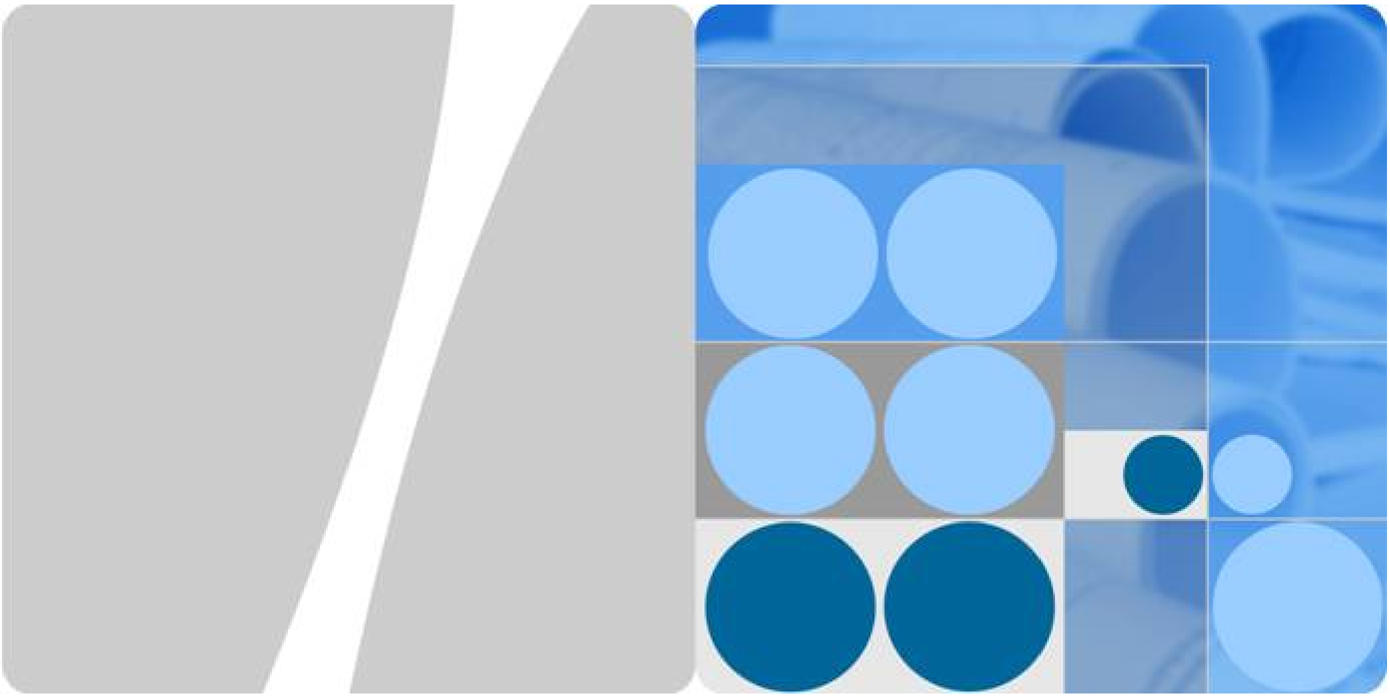


Database Security Service

User Guide

Date **2023-06-30**

Contents

1 Overview

1.1 DBSS

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

Supported Databases

Database audit provides the audit function in out-of-path mode for the following databases on the management console:

- Relational Database Service (RDS)
- 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	Edition
MySQL	● 5.0, 5.1, 5.5, 5.6, 5.7 ● 8.0 (8.0.11 and earlier) ● 8.0.23
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	Edition
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

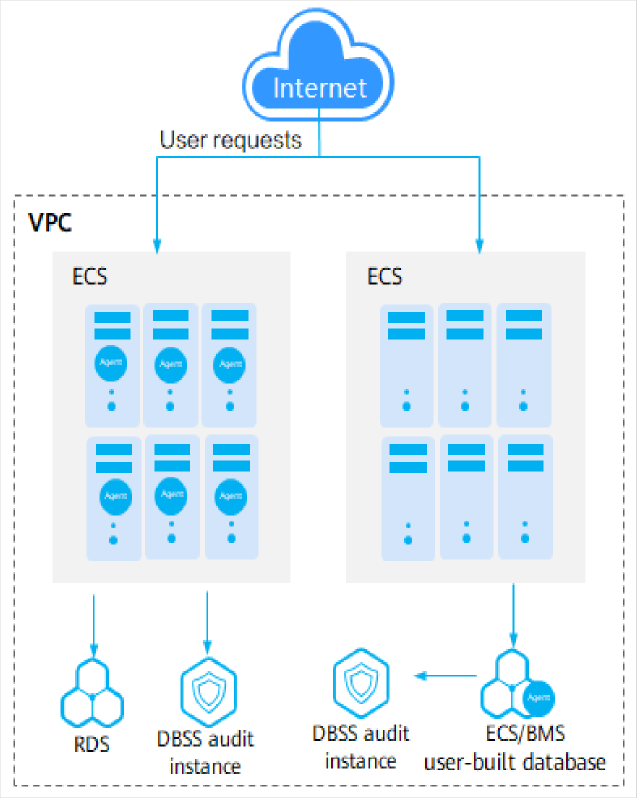
  Clearly divides permissions among the system administrator, security administrator, and audit administrator, meeting audit security requirements.

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, professional, and advanced editions. You can select one of them as needed.

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.
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.
Advanced	30	● CPU: 16 vCPUs ● Memory: 64 GB ● Disk: 2 TB	● Peak QPS: 30,000 queries/second ● Database load rate: 10.80 million statements/hour ● Stores 1.5 billion online SQL statements. ● Stores 60 billion archived SQL statements.

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:

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

Databases That Need Agents

The following database versions can be audited.

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

Database Type	Edition
MySQL	● 5.0, 5.1, 5.5, 5.6, 5.7 ● 8.0 (8.0.11 and earlier) ● 8.0.23
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

Database Type	Edition
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 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)

System Name	System version
SUSE	● SUSE 11 SP4 (64bit) ● SUSE 12 SP1 (64bit) ● SUSE 12 SP2 (64bit)
Ubuntu	● Ubuntu 14.04 (64bit) ● Ubuntu 16.04 (64bit) ● Ubuntu 18.04 (64bit) ● Ubuntu 20.04 (64-bit)
EulerOS	● Euler 2.2 (64bit) ● Euler 2.3 (64bit)
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 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 1-5 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.

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*.

2 Enabling and Using Database Audit (by Installing Agents)

2.1 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**.

- **AZ**: 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.
- **Type**: For details about the supported editions, see **Editions**.

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_subnet
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 **Instances** page, you can view the created database audit instance.

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

----End

2.2 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. In the dialog box displayed, set the database information. For details about related parameters, see Table 2-2.

Table 2-2 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

Parameter	Description	Example Value
Type	Supported database type. The options are as follows: ● MYSQL ● ORACLE ● POSTGRESQL ● SQLSERVER ● DWS ● GaussDB for MYSOL ● GaussDB ● DAMENG ● KINGBASE ● SHENTONG ● GBase 8a ● GBase XDM Cluster ● Greenplum ● HighGo ● Mariadb **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: ● 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 ● When **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: – DM8 ● When **Type** is set to **KINGBASE**, the following version is available:	5.0

Parameter	Description	Example Value
	– 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 ● WINDOWS64	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. See **Figure 2-1**.

Figure 2-1 Successfully adding a database

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

2.3 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.

NOTE

Currently, only the following types of databases support agent-free audit:

- GaussDB for MySQL
- RDS for SQLServer
- RDS for MySQL
  - 5.6 (5.6.51.1 or later)
  - 5.7 (5.7.29.2 or later)
  - 8.0 (8.0.20.3 or later)

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 2-2** and **Figure 2-3**.

Figure 2-2 One application connecting to multiple databases built on ECS/BMS

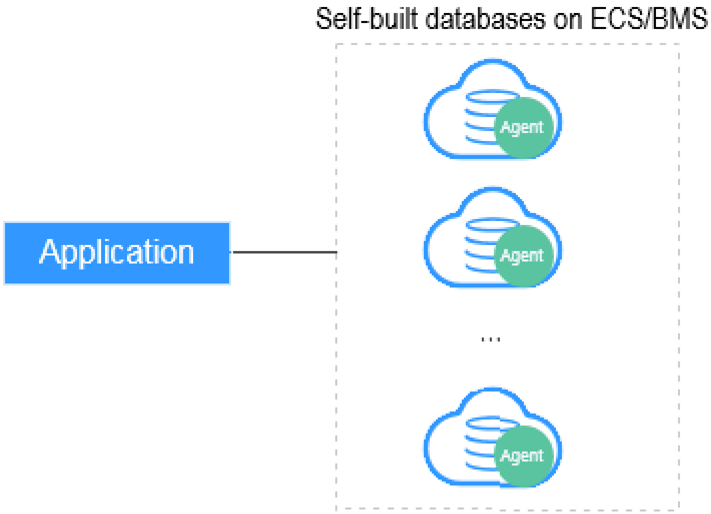
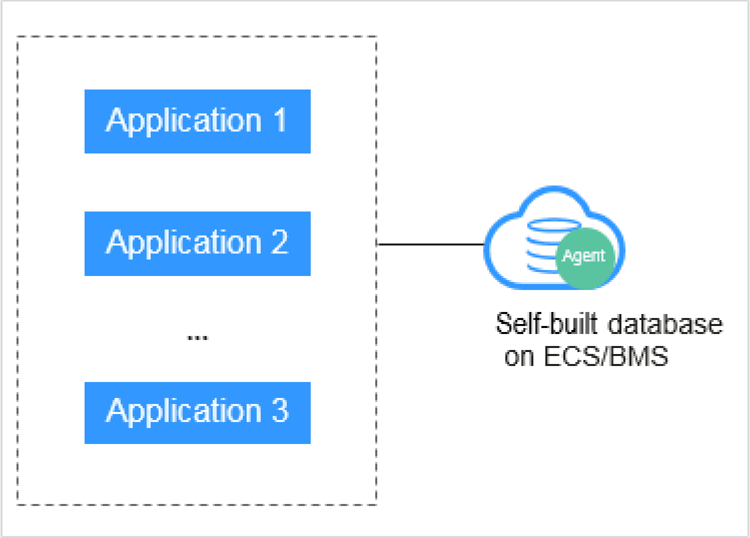


Figure 2-3 Multiple applications connecting to one database built on ECS/BMS



- Deploy DBSS for RDS databases. For details, see **Figure 2-4** and **Figure 2-5**.

Figure 2-4 One application connecting to multiple RDS databases

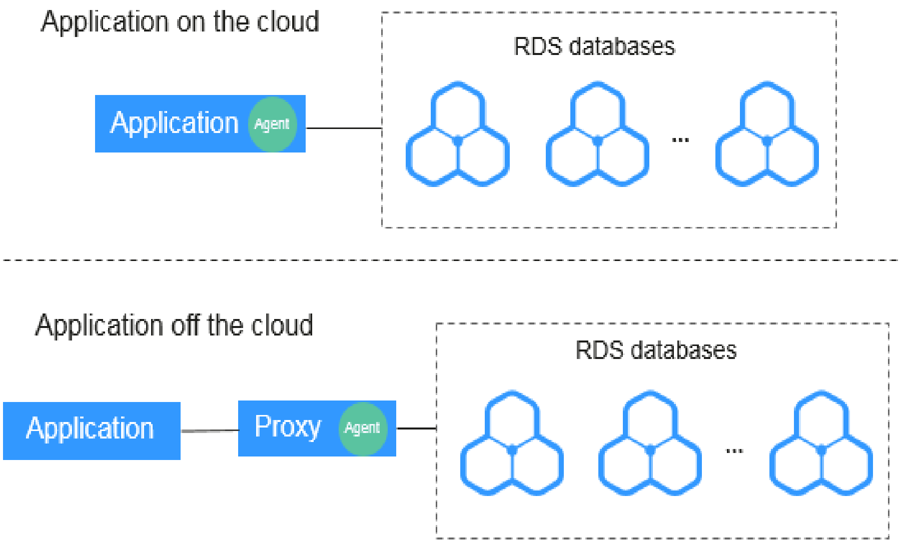


Figure 2-5 Multiple applications connecting to one RDS database

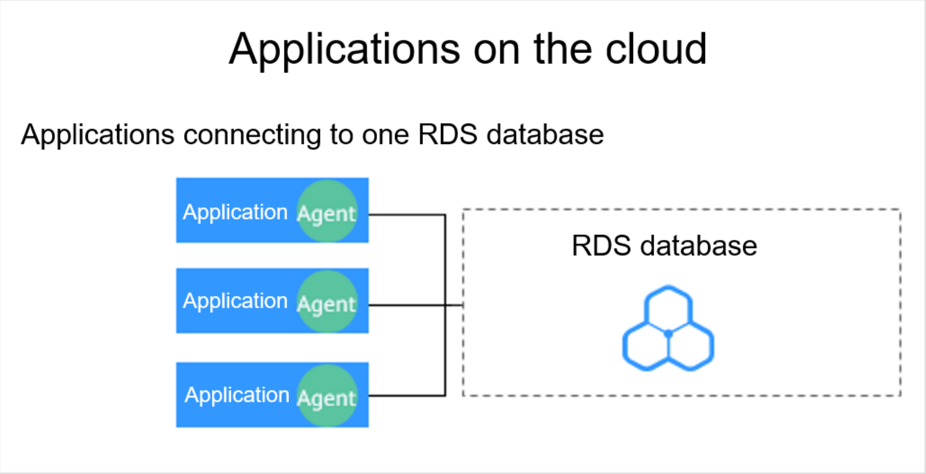

Applications on the cloud
Applications connecting to one RDS database
Application
Agent
Application
Agent
Application
Agent
RDS database

Table 2-3 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 2-3 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.

Scenario	Where to Add the Agent	Audit Scope	Description
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.

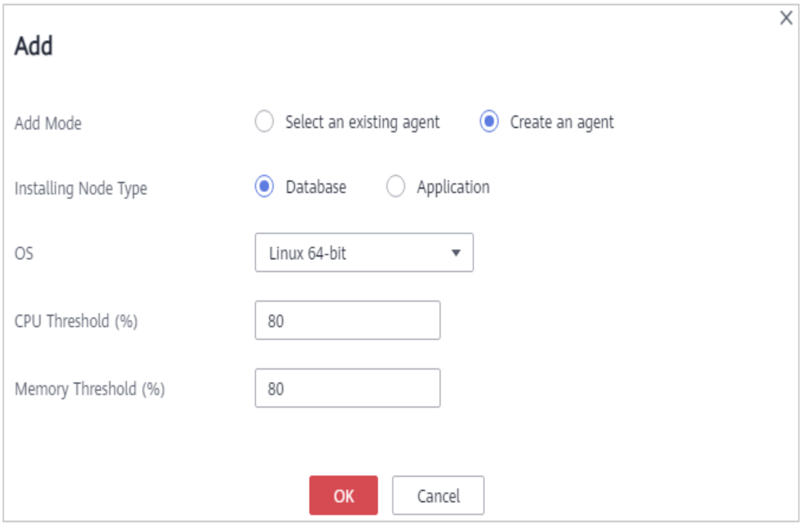
Step 3 In the navigation tree on the left, choose **Databases**.

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, as shown in **Figure 2-6**. For details about related parameters, see **Table 2-4**.

Figure 2-6 Adding an agent to a database


Add

Add Mode: ○ Select an existing agent ● Create an agent

Installing Node Type: ● Database ○ Application

OS: Linux 64-bit

CPU Threshold (%): 80

Memory Threshold (%): 80

Table 2-4 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 . **NOTE** Select **LINUX64_X86** or **LINUX64_ARM** based on the server architecture.	

Step 7 Click **OK**.

Step 8 Click ^ in the lower part of the database list page to expand the database details and view the information about the added agent.

NOTE

After adding the agent, confirm that the agent information is correct. If the agent is incorrectly added, locate the target agent, click **More** > **Delete** in the **Operation** column, 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**.

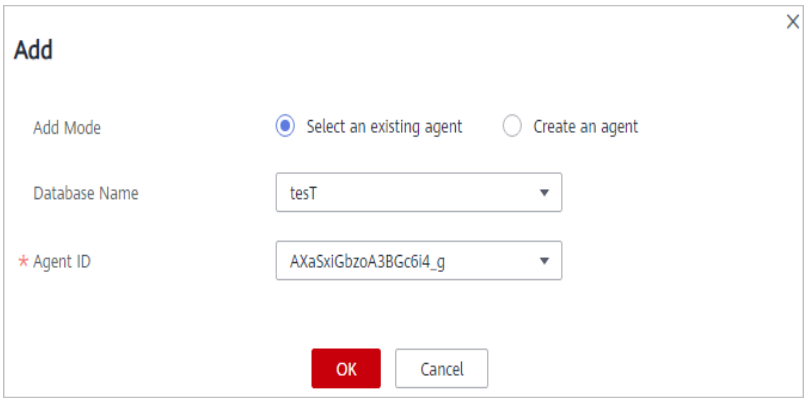
Step 6 In the displayed dialog box, select an add mode, as shown in **Figure 2-7** and **Figure 2-8**. For details about related parameters, see **Table 2-5**.

- 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.

Figure 2-7 Selecting an existing agent



Add

Add Mode ● Select an existing agent ○ Create an agent

Database Name: tesT

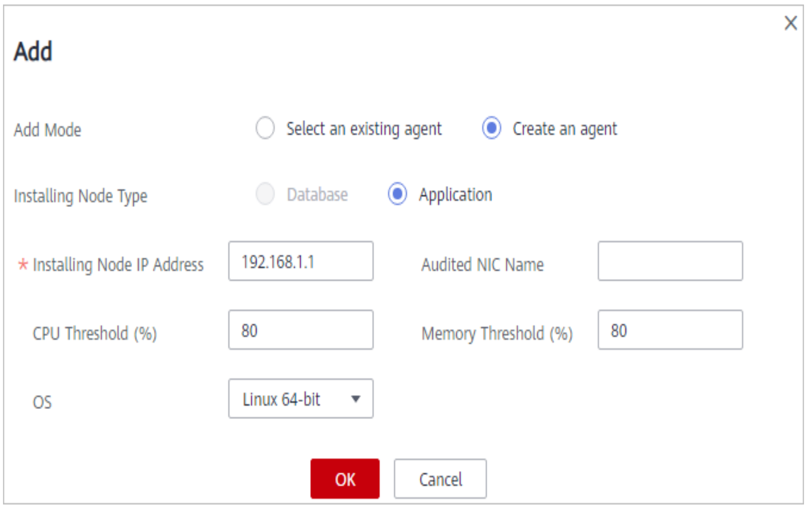
* Agent ID: AXaSxiGbzoA3BGc6i4_g

- 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.

Figure 2-8 Adding an agent to an application



Add

Add Mode ○ Select an existing agent ● Create an agent

Installing Node Type ○ Database ● Application

* Installing Node IP Address: 192.168.1.1

Audited NIC Name:

CPU Threshold (%): 80

Memory Threshold (%): 80

OS: Linux 64-bit

Table 2-5 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**.

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, locate the target agent, click **More** > **Delete** in the **Operation** column, and add an agent again.

----End

Follow-Up Procedure

After adding an agent, install the agent on the database or application based on the add mode you chose. Database audit works only when the database to be audited is connected to the database audit instance. For details about how to install an agent, see **Installing an Agent**.

2.4 Step 3: Download and Install the Agent

2.4.1 Downloading an Agent

Download and then install the agent on the database or application, as required by 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 ^ in the lower part of the database list to expand the agent details. Locate the target agent and click **Download Agent** in the **Operation** column. to download an agent installation package.

Download the agent installation package suitable for your OS.

- Linux OS

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

  Download the agent whose OS is **WINDOWS64**.

----End

2.4.2 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 2-9** and **Figure 2-10**.

  Figure 2-9 One application connecting to multiple databases built on ECS/BMS

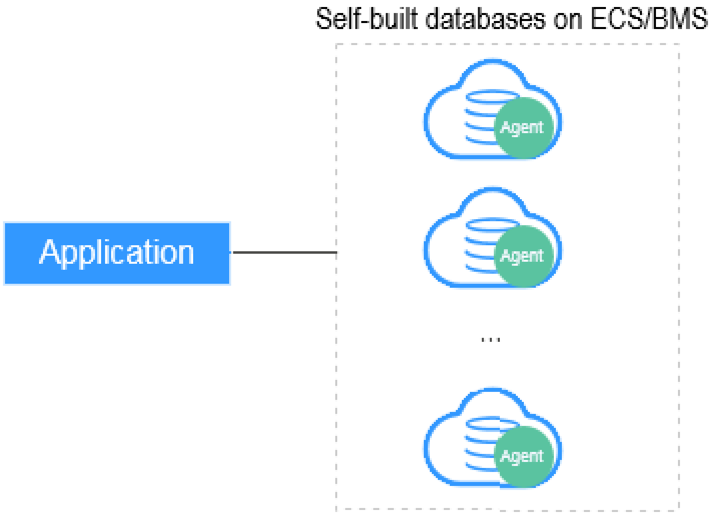
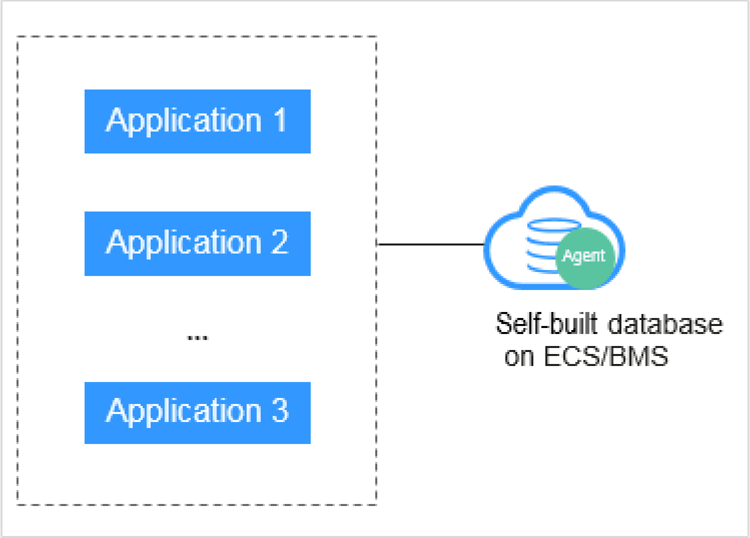


Figure 2-10 Multiple applications connecting to one database built on ECS/BMS



- Deploy DBSS for RDS databases. For details, see **Figure 2-11** and **Figure 2-12**.

Figure 2-11 One application connecting to multiple RDS databases

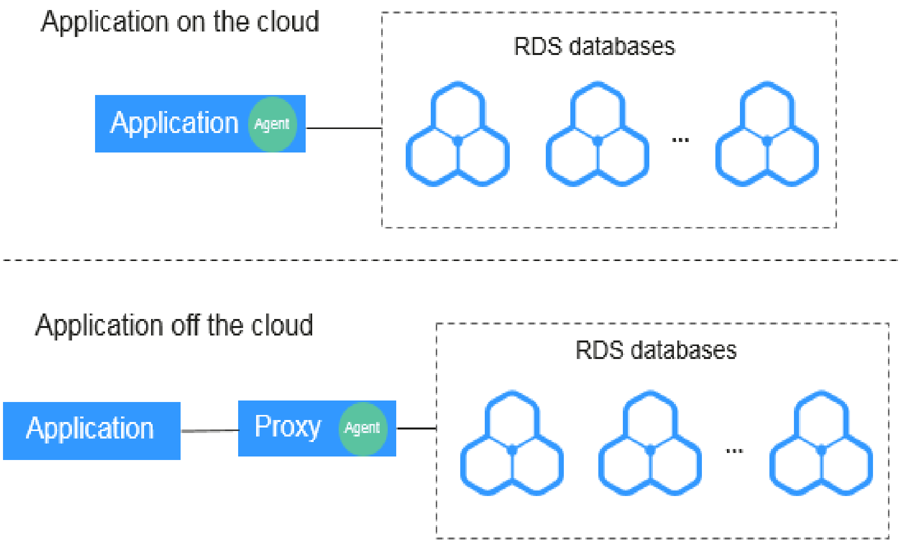


Figure 2-12 Multiple applications connecting to one RDS database

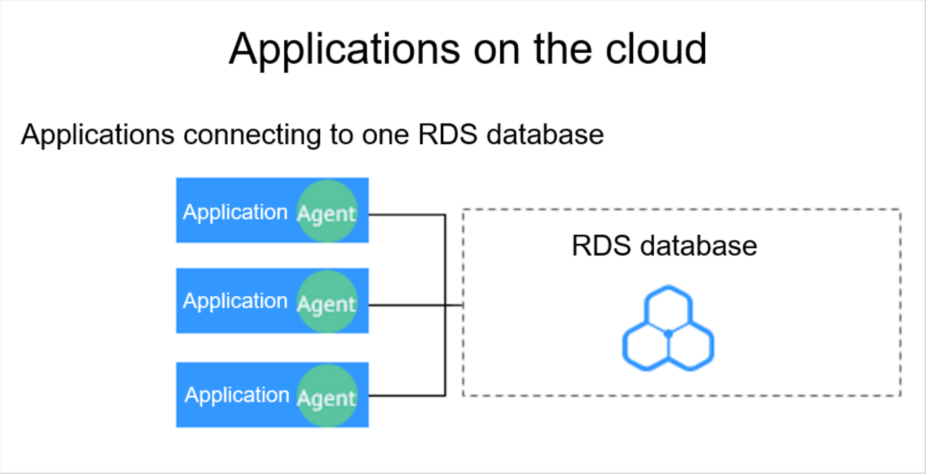

Applications on the cloud
Applications connecting to one RDS database
Application
Agent
Application
Agent
Application
Agent
RDS database

Table 2-6 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 2-6 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

2.4.3 Installing an Agent (Windows 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 Windows OS. For details about how to install an agent on the Linux OS, see **Installing an Agent (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 Windows OS.
- The Windows 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 2-13** and **Figure 2-14**.

Figure 2-13 One application connecting to multiple databases built on ECS/BMS

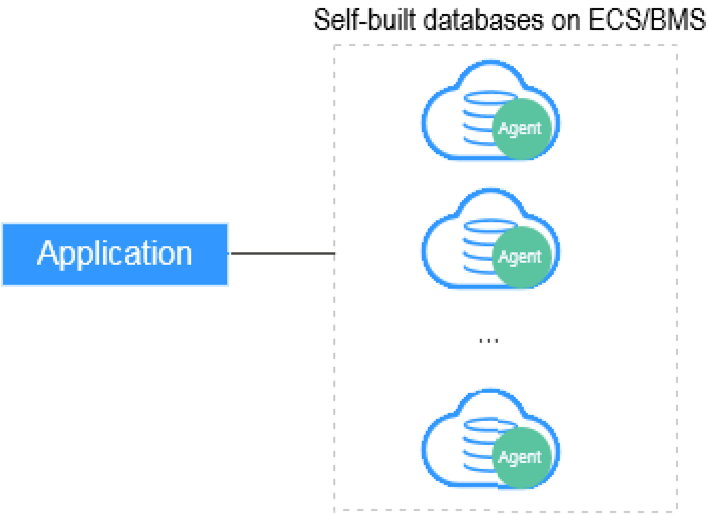
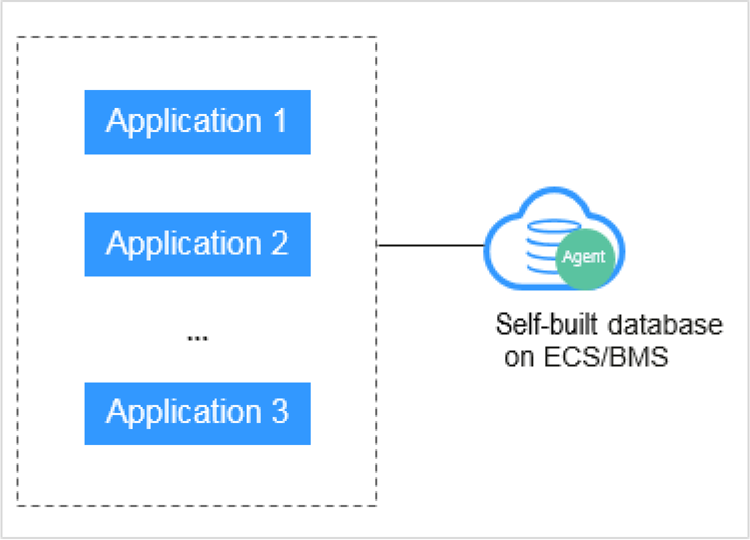


Figure 2-14 Multiple applications connecting to one database built on ECS/BMS



- Deploy DBSS for RDS databases. For details, see **Figure 2-15** and **Figure 2-16**.

Figure 2-15 One application connecting to multiple RDS databases

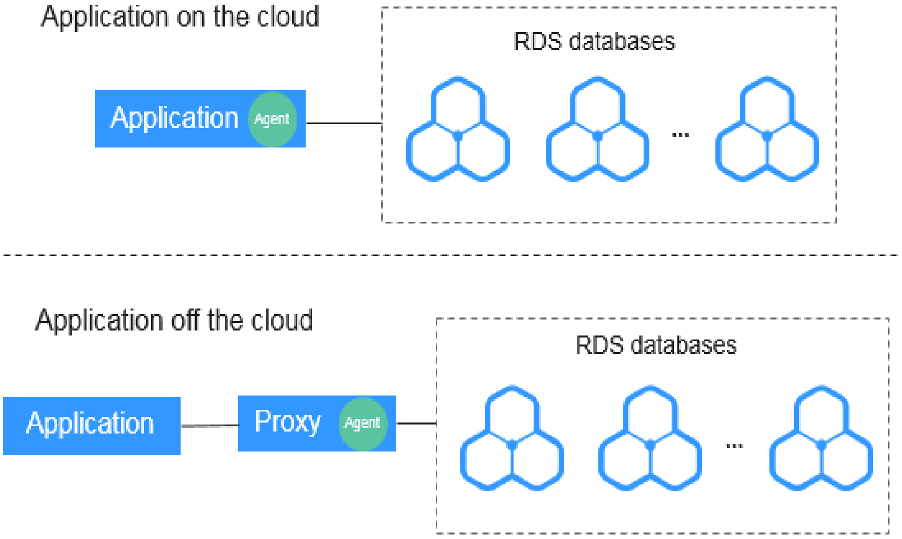


Figure 2-16 Multiple applications connecting to one RDS database

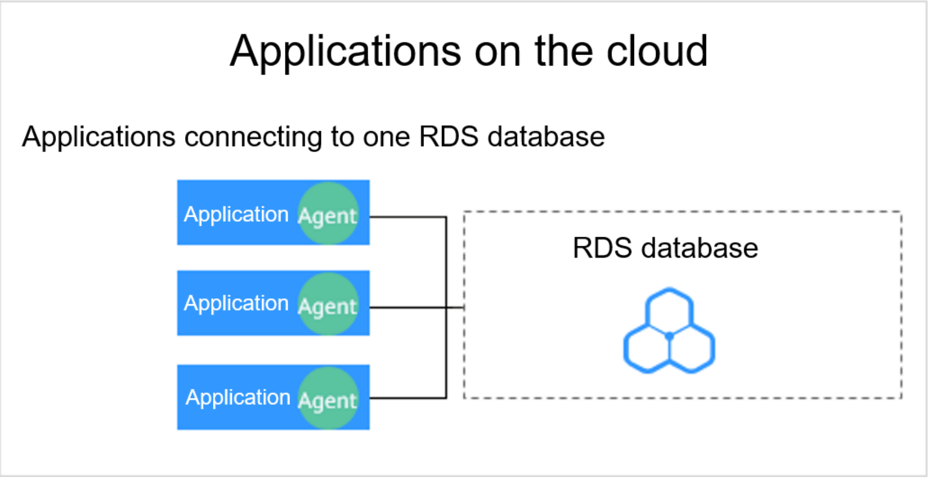

Applications on the cloud
Applications connecting to one RDS database
Application
Agent
Application
Agent
Application
Agent
RDS database

Table 2-7 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 2-7 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.
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.

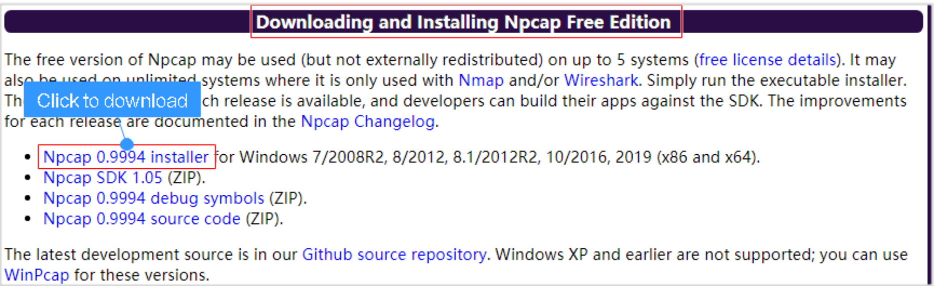
Installing an Agent

Step 1 Install Npcap on the Windows server.

- If Npcap has been installed on the Windows OS, go to **Step 2**.
- If the Npcap has not been installed on the Windows server, perform the following steps:

  a. Download the latest Npcap software installation package from **https://nmap.org/npcap/**.

  Figure 2-17 Downloading Npcap

  Downloading and Installing Npcap Free Edition

  The free version of Npcap may be used (but not externally redistributed) on up to 5 systems (free license details). It may also be used on unlimited systems where it is only used with Nmap and/or Wireshark. Simply run the executable installer. Th [illegible] ch release is available, and developers can build their apps against the SDK. The improvements for each release are documented in the Npcap Changelog.

  - Npcap 0.9994 installer for Windows 7/2008R2, 8/2012, 8.1/2012R2, 10/2016, 2019 (x86 and x64).
  - Npcap SDK 1.05 (ZIP).
  - Npcap 0.9994 debug symbols (ZIP).
  - Npcap 0.9994 source code (ZIP).

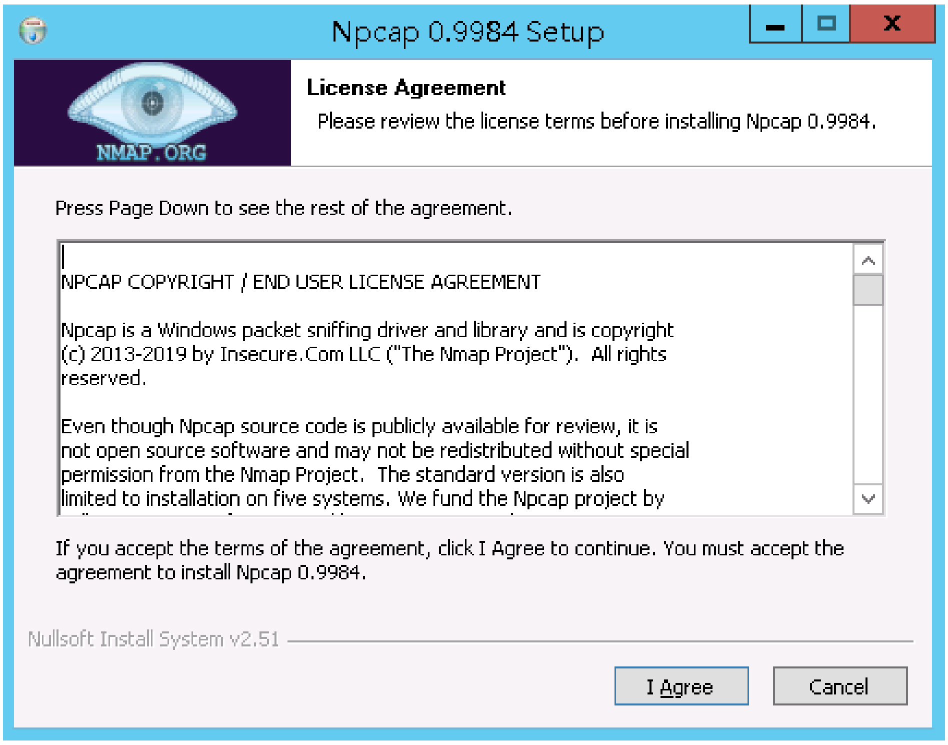
  The latest development source is in our Github source repository. Windows XP and earlier are not supported; you can use WinPcap for these versions.

  b. Upload the **npcap-*xxxx*.exe** software installation package to the VM where the agent is to be installed.

c. Double-click the Npcap installation package.

d. In the displayed dialog box, click **I Agree**, as shown in **Figure 2-18**.

Figure 2-18 Agreeing to install Npcap



License Agreement

Please review the license terms before installing Npcap 0.9984.

Press Page Down to see the rest of the agreement.

NPCAP COPYRIGHT / END USER LICENSE AGREEMENT

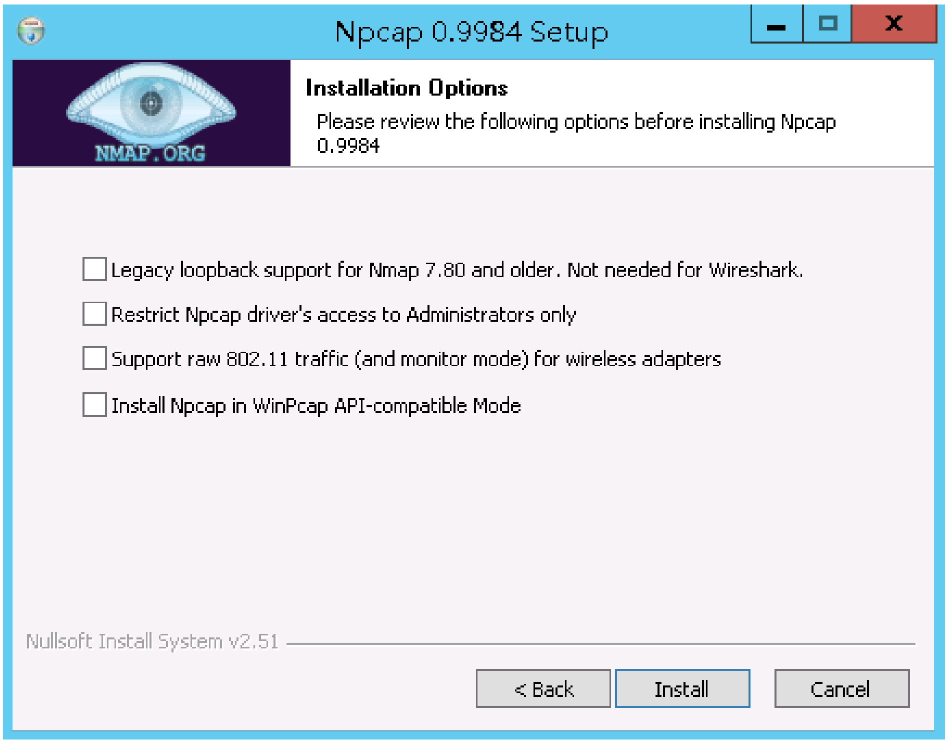
Npcap is a Windows packet sniffing driver and library and is copyright (c) 2013-2019 by Insecure.Com LLC ("The Nmap Project"). All rights reserved.

Even though Npcap source code is publicly available for review, it is not open source software and may not be redistributed without special permission from the Nmap Project. The standard version is also limited to installation on five systems. We fund the Npcap project by

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Npcap 0.9984.

e. In the displayed dialog box, leave all the check boxes unselected and click **Install**, as shown in **Figure 2-19**.

Figure 2-19 Installing Npcap



Installation Options

Please review the following options before installing Npcap 0.9984

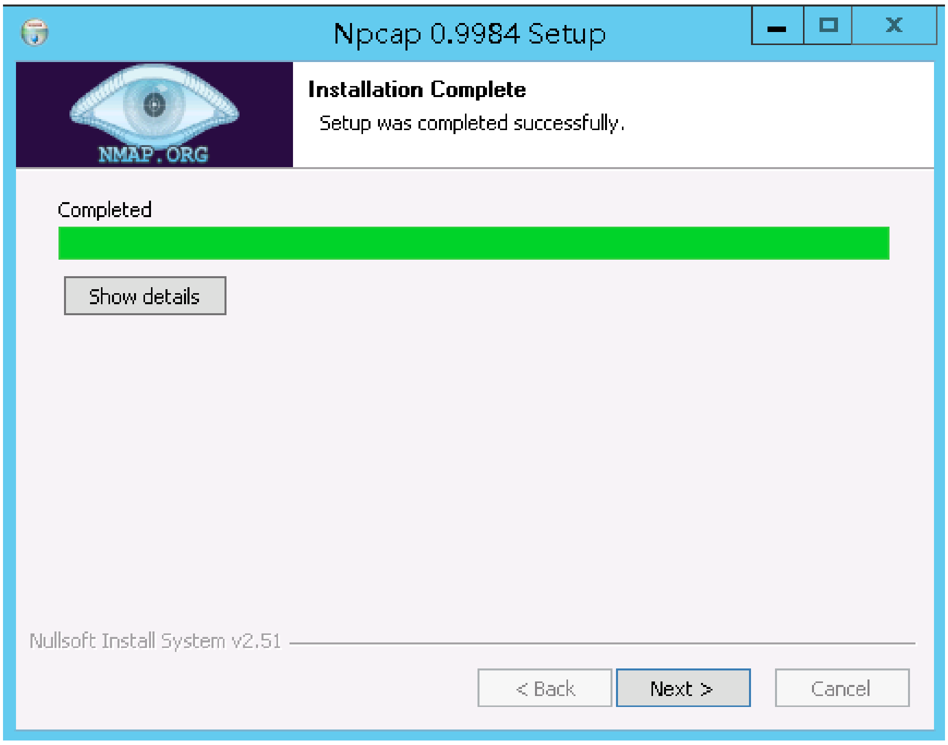
☐ Legacy loopback support for Nmap 7.80 and older. Not needed for Wireshark.

☐ Restrict Npcap driver's access to Administrators only

☐ Support raw 802.11 traffic (and monitor mode) for wireless adapters

☐ Install Npcap in WinPcap API-compatible Mode

f. In the displayed dialog box, click **Next**.



Npcap 0.9984 Setup

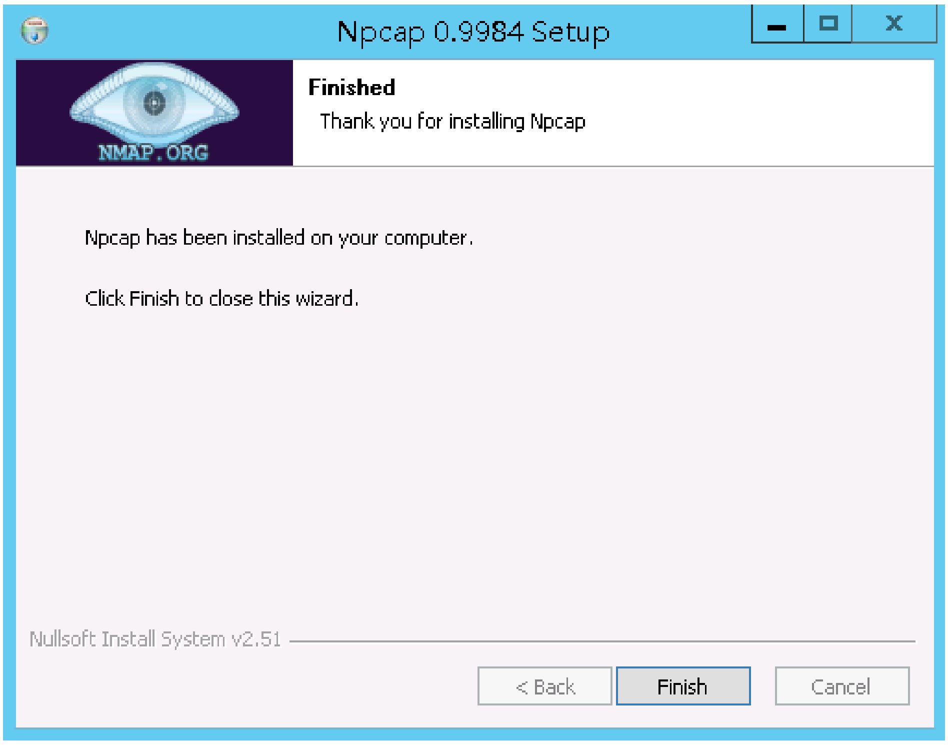
Installation Complete

Setup was completed successfully.

Completed

Nullsoft Install System v2.51

g. Click **Finish**.



Npcap 0.9984 Setup

Finished

Thank you for installing Npcap

Npcap has been installed on your computer.

Click Finish to close this wizard.

Nullsoft Install System v2.51

Step 2 Log in to the target Windows server as the **Administrator** user.

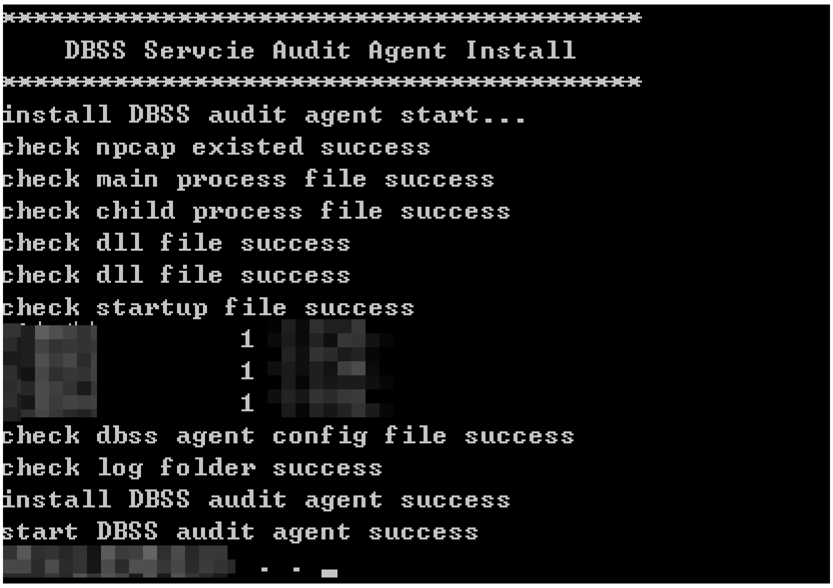
Step 3 Copy the downloaded .zip agent installation package to any directory on the server.

Step 4 Decompress the package.

Step 5 Double-click the **install.bat** file in the package directory.

Step 6 Press any key to complete installation after the output shown in **Figure 2-20** is displayed.

Figure 2-20 Installation completed



```
****************************************
    DBSS Servcie Audit Agent Install
****************************************
install DBSS audit agent start...
check npcap existed success
check main process file success
check child process file success
check dll file success
check dll file success
check startup file success
[redacted]      1  [redacted]
                1
                1
check dbss agent config file success
check log folder success
install DBSS audit agent success
start DBSS audit agent success
[redacted]  . . ._
```

Step 7 Check the installation result. If the dbss_audit_agent process can be found in the Windows Task Manager, the installation succeeded.

If it is not found, install the agent again.

----End

2.5 Step 4: 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 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 group name **default**.

Step 10 Click the **Inbound Rules** tab.

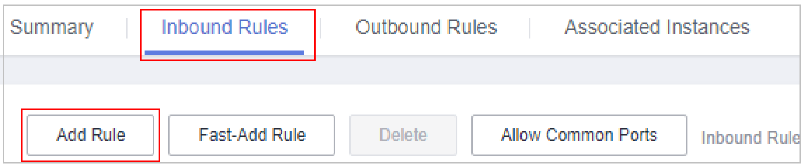
Check whether TCP (port number **8000**) and UDP protocols (port number from **7000** to **7100**) are configured in the inbound rules of the security group for the IP address of the installing node in #dbss_01_0354/li0918135319384.

- 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 11**.

Step 11 Add an inbound rule for the installing node.

1. On the **Inbound Rules** tab, click **Add Rule**.

Figure 2-21 Adding rules



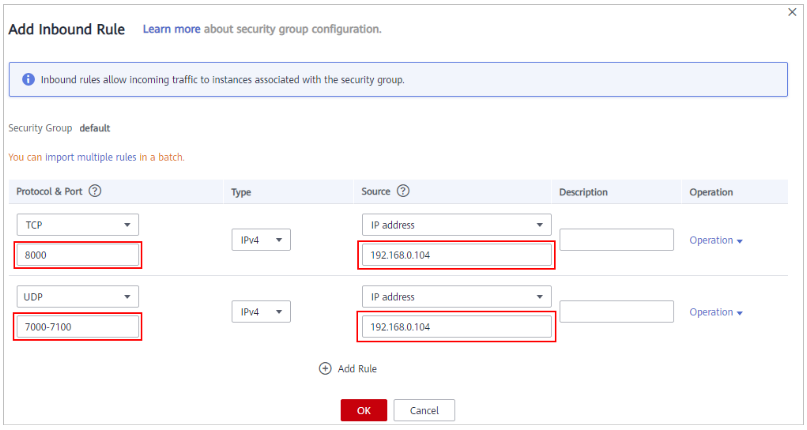
2. In the **Add Inbound Rule** dialog box, add **TCP** (port number **8000**) and **UDP** protocols (port number from **7000** to **7100**). See **Figure 2-22**.

NOTE

The source can be an IP address, an IP address segment, or a security group. Examples:

- IP address: **192.168.10.10/32**
- IP address segment: **192.168.52.0/24**
- All IP addresses: **0.0.0.0/0**
- Security group: **sg-abc**

Figure 2-22 Add Inbound Rule dialog box



Add Inbound Rule   Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group   default

You can import multiple rules in a batch.

Protocol & Port	Type	Source	Description	Operation
TCP 8000	IPv4	IP address 192.168.0.104		Operation
UDP 7000-7100	IPv4	IP address 192.168.0.104		Operation

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

2.6 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.

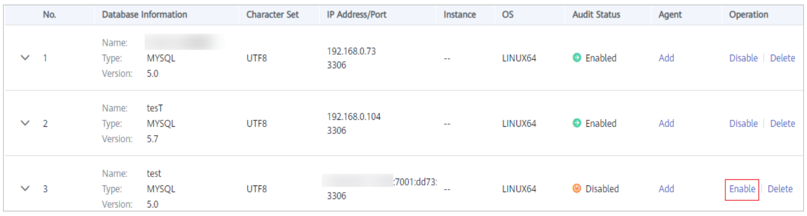
Step 3 In the navigation tree on the left, choose **Databases**.

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 you want to audit.

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

Figure 2-23 Enabling database audit



No.	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
1	Name: [redacted] Type: MYSQL Version: 5.0	UTF8	192.168.0.73 3306	--	LINUX64	● Enabled	Add	Disable | Delete
2	Name: tesT Type: MYSQL Version: 5.7	UTF8	192.168.0.104 3306	--	LINUX64	● Enabled	Add	Disable | Delete
3	Name: test Type: MYSQL Version: 5.0	UTF8	[redacted]:7001:dd73: 3306	--	LINUX64	● Disabled	Add	Enable | Delete

----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**.

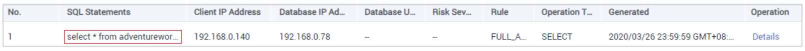
Step 5 In the navigation tree on the left, choose **Data Reports**. The **Data Reports** page is displayed.

Step 6 In the **Instance** drop-down list, select the instance that audits the target database.

Step 7 Click the **Statements** tab.

Step 8 Click 📅 next to **Time** to set the start and end time, and click **Submit**.

Figure 2-24 Viewing SQL statements



No.	SQL Statements	Client IP Address	Database IP Ad...	Database U...	Risk Sev...	Rule	Operation T...	Generated	Operation
1	select * from adventurewor...	192.168.0.140	192.168.0.78	--	--	FULL_A...	SELECT	2020/03/26 23:59:59 GMT+08:...	Details

----End

3 Enabling and Using Database Audit (Without Installing Agents)

3.1 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. In the dialog box displayed, set the database information. For details about related parameters, see **Table 3-1**.

Table 3-1 Parameters

Parameter	Description	Example Value
Name	Custom name of the database to be added	test1

Parameter	Description	Example Value
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
Type	Supported database type. The options are as follows: ● MYSQL ● ORACLE ● POSTGRESQL ● SQLSERVER ● DWS ● GaussDB for MYSOL ● GaussDB ● DAMENG ● KINGBASE ● SHENTONG ● GBase 8a ● GBase XDM Cluster ● Greenplum ● HighGo ● Mariadb **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: ● 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 ● When **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: – DM8 ● When **Type** is set to **KINGBASE**, the following version is available:	5.0

Parameter	Description	Example Value
	– 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 ● WINDOWS64	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. See **Figure 3-1**.

Figure 3-1 Successfully adding a database

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

3.2 Step 2: 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**.

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.

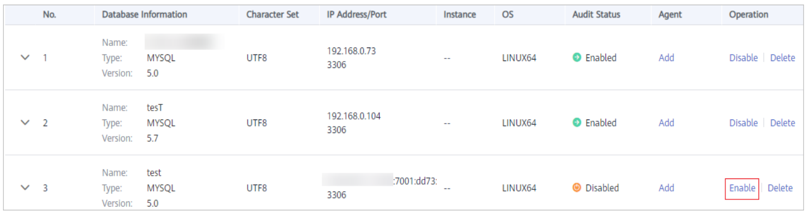
Step 3 In the navigation tree on the left, choose **Databases**.

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 you want to audit.

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

Figure 3-2 Enabling database audit



	No.	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
∨	1	Name: [redacted] Type: MYSQL Version: 5.0	UTF8	192.168.0.73 3306	--	LINUX64	● Enabled	Add	Disable | Delete
∨	2	Name: tesT Type: MYSQL Version: 5.7	UTF8	192.168.0.104 3306	--	LINUX64	● Enabled	Add	Disable | Delete
∨	3	Name: test Type: MYSQL Version: 5.0	UTF8	[redacted]:7001:dd73: 3306	--	LINUX64	● Disabled	Add	Enable | Delete

----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**.

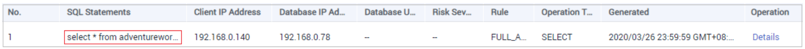
Step 5 In the navigation tree on the left, choose **Data Reports**. The **Data Reports** page is displayed.

Step 6 In the **Instance** drop-down list, select the instance that audits the target database.

Step 7 Click the **Statements** tab.

Step 8 Click 📅 next to **Time** to set the start and end time, and click **Submit**.

Figure 3-3 Viewing SQL statements



No.	SQL Statements	Client IP Address	Database IP Ad...	Database U...	Risk Sev...	Rule	Operation T...	Generated	Operation
1	select * from adventurewor...	192.168.0.140	192.168.0.78	--	--	FULL_A...	SELECT	2020/03/26 23:59:59 GMT+08:...	Details

----End

4 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**.

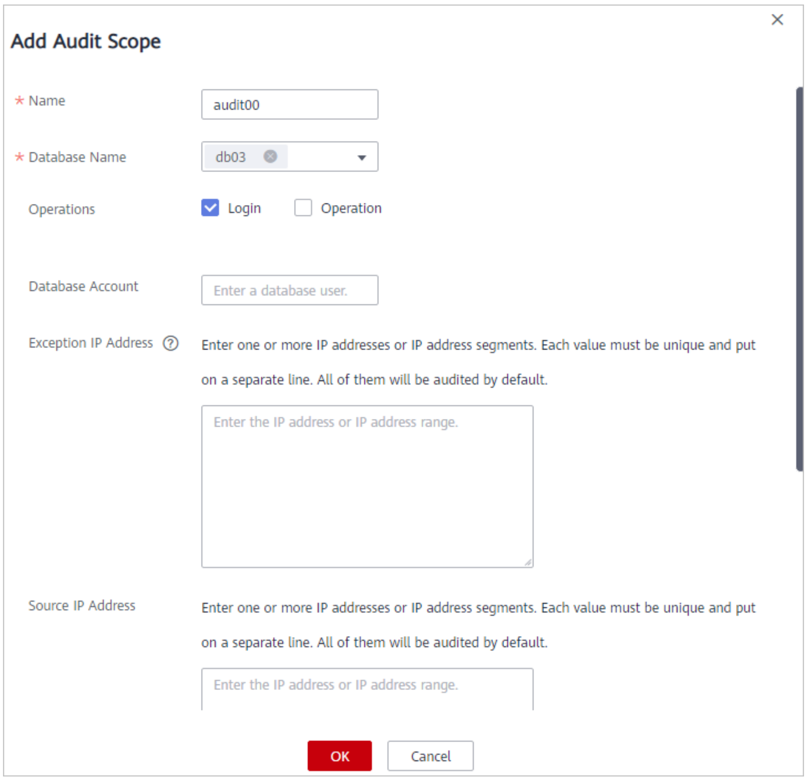
Step 4 In the **Instance** drop-down list, select an instance to add audit scope.

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, as shown in **Figure 4-1**. For details about related parameters, see **Table 4-1**.

Figure 4-1 Add Audit Scope dialog box



Add Audit Scope

* Name: audit00

* Database Name: db03

Operations: ☑ Login ☐ Operation

Database Account: Enter a database user.

Exception IP Address: Enter one or more IP addresses or IP address segments. Each value must be unique and put on a separate line. All of them will be audited by default.

Enter the IP address or IP address range.

Source IP Address: Enter one or more IP addresses or IP address segments. Each value must be unique and put on a separate line. All of them will be audited by default.

Enter the IP address or IP address range.

Table 4-1 Parameters

Parameter	Description	Example Value
Name	Name of the custom audit scope	audit00
Database Name	Database to be added to the audit scope	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.	-

Parameter	Description	Example Value
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.

5 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**.

Disabling 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.

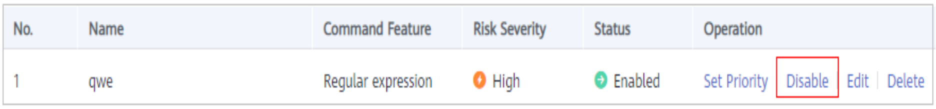
Step 5 Click the **SQL Injection** tab.

NOTE

Only user-defined rules can be edited and deleted. Default rules can only be enabled and disabled.

Step 6 Locate the SQL injection rule you want to disable, and click **Disable** in the **Operation** column.

Figure 5-1 Disabling an SQL injection detection rule



No.	Name	Command Feature	Risk Severity	Status	Operation
1	qwe	Regular expression	High	Enabled	Set Priority Disable Edit | Delete

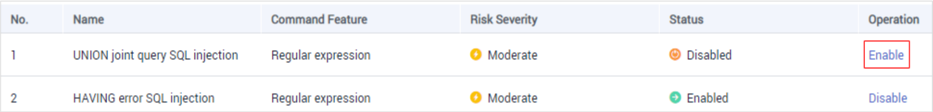
When the status of an SQL injection detection rule is **Disabled**, SQL injection detection is disabled successfully.

----End

Follow-Up Procedure

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

Figure 5-2 Enabling an SQL injection detection rule



No.	Name	Command Feature	Risk Severity	Status	Operation
1	UNION joint query SQL injection	Regular expression	Moderate	Disabled	Enable
2	HAVING error SQL injection	Regular expression	Moderate	Enabled	Disable

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

6 Adding Risky Operations

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.

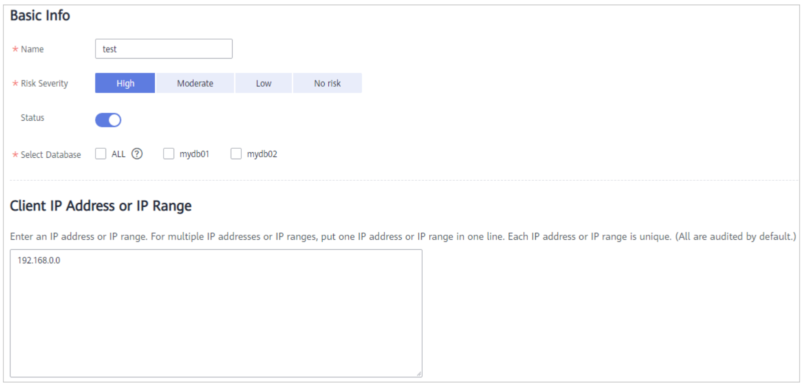
Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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, as shown in **Figure 6-1**. .

Figure 6-1 Setting the basic information and client IP address



Basic Info

* Name: test

* Risk Severity: [✓ High] Moderate Low No risk

Status: ●

* Select Database: □ ALL ⓘ □ mydb01 □ mydb02

Client IP Address or IP Range

Enter an IP address or IP range. For multiple IP addresses or IP ranges, put one IP address or IP range in one line. Each IP address or IP range is unique. (All are audited by default.)

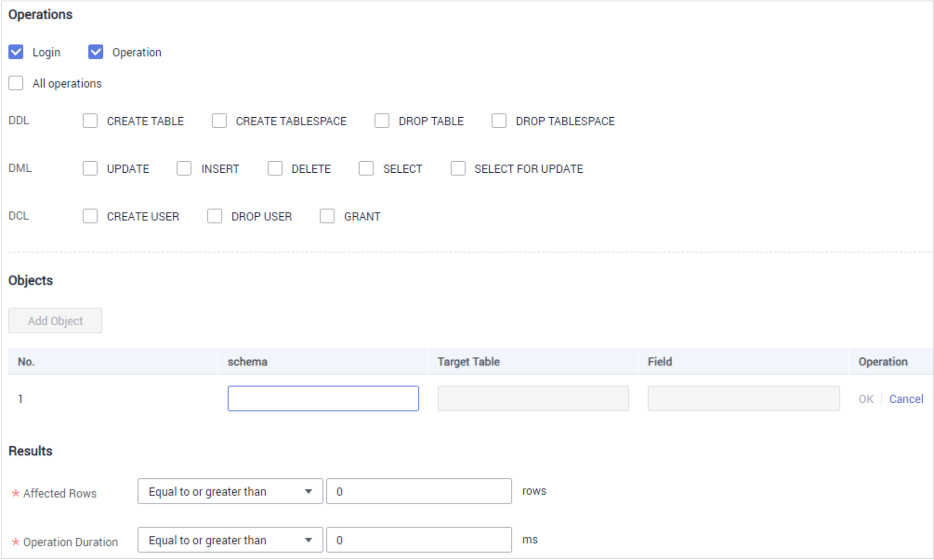
192.168.0.0

Table 6-1 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	●
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, as shown in **Figure 6-2**. For details about related parameters, see **Table 6-2**.

Figure 6-2 Setting the operation type, operation object, and execution result



Operations

☑ Login ☑ Operation

□ All operations

DDL □ CREATE TABLE □ CREATE TABLESPACE □ DROP TABLE □ DROP TABLESPACE

DML □ UPDATE □ INSERT □ DELETE □ SELECT □ SELECT FOR UPDATE

DCL □ CREATE USER □ DROP USER □ GRANT

Objects

Add Object

No.	schema	Target Table	Field	Operation
1				OK | Cancel

Results

* Affected Rows: Equal to or greater than ▾ 0 rows

* Operation Duration: Equal to or greater than ▾ 0 ms

Table 6-2 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 schema, 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

7 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.

NOTE

Only user-defined rules can be edited and deleted. Default rules can only be enabled and disabled.

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.

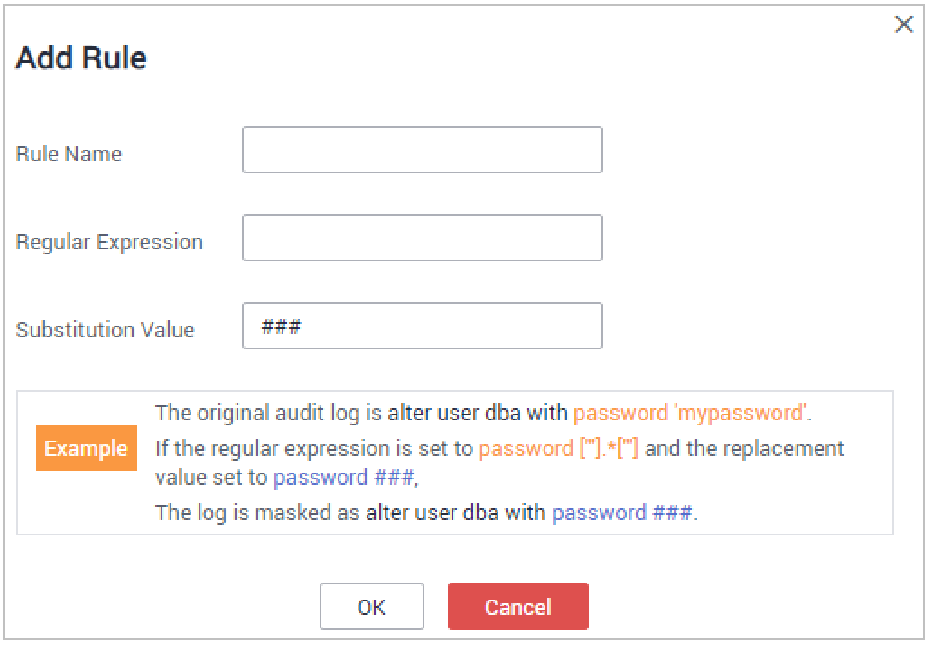
  Do not enable this function if you want to prepare for PCI DSS/PCI 3DS CSS certification.

- **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, as shown in **Figure 7-1**. For details about related parameters, see **Table 7-1**.

Figure 7-1 Add Rule dialog box



Add Rule

Rule Name

Regular Expression

Substitution Value ###

Example

The original audit log is alter user dba with password 'mypassword'.

If the regular expression is set to password ["].*["] and the replacement value set to password ###,

The log is masked as alter user dba with password ###.

Table 7-1 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.

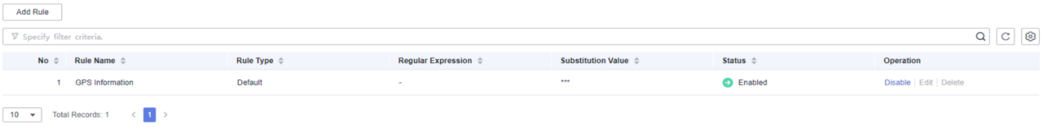
----End

Verifying a Rule

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

Step 1 Enable **Mask Privacy Data**, and ensure the "Passport NO." masking rule is enabled, as shown in **Figure 7-2**.

Figure 7-2 Enabling privacy data protection



No	Rule Name	Rule Type	Regular Expression	Substitution Value	Status	Operation
1	GPS Information	Default	-	***	Enabled	Disable | Edit | Delete

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="*Passport NO.*";

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

Step 5 In the navigation tree on the left, choose **Data Reports**. The **Data Reports** page is displayed.

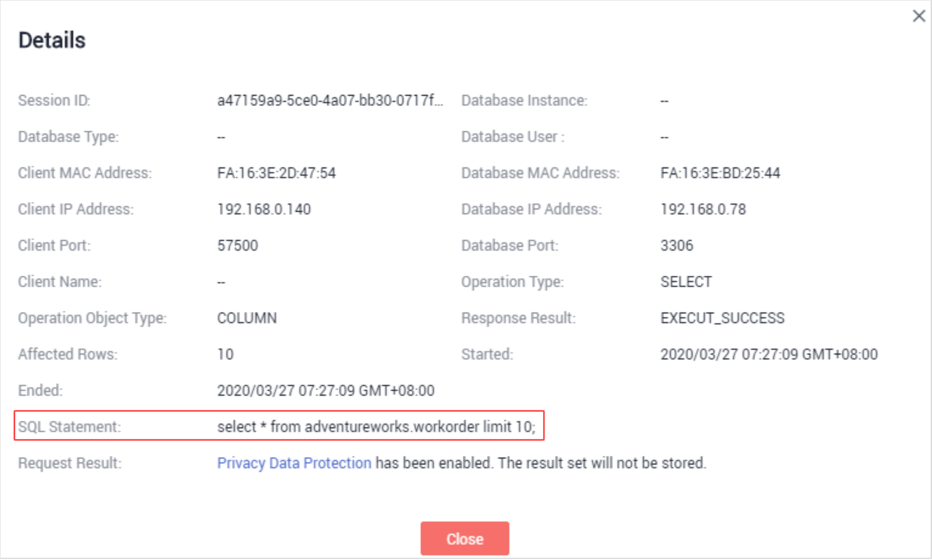
Step 6 In the **Instance** drop-down list, select the instance whose SQL statement information you want to view. Click the **Statements** tab.

Step 7 Set filtering conditions to find the entered SQL statement.

Step 8 In the row containing the SQL statement, click **Details** in the **Operation** column.

Step 9 Check the SQL statement information. The content of **SQL Statement** is shown in **Figure 7-3**, indicating that the masking function is normal.

Figure 7-3 SQL statement with sensitive data masked



Details

Session ID:	a47159a9-5ce0-4a07-bb30-0717f...	Database Instance:	--
Database Type:	--	Database User :	--
Client MAC Address:	FA:16:3E:2D:47:54	Database MAC Address:	FA:16:3E:BD:25:44
Client IP Address:	192.168.0.140	Database IP Address:	192.168.0.78
Client Port:	57500	Database Port:	3306
Client Name:	--	Operation Type:	SELECT
Operation Object Type:	COLUMN	Response Result:	EXECUT_SUCCESS
Affected Rows:	10	Started:	2020/03/27 07:27:09 GMT+08:00
Ended:	2020/03/27 07:27:09 GMT+08:00		
SQL Statement:	select * from adventureworks.workorder limit 10;		
Request Result:	Privacy Data Protection has been enabled. The result set will not be stored.		

----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.

8 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.

Procedure

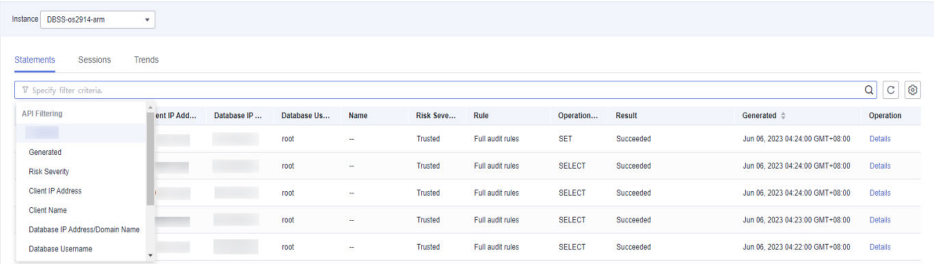
Step 1 Log in to the management console.

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

Step 3 Click the **Statements** tab.

Step 4 View SQL statement information.

Figure 8-1 Querying SQL statements



Instance DBSS-os2914-arm

ent IP Add...	Database IP ...	Database Us...	Name	Risk Seve...	Rule	Operation...	Result	Generated	Operation
[redacted]	[redacted]	root	--	Trusted	Full audit rules	SET	Succeeded	Jun 06, 2023 04:24:00 GMT+08:00	Details
[redacted]	[redacted]	root	--	Trusted	Full audit rules	SELECT	Succeeded	Jun 06, 2023 04:24:00 GMT+08:00	Details
[redacted]	[redacted]	root	--	Trusted	Full audit rules	SELECT	Succeeded	Jun 06, 2023 04:24:00 GMT+08:00	Details
[redacted]	[redacted]	root	--	Trusted	Full audit rules	SELECT	Succeeded	Jun 06, 2023 04:23:00 GMT+08:00	Details
[redacted]	[redacted]	root	--	Trusted	Full audit rules	SELECT	Succeeded	Jun 06, 2023 04:22:00 GMT+08:00	Details

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

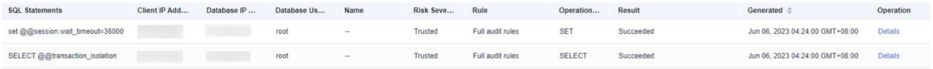
- Select **All**, **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days** for **Time** and click 🔍 to view SQL statements of the specified time range.
- Select **All**, **High**, **Moderate**, **Low**, or **Trusted** for **Risk Severity** and click 🔍. SQL statements of specified severity are displayed in the list.

NOTE

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

Step 5 In the row containing the desired SQL statement, click **Details** in the **Operation** column.

Figure 8-2 Viewing details of SQL statements



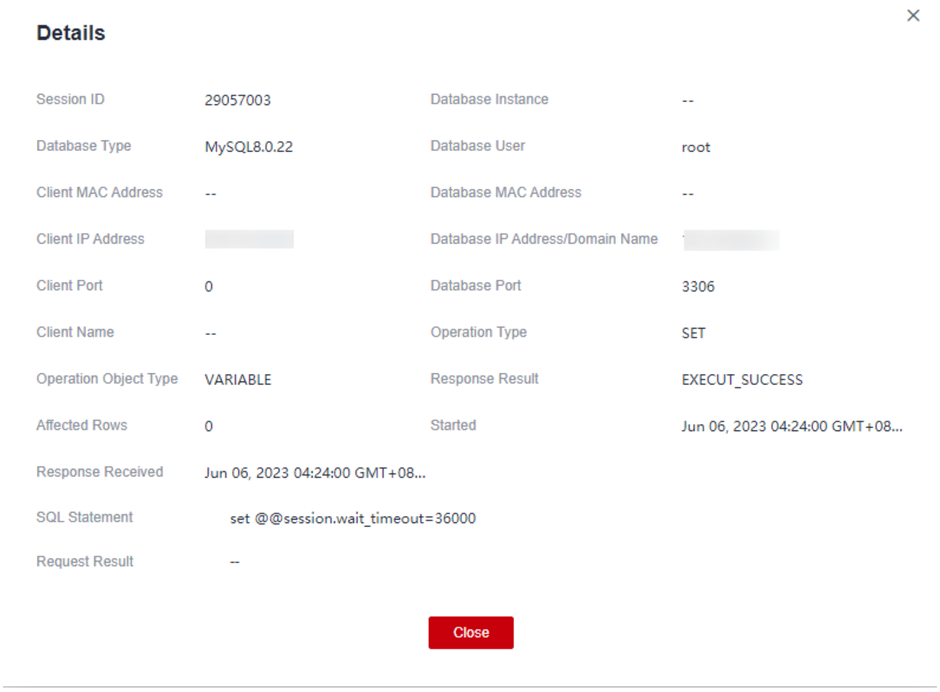
SQL Statements	Client IP Add...	Database IP ...	Database Us...	Name	Risk Seve...	Rule	Operation...	Result	Generated	Operation
set @@session.wait_timeout=36000	[redacted]	[redacted]	root	--	Trusted	Full audit rules	SET	Succeeded	Jun 06, 2023 04:24:00 GMT+08:00	Details
SELECT @@transaction_isolation	[redacted]	[redacted]	root	--	Trusted	Full audit rules	SELECT	Succeeded	Jun 06, 2023 04:24:00 GMT+08:00	Details

Step 6 View the SQL statement information in the **Details** dialog box, as shown in **Figure 8-3**. For details about related parameters, see **Table 8-1**.

NOTICE

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

Figure 8-3 Details dialog box



Details

Session ID	29057003	Database Instance	--
Database Type	MySQL8.0.22	Database User	root
Client MAC Address	--	Database MAC Address	--
Client IP Address	[redacted]	Database IP Address/Domain Name	[redacted]
Client Port	0	Database Port	3306
Client Name	--	Operation Type	SET
Operation Object Type	VARIABLE	Response Result	EXECUT_SUCCESS
Affected Rows	0	Started	Jun 06, 2023 04:24:00 GMT+08...
Response Received	Jun 06, 2023 04:24:00 GMT+08...		
SQL Statement	set @@session.wait_timeout=36000		
Request Result	--		

Table 8-1 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

Parameter	Description
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/Domain Name	IP address or the domain name 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 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.

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 **Data Reports**. The **Data Reports** page is displayed.

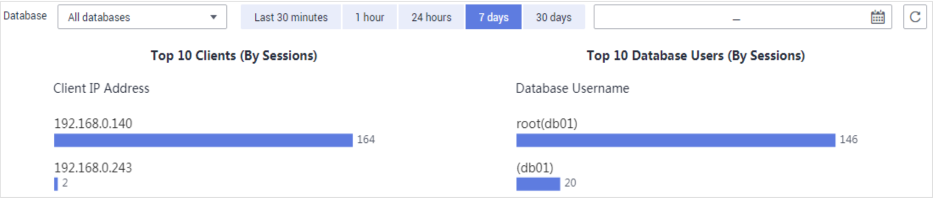
Step 4 In the **Instance** drop-down list, select the instance whose session information you want to view.

Step 5 Click the **Sessions** tab.

Step 6 View the session distribution chart, as shown in **Figure 9-1**.

- 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.

Figure 9-1 Viewing session distribution



Database: All databases

7 days

----End

10 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.

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 **Data Reports**. The **Data Reports** page is displayed.

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

Step 5 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**, **Today**, **7 days**, or **30 days**, or click 📅 to customize start time and end time to view the statistics of the specified time range.

----End

11 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.

Report Types

Database audit provides eight types of report templates. **Table 11-1** lists the report names. You can generate reports and set report tasks as needed.

Table 11-1 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.
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.

Template Name	Report Types	Description
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.

Step 1: Generating a Report

You can generate reports immediately or periodically. You can also customize the generation time, frequency, and format of reports.

- **Method 1: Generating a Report Immediately**

Step 1 Log in to the management console.

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

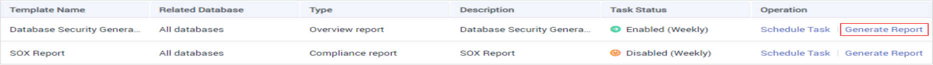
Step 3 In the navigation tree on the left, choose **Reports**.

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 In the **Operation** column of a report template, click **Generate Report**.

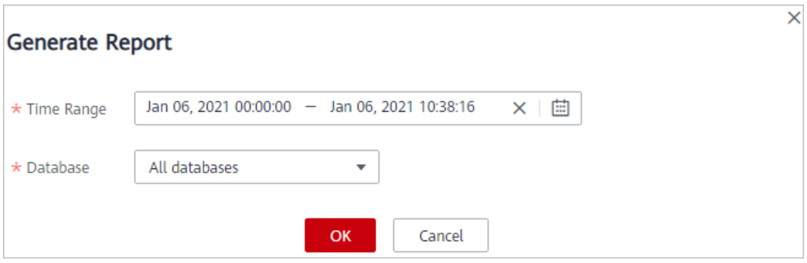
Figure 11-1 Report template list



Template Name	Related Database	Type	Description	Task Status	Operation
Database Security Genera...	All databases	Overview report	Database Security Genera...	Enabled (Weekly)	Schedule Task | Generate Report
SOX Report	All databases	Compliance report	SOX Report	Disabled (Weekly)	Schedule Task | Generate Report

Step 7

Figure 11-2 Generate Report



Generate Report

* Time Range: Jan 06, 2021 00:00:00 — Jan 06, 2021 10:38:16

* Database: All databases

Step 8 Click **OK**.

----End

- **Method 2: Setting Periodic Report Release**

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.

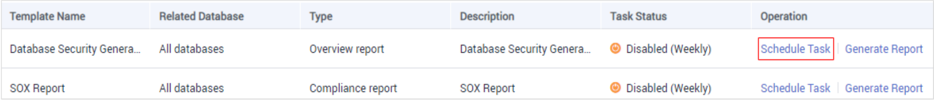
Step 3 In the navigation tree on the left, choose **Reports**.

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, as shown in **Figure 11-3**.

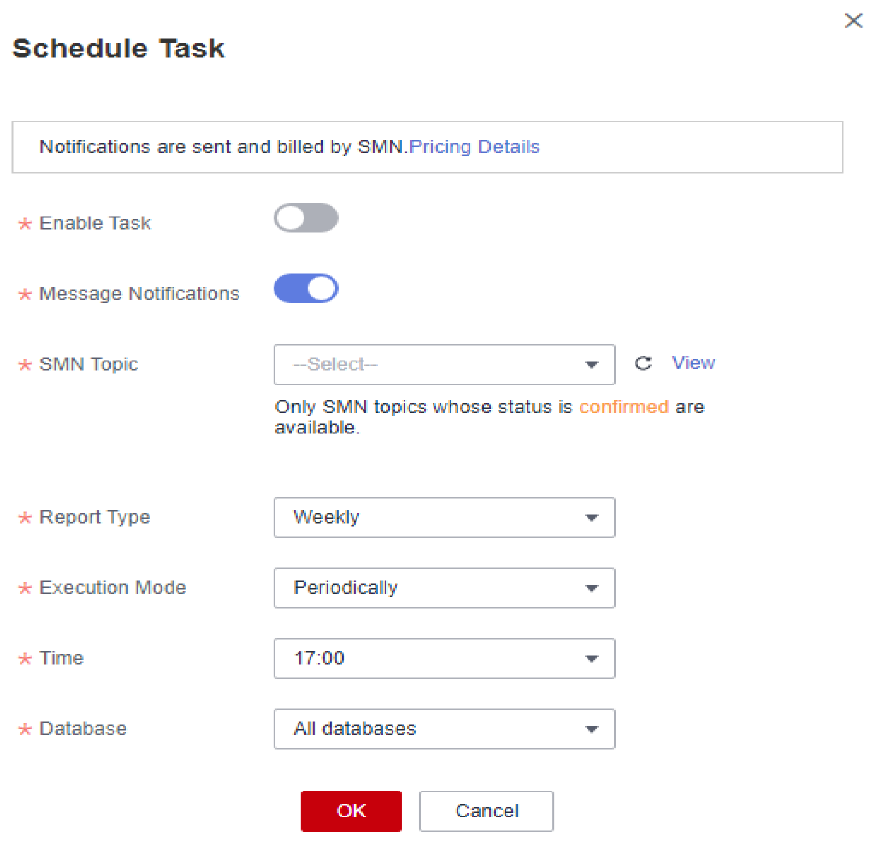
Figure 11-3 Setting a task



Template Name	Related Database	Type	Description	Task Status	Operation
Database Security Genera...	All databases	Overview report	Database Security Genera...	● Disabled (Weekly)	Schedule Task | Generate Report
SOX Report	All databases	Compliance report	SOX Report	● Disabled (Weekly)	Schedule Task | Generate Report

Step 7 In the displayed dialog box, set the parameters of the scheduled task, as shown in **Figure 11-4**. For details about related parameters, see **Table 11-2**.

Figure 11-4 Setting a scheduled task



Schedule Task

Notifications are sent and billed by SMN.Pricing Details

* Enable Task ○

* Message Notifications ●

* SMN Topic --Select-- View

Only SMN topics whose status is confirmed are available.

* Report Type Weekly

* Execution Mode Periodically

* Time 17:00

* Database All databases

Table 11-2 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*.	-

Parameter	Description	Example Value
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
Database	Database for which you want to execute the report task	-

Step 8 Click **OK**.

----End

Step 2: Previewing and Downloading Audit Reports

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.

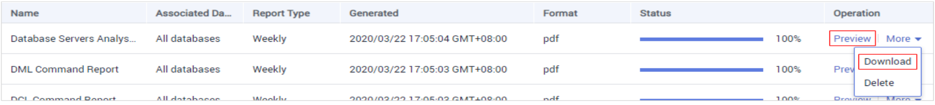
Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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. See **Figure 11-5**..

Figure 11-5 Previewing or downloading an audit report



Name	Associated Da...	Report Type	Generated	Format	Status	Operation
Database Servers Analys...	All databases	Weekly	2020/03/22 17:05:04 GMT+08:00	pdf	100%	Preview | More
DML Command Report	All databases	Weekly	2020/03/22 17:05:03 GMT+08:00	pdf	100%	Prev
DCL Command Report	All databases	Weekly	2020/03/22 17:05:03 GMT+08:00	pdf	100%	Preview | More

----End

12 Configuring Alarm Notifications

After configuring alarm notifications, you can receive DBSS alarms on database risks. If this function is not enabled, you have to log in to the management console to view alarms.

- Alarm notifications may be mistakenly blocked. If you have enabled notifications but not received any, check whether they have been blocked as spasms.
- The system collects alarm statistics every 5 minutes and sends alarm notifications (if any).
- You can also enable report notifications to get notified when the reports you subscribed to are generated. For details, see **Viewing Audit Reports**.

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.

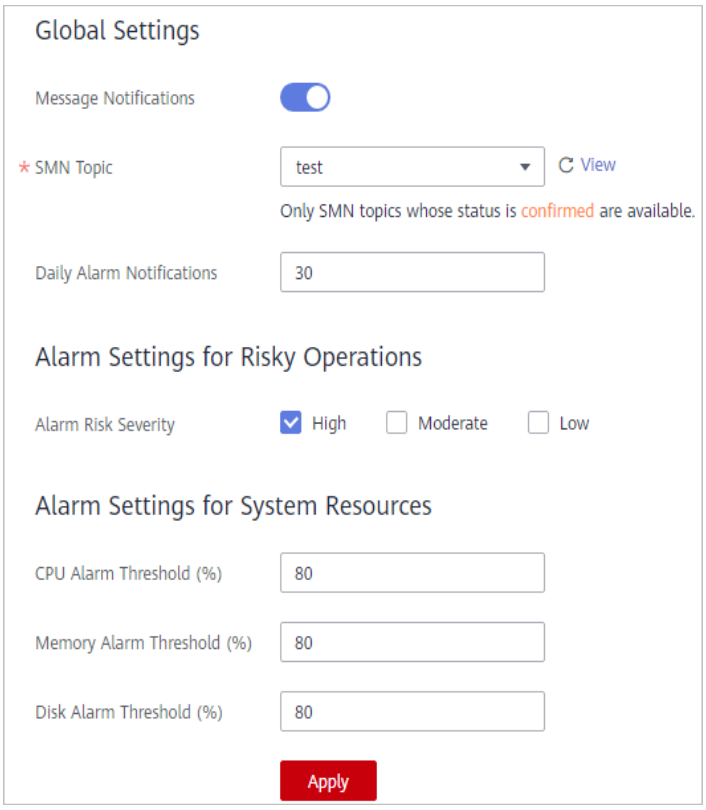
Step 3 In the navigation tree on the left, choose **Settings**.

Step 4 In the **Instance** drop-down list, select an instance to configure alarm notifications.

Step 5 Click the **Alarm Notifications** tab.

Step 6 Set alarm notifications. For details about related parameters, see **Table 12-1**.

Figure 12-1 Configuring alarm notifications



Global Settings

Message Notifications: on

* SMN Topic: test View

Only SMN topics whose status is confirmed are available.

Daily Alarm Notifications: 30

Alarm Settings for Risky Operations

Alarm Risk Severity: ☑ High □ Moderate □ Low

Alarm Settings for System Resources

CPU Alarm Threshold (%): 80

Memory Alarm Threshold (%): 80

Disk Alarm Threshold (%): 80

Apply

Table 12-1 Alarm notification parameters

Parameter	Description	Example Value
Message Notifications	Enables or disables notifications.	
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. **NOTE** Before selecting a topic, ensure that the subscription status of the topic is **Confirmed**. Otherwise, alarm notifications may not be received. For details about topics and subscriptions, see *Simple Message Notification User Guide*.	-
Daily Alarm Notifications	Total number of alarms allowed to be sent every day **NOTICE** ● If the number of alarms exceeds this value on a day, no more notification will be sent on that day. ● There is no fixed time point for sending alarm notifications. The system collects statistics every 5 minutes and sends alarm notifications (if any).	30

Parameter	Description	Example Value
Alarm Risk Severity	Risk severity of the risk log. The options are as follows: - **High** - **Moderate** - **Low**	High
CPU Alarm Threshold (%)	CPU alarm threshold of an audit instance. When the threshold is exceeded, an alarm notification is generated.	80
Memory Alarm Threshold (%)	Memory alarm threshold of an audit instance. When the threshold is exceeded, an alarm notification is generated.	80
Disk Alarm Threshold (%)	Disk alarm threshold of an audit instance. When the threshold is exceeded, an alarm notification is generated.	80

Step 7 Click **Apply**.

----End

13 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.

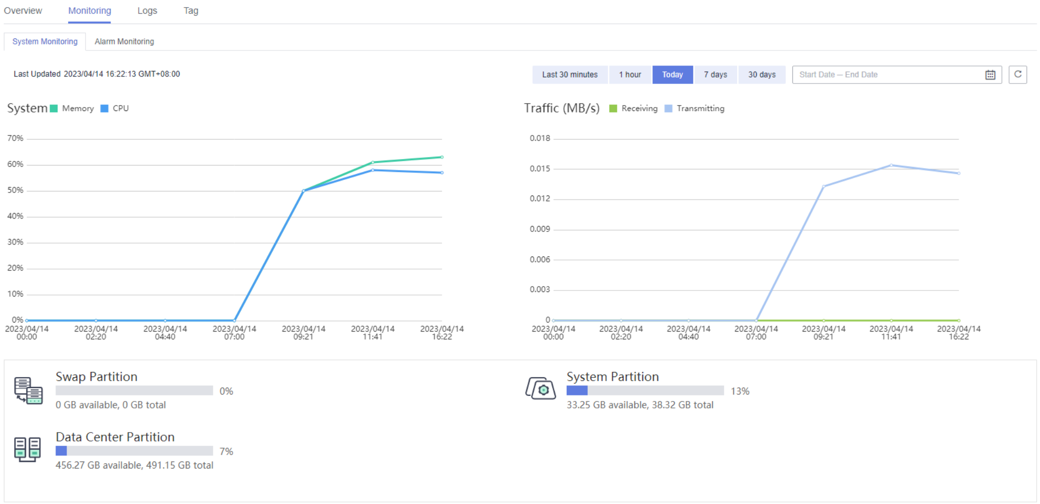
Step 3 In the navigation tree on the left, choose **Instances**.

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, as shown in**Figure 13-1**.

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.

Figure 13-1 Viewing the system monitoring



Last Updated 2023/04/14 16:22:13 GMT+08:00

Swap Partition 0%
0 GB available, 0 GB total

System Partition 13%
33.25 GB available, 38.32 GB total

Data Center Partition 7%
456.27 GB available, 491.15 GB total

----End

14 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

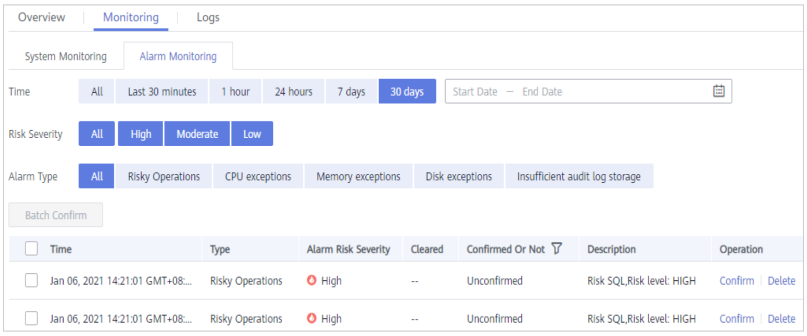
Step 1 Log in to the management console.

Step 2 In the navigation tree on the left, choose **Instances**.

Step 3 Click the name of an instance, click the **Monitoring** tab, and then the **Alarm Monitoring** tab.

Step 4 View the alarm information, as shown in **Figure 14-1**. For details about related parameters, see **Table 14-1**.

Figure 14-1 Viewing the alarms



□	Time	Type	Alarm Risk Severity	Cleared	Confirmed Or Not	Description	Operation
□	Jan 06, 2021 14:21:01 GMT+08:...	Risky Operations	High	--	Unconfirmed	Risk SQL,Risk level: HIGH	Confirm | Delete
□	Jan 06, 2021 14:21:01 GMT+08:...	Risky Operations	High	--	Unconfirmed	Risk SQL,Risk level: HIGH	Confirm | Delete

Table 14-1 Parameters of alarms

Parameter	Description
Time	Time when an alarm occurred.

Parameter	Description
Type	Alarm type. The options are as follows: ● Risky operations ● CPU exceptions ● Memory exceptions ● Disk exceptions ● Insufficient audit log storage
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:

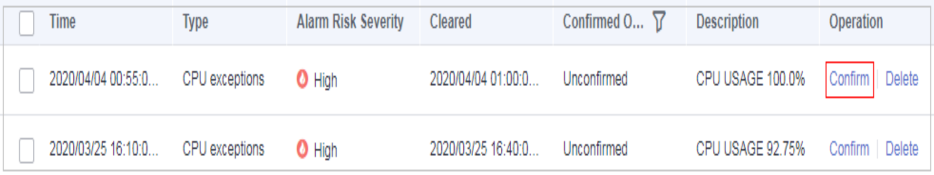
- Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days** for **Time**, and click 🔍 to view alarms of the specified time range.
- Select **All**, **High**, **Moderate**, or **Low** for **Risk Severity**. Alarms of specified severity are displayed in the list.
- Select an alarm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

Figure 14-2 Confirming an alarm



□	Time	Type	Alarm Risk Severity	Cleared	Confirmed O... ▽	Description	Operation
□	2020/04/04 00:55:0...	CPU exceptions	High	2020/04/04 01:00:0...	Unconfirmed	CPU USAGE 100.0%	Confirm | Delete
□	2020/03/25 16:10:0...	CPU exceptions	High	2020/03/25 16:40:0...	Unconfirmed	CPU USAGE 92.75%	Confirm | Delete

NOTE

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

15 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

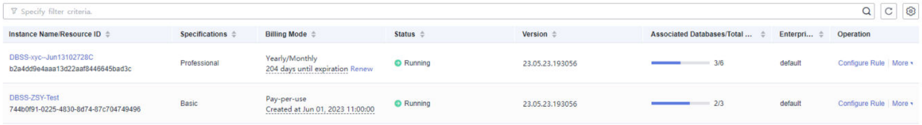
Step 1 Log in to the management console.

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 15-1**.

Figure 15-1 Viewing database audit instances



Specify filter criteria.

Instance Name/Resource ID	Specifications	Billing Mode	Status	Version	Associated Databases/Total ...	Enterpri...	Operation
DBSS-xyc--Jun13102728C b2a4dd9e4aaa13d22aaf8446645bad3c	Professional	Yearly/Monthly 204 days until expiration Renew	Running	23.05.23.193056	3/6	default	Configure Rule | More
DBSS-ZSY-Test 744b0f91-0225-4830-8d74-87c704749496	Basic	Pay-per-use Created at Jun 01, 2023 11:00:00	Running	23.05.23.193056	2/3	default	Configure Rule | More

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 15-1 Parameters

Parameter	Description
Instance Name/ID	Name and ID of an instance. Instance ID is automatically generated.
Specifications	Edition of an instance
Billing Mode	Billing mode (yearly/monthly) and expiration time of the 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
Enterprise Project	Enterprise project name of the instance

Parameter	Description
Operation	Operations can be performed on the instance. The options are as follows: ● Configure Rules ● Enable ● Disable ● Restart ● View Details ● Delete

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.

- View Details

  Locate the row that contains the instance that failed to be created, choose **More** > **View Details** in the **Operation** column. In the dialog box that is displayed, view the instance creation failure details.

----End

16 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.

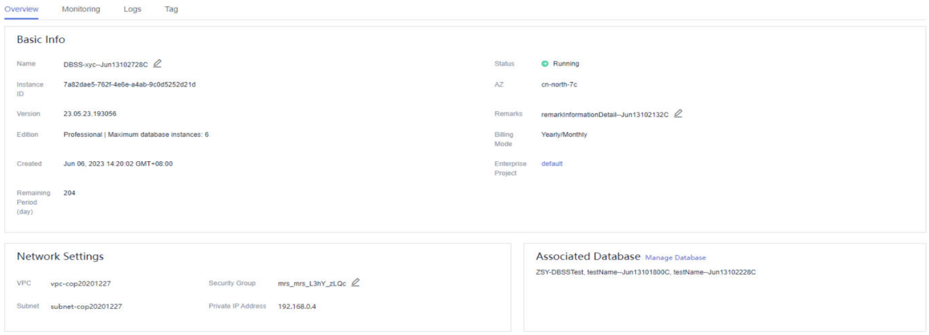
Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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. See **Figure 16-1**. For details about related parameters, see **Table 16-1**.

Figure 16-1 Viewing the instance overview



Basic Info

Name: DBSS-xyc--Jun13102728C

Instance ID: 7a82dae5-762f-4e6e-a4ab-9c0d5252d21d

Version: 23.05.23.193056

Edition: Professional | Maximum database instances: 6

Created: Jun 06, 2023 14:20:02 GMT+08:00

Remaining Period (day): 204

Status: Running

AZ: cn-north-7c

Remarks: remarkInformationDetail--Jun13102132C

Billing Mode: Yearly/Monthly

Enterprise Project: default

Network Settings

VPC: vpc-cop20201227

Subnet: subnet-cop20201227

Security Group: mrs_mrs_L3hY_zLQc

Private IP Address: 192.168.0.4

Associated Database

ZSY-DBSSTest, testName--Jun13101800C, testName--Jun13102228C

Table 16-1 Parameters of the instance overview

Category	Parameter	Description
Basic Info	Name	Name of an instance. You can click ✎ next to **Name** to change it.
	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 Click ✎ next to remarks to modify it.
	Edition	Edition of an instance
	Billing Mode	Billing mode of an instance
	Created	Time when an instance is created
	Enterprise Project	Enterprise project that the instance belongs to.
	Remaining Period (day)	Remaining days for which an instance can be used
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

Category	Parameter	Description
Associated Database	-	Database information associated with an instance Click **Manage Database**, and the **Databases** page is displayed.

----End

17 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.

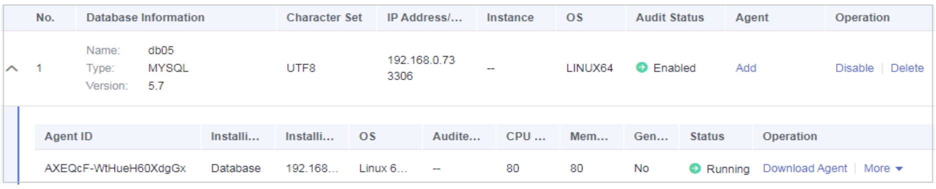
Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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 17-1**.

Figure 17-1 Viewing the database and agent information



No.	Database Information	Character Set	IP Address/...	Instance	OS	Audit Status	Agent	Operation
1	Name: db05 Type: MYSQL Version: 5.7	UTF8	192.168.0.73 3306	--	LINUX64	Enabled	Add	Disable | Delete

Agent ID	Installi...	Installi...	OS	Audite...	CPU ...	Mem...	Gen...	Status	Operation
AXEQcF-WtHueH60XdgGx	Database	192.168...	Linux 6...	--	80	80	No	Running	Download Agent | More ▾

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 17-1 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.	Add an agent.

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.

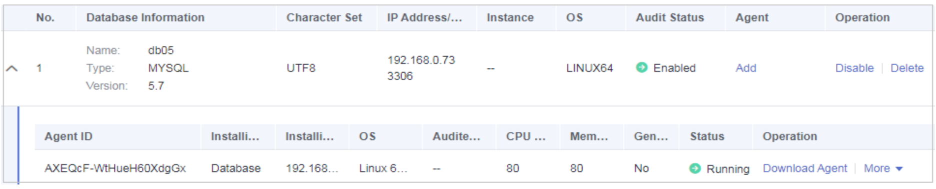
Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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, as shown in **Figure 17-2**. For details about related parameters, see **Table 17-2**.

Figure 17-2 Viewing the database and agent information



	No.	Database Information	Character Set	IP Address/...	Instance	OS	Audit Status	Agent	Operation
^	1	Name: db05 Type: MYSQL Version: 5.7	UTF8	192.168.0.73 3306	--	LINUX64	● Enabled	Add	Disable | Delete

Agent ID	Installi...	Installi...	OS	Audite...	CPU ...	Mem...	Gen...	Status	Operation
AXEQcF-WtHueH60XdgGx	Database	192.168...	Linux 6...	--	80	80	No	● Running	Download Agent | More ▾

Table 17-2 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.
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.
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

18 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:
  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

19 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.

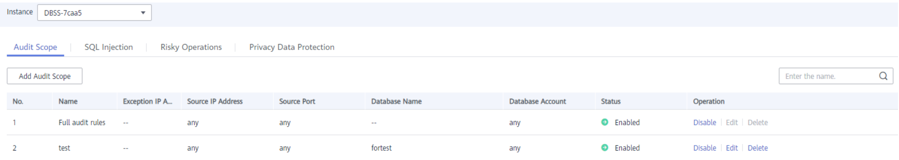
Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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 19-1**.

Figure 19-1 Viewing the audit scope



No.	Name	Exception IP A...	Source IP Address	Source Port	Database Name	Database Account	Status	Operation
1	Full audit rules	--	any	any	--	any	Enabled	Disable | Edit | Delete
2	test	--	any	any	fortest	any	Enabled	Disable | Edit | Delete

NOTE

Enter the key word of an audit scope to search.

Table 19-1 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 (supported in customized audit scopes only)

  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 (supported in customized audit scopes only)

  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

20 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.

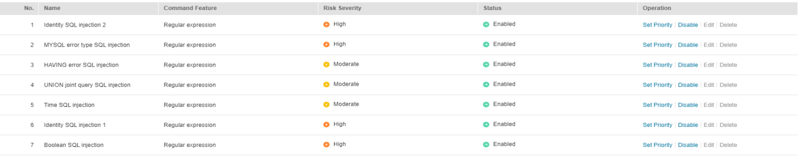
Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree, choose **Audit 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, as shown in **Figure 20-1**. For details about related parameters, see **Table 20-1**.

Figure 20-1 Viewing information about the SQL injection detection



No.	Name	Command Feature	Risk Severity	Status	Operation
1	Identity SQL injection 2	Regular expression	● High	● Enabled	Set Priority | Disable | Edit | Delete
2	MYSQL error type SQL injection	Regular expression	● High	● Enabled	Set Priority | Disable | Edit | Delete
3	HAVING error SQL injection	Regular expression	● Moderate	● Enabled	Set Priority | Disable | Edit | Delete
4	UNION joint query SQL injection	Regular expression	● Moderate	● Enabled	Set Priority | Disable | Edit | Delete
5	Time SQL injection	Regular expression	● Moderate	● Enabled	Set Priority | Disable | Edit | Delete
6	Identity SQL injection 1	Regular expression	● High	● Enabled	Set Priority | Disable | Edit | Delete
7	Boolean SQL injection	Regular expression	● High	● Enabled	Set Priority | Disable | Edit | Delete

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.
- Click **Set Priority** in the **Operation** column of an SQL injection rule to change its priority.

Table 20-1 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**
Operation	Operations on an SQL injection rule. The options are as follows: ● **Set Priority** ● **Disable** ● **Edit** ● **Delete**

----End

21 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, as shown in #dbss_01_0201/fig1952634845310.

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.

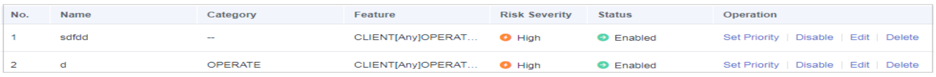
Step 3 In the navigation tree, choose **Rules**.

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 the risky operation information. For details about related parameters, see **Table 21-1**.

Figure 21-1 Viewing risky operations



No.	Name	Category	Feature	Risk Severity	Status	Operation
1	sdfdd	--	CLIENT[Any]OPERAT...	● High	● Enabled	Set Priority | Disable | Edit | Delete
2	d	OPERATE	CLIENT[Any]OPERAT...	● High	● Enabled	Set Priority | Disable | Edit | Delete

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 21-1 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

22 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 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 its privacy data protection rule.

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

NOTE

Only user-defined rules can be edited and deleted. Default rules can only be enabled and disabled.

Step 6 View the rules. For details about related parameters, see **Table 22-1**.

NOTE

- **Store Result Set**

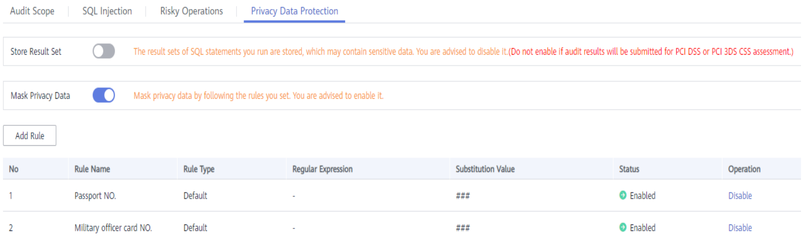
  You are advised to disable . After this function is disabled, database audit will not store the result sets of user SQL statements.

  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.

Figure 22-1 Masking rule information



Store Result Set ○ The result sets of SQL statements you run are stored, which may contain sensitive data. You are advised to disable it.(Do not enable if audit results will be submitted for PCI DSS or PCI 3DS CSS assessment.)

Mask Privacy Data ● Mask privacy data by following the rules you set. You are advised to enable it.

No	Rule Name	Rule Type	Regular Expression	Substitution Value	Status	Operation
1	Passport NO.	Default	-	###	● Enabled	Disable
2	Military officer card NO.	Default	-	###	● Enabled	Disable

Table 22-1 Masking rule parameters

Parameter	Description
Rule Name	Rule name
Rule Type	Rule type. ● Default ● User-defined
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

23 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.
- Audit reports have been generated.

Viewing a Report

Step 1 Log in to the management console.

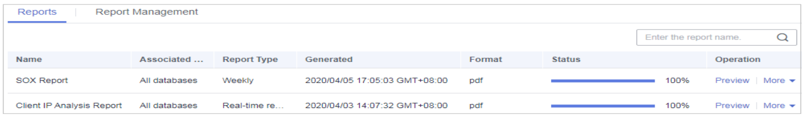
Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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 Viewing reports

Figure 23-1 Viewing a report



Name	Associated ...	Report Type	Generated	Format	Status	Operation
SOX Report	All databases	Weekly	2020/04/05 17:05:03 GMT+08:00	pdf	100%	Preview | More
Client IP Analysis Report	All databases	Real-time re...	2020/04/03 14:07:32 GMT+08:00	pdf	100%	Preview | More

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.

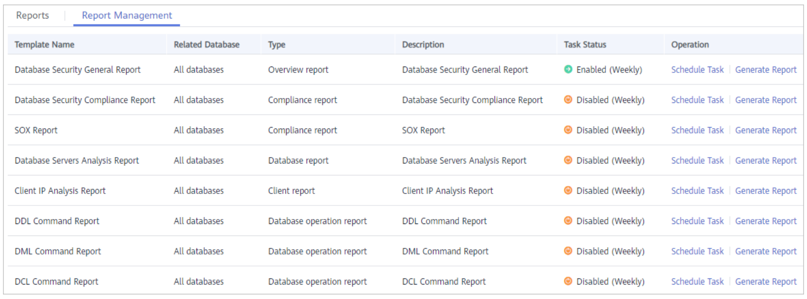
Step 3 In the navigation tree on the left, choose **Reports**.

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, as shown in **Figure 23-2**.

Figure 23-2 Viewing the template list



Template Name	Related Database	Type	Description	Task Status	Operation
Database Security General Report	All databases	Overview report	Database Security General Report	Enabled (Weekly)	Schedule Task | Generate Report
Database Security Compliance Report	All databases	Compliance report	Database Security Compliance Report	Disabled (Weekly)	Schedule Task | Generate Report
SOX Report	All databases	Compliance report	SOX Report	Disabled (Weekly)	Schedule Task | Generate Report
Database Servers Analysis Report	All databases	Database report	Database Servers Analysis Report	Disabled (Weekly)	Schedule Task | Generate Report
Client IP Analysis Report	All databases	Client report	Client IP Analysis Report	Disabled (Weekly)	Schedule Task | Generate Report
DDL Command Report	All databases	Database operation report	DDL Command Report	Disabled (Weekly)	Schedule Task | Generate Report
DML Command Report	All databases	Database operation report	DML Command Report	Disabled (Weekly)	Schedule Task | Generate Report
DCL Command Report	All databases	Database operation report	DCL Command Report	Disabled (Weekly)	Schedule Task | Generate Report

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

24 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.

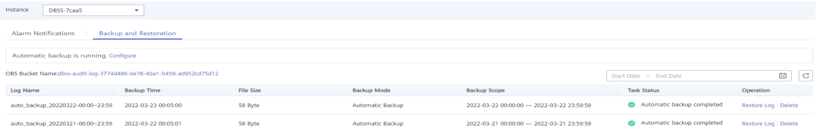
Step 3 In the navigation tree on the left, choose **Settings**.

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, as shown in **Figure 24-1**. For details about related parameters, see **Table 24-1**.

Figure 24-1 Viewing backup audit logs



Instance DBSS-7caa5

Alarm Notifications | Backup and Restoration

Automatic backup is running. Configure

OBS Bucket Name:dbss-audit-log-3774d489-be78-4ba1-b459-ad952cd75d12

Start Date — End Date

Log Name	Backup Time	File Size	Backup Mode	Backup Scope	Task Status	Operation
auto_backup_20220322-00:00~23:59	2022-03-23 00:05:00	58 Byte	Automatic Backup	2022-03-22 00:00:00 — 2022-03-22 23:59:59	Automatic backup completed	Restore Log | Delete
auto_backup_20220321-00:00~23:59	2022-03-22 00:05:01	58 Byte	Automatic Backup	2022-03-21 00:00:00 — 2022-03-21 23:59:59	Automatic backup completed	Restore Log | Delete

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 24-1 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

25 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.

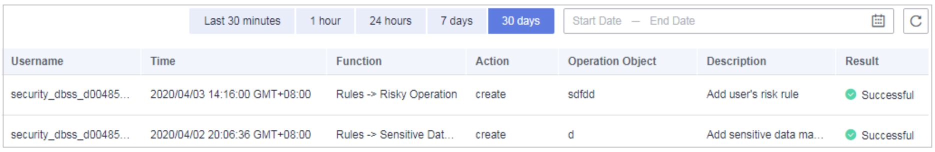
Step 3 In the navigation tree on the left, choose **Instances**.

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, as shown in **Figure 25-1**. For details about related parameters, see **Table 25-1**.

Figure 25-1 Viewing operation logs



Username	Time	Function	Action	Operation Object	Description	Result
security_dbss_d00485...	2020/04/03 14:16:00 GMT+08:00	Rules -> Risky Operation	create	sdfdd	Add user's risk rule	✓ Successful
security_dbss_d00485...	2020/04/02 20:06:36 GMT+08:00	Rules -> Sensitive Dat...	create	d	Add sensitive data ma...	✓ Successful

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 25-1 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

26 Viewing Tracing Logs

After you enable CTS, the system starts recording operations on DBSS. Operation records for the last seven days can be viewed on the CTS console.

Viewing a DBSS Trace on the CTS Console

Step 1 Log in to the management console.

Step 2 In the navigation pane on the left, click ☰ and choose **Management & Deployment** > **Cloud Trace Service**.

Step 3 Choose **Trace List** in the navigation pane.

Step 4 Click **Region** at the top of the **Trace List** page to set the corresponding conditions.

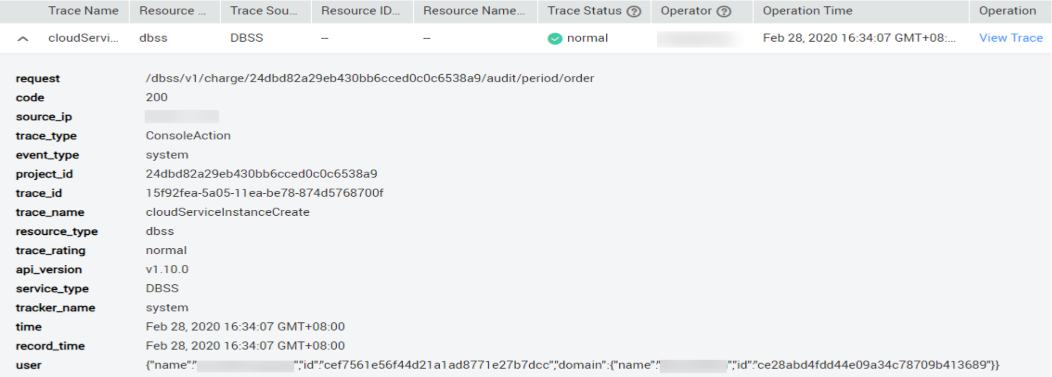
The following four filters are available:

- **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**
  - Select the filter from the drop-down list. Set **Trace Source** to **DBSS**.
  - When you select **Trace name** for **Search By**, you also need to select a specific trace name.
  - When you select **Resource ID** for **Search By**, you also need to select or enter a specific resource ID.
  - When you select **Resource name** for **Search By**, you also need to select or enter a specific resource name.
- **Operator**: Select a specific operator (a user other than tenant).
- **Trace Rating**: Available options include **All trace status**, **normal**, **warning**, and **incident**. You can only select one of them.
- In the upper right corner of the page, you can query traces in the last 1 hour, last 1 day, last 1 week, or within a customized period.

Step 5 Click **Query**.

Step 6 Click ⌄ on the left of a trace to expand its details.

Figure 26-1 Expanding trace details

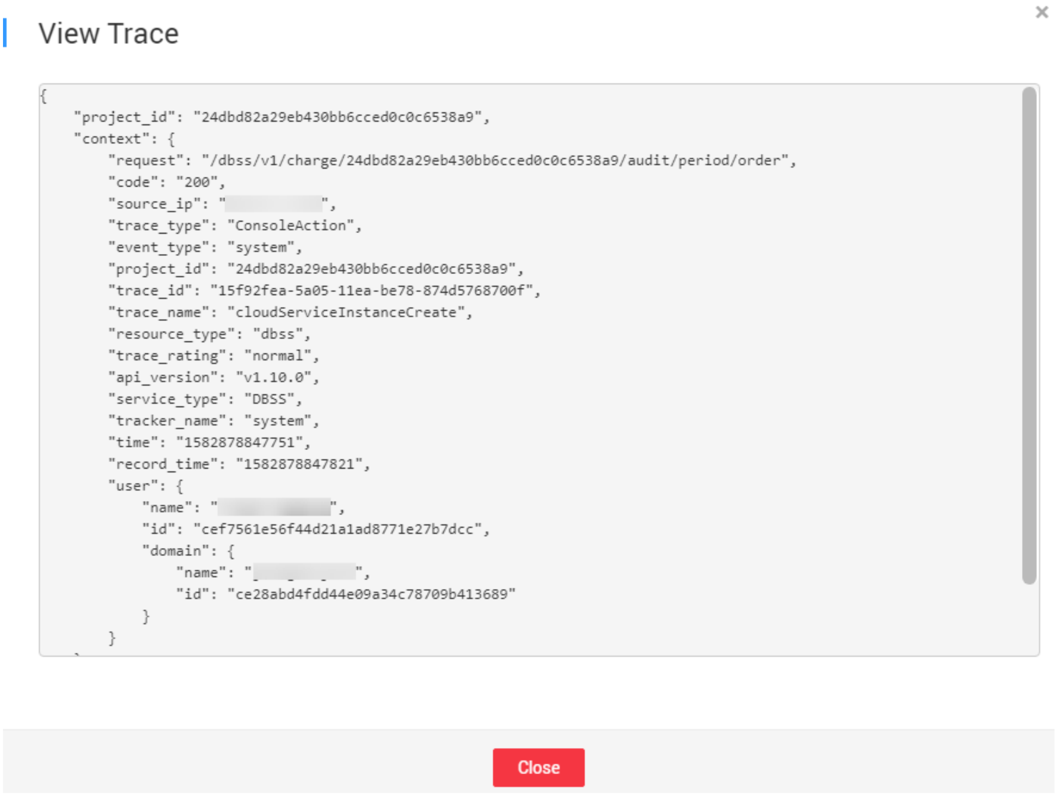


	Trace Name	Resource ...	Trace Sou...	Resource ID...	Resource Name...	Trace Status ⓘ	Operator ⓘ	Operation Time	Operation
^	cloudServi...	dbss	DBSS	--	--	● normal	[redacted]	Feb 28, 2020 16:34:07 GMT+08:...	View Trace

request	/dbss/v1/charge/24dbd82a29eb430bb6cced0c0c6538a9/audit/period/order
code	200
source_ip	[redacted]
trace_type	ConsoleAction
event_type	system
project_id	24dbd82a29eb430bb6cced0c0c6538a9
trace_id	15f92fea-5a05-11ea-be78-874d5768700f
trace_name	cloudServiceInstanceCreate
resource_type	dbss
trace_rating	normal
api_version	v1.10.0
service_type	DBSS
tracker_name	system
time	Feb 28, 2020 16:34:07 GMT+08:00
record_time	Feb 28, 2020 16:34:07 GMT+08:00
user	{"name":"[redacted]","id":"cef7561e56f44d21a1ad8771e27b7dcc","domain":{"name":"[redacted]","id":"ce28abd4fdd44e09a34c78709b413689"}}

Step 7 Click **View Trace** in the **Operation** column. On the displayed **View Trace** dialog box shown in **Figure 26-2**, the trace structure details are displayed.

Figure 26-2 Viewing a trace



```
{
    "project_id": "24dbd82a29eb430bb6cced0c0c6538a9",
    "context": {
        "request": "/dbss/v1/charge/24dbd82a29eb430bb6cced0c0c6538a9/audit/period/order",
        "code": "200",
        "source_ip": "[redacted]",
        "trace_type": "ConsoleAction",
        "event_type": "system",
        "project_id": "24dbd82a29eb430bb6cced0c0c6538a9",
        "trace_id": "15f92fea-5a05-11ea-be78-874d5768700f",
        "trace_name": "cloudServiceInstanceCreate",
        "resource_type": "dbss",
        "trace_rating": "normal",
        "api_version": "v1.10.0",
        "service_type": "DBSS",
        "tracker_name": "system",
        "time": "1582878847751",
        "record_time": "1582878847821",
        "user": {
            "name": "[redacted]",
            "id": "cef7561e56f44d21a1ad8771e27b7dcc",
            "domain": {
                "name": "[redacted]",
                "id": "ce28abd4fdd44e09a34c78709b413689"
            }
        }
```

----End

27 Auditable Operations

Cloud Trace Service (CTS) records all cloud service operations on DBSS, including requests initiated from the management console or open APIs and responses to the requests, for tenants to query, audit, and trace.

Table 27-1 lists DBSS operations recorded by CTS.

Table 27-1 DBSS operations that can be recorded by CTS

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

28 FAQs

28.1 Functions

28.1.1 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.

28.1.2 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.

28.1.3 Supported Database Types

Database audit supports the following database types and versions.

Table 28-1 Database types and versions supported by database audit

Database Type	Edition
MySQL	● 5.0, 5.1, 5.5, 5.6, 5.7 ● 8.0 (8.0.11 and earlier) ● 8.0.23
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

28.1.4 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 28-2**.

Table 28-2 Supported Linux OS versions

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

System Name	System version
Oracle Linux	- Oracle Linux 6.9 (64bit) - Oracle Linux 7.4 (64bit)

28.1.5 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.

28.1.6 Can Applications Using TLS Connections Be Audited?

No. Applications using TLS are encrypted.

28.1.7 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 or advanced edition.

  For more information, see **Table 28-3**.
- Back up audit logs.

Table 28-3 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.
Advanced	30	- CPU: 16 vCPUs - Memory: 64 GB - Disk: 2 TB	- Peak QPS: 30,000 queries/second - Database load rate: 10.80 million statements/hour - Stores 1.5 billion online SQL statements. - Stores 60 billion archived SQL statements.

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.

28.1.8 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.

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

Yes. One alarm message corresponds to one email notification.

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

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

28.1.11 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:

28.2 Agent

28.2.1 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

28.2.2 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 28-4** provides more details.

Table 28-4 Supported Linux OS versions

System Name	System version
CentOS	● CentOS 7.0 (64bit) ● CentOS 7.1 (64bit) ● CentOS 7.2 (64bit) ● CentOS 7.3 (64bit) ● CentOS 7.4 (64bit) ● CentOS 7.5 (64bit) ● CentOS 7.6 (64bit) ● CentOS 7.8 (64bit) ● CentOS 7.9 (64bit) ● CentOS 8.0 (64bit) ● CentOS 8.1 (64bit) ● CentOS 8.2 (64bit)
Debian	● Debian 7.5.0 (64bit) ● Debian 8.2.0 (64bit) ● Debian 8.8.0 (64bit) ● Debian 9.0.0 (64bit) ● Debian 10.0.0 (64bit)
Fedora	● Fedora 24 (64bit) ● Fedora 25 (64bit)
SUSE	● SUSE 11 SP4 (64bit) ● SUSE 12 SP1 (64bit) ● SUSE 12 SP2 (64bit)
Ubuntu	● Ubuntu 14.04 (64bit) ● Ubuntu 16.04 (64bit) ● Ubuntu 18.04 (64bit) ● Ubuntu 20.04 (64-bit)
EulerOS	● Euler 2.2 (64bit) ● Euler 2.3 (64bit)
Oracle Linux	● Oracle Linux 6.9 (64bit) ● Oracle Linux 7.4 (64bit)

28.2.3 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

28.2.4 (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

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

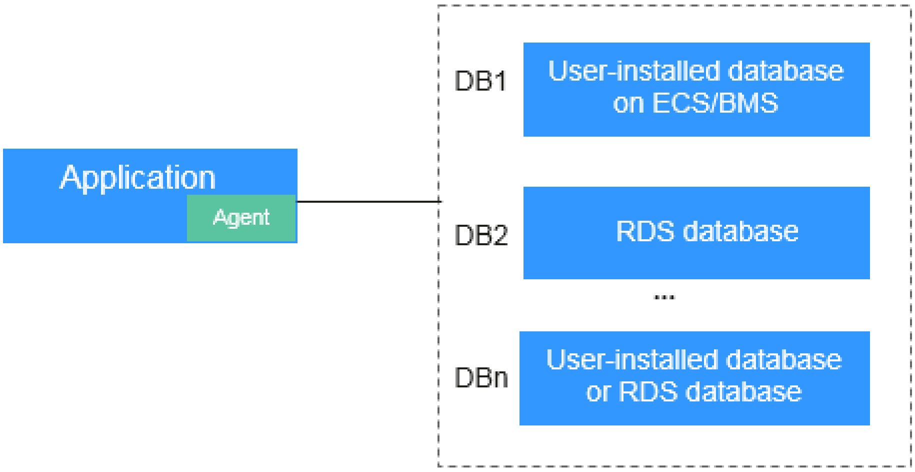
The path for saving agent logs is **/opt/dbss_audit_agent/log/audit_agent.log**.

28.2.6 When Should I Select an Existing Agent?

Do this if an application is connected to multiple databases, as shown in **Figure 28-1**, 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 28-2**.

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

Figure 28-1 An application connected to multiple databases

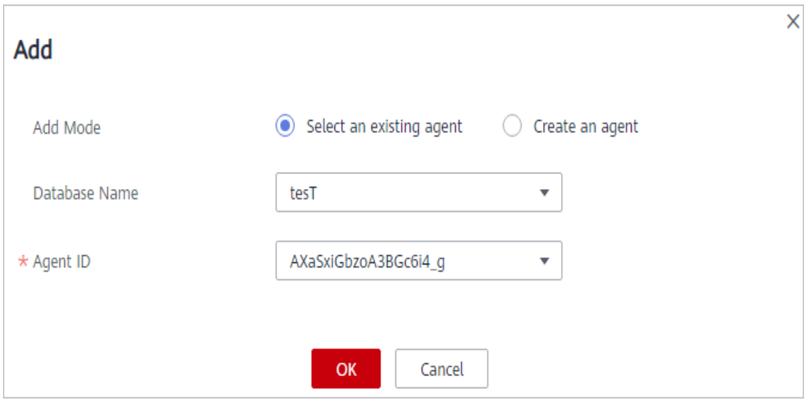

Application
Agent
DB1
User-installed database on ECS/BMS
DB2
RDS database
...
DBn
User-installed database or RDS database

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 28-2 Selecting an existing agent



Add

Add Mode ● Select an existing agent ○ Create an agent

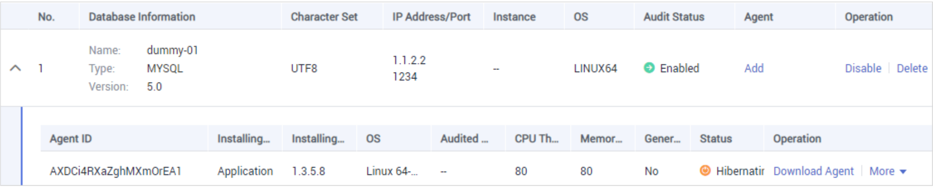
Database Name: tesT

* Agent ID: AXaSxiGbzoA3BGc6i4_g

28.2.7 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 28-3**.

Figure 28-3 Successfully adding an agent



No.	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
1	Name: dummy-01 Type: MYSQL Version: 5.0	UTF8	1.1.2.2 1234	--	LINUX64	Enabled	Add	Disable | Delete

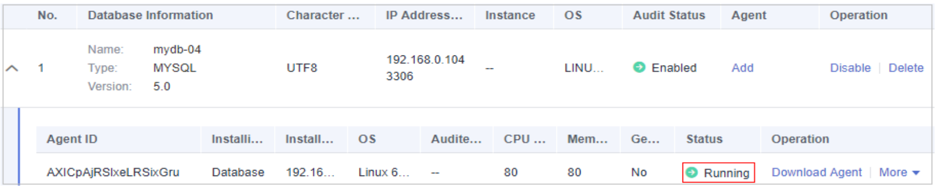
Agent ID	Installing...	Installing...	OS	Audited ...	CPU Th...	Memor...	Gener...	Status	Operation
AXDCi4RXaZghMXmOrEA1	Application	1.3.5.8	Linux 64-...	--	80	80	No	Hibernatir	Download Agent | More

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 28-4**, it indicates that the agent is running properly.

Figure 28-4 Agent running properly



	No.	Database Information	Character ...	IP Address...	Instance	OS	Audit Status	Agent	Operation
^	1	Name: mydb-04 Type: MYSQL Version: 5.0	UTF8	192.168.0.104 3306	--	LINU...	Enabled	Add	Disable | Delete

Agent ID	Installi...	Install...	OS	Audite...	CPU ...	Mem...	Ge...	Status	Operation
AXICpAjRSIxeLRSixGru	Database	192.16...	Linux 6...	--	80	80	No	Running	Download Agent | More ▾

- 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?**

28.2.8 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 28-5**.

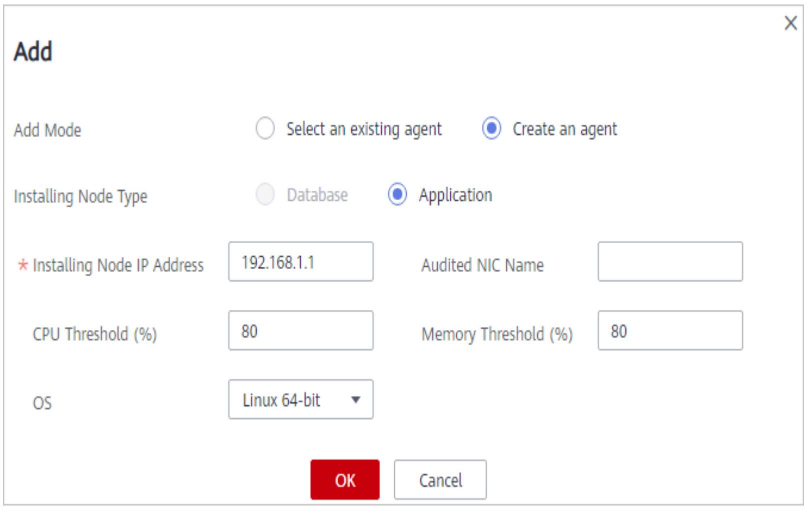
Table 28-5 Nodes to install agents

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**.
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 **Figure 28-5**. ● 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 28-5 Adding an agent to an application



Add

Add Mode ○ Select an existing agent ● Create an agent

Installing Node Type ○ Database ● Application

* Installing Node IP Address 192.168.1.1

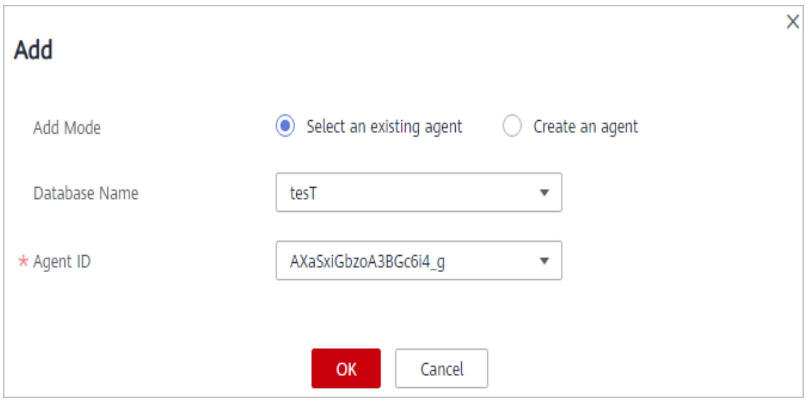
Audited NIC Name

CPU Threshold (%) 80

Memory Threshold (%) 80

OS Linux 64-bit

Figure 28-6 Selecting an existing agent



Add

Add Mode ● Select an existing agent ○ Create an agent

Database Name tesT

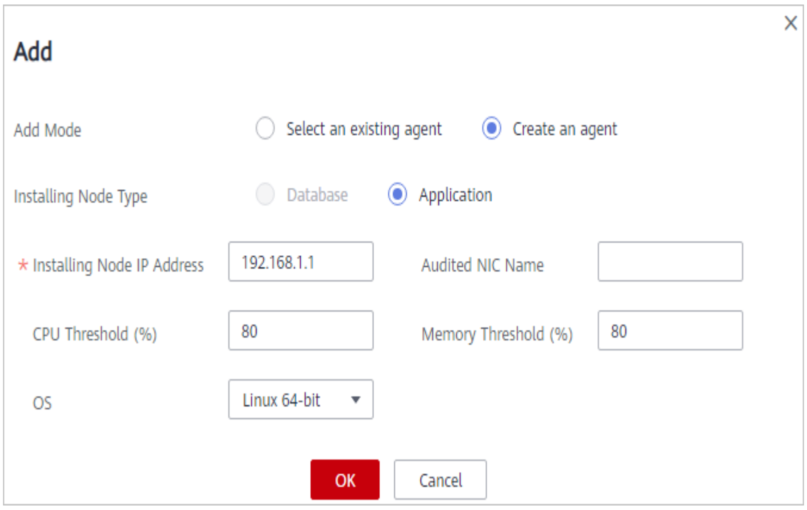
* Agent ID AXaSxiGbzoA3BGc6i4_g

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

Figure 28-7 Adding an agent to an application



Add

Add Mode: ○ Select an existing agent ● Create an agent

Installing Node Type: ○ Database ● Application

* Installing Node IP Address: 192.168.1.1

Audited NIC Name:

CPU Threshold (%): 80

Memory Threshold (%): 80

OS: Linux 64-bit

NOTICE

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

28.2.9 How Do I Download a Database Audit Agent?

Download and then install the agent on the database or application, as required by 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 ^ in the lower part of the database list to expand the agent details. Locate the target agent and click **Download Agent** in the **Operation** column. to download an agent installation package.

Download the agent installation package suitable for your OS.

- Linux OS

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

- Windows OS

  Download the agent whose OS is **WINDOWS64**.

----End

28.2.10 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

28.2.11 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.

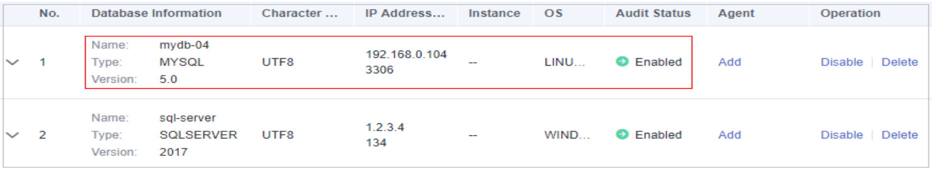
Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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, as shown in **Figure 28-8**.

Figure 28-8 Viewing the information about the database to be audited

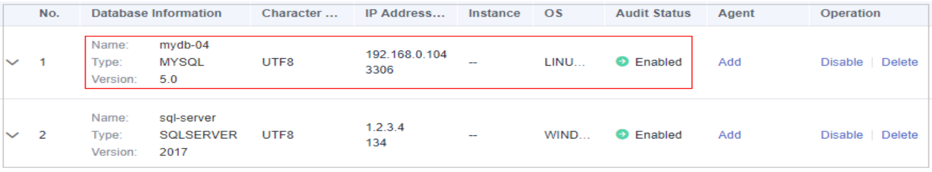


	No.	Database Information	Character ...	IP Address...	Instance	OS	Audit Status	Agent	Operation
﹀	1	Name: mydb-04 Type: MYSQL Version: 5.0	UTF8	192.168.0.104 3306	--	LINU...	● Enabled	Add	Disable | Delete
﹀	2	Name: sql-server Type: SQLSERVER Version: 2017	UTF8	1.2.3.4 134	--	WIND...	● Enabled	Add	Disable | Delete

- 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, as shown in **Figure 28-9**.

Figure 28-9 Checking the database audit status



	No.	Database Information	Character ...	IP Address...	Instance	OS	Audit Status	Agent	Operation
﹀	1	Name: mydb-04 Type: MYSQL Version: 5.0	UTF8	192.168.0.104 3306	--	LINU...	● Enabled	Add	Disable | Delete
﹀	2	Name: sql-server Type: SQLSERVER Version: 2017	UTF8	1.2.3.4 134	--	WIND...	● Enabled	Add	Disable | Delete

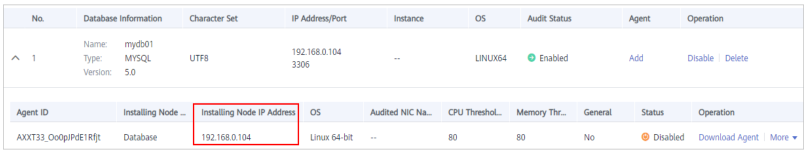
- If **Audit Status** is **Enabled**, go to **Checking the Security Group Rules of the Database Audit Instance**.
- If **Audit Status** is **Disabled**, click **Enable** to enable the database audit function.
  - If the fault is rectified, no further operation is required.
  - If the problem persists, 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**, as shown in **Figure 28-10**.

Figure 28-10 Recording the IP address of the installing node



No.	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
1	Name: mydb01 Type: MYSQL Version: 5.0	UTF8	192.168.0.104 3306	--	LINUX64	● Enabled	Add	Disable | Delete

Agent ID	Installing Node ...	Installing Node IP Address	OS	Audited NIC Na...	CPU Threshol...	Memory Thr...	General	Status	Operation
AXXT33_Oo0pJPdE1Rfjt	Database	192.168.0.104	Linux 64-bit	--	80	80	No	● Disabled	Download Agent | More ▾

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**.

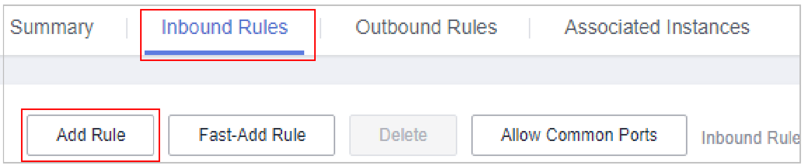
Check whether TCP (port number **8000**) and UDP protocols (port number from **7000** to **7100**) are configured in the inbound rules of the security group for the IP address of the installing node in **Step 1**.

- 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.

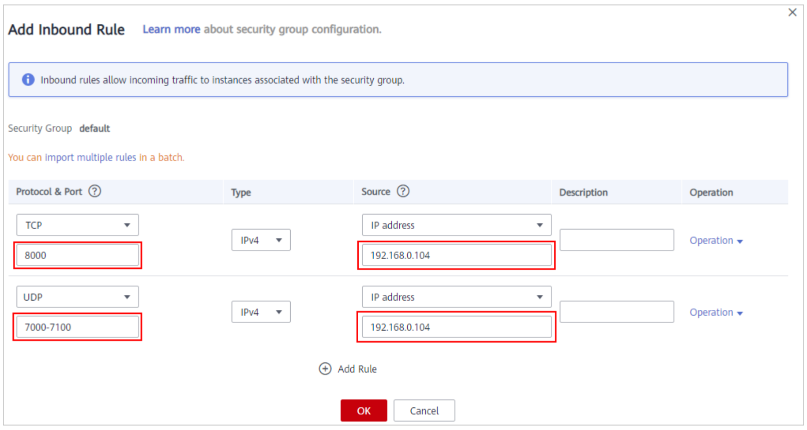
1. Click **Add Rule**, as shown in **Figure 28-11**.

Figure 28-11 Adding rules



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 in **Step 1**. See **Figure 28-12**.

Figure 28-12 Add Inbound Rule dialog box



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group default

You can import multiple rules in a batch.

Protocol & Port	Type	Source	Description	Operation
TCP 8000	IPv4	IP address 192.168.0.104		Operation
UDP 7000-7100	IPv4	IP address 192.168.0.104		Operation

3. 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.

28.3 Operations

28.3.1 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

28.3.2 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.

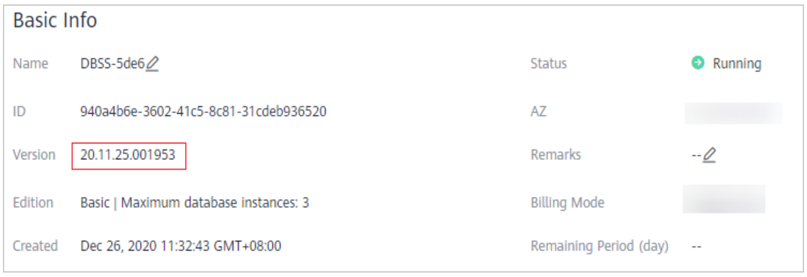
Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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, as shown in **Figure 28-13**.

Figure 28-13 Viewing the instance version



Basic Info

Name	DBSS-5de6	Status	Running
ID	940a4b6e-3602-41c5-8c81-31cdeb936520	AZ	[redacted]
Version	20.11.25.001953	Remarks	--
Edition	Basic | Maximum database instances: 3	Billing Mode	[redacted]
Created	Dec 26, 2020 11:32:43 GMT+08:00	Remaining Period (day)	--

----End

28.3.3 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.

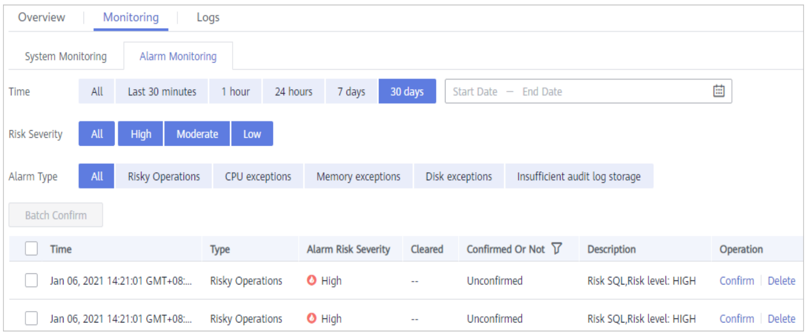
Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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, as shown in **Figure 28-14**.

Figure 28-14 Viewing the alarms



□	Time	Type	Alarm Risk Severity	Cleared	Confirmed Or Not	Description	Operation
□	Jan 06, 2021 14:21:01 GMT+08:...	Risky Operations	High	--	Unconfirmed	Risk SQL,Risk level: HIGH	Confirm | Delete
□	Jan 06, 2021 14:21:01 GMT+08:...	Risky Operations	High	--	Unconfirmed	Risk SQL,Risk level: HIGH	Confirm | Delete

To query specified alarms, perform the following steps:

- Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days** for **Time**, and click 🔍 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

28.3.4 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.

28.4 Troubleshooting

28.4.1 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

28.4.2 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.

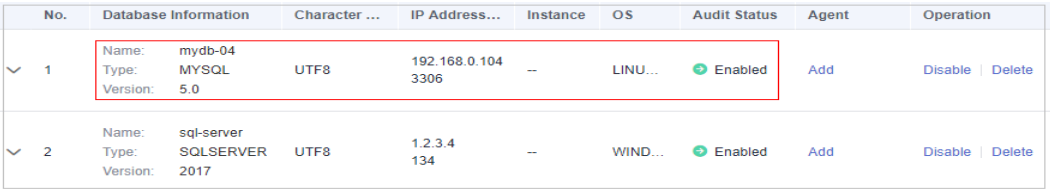
Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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 View the database information, as shown in **Figure 28-15**.

Figure 28-15 Viewing the information about the database to be audited



	No.	Database Information	Character ...	IP Address...	Instance	OS	Audit Status	Agent	Operation
⌄	1	Name: mydb-04 Type: MYSQL Version: 5.0	UTF8	192.168.0.104 3306	--	LINU...	Enabled	Add	Disable | Delete
⌄	2	Name: sql-server Type: SQLSERVER Version: 2017	UTF8	1.2.3.4 134	--	WIND...	Enabled	Add	Disable | Delete

Step 6 Check whether the database information is correct.

- If the database information is correct, go to **Step 7**.
- 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 7**.

Step 7 Check whether the database audit function is enabled.

- If **Audit Status** is **Enabled**, go to **Checking Audited Database Settings**.

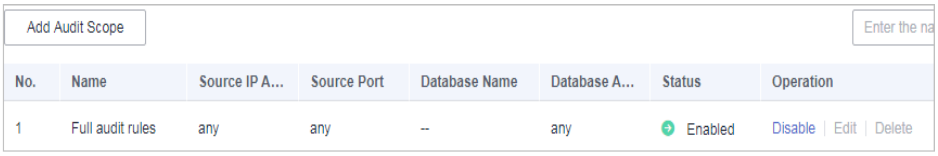
- If **Audit Status** is **Disabled**, click **Enable** to enable the database audit function.
  - If the fault is rectified, no further operation is required.
  - If the problem persists, go to **Checking Audited Database Settings**.

----End

Checking Audited Database Settings

In the navigation tree on the left, choose **Database Audit** > **Rules**. The **Audit Scope** page is displayed. See **Figure 28-16**.

Figure 28-16 Audit scope



No.	Name	Source IP A...	Source Port	Database Name	Database A...	Status	Operation
1	Full audit rules	any	any	--	any	● Enabled	Disable | Edit | Delete

- 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

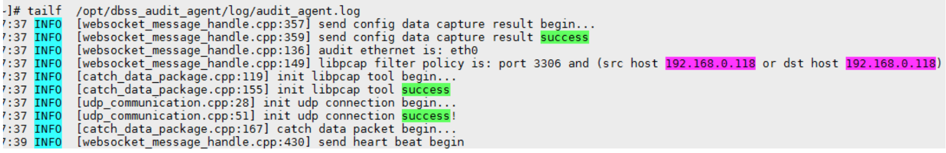
- If the fault is rectified, no further operation is required.
- If the problem persists, go to **Step 4**.

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**.

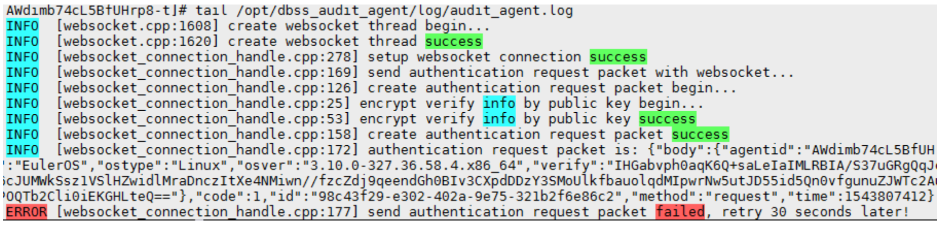
Figure 28-17 Normal communication



```
-]# tailf  /opt/dbss_audit_agent/log/audit_agent.log
':37 INFO  [websocket_message_handle.cpp:357] send config data capture result begin...
':37 INFO  [websocket_message_handle.cpp:359] send config data capture result success
':37 INFO  [websocket_message_handle.cpp:136] audit ethernet is: eth0
':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)
':37 INFO  [catch_data_package.cpp:119] init libpcap tool begin...
':37 INFO  [catch_data_package.cpp:155] init libpcap tool success
':37 INFO  [udp_communication.cpp:28] init udp connection begin...
':37 INFO  [udp_communication.cpp:51] init udp connection success!
':37 INFO  [catch_data_package.cpp:167] catch data packet begin...
':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 28-18 Communication error



```
AWdımb74cL5BfUHrp8-t]# taıl /opt/dbss_audıt_agent/log/audıt_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
;cJUMWkSsz1VSlHZwidlMraDnczItXe4NMiwn//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.

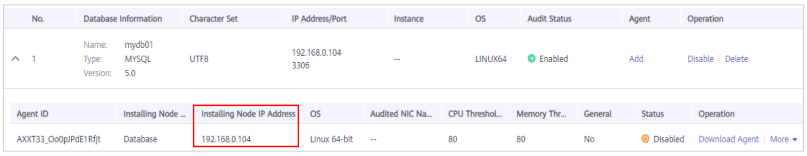
Step 2 In the navigation tree on the left, choose **Database Audit** > **Databases**. The **Databases** page is displayed.

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**. See **Figure 28-19**.

Figure 28-19 Installing node IP address



No.	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
^ 1	Name: mydb01 Type: MYSQL Version: 5.0	UTF8	192.168.0.104 3306	--	LINUX64	● Enabled	Add	Disable | Delete

Agent ID	Installing Node ...	Installing Node IP Address	OS	Audited NIC Na...	CPU Threshol...	Memory Thr...	General	Status	Operation
AXXT33_Oo0pJPdE1Rfjt	Database	192.168.0.104	Linux 64-bit	--	80	80	No	● Disabled	Download Agent | More ▾

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.

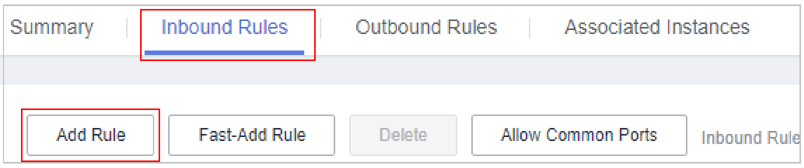
Check whether TCP (port number **8000**) and UDP protocols (port number from **7000** to **7100**) are configured in the inbound rules of the security group for the IP address of the installing node in **Step 4**.

- 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.

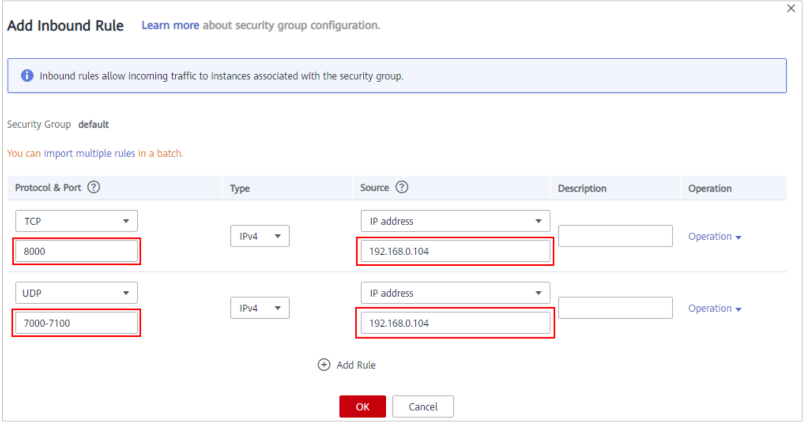
1. On the **Inbound Rules** tab, click **Add Rule**. See **Figure 28-20**.

Figure 28-20 Adding rules



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 in **Figure 28-19**. See **Figure 28-21**.

Figure 28-21 Adding an inbound rule



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group default

You can import multiple rules in a batch.

Protocol & Port	Type	Source	Description	Operation
TCP 8000	IPv4	IP address 192.168.0.104		Operation
UDP 7000-7100	IPv4	IP address 192.168.0.104		Operation

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.

28.5 Logs

28.5.1 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?**

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

The operation logs of database audit are permanently saved.

28.5.3 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.

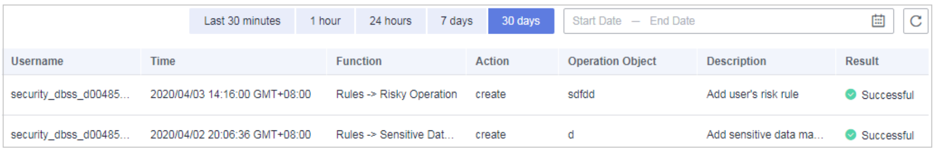
Step 3 In the navigation tree on the left, choose **Instances**.

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, as shown in **Figure 28-22**. For details about related parameters, see **Table 28-6**.

Figure 28-22 Viewing operation logs



Username	Time	Function	Action	Operation Object	Description	Result
security_dbss_d00485...	2020/04/03 14:16:00 GMT+08:00	Rules -> Risky Operation	create	sdfdd	Add user's risk rule	✓ Successful
security_dbss_d00485...	2020/04/02 20:06:36 GMT+08:00	Rules -> Sensitive Dat...	create	d	Add sensitive data ma...	✓ Successful

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 28-6 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

28.5.4 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.

28.5.5 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.

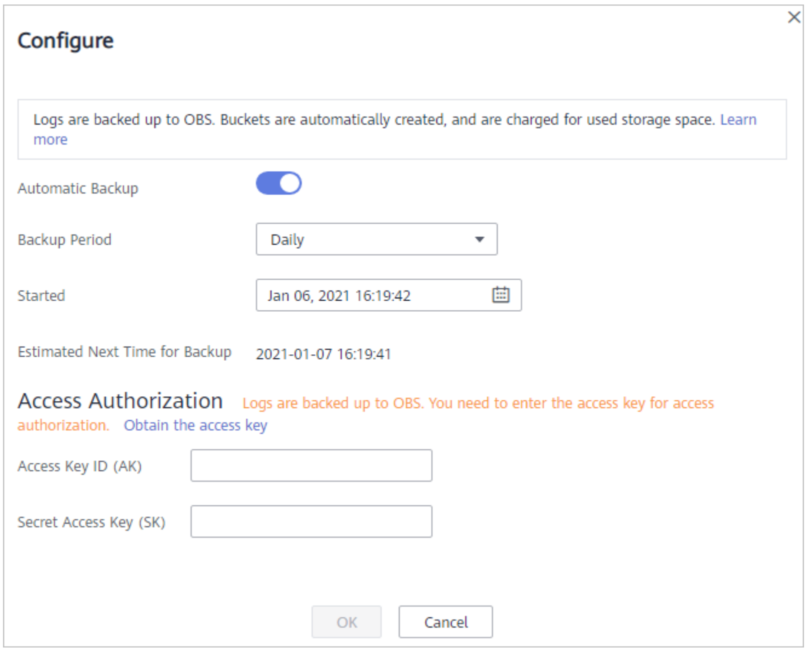
Step 2 Select a region, click ☰, and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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, as shown in Figure 28-23. For details about related parameters, see Table 28-7.

Figure 28-23 Configure Automatic Backup dialog box



Configure

Logs are backed up to OBS. Buckets are automatically created, and are charged for used storage space. Learn more

Automatic Backup: ●

Backup Period: Daily

Started: Jan 06, 2021 16:19:42

Estimated Next Time for Backup: 2021-01-07 16:19:41

Access Authorization: Logs are backed up to OBS. You need to enter the access key for access authorization. Obtain the access key

Access Key ID (AK):

Secret Access Key (SK):

Table 28-7 Parameters

Parameter	Description	Example Value
Automatic Backup	Status of automatic backup	
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
Estimated Next Time for Backup	Time when the next automatic backup starts	2020/01/15 20:21:29
Access Key ID(AK)	Access key (AK)	-
Secret Access Key(SK)	Secret access key (SK)	-

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

A Change History

Released On	Description
2023-06-30	This is the first official release.