# Database Security Service (DBSS)

# User Guide

| | |
|---|---|
| **Issue** | 01 |
| **Date** | 2025-06-26 |

**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.

**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

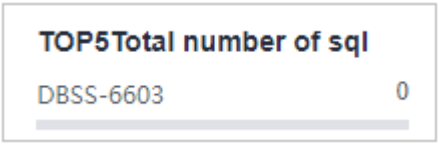
You can check the audit information about all instances by total number of SQLs, total number of risks, today's SQL, today's risks, and today's sessions.

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 1-1** 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 Using Agents

For a database whose type and version are listed in **Table 2-1**, you need to install an agent to enable the database audit.

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

| Database Type | Edition |
| --- | --- |
| MySQL | • 5.0, 5.1, 5.5, 5.6, 5.7<br>• 8.0 (8.0.11 and earlier)<br>• 8.0.30<br>• 8.0.35<br>• 8.1.0<br>• 8.2.0 |
| Oracle | • 11g<br>11.1.0.6.0, 11.2.0.1.0, 11.2.0.2.0, 11.2.0.3.0, and 11.2.0.4.0<br>• 12c<br>12.1.0.2.0, 12.2.0.1.0<br>• 19c |
| PostgreSQL | • 7.4<br>• 8.0, 8.1, 8.2, 8.3, 8.4<br>• 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6<br>• 10.0, 10.1, 10.2, 10.3, 10.4, 10.5<br>• 11<br>• 12<br>• 13<br>• 14 |
| SQL Server | • 2008<br>• 2012<br>• 2014<br>• 2016<br>• 2017 |
| GaussDB(for MySQL) | 8.0 |
| DWS | • 1.5 |
| DAMENG | DM8 |
| KINGBASE | V8 |
| SHENTONG | V7.0 |
| GBase 8a | V8.5 |
| GBase 8s | V8.8 |
| Gbase XDM Cluster | V8.0 |
| Greenplum | V6.0 |

| Database Type | Edition |
| --- | --- |
| HighGo | V6.0 |
| GaussDB | • 1.3 Enterprise Edition<br>• 1.4 Enterprise Edition<br>• 2.8 Enterprise Edition<br>• 3.223 Enterprise Edition |
| MongoDB | V5.0 |
| DDS | 4.0 |
| Hbase<br>(Supported by CTS instance 23.02.27.182148 and later versions) | • 1.3.1<br>• 2.2.3 |
| Hive | • 1.2.2<br>• 2.3.9<br>• 3.1.2<br>• 3.1.3 |
| MariaDB | 10.6 |
| TDSQL | 10.3.17.3.0 |
| Vastbase | G100 V2.2 |
| TiDB | • V4<br>• V5<br>• V6<br>• V7<br>• V8 |

**Figure 2-1** Procedure for quickly configuring database audit

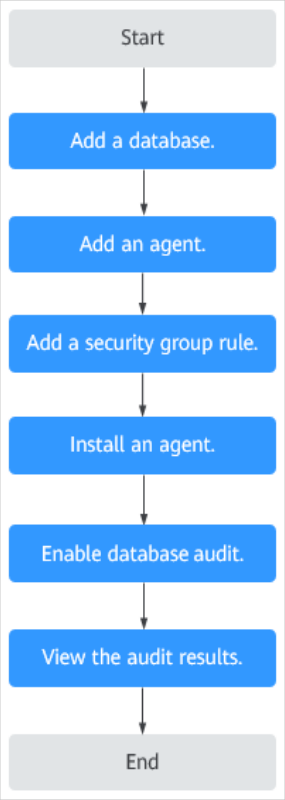



**Table 2-2** Procedure for quickly configuring database audit

| Step | Configuration | Description |
| --- | --- | --- |
| 1 | **Adding a Database** | Purchase database audit. Add a database to the database audit instance and enable audit for the database. |
| 2 | **Adding an Agent** | Select an agent add mode.<br>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. |
| 4 | **Installing an Agent (Linux OS)** | Download and then install the agent on the database or application based on the add mode you chose. |
| 5 | **Enabling Database Audit** | Enable database audit and connect the added database to the database audit instance. |

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

This section describes how to purchase DBSS. DBSS 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

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

### Prerequisites

Check whether the instance account has the required permissions. .

**NOTICE**

Ensure that the **DBSS System Administrator**, **VPC Administrator**, **ECS Administrator**, and **DBSS 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.
- **DBSS 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** > **Database Security Service**. The **Dashboard** page is displayed.

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

**Step 4** On the displayed page, set **Service Type** to **Database Audit Service**, and select the region, AZ, and other information as required.

Table 2-3 describes the database audit editions.

**Table 2-3** DBSS editions

| Edition | Maximum Databases | Performance |
| --- | --- | --- |
| Professional | 6 | • Peak QPS: 6,000 queries/second<br>• Database load rate: 7.2 million statements/hour<br>• Online SQL statement storage: 600 million statements |
| Advanced | 30 | • Peak QPS: 30,000 queries/second<br>• Database load rate: 10.8 million records/hour<br>• Online SQL statement storage: 1.5 billion 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.
- 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 2-2** and **Figure 2-3**. For details about related parameters, see **Table 2-4**.

**Figure 2-2** Network configuration


**Figure 2-3** Advanced configuration

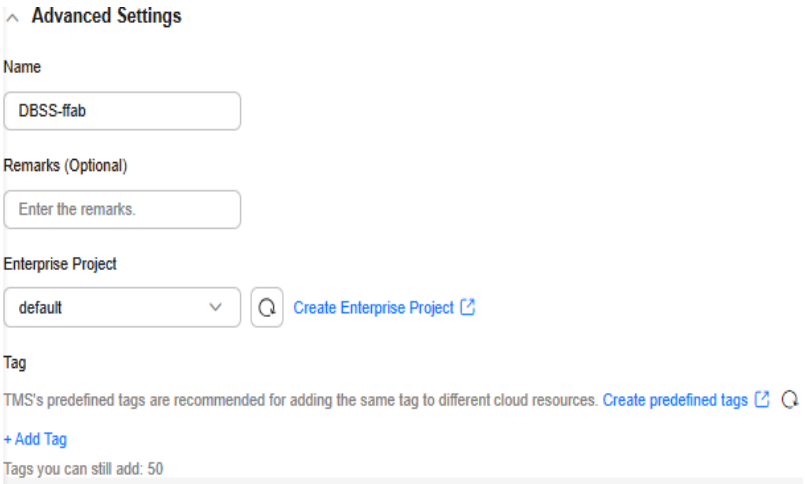


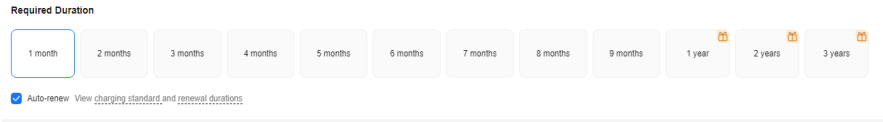
**Table 2-4** Database audit parameters

| Parameter | Description |
| --- | --- |
| VPC | You can select an existing VPC, or click **View VPC** to create one on the VPC console.<br>**NOTE**<br>• 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?**<br>• To change the VPC of a DBSS instance, unsubscribe from it and purchase a new one.<br>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.<br>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 |
| Remarks | You can add instance remarks. |
| Enterprise Project | This parameter is provided for enterprise users.<br>An enterprise project groups cloud resources, so you can manage resources and members by project. The default project is **default**.<br>Select an enterprise project from the drop-down list. For more information about enterprise projects, see ***Enterprise Management User Guide***. |
| Tag | (Optional) Identifier of the database audit instance. Adding tags helps you better identify and manage your database instances. A maximum of 50 tags for each instance<br>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 6** Set **Required Duration**. See **Figure 2-4**.

**Figure 2-4** 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 2-5** describes the auto-renewal period.

**Table 2-5** Auto-renewal period description

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

**Step 7** Confirm the configuration and click **Next**.

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

**Step 8** On the **Details** page, read the *Database Security Service Statement*, select **I have read and agree to the Database Security Service Statement**, and click **Submit**.

**Step 9** On the displayed page, select a payment method.

**Step 10** 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

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

## Adding a Database

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

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

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

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

**Step 5** Click **Add Database**.

**Figure 2-5** Adding a database


**Step 6** In the displayed dialog box, configure the database information.

**Table 2-6** Parameters

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

| Parameter | Description | Example Value |
| --- | --- | --- |
| Type | Supported database type. The options are as follows:<br>• MYSQL<br>• ORACLE<br>• PostgreSQL<br>• SQLServer<br>• DWS<br>• GaussDB(for MySQL)<br>• GaussDB<br>• DAMENG<br>• KINGBASE<br>• MongoDB<br>• Hbase<br>• SHENTONG<br>• GBase 8a<br>• GBase XDM Cluster<br>• Greenplum<br>• HighGo<br>• MariaDB<br>• Hive<br>• DDS<br>• GBase 8s<br>• TDSQL<br>• Vastbase<br>• TiDB<br>**NOTE**<br>• If **ORACLE** is selected, to make the audit settings take effect, restart the applications to be audited and log in to the database again.<br>• To use the Hive database to audit an MRS cluster, you need to disable SSL encryption on the server (for details, see **SSL Encryption Function Used by a Client**) and disable Kerberos authentication on the cluster purchase page. | MYSQL |
| Port | Port number of the database to be added | 3306 |

| Parameter | Description | Example Value |
| --- | --- | --- |
| Version | Supported database versions<br>• When **Type** is set to **MySQL**, the following versions are available:<br>– 5.0, 5.1, 5.5, 5.6, and 5.7<br>– 8.0 (8.0.11 and earlier)<br>– 8.0.30<br>– 8.0.35<br>– 8.1.0<br>– 8.2.0<br>• When **Type** is set to **ORACLE**, the following versions are available:<br>– 11g<br>– 12c<br>– 19c<br>• When **Type** is set to **PostgreSQL**, the following versions are available:<br>– 7.4<br>– 8.0, 8.1, 8.2, 8.3, and 8.4<br>– 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, and 9.6<br>– 10.0, 10.1, 10.2, 10.3, 10.4, and 10.5<br>– 11.0<br>– 12.0<br>– 13.0<br>– 14.0<br>• When **Type** is set to **SQLServer**, the following versions are available:<br>– 2008<br>– 2012<br>– 2014<br>– 2016<br>– 2017<br>• When **Type** is set to **DWS**, the following versions are available:<br>– 1.5<br>• When **Type** is set to **GaussDB(for MySQL)**, the following versions are available:<br>– When **Database Type** is set to **Self-built database**, you can select the **Mysql 8.0** version. | 5.0 |

| Parameter | Description | Example Value |
| --- | --- | --- |
| | – 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.<br>• When **Type** is set to **GaussDB**, the following version is available:<br>– 1.4 Enterprise Edition<br>– 1.3 Enterprise Edition<br>– 2.8 Enterprise Edition<br>– 3.223 Enterprise Edition<br>• When **Type** is set to **DAMENG**, the following version is available:<br>– DM8<br>• When **Type** is set to **KINGBASE**, the following version is available:<br>– V8<br>• When **Type** is set to **HBase**, the following versions are available:<br>– 1.3.1<br>– 2.2.3<br>• When **Type** is set to **SHENTONG**, the following version is available:<br>– 7.0<br>• When **Type** is set to **GBase 8a**, the following version is available:<br>– 8.5<br>• When **Type** is set to **GBase XDM Cluster**, the following version is available:<br>– 8.0<br>• When **Type** is set to **GBase 8s**, the following version is available:<br>– v8.8<br>• When **Type** is set to **Greenplum**, the following version is available:<br>– v6.0<br>• When **Type** is set to **HighGo**, the following version is available:<br>– v6.0<br>• When **Type** is set to **MongoDB**, the following version is available:<br>– v5.0 | |

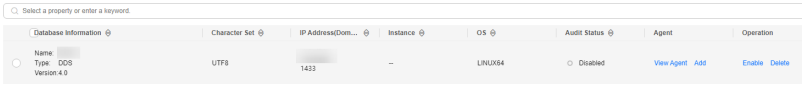
  

| Parameter | Description | Example Value |
| --- | --- | --- |
| | • When **Type** is set to **MariaDB**, the following version is available:<br>– 10.6<br>• When **Type** is set to **Hive**, the following versions are available:<br>– 1.2.2<br>– 2.3.9<br>– 3.1.2<br>– 3.1.3<br>• When **Type** is set to **TDSQL**, the following version is available:<br>– 10.3.17.3.0<br>• When **Type** is set to **Vastbase**, the following edition is available:<br>– G100 V2.2<br>• When **Type** is set to **TiDB**, the following editions are available:<br>– V4<br>– V5<br>– V6<br>– V7<br>– V8 | |
| Instance | Instance name of the database to be audited<br>**NOTE**<br>• If you do not configure the **Instance** field, database audit will audit all instances in the database.<br>• 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:<br>• UTF-8<br>• GBK | UTF-8 |
| OS | OS of the added database. The options are as follows:<br>• LINUX64<br>• WINDOWS64 | LINUX64 |

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

**Figure 2-6** Successfully adding a database




NOTE

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

**----End**

# 2.4 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.

NOTE

Currently, only the following types of databases support agent-free installation: After the database is added, you do not need to install the agent and can directly go to **Step 4: Add a Security Group Rule**.

- 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
- PostgreSQL
  - 14 (14.4 or later)
  - 13 (13.6 or later)
  - 12 (12.10 or later)
  - 11 (11.15 or later)
  - 9.6 (9.6.24 or later)
  - 9.5 (9.5.25 or later)
- RDS for MariaDB

## Prerequisites

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

## 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 2-7** and **Figure 2-8**.

  **Figure 2-7** One application connecting to multiple databases built on ECS/BMS

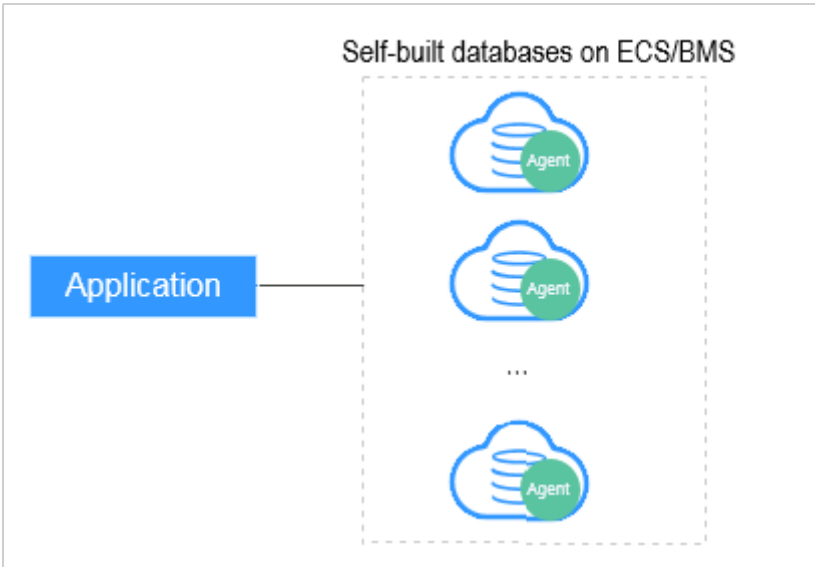
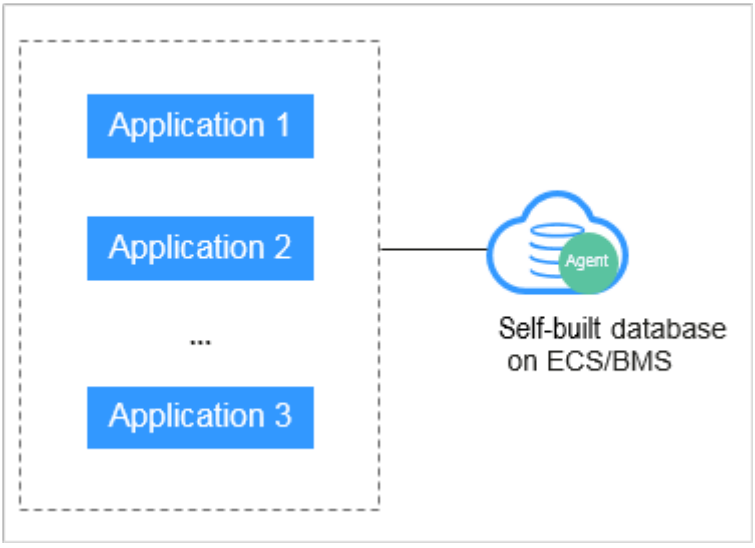
  
  

  **Figure 2-8** Multiple applications connecting to one database built on ECS/BMS

- Deploy DBSS for RDS databases. For details, see **Figure 2-9** and **Figure 2-10**.

**Figure 2-9** One application connecting to multiple RDS databases

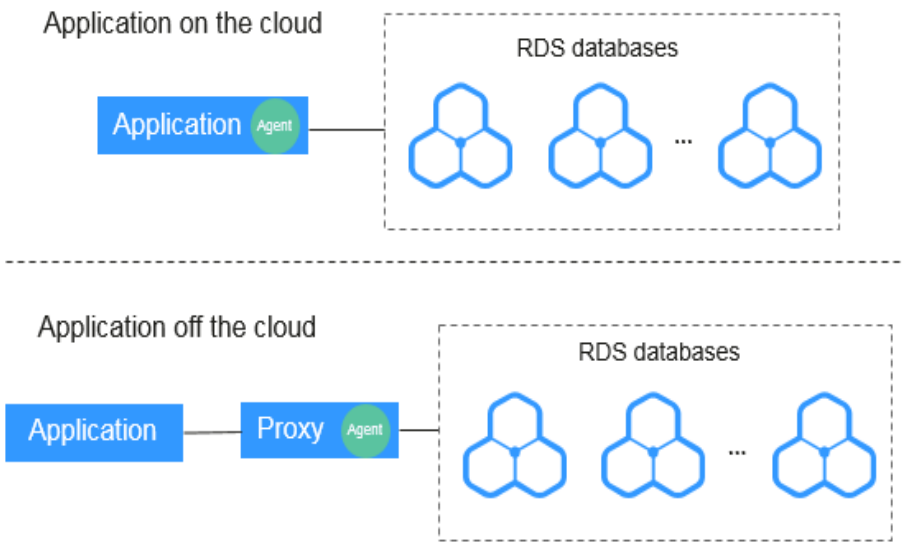



**Figure 2-10** Multiple applications connecting to one RDS database

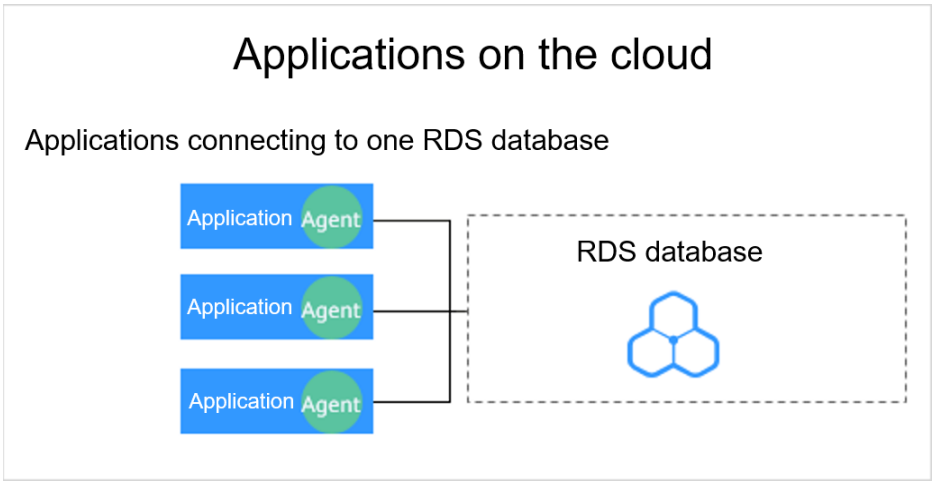



Table 2-7 provides more details.

**NOTICE**

- If your applications and databases (databases built on ECS/BMS) are deployed on the same node, add the agent on the database side.
- For easier O&M, you can deploy the database audit agent in a large number of containerized applications or databases in batches. This makes configuration quicker and easier. For details, see **Container-based database audit agent**

**Table 2-7** Agent locations

| Scenario | Where to Add the Agent | Audit Scope | Description |
| --- | --- | --- | --- |
| Databases built on ECS/BMS | Database or application | All access records of applications that have accessed the database | • Add the agent on the database side.<br>• 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.<br>• If an application connects to multiple RDS databases, add an agent on each of the databases. Set **Create an agent** for one of them and select **Select an existing agent** for the rest of them. For details, see **Selecting an existing agent**.<br>• If multiple applications connect to the same RDS database, add an agent on each of the databases. |
| | 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.<br>• **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** For details, see **Step 1**.

**Step 2** Log in to the management console.

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

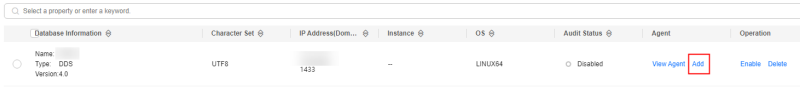
**Step 4** In the navigation tree on the left, choose **Databases**.

**Step 5** In the **Instance** drop-down list, select the instance whose agent is to be added.

**Step 6** In the **Agent** column of the desired database, click **Add**.

**Figure 2-11** Adding an agent




**Step 7** In the displayed dialog box, select an add mode, as shown in **Figure 2-12**. For details about related parameters, see **Table 2-8**.

**Figure 2-12** Adding an agent to a database

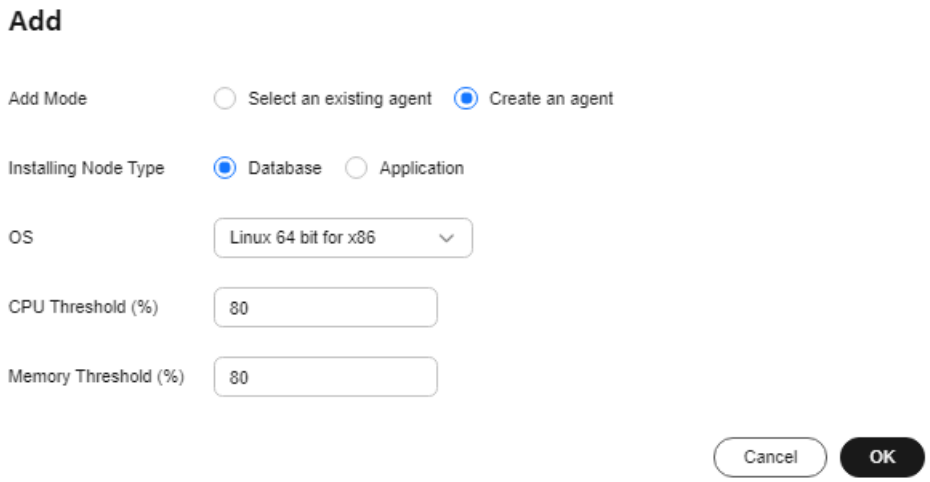



**Table 2-8** Parameters for adding an agent (user-built databases on ECS/BMS)

| Parameter | Description | Example Value |
| --- | --- | --- |
| Add Mode | Mode for adding an agent<br>• **Select an existing agent**<br>If an agent has been installed on a database connected to the same application as the desired database, select **Select an existing agent**.<br>• **Create an agent**<br>If no agent is available, select **Create an agent** to create one. | Create an agent |
| Database Name | Optional. If you select **Select an existing agent** for **Add Mode**, you need to select a database that already has an agent. | test1 |
| Agent ID | This parameter is mandatory when **Add Mode** is set to **Select an existing agent**.<br>Select an added agent ID of the instance. The agent ID is automatically generated by the system. | - |

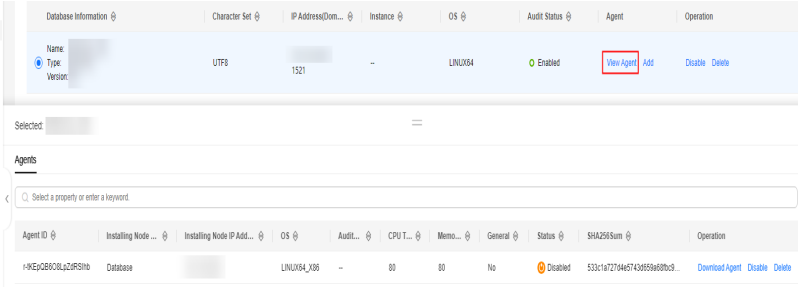
  

| Parameter | Description | Example Value |
| --- | --- | --- |
| Installing Node Type | This parameter is mandatory when **Add Mode** is set to **Create an agent**.<br>When auditing user-installed databases on ECS/BMS, select **Database** or **Application** for **Installing Node Type**. | Database |
| Installing Node IP Address | This parameter is mandatory if **Installing Node Type** is set to **Application**. IP address of the application node to be audited. You can enter only one IP address.<br>The IP address must be the internal IP address of the application node. IPv4 and IPv6 formats are both supported. | 192.168.1.1 |
| OS | This parameter is mandatory when **Add Mode** is set to **Create an agent**.<br>OS of the database to be audited. The value can be **LINUX64_x86 , LINUX64_Arm,** or **WINDOWS64**.<br>**NOTE**<br>Select an OS version based on the server architecture. | LINUX64_X86 |
| CPU Threshold (%) | Optional. CPU threshold of the application node to be audited. The default value is **80**. | 80 |
| Memory Threshold (%) | Optional. Memory threshold of the application node to be audited. The default value is **80**. | 80 |

**Step 8** Click **OK**.

**Step 9** In the **Agent** column of the desired database, click **View Agent**. In the **Agents** area, view information about the added agent.

**Figure 2-13** Successfully adding an agent



NOTE

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

**----End**

## Adding an Agent (RDS Databases)

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** For details, see **Step 1**.

**Step 2** Log in to the management console.

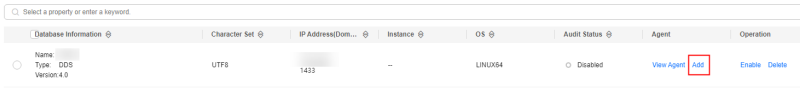
**Step 3** Click ☰ and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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

**Step 5** In the **Instance** drop-down list, select the instance whose agent is to be added.

**Step 6** In the **Agent** column of the desired database, click **Add**.

**Figure 2-14** Adding an agent




**Step 7** In the displayed dialog box, select an add mode, as shown in **Figure 2-15** and **Figure 2-16**. For details about related parameters, see **Table 2-9**.

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

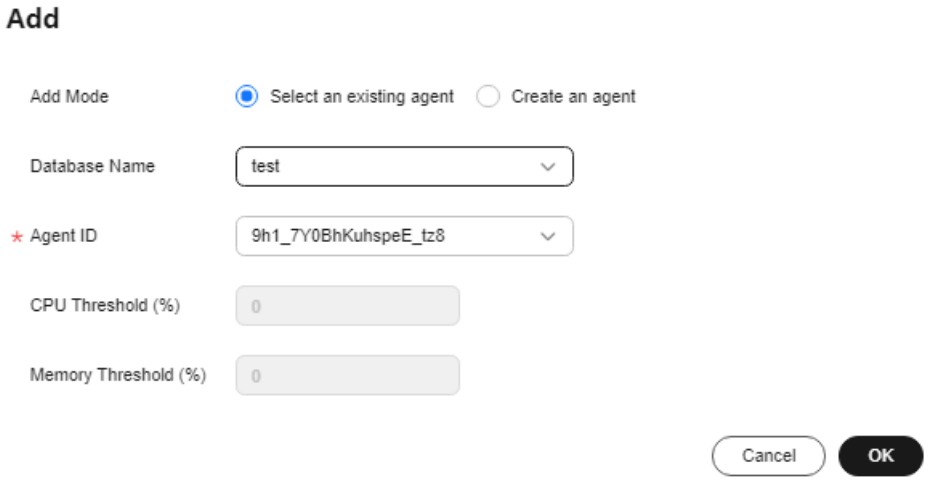
  For details about when you should select this option, see **When Should I Select an Existing Agent?**

  NOTE

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

**Figure 2-15** 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 2-16** Adding an agent to an application

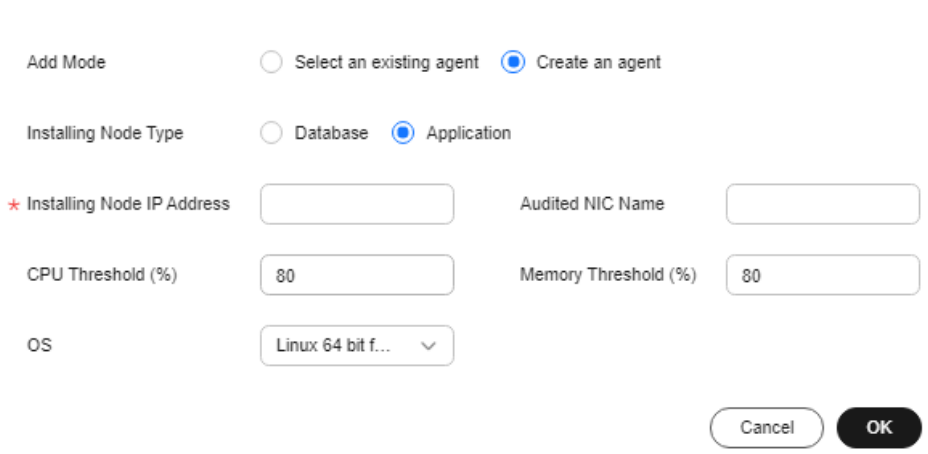


**Table 2-9** Parameters for adding an agent (RDS databases)

| Parameter | Description | Example Value |
| --- | --- | --- |
| Add Mode | Mode for adding an agent<br>• **Selecting an existing agent**<br>If an agent has been installed on a database connected to the same application as the desired database, select **Select an existing agent**.<br>• **Create an agent**<br>If no agent is available, select **Create an agent** to create one. | Create an agent |
| Database Name | Optional. If you select **Select an existing agent** for **Add Mode**, you need to select a database that already has an agent. | tesT |
| Agent ID | This parameter is mandatory when **Add Mode** is set to **Select an existing agent**.<br>Select an added agent ID of the instance. The agent ID is automatically generated by the system. | - |
| Installing Node Type | This parameter is mandatory when **Add Mode** is set to **Create an agent**.<br>To audit the RDS databases, select **Application**. | Application |
| Installing Node IP Address | This parameter is mandatory when **Installing Node Type** is set to **Application**. IP address of the application node to be audited. You can enter only one IP address.<br>The IP address must be the internal IP address of the application node. IPv4 and IPv6 formats are both supported.<br>**NOTICE**<br>To audit an RDS database connected to an off-cloud application, set this parameter to the IP address of the proxy. | 192.168.1.1 |
| Audited NIC Name | Optional. This parameter is configurable if **Installing Node Type** is set to **Application**.<br>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**.<br>CPU threshold of the application node to be audited. The default value is **80**.<br>**NOTICE**<br>If the CPU usage of a server exceeds the threshold, the agent on the server will stop running. | 80 |

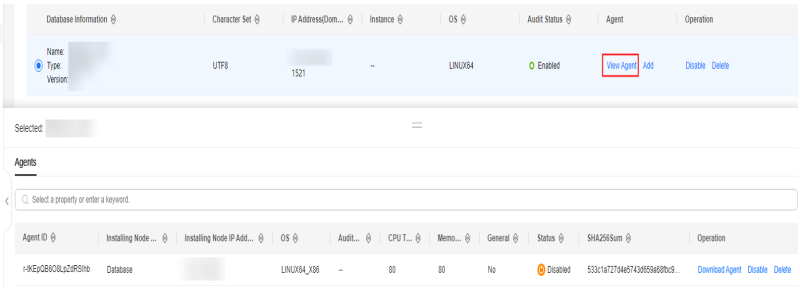
  

| Parameter | Description | Example Value |
| --- | --- | --- |
| Memory Threshold (%) | Optional. This parameter is configurable if **Installing Node Type** is set to **Application**.<br>Memory threshold of the application node to be audited. The default value is **80**.<br>**NOTICE**<br>If the memory 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**.<br>OS of the application node to be audited. The value can be **LINUX64_X86**, **LINUX64_ARM**, or **WINDOWS64**. | **LINUX64_X86** |

**Step 8** Click **OK**.

**Step 9** In the **Agent** column of the desired database, click **View Agent**. In the **Agents** area, view information about the added agent.

**Figure 2-17** Successfully adding an agent




NOTE

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

**----End**

## 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, as required by the add mode you chose.

**NOTE**

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

## Prerequisites

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

## Procedure

**Step 1** For details about how to add an agent, see **Step 2**.

**Step 2** Log in to the management console.

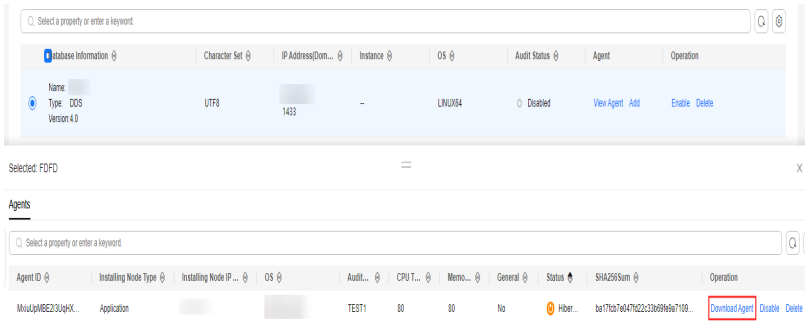
**Step 3** Click ☰ and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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

**Step 5** In the **Instance** drop-down list, select the instance whose agent is to be downloaded.

**Step 6** Locate the row that contains the target database, and click **View Agent** in the **Agent** column. In the **Agents** area, locate the row that contains the target agent and click **Download Agent** in the **Operation** column to download the agent installation package.

**Figure 2-18** 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

- 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 2-19** and **Figure 2-20**.

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

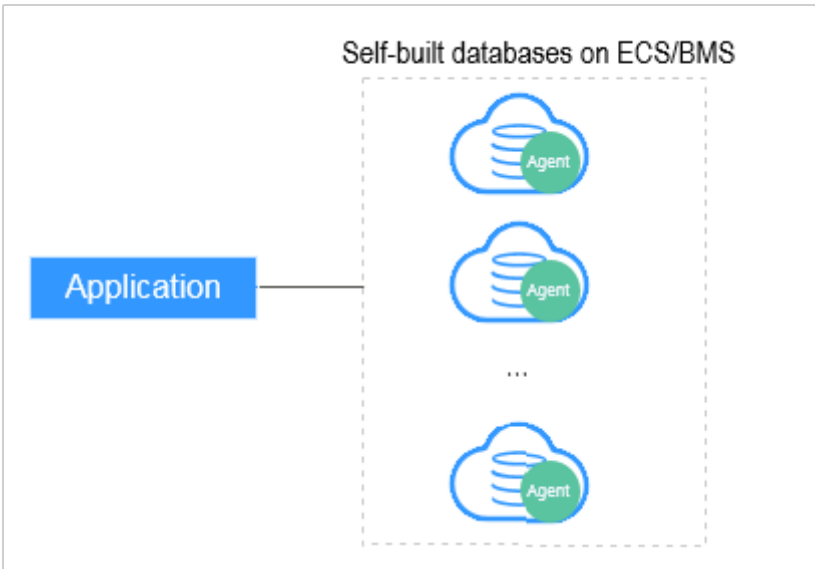
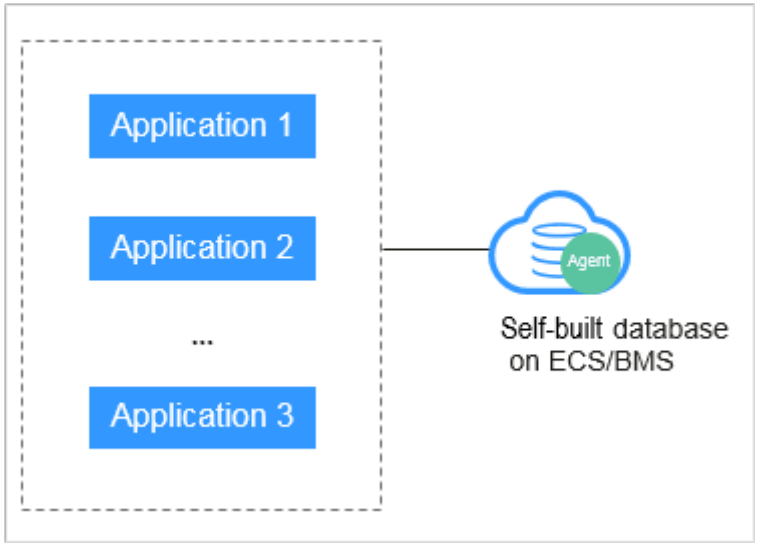


**Figure 2-20** Multiple applications connecting to one database built on ECS/BMS




- 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

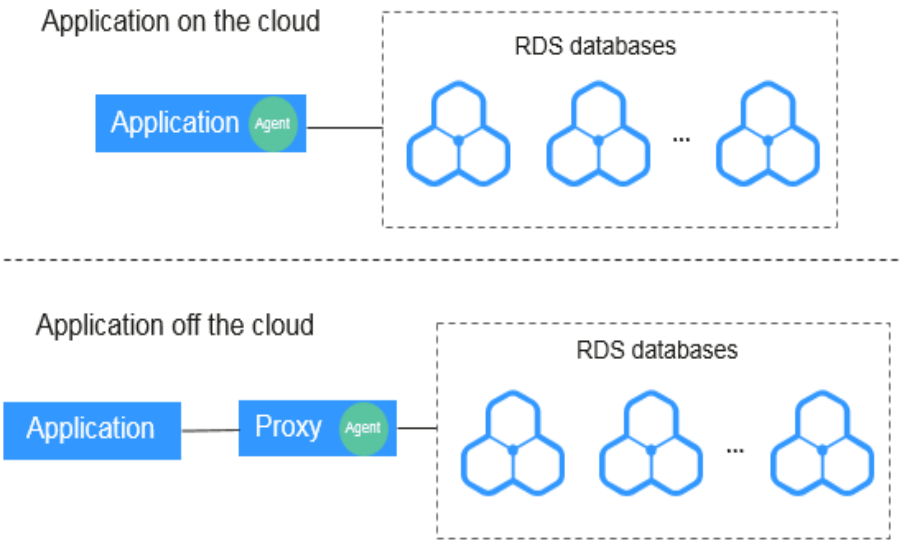


**Figure 2-22** Multiple applications connecting to one RDS database

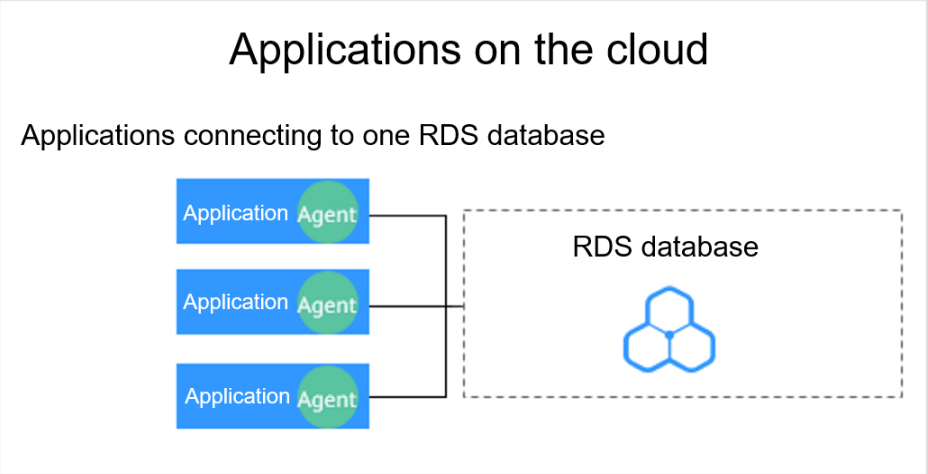



Table 2-10 describes where to install the agent in the preceding scenarios.

**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 2-10** 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.<br>• 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.<br>• 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** For details about how to add an agent, see **Step 2**.

**Step 2** For details about how to obtain the agent installation package of the Linux, see **Downloading an Agent**.

**Step 3** Upload the downloaded agent installation package **xxx.tar.gz** to the node (for example, using WinSCP).

**Step 4** Log in to the node as user **root** using SSH through a cross-platform remote access tool (for example, PuTTY).

**Step 5** 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                _9syBZIsBbeAhEFqE_hhD.tar.gz
[root@ecs-test agent]#
```

**Step 6** 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                _9syBZIsBbeAhEFqE_hhD.tar.gz
```

**Step 7** 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               _9syBZIsBbeAhEFqE_hhD]#
```

**Step 8** Run the following command to check whether you have the permission for executing the **install.sh** script:

**ll**

- If you do, go to **Step 9**.
- 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 9** 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

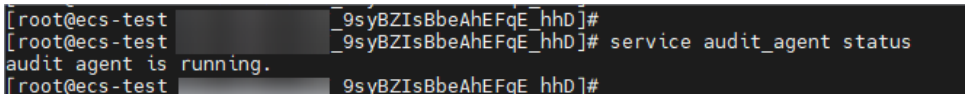
If the agent installation failed, ensure the OS version of the target node is supported and try again.

**Step 10** Run the following command to view the running status of the agent program:

**service audit_agent status**

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




audit agent is running.

**----End**

## 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

- 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 2-23** and **Figure 2-24**.

**Figure 2-23** One application connecting to multiple databases built on ECS/BMS

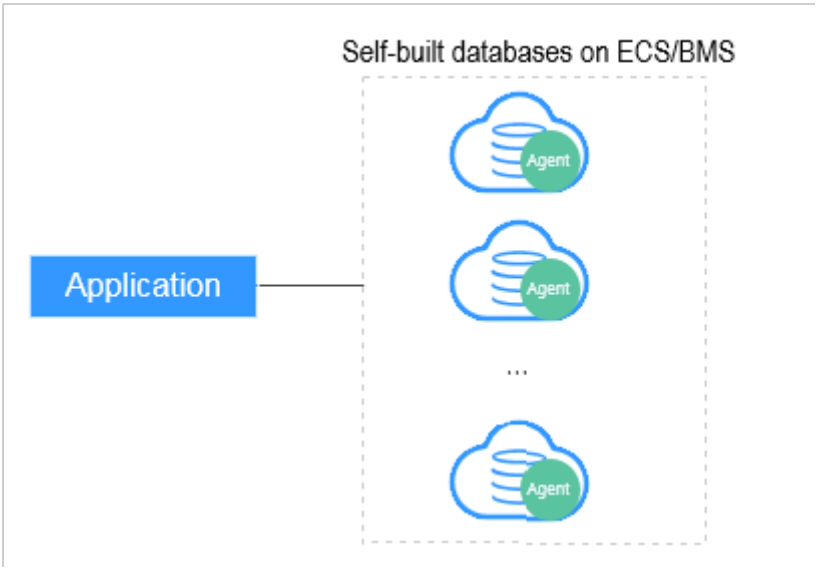
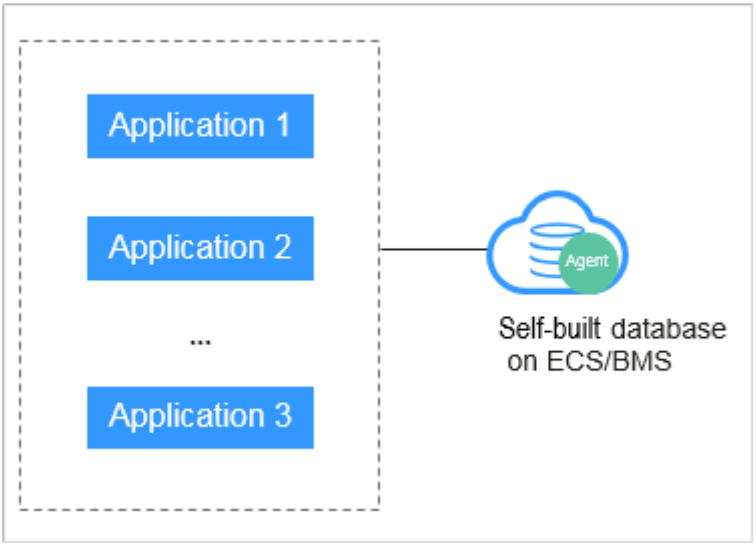



**Figure 2-24** Multiple applications connecting to one database built on ECS/BMS




- Deploy DBSS for RDS databases. For details, see **Figure 2-25** and **Figure 2-26**.

**Figure 2-25** One application connecting to multiple RDS databases

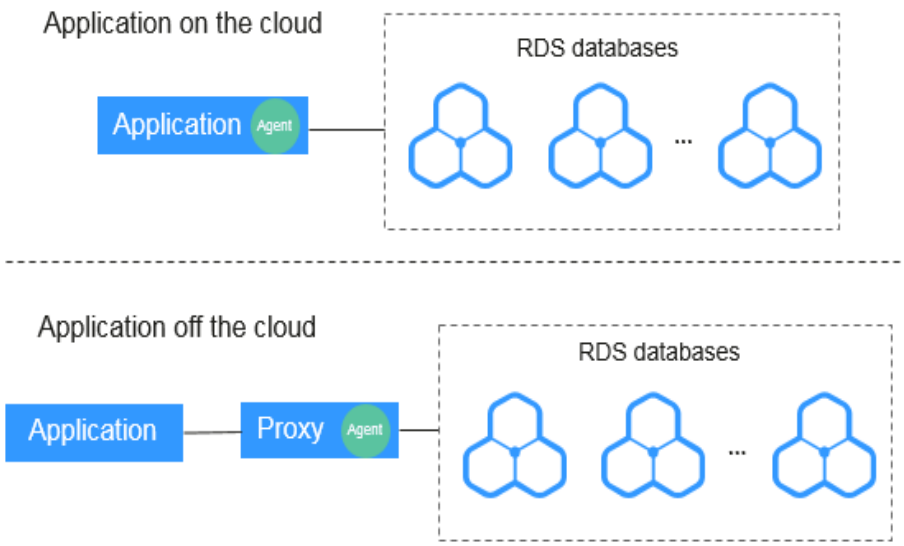



**Figure 2-26** Multiple applications connecting to one RDS database

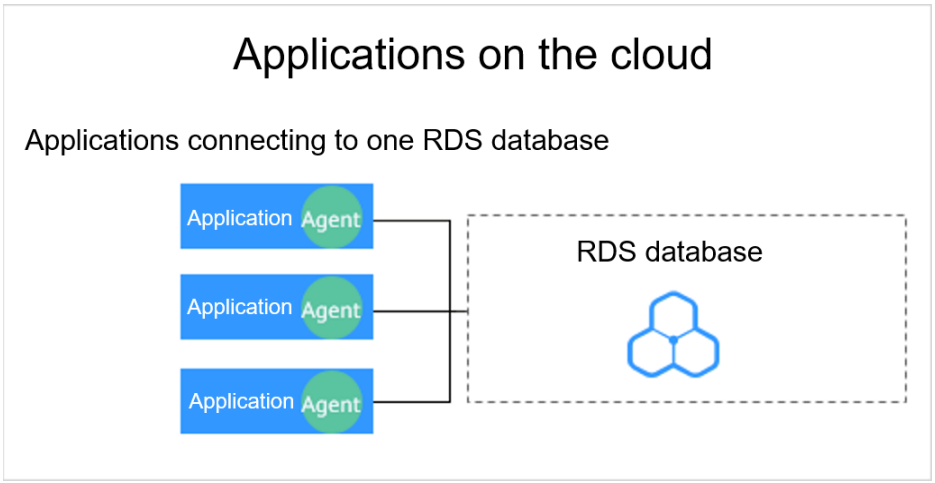



Table 2-11 describes where to install the agent in the preceding scenarios.

**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 | Node | Audit Scope | Precautions |
| --- | --- | --- | --- |
| Self-built database on ECS/BMS | Database | All access records of applications that have accessed the database | • Install the agent on the database side.<br>• 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.<br>• If multiple applications are connected to the same RDS database, the agent must be installed on all these applications. |
| RDS database | Proxy side (if applications are deployed off the cloud) | Only the access records between the proxy and database. Those between the applications and database cannot be audited. | Install the agent on the proxy side. |

## Installing an Agent

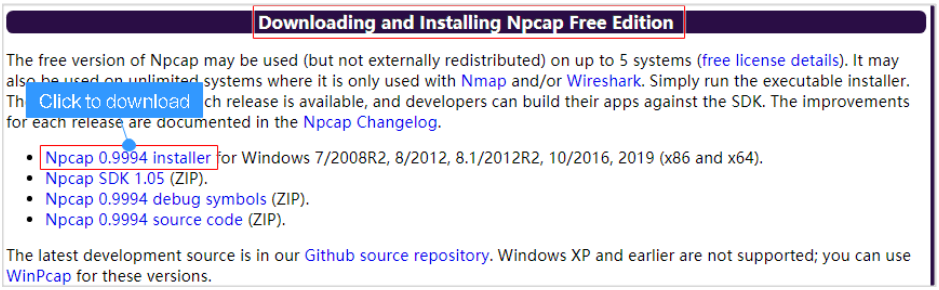
**Step 1** For details about how to add an agent, see **Step 2**.

**Step 2** Install Npcap on the Windows server.

- If Npcap has been installed on the Windows OS, go to **Step 4**.
- If the Npcap has not been installed on the Windows server, perform the following steps:

  a. **Download Npcap** to obtain the latest software installation package.

  **Figure 2-27** Downloading Npcap

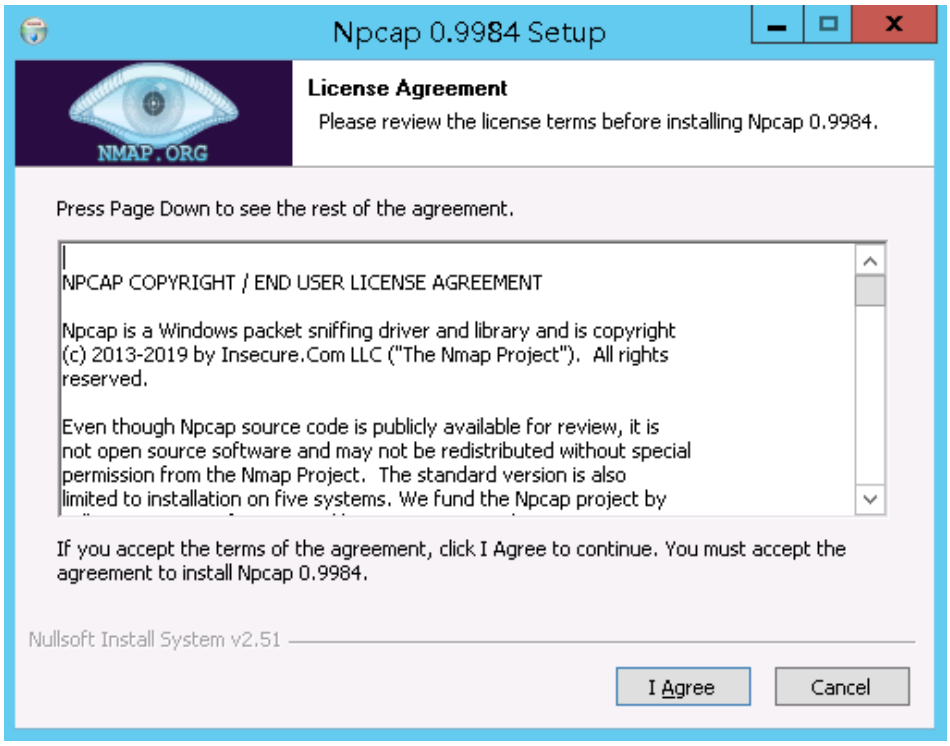
  b. Upload the **npcap-*xxxx*.exe** software installation package to the VM where the agent is to be installed.

c. Double-click the Npcap installation package.

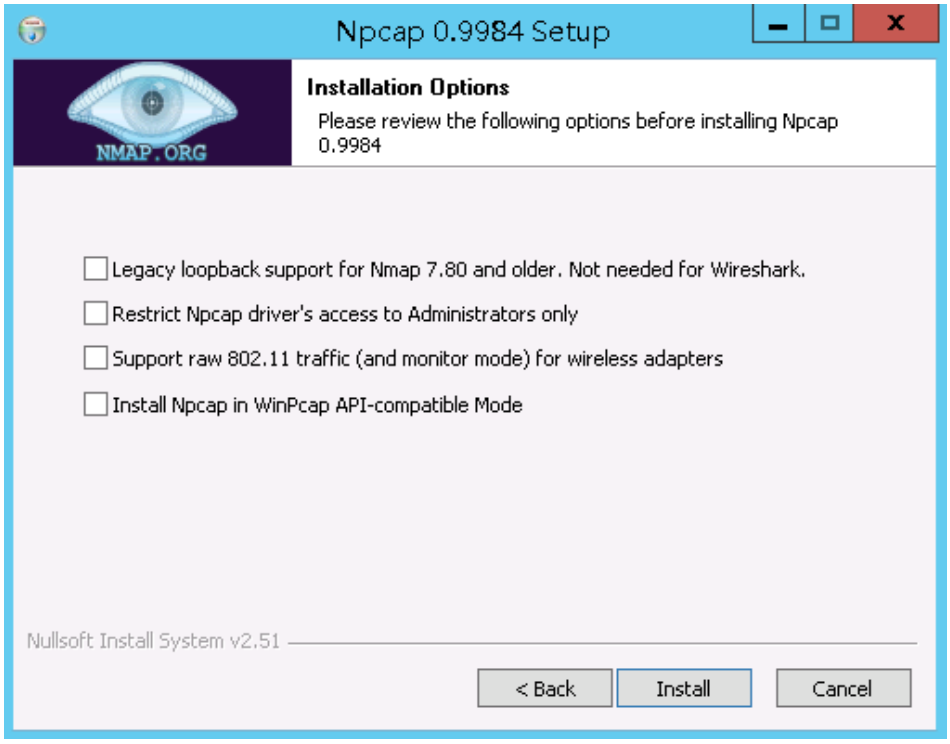
d. In the displayed dialog box, click **I Agree**, as shown in **Figure 2-28**.

**Figure 2-28** Agreeing to install Npcap



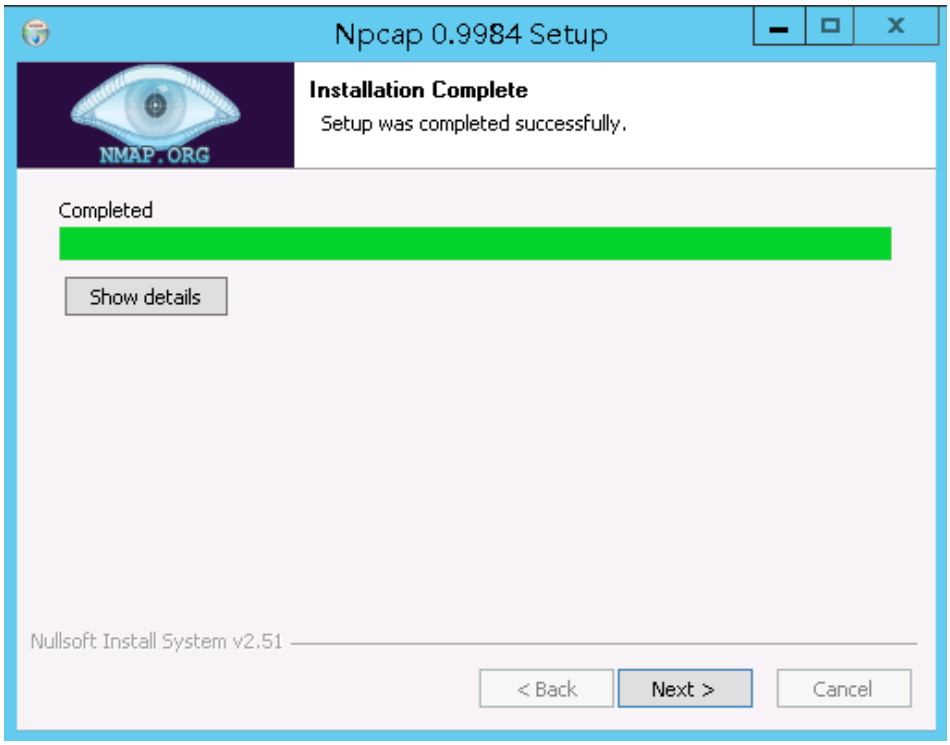

e. In the displayed dialog box, leave all the check boxes unselected and click **Install**, as shown in **Figure 2-29**.

**Figure 2-29** Installing Npcap

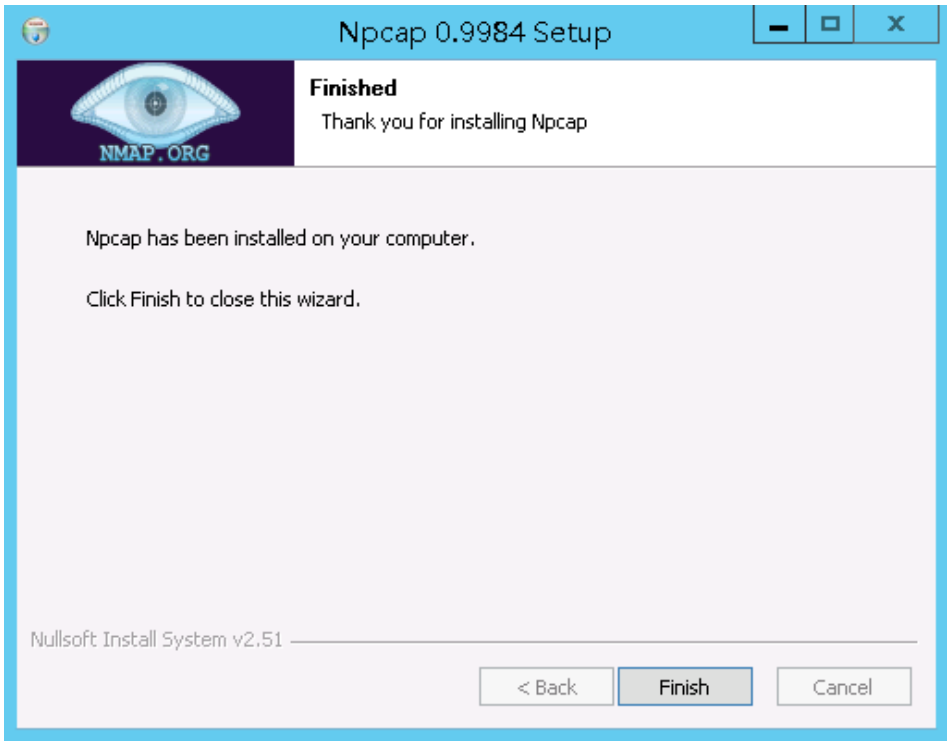


f. In the displayed dialog box, click **Next**.




g. Click **Finish**.

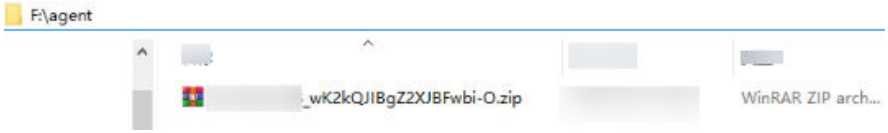



**Step 3** For details about how to obtain the agent installation package of the Windows, see **Downloading an Agent**.

**Step 4** Log in to the Windows host as the **Administrator** user and copy the downloaded agent installation package **xxx.zip** to any directory on the host.

**Figure 2-30** Agent installation package



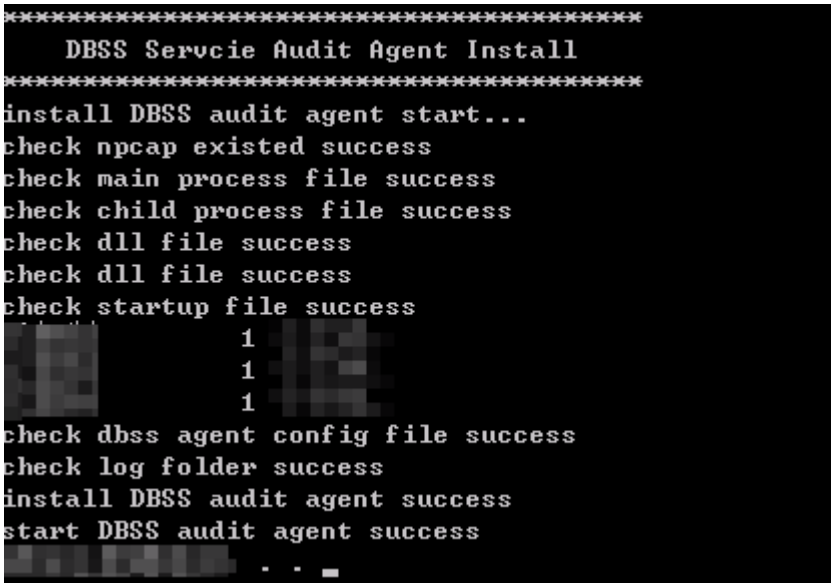

**Step 5** Decompress the package.

**Step 6** Double-click the **install.bat** file in the package directory.

**Figure 2-31** Double-click install.bat

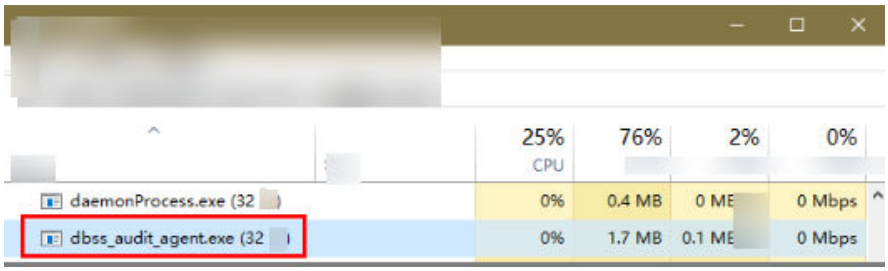

**Step 7** Press any key to complete installation after the output shown in **Figure 2-32** is displayed.

**Figure 2-32** Installation completed




**Step 8** Check the installation result. If the dbss_audit_agent process can be found in the Windows Task Manager, the installation succeeded, as shown in the **Figure 2-33**.

**Figure 2-33** Checking the dbss_audit_agent process



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 installing an agent.

## Prerequisites

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

## Adding a Security Group Rule

**Step 1** For details about how to add an agent, see **Step 2**.

**Step 2** Log in to the management console.

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

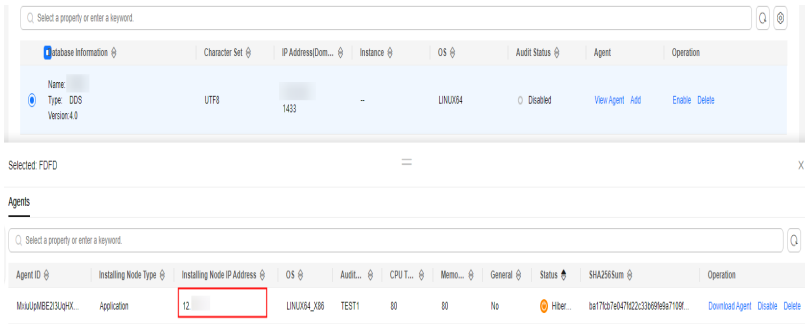
**Step 4** In the navigation tree on the left, choose **Databases**.

**Step 5** In the **Instance** drop-down list, select the instance whose security group rule is to be added.

**Step 6** Record the IP address of the agent node.

Locate the row that contains the target database, and click **View Agent** in the **Agent** column. In the **Agents** area, record the **Installing Node IP Address**.

**Figure 2-34** Installing Node IP Address

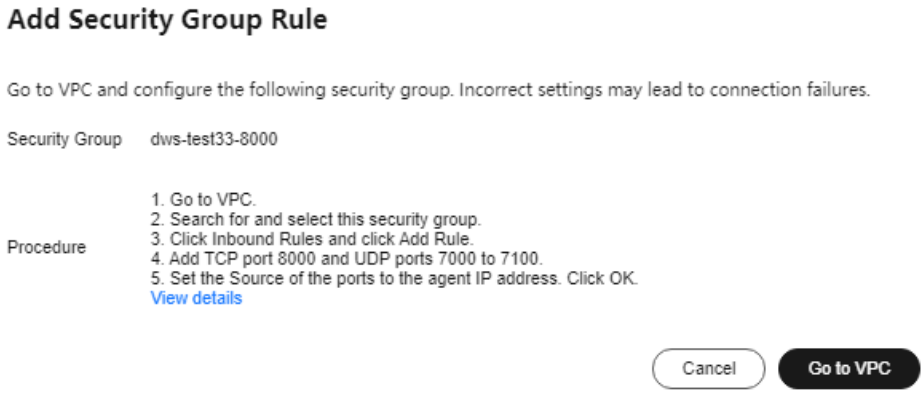



**Step 7** Click **Add Security Group Rule**.

**Step 8** In the displayed dialog box, record the security group name (for example, **default**) of the database audit instance, as shown in **Figure 2-35**.

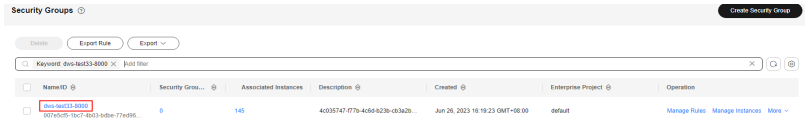
**Figure 2-35** Adding a security group rule




**Step 9** Click **Go to VPC**.

**Step 10** In the search box above the list, select an attribute or enter a keyword to search for a security group. Click the security group name.

**Figure 2-36** Security group




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

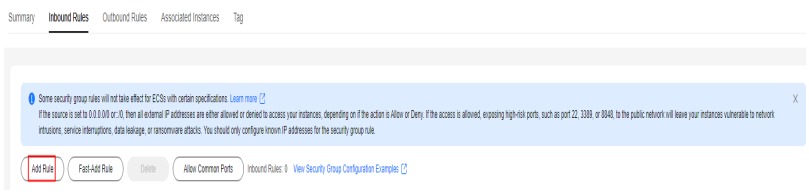
Check whether TCP (port number **8000**) and UDP protocols (port number from **7000** to **7100**) are configured in the inbound rules of the security group for the IP address of the installing node.

- If the inbound rules of the security group have been configured for the installing node, go to **Enabling database audit**.
- If no inbound rules of the security group have been configured for the installing node, go to **20**.

**Step 12** Add an inbound rule for the installing node.

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

   **Figure 2-37** Adding rules

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

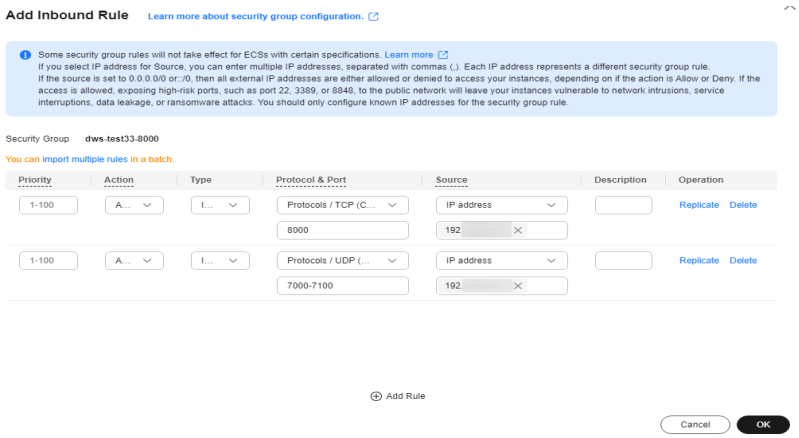
  

**NOTE**

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 2-38** Add Inbound Rule dialog box




3. Click **OK**.

**----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

The status of the agent is **Running**.

## Enabling Database Audit

**Step 1** For details about how to install agents, see **Step 3**.

**Step 2** For details about how to add a security group rule, see **Step 4**.

**Step 3** Log in to the management console.

**Step 4** Click ☰ and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

**Step 5** In the navigation tree on the left, choose **Databases**.

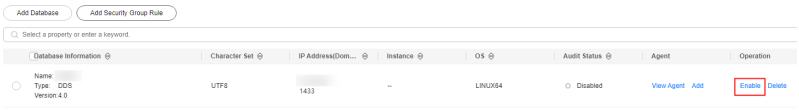
**Step 6** Select a database audit instance from the **Instance** drop-down list.

**Step 7** 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 2-39** 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** Click  and choose **Security** > **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** Locate the row that contains the target time, click  , select the start time and end time, and click **Submit**. In the upper part of the list, select **All time**, **Last 30 minutes**, **Last hour**, **Today**, **Last week**, **Last month**, or **Custom**.

**Figure 2-40** 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

| Type | Supported Edition |
| --- | --- |
| GaussDB(for MySQL) | All editions are supported by default. |
| RDS for SQLServer | All editions are supported by default. |
| RDS for MySQL | • 5.6 (5.6.51.1 or later)<br>• 5.7 (5.7.29.2 or later)<br>• 8.0 (8.0.20.3 or later) |

| Type | Supported Edition |
| --- | --- |
| GaussDB(DWS) | • 8.2.0.100 or later |
| PostgreSQL<br>**NOTICE**<br>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. | • 14 (14.4 or later)<br>• 13 (13.6 or later)<br>• 12 (12.10 or later)<br>• 11 (11.15 or later)<br>• 9.6 (9.6.24 or later)<br>• 9.5 (9.5.25 or later) |
| RDS for MariaDB | All editions are supported by default. |

**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

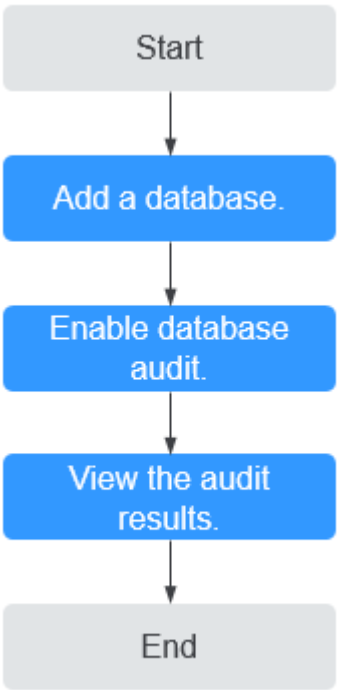


**Table 3-2** Procedure for quickly configuring database audit

| Step | Configuration | Description |
| --- | --- | --- |
| 1 | **Adding a Database** | After purchasing DBSS, you need to add the database to be audited to the instance. |
| 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.<br>**NOTICE**<br>You can set database audit rules as required. For details, see **Adding Audit Scope**. |

# 3.2 Purchasing DBSS

This section describes how to purchase DBSS. DBSS 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

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

## Prerequisites

Check whether the instance account has the required permissions. .

**NOTICE**

Ensure that the **DBSS System Administrator**, **VPC Administrator**, **ECS Administrator**, and **DBSS 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.
- **DBSS 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** > **Database Security Service**. The **Dashboard** page is displayed.

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

**Step 4** On the displayed page, set **Service Type** to **Database Audit Service**, and select the region, AZ, and other information as required.

Table 3-3 describes the database audit editions.

**Table 3-3** DBSS editions

| Edition | Maximum Databases | Performance |
| --- | --- | --- |
| Professional | 6 | • Peak QPS: 6,000 queries/second<br>• Database load rate: 7.2 million statements/hour<br>• Online SQL statement storage: 600 million statements |
| Advanced | 30 | • Peak QPS: 30,000 queries/second<br>• Database load rate: 10.8 million records/hour<br>• Online SQL statement storage: 1.5 billion 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.
- 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 3-2** and **Figure 3-3**. For details about related parameters, see **Table 3-4**.

**Figure 3-2** Network configuration


**Figure 3-3** Advanced configuration

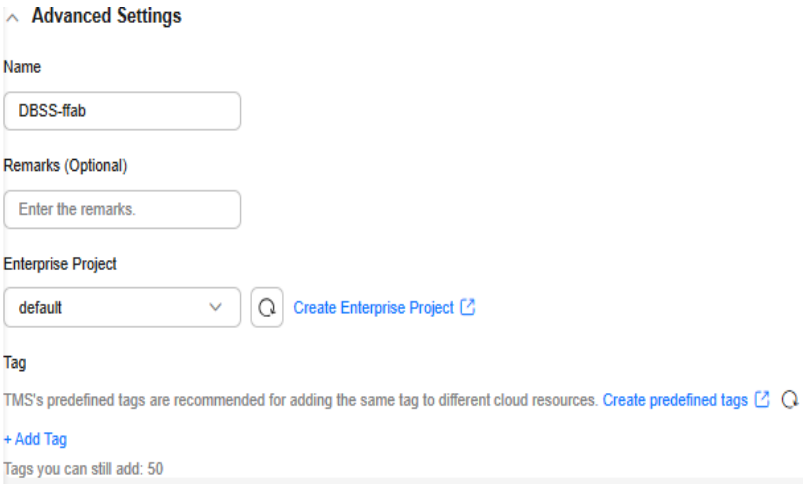


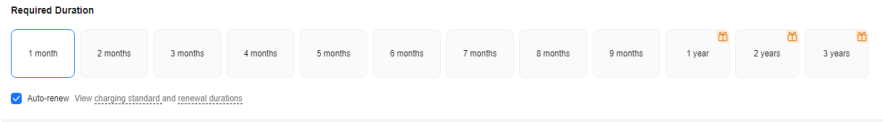
**Table 3-4** Database audit parameters

| Parameter | Description |
| --- | --- |
| VPC | You can select an existing VPC, or click **View VPC** to create one on the VPC console.<br>**NOTE**<br>• 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?**<br>• To change the VPC of a DBSS instance, unsubscribe from it and purchase a new one.<br>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.<br>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 |
| Remarks | You can add instance remarks. |
| Enterprise Project | This parameter is provided for enterprise users.<br>An enterprise project groups cloud resources, so you can manage resources and members by project. The default project is **default**.<br>Select an enterprise project from the drop-down list. For more information about enterprise projects, see ***Enterprise Management User Guide***. |
| Tag | (Optional) Identifier of the database audit instance. Adding tags helps you better identify and manage your database instances. A maximum of 50 tags for each instance<br>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 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 |
| 1/2/3 years | 1 year |

**Step 7** Confirm the configuration and click **Next**.

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

**Step 8** On the **Details** page, read the *Database Security Service Statement*, select **I have read and agree to the Database Security Service Statement**, and click **Submit**.

**Step 9** On the displayed page, select a payment method.

**Step 10** 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

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

## Adding a Database

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

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

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

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

**Step 5** Click **Add Database**.

**Figure 3-5** Adding a 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**.<br>**NOTE**<br>If you select **RDS database**, you can directly select the databases that you want to add to DBSS. | Self-built database |
| Name | Custom name of the database to be added | test1 |
| IP Address | IP address of the database to be added.<br>The IP address must be an internal IP address in IPv4 or IPv6 format. | IPv4: 192.168.1.1<br>IPv6: fe80:0000:0000:0000:0000:0000:0000:0000 |

| Parameter | Description | Example Value |
| --- | --- | --- |
| Type | Supported database type. The options are as follows:<br>• MYSQL<br>• ORACLE<br>• PostgreSQL<br>• SQLServer<br>• DWS<br>• GaussDB(for MySQL)<br>• GaussDB<br>• DAMENG<br>• KINGBASE<br>• MongoDB<br>• Hbase<br>• SHENTONG<br>• GBase 8a<br>• GBase XDM Cluster<br>• Greenplum<br>• HighGo<br>• MariaDB<br>• Hive<br>• DDS<br>• GBase 8s<br>• TDSQL<br>• Vastbase<br>• TiDB<br>**NOTE**<br>• If **ORACLE** is selected, to make the audit settings take effect, restart the applications to be audited and log in to the database again.<br>• To use the Hive database to audit an MRS cluster, you need to disable SSL encryption on the server (for details, see **SSL Encryption Function Used by a Client**) and disable Kerberos authentication on the cluster purchase page. | MYSQL |
| Port | Port number of the database to be added | 3306 |

| Parameter | Description | Example Value |
| --- | --- | --- |
| Version | Supported database versions<br>• When **Type** is set to **MySQL**, the following versions are available:<br>– 5.0, 5.1, 5.5, 5.6, and 5.7<br>– 8.0 (8.0.11 and earlier)<br>– 8.0.30<br>– 8.0.35<br>– 8.1.0<br>– 8.2.0<br>• When **Type** is set to **ORACLE**, the following versions are available:<br>– 11g<br>– 12c<br>– 19c<br>• When **Type** is set to **PostgreSQL**, the following versions are available:<br>– 7.4<br>– 8.0, 8.1, 8.2, 8.3, and 8.4<br>– 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, and 9.6<br>– 10.0, 10.1, 10.2, 10.3, 10.4, and 10.5<br>– 11.0<br>– 12.0<br>– 13.0<br>– 14.0<br>• When **Type** is set to **SQLServer**, the following versions are available:<br>– 2008<br>– 2012<br>– 2014<br>– 2016<br>– 2017<br>• When **Type** is set to **DWS**, the following versions are available:<br>– 1.5<br>• When **Type** is set to **GaussDB(for MySQL)**, the following versions are available:<br>– When **Database Type** is set to **Self-built database**, you can select the **Mysql 8.0** version. | 5.0 |

| Parameter | Description | Example Value |
| --- | --- | --- |
| | – 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.<br>• When **Type** is set to **GaussDB**, the following version is available:<br>– 1.4 Enterprise Edition<br>– 1.3 Enterprise Edition<br>– 2.8 Enterprise Edition<br>– 3.223 Enterprise Edition<br>• When **Type** is set to **DAMENG**, the following version is available:<br>– DM8<br>• When **Type** is set to **KINGBASE**, the following version is available:<br>– V8<br>• When **Type** is set to **HBase**, the following versions are available:<br>– 1.3.1<br>– 2.2.3<br>• When **Type** is set to **SHENTONG**, the following version is available:<br>– 7.0<br>• When **Type** is set to **GBase 8a**, the following version is available:<br>– 8.5<br>• When **Type** is set to **GBase XDM Cluster**, the following version is available:<br>– 8.0<br>• When **Type** is set to **GBase 8s**, the following version is available:<br>– v8.8<br>• When **Type** is set to **Greenplum**, the following version is available:<br>– v6.0<br>• When **Type** is set to **HighGo**, the following version is available:<br>– v6.0<br>• When **Type** is set to **MongoDB**, the following version is available:<br>– v5.0 | |

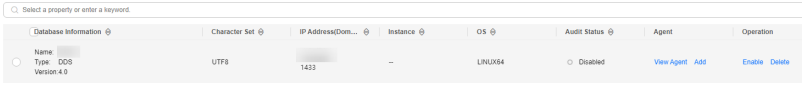
  

| Parameter | Description | Example Value |
| --- | --- | --- |
| | • When **Type** is set to **MariaDB**, the following version is available:<br>– 10.6<br>• When **Type** is set to **Hive**, the following versions are available:<br>– 1.2.2<br>– 2.3.9<br>– 3.1.2<br>– 3.1.3<br>• When **Type** is set to **TDSQL**, the following version is available:<br>– 10.3.17.3.0<br>• When **Type** is set to **Vastbase**, the following edition is available:<br>– G100 V2.2<br>• When **Type** is set to **TiDB**, the following editions are available:<br>– V4<br>– V5<br>– V6<br>– V7<br>– V8 | |
| Instance | Instance name of the database to be audited<br>**NOTE**<br>• If you do not configure the **Instance** field, database audit will audit all instances in the database.<br>• 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:<br>• UTF-8<br>• GBK | UTF-8 |
| OS | OS of the added database. The options are as follows:<br>• LINUX64<br>• WINDOWS64 | LINUX64 |

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

**Figure 3-6** Successfully adding a database




NOTE

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

**----End**

# 3.4 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**.

## Enabling Database Audit

**Step 1** For details about how to install agents, see **Step 3**.

**Step 2** For details about how to add a security group rule, see **Step 4**.

**Step 3** Log in to the management console.

**Step 4** Click ☰ and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

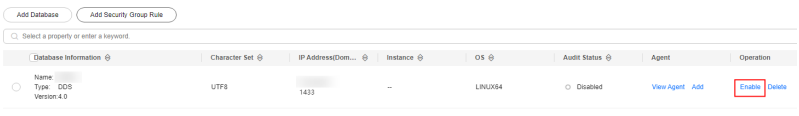
**Step 5** In the navigation tree on the left, choose **Databases**.

**Step 6** Select a database audit instance from the **Instance** drop-down list.

**Step 7** 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 3-7** 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** Click ☰ and choose **Security** > **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** Locate the row that contains the target time, click 📅, select the start time and end time, and click **Submit**. In the upper part of the list, select **All time**, **Last 30 minutes**, **Last hour**, **Today**, **Last week**, **Last month**, or **Custom**.

**Figure 3-8** Viewing SQL statements


**----End**

# 4 Upgrading the Database Audit Instance Version

This section describes how to upgrade your database instance version.

## Prerequisites

- The database audit instance is in the **Running** state.
- The database instance version is earlier than the latest version.

## Procedure

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

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

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

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

**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

- The database audit instance is in the **Running** state.
- For details about how to enable database audit, see **Enable Database Audit**.

### Procedure

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

**Step 2** Click ☰ and choose **Security** > **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.
- 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.

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

**Table 5-1** Parameters

| Parameter | Description | Example Value |
| --- | --- | --- |
| Name | Name of the custom audit scope | audit00 |
| Database Name | Select a database or **ALL**. | db03 |
| Operations | Audited operation type. It can be **Login** or **Operation**.<br>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.<br>You can specify multiple accounts, separated by commas (,). | - |
| Exception IP Address | (Optional) IP addresses that do not need to be audited.<br>**NOTE**<br>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<br>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

- The database audit instance is in the **Running** state.
- For details about how to enable database audit, see **Enable Database Audit**.

## Procedure

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

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

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

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

**Step 5** 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** Click **Add Rule** and configure parameters.

**Figure 5-1** Adding an SQL injection rule

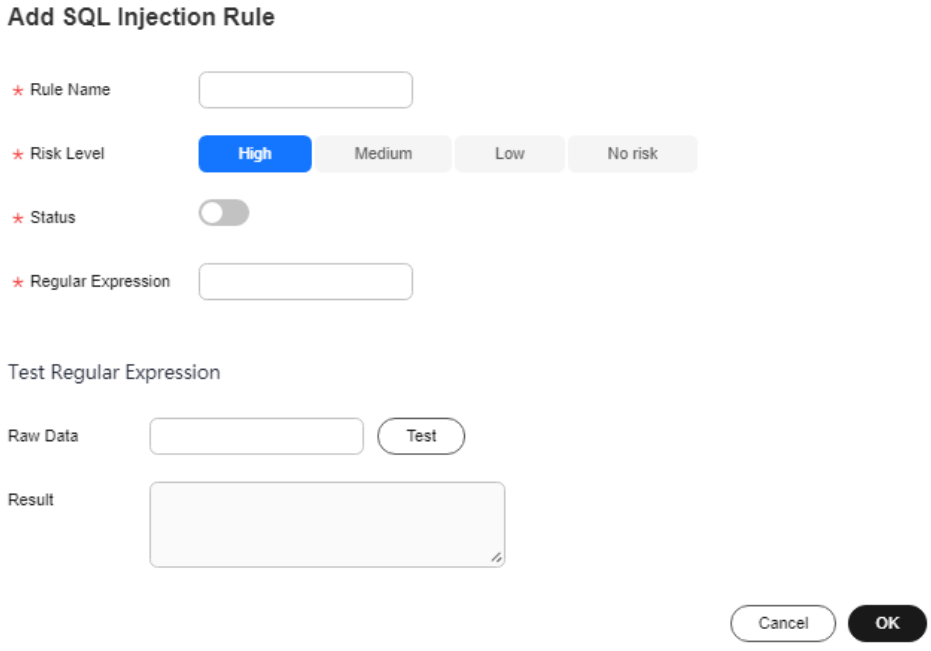



**Table 5-2** SQL injection rule parameters

| Parameter | Description | Example Value |
| --- | --- | --- |
| Rule Name | Name of an SQL rule. | Postal Code SQL injection Rule |

| Parameter | Description | Example Value |
| --- | --- | --- |
| Risk Level | Level of risks matching a SQL rule. Its value can be:<br>• **High**<br>• **Medium**<br>• **Low**<br>• **No risk** | **Medium** |
| Status | Enables or disables an SQL injection rule.<br>•  : enabled<br>•  : disabled |  |
| Regular Expression | Regular expression that checks for content in certain pattern. | ^\d{6}$ |
| Raw Data | Content that matches the regular expression.<br>Enter content and click **Test** to verify that the regular expression works properly. | 628307 |
| Result | Test result. It can be:<br>• Hit<br>• Miss<br>**NOTE**<br>– If the test result is **Hit**, the regular expression is correct.<br>– If the test result is **Miss**, the regular expression is incorrect. | Hit |

**Step 7** Confirm the information and click **OK**.

**----End**

# 5.3 Managing SQL Injection Rules

SQL injection rules of database audit are enabled by default. You can disable, enable, edit, and set priorities for SQL injection rules.

**NOTICE**

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

## Prerequisites

- The database audit instance is in the **Running** state.
- Before enabling an SQL injection rule, ensure that the rule is in the **Disabled** state.
- Before disabling an SQL injection rule, ensure that the rule is in the **Enabled** state.

## Disabling SQL Injection Rules

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

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

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

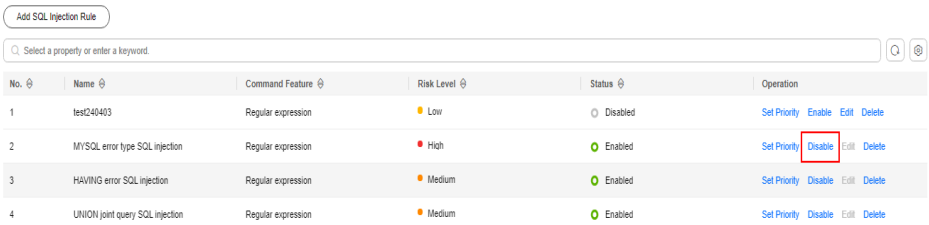
**Step 3** In the navigation tree, choose **Rules**.

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

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

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

**Figure 5-2** Disabling an SQL injection rule




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

**----End**

## Enabling SQL Injection Rules

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

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

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

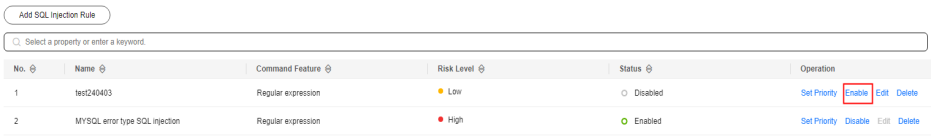
**Step 4** In the **Instance** drop-down list, select the instance for which you want to enable SQL injection rule.

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

**Step 6** In the **Operation** column of the row containing the SQL injection rule, click **Enable** to enable the rule.

**Figure 5-3** Enabling an SQL injection rule




**Step 7** The SQL injection rule is enabled and its status changes to **Enabled**.

**----End**

## Setting the Priority of SQL Injection Rules

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

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

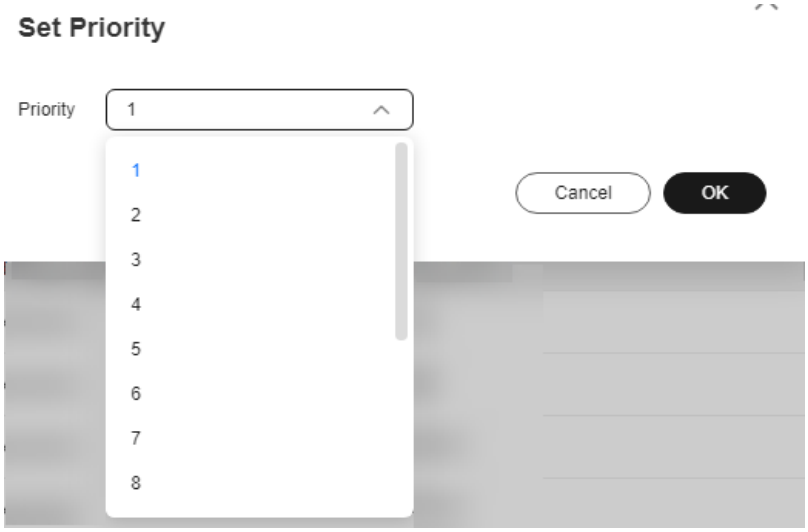
**Step 3** In the navigation tree, choose **Rules**.

**Step 4** In the **Select Instance** drop-down list, select the instance for which you want to set the priority for the SQL injection rule.

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

**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 5-4** Configuring the priority




**----End**

## Editing an SQL Injection Rule

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

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

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

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

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

NOTE

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

**Step 6** Click **Edit** in the **Operation** column to edit the parameters of the target rule. For details about the parameters, see **Table 5-3**.

**Figure 5-5** Editing an SQL injection rule

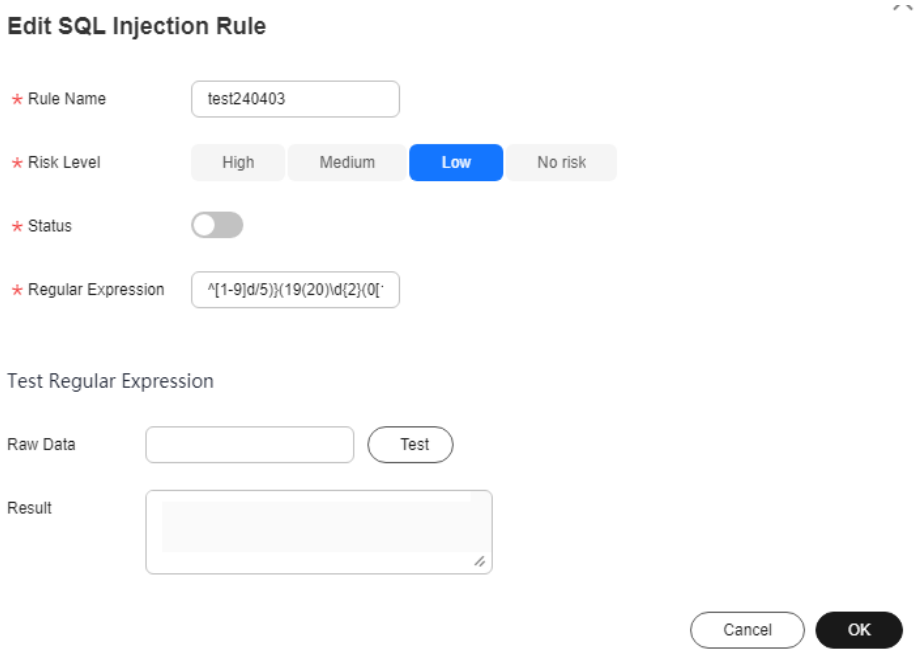



**Table 5-3** SQL injection rule parameters

| Parameter | Description | Example Value |
| --- | --- | --- |
| Name | Name of an SQL rule. | Postal Code SQL injection Rule |

| Parameter | Description | Example Value |
| --- | --- | --- |
| Risk Level | Level of risks matching a SQL rule. Its value can be:<br>• **High**<br>• **Moderate**<br>• **Low**<br>• **No risk** | **Moderate** |
| Status | Enables or disables an SQL injection rule.<br>•  : enabled<br>•  : disabled |  |
| Test Regular Expression | Regular expression that checks for content in certain pattern. | ^\d{6}$ |
| Data | Content that matches the regular expression.<br>Enter content and click **Test** to verify that the regular expression works properly. | 628307 |
| Result | Test result. It can be:<br>• Hit<br>• Miss<br>**NOTE**<br>– If the test result is **Hit**, the regular expression is correct.<br>– If the test result is **Miss**, the regular expression is incorrect. | Hit |

**Step 7** Confirm the information and click **OK**.

**----End**

## Deleting an SQL Injection Rule

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

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

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

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

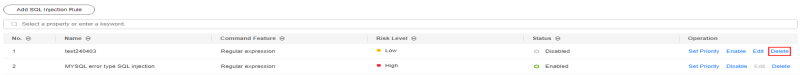
**Step 5** Click the **SQL Injection** tab.

NOTE

Only user-defined SQL injection rules can be deleted. Default rules can only be enabled or disabled.

**Step 6** In the **Operation** column, click **Delete**.

**Figure 5-6** Deleting SQL injection



**----End**

# 5.4 Adding Risky Operations

Database audit has four built-in detection rules, including database reduction detection, slow SQL statements detection, batch data tampering detection, and batch data deletion detection, helping you detect database security risks in a timely manner. You can also add risky operations and customize detection rules.

NOTICE

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

## Prerequisites

- The database audit instance is in the **Running** state.
- For details about how to enable database audit, see **Enable Database Audit**.

## Procedure

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

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

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

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

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

**Step 6** Click **Add** above the risky operation list.

**Step 7** On the **Add Risky Operation** page, set the basic information and IP address or IP range. For details about related parameters, see **Table 5-4**.

**Figure 5-7** Configuring basic information and IP addresses or IP address segments

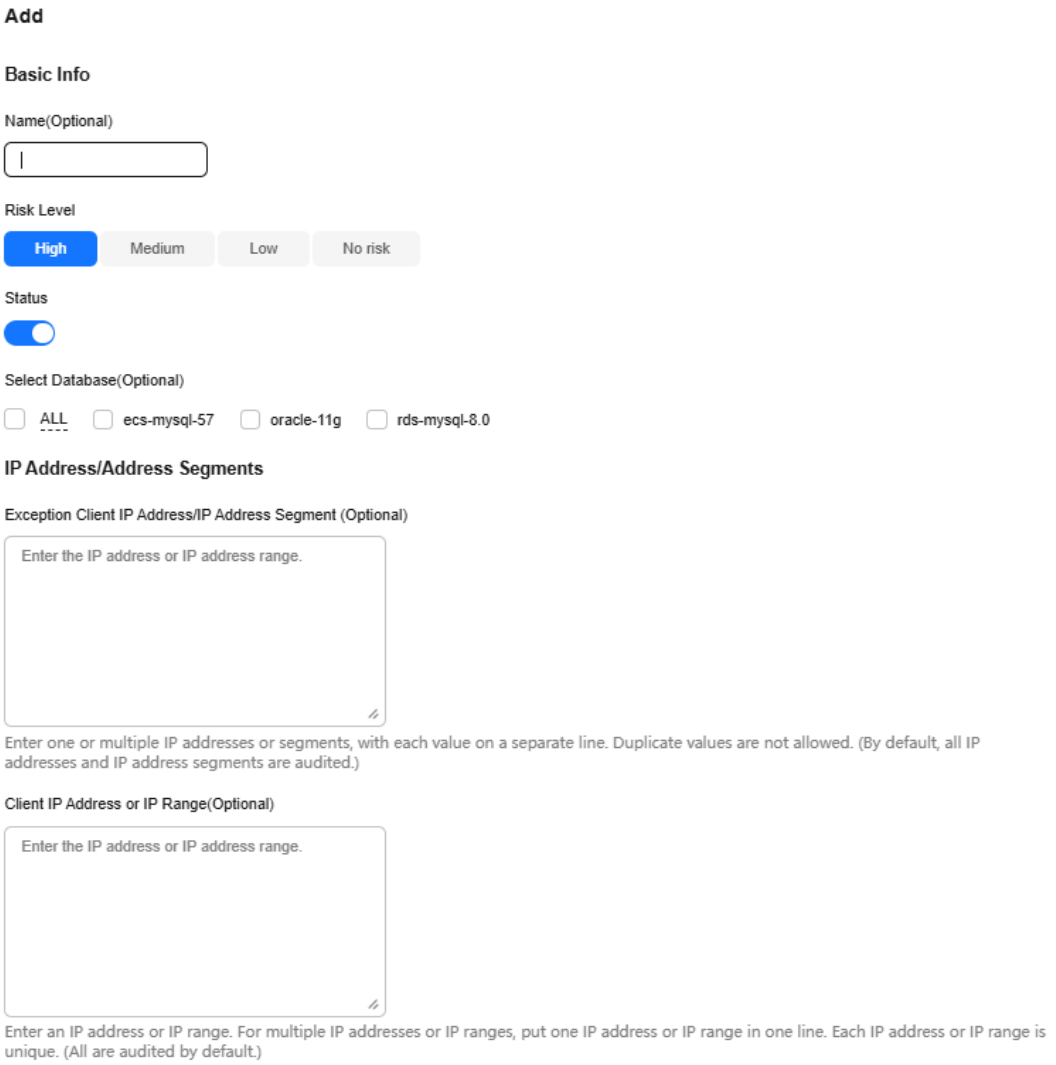



**Table 5-4** Parameters

| Parameter | Description | Example Value |
| --- | --- | --- |
| Name | Custom name of a risky operation | test |
| Risk Severity | Severity of a risky operation. The options are as follows:<br>• **High**<br>• **Moderate**<br>• **Low**<br>• **No risks** | High |

| Parameter | Description | Example Value |
| --- | --- | --- |
| Status | Status of a risky operation<br>•  : enabled<br>•  : disabled |  |
| Select Database | Database that the risky operation will be applied to<br>You can select **ALL** or a specific database. | - |
| Exception Client IP Address or IP Range | To report risky operation alarms set by users, configure the client IP address or IP address range that is not in the trusted client IP address or IP address range.<br>The IP address can be an IPv4 address (for example, 192.168.1.2) or an IPv6 address (for example, fe80:0000:0000:0000:0000:0000:0000:0000). | 192.168.xx.xx |
| Client IP Address or IP Range | IP address or IP address range of the client<br>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.xx.xx |

**Step 8** 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

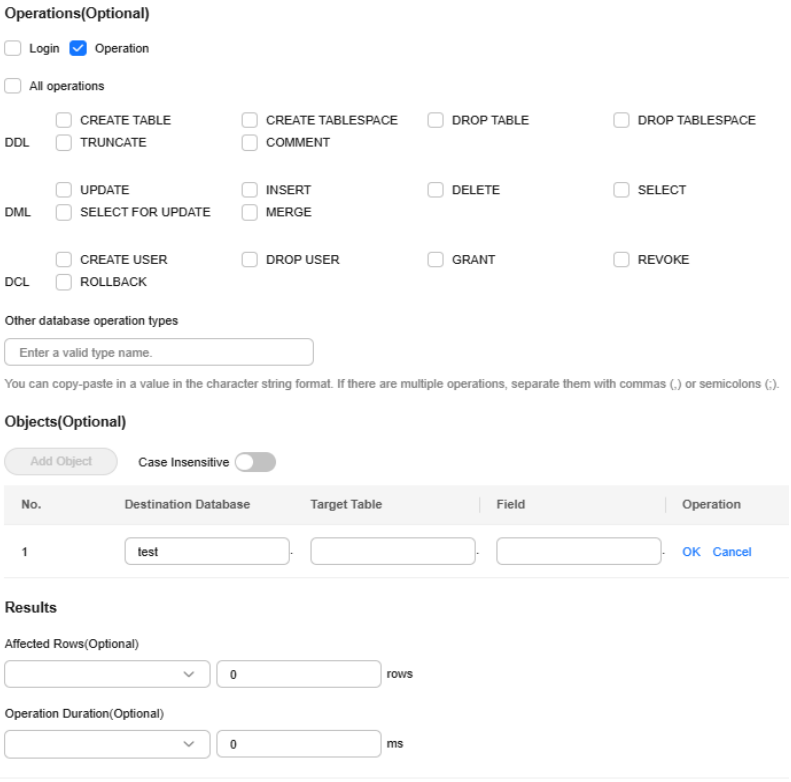



**Table 5-5** Parameters

| Parameter | Description | Example Value |
| --- | --- | --- |
| Operations | Type of a risky operation, including **Login** and **Operation**<br>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:<br>• **Greater than**<br>• **Less than**<br>• **Equal To**<br>• **Greater than or equal to**<br>• **Less than or equal to** | - |

**Step 9** 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

- The database audit instance is in the **Running** state.
- For details about how to enable database audit, see **Enable Database Audit**.

## Procedure

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

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

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

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

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

NOTE

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

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

- **Store Result Set**

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

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

  **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** Adding a user-defined rule

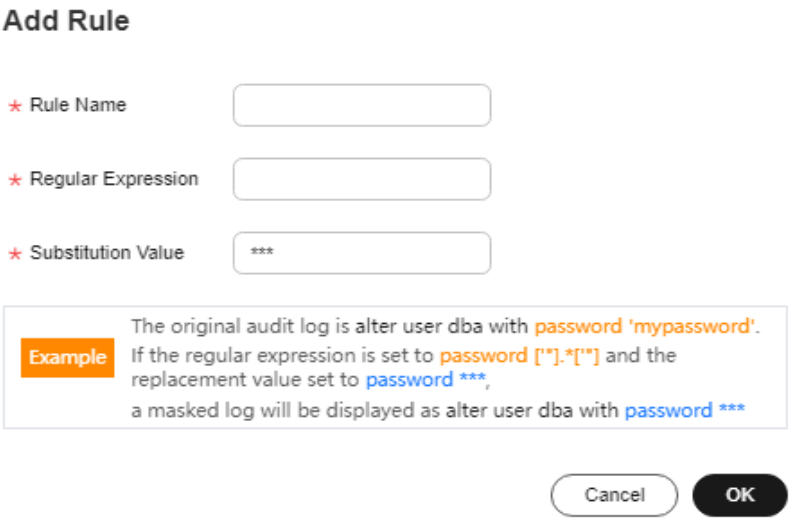



**Table 5-6** Rule parameters

| 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.

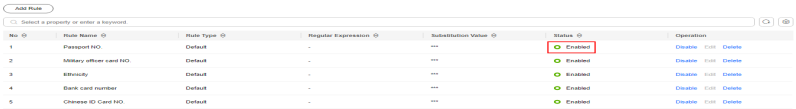
**----End**

## 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** 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

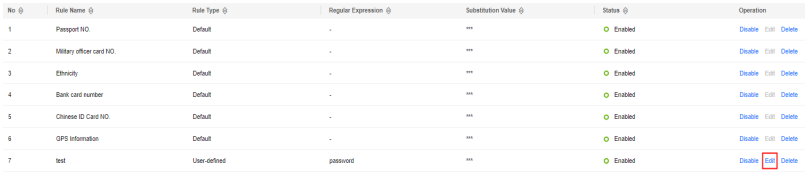
  Locate the row that contains the rule to be disabled and click **Disable** in the **Operation** column. A disabled rule cannot be used.

  **Figure 5-11** Disabling a custom masking rule


- 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.

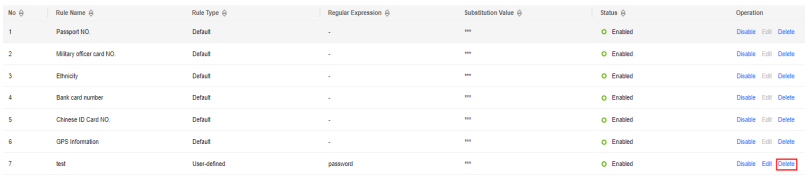
  **Figure 5-12** Editing a custom masking rule




- 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.

  **Figure 5-13** Deleting a custom masking rule



# 5.6 SQL Whitelist

## 5.6.1 Adding an SQL Whitelist

You can add risky SQL statements to the whitelist. The SQL statements in the whitelist will be ignored during the audit.

### Constraints and Limitations

The risky SQL statements can be added to the whitelist in data reports.

### Procedure

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

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

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

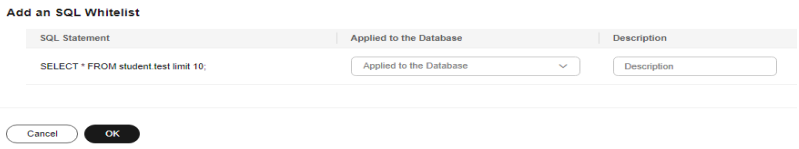
**Step 4** In the **Instance** drop-down list, select the instance whose session information you want to view.

**Step 5** Click the **Statements** tab to view risky SQL statements.

**Step 6** Add SQL statements to the whitelist.

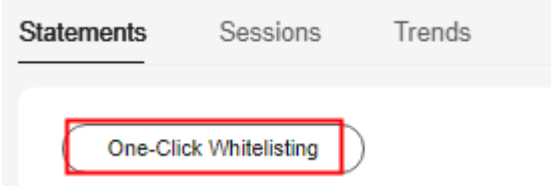
- Add a single SQL statement.
  a. Click **Add to Whitelist** in the **Operation** column of the target SQL statement.
  b. In the displayed dialog box, select the database and description of the target SQL statement.

  **Figure 5-14** Adding an SQL whitelist

  c. Click **OK**.
- Add SQL statements in batches.
  a. Select the target SQL statement and click **One-Clink Whitelisting**.

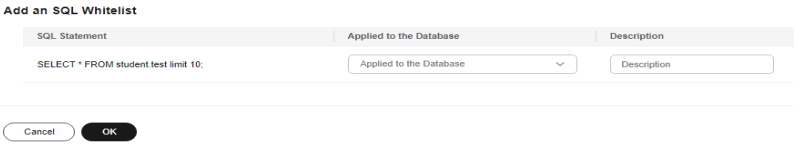
  **Figure 5-15** One-click whitelisting

b. In the displayed dialog box, select the database and description of the target SQL statement.

**Figure 5-16** Adding an SQL whitelist




c. Click **OK**.

**----End**

## 5.6.2 Managing an SQL Whitelist

You can edit, disable, and delete the added SQL statement whitelist.

### Prerequisites

The SQL statements to be associated have been added to the whitelist.

### Procedure

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

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

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

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

**Step 5** Click the **SQL Whitelist** tab to view all SQL statement whitelists.

**Step 6** Manage the whitelist.

- Click **Edit** in the **Operation** column of the target SQL statement to modify the description and applied database.
- Click **Disable** in the **Operation** column of the target SQL statement. The disabled statement does not execute the rule in the audit.

  NOTE

  After the SQL statement is disabled, there is a delay of about 1 minute.
- Click **Delete** in the **Operation** column of the target SQL statement. The deleted SQL statement cannot be restored. You can only add the SQL statement to the whitelist again. The SQL statement will be scanned again.

  To delete multiple SQL statements from the whitelist, select the SQL statements to be deleted, click **Delete All** and confirm the deletion.

NOTE

After the SQL whitelist is modified, the modification does not take effect on the audited data.

**----End**

# 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

- The database audit instance is in the **Running** state.
- For details about how to enable database audit, see **Enable Database Audit**.

### Procedure

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

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

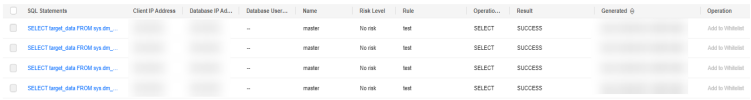
**Step 3** In the navigation tree on the left, choose **Data Reports**. The **Data Reports** page is displayed.

**Step 4** In the **Instance** drop-down list, select the instance whose 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 the time range ( **All** time, **Last 30 minutes**, **1 hour**, **Today**, **7 days**, or **30 days** Click , the SQL statements in the time period are displayed in the list.
- Select **All**, **High**, **Moderate**, **Low**, or **No risk** for **Risk Level** 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** Click the SQL statement.

**Step 8** View the SQL statement information in the **StatementDetails** 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.

**Figure 6-2 Statement** dialog box

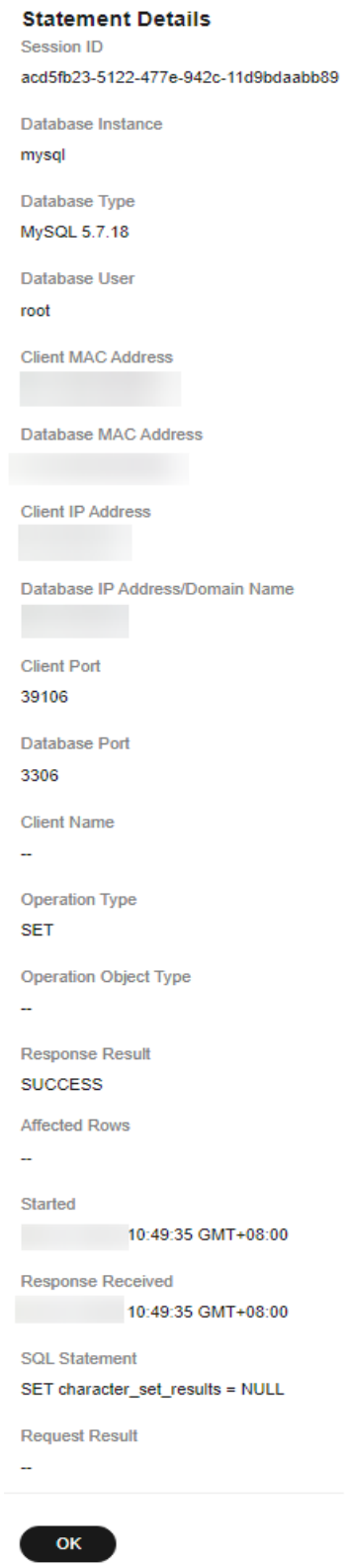


**Table 6-1** Parameters for details of SQL statements

| 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 |
| 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

- The database audit instance is in the **Running** state.
- For details about how to enable database audit, see **Enable Database Audit**.

## Procedure

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

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

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

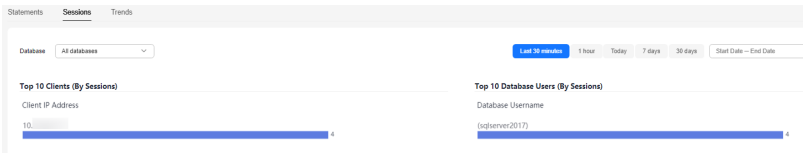
**Step 4** In the **Instance** drop-down list, select the instance whose session information you want to view.

**Step 5** Click the **Sessions** tab.

**Step 6** View the session distribution chart.

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

**Figure 6-3** Viewing session distribution




**----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.
- The database audit instance is in the **Running** state.
- For details about how to enable database audit, see **Enable Database Audit**.

## Procedure

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

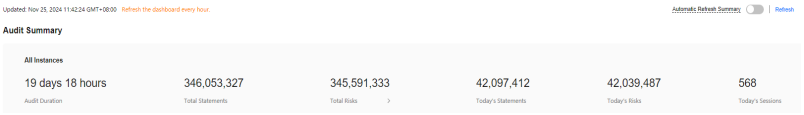
**Step 2** Click ☰ and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

**Step 3** 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 6-4** Viewing audit summary

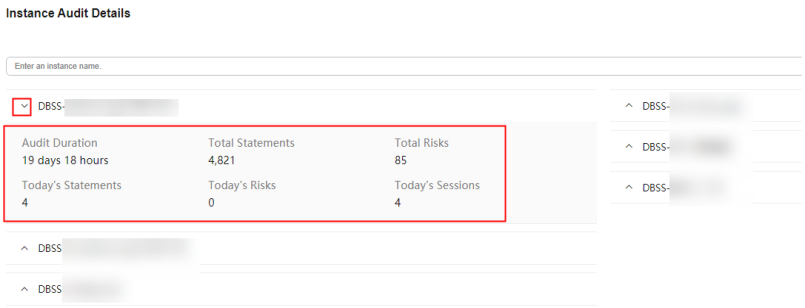
  
  

  Click  in the upper right corner to enable regular information summary refreshing. Refresh the dashboard every hour. Click **Refresh** in the upper right corner to refresh the audit information immediately.

- 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 6-5** Viewing single instance information

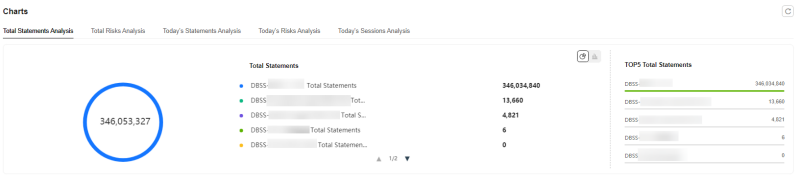
  
  

- Data analysis charts

  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 6-6** Viewing the data analysis chart

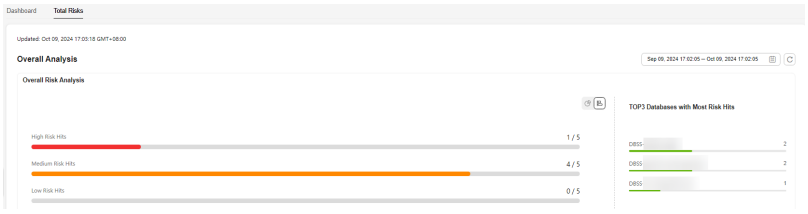



**Step 4** Click **Total Risks**. The **Total Risks** page is displayed. Click and select a time range to view the risk analysis of all database audit instances in the specified time range.

- 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 6-7** Overall risk analysis

- Overall risk rule analysis

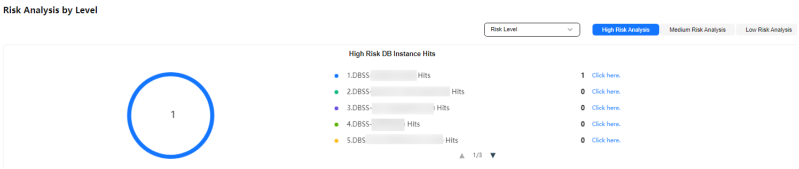
  Displays the number of risk rule hits of all databases and top 5 risk rule hits.

  **Figure 6-8** Overall risk rule analysis

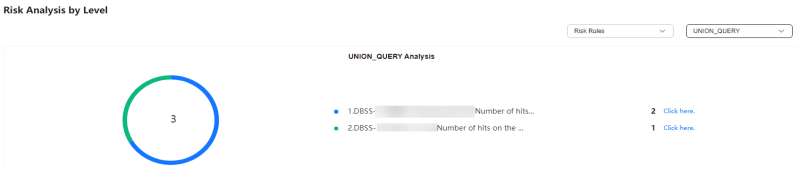
- Risk analysis by level
  - Risk level: displays the high-risk hit analysis, medium-risk hit analysis, and low-risk hit analysis of each database.

    **Figure 6-9** Risk level analysis

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

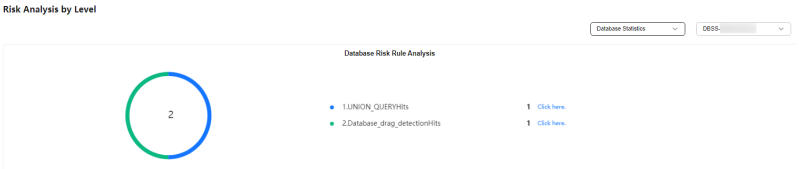
    **Figure 6-10** Risk rule analysis

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

  **Figure 6-11** Database statistics analysis

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

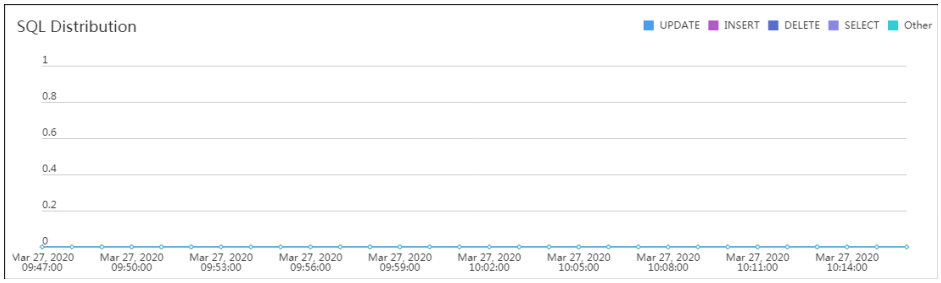
**Step 6** Click the **Trends** tab. The trend analysis page is displayed.

**Step 7** In the **Instance** drop-down list, select the instance whose audit information you want to view.

**Step 8** 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 6-12** 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

- The database audit instance is in the **Running** state.
- For details about how to enable database audit, see **Enable Database Audit**.

## 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. |
| 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** Click ☰ and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

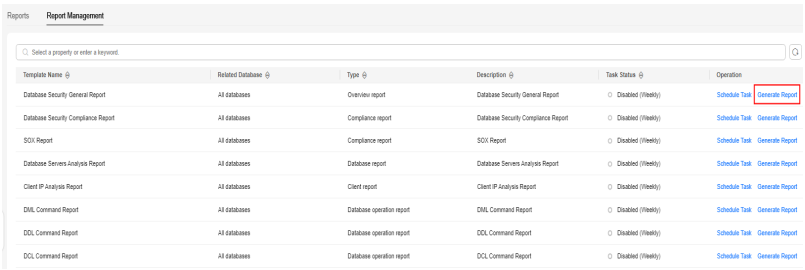
**Step 3** In the navigation tree on the left, choose **Reports**.

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

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

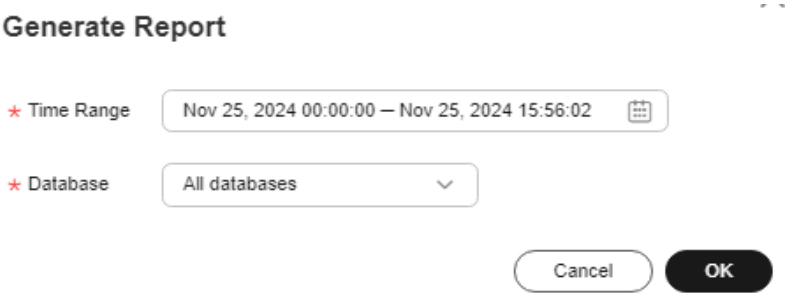
**Step 6** In the **Operation** column of a report template, click **Generate Report**.

**Figure 6-13** Report template list




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

**Figure 6-14** Generate Report




**Step 8** Click **OK**.

**----End**

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

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

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

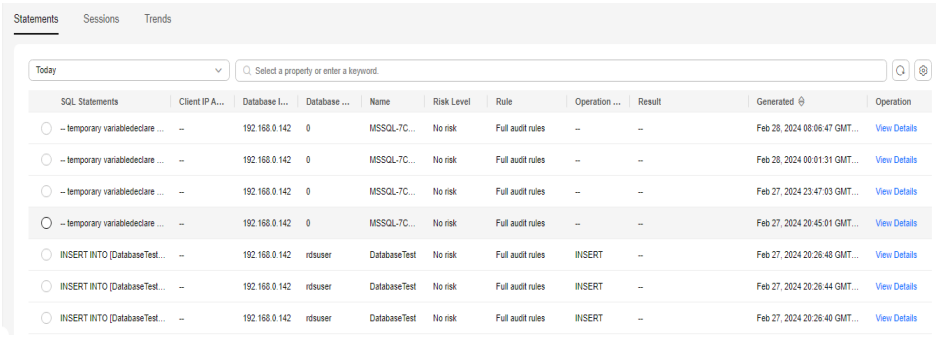
**Step 3** In the navigation tree on the left, choose **Reports**.

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

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

**Step 6** Locate the target template and click **Schedule Task** in the **Operation** column, as shown in **Figure 6-15**.

**Figure 6-15** Setting a task




**Step 7** In the displayed dialog box, set the parameters of the scheduled task, as shown in **Figure 6-16**. For details about related parameters, see **Table 6-3**.

**Figure 6-16** Setting a scheduled task

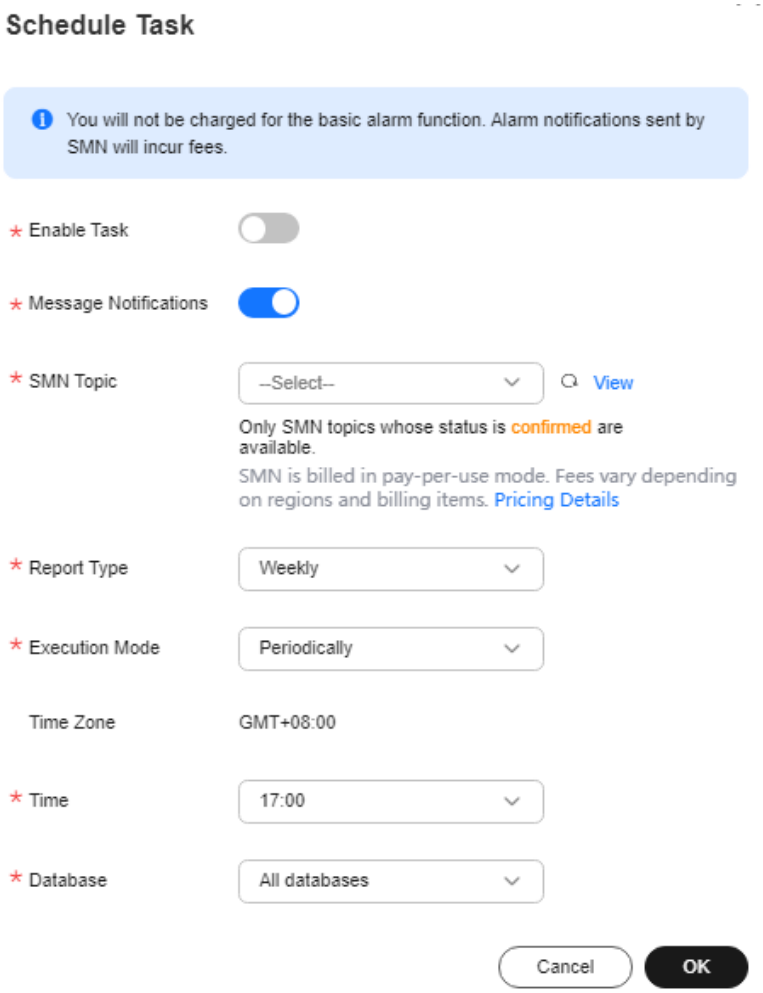



**Table 6-3** Parameters for setting a task

| Parameter | Description | Example Value |
| --- | --- | --- |
| Enable Task | Status of a scheduled task.<br>• : enabled<br>• : disabled | |
| Message Notifications | Enables or disables notifications.<br>Notifications are sent and billed by SMN in pay-per-use mode. Fees vary depending on regions and billing items. For details, see **SMN Pricing Details**.<br>• : enabled<br>• : disabled | |

| Parameter | Description | Example Value |
| --- | --- | --- |
| SMN Topic | • Select an existing topic from the drop-down list or click **View** to create a topic. For details, see **Creating a Topic**.<br>• 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**.<br>For details about topics and subscriptions, see *Simple Message Notification User Guide*. | - |
| Report Type | Type of a report. The options are as follows:<br>• **Daily**<br>• **Weekly**<br>• **Monthly** | Weekly |
| Execution Mode | Execution mode of the report. The options are as follows:<br>• **Once**<br>• **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** Click ☰ and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

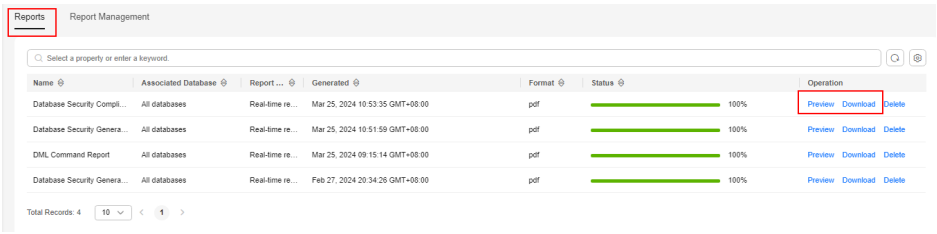
**Step 3** In the navigation tree on the left, choose **Reports**.

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

**Step 5** Locate the target template, and click **Preview** or **Download** in the **Operation** column to preview or download the report. See **Figure 6-17**..

**Figure 6-17** 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

- This function is supported by database instance of 23.05.23.193055 and later versions.
- The database audit instance is in the **Running** state.
- For details about how to enable database audit, see **Enable Database Audit**.

## Procedure

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

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

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

**Step 4** 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 statement and risk trend analysis of all databases or a specified database in the instance.

- Select **Last 30 minutes**, **1 hour**, **Today**, **7 days**, or **30 days**, or click to customize start time and end time to view the statement and risk trend analysis in a specified period.

**Figure 6-18** Statement quantity

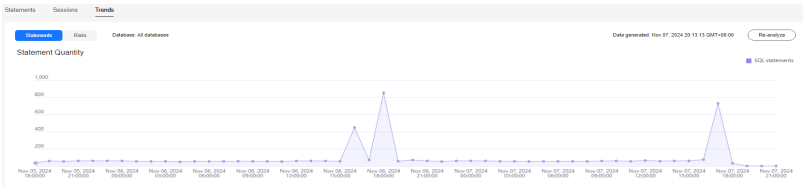



**Figure 6-19** Session statistics

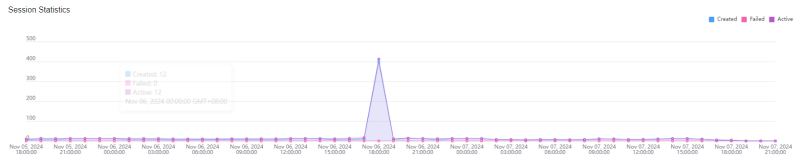



**Figure 6-20** SQL distribution

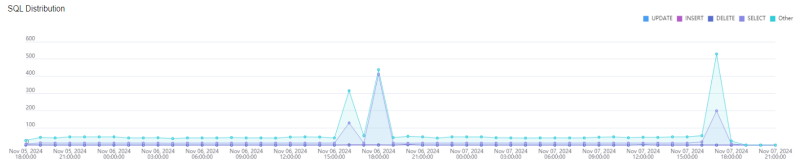



**Figure 6-21** Risk distribution

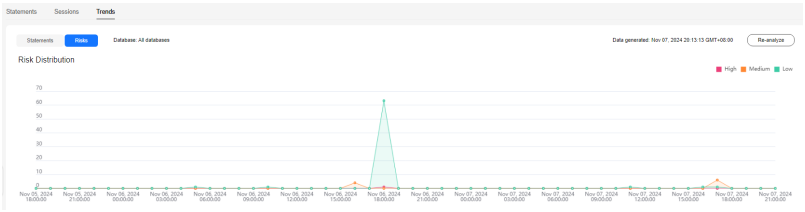
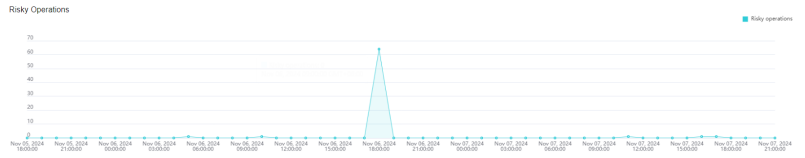



**Figure 6-22** SQL injections


**Figure 6-23** Risky operations




**----End**

# 7 Notification Settings Management

## 7.1 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** Log in to the management console.

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

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

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

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

**Step 6** Set alarm notifications. For details about related parameters, see **Table 7-1**.

**Figure 7-1** Configuring alarm notifications

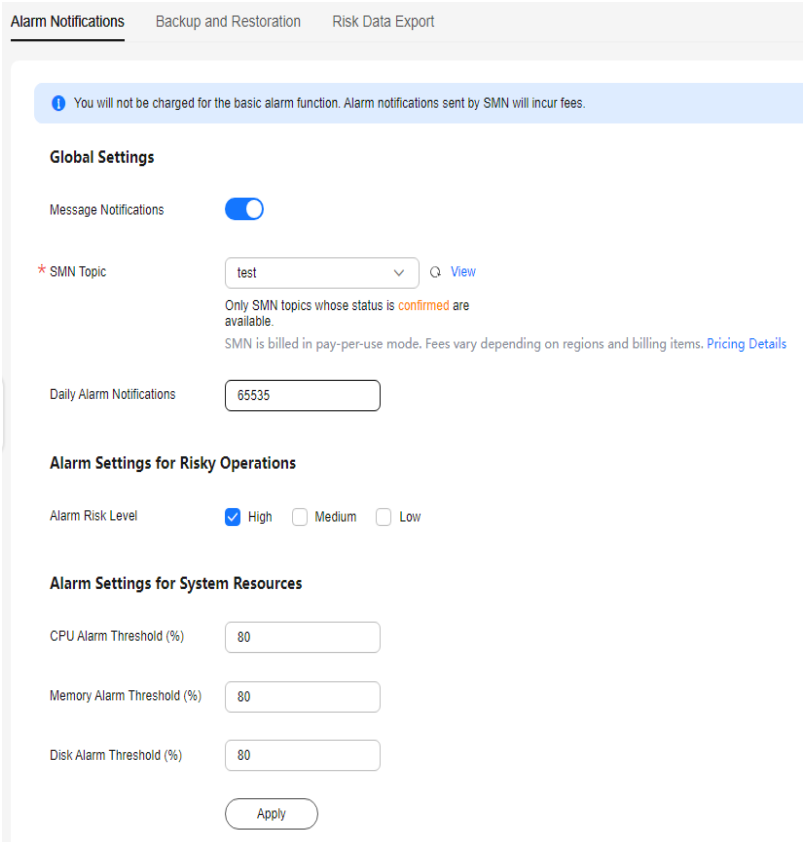



**Table 7-1** Alarm notification parameters

| 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**.<br>• : disabled<br>• : enabled | |

| Parameter | Description | Example Value |
| --- | --- | --- |
| SMN Topic | • Select an existing topic from the drop-down list or click **View** to create a topic. For details, see **Creating a Topic**.<br>• 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**.<br>**NOTE**<br>Before selecting a topic, ensure that the subscription status of the topic is **Confirmed**. Otherwise, alarm notifications may not be received.<br>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<br>**NOTICE**<br>• If the number of alarms exceeds this value on a day, no more notification will be sent on that day.<br>• 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:<br>• **High**<br>• **Moderate**<br>• **Low** | High |
| CPU Alarm Threshold (%) | CPU alarm threshold of an audit instance. When the threshold is exceeded, an alarm notification is generated. | 80 |
| Memory Alarm Threshold (%) | Memory alarm threshold of an audit instance. When the threshold is exceeded, an alarm notification is generated. | 80 |
| Disk Alarm Threshold (%) | Disk alarm threshold of an audit instance. When the threshold is exceeded, an alarm notification is generated. | 80 |

**Step 7** Click **Apply**.

**----End**

# 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

- The database audit instance is in the **Running** state.
- For details about how to enable database audit, see **Enable Database Audit**.

### Procedure

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

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

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

**Step 4** Click the name of the instance 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**, **Today**, **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

- The database audit instance is in the **Running** state.
- For details about how to enable database audit, see **Enable Database Audit**.
- Set alarm notification by referring to **Configuring Alarm Notifications**.

## Procedure

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

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

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

**Step 4** Click the name of an instance, click the **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 alarms

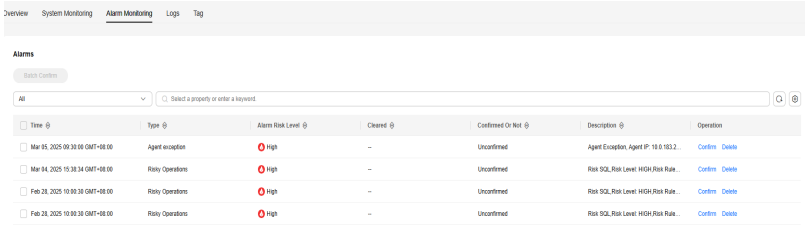


**Table 8-1** Parameters of alarms

| Parameter | Description |
| --- | --- |
| Time | Time when an alarm occurred. |
| Type | Alarm type. The options are as follows:<br>• Audit traffic exceeds threshold<br>• CPU exceptions<br>• Memory exceptions<br>• Disk exceptions<br>• Insufficient audit log storage<br>• Log backup to OBS failed<br>• Agent exceptions<br>• Risky operations |
| Alarm Risk Severity | Risk severity of an alarm. The options are as follows:<br>• **High**<br>• **Moderate**<br>• **Low** |
| Cleared | Time when an alarm is cleared |
| Confirmed Or Not | Confirmation status of an alarm. |
| Description | Description of an alarm |
| Operation | Operations supported by alarms, including:<br>• Confirm<br>• Delete<br>• Database backup |

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.
- Set the confirmation status (**Unconfirmed** or **Confirmed**). Alarms in this status are displayed in the list.

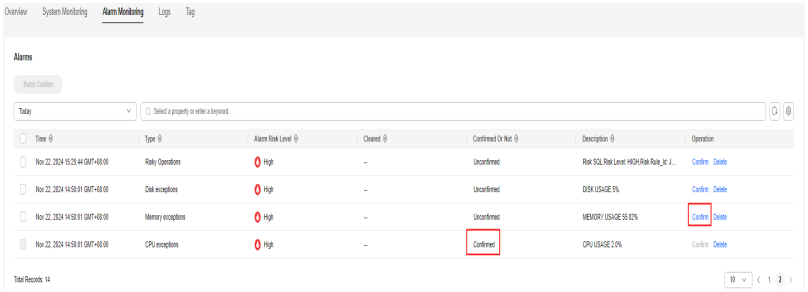
**----End**

## Follow-Up Procedure

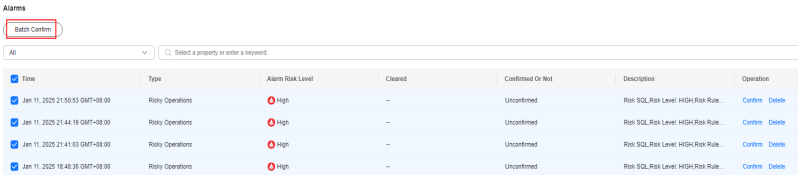
- To confirm an alarm, click **Confirm** in the **Operation** column of the alarm. The alarm status changes to **Confirmed**.

  **Figure 8-3** Confirming an alarm

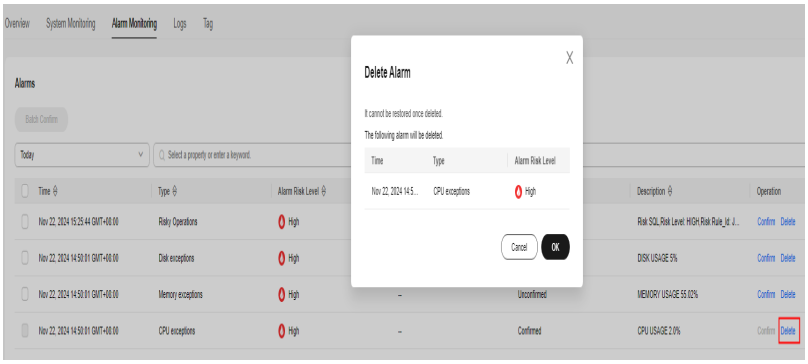
  You can select multiple alarms to be confirmed and click **Batch Confirm** to batch confirm alarms.

  **Figure 8-4** Confirming alarms in batches

- If an alarm has been handled, you can click **Delete** in the **Operation** column of the row that contains the alarm. In the dialog box that is displayed, click **OK**.

  **Figure 8-5** Deleting an alarm

- If the alarm type of an alarm is ransomware protection rule, locate the row that contains the alarm and click database backup in the **Operation** column. For details, see **Creating a Manual Backup**.

# 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

- The database audit instance is in the **Running** state.
- For details about how to enable database audit, see **Enable Database Audit**.

## 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:

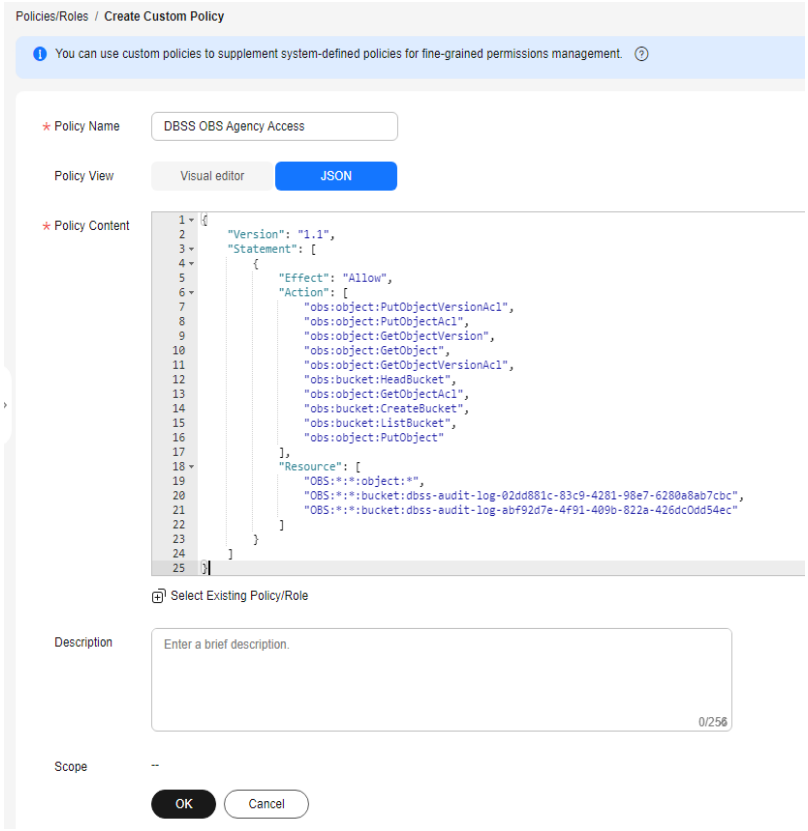
```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "obs:object:PutObjectVersionAcl",
            "obs:object:PutObjectAcl",
            "obs:object:GetObjectVersion",
```

```
            "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

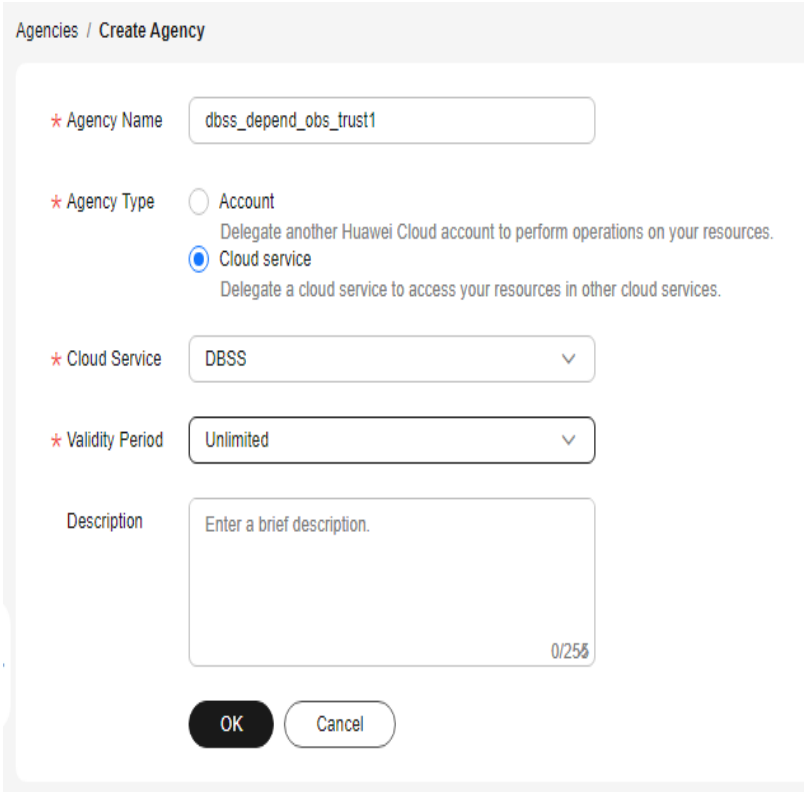



**Step 5** In the navigation pane, choose **Agencies** and then click **Create Agency** in the upper right corner.

**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**.

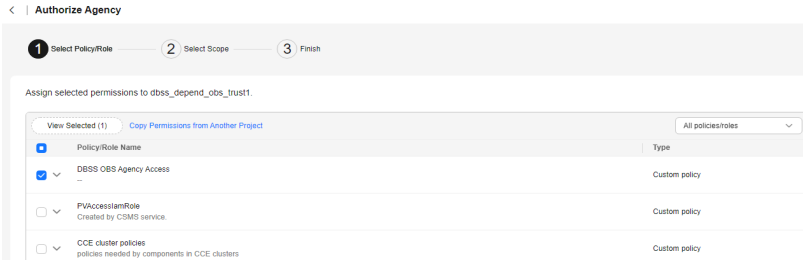
  

**Figure 9-2** Creating an agency




**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.

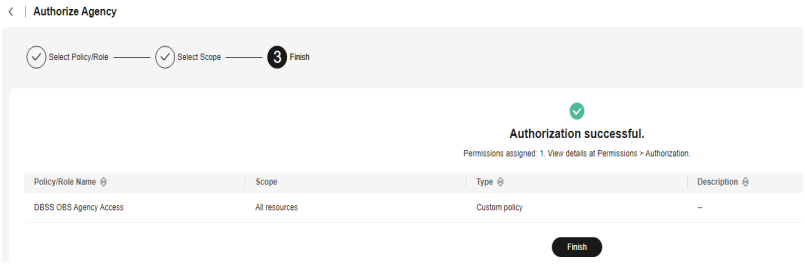
**Figure 9-3** Selecting a policy




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

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

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

**Step 5** Click **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

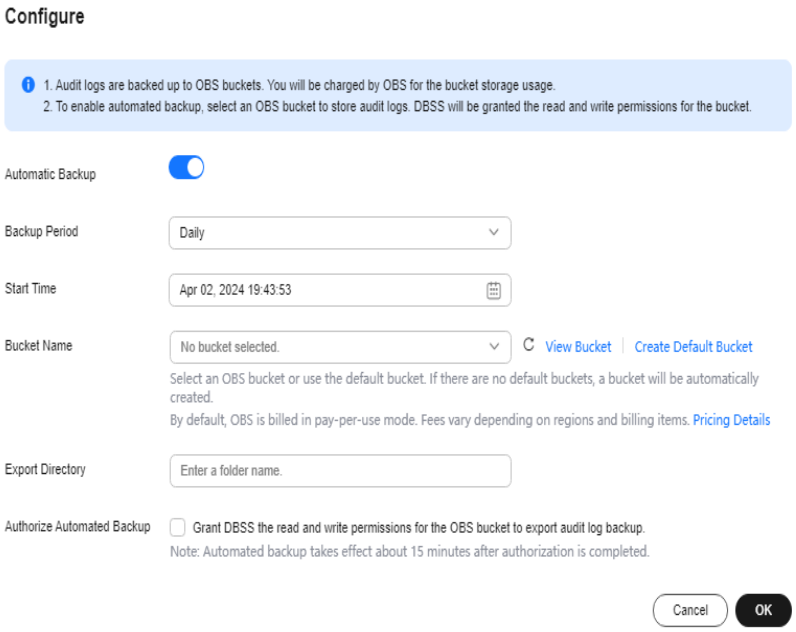


**Table 9-1** Parameters

| Parameter | Description | Example Value |
| --- | --- | --- |
| Automatic Backup | Status of automatic backup<br>•  : enabled<br>•  : disabled |  |
| Backup Period | Automatic backup period. Its options are as follows:<br>• **Daily**<br>• **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:<br>• Create Default Bucket<br>• Select Bucket<br>**NOTE**<br>• If you click **Create Default Bucket**, you will be prompted to authorize OBS for exporting audit log backups.<br>• 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 |
| Authorize Automated Backup | Authorize automatic backup before setting an automatic backup task. If you select this option, DBSS can read and write the OBS bucket for audit log backup and export.<br>**CAUTION**<br>Automated backup takes effect about 15 minutes after authorization is completed. | Selected |

**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.

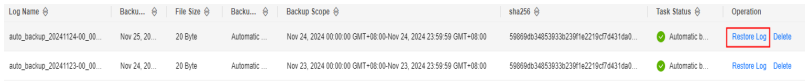
**Step 2** Click ☰ and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

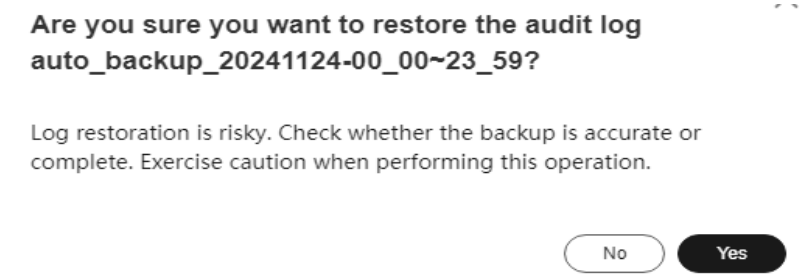
**Step 5** In the **Operation** column of the backup log to be restored, click **Restore Log**.

**Figure 9-6** Restoring logs




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

**Figure 9-7** Confirming the restoration of audit logs




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

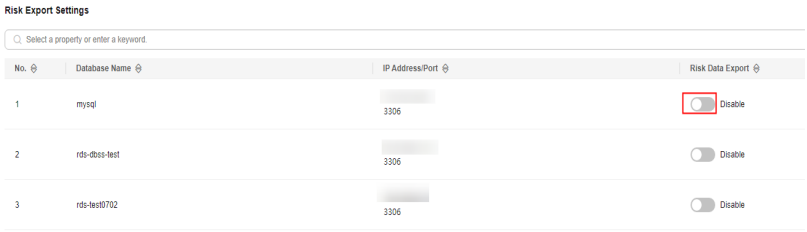
**Step 3** In the navigation tree on the left, choose **Settings**.

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

**Step 5** Click  in the row of a database to export risk data.

**Figure 9-8** Enabling risk export



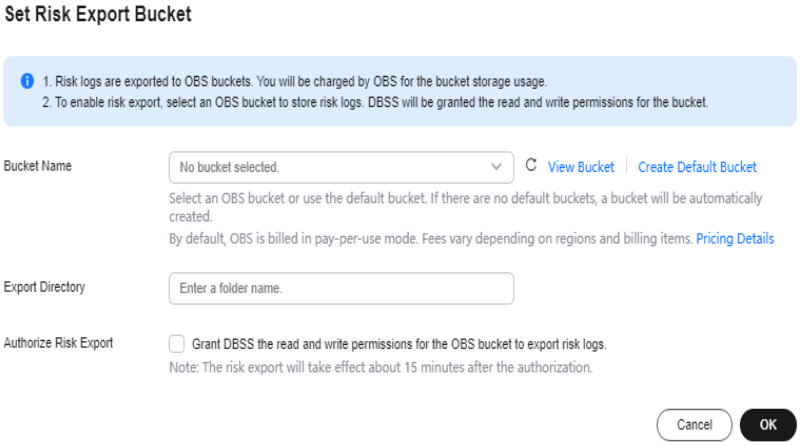

**Step 6** An OBS bucket will be automatically created to store risk logs.

- **Bucket Name**:Click **Create Default Bucket** or **Select Bucket**.
- **File Export Directory**: Create a directory for storing risk files in the OBS bucket.
- Risk export authorization: Authorize risk export before setting the risk export bucket. After the risk export authorization is selected, DBSS can obtain the read and write permissions of the OBS bucket for exporting risk logs.

**CAUTION**

The risk export takes effect about 15 minutes after the authorization is successful.

**Figure 9-9** 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

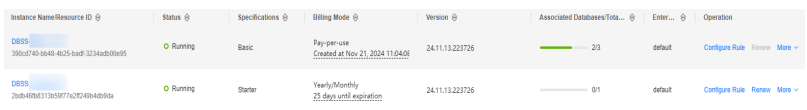
**Step 1** Log in to the management console.

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

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

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

**Figure 10-1** Viewing database audit instances




NOTE

- You can click the name of an instance to view its overview.
- You can search for an instance by instance name, status, instance specifications, resource ID, billing mode, version, or enterprise project in the filter box above the list.

**Table 10-1** Parameters

| Parameter | Description |
| --- | --- |
| Instance Name/ Resource ID | Instance name and resource ID. The resource ID is automatically generated by the system. |
| 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:<br>• **Running**<br>• **Creating**<br>• **Faulty**<br>• **Disabled**<br>• **Frozen**<br>• **Frozen for legal management**<br>• **Frozen due to abuse**<br>• **Frozen due to lack of identity verification**<br>• **Frozen for partnership**<br>• **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:<br>• Configure Rules<br>• Renewal<br>• Enable<br>• Disable<br>• Restart<br>• View Details<br>• View Metric<br>• Auto-renew<br>• Unsubscribing<br>• Release<br>• 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

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

## Procedure

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

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

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

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

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

**Figure 10-2** Viewing the instance overview

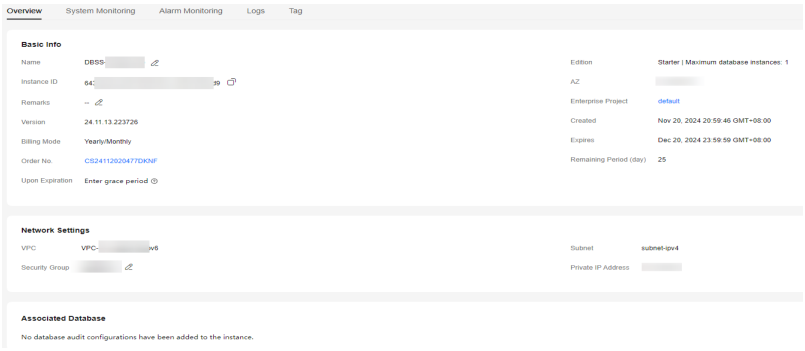



**Table 10-2** Parameters of the instance overview

| Category | Parameter | Description |
| --- | --- | --- |
| Basic Info | Name | Instance name. You can click next to **Name** to change it. |
| | ID | Instance ID, which is automatically generated |
| | AZ | Availability Zone (AZ) where an instance resides |
| | Version | Version of the DBSS instance when you create the DBSS instance. The version of the DBSS instance created at different time may be different.<br>Impact scope of DBSS instance versions:<br>● Supported database types<br>● Supported database versions |
| | Remarks | Remarks about an instance. You can click next to **Remarks** to modify it. |
| | Edition | Edition of an instance |
| | Created | Time when an instance is created |
| | Expiration | Time when an instance expires |
| | Enterprise Project | Enterprise project name of the instance |
| | Billing Mode | The billing mode is yearly/monthly. |
| | Order No. | Order number of the instance. Click the order number to view the order details. |
| | Upon Expiration | Policy used after an instance expires. The options are as follows:<br>● Auto-renewal<br>● Enter grace period |

| Category | Parameter | Description |
| --- | --- | --- |
| | Remaining Period (day) | Remaining days before the instance expires. |
| 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<br>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

- The database audit instance is in the **Running** state.
- Add a database by referring to **Adding Databases**.
- 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** Click ☰ and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

**Step 5** View the database information. For details about related parameters, see **Table 10-3**.

You can select an attribute from the search box above the list or enter a keyword to search for a specified database.

**Table 10-3** Parameters

| Parameter | Description |
| --- | --- |
| Database Information | Name, type, and version of a database |
| Character Set | Encoding character set of the database |
| IP Address/Port | The IP address and port number of the database. |
| Instance | Database instance name |
| OS | Operating system of the database |
| Audit Status | Audit status of the database. The options are as follows:<br>• **Enabled**<br>• **Disabled** |
| Agent | Click **Add** to add an agent for the database. |

NOTE

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

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

**----End**

## Viewing an Agent

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

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

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

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

**Step 5** Click ⌄ on the left of the database to expand the agent details. For details about related parameters, see **Table 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**.<br>**NOTE**<br>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**.<br>**NOTE**<br>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

- The database audit instance is in the **Running** state.
- The audit scope is added. For details, see **Adding Audit Scope**.
- 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** Click ☰ and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

**Step 5** View the audit scope information. For details about related parameters, see **Table 10-5**.

You can select an attribute from the search box above the list or enter a keyword to search for the specified audit scope.

**Figure 10-3** Viewing the audit scope


**Table 10-5** Parameters

| Parameter | Description |
| --- | --- |
| Name | Name of the audit scope |

| Parameter | Description |
| --- | --- |
| 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:<br>• **Enabled**<br>• **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

- The database audit instance is in the **Running** state.
- For details about how to enable database audit, see **Enable Database Audit**.

## Procedure

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

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

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

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

**Step 5** View information about SQL injection detection. For details about related parameters, see **Table 10-6**.

You can select an attribute from the search box above the list or enter a keyword to search for a specified SQL injection rule.

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

**Figure 10-4** Viewing information about the SQL injection detection

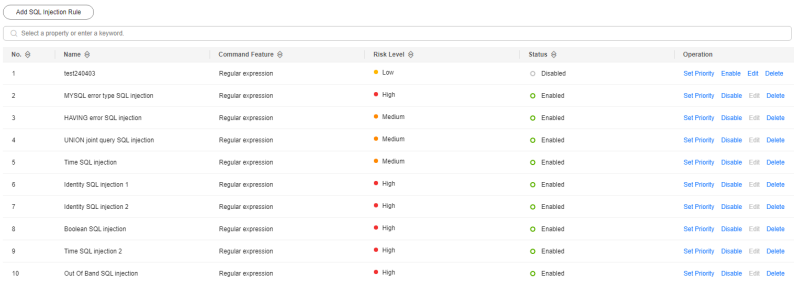



**Table 10-6** Parameters

| 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:<br>• **High**<br>• **Medium**<br>• **Low**<br>• **No risks** |
| Status | Status of the SQL injection detection. The options are as follows:<br>• Enabled<br>• Disabled |

| Parameter | Description |
| --- | --- |
| Operation | Operations on an SQL injection rule. The options are as follows:<br>• **Set Priority**<br>• **Disable**<br>• **Edit**<br>• **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

- The database audit instance is in the **Running** state.
- The risky operation is added. For details, see **Adding Risky Operations**.
- Before enabling the risky operation, ensure that its status is **Disabled**.
- Before disabling the risky operation, ensure that its status is **Enabled**.

## Precautions

If the risky operation is a system rule, setting priorities, editing, or deleting operations are not supported.

## Sets the Priority of the Risky Operation

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

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

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

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

**Step 5** In the row containing the risky operation for which you want to set a priority, click  in the **Priority** column.

**Step 6** Click **OK**.

**----End**

## Viewing the Risky Operation

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

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

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

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

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

**Step 6** View the risky operation information. For details about related parameters, see **Table 10-7**.

You can select an attribute from the search box above the list or enter a keyword to search for a specified risky operation.

**Figure 10-5** Viewing risky operations

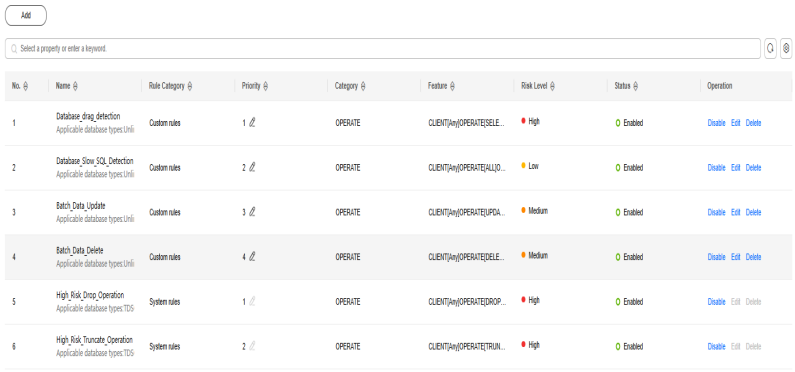



**Table 10-7** Parameters

| Parameter | Description |
| --- | --- |
| Name | Name of the risky operation |
| Rule Category | Risky operation type. The options are as follows:<br>• Custom rules<br>• System rules |
| Priority | Priority of a risky operation. |
| Category | Category of the risky operation |
| Feature | Feature of the risky operation |

| Parameter | Description |
| --- | --- |
| Risk Severity | Risk severity of the risky operation. The options are as follows:<br>• **High**<br>• **Moderate**<br>• **Low**<br>• **No risks** |
| Status | Status of the risky operation. The options are as follows:<br>• **Enabled**<br>• **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

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

## Viewing Privacy Data Protection Rules

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

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

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

**Step 4** In the **Instance** drop-down list, select an instance to view its privacy data protection rule.

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

NOTE

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

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

**Figure 10-6** Masking rule information

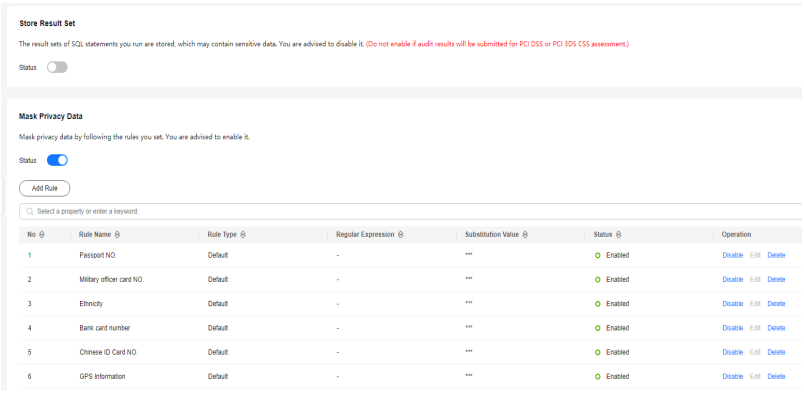



**Table 10-8** Masking rule parameters

| Parameter | Description |
| --- | --- |
| Rule Name | Rule name |
| Rule Type | Rule type.<br>• Default<br>• User-defined |
| Regular Expression | Regular expression that specifies the sensitive data pattern |

| Parameter | Description |
| --- | --- |
| Substitution Value | Value used to replace sensitive data specified by the regular expression |
| Status | Status of a rule. Its value can be:<br>• **Enabled**<br>• **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

- The database audit instance is in the **Running** state.
- For details about how to enable database audit, see **Enable Database Audit**.
- For details about how to generate an audit report, see **Step 1: Generating a Report**.

## Viewing a Report

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

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

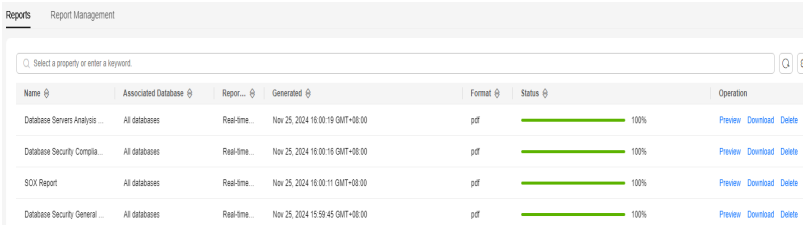
**Step 3** In the navigation tree on the left, choose **Reports**.

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

**Step 5** Viewing reports

**Figure 10-7** Viewing a report




**NOTE**

- You can select an attribute from the search box above the list or enter a keyword to search for a specified report.
- 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** Click  and choose **Security** > **Database Security Service**. The **Dashboard** page is displayed.

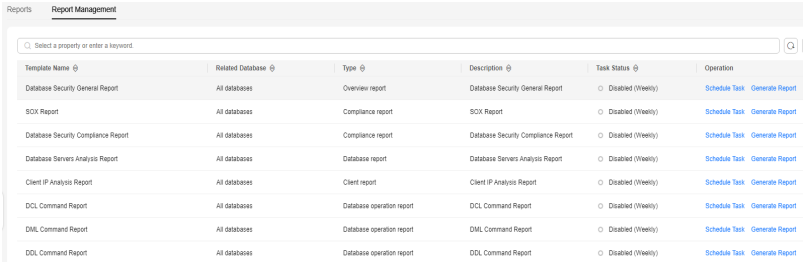
**Step 3** In the navigation tree on the left, choose **Reports**.

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

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

**Step 6** View the report template.

**Figure 10-8** Viewing the template list



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

- The database audit instance is in the **Running** state.
- For details about how to enable database audit, see **Enable Database Audit**.
- For details about how to back up audit logs, see **Backing Up and Restoring Database Audit Logs**.

## Viewing Backup Audit Logs

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

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

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

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

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

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

You can select **All**, **1 hour**, **24 hours**, **7 days**, **30 days**, or a custom time range above the list to view backup logs. You can also select an attribute from the search box above the list or enter a keyword to search for specified backup logs.

**Figure 10-9** Viewing backup audit logs

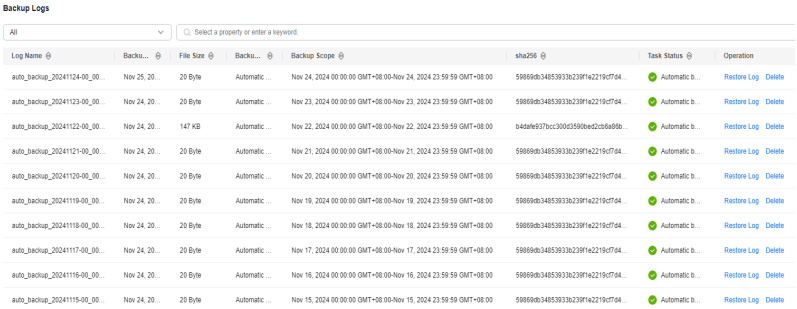


**Table 10-9** Parameters of audit logs

| 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. |
| sha256 | Verification value of the backup log |
| 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

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

## Procedure

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

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

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

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

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

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

Above the list, you can select **All**, **30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days**, or a custom time range to view the operation logs. You can also select an attribute from the search box above the list or enter a keyword to search for specified operation logs.

**Figure 10-10** Viewing operation logs

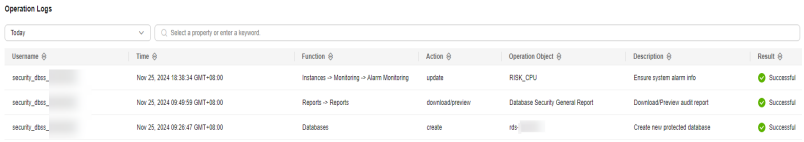



**Table 10-10** Parameters

| 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

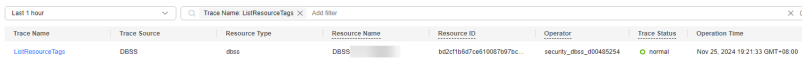
**Step 1** Log in to the management console.

**Step 2** In the navigation pane on the left, click  and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.

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

**Step 4** You can select **Last 1 hour**, **Last 1 day**, **Last 1 week**, or customize a time range above the list to view the events generated in the selected time range. You can also select an attribute from the search box above the list or enter a keyword to search for specified events.

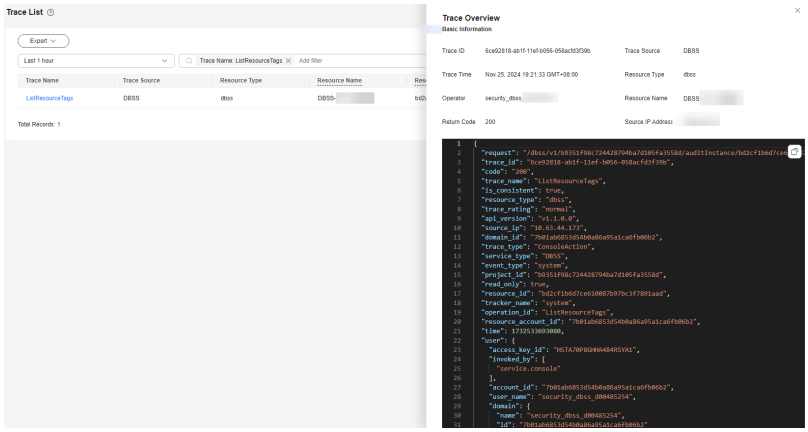
**Figure 11-1** Trace list




**Step 5** Click the name of an event to view its details.

**Figure 11-2** Viewing traces




**----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 | Unit | Number System | Monitored Object | Monitoring Interval (Raw Data) |
|---|---|---|---|---|---|---|---|
| cpu_util | CPU Usage | CPU consumed by the monitored object<br>Unit: %<br>Collection method: 100% minus idle CPU usage percentage | 0 to 100%<br>Value type: Float | % | N/A | Database audit instance | 1 minute |
| mem_util | Memory Usage | Memory usage of the monitored object<br>Unit: %<br>Collection method: 100% minus idle memory percentage | 0 to 100%<br>Value type: Float | % | N/A | Database audit instance | 1 minute |
| disk_util | Disk usage | Disk usage of the monitored object<br>Unit: %<br>Collection method: 100% minus idle disk space percentage | 0 to 100%<br>Value type: Float | % | N/A | Database audit instance | 1 minute |

| Metric ID | Metric Name | Description | Value Range | Unit | Number System | Monitored Object | Monitoring Interval (Raw Data) |
|---|---|---|---|---|---|---|---|
| hx_process_status | Protected Instance Process Status | The process status of a protected instance.<br>**NOTE**<br>This protected instance is no longer maintained. | 0/1<br>• **0**: The process status is abnormal.<br>• **1**: The process status is normal. | N/A | N/A | Database audit instance | 1 minute |
| hx_port_stats | Protected Instance Port Status | The port status of a protected instance.<br>**NOTE**<br>This protected instance is no longer maintained. | 0/1<br>• **0**: The port status is abnormal.<br>• **1**: The port status is normal. | N/A | N/A | Database audit instance | 1 minute |
| hx_proxy_num | Protected Instance Agents | The number of agents of a protected instance.<br>**NOTE**<br>This protected instance is no longer maintained. | ≥0 | Count | N/A | Database audit instance | 1 minute |

| Metric ID | Metric Name | Description | Value Range | Unit | Number System | Monitored Object | Monitoring Interval (Raw Data) |
|---|---|---|---|---|---|---|---|
| hx_proxy_status | Protected Instance Agent Status | The agent status of a protected instance.<br>**NOTE**<br>This protected instance is no longer maintained. | 0/1<br>• **0**: The agent status is abnormal.<br>• **1**: The agent status is normal. | N/A | N/A | Database audit instance | 1 minute |
| hx_qps | Queries per Second | The number of queries per second on the instance.<br>**NOTE**<br>This protected instance is no longer maintained. | ≥0 | Count/s | N/A | Database audit instance | 1 minute |
| hx_rps | Requests per Second | The number of requests per second on the instance.<br>**NOTE**<br>This protected instance is no longer maintained. | ≥0 | Count/s | N/A | Database audit instance | 1 minute |

| Metric ID | Metric Name | Description | Value Range | Unit | Number System | Monitored Object | Monitoring Interval (Raw Data) |
|---|---|---|---|---|---|---|---|
| hx_active_connections_num | Protected Instance Active Connections | The number of active connections of a protected instance.<br>**NOTE**<br>This protected instance is no longer maintained. | ≥0 | Count | N/A | 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

Purchase database audit by referring to **Purchasing DBSS**.

## 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**.

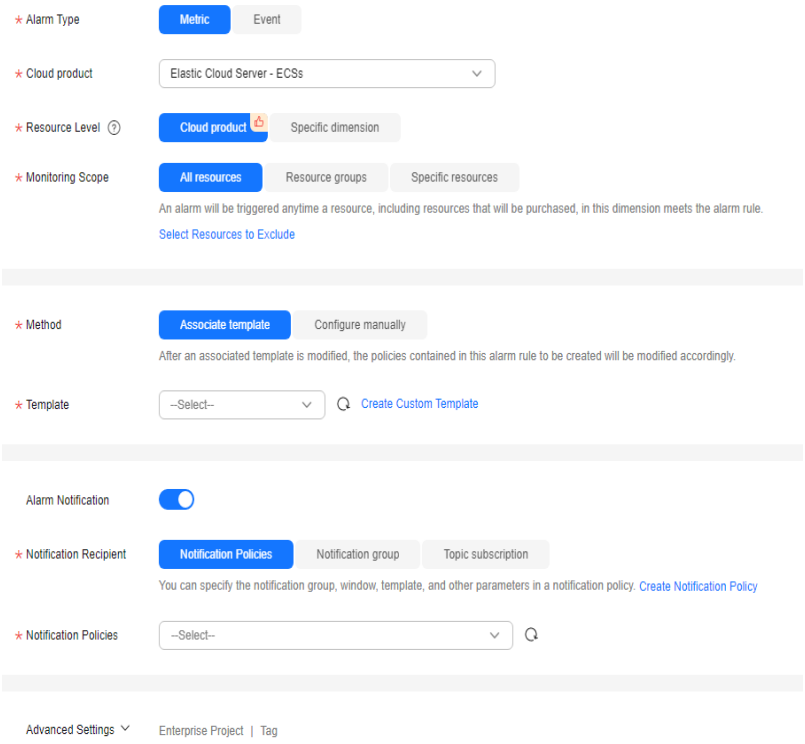
**Step 5** Set the alarm rule name.

**Figure 12-1** Setting the alarm rule name

**Step 6** Select **Metric** for **Alarm Type**, select **DBSS** from the **Cloud Product** drop-down list, and set the **Resource Level**, **Monitoring Scope**, **Method**, **Template**, **Alarm Notification**, **Notification Recipient**, and **Notification Policies**, as shown in **Figure 12-2**.

**Figure 12-2** 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.

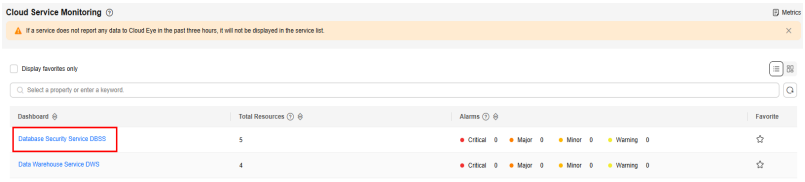
**Step 2** Click ☰ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

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

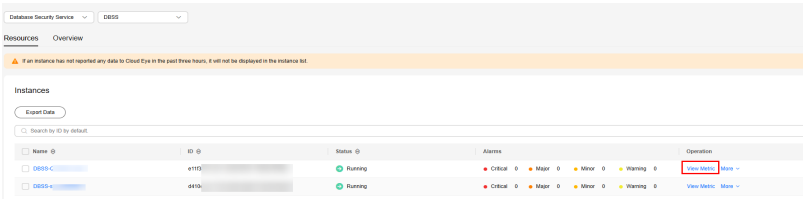
**Step 4** Click the dashboard name **Database Security Service DBSS**.

**Figure 12-3** Cloud service monitoring




**Step 5** In the row containing the dedicated DBSS instance, click **View Metric** in the **Operation** column.

**Figure 12-4** Viewing monitoring metrics




**----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.

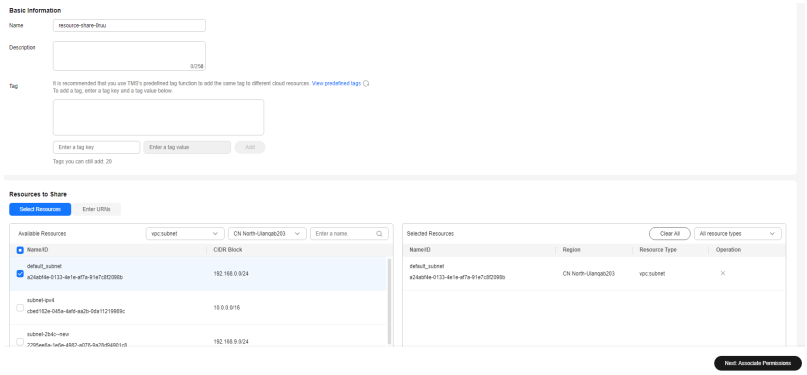
**Step 2** Click in the upper left corner, choose **Management & Governance** > **Resource Access Manager**, and go to the resource access management page.

**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**.

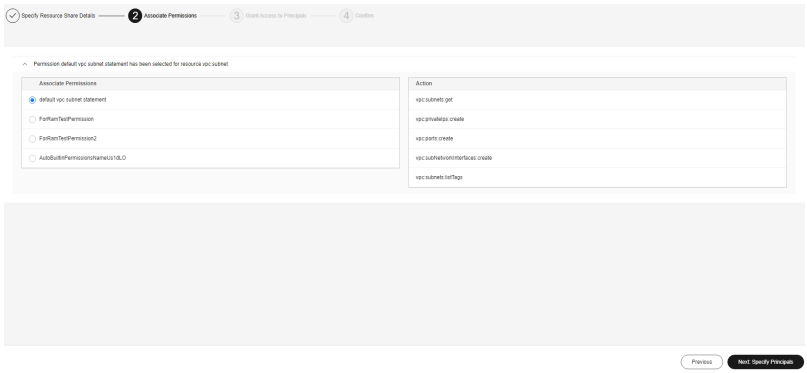
**Figure 13-1** Specifying shared resources




**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.

**Figure 13-2** Configuring permissions



**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.

**Figure 13-3** Specifying principals

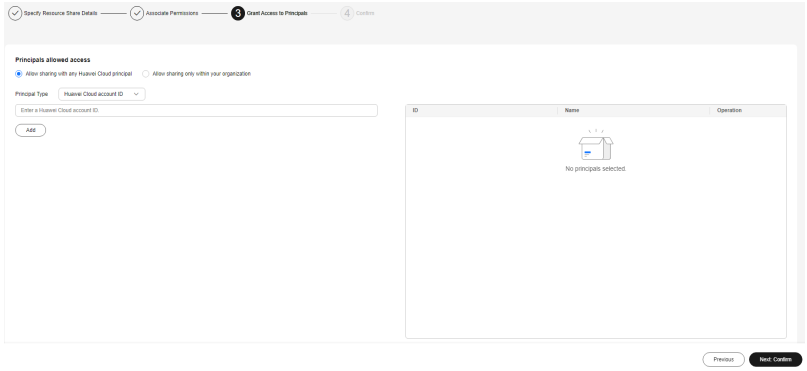


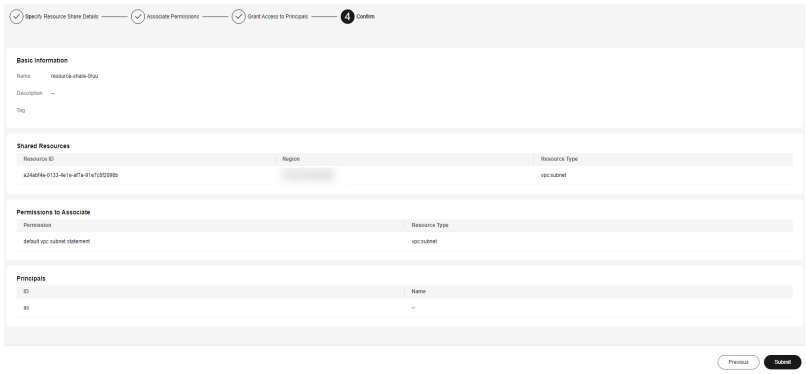
**Table 13-1** Parameter descriptions

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

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

**Figure 13-4** Confirming configurations




**----End**

## Using a VPC

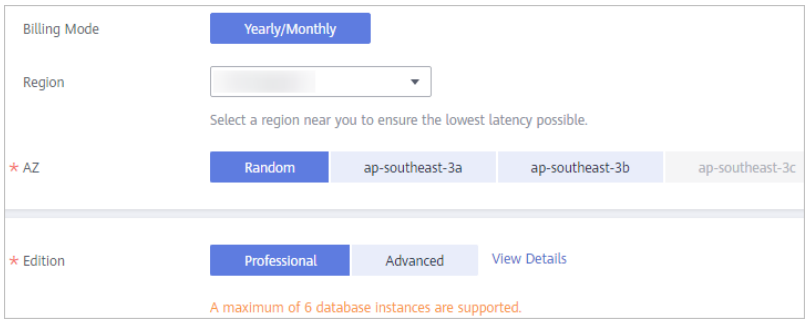
**Step 1** Log in to the management console.

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

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

**Step 4** Select a region, an AZ type, an AZ, and an edition.

**Figure 13-5** 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** DBSS editions

| Edition | Maximum Databases | Performance |
| --- | --- | --- |
| Professional | 6 | • Peak QPS: 6,000 queries/second<br>• Database load rate: 7.2 million statements/hour<br>• Online SQL statement storage: 600 million statements |
| Advanced | 30 | • Peak QPS: 30,000 queries/second<br>• Database load rate: 10.8 million records/hour<br>• Online SQL statement storage: 1.5 billion 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 13-6** Setting database audit parameters

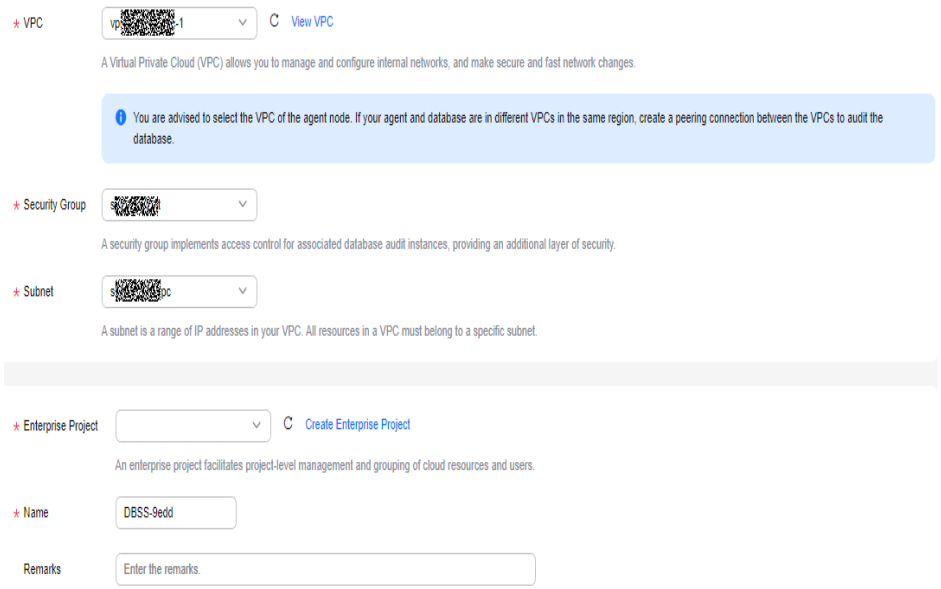



**Table 13-3** Database audit instance parameters

| Parameter | Description |
| --- | --- |
| VPC | You can select an existing VPC, or click **View VPC** to create one on the VPC console.<br>**NOTE**<br>• 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?**<br>• To change the VPC of a DBSS instance, unsubscribe from it and purchase a new one.<br>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.<br>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

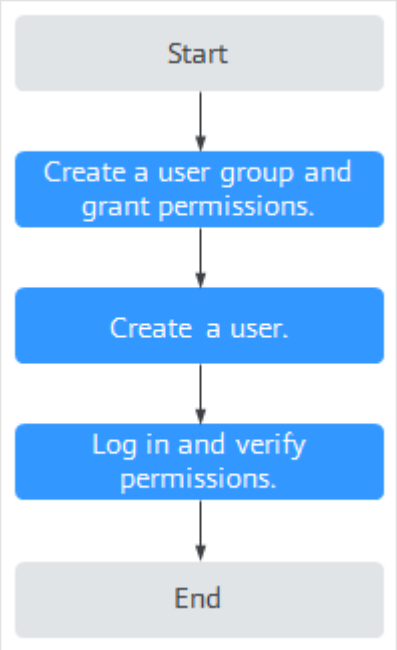
| Role/Policy Name | Description | Type | Dependency |
| --- | --- | --- | --- |
| DBSS Audit Administrator | DBSS audit administrator, who has the permissions to check DBSS security logs. | System-defined role | None |

| 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 |