **DDL**, **DML**, and **DCL**.	Operation
Objects	Enter the target database, target table, and field information after clicking **Add Operation Object**. Click **OK** to add an operation object.	-
Results	Set **Affected Rows** and **Operation Duration**. The operation conditions are as follows: ● **Greater than** ● **Less than** ● **Equal To** ● **Equal to or greater than** ● **Less than or equal to**	-

Step 7 Click **Save**.

----End

10.4 Configuring Privacy Data Protection Rules

To mask sensitive information in entered SQL statements, you can enable the function of masking privacy data and configure masking rules to prevent sensitive information leakage.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.

Procedure

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree, choose **Rules**.

Step 4 In the **Instance** drop-down list, select the instance whose privacy data protection rule is to be configured.

Step 5 Click the **Privacy Data Protection** tab.

Step 6 Enable or disable **Store Result Set** and **Mask Privacy Data**.

- **Store Result Set**

  You are advised to disable ○. After this function is disabled, database audit will not store the result sets of user SQL statements.

  Do not enable this function if you want to prepare for PCI DSS/PCI 3DS CSS certification.

- **Mask Privacy Data**

  You are advised to enable ●. After this function is enabled, you can configure masking rules to prevent privacy data leakage.

Step 7 Click **Add Rule**. In the displayed **Add Rule** dialog box, set the data masking rule.

Table 10-4 Rule parameters

Parameter	Description	Example Value
Rule Name	Name of a rule	test
Regular Expression	Regular expression that specifies the sensitive data pattern	-
Substitution Value	Value used to replace sensitive data specified by the regular expression	###

Step 8 Click **OK**.

A masking rule in the **Enabled** status is added to the rule list.

----End

Verifying a Rule

Perform the following steps to check whether a rule takes effect. The audit information about military officer card No. in a MySQL database is used as an example.

Step 1 Enable **Mask Privacy Data**, and ensure the "Military officer card NO." masking rule is enabled.

Step 2 Log in to the database as user **root** through the MySQL database client.

Step 3 On the database client, enter an SQL statement.

select * from db where HOST="*Military officer card No.*";

Step 4 In the navigation pane, choose **Dashboard**.

Step 5 In the **Instance** drop-down list, select the instance whose SQL statement information you want to view. Click the **Statements** tab.

Step 6 In the **Instance** drop-down list, select the instance whose SQL statement information you want to view.

Step 7 Click the **Statements** tab.

Step 8 Set filtering conditions to find the entered SQL statement.

Step 9 In the row containing the SQL statement, click **Details** in the **Operation** column.

Step 10 Check the SQL statement information in **SQL Statement**.

----End

Common Operations

After adding a user-defined masking rule, you can perform the following operations on it:

- Disable

  Locate the row that contains the rule to be disabled and click **Disable** in the **Operation** column. A disabled rule cannot be used.

- Edit

  Locate the row that contains the rule to be modified, click **Edit** in the **Operation** column, and modify the rule in the displayed dialog box.

- Delete

  Locate the row that contains the rule to be deleted, click **Delete** in the **Operation** column, and click **OK** in the displayed dialog box.

11 Viewing Monitoring Information

11.1 Viewing the System Monitoring

This section describes how to view the system monitoring of database audit and learn about system resources and traffic usage.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.

Procedure

Step 1 Log in to the management console.

Step 2 Select a region, click ≡, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Instances**.

Step 4 Click an instance name and then click the **Monitoring** tab. The **System Monitoring** page is displayed.

Step 5 View the system monitoring information.

Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days**, or click 📅 to customize start time and end time to view the system monitoring information of the specified time range.

----End

11.2 Viewing the Alarms

This section describes how to view and confirm alarms of database audit.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.
- You have configured alarm notifications.

Procedure

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Instances**.

Step 4 Click the name of an instance, click the **Monitoring** tab, and then the **Alarm Monitoring** tab.

Step 5 View the alarm information. For details about related parameters, see **Table 11-1**.

Table 11-1 Parameters of alarms

Parameter	Description
Time	Time when an alarm occurred.
Type	Alarm type. The options are as follows: ● Risky operations ● CPU exceptions ● Memory exceptions ● Disk exceptions ● Insufficient audit log storage ● Log backup to OBS failed
Alarm Risk Severity	Risk severity of an alarm. The options are as follows: ● **High** ● **Moderate** ● **Low**
Cleared	Time when an alarm is cleared
Confirmed Or Not	Confirmation status of an alarm. Click ▽ to filter alarms in **Unconfirmed** or **Confirmed** state.
Description	Description of an alarm

To query specified alarms, perform the following steps:

- Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days** for **Time**, or click 📅 to set start time and end time, and click **OK** to view alarms of the specified time range.

- Select **All**, **High**, **Moderate**, or **Low** for **Risk Severity**. Alarms of specified severity are displayed in the list.
- Select an alarm type, and alarms of specified alarm type is displayed in the list.

----End

Follow-Up Procedure

To confirm an alarm, click **Confirm** in the **Operation** column of the alarm.

NOTE

You can select multiple alarms to be confirmed and click **Batch Confirm** to batch confirm alarms.

12 Backing Up and Restoring Database Audit Logs

Database audit logs can be backed up to OBS buckets to achieve high availability for disaster recovery. You can back up or restore database audit logs as required.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.

Precautions

- Audit logs are backed up to OBS. Buckets are automatically created for you and billed per use.

Automatically Backing Up Database Audit Logs

Step 1 Log in to the management console.

Step 2 Select a region, click ≡, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Settings**.

Step 4 In the **Instance** drop-down list, select the required instance and click the **Backup and Restoration** tab.

Step 5 Click **Configure**. In the displayed dialog box, set the parameters. For details about related parameters, see **Table 12-1**.

Table 12-1 Parameters

Parameter	Description	Example Value
Automatic Backup	Status of automatic backup ● ◉: enabled ● ○: disabled	◉
Backup Period	Automatic backup period. Its options are as follows: ● **Daily** ● **Hourly**	Daily
Started	Start time of the backup. Click 📅 to configure.	2020/01/14 20:27:08

Step 6 Click **OK**.

NOTE

After the automatic backup function is configured, new data in the database will be backed up one hour later. Then you can view the backup information.

----End

Restoring Database Audit Logs

After backing up database audit logs, you can restore the audit logs as required.

NOTICE

Restoring logs is risky. Therefore before restoring logs, ensure that the backup log data is correct or complete.

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Settings**.

Step 4 In the **Instance** drop-down list, select the required instance and click the **Backup and Restoration** tab.

Step 5 In the **Operation** column of the backup log to be restored, click **Restore Log**.

Step 6 In the displayed dialog box, click **OK**.

----End

13 Other Operations

13.1 Managing Database Audit Instances

After applying for a database audit instance, you can view, enable, restart, disable, or delete the instance.

Prerequisites

- Before restarting and disabling an instance, ensure that its **Status** is **Running**.
- Before enabling or deleting an instance, ensure that its **Status** is **Disabled**.

Deleting an Instance

You can delete a database audit instance that is no longer needed. You can also delete the associated EIP at the same time.

Step 1 Log in to the management console.

Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 4 In the navigation tree on the left, choose **Instances**.

Step 5 In the row containing the desired instance, choose **More** > **Delete** in the **Operation** column.

Step 6 In the displayed dialog box, click **OK**.

----End

Viewing the Instance

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Instances**.

Step 4 View the database audit instances information. For details about related parameters, see **Table 13-1**.

NOTE

- You can click the name of an instance to view its overview.
- Select an instance status from the **All statuses** drop-down list in the upper right corner of the list, or enter a key word of an instance to search for it.

Table 13-1 Parameters

Parameter	Description
Instance Name/ID	Name and ID of an instance. Instance ID is automatically generated.
Specifications	Edition of an instance
Status	Running status of an instance. The options are as follows: ● **Running** ● **Creating** ● **Faulty** ● **Disabled** ● **Frozen** ● **Frozen for legal management** ● **Frozen due to abuse** ● **Frozen due to lack of identity verification** ● **Frozen for partnership** ● **Creation failed**
Associated Databases/ Total Databases	Number of databases an instance has associated with and Number of databases an instance supports
Operation	Configure audit rules for an instance, or restart or enable the instance.

NOTE

You can perform the following operations on instances as required:

- Restart

  Locate the row that contains the desired instance, choose **More** > **Restart** in the **Operation** column, and click **OK** in the displayed dialog box.

- Enable

  Locate the row that contains the desired instance, choose **More** > **Enable** in the **Operation** column, and click **OK** in the displayed dialog box.

- Disable

  Locate the row that contains the desired instance, choose **More** > **Disable** in the **Operation** column, and click **OK** in the displayed dialog box. When an instance is disabled, the audit function is disabled for the databases on the instance.

- Delete

  Locate the row that contains the instance that failed to be created, choose **More** > **Delete** in the **Operation** column, and click **Delete** in the displayed dialog box. Deleted instances will not be displayed in the instance list.

----End

13.2 Viewing the Instance Overview

This section describes how to view the instance overview, including the basic information, network settings and associated databases.

Prerequisites

You have applied for a database audit instance and the **Status** is **Running**.

Procedure

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Instances**.

Step 4 Click the name of the instance whose information you want to view. The **Overview** page is displayed.

Step 5 View the basic information, network settings, and associated databases about the instance. For details about related parameters, see **Table 13-2**.

Table 13-2 Parameters of the instance overview

Category	Parameter	Description
Basic Info	Name	Instance name. You can click ✎ next to **Name** to change it.

Category	Parameter	Description
	Status	Running status of an instance. The options are as follows: ● **Running** ● **Creating** ● **Faulty** ● **Disabled** ● **Frozen** ● **Frozen for legal management** ● **Frozen due to abuse** ● **Frozen due to lack of identity verification** ● **Frozen for partnership** ● **Creation failed**
	ID	Instance ID, which is automatically generated
	AZ	Availability Zone (AZ) where an instance resides
	Version	Version of an instance
	Remarks	Remarks about an instance. You can click ✎ next to **Remarks** to modify it.
	Edition	Edition of an instance
	Created	Time when an instance is created
Network Settings	VPC	VPC where an instance resides
	Security Group	Security group where an instance resides
	Subnet	Subnet where an instance resides
	Private IP Address	IP address of an instance
Associated Database	-	Database information associated with an instance Click **Manage Database**, and the **Databases** page is displayed.

----End

13.3 Managing Databases and Agents

After adding a database successfully, you can view, disable or delete the database. After adding an agent to the database, you can view, disable or delete the agent.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- You have added a database successfully.
- Before disabling a database, ensure that **Audit Status** of the database is **Enabled**.

Viewing the Database Information

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Databases**.

Step 4 In the **Instance** drop-down list, select the instance whose database you want to view.

Step 5 View the database information. For details about related parameters, see **Table 13-3**.

NOTE

Select an audit status from the **All audit statuses** drop-down list in the upper right corner of the list, or enter a key word of a database to search for it.

Table 13-3 Parameters

Parameter	Description	Example Value
Database Information	Name, type, and version of a database	-
Character Set	Encoding character set of the database	UTF8
IP Address/ Port	IP address of the database	192.168.0.104 3306
Instance	Database instance name	-
OS	Operating system of the database	LINUX64
Audit Status	Audit status of the database. The options are as follows: ● **Enabled** ● **Disabled**	Enabled
Agent	Click **Add** to add an agent for the database.	-

NOTE

You can perform the following operations on a database you added:

- Disable
  - Locate the row that contains the database to be disabled, click **Disable** in the **Operation** column, and click **OK** in the displayed dialog box. The **Audit Status** of the database will change to **Disabled**.
  - When a database is disabled, database audit is disabled for the database.
- Delete
  - Locate the row that contains the database to be deleted, click **Delete** in the **Operation** column, and click **OK** in the displayed dialog box.
  - You need to add the database again if a database is deleted and you want to audit the database.

----End

Viewing an Agent

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Databases**.

Step 4 In the **Instance** drop-down list, select the instance whose agent you want to view.

Step 5 Click ⌄ on the left of the database to expand the agent details. For details about related parameters, see **Table 13-4**.

Table 13-4 Parameters of an agent

Parameter	Description
Agent ID	Agent ID, which is automatically generated
Installing Node Type	Type of the installing node. The options are **Database** and **Application**.
Installing Node IP Address	IP address of the node where an agent is installed
OS	Agent OS
Audited NIC Name	NIC name of an installing node
CPU Threshold (%)	CPU threshold of the installing node. The default value is **80**. **NOTE** The agent on a node will stop working if the CPU usage of the node exceeds this threshold. You can scale up CPU resources to avoid this problem.

Parameter	Description
Memory Threshold (%)	Memory threshold of the installing node. The default value is **80**. **NOTE** The agent on a node will stop working if the memory usage of the node exceeds this threshold. You can scale up memory resources to avoid this problem.
General	Whether an agent is a general-purpose agent.
SHA256Sum	Verification value of the agent installation package.
Status	Running status of the installing node

NOTE

You can perform the following operations on an agent you added:

- Disable
  - Locate the row that contains the agent to be disabled, click **Disable** in the **Operation** column, and click **OK** in the displayed dialog box. The status of the agent will change to **Disabled**.
  - When an agent is disabled, database audit is disabled for the associated database.
- Delete
  - Locate the row that contains the agent to be deleted, click **Delete** in the **Operation** column, and click **OK** in the displayed dialog box.
  - After an agent is deleted, add another agent again if you want to audit the database.

----End

13.4 Uninstalling an Agent

You can uninstall an agent from the database or application if you do not need to audit the database.

Prerequisites

You have installed an agent on the desired node.

Uninstalling the Agent from a Linux OS

Step 1 Log in to the node where the agent is installed as user **root** using SSH through a cross-platform remote access tool (such as PuTTY).

Step 2 Run the following command to access the directory where the decompressed **xxx.tar.gz** agent installation package is stored:

cd *directory containing the decompressed agent installation package*

Step 3 Run the following command to check whether you have the permission for executing the **uninstall.sh** script:

ll

- If you do, go to **Step 4**.
- If you do not, perform the following operations:
  1. Run the following command to get the script execution permission:

     chmod +x uninstall.sh
  2. Verify you have the required permissions.

Step 4 Run the following command to uninstall the agent:

sh uninstall.sh

If the following information is displayed, the agent has been uninstalled successfully:

```
uninstall audit agent...
exist os-release file
stopping audit agent
audit agent stopped
stop audit_agent success
service audit_agent does not support chkconfig
uninstall audit agent completed!
```

----End

13.5 Management an Audit Scope

After adding an audit scope, you can view, enable, edit, disable, or delete the audit scope.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- The audit scope has been added.
- Before enabling, editing, or deleting the audit scope, ensure that the status of audit scope is **Disabled**.
- Before disabling the audit scope, ensure that the status of audit scope is **Enabled**.

Precautions

By default, database audit complies with a **full audit rule**, which is used to audit all databases that are connected to the database audit instance. This audit rule is enabled by default. You can disable it but cannot delete it.

Viewing the Audit Scope

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree, choose **Rules**.

Step 4 In the **Instance** drop-down list, select an instance to view audit scope.

Step 5 View the audit scope information. For details about related parameters, see **Table 13-5**.

NOTE

Enter the key word of an audit scope to search.

Table 13-5 Parameters

Parameter	Description
Name	Name of the audit scope
Exception IP Address	Whitelisted IP addresses within the audit scope
Source IP Address	IP address or IP address range used for accessing the database
Source Port	Port number of the IP address to be audited
Database Name	Database in the audit scope
Database Account	Database username
Status	Status of the audit scope. The options are as follows: ● **Enabled** ● **Disabled**

NOTE

You can perform the following operations on audit scopes as required:

- Enable

  Locate the row that contains the audit scope to be enabled, and click **Enable** in the **Operation** column. Databases within the scope will be audited.
- Edit

  Locate the row that contains the audit scope to be edited, click **Edit** in the **Operation** column, and modify the scope in the displayed dialog box.
- Disable

  Locate the row that contains the audit scope to be disabled, click **Disable** in the **Operation** column, and click **OK** in the displayed dialog box. When the audit scope is disabled, the audit scope rule will not be executed in the audit.
- Delete

  Locate the row that contains the audit scope to be deleted, click **Delete** in the **Operation** column, and click **OK** in the displayed dialog box. You need to add the audit scope again if it is deleted and you want to audit it.

----End

13.6 Viewing Information About SQL Injection Detection

This section describes how to view SQL injection detection information of a database audit instance.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.

Procedure

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree, choose **Rules**.

Step 4 In the **Instance** drop-down list, select the instance for which you want to view SQL injection detection. Click the **SQL Injection** tab.

Step 5 View information about SQL injection detection. For details about related parameters, see **Table 13-6**.

NOTE

Select a risk severity from the **All risk severities** drop-down list in the upper right corner of the list, or enter a key word of an SQL injection rule name to search.

Table 13-6 Parameters

Parameter	Description
Name	Name of the SQL injection detection
Command Feature	Command features of the SQL injection detection
Risk Severity	Risk level of the SQL injection detection. The options are as follows: ● **High** ● **Moderate** ● **Low** ● **No risks**
Status	Status of the SQL injection detection. The options are as follows: ● **Enabled** ● **Disabled**

----End

13.7 Managing Risky Operations

After adding a risky operation, you can view the risk, enable, edit, disable, or delete the risky operation, or set its priority.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- The risky operation has been added.
- Before enabling the risky operation, ensure that its status is **Disabled**.
- Before disabling the risky operation, ensure that its status is **Enabled**.

Sets the Priority of the Risky Operation

Step 1 Log in to the management console.

Step 2 Select a region, click ≡, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree, choose **Rules**.

Step 4 In the **Instance** drop-down list, select an instance to set risky operation priority. Click the **Risky Operations** tab.

Step 5 Locate the target risky operation, and click **Set Priority** in the **Operation** column.

Step 6 In the displayed dialog box, select a priority and click **OK**.

----End

Viewing the Risky Operation

Step 1 Log in to the management console.

Step 2 Select a region, click ≡, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree, choose **Rules**.

Step 4 In the **Instance** drop-down list, select an instance to view risky operations.

Step 5 Click the **Risky Operations** tab.

Step 6 View risky operations information. For details about related parameters, see Table 13-7.

NOTE

Select a risk severity from the **All risk severities** drop-down list in the upper right corner of the list, or enter a key word of a risky operation name to search.

Table 13-7 Parameters

Parameter	Description
Name	Name of the risky operation
Category	Category of the risky operation
Feature	Feature of the risky operation
Risk Severity	Risk severity of the risky operation. The options are as follows: ● **High** ● **Moderate** ● **Low** ● **No risks**
Status	Status of the risky operation. The options are as follows: ● **Enabled** ● **Disabled**

NOTE

You can perform the following operations on risky operations as required:

- Enable

  Locate the row that contains the risky operation to be enabled, and click **Enable** in the **Operation** column. The operation will be audited.

- Edit

  Locate the row that contains the risky operation to be edited, click **Edit** in the **Operation** column, and modify the operation in the displayed dialog box.

- Disable

  Locate the row that contains the risky operation to be disabled, click **Disable** in the **Operation** column, and click **OK** in the displayed dialog box. When a risky operation is disabled, the risky operation rule will not be executed in the audit.

- Delete

  Locate the row that contains the risky operation to be deleted, click **Delete** in the **Operation** column, and click **OK** in the displayed dialog box. You need to add the risky operation again if a risky operation is deleted and you need to audit its rule.

----End

13.8 Managing Privacy Data Protection Rules

You can view, enable, edit, disable, or delete data masking rules.

Prerequisites

You have applied for a database audit instance and the **Status** is **Running**.

Viewing Privacy Data Protection Rules

Step 1 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 2 In the navigation tree, choose **Rules**.

Step 3 In the **Instance** drop-down list, select an instance to view its privacy data protection rule.

Step 4 Click the **Privacy Data Protection** tab.

Step 5 View the rules. For details about related parameters, see **Table 13-8**.

NOTE

- **Store Result Set**

  You are advised to disable . After this function is disabled, database audit will not store the result sets of user SQL statements.

  Do not enable this function if you want to prepare for PCI DSS/PCI 3DS CSS certification.

- **Mask Privacy Data**

  You are advised to enable . After this function is enabled, you can configure masking rules to prevent privacy data leakage.

Table 13-8 Masking rule parameters

Parameter	Description
Rule Name	Rule name
Rule Type	Rule type
Regular Expression	Regular expression that specifies the sensitive data pattern
Substitution Value	Value used to replace sensitive data specified by the regular expression
Status	Status of a rule. Its value can be: - **Enabled** - **Disabled**

NOTE

You can perform the following operations on a rule:

- Disable

  Locate the row that contains the rule to be disabled and click **Disable** in the **Operation** column. A disabled rule cannot be used.

- Edit

  Locate the row that contains the rule to be modified, click **Edit** in the **Operation** column, and modify the rule in the displayed dialog box.

- Delete

  Locate the row that contains the rule to be deleted, click **Delete** in the **Operation** column, and click **OK** in the displayed dialog box.

----End

13.9 Managing Audit Reports

By default, database audit complies with a full audit rule, which is used to audit all databases that are successfully connected to the database audit instance. After connecting the database to the database audit instance, view report templates and report results.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.

Viewing a Report

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Reports**.

Step 4 In the **Instance** drop-down list, select the instance whose report information you want to view.

Step 5 View the report information.

NOTE

- Enter a report name in the upper right corner to search.
- A real-time report is automatically generated in PDF format.
- Locate the row that contains the report to be deleted, click **Delete** in the **Operation** column, and click **OK** in the displayed dialog box. When a report is deleted, you need to manually generate a report if you want to view the report result.

----End

Viewing a Report Template

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Reports**.

Step 4 In the **Instance** drop-down list, select the instance whose report template you want to view.

Step 5 Click the **Report Management** tab.

Step 6 View the report template information.

NOTE

- Report types include **Compliance report**, **Overview report**, **Database report**, **Client report**, and **Database operation report**.
- You can enable or disable scheduled tasks, or set their frequency to daily, weekly, or monthly.
- To modify the scheduled task of a report template, click **Schedule Task** in the **Operation** column. Modify and save the settings, click **Generate Report**, and you can check the reports.

----End

13.10 Managing Backup Audit Logs

After backing up audit logs, you can view or delete backup audit logs.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.
- You have backed up audit logs.

Viewing Backup Audit Logs

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Settings**.

Step 4 In the **Instance** drop-down list, select the instance whose log template you want to view.

Step 5 Click the **Backup and Restoration** tab.

Step 6 View the backup audit log information. For details about related parameters, see **Table 13-9**.

Click 📅 in the upper right corner of the list and select the start time and end time to view backup logs in a specified time range.

Table 13-9 Parameters of audit logs

Parameter	Description
Log Name	Name of a log, which is automatically generated
Backup Time	Time when a log is backed up
File Size	Log file size
Backup Mode	Log backup mode.
Backup Scope	Backup time window
Task Status	Backup status of a log

NOTE

Locate the row that contains the log to be deleted, click **Delete** in the **Operation** column, and click **OK** in the displayed dialog box.

----End

13.11 Viewing Operation Logs

This section describes how to view operation logs of a database audit instance.

Prerequisites

You have applied for a database audit instance and the **Status** is **Running**.

Procedure

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Instances**.

Step 4 Click the name of the instance whose operation logs you want to view. The **Overview** page is displayed.

Step 5 Click the **Logs** tab. The log list page is displayed.

Step 6 View operation logs. For details about related parameters, see **Table 13-10**.

NOTE

Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days**, or click 📅 to set start time and end time to view the operation logs of a specified time range.

Table 13-10 Parameters

Parameter	Description
Username	User who performs the operation
Time	Time when the operation was performed
Function	Function of the operation
Action	Action of the operation
Operation Object	Object of the operation
Description	Description of the operation
Result	Result of the operation

----End

14 FAQs

14.1 Product Consulting

14.1.1 What Is Database Audit?

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

14.1.2 What Are the Differences Between DBSS Database Audit and RDS SQL Audit?

The following table describes the differences between DBSS database audit and RDS SQL audit regarding their functions and applicable scope.

Table 14-1 Audit service differences

Audit	Function	Scenario
RDS SQL audit	Only SQL access operations are recorded.	Edit only RDS databases.
DBSS audit	All the unsafe operations on the database are audited. DBSS records SQL access, performs security scans and statistical analysis, identifies risks, and generates reports to help you enhance the security of databases on the cloud.	Edit all the database scenarios, including user-built databases.

14.1.3 What Editions Does DBSS Provide?

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

Table 14-2 describes the database audit editions.

Table 14-2 Database audit editions

Version	Maximum Databases	System Resource	Performance
Basic	3	- CPU: 4 vCPUs - Memory: 16 GB - Disk: 500 GB	- Peak QPS: 3,000 queries/second - Database load rate: 3.6 million statements/hour - Stores 400 million online SQL statements. - Stores 5 billion archived SQL statements.
Professional	6	- CPU: 8 vCPUs - Memory: 32 GB - Disk: 1 TB	- 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.

14.1.4

DBSS protects databases built on Elastic Cloud Server (ECS) and Bare Metal Server (BMS), and RDS instances within the same VPC and its subnets. Due to network restrictions, DBSS cannot protect databases built and RDS instances on ECSs and BMSs if they are not in the same VPC and its subnets.

14.1.5 What Databases Does DBSS Support?

DBSS supports the following databases on the management console:

- RDS instances
- Databases built on ECS
- Databases built on BMS

14.1.6

14.2 Functions

14.2.1 Does Database Audit (in Bypass Mode) Affect My Services?

No. Your databases are audited in out-of-path mode. Database audit neither affects your services nor conflicts with local audit tools.

14.2.2 What Are the Functions of Database Audit?

Database audit is deployed in out-of-path pattern. You can perform flexible audit on databases built on ECS, BMS, and RDS without affecting services. Database audit provides the following functions:

- 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 learn the database situation in a timely manner.
- 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.

14.2.3 Supported Database Types

Database audit supports the following database types and versions.

Table 14-3 Database types and versions supported by database audit

Database Type	Version
MySQL	● 5.0, 5.1, 5.5, 5.6, 5.7 ● 8.0 (8.0.11 and earlier)
Oracle	● 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

Database Type	Version
SQL Server	● 2008, 2008R2 ● 2012 ● 2014 ● 2016 ● 2017
DWS	● 1.5
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8
Gbase XDM Cluster	V8.0
GaussDB for MYSQL	MySQL 8.0
GaussDB	1.4 Enterprise Edition
DAMENG	DM8
KINGBASE	V8

14.2.4 What OSs Can I Install the Database Audit Agent On?

To use database audit, you need to install its agent on the required database, application, or proxy side, and then connect to the database audit instance.

The database audit agent can run on 64-bit Linux. The following table describes the supported OSs.

- For more information, see **Table 14-4**.

Table 14-4 Supported Linux OS versions

System Name	System version
CentOS	● CentOS 6.3 (64bit) ● CentOS 6.5 (64bit) ● CentOS 6.8 (64bit) ● CentOS 6.9 (64bit) ● 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)
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)
EulerOS	● Euler 2.2 (64bit) ● Euler 2.3 (64bit)
Oracle Linux	● Oracle Linux 6.9 (64bit) ● Oracle Linux 7.4 (64bit)

14.2.5 Does Database Audit Support Bidirectional Audit?

Yes. In bidirectional audit, both requests and responses to the database are audited.

Bidirectional audit is used for database audit by default.

14.2.6 Can I Audit Databases Across Different VPCs?

Yes. To audit databases in different VPCs, ensure the VPCs can communicate with each other. You can create peering connections between the VPCs. For details, see .

14.2.7 Can Applications Using TLS Connections Be Audited?

No. Applications using TLS are encrypted.

14.2.8 How Long Is the Database Audit Data Stored by Default?

Database audit can store online and archived audit data for at least 180 days.

On the **Dashboard** of database audit, you can select the database and audit period to view audit data.

However, the storage duration also depends on the disk capacity of the log database. To store your audit data long enough, you are advised to:

- Choose a database audit edition suitable for your business.
  - To audit a small volume of data, apply for the basic edition.
  - To audit a large volume of data, apply for the professional edition.

  For more information, see **Table 14-5**.
- Back up audit logs.

Table 14-5 Database audit editions

Version	Maximum Databases	System Resource	Performance
Basic	3	● CPU: 4 vCPUs ● Memory: 16 GB ● Disk: 500 GB	● Peak QPS: 3,000 queries/second ● Database load rate: 3.6 million statements/hour ● Stores 400 million online SQL statements. ● Stores 5 billion archived SQL statements.

Version	Maximum Databases	System Resource	Performance
Professional	6	● CPU: 8 vCPUs ● Memory: 32 GB ● Disk: 1 TB	● 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.

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 apply for a new one.
- Online SQL statements are counted based on the assumption that the capacity of an SQL statement is 1 KB.

14.2.9 How Soon Can I Receive an Alarm Notification If an Exception Occurs in Database Audit?

When database audit is running properly, if an exception occurs, you will receive an alarm notification within 5 minutes.

If you set alarm notifications, when database audit is running properly, the system generates an alarm notification when a metric of a database audit instance resource (CPU, memory, or disk) exceeds the alarm threshold. You can receive the notification within about 5 minutes.

14.2.10 Is the Total Number Of Alarms Every Day the Same as that of Emails?

Yes. One alarm message corresponds to one email notification.

14.2.11 Why I Cannot Preview the Database Security Audit Report Online?

To preview a report online, use Google Chrome or Mozilla FireFox.

14.2.12 If I Use Middleware at the Service Side, Will It Affect Database Audit?

No.

Middleware is a type of software deployed between applications and software including OSs, networks, and databases. Middleware provides an environment for application operation and development, helping users flexibly and efficiently develop and integrate complex application software.

Database audit is deployed in out-of-path mode. The database audit agent (installed on database or application nodes) obtains database access traffic, uploads the traffic to the audit system, receives commands issued by the audit system, and reports database status.

Using middleware on the service side does not affect the agent during SQL listening or auditing.

If database audit cannot obtain any data, troubleshoot the problem by referring to:

14.2.13 What Should I Do If an Alarm of Insufficient DBSS Capacity Is Displayed?

The disk capacity of an existing DBSS instance cannot be expanded. If you find your disk space insufficient to store logs for at least 180 days, as required by compliance standards, you need to back up the logs.

This alarm indicates that the disk usage of your instances is high. You are advised to back up data every hour. If you have enabled backup, ignore this alarm.

14.3 Agent

14.3.1 Which Functions Do the Database Audit Agent Provide?

To use database audit, you need to install its agent on database nodes or application nodes.

The database audit agent delivers the following functions:

- Obtain database access traffic
- Upload traffic data to the audit system
- Receive configuration commands from the audit system
- Report database status monitoring data

14.3.2 On What Linux OSs Can I Install the Agent?

To use database audit, you need to install its agent on database nodes or application nodes.

The database audit agent can be installed on a 64-bit Linux OS. **Table 14-6** provides more details.

Table 14-6 Supported Linux OS versions

System Name	System version
CentOS	● CentOS 6.3 (64bit) ● CentOS 6.5 (64bit) ● CentOS 6.8 (64bit) ● CentOS 6.9 (64bit) ● 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)
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)
EulerOS	● Euler 2.2 (64bit) ● Euler 2.3 (64bit)
Oracle Linux	● Oracle Linux 6.9 (64bit) ● Oracle Linux 7.4 (64bit)

14.3.3 What Is the Process Name of the Database Audit Agent?

Linux OS

The process name of the agent is **/opt/dbss_audit_agent/bin/audit_agent**

After installing the agent, you can perform the following steps to view its operating status:

Step 1 Log in to the node where the agent is installed as user **root** by using a cross-platform remote access tool (for example, PuTTY) via SSH.

Step 2 Run the following command to view the operating status of the agent:

ps -ef|grep audit_agent

- If the following information is displayed, the agent is running properly:
```
/opt/dbss_audit_agent/bin/audit_agent
```
- If no information is displayed, the agent does not run properly.

----End

14.3.4 (Linux OS) What Should I Do If I Lack the Permission to Run the Agent Installation Script?

Run the following command on the node where the agent will be installed to add the execute permission on the installation script:

chmod +x install.sh

14.3.5 (Linux OS) Where Are the Logs of the Database Audit Agent Saved?

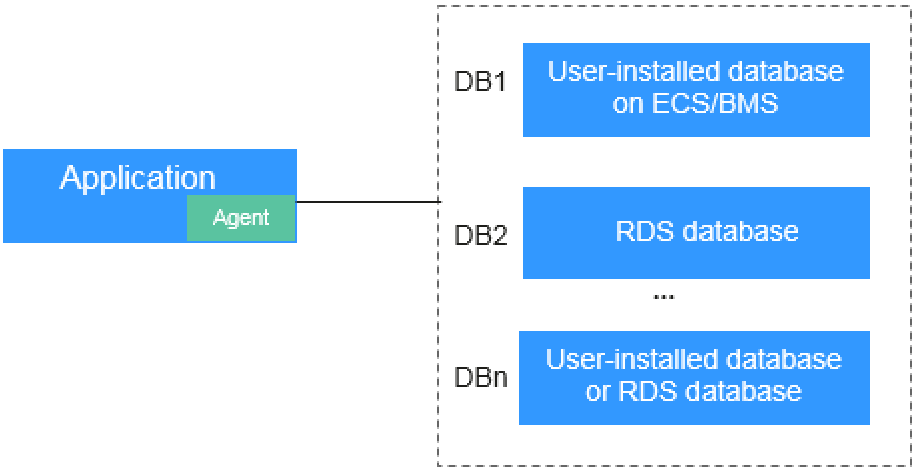
The path for saving agent logs is **/opt/dbss_audit_agent/log/audit_agent.log**.

14.3.6 When Should I Select an Existing Agent?

Do this if an application is connected to multiple databases, as shown in **Figure 14-1**, and an agent has been installed on the application (by setting **Installing Node Type** to **Application**) for one of the databases (for example, **DB1**). To add an agent for another of them, select **Selecting an existing agent** for **Add Mode**, and select the agent added for **DB1**, as shown in **Figure 14-2**.

After the agent is added, the database can be audited.

Figure 14-1 An application connected to multiple databases


Application
Agent
DB1
User-installed database on ECS/BMS
DB2
RDS database
...
DBn
User-installed database or RDS database

NOTE

Possible combinations of connected databases are:

- User-installed databases on ECS/BMS
- RDS databases
- User-installed databases on ECS/BMS and RDS databases

Figure 14-2 Selecting an existing agent

14.3.7 What Do I Do If the Database Audit Agent Is Hibernating?

After an agent is added for a database to be audited, the initial status of the agent will be **Hibernating**, as shown in **Figure 14-3**.

Figure 14-3 Successfully adding an agent

To use database audit, you need to install the agent.

Check the agent status after you installed it.

- If the agent status changes to **Running** after the installation, as shown in **Figure 14-4**, it indicates that the agent is running properly.

  Figure 14-4 Agent running properly

- If the agent status is still **Hibernating** after the installation, troubleshoot the problem by following the instructions provided in **What Do I Do If the Communication Between the Agent and Database Audit Instance Is Abnormal?**

14.3.8 How Do I Determine Where to Install an Agent?

The database audit agent can be installed on the database, application, or proxy node (ranked in descending order of preference).

For details about the nodes, see **Table 14-7**.

Table 14-7 Nodes to install agents

Node	Scenario	Audit Scope	Configuration
Database	Self-built database on ECS/BMS	All access records of applications that have accessed the database	Set **Installing Node Type** to **Database**, as shown in #dbss_01_0282/fig090811115473.
Application	You cannot log in to the node where your database (for example, RDS database) is deployed.	Access records of all the databases connected to the application	● Set **Installing Node Type** to **Application**, as shown in #dbss_01_0282/fig19931695536. ● If an agent has been installed on a database connected to the same application as the desired database, select **Select an existing agent**.
Proxy	You cannot log in to the node where your database (for example, RDS database) is deployed, and cannot install an agent on your application (for example, an off-cloud application).	Only the access records between the proxy and database. Those between the application and database cannot be audited.	Set **Installing Node Type** to **Application**, and set **Installing Node IP Address** to the IP address of the proxy.

Adding an Agent

- Application

  Figure 14-5 Selecting an existing agent

  NOTICE

  If an agent has been installed on a database connected to the same application as the desired database, select **Select an existing agent**. For details, see **When Should I Select an Existing Agent?**

- Proxy

  NOTICE

  Installing Node IP Address must be set to the IP address of the proxy.

14.3.9 How Do I Download a Database Audit Agent?

Download and then install the agent on the database or application based on the add mode you chose.

NOTE

Each agent has a unique ID, which is used as the key for connecting to a database audit instance. If you delete an agent and add it back, you need to download the agent again.

Prerequisites

- You have applied for a database audit instance and the **Status** is **Running**.
- You have added an agent to the database.

Procedure

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Databases**.

Step 4 In the **Instance** drop-down list, select the instance whose agent is to be downloaded.

Step 5 Click ⌄ next to the database to view details of its agent. In the **Operation** column of the agent, click **Download Agent**, to download an agent installation package.

Download the agent installation package suitable for your OS.

- Linux OS

  Download the agent whose OS is **LINUX64**.

----End

14.3.10 How Do I Uninstall a Database Audit Agent?

You can uninstall an agent from the database or application if you do not need to audit the database.

Prerequisites

You have installed an agent on the desired node.

Uninstalling the Agent from a Linux OS

Step 1 Log in to the node where the agent is installed as user **root** using SSH through a cross-platform remote access tool (such as PuTTY).

Step 2 Run the following command to access the directory where the decompressed **xxx.tar.gz** agent installation package is stored:

cd *directory containing the decompressed agent installation package*

Step 3 Run the following command to check whether you have the permission for executing the **uninstall.sh** script:

ll

- If you do, go to **Step 4**.
- If you do not, perform the following operations:
  a. Run the following command to get the script execution permission:

     chmod +x uninstall.sh

  b. Verify you have the required permissions.

Step 4 Run the following command to uninstall the agent:

sh uninstall.sh

If the following information is displayed, the agent has been uninstalled successfully:

```
uninstall audit agent...
exist os-release file
stopping audit agent
audit agent stopped
stop audit_agent success
service audit_agent does not support chkconfig
uninstall audit agent completed!
```

----End

14.3.11 What Do I Do If the Communication Between the Agent and Database Audit Instance Is Abnormal?

Symptom

An agent has been installed on the database or application, but the SQL statement is not displayed in the SQL statement list after you enter an SQL statement in the database.

Perform the following operations to troubleshoot the problem:

- **Checking the Audited Database**
- **Checking the Security Group Rules of the Database Audit Instance**
- **Check the running status of the agent on the installing node.**

Checking the Audited Database

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Databases**.

Step 4 In the **Instance** drop-down list, select the instance whose database is to be checked.

Step 5 Check the information about the database to be audited.

- If the database information is correct, go to **Step 6**.
- If the database information is incorrect, click **Delete** to delete the database, and then click **Add Database** to add the database again.
  - If the fault is rectified, no further operation is required.
  - If the problem persists, go to **Step 6**.

Step 6 Check the audit status of the database to be audited.

- If **Audit Status** is **Enabled**, go to **Checking the Security Group Rules of the Database Audit Instance**.
- If **Audit Status** is **Disabled**, click **Enable** to enable the database audit function.
  - If the fault is rectified, no further operation is required.
  - If the problem persists, go to **Checking the Security Group Rules of the Database Audit Instance**.

----End

Checking the Security Group Rules of the Database Audit Instance

Step 1 Click ∨ next to the database to expand the details about the agent and record the value of **Installing Node IP Address**.

Step 2 Click **Add Security Group Rule**.

Step 3 In the displayed dialog box, record the security group name (for example, **default**) of the database audit instance.

Step 4 Click **Go to VPC**.

Step 5 In the security group list, enter the group name **default** in the search box in the upper right corner of the list, and click 🔍 or press **Enter**. The group information is displayed in the list.

Step 6 Click the name of the security group **default**. Click the **Inbound Rules** tab.

Step 7 Check inbound rules of the security group **default**.

Check whether TCP (port number **8000**) and UDP protocols (port number from **7000** to **7100**) are configured in the inbound rules of the security group for the IP address of the installing node in **Step 1**.

- If inbound rules have been configured for the security group, go to **Check the running status of the agent on the installing node.**.
- If no inbound rule is configured for the security group, go to **Step 8**.

Step 8 Add inbound rules for the security group of the database audit instance.

1. Click **Add Rule**. In the **Add Inbound Rule** dialog box, add **TCP** (port number **8000**) and **UDP** protocols (port number from **7000** to **7100**) for the installing node IP address in **Step 1**.
2. Click **OK**.
   - If the fault is rectified, no further operation is required.

- If the problem persists, go to **Check the running status of the agent on the installing node.**.

----End

Check the running status of the agent on the installing node.

- Linux OS
  a. Log in to the node where the agent is installed as user **root** using SSH through a cross-platform remote access tool (such as PuTTY).
  b. Run the following command to view the running status of the agent:

     service audit_agent status

     - If the following information is displayed, the agent is running properly. Go to **Verifying the Result**.

       ```
       audit agent is running.
       ```

     - If no information is displayed, the agent is running abnormally. Run the following command to restart the agent:

       service audit_agent restart

Verifying the Result

In your database, run an SQL statement on the node where the agent is installed. Choose **Overview** > **Statements** and then search for the executed statement.

- If the SQL statement is found, the problem has been solved.
- If the SQL statement is not found, the problem persists. Contact customer service.

14.3.12 How Many Resources Are Consumed by an Agent When It Runs on a Node?

When an agent is running, it consumes no more than 5% CPU and no more than 300 MB memory. The following resource metrics are monitored to prevent the agent from consuming too many resources:

- Overall CPU and memory usage of the system. If the CPU or memory usage exceeds the specified threshold (80% by default), the agent will stop running.
- CPU and memory of the agent process

14.3.13 What Do I Do If Agent Installation Fails?

Check whether your agent ID is correct. If it is, perform the following operations to uninstall and then reinstall the agent:

Step 1 **Uninstalling an Agent** from the target database.

Step 2 **Step 2: Add an Agent**.

Step 3 **Step 4: Download and Install the Agent**.

Step 4 Perform the operations in **Installing an Agent (Linux OS)**.

----End

14.4 Operations

14.4.1 How Do I Disable SSL for a Database?

If SSL is enabled for a database, the database cannot be audited. To use database audit, disable SSL first.

The MySQL database client is used as an example. Perform the following steps:

Step 1 Log in to the MySQL database client as user **root**.

Step 2 Run the following command to check the connection mode of the MySQL database:

\s

- If information similar to the following is displayed, SSL has been disabled for the MySQL database.

```
SSL:                    Not in use
```

- If information similar to the following is displayed, SSL has been enabled for the MySQL database. Go to **Step 3**.

```
SSL:                    Cipher in use is XXX-XXX-XXXXXX-XXX
```

Step 3 Log in to the MySQL database in SSL mode.

1. Run the following command to exit from the MySQL database:

   exit

2. Log in to the MySQL database as user **root**.

   Add the following parameters at the end of the login command:

   --ssl-mode=DISABLED

   Or

   --ssl=0

   NOTICE

   If you logged in to the MySQL database in SSL mode, you can disable SSL only for this login. To use the database audit function, log in to the MySQL database as instructed in this step.

3. Run the following command to check the connection mode of the MySQL database:

   \s

   If information similar to the following is displayed, SSL has been disabled for the MySQL database.

```
SSL:                    Not in use
```

----End

14.4.2 How Do I Check the Version of Database Audit?

To check the version of database audit, perform the following steps:

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Instances**.

Step 4 Click the name of the instance whose information you want to view. The **Overview** page is displayed.

Step 5 View the instance version.

----End

14.4.3 How Do I View All Alarms in Database Audit?

To check the alarms of database audit, perform the following steps:

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Instances**.

Step 4 Click the name of an instance, click the **Monitoring** tab, and then the **Alarm Monitoring** tab.

Step 5 View the alarm information.

To query specified alarms, perform the following steps:

- Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days** for **Time**, or click 📅 to set start time and end time, and click **OK** to view alarms of the specified time range.
- Select **All**, **High**, **Moderate**, or **Low** for **Risk Severity**. Alarms of specified severity are displayed in the list.
- Select an alarm type, and alarms of specified alarm type is displayed in the list.

----End

14.4.4 How Do I Audit an RDS Database Accessed through Intranet (by Applications Off the Cloud)?

If your PC accesses RDS through a private line, you can install the agent on a proxy your set up. Access from the proxy to the database can be audited. Access from applications to the proxy cannot be audited.

14.5 Troubleshooting

14.5.1 Database Audit Is Running Properly But Generates No Audit Records

Symptom

The functions of the database audit instance are normal. When there is database traffic, audit information about the executed SQL statement cannot be found in the SQL statement list.

Possible Causes

- SSL is enabled for the database.
- ForceEncryption is enabled for the SQL Server database protocol.
- The data volume is too large. As a result, the Agent process is suspended. You are advised to restart the container or optimize audit rules to reduce the data volume.

NOTE

- If SSL is enabled for a database, the database cannot be audited.
- If ForceEncryption is enabled for a database, database audit cannot obtain file content from the database for analysis.

Disabling Database SSL

The MySQL database client is used as an example. Perform the following steps:

Step 1 Log in to the MySQL database client as user **root**.

Step 2 Run the following command to check the connection mode of the MySQL database:

\s

- If information similar to the following is displayed, SSL has been disabled for the MySQL database. Go to **Step 4**.

```
SSL:                    Not in use
```

- If information similar to the following is displayed, SSL has been enabled for the MySQL database. Go to **Step 3**.

```
SSL:                    Cipher in use is XXX-XXX-XXXXXX-XXX
```

Step 3 Log in to the MySQL database in SSL mode.

1. Run the following command to exit from the MySQL database:

   exit

2. Log in to the MySQL database as user **root**.

   Add the following parameters at the end of the login command:

   --ssl-mode=DISABLED

   or

   --ssl=0

NOTICE

If you log in to the MySQL database in SSL mode, you can only disable SSL for this login. To use the database audit function, log in to the MySQL database in the mode described in **Step 3.2**.

3. Run the following command to check the connection mode of the MySQL database:

   \s

   If information similar to the following is displayed, SSL has been disabled for the MySQL database. Go to **Step 4**.

```
SSL:                    Not in use
```

Step 4 Run an SQL statement and search for it in the SQL statement list.

- If the SQL statement is found, the problem has been solved.
- If the SQL statement is not found, the problem persists. In this case, **Disable ForceEncryption for the SQL Server protocol**.

----End

Disabling ForceEncryption for the SQL Server Protocol

Step 1 Open the **SQL Server Configuration Manager** dialog box.

Step 2 Select **SQL Server Network Configuration**.

Step 3 Right-click **Protocols for MSSQLSERVER** and choose **Properties**.

Step 4 Click the **Flags** tab. Set **ForceEncryption** to **No**.

Step 5 Restart the SQL Server service for the modification to take effect.

Step 6 Run an SQL statement and search for it in the SQL statement list.

- If the SQL statement is found, the problem has been solved.
- If the SQL statement is not found, the problem persists. Contact customer service.

----End

14.5.2 Database Audit Is Unavailable

Symptom

After the database traffic is triggered, you cannot find the audit information about an executed statement in the SQL statement list.

In this case, perform the following operations to troubleshoot the problem:

- **Checking Database Information and Audit Function Settings**
- **Checking Audited Database Settings**

- Checking Database Agent Status
- Checking the Security Group Rules of the Database Audit Instance

Checking Database Information and Audit Function Settings

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Databases**.

Step 4 Select an instance where the database is located from the **Instance** drop-down list.

Step 5 Check whether the database information is correct.

- If the database information is correct, go to **Step 6**.
- If the database information is incorrect, click **Delete** to delete the database, and then click **Add Database** to add the database again.
  - If the fault is rectified, no further operation is required.
  - If the problem persists, go to **Step 6**.

Step 6 Check whether the database audit function is enabled.

- If **Audit Status** is **Enabled**, go to **Checking Audited Database Settings**.
- If **Audit Status** is **Disabled**, click **Enable** to enable the database audit function.
  - If the fault is rectified, no further operation is required.
  - If the problem persists, go to **Checking Audited Database Settings**.

----End

Checking Audited Database Settings

In the navigation tree on the left, choose **Database Audit** > **Rules**. The **Audit Scope** page is displayed.

- If **Status** is **Enabled**, go to **Checking Database Agent Status**.
- If **Status** is **Disabled**, click **Enable** to enable the desired audit scope rule of the database.
  - If the fault is rectified, no further operation is required.
  - If the problem persists, go to **Checking Database Agent Status**.

Checking Database Agent Status

Step 1 Log in to the node where the agent is installed as user **root** by using a cross-platform remote access tool (for example, PuTTY) via SSH.

Step 2 Run the following command to view the running status of the agent program:

```
ps -ef|grep audit_agent
```

- If the following information is displayed, the agent is running properly. Go to **Step 4**.

```
/opt/dbss_audit_agent/bin/audit_agent
```

- If no information is displayed, the agent does not run properly. Go to **Step 3**.

Step 3 Run the following command to restart the agent:

service audit_agent restart

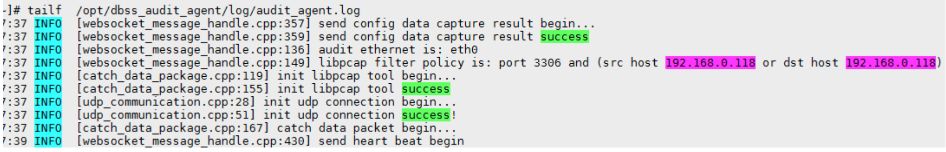
- If the fault is rectified, no further operation is required.
- If the problem persists, go to **Step 4**.

Step 4 Run the following command to check the communication status between the agent and database audit instance:

tailf /opt/dbss_audit_agent/log/audit_agent.log

- If information similar to the following is displayed, the communication between the agent and database audit instance is normal. Go to **Verifying the Result**.

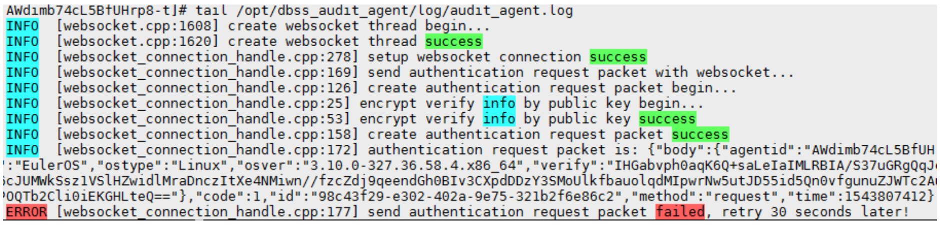
Figure 14-6 Normal communication



```
-]# tailf  /opt/dbss_audit_agent/log/audit_agent.log
7:37 INFO  [websocket_message_handle.cpp:357] send config data capture result begin...
7:37 INFO  [websocket_message_handle.cpp:359] send config data capture result success
7:37 INFO  [websocket_message_handle.cpp:136] audit ethernet is: eth0
7:37 INFO  [websocket_message_handle.cpp:149] libpcap filter policy is: port 3306 and (src host 192.168.0.118 or dst host 192.168.0.118)
7:37 INFO  [catch_data_package.cpp:119] init libpcap tool begin...
7:37 INFO  [catch_data_package.cpp:155] init libpcap tool success
7:37 INFO  [udp_communication.cpp:28] init udp connection begin...
7:37 INFO  [udp_communication.cpp:51] init udp connection success!
7:37 INFO  [catch_data_package.cpp:167] catch data packet begin...
7:39 INFO  [websocket_message_handle.cpp:430] send heart beat begin
```

- If information similar to the following is displayed, the communication between the agent and database audit instance is abnormal. Go to **Checking the Security Group Rules of the Database Audit Instance**.

Figure 14-7 Communication error



```
AWdimb74cL5BfUHrp8-t]# tail /opt/dbss_audit_agent/log/audit_agent.log
INFO  [websocket.cpp:1608] create websocket thread begin...
INFO  [websocket.cpp:1620] create websocket thread success
INFO  [websocket_connection_handle.cpp:278] setup websocket connection success
INFO  [websocket_connection_handle.cpp:169] send authentication request packet with websocket...
INFO  [websocket_connection_handle.cpp:126] create authentication request packet begin...
INFO  [websocket_connection_handle.cpp:25] encrypt verify info by public key begin...
INFO  [websocket_connection_handle.cpp:53] encrypt verify info by public key success
INFO  [websocket_connection_handle.cpp:158] create authentication request packet success
INFO  [websocket_connection_handle.cpp:172] authentication request packet is: {"body":{"agentid":"AWdimb74cL5BfUH
':"EulerOS","ostype":"Linux","osver":"3.10.0-327.36.58.4.x86_64","verify":"IHGabvph0aqK6Q+saLeIaIMLRBIA/S37uGRgQqJ
5cJUMWkSsz1VSlHZwidlMraDnczItXe4NMiwn//fzcZdj9qeendGh0BIv3CXpdDDzY3SMoUlkfbauolqdMIpwrNw5utJD55id5Qn0vfgunuZJWTc2A
'0QTb2Cli0iEKGHLteQ=="},"code":1,"id":"98c43f29-e302-402a-9e75-321b2f6e86c2","method":"request","time":1543807412}
ERROR [websocket_connection_handle.cpp:177] send authentication request packet failed, retry 30 seconds later!
```

----End

Checking the Security Group Rules of the Database Audit Instance

Step 1 Go to the **Database Security Service** page.

Step 2 In the navigation tree on the left, choose **Database Audit** > **Databases**. The **Databases** page is displayed.

Step 3 Select an instance where the database is located from the **Instance** drop-down list.

Step 4 Record the IP address of the agent node.

Click ⌄ next to the database to view the information of its agent, and record **Installing Node IP Address**.

Step 5 Click **Add Security Group Rule**.

Step 6 In the displayed dialog box, record the security group name (for example, **default**) of the database audit instance.

Step 7 Click **Go to VPC**.

Step 8 In the security group list, enter the group name **default** in the search box in the upper right corner of the list, and click 🔍 or press **Enter**. The group information is displayed in the list.

Step 9 Click the name of the security group **default**. Click the **Inbound Rules** tab.

Step 10 Check the inbound access rules of the security group.

Check whether TCP (port number **8000**) and UDP protocols (port number from **7000** to **7100**) are configured in the inbound rules of the security group for the IP address of the installing node in **Step 4**.

- If the inbound rules of the security group have been configured for the installing node, go to **Verifying the Result**.
- If no inbound rules of the security group have been configured for the installing node, go to **Step 11**.

Step 11 Add an inbound rule for the installing node.

1. On the **Inbound Rules** page, click **Add Rule**.
2. In the **Add Inbound Rule** dialog box, add **TCP** (port number **8000**) and **UDP** protocols (port number from **7000** to **7100**) for the installing node IP address.
3. Click **OK**.

----End

Verifying the Result

In your database, run an SQL statement on the node where the agent is installed, and then search for the statement in the SQL statement list.

- If the SQL statement is found, the problem has been solved.
- If the SQL statement is not found, the problem persists. Contact customer service.

14.5.3 Alarm Notifications Are Abnormal

Symptom

- The database audit instance is running properly. An alarm about a high-risk statement alarm is sent via email, but no high-risk SQL statements are displayed on the console.
- Alarm email sending is delayed.

Possible Causes

There are too many audit logs and data audit is delayed.

Suggestion

- Add DBSS instances and balance the loads processed by each instance. Alternatively, modify audit rules to narrow down the audit scope.
- Create an automated hourly backup task to prevent log deletion, which will be triggered if the disk usage reaches 85%.

14.6 Logs

14.6.1 Can the Operation Logs of Database Audit Be Migrated?

No. Database audit does not support migrating database operation logs.

You can view the operation logs of database audit. For details, see **How Long Are the Operation Logs of Database Audit Saved by Default?**

14.6.2 How Long Are the Operation Logs of Database Audit Saved by Default?

The operation logs of database audit are permanently saved.

14.6.3 How Do I Check the Operation Logs of Database Audit?

To check the operation logs of database audit, perform the following steps:

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Instances**.

Step 4 Click the name of the instance whose operation logs you want to view. The **Overview** page is displayed.

Step 5 Click the **Logs** tab. The log list page is displayed.

Step 6 View operation logs. For details about related parameters, see **Table 14-8**.

NOTE

Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days**, or click 📅 to set start time and end time to view the operation logs of a specified time range.

Table 14-8 Parameters

Parameter	Description
Username	User who performs the operation
Time	Time when the operation was performed

Parameter	Description
Function	Function of the operation
Action	Action of the operation
Operation Object	Object of the operation
Description	Description of the operation
Result	Result of the operation

----End

14.6.4 How Does Database Audit Process Logs?

Database audit logs are stored in a log database and processed based on disk usage.

- If the disk usage of the log database is 85% or higher, the system automatically deletes the audit logs generated on the earliest date until the disk usage drops below 85%.
- If the disk usage is 90% or higher, database audit stops and the system no longer saves new audit logs.

14.6.5 How Do I Back Up the Database Audit Logs?

Database audit supports manual backup and automatic backup. Audit logs are backed up to OBS. Buckets will be automatically created and will incur a separate bill.

Perform the following operations to automatically back up audit logs.

Automatically Backing Up Database Audit Logs

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, choose **Settings**.

Step 4 In the **Instance** drop-down list, select the required instance and click the **Backup and Restoration** tab.

Step 5 Click **Configure**. In the displayed dialog box, set the parameters. For details about related parameters, see **Table 14-9**.

Table 14-9 Parameters

Parameter	Description	Example Value
Automatic Backup	Status of automatic backup - ◉: enabled - ○: disabled	◉
Backup Period	Automatic backup period. Its options are as follows: - **Daily** - **Hourly**	Daily
Started	Start time of the backup. Click 📅 to configure.	2020/01/14 20:27:08

Step 6 Click **OK**.

NOTE

After the automatic backup function is configured, new data in the database will be backed up one hour later. Then you can view the backup information.

----End

14.6.6 Can Database Audit Logs Be Directly Saved to OBS?

No. Database audit logs are directly saved to the log database. You can back up the logs to Object Storage Service (OBS).

Database audit logs can be manually or automatically backed up.

Automatic backup: Logs can be automatically backed up on a daily, weekly, or monthly basis.

Manual backup: You can back up logs generated in the last 24 hours, last 7 days, last 30 days, and or all logs.

If there are a large number of logs generated, you are advised to automatically back up logs every day.

If you back up logs to OBS, an OBS bucket will be automatically created to store the logs Buckets are billed per use.

14.6.7 Backup Gets Stuck at the Backup File Uploading Phase

This problem occurs probably because the amount of data to be backed up is too large. You are advised to perform hourly backup.

A Change History

Released On	Description
2022-10-30	This issue is the fourth official release. Added: **What Is Database Audit?**, **What Editions Does DBSS Provide?**, and **What Databases Does DBSS Support?**
2022-06-30	This is the third official release. Added: **What Do I Do If Agent Installation Fails?**
2021-06-30	This is the second official release.
2021-04-30	This is the first official release.