Database Security Service (DBSS)

User Guide

Issue	01
Date	2024-12-11

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

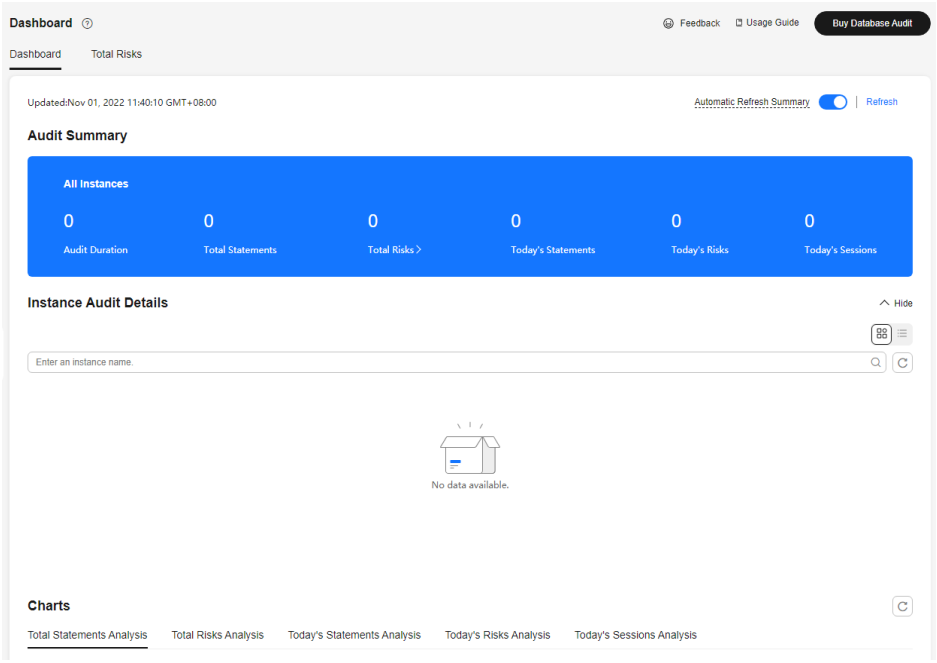
1 Overview

On the **Dashboard** page, you can enable regular update for the audit information, view the audit information of each instance, and view the total number of SQLs, risks, and sessions of all instances.

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.

Figure 1-1 Accessing the Dashboard page



Step 3 Toggle on the **Summarized information is refreshed regularly** switch in the upper right corner.

NOTE

After this function is enabled, the system updates the audit information of all instances every hour based on the preset rules.

----End

My Audit Information

Displays the scanning and detection statistics of all instances.

Table 1-1 Parameters

Parameter	Description
Audit duration	Total duration used for auditing all instances.
Total number of sql	Number of SQLs used for auditing all instances.
Total risk	Number of risks detected from all instances.
Today's sql	Number of SQLs used for auditing instances today.
Today's risk	Number of risks detected from the audited instances today.
Today's session	Number of sessions established for auditing instances today.

Single Instance Information

You can check the audit statistics of each instance. By default, 10 records are displayed on each page.

Data Analysis Chart Display

You can check the audit information about all instances by total number of SQLs, total number of risks, today's SQL, today's risks, and today's sessions.

Switch tabs to view the analysis charts as required.

Top 5 Total Number of SQL

You can check the five instances that have used the highest number of SQLs.

Figure 1-2 Top 5 total number of sql

Overall Risk Analysis

You can view the statistics of **High Risk Hits**, **Medium Risk Hits**, and **Low Risk Hits** among all instances. The three databases with the most risk hits are displayed in descending order in the right area.

NOTE

You can click  in the upper right corner to select a time period and view the overall risks in that period.

Overall Risk Rule Analysis

You can view the statistics on the number of risk rule hits. The five rules with most risk hits are displayed in descending order in the right area.

Risk Analysis by Level

You can view the analysis report from the following three aspects:

- **Risk Level**: Select **High Risk Analysis**, **Medium Risk Analysis**, or **Low Risk Analysis**.
- **Risk Rules**: Select a risk rule.
- **Database Statistics**: Select a database to view the number of risk hits.

2 Enabling and Using Database Audit (by Installing Agents)

2.1 Process Overview

This section describes how to quickly enable database audit.

Background

Database audit supports auditing user-installed databases on ECS/BMS as well as RDS databases on Huawei Cloud.

NOTICE

- Database audit cannot be used across regions. The database to be audited and the database audit instance you purchased must be in the same region.
- If SSL is enabled for a database, the database cannot be audited. To use database audit, disable SSL first. For details, see **How Do I Disable SSL for a Database?**
- For details about audit data storage, see **How Long Is the Audit Data of Database Audit Stored by Default?**

Create a database audit instance, connect the instance with the target database, and enable database audit.

Auditing Databases Without Agents

Databases of some types and versions can be audited without using agents, as shown in **Table 2-1**.

Table 2-1 Agent-free relational databases

Type	Supported Edition
MySQL	All editions are supported by default.
PostgreSQL **NOTICE** If the size of an SQL statement exceeds 4 KB, the SQL statement will be truncated during auditing. As a result, the SQL statement is incomplete.	All editions are supported by default.
SQLServer	• 2008 • 2012 • 2014 • 2016 • 2017
GaussDB(for MySQL)	Mysql8.0
DWS	• 1.5 • 8.1
MariaDB	10.2

NOTE

- DBSS without agents is easy to configure and use, but the following functions are not supported:
  - Successful and failed login sessions cannot be counted.
  - The port number of the client for accessing the database cannot be obtained.
- GaussDB(DWS) has the permission control policy for the log audit function. Only Huawei Cloud accounts and users with the **Security Administrator** permission can enable or disable the DWS database audit function.

Figure 2-1 Agent-free auditing process

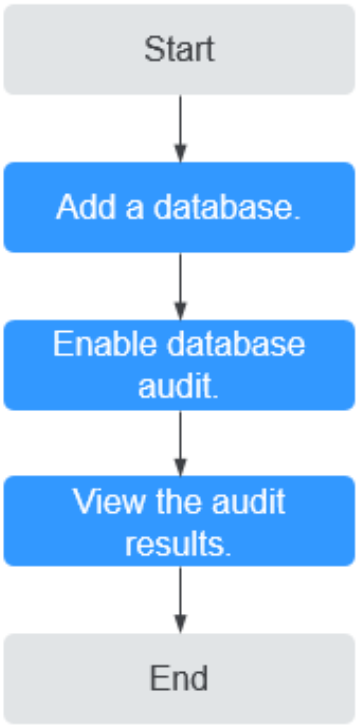


Table 2-2 Procedure for quickly configuring database audit

Step	Configuration	Description
1	**Adding a Database**	Purchase database audit. Add a database to the database audit instance and enable audit for the database. Apply for database audit. Add a database to the database audit instance and enable audit for the database.
2	**Enabling Database Audit**	Enable database audit and connect the added database to the database audit instance.
3	**Viewing the Audit Results**	By default, database audit complies with a **full audit rule**, which is used to audit all databases that are connected to the database audit instance. You can view the audit result on the database audit page. **NOTICE** You can set database audit rules as required. For details, see **Adding Audit Scope**.

Auditing Databases Using Agents

For a database whose type and version are not listed in **Table 2-1**, you need to install an agent to enable the database audit.

Figure 2-2 Procedure for quickly configuring database audit

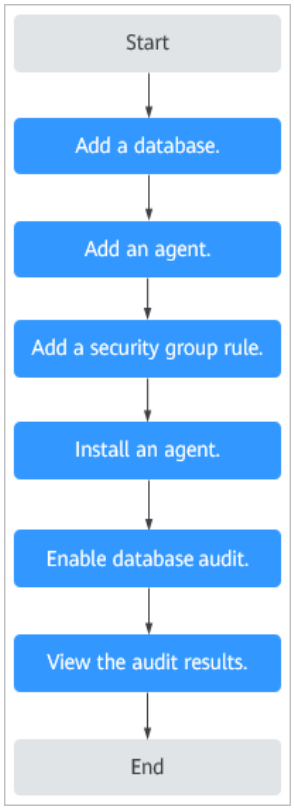


Table 2-3 Procedure for quickly configuring database audit

Step	Configuration	Description
1	**Adding a Database**	Purchase database audit. Add a database to the database audit instance and enable audit for the database.
2	**Adding an Agent**	Select an agent add mode. Database audit supports auditing databases built on ECS, BMS, and RDS on Huawei Cloud. Select an agent add mode based on your database deployed on Huawei Cloud.
3	**Adding Security Group Rules**	Configure TCP (port 8000) and UDP (ports 7000 to 7100) in the security group inbound rule of the database audit instance to allow the agent to communicate with the audit instance.

Step	Configuration	Description
4	**Installing an Agent (Linux OS)**	Download and then install the agent on the database or application based on the add mode you chose.
5	**Enabling Database Audit**	Enable database audit and connect the added database to the database audit instance.
6	**Viewing the Audit Results**	By default, database audit complies with a **full audit rule**, which is used to audit all databases that are connected to the database audit instance. You can view the audit result on the database audit page. **NOTICE** You can set database audit rules as required. For details, see **Adding Audit Scope**.

Helpful Links

- Choose the way to add an agent and the node to install it. For details, see **How Do I Install a Database Audit Agent?**
- If the audit function is unavailable, rectify the fault by following the instructions provided in **Database Audit Is Unavailable**.

Verifying the Result

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

2.2 Purchasing Database Audit

Before using the database audit function, you need to purchase database audit. Database audit charges yearly or monthly.

Constraints

- DBSS cannot be used across regions. The database to be audited and the database audit instance you purchased must be in the same region.
- Ensure the VPC of the database audit instance is the same as that of the node (application side or database side) where you plan to install the database audit agent. Otherwise, the instance will be unable to connect to the agent or perform audit.

  For details about how to choose the node, see **How Do I Determine Where to Install an Agent?**

Impact on the System

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

Prerequisites

The instance account has related permissions.

NOTICE

Ensure that the **DBSS System Administrator**, **VPC Administrator**, **ECS Administrator**, and **BSS Administrator** policies have been configured for the account used for purchasing instances.

- **VPC Administrator**: Users with this set of permissions can perform all execution permission for VPC. It is a project-level role, which must be assigned in the same project.
- **BSS Administrator**: Users with this set of permissions can perform any operation on menu items on pages **My Account**, **Billing Center**, and **Resource Center**. It is a project-level role, which must be assigned in the same project.
- **ECS Administrator**: Users with this set of permissions can perform any operations on an ECS. It is a project-level role, which must be assigned in the same project.

Procedure

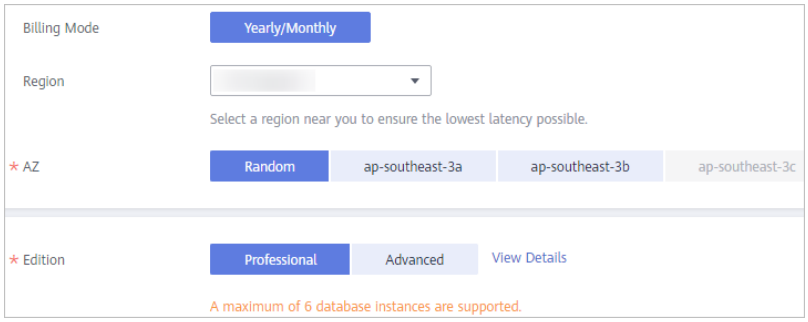
Step 1 Log in to the management console.

Step 2 Click ☰ and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

Step 4 Select a region, a project, an AZ, and an edition.

Figure 2-3 Selecting an AZ and an edition



Select an enterprise project. The DBSS you purchase will be put under this project. Billing and permissions management are performed based on enterprise projects.

Table 2-4 describes the database audit editions.

Table 2-4 Database audit editions

Edition	Maximum Databases	System Resource	Performance
Professional	6	• CPU: 8 vCPUs • Memory: 32 GB • Hard disk: 1,084 GB	• Peak QPS: 6,000 queries/second • Database load rate: 7.2 million statements/hour • Stores 600 million online SQL statements. • Stores 10 billion archived SQL statements.
Advanced	30	• CPU: 16 vCPUs • Memory: 64 GB • Hard disk: 2,108 GB	• Peak QPS: 30,000 queries/second • Database load rate: 10.8 million records/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 purchase a new one.
- The cloud native edition can be purchased only on the RDS console.
- The table above lists the system resources consumed by a database audit instance. Ensure your system has the required configurations before purchasing database audit instances.
- Online SQL statements are counted based on the assumption that the capacity of an SQL statement is 1 KB.

Step 5 Set database audit parameters, as shown in **Figure 2-4**. For details about related parameters, see **Table 2-5**.

Figure 2-4 Setting database audit parameters

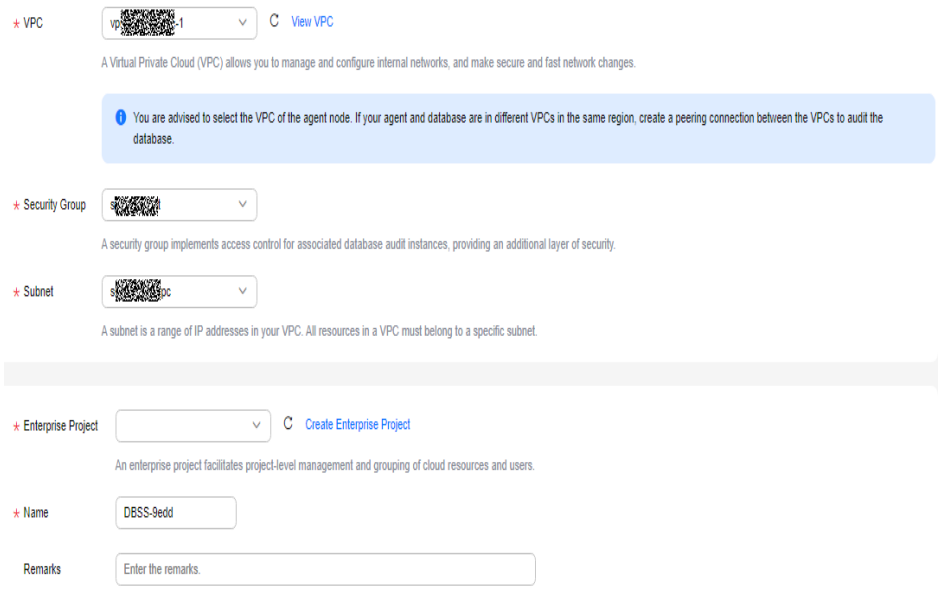
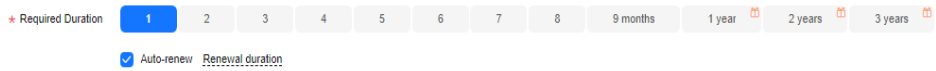


Table 2-5 Database audit parameters

Parameter	Description
VPC	You can select an existing VPC, or click **View VPC** to create one on the VPC console. **NOTE** • Select the VPC of the node (application or database side) where you plan to install the agent. For more information, see **How Do I Determine Where to Install an Agent?** • To change the VPC of a DBSS instance, unsubscribe from it and purchase a new one. For more information about VPC, see *Virtual Private Cloud User Guide*.
Security Group	You can select an existing security group in the region or create a security group on the VPC console. 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*.
Subnet	You can select a subnet configured in the VPC or create a subnet on the VPC console.
Name	Instance name

Step 6 Set **Required Duration**. See **Figure 2-5**.

Figure 2-5 Setting the required duration



After you select **Auto-renew**, the system automatically renews the instance upon expiry if your account balance is sufficient. You can continue to use the instance. **Table 2-6** describes the auto-renewal period.

Table 2-6 Auto-renewal period description

Required Duration	Auto-renewal Period
1/2/3/4/5/6/7/8/9 months	1 month
1 year	1 year

Step 7 (Optional) Add tags to the database audit instance. If you have configured tag policies for DBSS, you need to add tags to your DBSS instances based on the tag policies. If a tag does not comply with the policies, DBSS instance may fail to be created. Contact your organization administrator to learn more about tag policies.

Step 8 Confirm the configuration and click **Next**.

For any doubt about the pricing, click **Pricing details** to understand more.

Step 9 On the **Details** page, read the *Database Audit of Database Security Service Disclaimer*, select **I have read and agree to the Database Audit of Database Security Service Disclaimer**, and click **Submit**.

Step 10 On the displayed page, select a payment method.

Step 11 After you pay for your order, you can view the creation status of your instances.

----End

Follow-Up Procedure

- If the **Status** of the instance is **Running**, you have successfully purchased the database audit instance.
- If the instance status is **Creation failed**, you will be automatically refunded. You can click **More** in the **Operation** column and view details in the **Failure Details** dialog box.

2.3 Step 1: Add a Database

Database audit supports databases built on ECS, BMS, and RDS on Huawei Cloud. After purchasing a database audit instance, you need to add the database to be audited to the instance.

For details about the types and versions of databases that can be audited by database audit, see **Supported Database Types and Versions**.

Prerequisites

You have purchased 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 & Compliance** > **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 displayed dialog box, configure the database information.

Table 2-7 Parameters

Parameter	Description	Example Value
Database Type	Type of the database to be added. You can select **RDS database** or **Self-built database**. **NOTE** If you select **RDS database**, you can directly select the databases that you want to add to DBSS.	RDS database
Name	Custom name of the database to be added	test1
IP Address	IP address of the database to be added. The IP address must be an internal IP address in IPv4 or IPv6 format.	IPv4: 192.168.1.1 IPv6: fe80:0000:0000:0000:0000:0000:0000:0000

Parameter	Description	Example Value
Type	Supported database type. The options are as follows: • MYSQL • ORACLE • PostgreSQL • SQL Service • DWS • GaussDB(for MYSQL) • GaussDB • DAMENG • KINGBASE • MongoDB • Hbase • SHENTONG • GBase 8a • GBase XDM Cluster • Greenplum • HighGo • MariaDB • Hive • DDS • GBase 8s • TDSQL **NOTE** • If **ORACLE** is selected, to make the audit settings take effect, restart the applications to be audited and log in to the database again.	MYSQL
Port	Port number of the database to be added	3306

Parameter	Description	Example Value
Version	Supported database versions • When **Type** is set to **MYSQL**, the following versions are available: – 5.0, 5.1, 5.5, 5.6, 5.7 – 8.0 (8.0.11 and earlier) – 8.0.30 – 8.0.35 – 8.1.0 – 8.2.0 – If **RDS database** is selected, a list of database instances will be displayed for you to choose from. You do not need to install the agent. • 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 – 14.0 • 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:	5.0

Parameter	Description	Example Value
	– 1.5 – 8.1 • When **Type** is set to **GaussDB(for MySQL)**, the following versions are available: – When **Database Type** is set to **Self-built database**, you can select the **MySQL 8.0** version. – If **RDS database** is selected, a list of database instances will be displayed for you to choose from. You do not need to install the agent. • When **Type** is set to **GaussDB**, the following version is available: – 1.4 Enterprise Edition – 1.3 Enterprise Edition – 2.8 Enterprise Edition – 3.223 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: – V8 • When **Type** is set to **Hbase**, the following versions are available: – 1.3.1 – 2.2.3 • When **Type** is set to **SHENTONG**, the following version is available: – V7.0 • When **Type** is set to **GBase 8a**, the following version is available: – v8.5 • When **Type** is set to **GBase 8s**, the following version is available: – v8.8 • When **Type** is set to **Greenplum**, the following version is available: – v6.0 • When **Type** is set to **HighGo**, the following version is available:	

Parameter	Description	Example Value
	– v6.0 • When **Type** is set to **MongoDB**, the following version is available: – v5.0 • When **Type** is set to **MariaDB**, the following version is available: – 10.6 • When **Type** is set to **Hive**, the following versions are available: – 1.2.2 – 2.3.9 – 3.1.2 – 3.1.3 • When **Type** is set to **TDSQL**, the following version is available: – 10.3.17.3.0	
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

Step 7 Click **OK**. A database whose **Audit Status** is **Disabled** is added to the database list.

NOTE

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

----End

2.4 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)
- GaussDB(DWS): 8.2.0.100 or later

Prerequisites

- You have purchased 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 2-6** and **Figure 2-7**.

Figure 2-6 One application connecting to multiple databases built on ECS/BMS

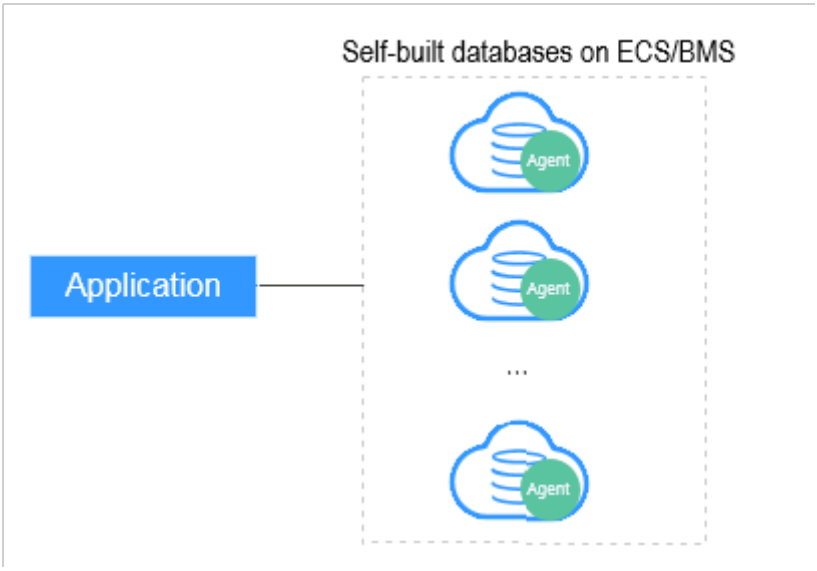
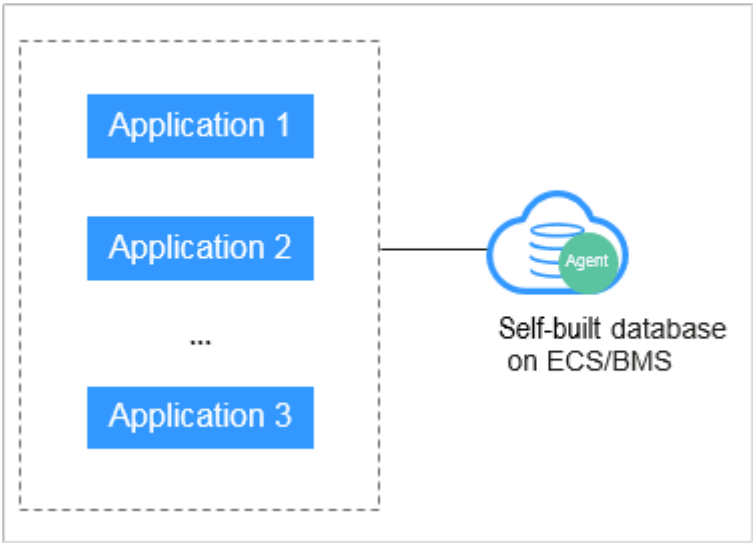


Figure 2-7 Multiple applications connecting to one database built on ECS/BMS



- Deploy DBSS for RDS databases. For details, see **Figure 2-8** and **Figure 2-9**.

Figure 2-8 One application connecting to multiple RDS databases

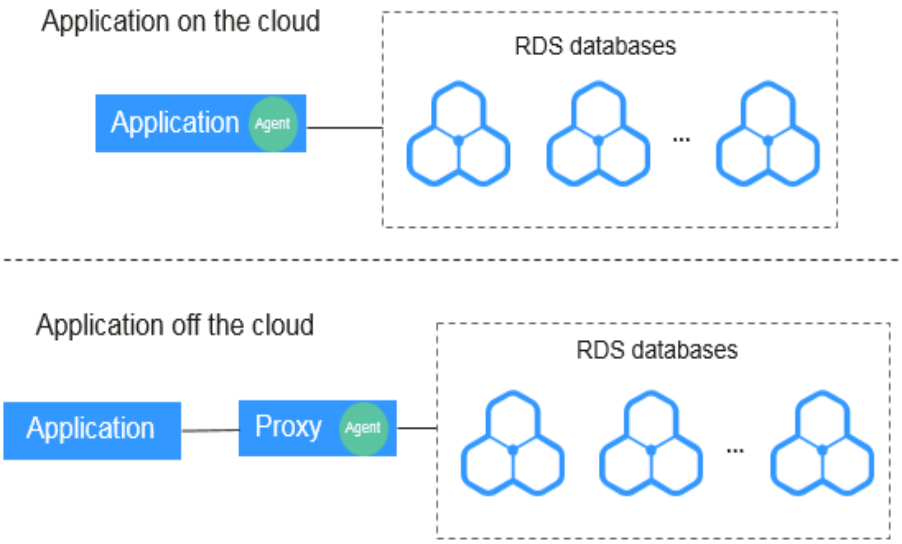


Figure 2-9 Multiple applications connecting to one RDS database

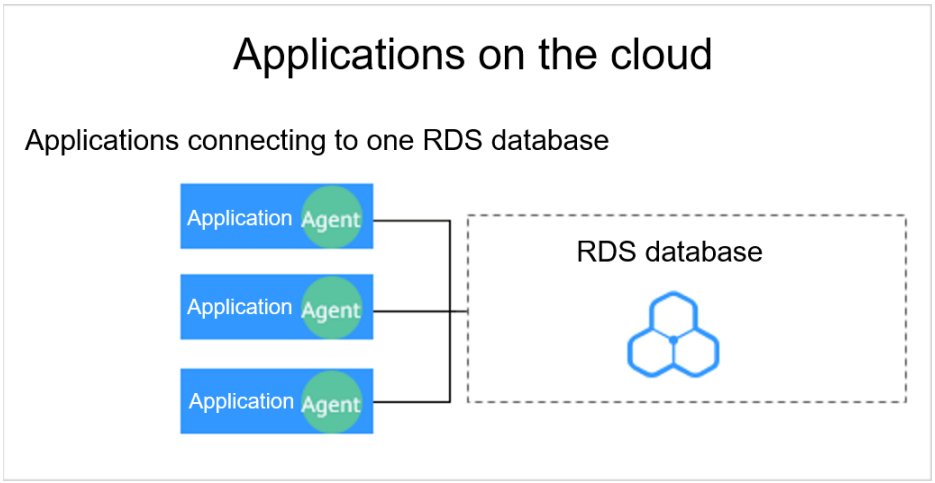


Table 2-8 provides more details.

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 2-8 Agent locations

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

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

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 **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 2-10**. For details about related parameters, see **Table 2-9**.

Figure 2-10 Adding an agent to a database

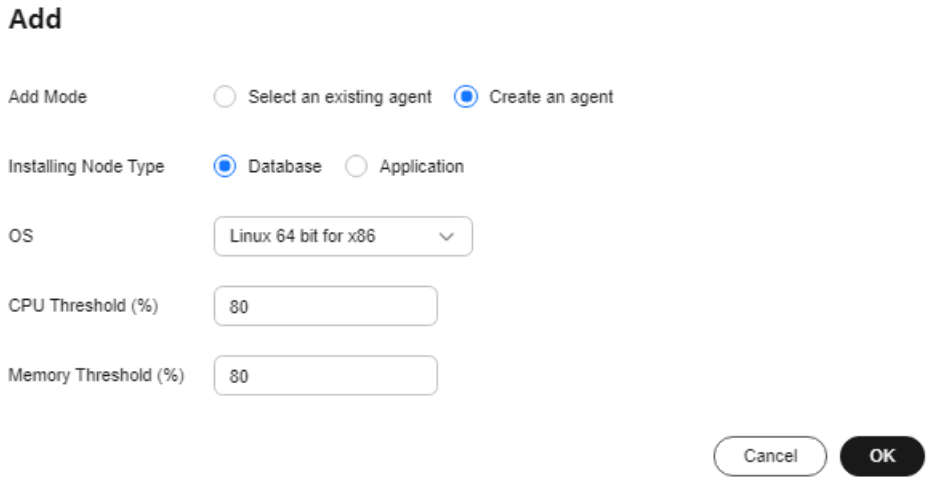


Table 2-9 Parameters for adding an agent (user-built databases on ECS/BMS)

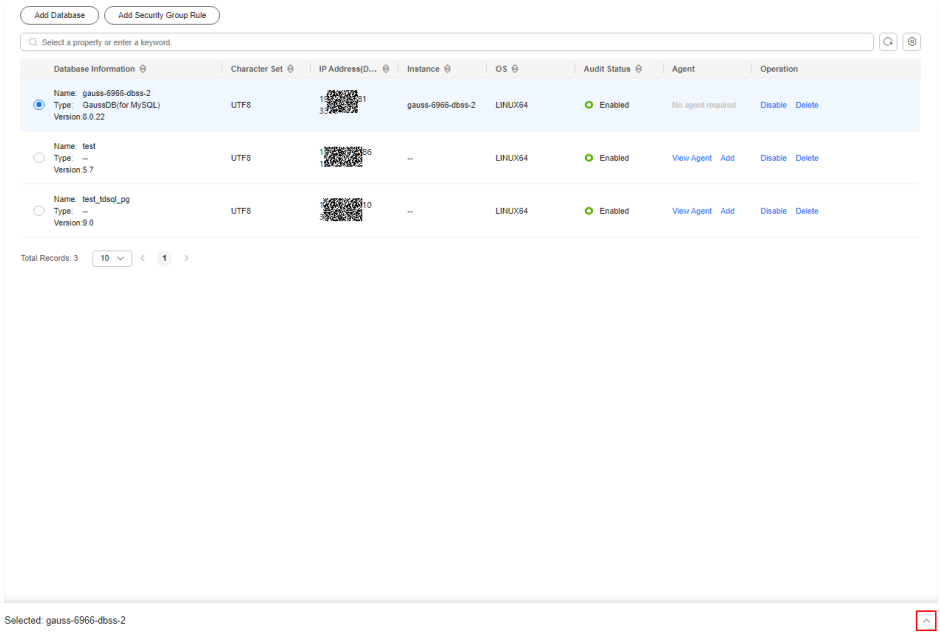
Parameter	Description	Example Value
Add Mode	Mode for adding an agent • **Select an existing agent** If an agent has been installed on a database connected to the same application as the desired database, select **Select an existing agent**. • **Create an agent** If no agent is available, select **Create 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 . You can select **LINUX64-X86**, **LINUX64-ARM**, or **WINDOWS64**. **NOTE** Select **LINUX64_X86** or **LINUX64_ARM** based on the server architecture.	LINUX64-X86

Parameter	Description	Example Value
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**.	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**.	80

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.

Figure 2-11 Successfully adding an 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 of the row to delete it, and add an agent again.

----End

Adding an Agent (RDS Databases)

NOTE

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

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

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

Step 1 Log in to the management console.

Step 2 Select a region, click ☰, and choose **Security & Compliance** > **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 2-12 and Figure 2-13. For details about related parameters, see Table 2-10.

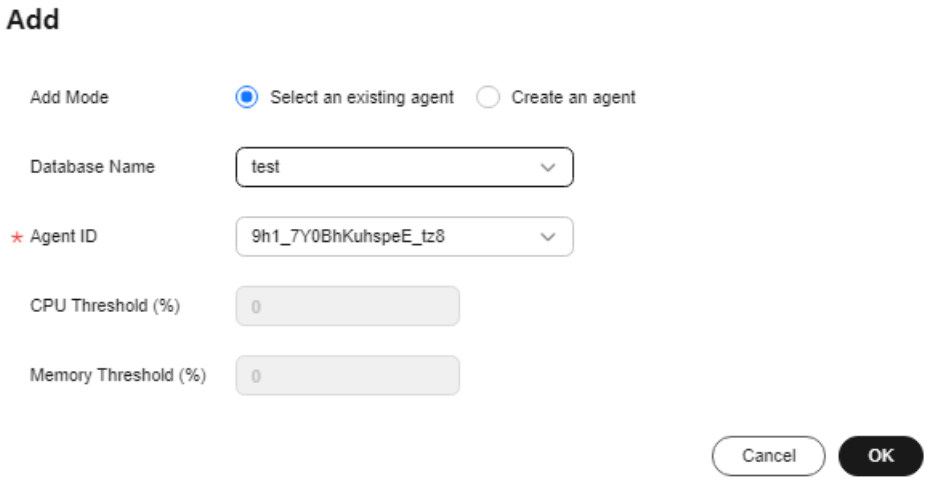
- Select **Select an existing agent** for **Add Mode**.

  For details about when you should select this option, see **When Should I Select an Existing Agent?**

  NOTE

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

  Figure 2-12 Selecting an existing agent

- 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 2-13 Adding an agent to an application

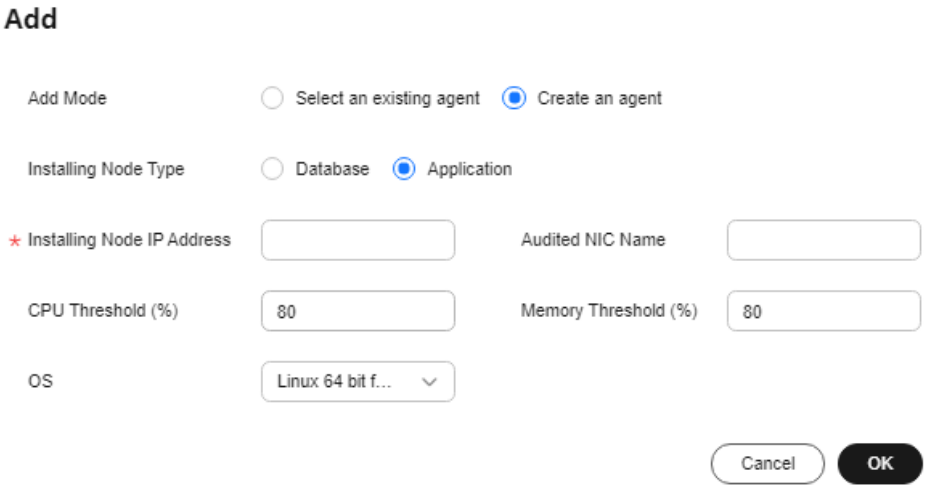


Table 2-10 Parameters for adding an agent (RDS databases)

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
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

Parameter	Description	Example Value
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	Optional. This parameter is configurable if **Installing Node Type** is set to **Application**. OS of the application node to be audited. The value can be **LINUX64** or **WINDOWS64**.	LINUX64

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 of the row to delete it, and add an agent again.

----End

Follow-Up Procedure

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

2.5 Step 3: Download and Install the Agent

2.5.1 Downloading an Agent

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

NOTE

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

Prerequisites

- You have purchased 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.

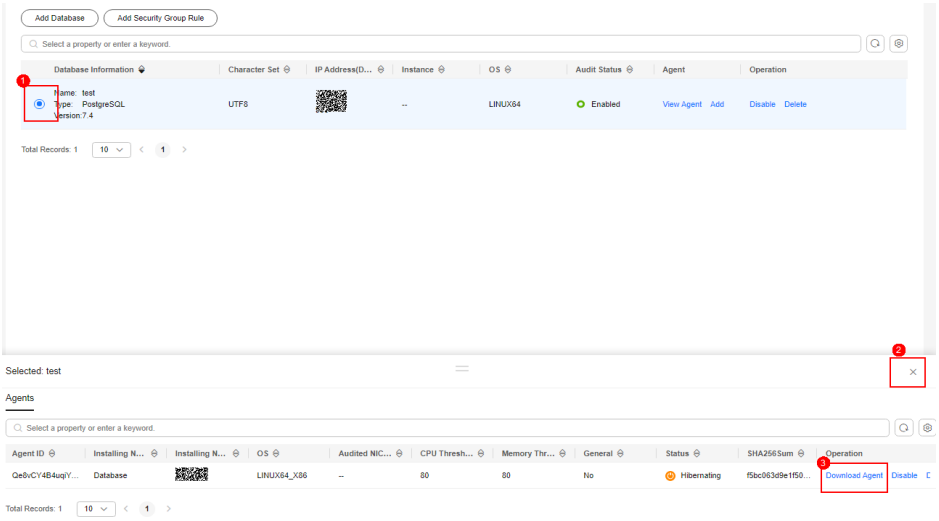
Step 2 Select a region, click , and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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.

Figure 2-14 Downloading an agent



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

2.5.2 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. For details about how to install an agent on the Windows OS, see **Installing an Agent (Windows OS)**.

Prerequisites

- You have purchased 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. For details about the supported Linux versions, see **On What Linux OSs Can I Install 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 2-15** and **Figure 2-16**.

  Figure 2-15 One application connecting to multiple databases built on ECS/BMS

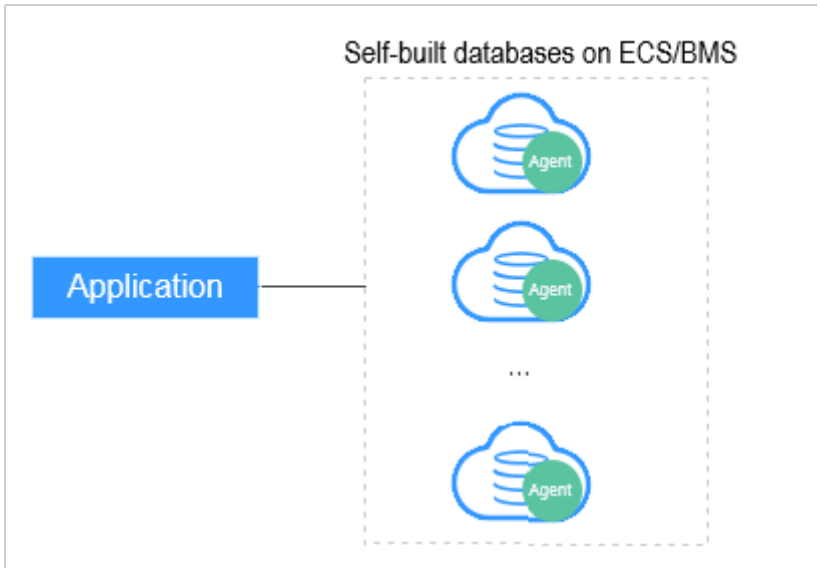
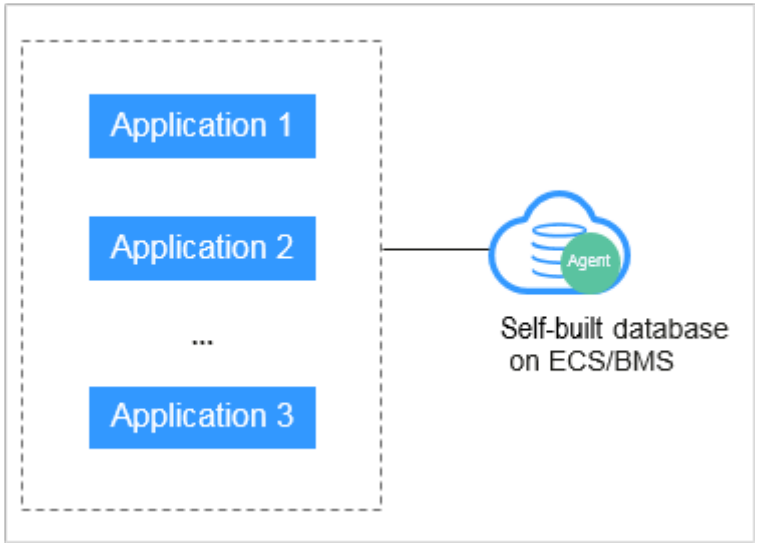


Figure 2-16 Multiple applications connecting to one database built on ECS/BMS



- Deploy DBSS for RDS databases. For details, see **Figure 2-17** and **Figure 2-18**.

Figure 2-17 One application connecting to multiple RDS databases

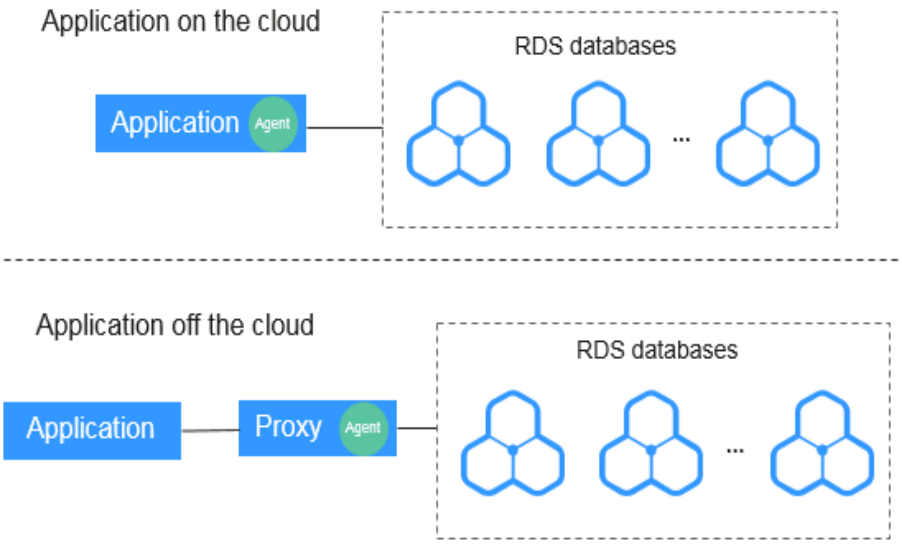


Figure 2-18 Multiple applications connecting to one RDS database

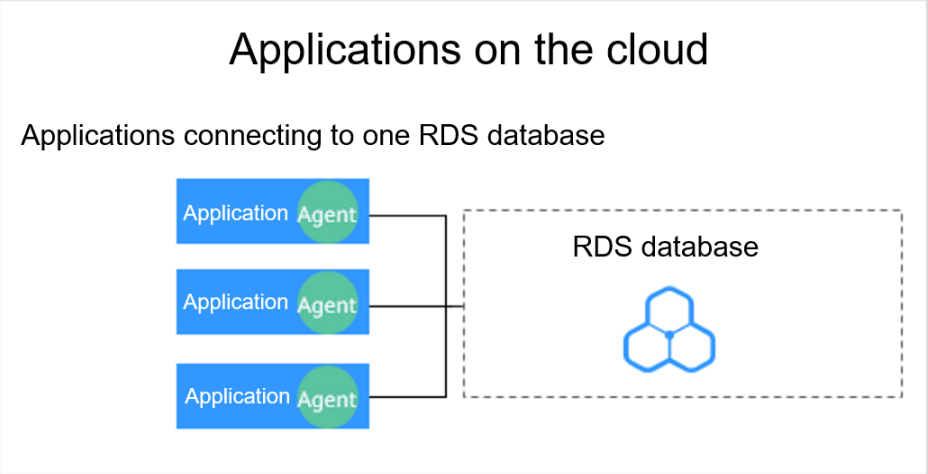


Table 2-11 describes where to install the agent in the preceding scenarios.

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 2-11 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

NOTE

When installing a new agent, you need to customize a password for it.

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*

```
[root@ecs-test ~]#
[root@ecs-test ~]# cd /agent
[root@ecs-test agent]# ll
total 5080
-rw-r--r-- 1 root root 5199159 Oct 25 09:47 [redacted]_9syBZIsBbeAhEFqE_hhD.tar.gz
[root@ecs-test agent]#
```

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

tar -xvf *xxx.tar.gz*

```
[root@ecs-test agent]#
[root@ecs-test agent]# tar -xvf [redacted]_9syBZIsBbeAhEFqE_hhD.tar.gz
```

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

cd *Decompressed_package_directory*

```
[root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]# chmod +x install.sh
[root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]# ll
total 36
drwxr-xr-x 2 root root 4096 Oct 25 09:50 bin
drwxr-xr-x 2 root root 4096 Oct 25 09:50 boot
drwxr-xr-x 2 root root 4096 Oct 25 09:50 cert
drwxr-xr-x 2 root root 4096 Oct 25 09:50 conf
drwxr-xr-x 2 root root 4096 Oct 25 09:50 crond
-rwxr-xr-x 1 root root  527 Oct 25 09:45 install.sh
drwxr-xr-x 2 root root 4096 Oct 25 09:50 lib
-rw-r--r-- 1 root root  308 Oct 25 09:45 uninstall.sh
drwxr-xr-x 2 root root 4096 Oct 25 09:50 utils
[root@ecs-test [redacted]_9syBZIsBbeAhEFqE_hhD]#
```


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

```
[root@ecs-test                _9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test                _9syBZIsBbeAhEFqE_hhD]# sh install.sh
check system bit.
check system bit success!
exist system-release file
Linux version is CentOS 7
dbss user not exists, create dbss user now. Please set user password!
Enter password :
```

NOTE

- In Ubantu, run the **bash install.sh** command to install the agent.
- The agent program is run by common DBSS users. When installing the agent for the first time, you need to create an agent user. After running the **sh install.sh** command, you need to set a password for the DBSS user.

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:

```
[root@ecs-test                _9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test                _9syBZIsBbeAhEFqE_hhD]# service audit_agent status
audit agent is running.
[root@ecs-test                9syBZIsBbeAhEFqE_hhD]#
```

```
audit agent is running.
```

----End

Helpful Links

- If SSL is enabled for a database, the database cannot be audited. To use database audit, disable SSL first. For details, see **How Do I Disable SSL for a Database?**
- For details about how to add an agent, see **Step 2: Add an Agent**.
- For details about how to uninstall an agent, see **Uninstalling an Agent**.

2.5.3 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 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. For details about the supported Windows versions, see **On What Windows OSs Can I Install 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 2-19** and **Figure 2-20**.

  Figure 2-19 One application connecting to multiple databases built on ECS/BMS

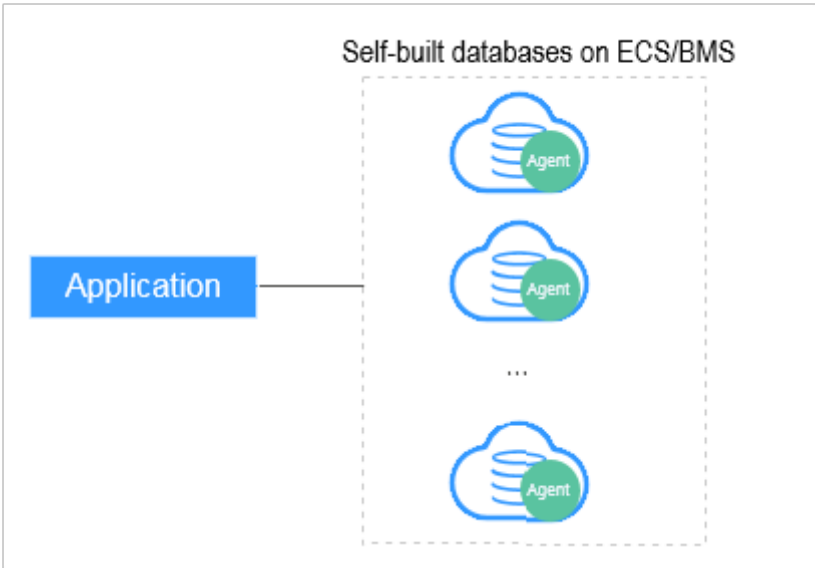
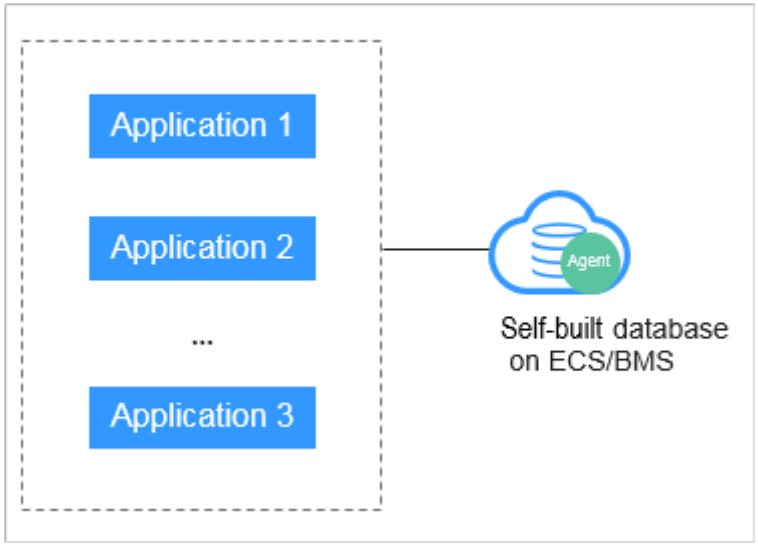


Figure 2-20 Multiple applications connecting to one database built on ECS/BMS



- Deploy DBSS for RDS databases. For details, see **Figure 2-21** and **Figure 2-22**.

Figure 2-21 One application connecting to multiple RDS databases

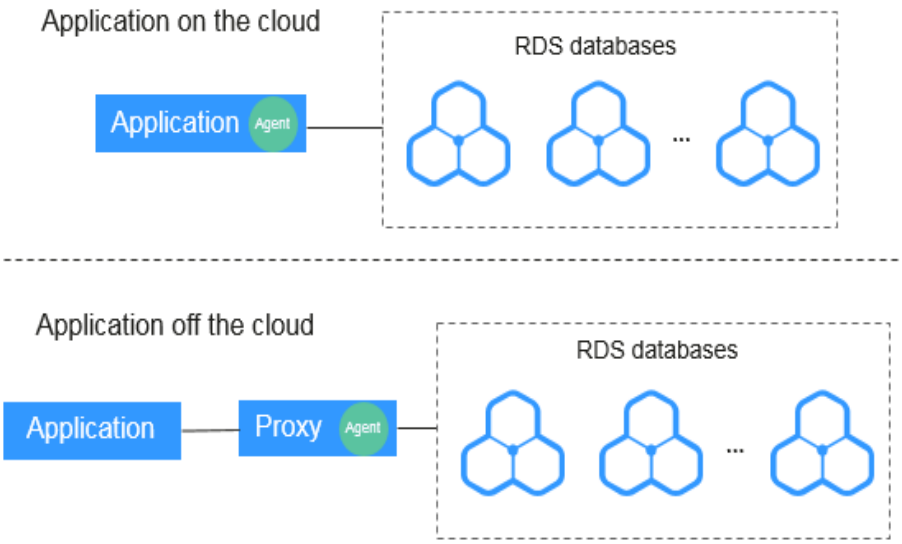


Figure 2-22 Multiple applications connecting to one RDS database

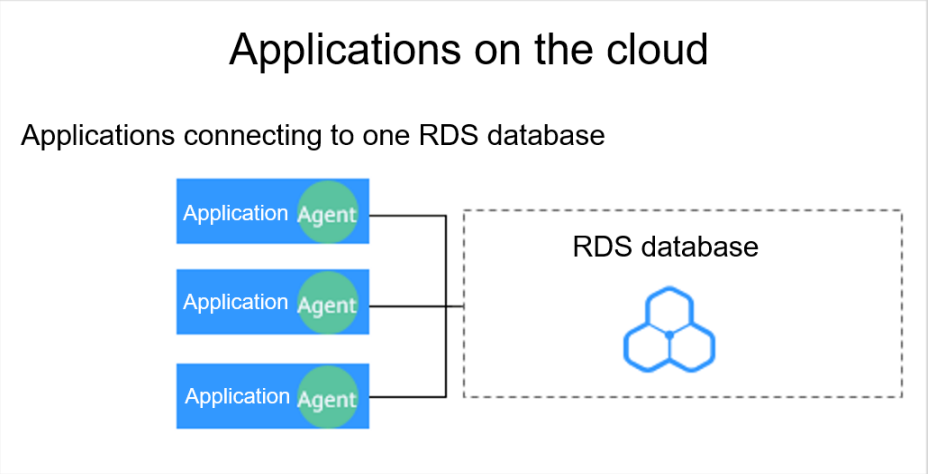


Table 2-12 describes where to install the agent in the preceding scenarios.

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 2-12 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.

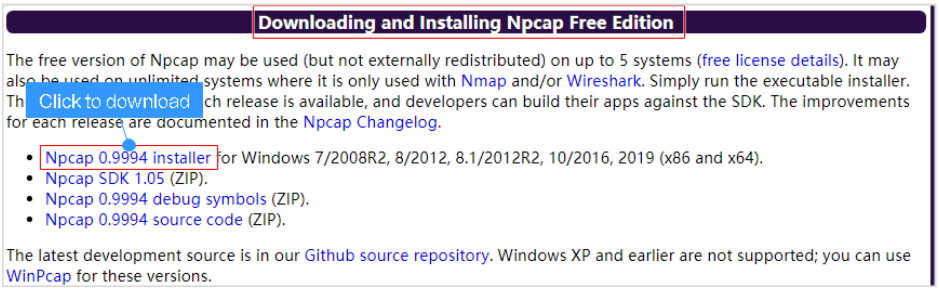
Installing an Agent

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 2-23 Downloading Npcap

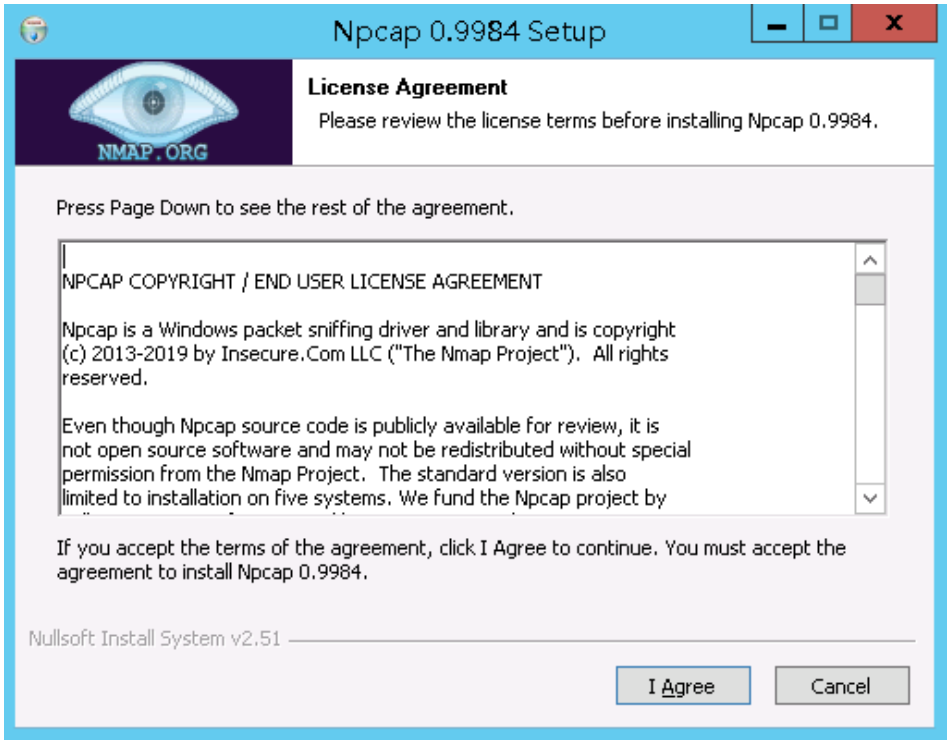
  

  b. Upload the **npcap-*xxxx*.exe** software installation package to the VM where the agent is to be installed.

  c. Double-click the Npcap installation package.

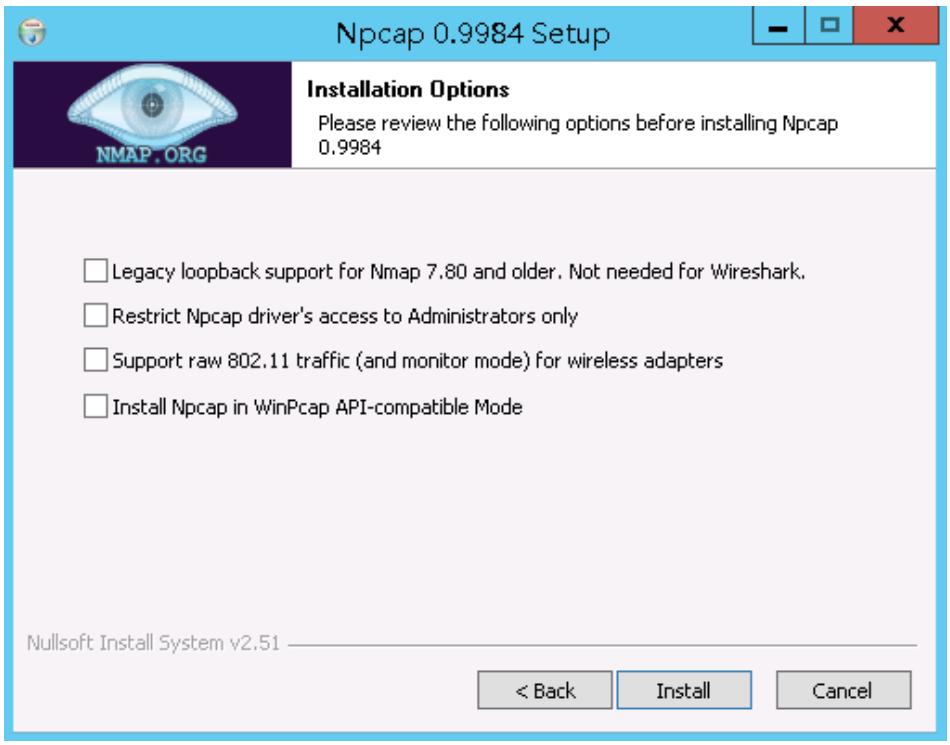
  d. In the displayed dialog box, click **I Agree**, as shown in **Figure 2-24**.

Figure 2-24 Agreeing to install Npcap

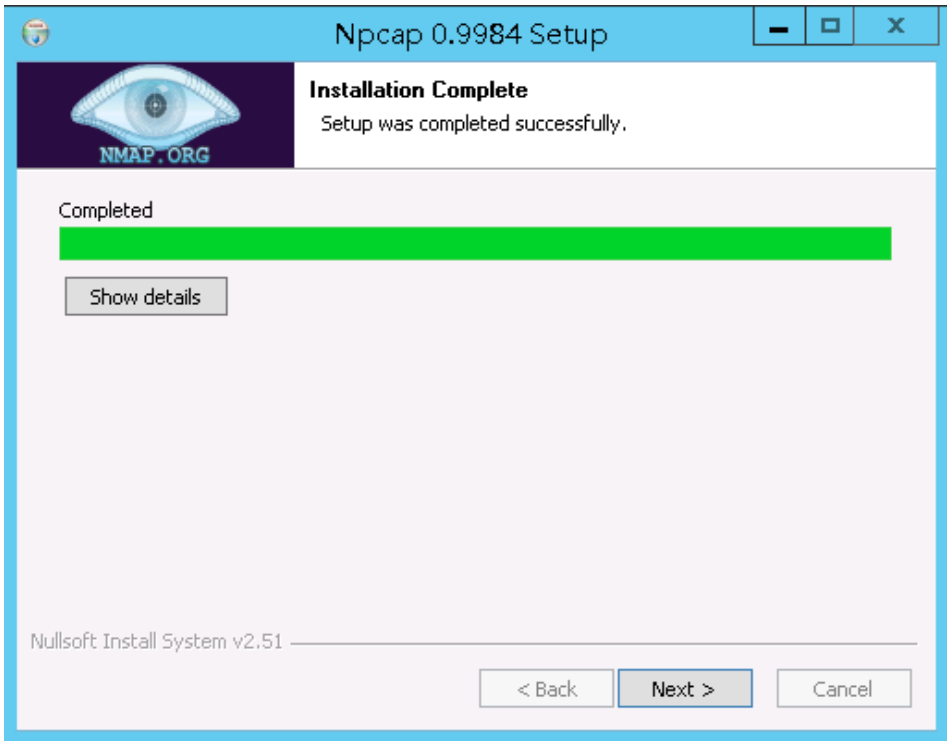


e. In the displayed dialog box, leave all the check boxes unselected and click **Install**, as shown in **Figure 2-25**.

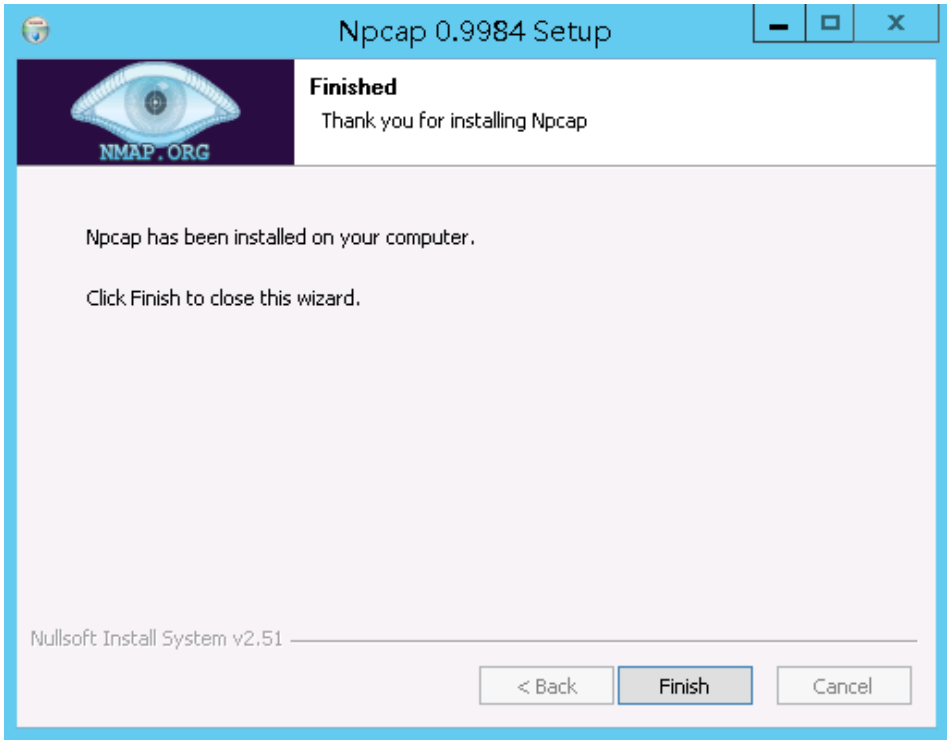
Figure 2-25 Installing Npcap



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



g. Click **Finish**.



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

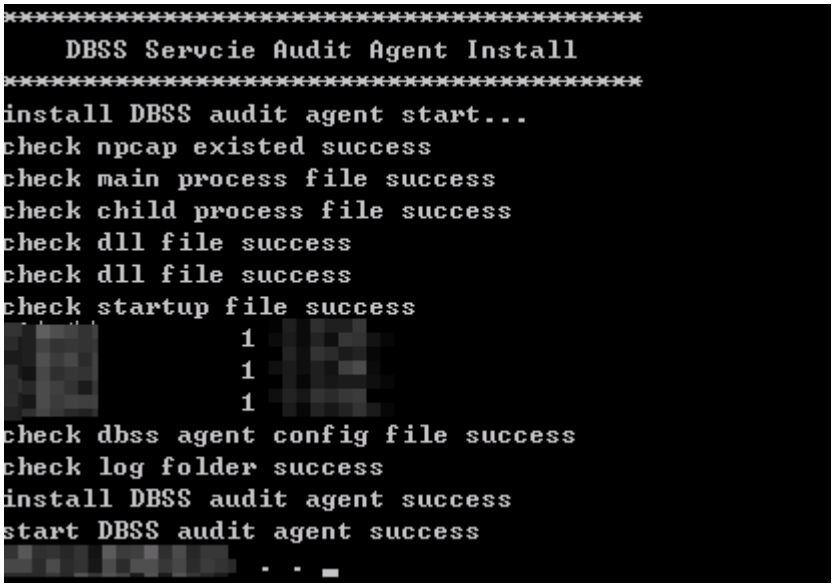
Step 3 Copy the downloaded .zip agent installation package to any directory on the server.

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 2-26** is displayed.

Figure 2-26 Installation completed



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

2.6 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 purchased 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 & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

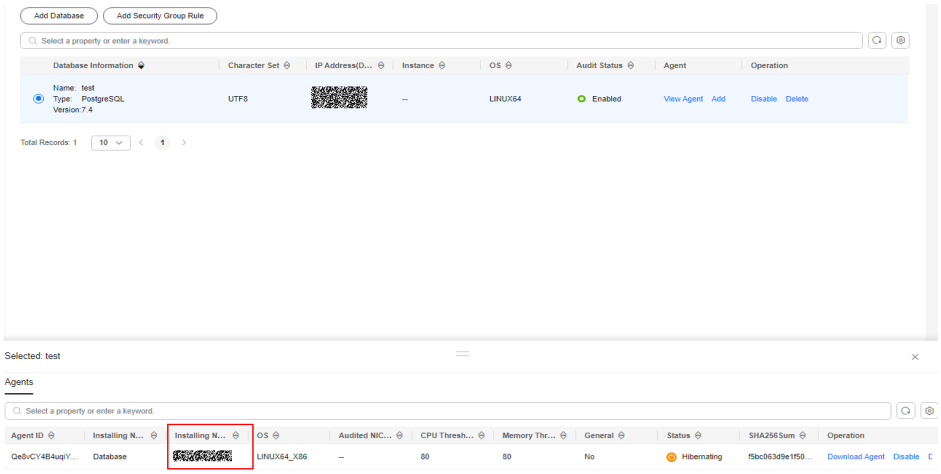
Step 3 In the navigation tree on the left, choose **Database Audit** > **Databases**.

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

Step 5 Record the IP address of the agent node.

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

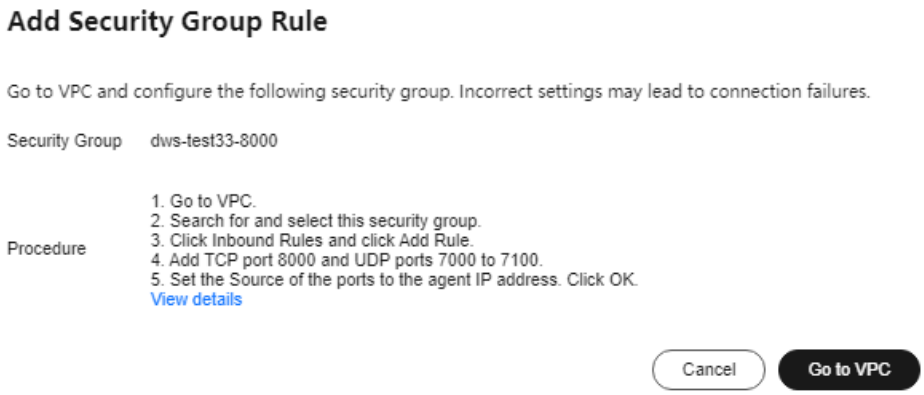
Figure 2-27 Installing Node IP Address



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

Step 7 In the displayed dialog box, record the security group name (for example, **default**) of the database audit instance, as shown in **Figure 2-28**.

Figure 2-28 Adding a security group rule



Step 8 Click **Go to VPC**.

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

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

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

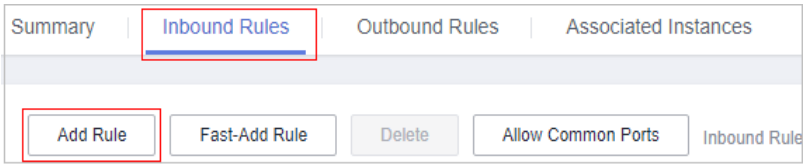
Check whether TCP (port number **8000**) and UDP protocols (port number from **7000** to **7100**) are configured in the inbound rules of the security group for the IP address of the installing node.

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

Step 12 Add an inbound rule for the installing node.

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

Figure 2-29 Adding rules



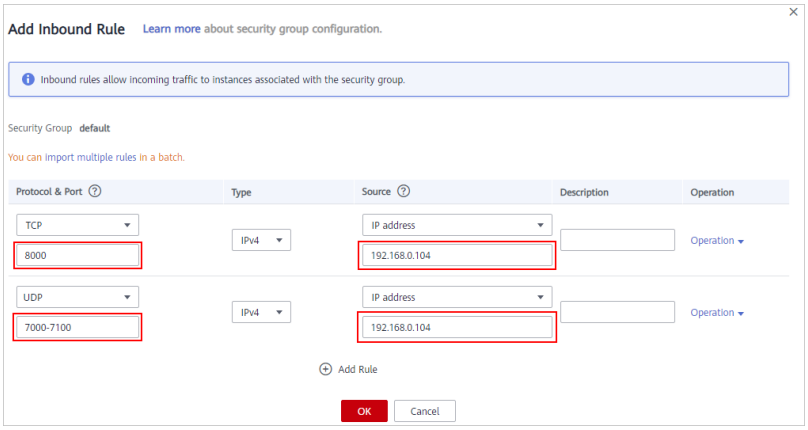
2. In the **Add Inbound Rule** dialog box, add **TCP** (port number **8000**) and **UDP** protocols (port number from **7000** to **7100**).

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 2-30 Add Inbound Rule dialog box



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

2.7 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.

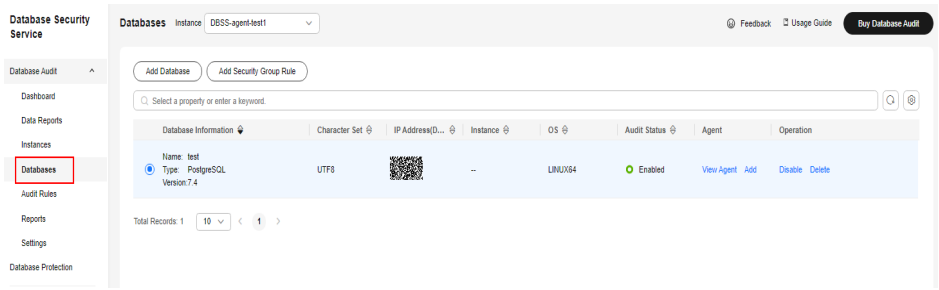
Enabling Database Audit

Step 1 **Log in to the management console.**

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

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

Figure 2-31 Going to the Databases page

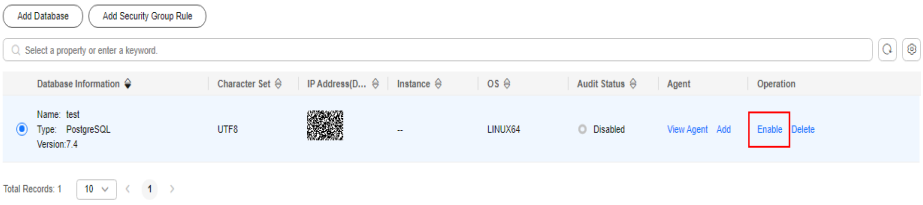


Step 4 Select a database audit instance from the **Instance** drop-down list.

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 2-32 Enabling database audit



----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 & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

Step 4 In the navigation tree on the left, choose **Data Reports**. The **Data Reports** page is displayed.

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

Step 6 Click the **Statements** tab.

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

Figure 2-33 Viewing SQL statements

- If the entered SQL statement is not displayed, the connection between the agent and the database audit instance is abnormal. Rectify the fault by following the instructions in **What Do I Do If the Communication Between the Agent and Database Audit Instance Is Abnormal?**

----End

3 Enabling and Using Database Audit (Without Installing Agents)

3.1 Process Overview

Context

Database audit supports auditing user-installed databases on ECS/BMS as well as RDS databases on Huawei Cloud.

NOTICE

- Database audit cannot be used across regions. The database to be audited and the database audit instance you purchased must be in the same region.
- For details about audit data storage, see **How Long Is the Audit Data of Database Audit Stored by Default?**

Auditing Databases Without Agents

Databases of some types and versions can be audited without using agents, as shown in **Table 3-1**.

Table 3-1 Agent-free relational databases

Database Type	Supported Edition
MySQL	All editions are supported by default.
PostgreSQL **NOTICE** If the size of an SQL statement exceeds 4 KB, the SQL statement will be truncated during auditing. As a result, the SQL statement is incomplete.	All editions are supported by default.

Database Type	Supported Edition
SQLServer	• 2008 • 2012 • 2014 • 2016 • 2017
GaussDB(for MySQL)	Mysql8.0
DWS	• 8.2.0.100 or later
MariaDB	10.2

NOTE

- DBSS without agents is easy to configure and use, but the following functions are not supported:
  - Successful and failed login sessions cannot be counted.
  - The port number of the client for accessing the database cannot be obtained.
- GaussDB(DWS) has the permission control policy for the log audit function. Only Huawei Cloud accounts and users with the **Security Administrator** permission can enable or disable the DWS database audit function.

Figure 3-1 Agent-free auditing process

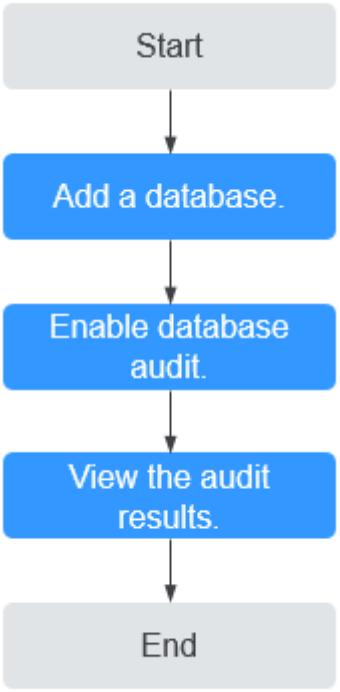


Table 3-2 Procedure for quickly configuring database audit

Step	Configuration	Description
1	**Adding a Database**	Purchase database audit. Add a database to the database audit instance and enable audit for the database. Apply for database audit. Add a database to the database audit instance and enable audit for the database.
2	**Enabling Database Audit**	Enable database audit and connect the added database to the database audit instance.
3	**Viewing the Audit Results**	By default, database audit complies with a **full audit rule**, which is used to audit all databases that are connected to the database audit instance. You can view the audit result on the database audit page. **NOTICE** You can set database audit rules as required. For details, see **Adding Audit Scope**.

3.2 Purchasing Database Audit

Before using the database audit function, you need to purchase database audit. Database audit charges yearly or monthly.

Constraints

- DBSS cannot be used across regions. The database to be audited and the database audit instance you purchased must be in the same region.
- Ensure the VPC of the database audit instance is the same as that of the node (application side or database side) where you plan to install the database audit agent. Otherwise, the instance will be unable to connect to the agent or perform audit.

  For details about how to choose the node, see **How Do I Determine Where to Install an Agent?**

Impact on the System

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

Prerequisites

The instance account has related permissions.

NOTICE

Ensure that the **DBSS System Administrator**, **VPC Administrator**, **ECS Administrator**, and **BSS Administrator** policies have been configured for the account used for purchasing instances.

- **VPC Administrator**: Users with this set of permissions can perform all execution permission for VPC. It is a project-level role, which must be assigned in the same project.
- **BSS Administrator**: Users with this set of permissions can perform any operation on menu items on pages **My Account**, **Billing Center**, and **Resource Center**. It is a project-level role, which must be assigned in the same project.
- **ECS Administrator**: Users with this set of permissions can perform any operations on an ECS. It is a project-level role, which must be assigned in the same project.

Procedure

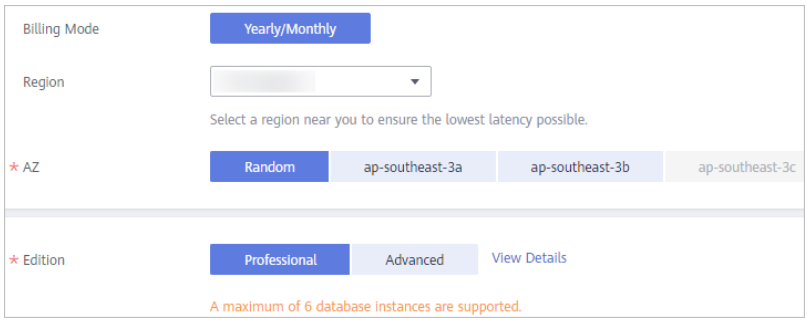
Step 1 Log in to the management console.

Step 2 Click ☰ and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

Step 4 Select a region, a project, an AZ, and an edition.

Figure 3-2 Selecting an AZ and an edition



Select an enterprise project. The DBSS you purchase will be put under this project. Billing and permissions management are performed based on enterprise projects.

Table 3-3 describes the database audit editions.

Table 3-3 Database audit editions

Edition	Maximum Databases	System Resource	Performance
Professional	6	• CPU: 8 vCPUs • Memory: 32 GB • Hard disk: 1,084 GB	• Peak QPS: 6,000 queries/second • Database load rate: 7.2 million statements/hour • Stores 600 million online SQL statements. • Stores 10 billion archived SQL statements.
Advanced	30	• CPU: 16 vCPUs • Memory: 64 GB • Hard disk: 2,108 GB	• Peak QPS: 30,000 queries/second • Database load rate: 10.8 million records/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 purchase a new one.
- The cloud native edition can be purchased only on the RDS console.
- The table above lists the system resources consumed by a database audit instance. Ensure your system has the required configurations before purchasing database audit instances.
- Online SQL statements are counted based on the assumption that the capacity of an SQL statement is 1 KB.

Step 5 Set database audit parameters, as shown in **Figure 3-3**. For details about related parameters, see **Table 3-4**.

Figure 3-3 Setting database audit parameters

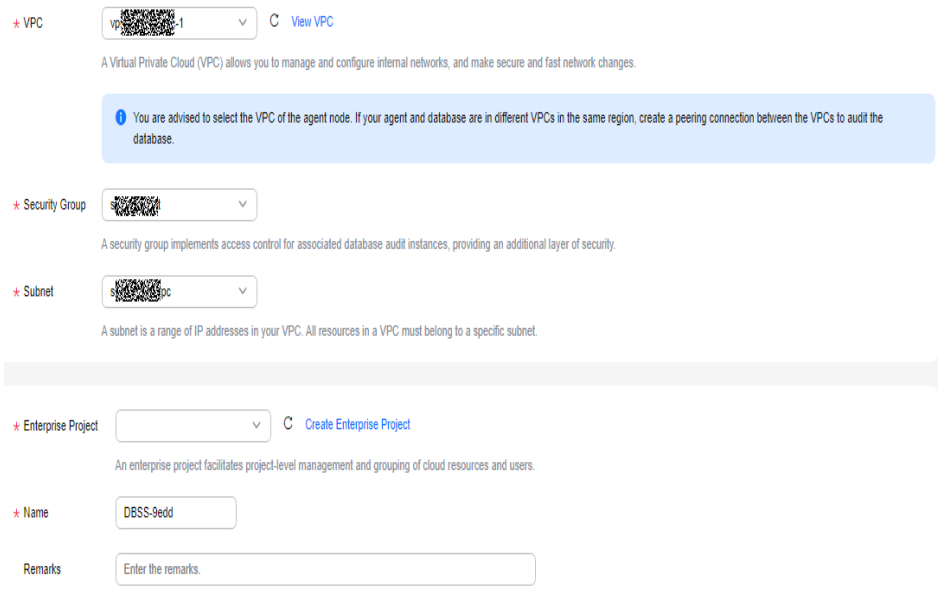
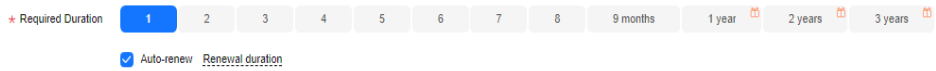


Table 3-4 Database audit parameters

Parameter	Description
VPC	You can select an existing VPC, or click **View VPC** to create one on the VPC console. **NOTE** • Select the VPC of the node (application or database side) where you plan to install the agent. For more information, see **How Do I Determine Where to Install an Agent?** • To change the VPC of a DBSS instance, unsubscribe from it and purchase a new one. For more information about VPC, see *Virtual Private Cloud User Guide*.
Security Group	You can select an existing security group in the region or create a security group on the VPC console. 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*.
Subnet	You can select a subnet configured in the VPC or create a subnet on the VPC console.
Name	Instance name

Step 6 Set **Required Duration**. See **Figure 3-4**.

Figure 3-4 Setting the required duration



After you select **Auto-renew**, the system automatically renews the instance upon expiry if your account balance is sufficient. You can continue to use the instance. **Table 3-5** describes the auto-renewal period.

Table 3-5 Auto-renewal period description

Required Duration	Auto-renewal Period
1/2/3/4/5/6/7/8/9 months	1 month
1 year	1 year

Step 7 (Optional) Add tags to the database audit instance. If you have configured tag policies for DBSS, you need to add tags to your DBSS instances based on the tag policies. If a tag does not comply with the policies, DBSS instance may fail to be created. Contact your organization administrator to learn more about tag policies.

Step 8 Confirm the configuration and click **Next**.

For any doubt about the pricing, click **Pricing details** to understand more.

Step 9 On the **Details** page, read the *Database Audit of Database Security Service Disclaimer*, select **I have read and agree to the Database Audit of Database Security Service Disclaimer**, and click **Submit**.

Step 10 On the displayed page, select a payment method.

Step 11 After you pay for your order, you can view the creation status of your instances.

----End

Follow-Up Procedure

- If the **Status** of the instance is **Running**, you have successfully purchased the database audit instance.
- If the instance status is **Creation failed**, you will be automatically refunded. You can click **More** in the **Operation** column and view details in the **Failure Details** dialog box.

3.3 Step 1: Add a Database

Database audit supports databases built on ECS, BMS, and RDS on Huawei Cloud. After purchasing a database audit instance, you need to add the database to be audited to the instance.

For details about the types and versions of databases that can be audited by database audit, see **Supported Database Types and Versions**.

Prerequisites

You have purchased 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 & Compliance** > **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 displayed dialog box, configure the database information.

Table 3-6 Parameters

Parameter	Description	Example Value
Database Type	Type of the database to be added. You can select **RDS database** or **Self-built database**. **NOTE** If you select **RDS database**, you can directly select the databases that you want to add to DBSS.	RDS database
Name	Custom name of the database to be added	test1
IP Address	IP address of the database to be added. The IP address must be an internal IP address in IPv4 or IPv6 format.	IPv4: 192.168.1.1 IPv6: fe80:0000:0000:0000:0000:0000:0000:0000

Parameter	Description	Example Value
Type	Supported database type. The options are as follows: • MYSQL • ORACLE • PostgreSQL • SQL Service • DWS • GaussDB(for MYSQL) • GaussDB • DAMENG • KINGBASE • MongoDB • Hbase • SHENTONG • GBase 8a • GBase XDM Cluster • Greenplum • HighGo • MariaDB • Hive • DDS • GBase 8s • TDSQL **NOTE** • If **ORACLE** is selected, to make the audit settings take effect, restart the applications to be audited and log in to the database again.	MYSQL
Port	Port number of the database to be added	3306

Parameter	Description	Example Value
Version	Supported database versions • When **Type** is set to **MYSQL**, the following versions are available: – 5.0, 5.1, 5.5, 5.6, 5.7 – 8.0 (8.0.11 and earlier) – 8.0.30 – 8.0.35 – 8.1.0 – 8.2.0 – If **RDS database** is selected, a list of database instances will be displayed for you to choose from. You do not need to install the agent. • 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 – 14.0 • 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:	5.0

Parameter	Description	Example Value
	– 1.5 – 8.1 • When **Type** is set to **GaussDB(for MySQL)**, the following versions are available: – When **Database Type** is set to **Self-built database**, you can select the **MySQL 8.0** version. – If **RDS database** is selected, a list of database instances will be displayed for you to choose from. You do not need to install the agent. • When **Type** is set to **GaussDB**, the following version is available: – 1.4 Enterprise Edition – 1.3 Enterprise Edition – 2.8 Enterprise Edition – 3.223 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: – V8 • When **Type** is set to **Hbase**, the following versions are available: – 1.3.1 – 2.2.3 • When **Type** is set to **SHENTONG**, the following version is available: – V7.0 • When **Type** is set to **GBase 8a**, the following version is available: – v8.5 • When **Type** is set to **GBase 8s**, the following version is available: – v8.8 • When **Type** is set to **Greenplum**, the following version is available: – v6.0 • When **Type** is set to **HighGo**, the following version is available:	

Parameter	Description	Example Value
	– v6.0 • When **Type** is set to **MongoDB**, the following version is available: – v5.0 • When **Type** is set to **MariaDB**, the following version is available: – 10.6 • When **Type** is set to **Hive**, the following versions are available: – 1.2.2 – 2.3.9 – 3.1.2 – 3.1.3 • When **Type** is set to **TDSQL**, the following version is available: – 10.3.17.3.0	
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

Step 7 Click **OK**. A database whose **Audit Status** is **Disabled** is added to the database list.

NOTE

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

----End

3.4 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**.
- A security group rule has been configured for the database audit instance.

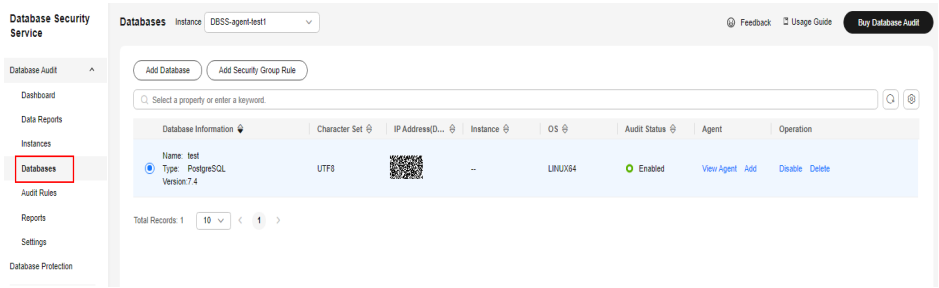
Enabling Database Audit

Step 1 **Log in to the management console.**

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

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

Figure 3-5 Going to the Databases page

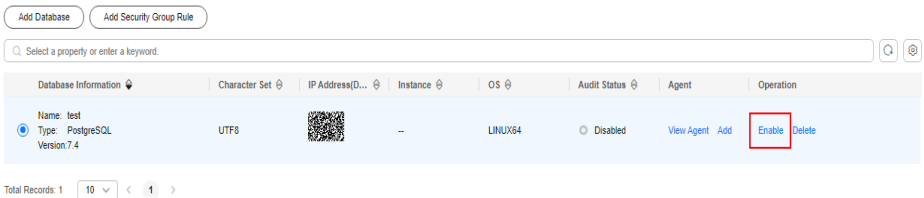


Step 4 Select a database audit instance from the **Instance** drop-down list.

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 3-6 Enabling database audit



----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 & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

Step 4 In the navigation tree on the left, choose **Data Reports**. The **Data Reports** page is displayed.

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

Step 6 Click the **Statements** tab.

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

Figure 3-7 Viewing SQL statements

- If the entered SQL statement is not displayed, the connection between the agent and the database audit instance is abnormal. Rectify the fault by following the instructions in **What Do I Do If the Communication Between the Agent and Database Audit Instance Is Abnormal?**

----End

4 Upgrading the Database Audit Instance Version

This section describes how to upgrade your database instance version.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.
- A security group rule has been configured for the database audit instance.
- The database instance version is earlier than the latest version.

Procedure

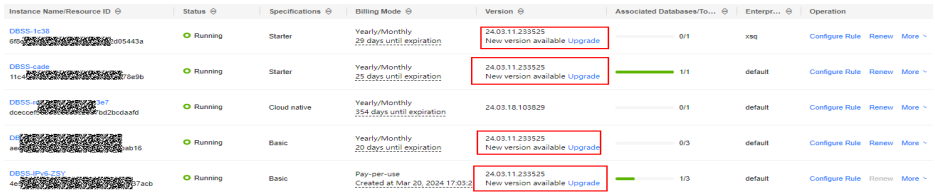
Step 1 **Log in to the management console**.

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 **Instances**.

Step 4 Click **Upgrade** in the **Version** column.

Figure 4-1 Upgrading the instance version



Step 5 In the dialog box that is displayed, click **OK**.

----End

5 Configuring Audit Rules

5.1 Adding Audit Scope

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 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 purchased 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 & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation tree on the left, 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 5-1**. For details about related parameters, see **Table 5-1**.

Figure 5-1 Add Audit Scope dialog box

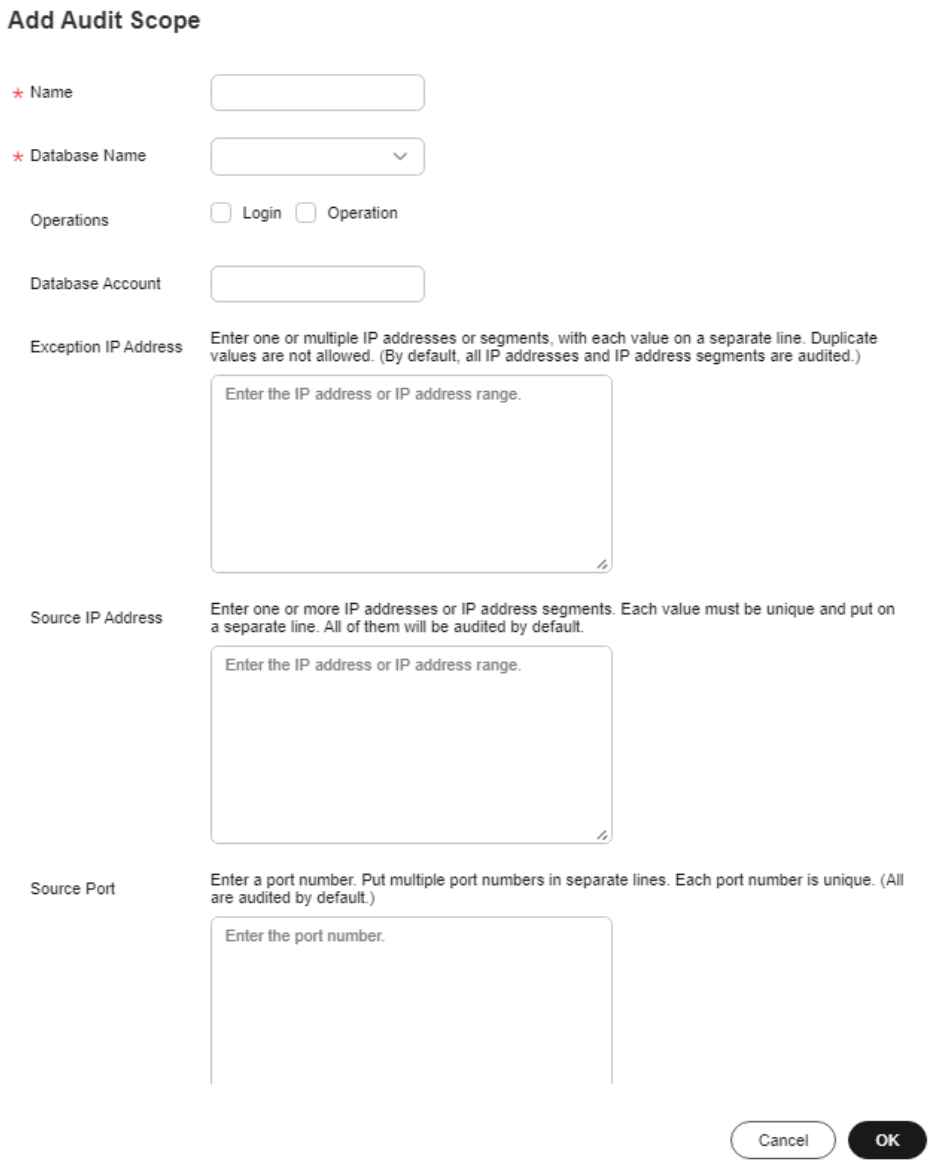


Table 5-1 Parameters

Parameter	Description	Example Value
Name	Name of the custom audit scope	audit00
Database Name	Select a database or **ALL**.	db03
Database Account	Optional. Username of the database. You can specify multiple accounts, separated by commas (,).	-

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

Step 7 Click **OK**.

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

----End

Related Operations

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

5.2 Adding an SQL Injection Rule

You can add SQL injection rules to audit your databases.

Prerequisites

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

Procedure

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 Click **Add Rule** and configure parameters.

Figure 5-2 Adding an SQL injection rule

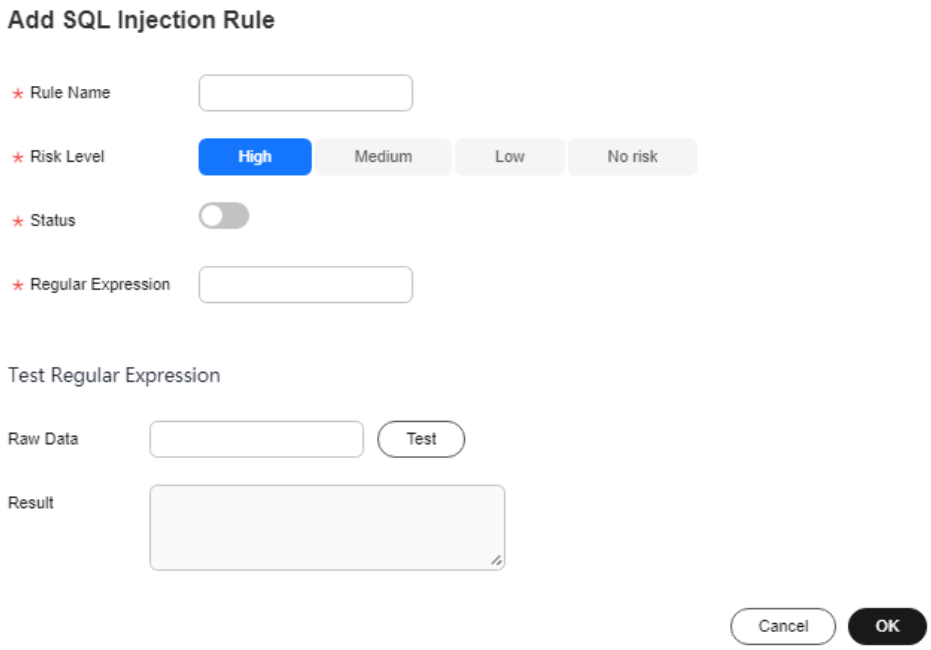


Table 5-2 SQL injection rule parameters

Parameter	Description	Example Value
Name	Name of an SQL rule.	Postal Code SQL injection Rule
Risk Level	Level of risks matching a SQL rule. Its value can be: • **High** • **Moderate** • **Low** • **No risk**	**Moderate**
Status	Enables or disables an SQL injection rule. • : enabled • : disabled	

Parameter	Description	Example Value
Test Regular Expression	Regular expression that checks for content in certain pattern.	^\d{6}$
Data	Content that matches the regular expression. Enter content and click **Test** to verify that the regular expression works properly.	628307
Result	Test result. It can be: • Hit • Miss **NOTE** If the test result is **Hit**, the regular expression is correct. If the test result is **Miss**, the regular expression is incorrect.	Hit

Step 4 Confirm the information and click **OK**.

----End

5.3 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 purchased 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 & Compliance** > **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.

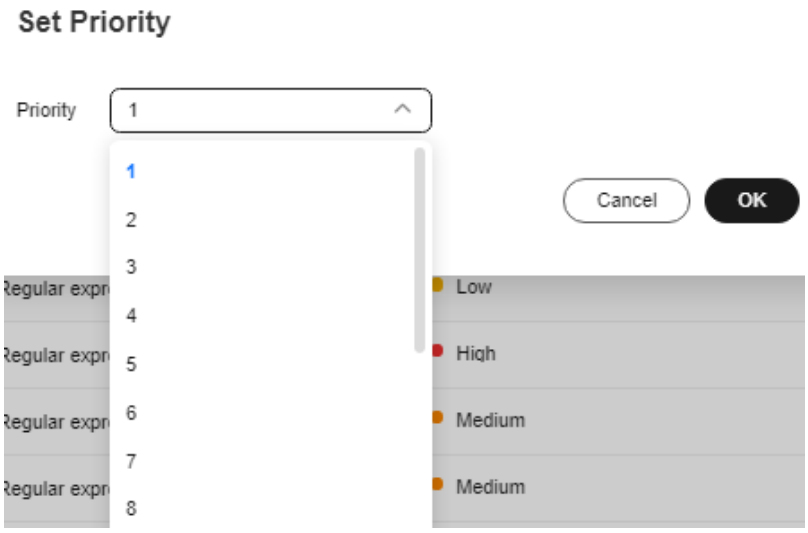
Step 5 Click the **SQL Injection** tab.

NOTE

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

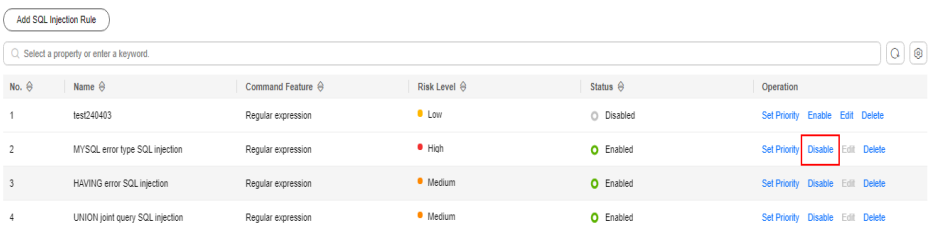
Step 6 In the **Operation** column of a rule, click **Set Priority**. In the displayed dialog box, select a priority. The smallest number indicates the highest priority. Click **OK**.

Figure 5-3 Configuring the priority



Step 7 Locate the SQL injection rule you want to disable, and click **Disable** in the **Operation** column.

Figure 5-4 Disabling an SQL injection detection rule



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

Step 8 In the **Operation** column of a rule, click **Edit**. Configure parameters and click **OK**.

Figure 5-5 Editing an SQL injection rule

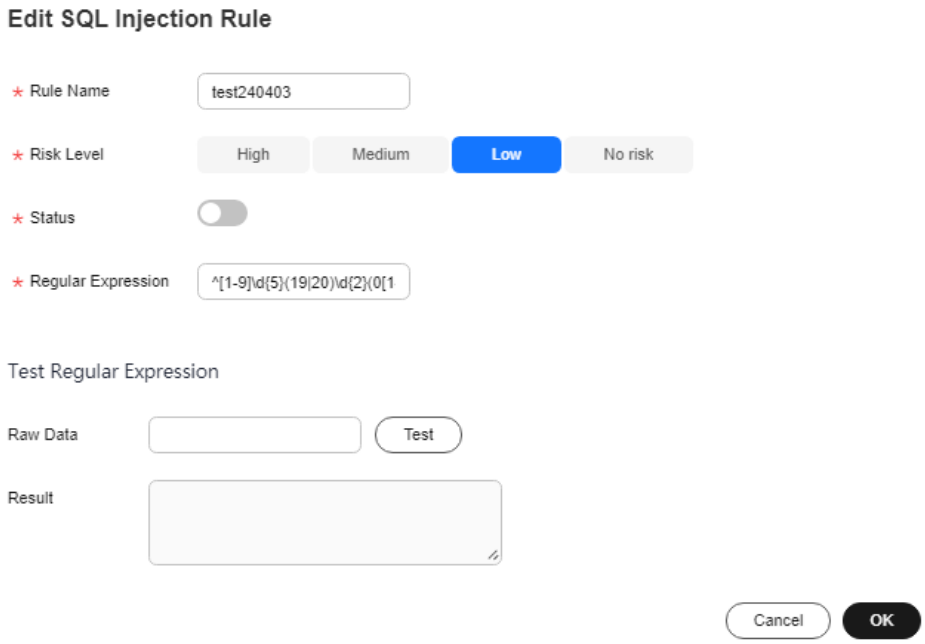


Table 5-3 SQL injection rule parameters

Parameter	Description	Example Value
Name	Name of an SQL rule.	Postal Code SQL injection Rule
Risk Level	Level of risks matching a SQL rule. Its value can be: • **High** • **Moderate** • **Low** • **No risk**	**Moderate**
Status	Enables or disables an SQL injection rule. • : enabled • : disabled	
Test Regular Expression	Regular expression that checks for content in certain pattern.	^\d{6}$

Parameter	Description	Example Value
Data	Content that matches the regular expression. Enter content and click **Test** to verify that the regular expression works properly.	628307
Result	Test result. It can be: • Hit • Miss **NOTE** If the test result is **Hit**, the regular expression is correct. If the test result is **Miss**, the regular expression is incorrect.	Hit

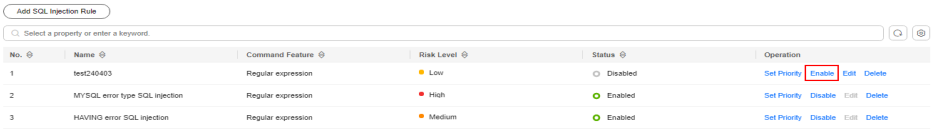
Step 9 In the **Operation** column, click **Delete**.

----End

Follow-Up Procedure

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

Figure 5-6 Enabling an SQL injection detection rule



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

5.4 Adding Risky Operations

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

NOTICE

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

Prerequisites

- You have purchased 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 & Compliance** > **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 In the **Instance** drop-down list, select an instance to add risky operations.

Step 6 Click the **Risky Operation** tab.

Step 7 Click **Add** above the risky operation list.

Step 8 On the **Add Risky Operation** page, set the basic information and client IP address. For details about related parameters, see **Table 5-4**.

Figure 5-7 Setting the basic information and client IP address

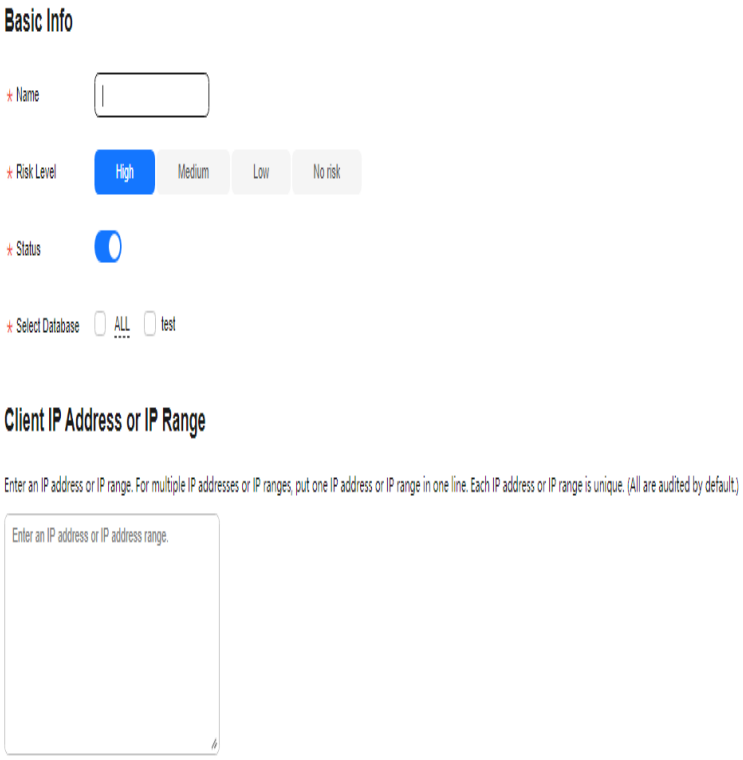


Table 5-4 Parameters

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

Step 9 Set the operation type, operation object, and execution result. For details about related parameters, see **Table 5-5**.

Figure 5-8 Setting the operation type, operation object, and execution result

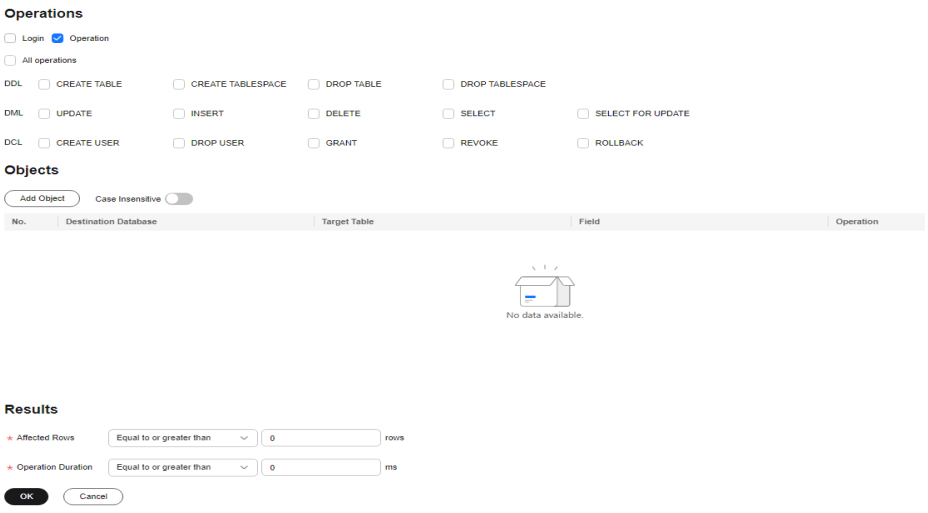


Table 5-5 Parameters

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

Step 10 Click **Save**.

----End

5.5 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 purchased 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 & Compliance** > **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.

  Note: The result set storage supports only the database audit in agent mode.

- **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 5-9**. For details about related parameters, see **Table 5-6**.

Figure 5-9 Add Rule dialog box

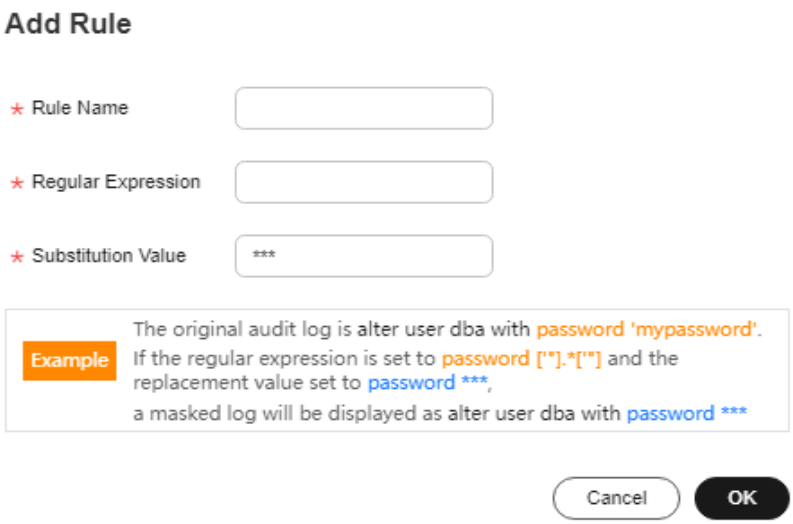


Table 5-6 Rule parameters

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.

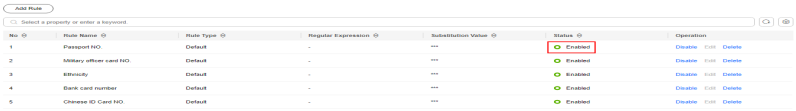
----End

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 5-10**.

Figure 5-10 Enabled rule



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 in **SQL Statement**.

----End

Common Operations

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

- Disable

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

- Edit

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

- Delete

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

6 Viewing Audit Results

6.1 Viewing SQL Statement Details

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

Prerequisites

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

Procedure

Step 1 Log in to the management console.

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

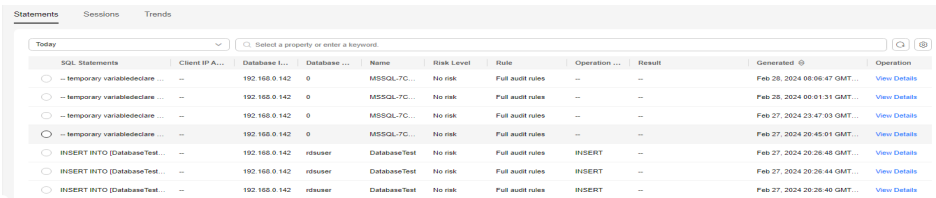
Step 3 In the navigation tree on the left, choose **Data Reports**. The **Data Reports** page is displayed.

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

Step 5 Click the **Statements** tab.

Step 6 View SQL statement information.

Figure 6-1 Querying SQL statements



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

Figure 6-2 Viewing details of SQL statements

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

NOTICE

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

Table 6-1 Parameters for details of SQL statements

Parameter	Description
Session ID	ID of an SQL statement, which is automatically generated
Database Instance	Database where an SQL statement is executed
Database Type	Type of the database where an SQL statement is executed
Database User	Database user for executing an SQL statement
Client MAC Address	MAC address of the client where an SQL statement is executed
Database MAC Address	MAC address of the database where an SQL statement is executed
Client IP Address	IP address of the client where an SQL statement is executed
Database IP Address/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

Parameter	Description
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

Helpful Links

- If the entered SQL statement is not displayed, the connection between the agent and the database audit instance is abnormal. Rectify the fault by following the instructions in **What Do I Do If the Communication Between the Agent and Database Audit Instance Is Abnormal?**
- If SSL is enabled for a database, the database cannot be audited. To use database audit, disable SSL first. For details, see **How Do I Disable SSL for a Database?**

6.2 Viewing Session Distribution

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

Prerequisites

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

Procedure

Step 1 **Log in to the management console.**

Step 2 Select a region, click ☰, and choose **Security & Compliance** > **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.

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

----End

6.3 Viewing the Audit Dashboard

After connecting the database to the database audit instance, view the audit statistics, including the database audit information, instance information, and data analysis information.

Prerequisites

- This function is supported by database instance of 23.05.23.193055 and later versions.
- You have purchased a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.

Procedure

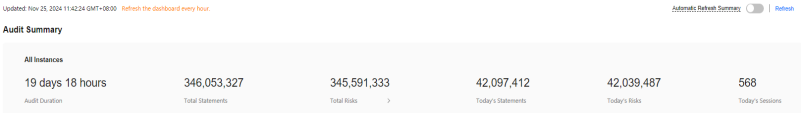
Step 1 Select a region, click , and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

Step 2 View audit information, single instance information, and data analysis charts.

- Audit information

  Displays the audit duration, total number of statements, total number of risks, and the statements, risks, and sessions today of all database audit instances.

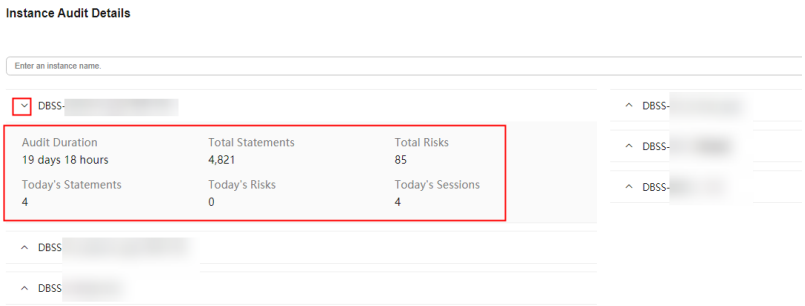
  Figure 6-3 Viewing audit summary

  Click in the upper right corner to enable regular information summary refreshing. Refresh the dashboard every hour. Click **Refresh** in the upper right corner to refresh the audit information immediately.
- Single instance information

Click ⌄ to view the audit duration, total number of statements, total number of risks, and the statements, risks, and sessions today of all database audit instances.

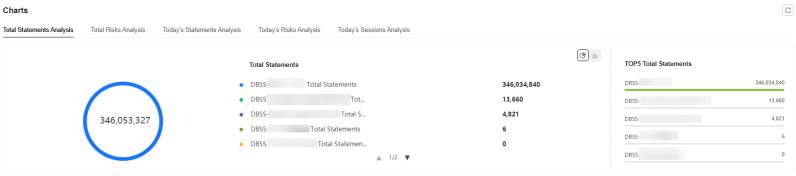
Figure 6-4 Viewing single instance information



- Data analysis charts

  Click  or  to display audit information about all instances by total number of statements, total number of risks, today's statements, today's risks, and today's sessions in pie charts or bar charts. In addition, top 5 data records are displayed.

Figure 6-5 Viewing the data analysis chart

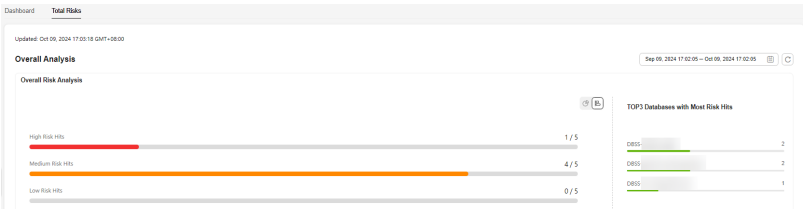


Step 3 Click **Total Risks**. The **Total Risks** page is displayed. Click  and select a time range to view the risk analysis of all database audit instances in the specified time range.

- Overall risk analysis

  Click  or  . You can view the statistics of **High Risk Hits**, **Medium Risk Hits**, and **Low Risk Hits** among all databases in a pie chart or bar chart. In addition, the top 3 risk hits of databases are displayed.

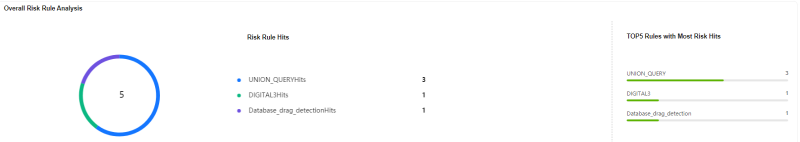
Figure 6-6 Overall risk analysis



- Overall risk rule analysis

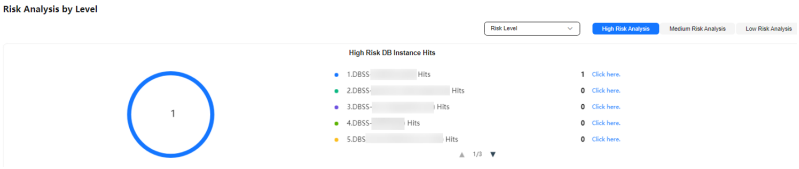
  Displays the number of risk rule hits of all databases and top 5 risk rule hits.

Figure 6-7 Overall risk rule analysis



- Risk analysis by level
  - Risk level: displays the high-risk hit analysis, medium-risk hit analysis, and low-risk hit analysis of each database.

    Figure 6-8 Risk level analysis

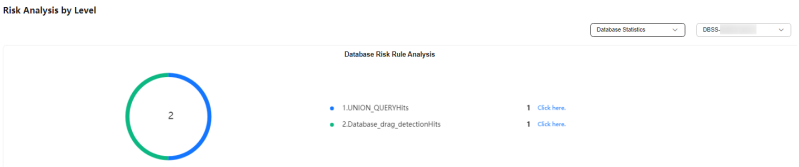
  - Risk rule: displays the analysis when a database is hit by a risk rule.

    Figure 6-9 Risk rule analysis

  - Database statistics: displays the analysis of each database that is hit by a risk rule.

    Figure 6-10 Database statistics analysis

Step 4 In the navigation tree on the left, choose **Data Reports**. The **Data Reports** page is displayed.

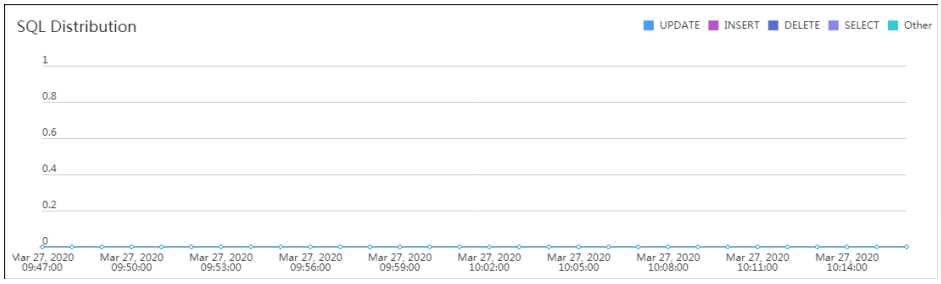
Step 5 Click the **Trends** tab. The trend analysis page is displayed.

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

Step 7 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.

Figure 6-11 SQL distribution



----End

Helpful Links

- If SSL is enabled for a database, the database cannot be audited. To use database audit, disable SSL first. For details, see **How Do I Disable SSL for a Database?**
- If the audit function is unavailable, rectify the fault by following the instructions provided in **Database Audit Is Unavailable**.
- You can configure database audit rules. For details, see **Adding Audit Scope**.

6.4 Viewing Audit Reports

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. After connecting the database to the database audit instance, generate an audit report and preview online or download it.

Prerequisites

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

Report Types

Database audit provides eight types of report templates. **Table 6-2** lists the report names. You can generate reports and set report tasks as needed.

Table 6-2 Description

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

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

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

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

Step 5 In the **Instance** drop-down list, select the instance whose instance report you want to generate.

Step 6 Click the **Report Management** tab.

Step 7 In the **Operation** column of a report template, click **Generate Report**.

Step 8 In the displayed dialog box, click to set the start time and end time of the report, and select the database for which you want to generate a report.

Step 9 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 & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

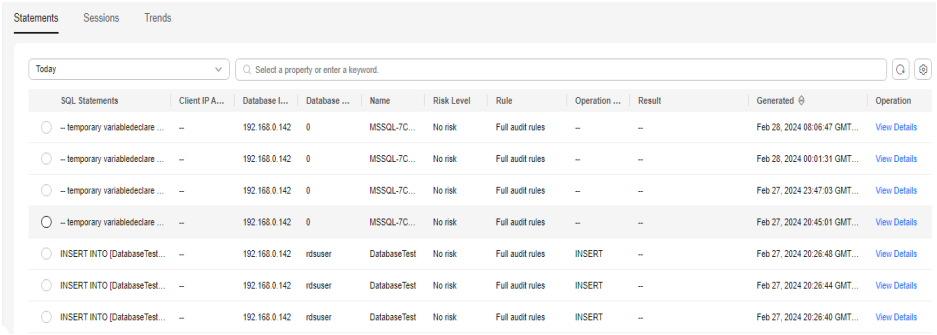
Step 3 In the navigation tree on the left, choose **Reports**.

Step 4 In the **Instance** drop-down list, select the instance 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 6-12**.

Figure 6-12 Setting a task



Step 7 In the displayed dialog box, set the parameters of the scheduled task, as shown in **Figure 6-13**. For details about related parameters, see **Table 6-3**.

Figure 6-13 Setting a scheduled task

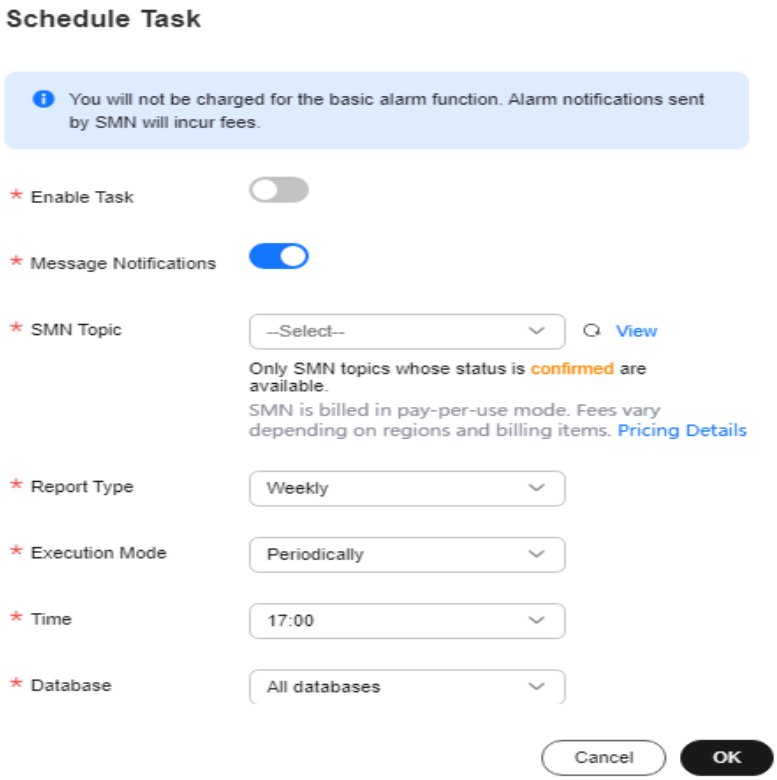


Table 6-3 Parameters for setting a task

Parameter	Description	Example Value
Enable Task	Status of a scheduled task. • : enabled • : disabled	
Message Notifications	Enables or disables notifications. Notifications are sent by Simple SMN and will probably incur a small fee. See **SMN Pricing Details**. • : enabled • : disabled	
Report Type	Type of a report. The options are as follows: • **Daily** • **Weekly** • **Monthly**	Weekly

Parameter	Description	Example Value
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.**

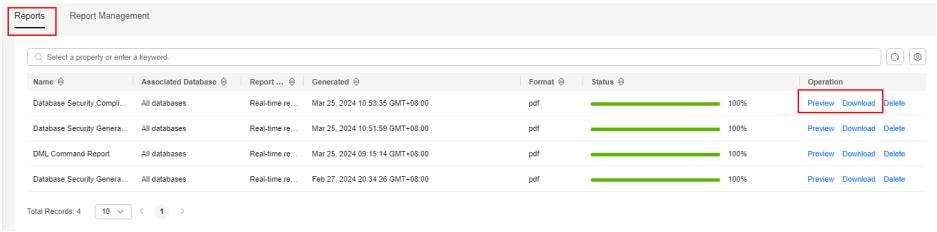
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

Step 4 In the **Instance** drop-down list, select the instance whose 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 6-14**..

Figure 6-14 Previewing or downloading an audit report



----End

Helpful Links

Why I Cannot Preview the Database Security Audit Report Online?

6.5 Viewing Trend Analysis

After connecting the database to the database audit instance, you can view the statement trend analysis (including statement quantity, session statistics, and SQL distribution) and risk trend analysis (including risk distribution, SQL injections, and risky operations).

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.
- A security group rule has been configured for the database audit instance.
- This function is supported by database instance of 23.05.23.193055 and later versions.

Procedure

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

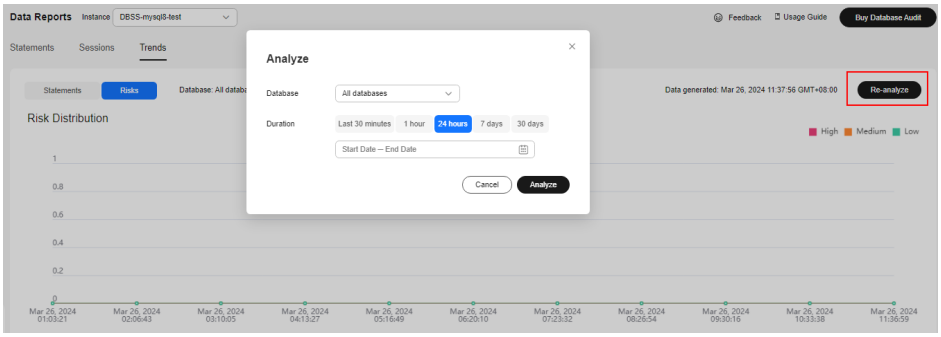
Step 4 Click the **Trends** tab. The trend analysis page is displayed.

Step 5 In the **Instance** drop-down list, select the instance whose audit information you want to view.

Step 6 View the overall trend of the database.

- Click **Re-analyze** on the right of the console.
- 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.

Figure 6-15 Re-analyze



----End

7 Notification Settings Management

7.1 Configuring Email Notifications

After enabling email notifications, you can receive an email when an alarm is triggered or an audit report is generated.

Prerequisites

You have purchased 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 & Compliance** > **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 email settings

Step 5 Configure the email notification. **Table 7-1** describes the parameters

Figure 7-1 Configuring email notifications

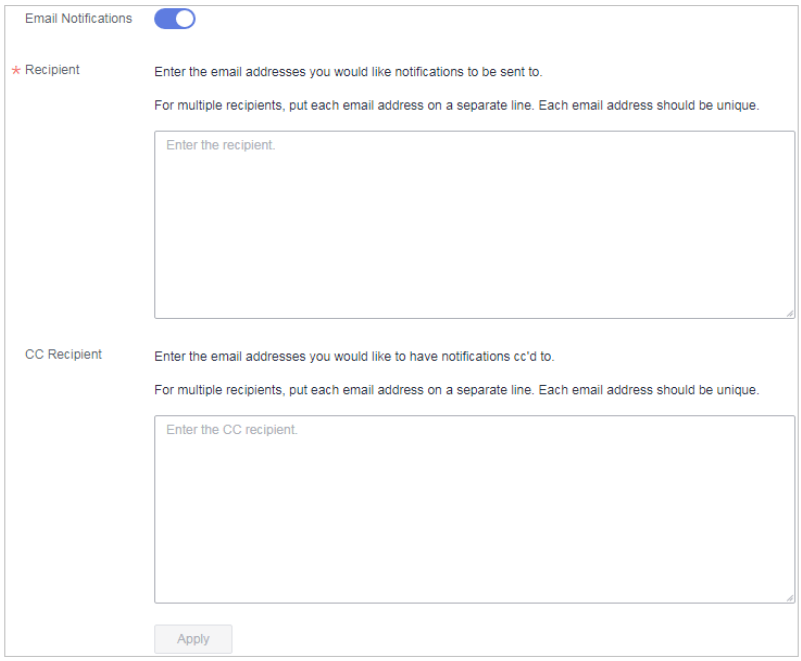


Table 7-1 Parameters

Parameter	Description	Example Value
Email Notifications	Status of the email notification function. By default, **Email Notifications** is enabled for database audit. You will receive an email when a configured alarm is triggered or an audit report is generated. • : enabled • : disabled	
Recipient	Email address of the recipient	-
CC Recipient	Optional. Email address of the CC recipient	-

Step 6 Click **Apply**.

----End

7.2 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 spam.
- The system collects alarm statistics every 5 minutes and sends alarm notifications (if any).
- Database audit alarm notifications are sent by SMN and will incur fees. See **SMN Pricing Details**.

Prerequisites

The database audit instance is in the **Running** state.

Procedure

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

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

Step 3 In the **Instance** drop-down list, select an instance to configure alarm notifications.

Step 4 Click the **Alarm Notifications** tab.

Step 5 Set alarm notifications. For details about related parameters, see **Table 7-2**.

Figure 7-2 Configuring alarm notifications

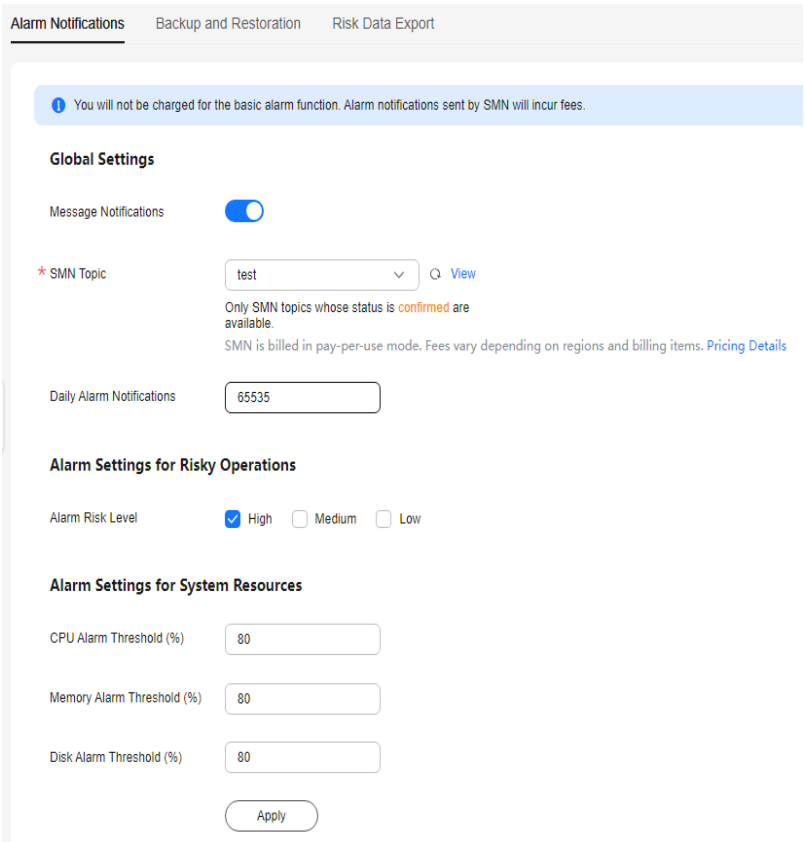


Table 7-2 Alarm notification parameters

Parameter	Description	Example Value
Message Notifications	Enables or disables notifications. Database audit alarm notifications are sent by SMN and will probably incur a small fee. See **SMN Pricing Details**. •  : disabled •  : enabled	
SMN Topic	• Select an existing topic from the drop-down list or click **View** to create a topic. For details, see **Creating a Topic**. • You can add multiple subscriptions to a topic and select multiple subscription endpoints (such as SMS messages and emails). For details, see **Adding a Subscription**. **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
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

Parameter	Description	Example Value
Disk Alarm Threshold (%)	Disk alarm threshold of an audit instance. When the threshold is exceeded, an alarm notification is generated.	80

Step 6 Click **Apply**.

----End

8 Viewing Monitoring Information

8.1 Viewing the System Monitoring

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

Prerequisites

- You have purchased 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 & Compliance** > **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 for which you want to view the system monitoring. The **Overview** page is displayed.

Step 5 Click the **System Monitoring** tab. The **System Monitoring** page is displayed.

Step 6 View the system monitoring information.

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

Figure 8-1 Viewing the system monitoring

----End

8.2 Viewing the Alarms

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

Prerequisites

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

Procedure

Step 1 **Log in to the management console.**

Step 2 Select a region, click  , and choose **Security & Compliance** > **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 **Alarm Monitoring** tab.

Step 5 View the alarm information, as shown in **Figure 8-2**. For details about related parameters, see **Table 8-1**.

Figure 8-2 Viewing the alarms

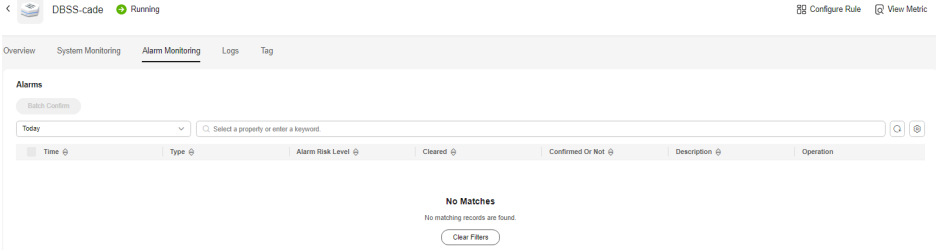


Table 8-1 Parameters of alarms

Parameter	Description
Time	Time when an alarm occurred.
Type	Alarm type. The options are as follows: • Audit traffic exceeds threshold • CPU exceptions • Memory exceptions • Disk exceptions • Insufficient audit log storage • Log backup to OBS failed • Agent exceptions
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** from the drop-down list, 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.

NOTE

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

9 Backing Up and Restoring Database Audit Logs

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

Prerequisites

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

Precautions

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

OBS Fine-grained Authorization

DBSS backup and restoration require OBS permissions. Users without IAM authorization permissions must be manually authorized by a user having the **Security Administrator** permission.

Step 1 **Log in to the management console**.

Step 2 Select a region, click  in the upper left corner, and choose **Management & Governance** > **Identity and Access Management**.

Step 3 In the navigation pane, choose **Permissions** > **Authorization**. Click **Create Custom Policy**.

Step 4 Configure policy parameters. Set **Policy Name** to **DBSS OBS Agency Access**. Set **Policy View** to **JSON**. The policy content is as follows:

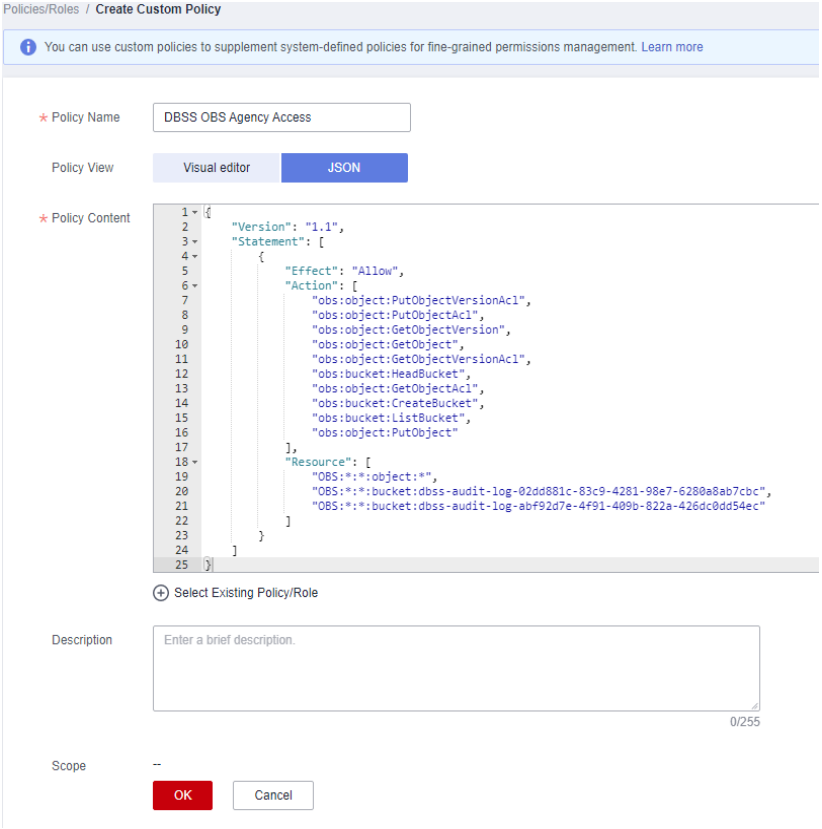
```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "obs:object:PutObjectVersionAcl",
            "obs:object:PutObjectAcl",
            "obs:object:GetObjectVersion",
```



```
            "obs:object:GetObject",
            "obs:object:GetObjectVersionAcl",
            "obs:bucket:HeadBucket",
            "obs:object:GetObjectAcl",
            "obs:bucket:CreateBucket",
            "obs:bucket:ListBucket",
            "obs:object:PutObject"
        ],
        "Resource": [
            "OBS:*:*:object:*",
            "OBS:*:*:bucket:OBS_Bucket_Name_1",
            "OBS:*:*:bucket:OBS_bucket_2" //You can add multiple buckets.
        ]
    }
  ]
}
```

See **Figure 9-1**. Click **OK**.

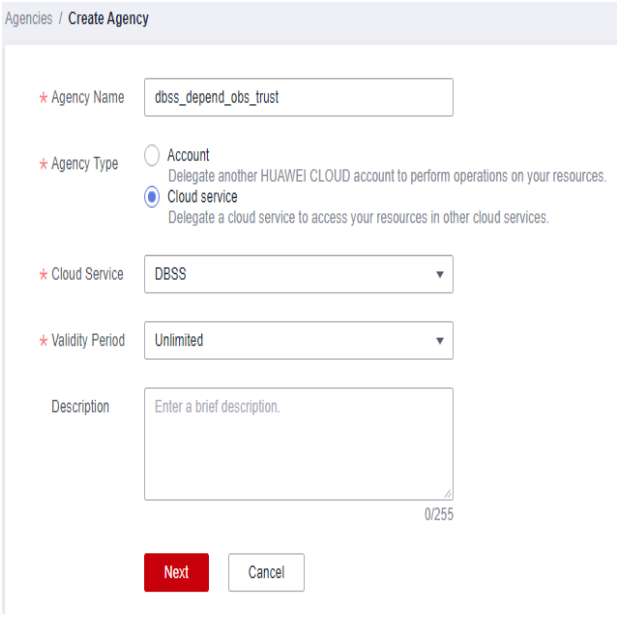
Figure 9-1 Creating a custom policy



Step 5 In the navigation pane, choose **Agencies** and then click **Create Agency** in the upper right corner.

Step 6 Configure agency parameters. Set **Agency Name** to **dbss_depend_obs_trust**. Set **Agency Type** to **Cloud service**. Set **Cloud Service** to **DBSS**. See **Figure 9-2**.

Figure 9-2 Creating an agency

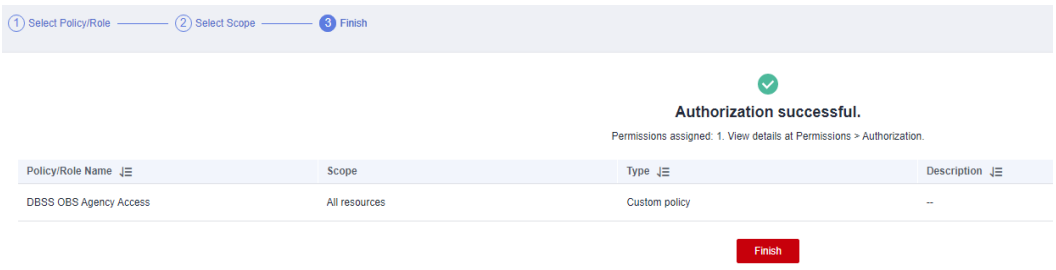


Step 7 Click **Next**. Select the custom policy created in **Step 4**, and add the permission **DBSS OBS Agency Access** to the agency **dbss_depend_obs_trust**, as shown in **Figure 9-3**. Click **Next** in the lower right corner.

Figure 9-3 Selecting a policy

Step 8 Set **Scope** to **All resources** and click **OK**. If the message in **Figure 9-4** is displayed, the authorization is successful. Click **Finish**. The authorization will take effect in about 15 minutes.

Figure 9-4 Authorization completed



----End

Automatically Backing Up Database Audit Logs

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 **Settings**.

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

Step 5 Click **Modify Automated Backup Settings**. In the displayed dialog box, set the auto backup parameters. **Table 9-1** describes the parameters.

Figure 9-5 Configure Automatic Backup dialog box

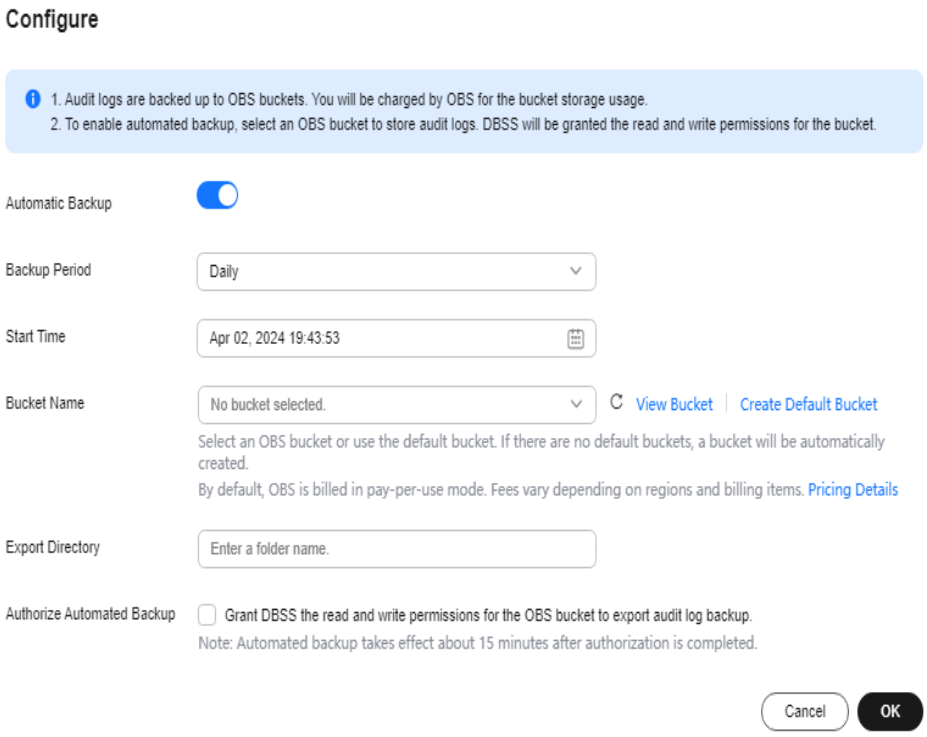


Table 9-1 Parameters

Parameter	Description	Example Value
Automatic Backup	Status of automatic backup • : enabled • : disabled	

Parameter	Description	Example Value
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
Bucket Name	Name of the OBS bucket used for backup. Its options are as follows: • Create Default Bucket • Select Bucket **NOTE** • If you click **Create Default Bucket**, you will be prompted to authorize OBS for exporting audit log backups. • Audit logs can be exported only to the bucket created by DBSS.	20f18-7a5a-4042
Export Directory	Directory for storing backup files in the OBS bucket.	test

Step 6 Click **OK**.

NOTE

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

----End

Restoring Database Audit Logs

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

NOTICE

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

Step 1 Log in to the management console.

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

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

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

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

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

----End

Exporting Risk Data

You can export the logs that record high-risk operations to OBS. An OBS bucket will be automatically created to store these logs and will charge per use.

NOTE

Before you enable risk export, perform operations in **OBS Fine-grained Authorization**.

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.

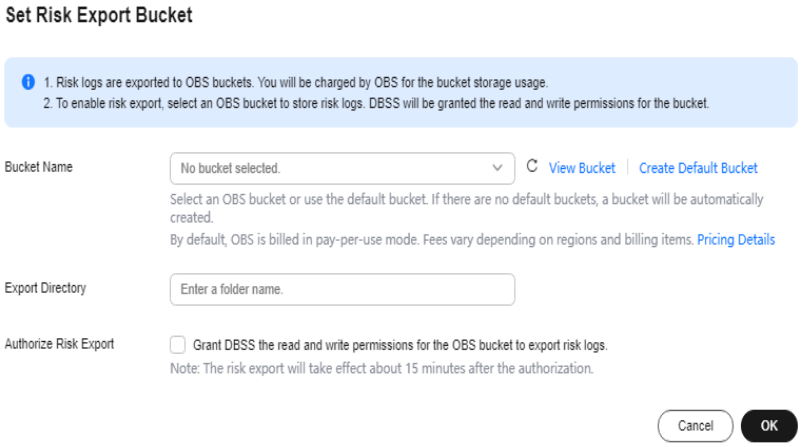
Step 3 In the navigation tree on the left, choose **Settings**.

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

Step 5 Click in the row of a database to export risk data. An OBS bucket will be automatically created to store risk logs.

- **Bucket Name**:Click **Create Default Bucket** or **Select Bucket**.
- **Export Directory**: Create a directory for storing risk files in the OBS bucket.

Figure 9-6 Automatically creating an OBS bucket



----End

10 Other Operations

10.1 Managing Database Audit Instances

After purchasing a database audit instance, you can view, enable, restart, and disable the instance.

Prerequisites

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

Viewing the Instance

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 **Instances**.

Step 4 View the database audit instances information. For details about related parameters, see **Table 10-1**.

NOTE

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

Table 10-1 Parameters

Parameter	Description
Instance Name/ID	Name and ID of an instance. Instance ID is automatically generated.

Parameter	Description
Specifications	Edition of an instance
Billing Mode	Billing mode (yearly/monthly) and expiration time of the instance
Version	Version of database audit 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
Operation	Operations can be performed on the instance. The options are as follows: • Configure Rules • Enable • Disable • Restart • View Details • View Metric • 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

10.2 Viewing the Instance Overview

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

Prerequisites

You have purchased 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 & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 View the basic information, network settings, and associated databases about the instance. For details about related parameters, see **Table 10-2**.

Table 10-2 Parameters of the instance overview

Category	Parameter	Description
Basic Info	Name	Name of an instance. You can click next to **Name** to change it.
	Version	Version of an instance
	Remarks	Remarks about an instance. Click next to remarks to modify it.
	Billing Mode	Billing mode of an instance
	Created	Time when an instance is created
Network Settings	VPC	VPC where an instance resides
	Security Group	Security group where an instance resides
	Subnet	Subnet where an instance resides
	Private IP Address	IP address of an instance
Associated Database	-	Database information associated with an instance Click **Manage Database**, and the **Databases** page is displayed. For details about how to add a database, see **Step 1: Add a Database**.

----End

10.3 Managing Databases and Agents

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

Prerequisites

- You have purchased 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 & Compliance** > **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 10-3**.

NOTE

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

Table 10-3 Parameters

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

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

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

Step 5 Click ⌄ on the left of the database to expand the agent details. For details about related parameters, see **Table 10-4**.

Table 10-4 Parameters of an agent

Parameter	Description
Agent ID	Agent ID, which is automatically generated
Installing Node Type	Type of the installing node. The options are **Database** and **Application**.
Installing Node IP Address	IP address of the node where an agent is installed
OS	Agent OS
Audited NIC Name	NIC name of an installing node
CPU Threshold (%)	CPU threshold of the installing node. The default value is **80**. **NOTE** The agent on a node will stop working if the CPU usage of the node exceeds this threshold. You can scale up CPU resources to avoid this problem.
Memory Threshold (%)	Memory threshold of the installing node. The default value is **80**. **NOTE** The agent on a node will stop working if the memory usage of the node exceeds this threshold. You can scale up memory resources to avoid this problem.
General	Whether an agent is a general-purpose agent.
SHA256Sum	Verification value of the agent installation package.
Status	Running status of the installing node

NOTE

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

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

----End

10.4 Uninstalling an Agent

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

Prerequisites

You have installed an agent on the desired node.

Uninstalling the Agent from a Linux OS

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

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

cd *directory containing the decompressed agent installation package*

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

ll

- If you do, go to **Step 4**.
- If you do not, perform the following operations:
  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

Uninstalling the Agent from a Windows OS

Step 1 Enter the directory where the agent installation file is stored.

Step 2 Double-click the **uninstall.bat** file to uninstall the agent.

Step 3 Verify the agent has been uninstalled.

1. Open the Task Manager and verify the dbss_audit_agent process is stopped.
2. Verify the entire agent installation directory has been deleted.

----End

10.5 Management an Audit Scope

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

Prerequisites

- You have purchased 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 & Compliance** > **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 10-5**.

NOTE

Enter the key word of an audit scope to search.

Table 10-5 Parameters

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

NOTE

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

- Enable

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

10.6 Viewing Information About SQL Injection Detection

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

Prerequisites

- You have purchased 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 & Compliance** > **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. For details about related parameters, see **Table 10-6**.

NOTE

- Select a risk severity from the **All risk severities** drop-down list in the upper right corner of the list, or enter a key word of an SQL injection rule name to search.
- Click **Set Priority** in the **Operation** column of an SQL injection rule to change its priority.

Table 10-6 Parameters

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

Parameter	Description
Operation	Operations on an SQL injection rule. The options are as follows: • **Set Priority** • **Disable** • **Edit** • **Delete**

----End

10.7 Managing Risky Operations

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

Prerequisites

- You have purchased 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 & Compliance** > **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 In the **Operation** column of the desired risky operation, click **Set Priority**.

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 & Compliance** > **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 10-7**.

NOTE

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

Table 10-7 Parameters

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

NOTE

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

- Enable

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

- Edit

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

- Disable

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

- Delete

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

----End

10.8 Managing Privacy Data Protection Rules

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

Prerequisites

You have purchased 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 & Compliance** > **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 10-8**.

NOTE

- **Store Result Set**

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

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

  Note: The result set storage supports only the database audit in agent mode.

- **Mask Privacy Data**

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

Table 10-8 Masking rule parameters

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

Parameter	Description
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

10.9 Managing Audit Reports

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

Prerequisites

- You have purchased 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 & 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 report information you want to view.

Step 5 Viewing reports

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 & 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 report template you want to view.

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

Step 6 View the report template.

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

10.10 Managing Backup Audit Logs

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

Prerequisites

- You have purchased 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 & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

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

Step 6 View the backup audit log information. For details about related parameters, see **Table 10-9**.

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

Table 10-9 Parameters of audit logs

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

NOTE

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

----End

10.11 Viewing Operation Logs

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

Prerequisites

You have purchased 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 & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

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

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

NOTE

You can select last 30 minutes, last 1 hour, 24 hours, last 7 days, last 30 days, or a custom time range.

Table 10-10 Parameters

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

----End

11 Key Operations Recorded by CTS

11.1 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 & Governance** > **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.

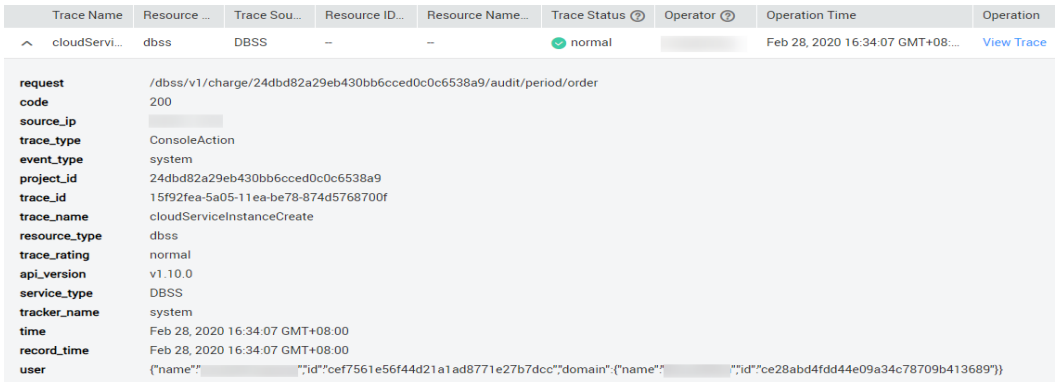
The following four filters are available:

- **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**.

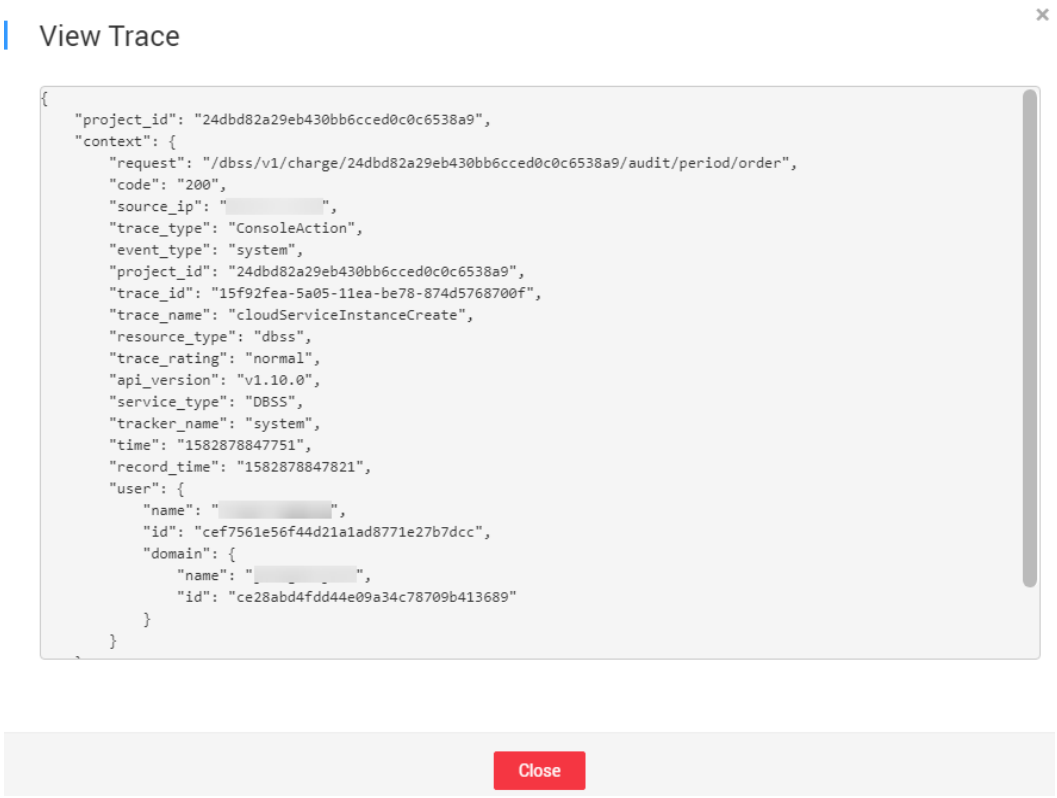
Step 6 Click  on the left of a trace to expand its details.

Figure 11-1 Expanding trace details



Step 7 Click **View Trace** in the **Operation** column. On the displayed **View Trace** dialog box shown in **Figure 11-2**, the trace structure details are displayed.

Figure 11-2 Viewing a trace



----End

11.2 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 11-1 lists DBSS operations recorded by CTS.

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

Operation	Resource Type	Trace Name
Creating an instance	dbss	createInstance
Deleting an instance	dbss	deleteInstance
Starting an instance	dbss	startInstance
Stopping an instance	dbss	stopInstance
Restarting an instance	dbss	rebootInstance
Changing the instance status	dbss	cloudServiceInstanceStatus
Creating a yearly/monthly instance	dbss	cloudServiceInstanceCreate
Changing the instance metadata	dbss	updateMetaData

12 Monitoring

12.1 DBSS Monitored Metrics

Description

This section describes monitored metrics reported by DBSS to Cloud Eye as well as their namespaces and dimensions. You can use console or APIs provided by Cloud Eye to query the metrics of the monitored objects and alarms generated for DBSS.

Namespace

SYS.DBSS

NOTE

A namespace is an abstract collection of resources and objects. Multiple namespaces can be created in a single cluster with the data isolated from each other. This enables namespaces to share the same cluster services without affecting each other.

Metrics

Table 12-1 DBSS metrics

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
cpu_util	CPU Usage	CPU consumed by the monitored object Unit: % Collection method: 100% minus idle CPU usage percentage	0 to 100% Value type: Float	Database audit instance	1 minute
mem_util	Memory Usage	Memory usage of the monitored object Unit: % Collection method: 100% minus idle memory percentage	0 to 100% Value type: Float	Database audit instance	1 minute
disk_util	Disk usage	Disk usage of the monitored object Unit: % Collection method: 100% minus idle disk space percentage	0 to 100% Value type: Float	Database audit instance	1 minute
hx_process_status	Protected Instance Process Status	The process status of a protected instance. **NOTE** This protected instance is no longer maintained.	0/1 • **0**: The process status is abnormal. • **1**: The process status is normal.	Database audit instance	1 minute

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
hx_port_stats	Protected Instance Port Status	The port status of a protected instance. **NOTE** This protected instance is no longer maintained.	0/1 • **0**: The port status is abnormal. • **1**: The port status is normal.	Database audit instance	1 minute
hx_proxy_num	Protected Instance Agents	The number of agents of a protected instance. **NOTE** This protected instance is no longer maintained.	≥0	Database audit instance	1 minute
hx_proxy_status	Protected Instance Agent Status	The agent status of a protected instance. **NOTE** This protected instance is no longer maintained.	0/1 • **0**: The agent status is abnormal. • **1**: The agent status is normal.	Database audit instance	1 minute
hx_qps	Queries per Second	The number of queries per second on the instance. **NOTE** This protected instance is no longer maintained.	≥0	Database audit instance	1 minute

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
hx_rps	Requests per Second	The number of requests per second on the instance. **NOTE** This protected instance is no longer maintained.	≥0	Database audit instance	1 minute
hx_active_connections_num	Protected Instance Active Connections	The number of active connections of a protected instance. **NOTE** This protected instance is no longer maintained.	≥0	Database audit instance	1 minute

12.2 Configuring Alarm Monitoring Rules

You can set DBSS alarm rules to customize the monitored objects and notification policies, and set parameters such as the alarm rule name, monitored object, metric, threshold, monitoring scope, and whether to send notifications. This helps you learn the database security status in a timely manner.

Prerequisites

You have purchased a DBSS instance.

Procedure

Step 1 Log in to the management console.

Step 2 Click ☰ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

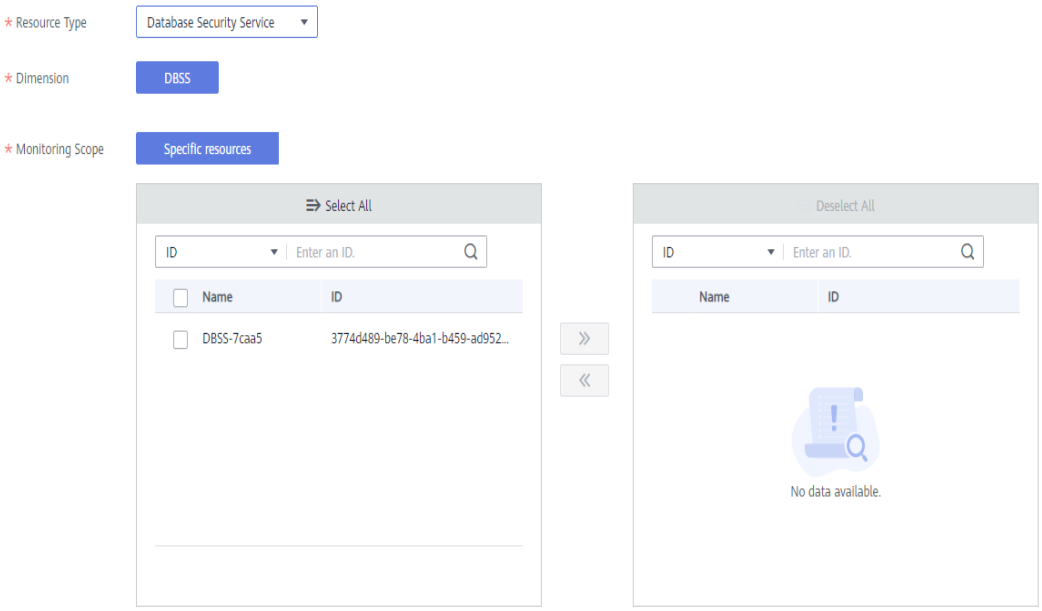
Step 3 In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.

Step 4 In the upper right corner of the page, click **Create Alarm Rule**.

Step 5 Set the alarm rule name and select an enterprise project to which the alarm rule belongs.

Step 6 Select **Database Security Service** from the **Resource Type** drop-down list, and select a dimension, monitoring scope, alarm template, and whether to send a notification. **Figure 12-1** shows an example.

Figure 12-1 Configuring a DBSS alarm monitoring rule



Step 7 Click **Create**. In the displayed dialog box, click **OK**.

----End

12.3 Viewing Monitoring Metrics

You can view DBSS metrics on the management console to learn about the database security status in a timely manner and configure protection policies based on the metrics.

Prerequisites

DBSS alarm rules have been configured in Cloud Eye. For more details, see **Configuring Alarm Monitoring Rules**.

Procedures

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 3 In the navigation pane on the left, choose **Cloud Service Monitoring** > **Database Security Service**.

Step 4 In the row containing the dedicated DBSS instance, click **View Metric** in the **Operation** column.

----End

13 Shared VPC

Scenario

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.

Creating a VPC

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner, choose **Management & Governance** > **Resource Access Manager**, and go to the resource access management page.

Step 3 Choose **Shared by Me** > **Resource Shares**.

Step 4 Click **Create Resource Share** in the upper right corner.

Step 5 Set resource type to **vpc:subnet**, choose the corresponding region, and select VPCs to be shared. Click **Next: Associate Permissions**.

Step 6 Associate a RAM managed permission with each resource type on the displayed page. Then, click **Next: Grant Access to Principals** in the lower right corner.

Step 7 Specify the principals that you want to have access to the resources on the displayed page. Then, click **Next: Confirm** in the lower right corner.

Table 13-1 Parameter descriptions

Parameter	Description
Principal Type	• Organization For details about how to create an organization, see . **NOTE** If you have not enabled resource sharing with organizations, this parameter cannot be set to **Organization**. For details, see . • Huawei Cloud account ID

Step 8 Check the configurations and click **OK**.

----End

Using a VPC

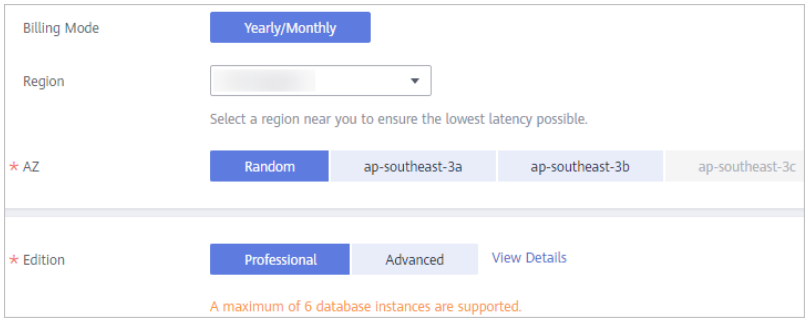
Step 1 **Log in to the management console.**

Step 2 Click ☰ and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

Step 4 Select a region, a project, an AZ, and an edition.

Figure 13-1 Selecting an AZ and an edition



Select an enterprise project. The DBSS you purchase will be put under this project. Billing and permissions management are performed based on enterprise projects.

Table 13-2 describes the database audit editions.

Table 13-2 Database audit editions

Edition	Maximum Databases	System Resource	Performance
Professional	6	• CPU: 8 vCPUs • Memory: 32 GB • Hard disk: 1,084 GB	• Peak QPS: 6,000 queries/second • Database load rate: 7.2 million statements/hour • Stores 600 million online SQL statements. • Stores 10 billion archived SQL statements.
Advanced	30	• CPU: 16 vCPUs • Memory: 64 GB • Hard disk: 2,108 GB	• Peak QPS: 30,000 queries/second • Database load rate: 10.8 million records/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 purchase a new one.
- The cloud native edition can be purchased only on the RDS console.
- The table above lists the system resources consumed by a database audit instance. Ensure your system has the required configurations before purchasing database audit instances.
- Online SQL statements are counted based on the assumption that the capacity of an SQL statement is 1 KB.

Step 5 Select the VPC and subnet for database audit. For details about related parameters, see **Table 13-3**.

Figure 13-2 Setting database audit parameters

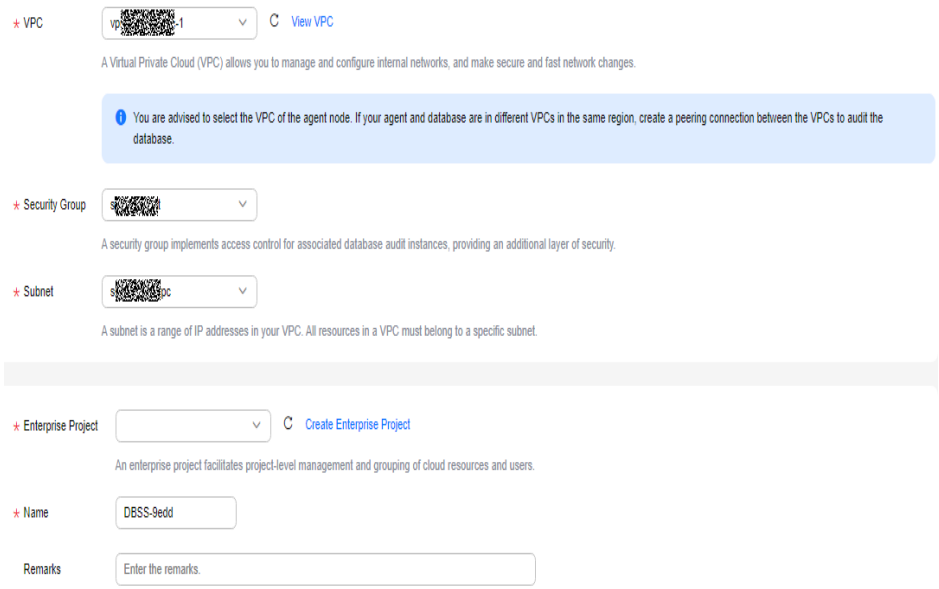


Table 13-3 Database audit instance parameters

Parameter	Description
VPC	You can select an existing VPC, or click **View VPC** to create one on the VPC console. **NOTE** • Select the VPC of the node (application or database side) where you plan to install the agent. For more information, see **How Do I Determine Where to Install an Agent?** • To change the VPC of a DBSS instance, unsubscribe from it and purchase a new one. For more information about VPC, see *Virtual Private Cloud User Guide*.
Security Group	You can select an existing security group in the region or create a security group on the VPC console. 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*.
Subnet	You can select a subnet configured in the VPC or create a subnet on the VPC console.
Name	Instance name

----End

14 Permission Control

14.1 Creating a User and Granting Permissions

You can use **IAM** to implement refined permission control for DBSS resources. To be specific, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to DBSS resources.
- Grant only the permissions required for users to perform a task.
- Entrust your Huawei Cloud account or cloud service to perform professional and efficient O&M on your DBSS resources.

If your Huawei Cloud account does not require individual IAM users, skip this chapter.

This section describes the procedure for granting permissions (see **Figure 14-1**).

Prerequisites

Before authorizing permissions to a user group, you need to know which DBSS permissions can be added to the user group. **Table 14-1** describes the policy details. For details about system permissions supported by DBSS, see **DBSS Permissions**.

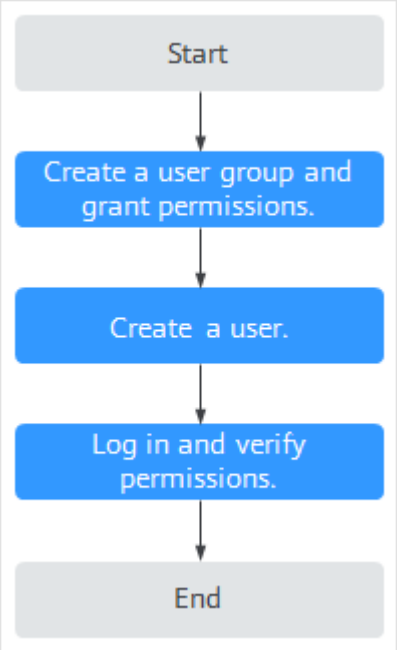
Table 14-1 System permissions

Role/Policy Name	Description	Type	Dependency
DBSS Audit Administrator	DBSS audit administrator, who has the permissions to check DBSS security logs.	System-defined role	None

Role/Policy Name	Description	Type	Dependency
DBSS FullAccess	Full permissions for DBSS	System-defined policy	
DBSS ReadOnlyAccess	Read-only permissions for DBSS. Users granted these permissions can only view this service and cannot configure resources in it.	System-defined policy	

Process Flow

Figure 14-1 Process for granting permissions



1. **Create a user group and assign permissions**.

   Create a user group on the IAM console and grant the user group the **DBSS Security Administrator** permission for DBSS.

2. **Create a user and add it to a user group**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

Log in to the DBSS console by using the created user, and verify that the user only has read permissions for DBSS.

Example verification method: Try starting or stopping an instance. If a message indicating Insufficient permissions are displayed, the **DBSS Security Administrator** role has taken effect.

14.2 DBSS Custom Policies

Custom policies can be created to supplement the system-defined policies of DBSS. For the actions supported for custom policies, see **DBSS Permissions and Supported Actions**.

Examples of Custom Policies

- Example 1: Allowing a user to query the database audit list

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "dbss:auditInstance:list"
         ]
      }
   ]
}
```

- Example 2: Denying database audit instance deletion

  A deny policy must be used together with other policies. If the policies assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

  The following method can be used if you need to assign permissions of the **DBSS FullAccess** policy to a user but also forbid the user from deleting database audit instances. Create a custom policy to disallow audit instance deletion and assign both policies to the group the user belongs to. Then the user can perform all operations on DBSS except deleting database audit instances. The following is an example of a deny policy:

```
{
      "Version": "1.1",
      "Statement": [
            {
                  "Action": [
                        "dbss:auditInstance:delete"
                  ],
                  "Effect": "Deny"
            }
      ]
}
```

- Example 3: Defining permissions for multiple services in a policy

  A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
```



```
            "dbss:defendInstance:eipOperate",
            "dbss:auditInstance:getSpecification"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "hss:accountCracks:unblock",
            "hss:commonIPs:set"
        ]
    }
  ]
}
```

14.3 DBSS Permissions and Supported Actions

This section describes fine-grained permissions management for your DBSS resources. If your Huawei Cloud account does not need individual IAM users, you can skip this section.

By default, new IAM users do not have any permissions. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added. Users inherit permissions from the groups and can perform operations on cloud services as allowed by the permissions.

Supported Actions

DBSS provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control. Operations supported by policies are specific to APIs. The following are common concepts related to policies:

- Permissions: Statements in a policy that allow or deny certain operations.
- Actions: Specific operations that are allowed or denied.
- Related actions: Actions on which a specific action depends to take effect. When assigning permissions for the action to a user, you also need to assign permissions for the related actions.

Table 14-2 lists the API actions supported by DBSS.

Table 14-2 Actions

Permission	Action
Query the list of database audit instances	dbss:auditInstance:list
Obtain available specifications of database audit instances	dbss:auditInstance:getSpecification
View database protection instance details	dbss:defendInstance:list
Bind or unbind an EIP	dbss:defendInstance:eipOperate

Permission	Action
Delete a database protection instance	dbss:defendInstance:delete
Delete a database audit instance	dbss:auditInstance:delete
Purchase database protection instances on demand	dbss:defendInstance:createOnDemand
Purchase database audit instances on demand	dbss:auditInstance:createOnDemand
Purchase a database protection instance on demand	dbss:defendInstance:createOnOrder
Purchase database audit instances on demand	dbss:auditInstance:createOnOrder
Restart a database protection instance	dbss:defendInstance:reboot
Start a database audit instance	dbss:auditInstance:start
Stop a database audit instance	dbss:auditInstance:stop
Restart a database audit instance	dbss:auditInstance:reboot
Start a database protection instance	dbss:defendInstance:start
Stop a database protection instance	dbss:defendInstance:stop

14.4 Configuring FullAccess Sensitive Permissions

The full permission set of DBSS involves sensitive permissions of some users, such as order payment, OBS bucket creation, file upload, agent creation, and agent permission setting.

These permissions have great impact on user assets. Therefore, they are not added to the preset permission set of the system but need to be manually added by users through description documents.

For details about sensitive permissions, see **Table 14-3**. The permission details are as follows:

```
"obs:bucket:CreateBucket",
"obs:object:PutObject",
"bss:order:pay",
"iam:agencies:createAgency",
"iam:permissions:grantRoleToAgency",
"iam:permissions:grantRoleToAgencyOnEnterpriseProject",
"iam:permissions:grantRoleToAgencyOnDomain",
"iam:permissions:grantRoleToAgencyOnProject"
```


Table 14-3 Description of sensitive permissions

Sensitive Permission Item	Application Scenario	Global Permission or Not	Workaround
obs:bucket:CreateBucket	• When the agent is deployed in the CCE scenario, if the OBS bucket where the data is to be uploaded does not exist, this API is called to create an OBS bucket. The name of the OBS bucket to which the data is uploaded is **dbss-audit-agent-{*project_id*}**. **project_id** indicates the ID of the project where the current instance is located. • In the backup and risk export scenarios, if the selected bucket does not exist, an OBS bucket will be created.	Yes	• If no permission application scenarios are involved, you do not need to configure this permission. • If permission application scenarios are involved, you can use an authorized account to create an OBS bucket in advance.
obs:object:PutObject	When the agent is deployed in the CCE scenario, the instance configuration information is uploaded to the OBS bucket.	Yes	• If no permission application scenarios are involved, you do not need to configure this permission. • If you need to use this permission, configure this permission to export instance information.

Sensitive Permission Item	Application Scenario	Global Permission or Not	Workaround
iam:agencies:createAgency iam:permissions:grantRoleToAgency iam:permissions:grantRoleToAgencyOnEnterpriseProject iam:permissions:grantRoleToAgencyOnDomain iam:permissions:grantRoleToAgencyOnProject	• In the backup and risk export scenarios, create an agent named **dbss_depend_obs_trust** and grant OBS operation permissions to the agent. • In the agent-free DWS scenarios, DWS creates an agent named **DWSAccessLTS** and grants it the permission to access LTS for uploading audit logs to the tenant's LTS. DBSS creates an agent named **dbss_dws_lts_trust** and grants the LTS access permission to the agent for downloading audit logs from LTS.	Yes	• If no permission application scenarios are involved, you do not need to configure this permission. • You can use an authorized account to enable this function.
bss:order:pay	Pay for the order when purchasing an audit instance.	No	• If no permission application scenarios are involved, you do not need to configure this permission. • You can use an authorized account to purchase instances in advance.

