## Database Security Service (DBSS)

# User Guide

| | |
|---|---|
| **Issue** | 01 |
| **Date** | 2025-07-11 |

**HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.**

## Trademarks and Permissions

## 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

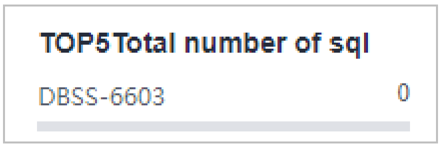
You can check the audit information about all instances by total number of SQLs, total number of risks, today's SQL, today's risks, and today's sessions.

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



TOP5Total number of sql

DBSS-6603 0

## 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>• 8.0.33<br>• 8.0.35<br>• 8.1.0<br>• 8.2.0 |
| Oracle | • 11g 11.1.0.6.0, 11.2.0.1.0, 11.2.0.2.0, 11.2.0.3.0, and 11.2.0.4.0<br>• 12c 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<br>• 8.1 |
| DAMENG | DM8 |
| KINGBASE | V8 |
| SHENTONG | V7.0 |
| GBase 8a | V8.5 |
| GBase 8s | V8.8_3.3.0 |
| Gbase XDM Cluster | V8.0 |

| Database Type | Edition |
|---|---|
| Greenplum | V6.0 |
| 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

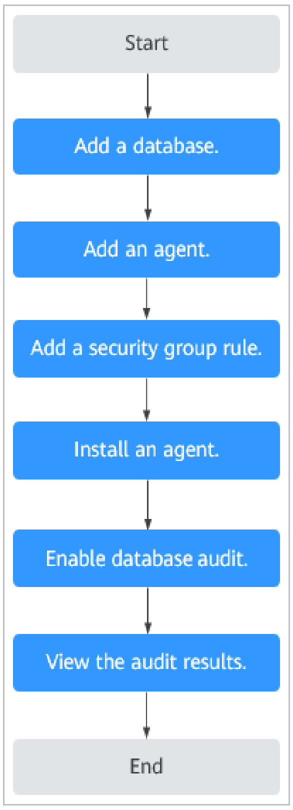


**Table 2-2** Procedure for quickly configuring database audit

| 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**. |

## Deploying the Database Audit Agent in a Container

For a database of any types and versions, you can deploy the agent using a container to enable database audit.

For details, see **Deploying the Database Audit Agent in a Container**

## 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 create a shared VPC, see **Shared VPC**.

  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. For details, see DBSS Permission Management .

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

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

**Step 4** Set **Basic Settings** and **Edition**.

**Table 2-3** Basic settings parameters

| Parameter | Description |
|---|---|
| Service Type | The value is fixed at **Database Audit Service**. |
| Billing Mode | Only the yearly/monthly mode is available. |
| Region | Select the region where the instance is located. Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region. |
| AZ Type | Only general AZs are supported. |

| Parameter | Description |
|---|---|
| AZ | An AZ is a physical location that uses an independent power supply and network. AZs in the same region can communicate with each other over an intranet.<br>You can select random allocation or specify an AZ. |

**Table 2-4** Edition specifications

| Parameter | Description |
|---|---|
| Edition specifications | **Basic**, **Standard**, **Professional**, and **Advanced** editions are available.<br>For details about the specifications supported by each edition, see **Table 2-5**. |

**Table 2-5** Database audit editions

| Edition | Specification | Maximum Databases | Performance |
|---|---|---|---|
| Starter | Database audit starter edition | 1 | ● Peak QPS: 1,000 queries/second<br>● Database load rate: 1.2 million statements/hour<br>● Online SQL statement storage: 100 million statements |
| Basic | Database audit basic edition | 3 | ● Peak QPS: 3,000 queries/second<br>● Database load rate: 3.6 million statements/hour<br>● Online SQL statement storage: 400 million statements |
| Professional | Database audit professional edition | 6 | ● Peak QPS: 6,000 queries/second<br>● Database load rate: 7.2 million statements/hour<br>● Online SQL statement storage: 600 million statements |

| Edition | Specification | Maximum Databases | Performance |
|---|---|---|---|
| Advanced | Database audit advanced edition | 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

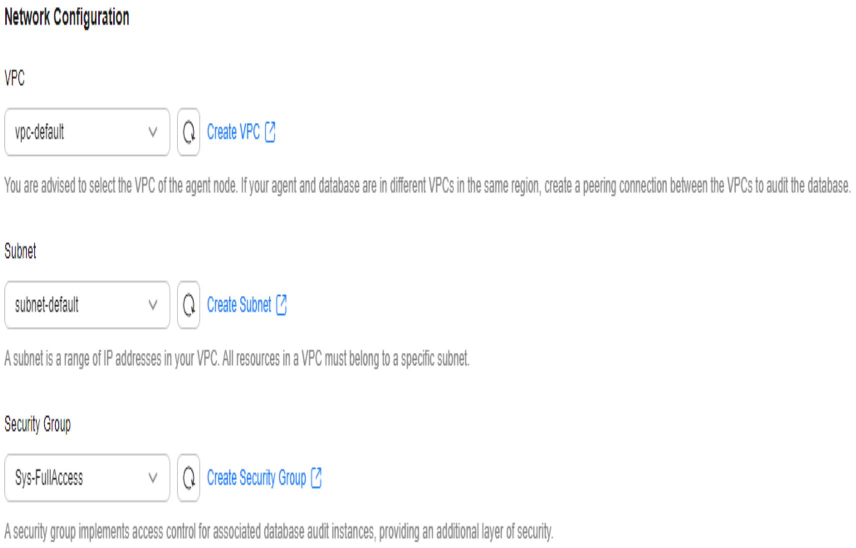
- A database instance is uniquely defined by its **database IP address and port**.

  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 2-6**.

**Figure 2-2** Network configuration



Network Configuration

VPC

vpc-default

You are advised to select the VPC of the agent node. If your agent and database are in different VPCs in the same region, create a peering connection between the VPCs to audit the database.

Subnet

subnet-default

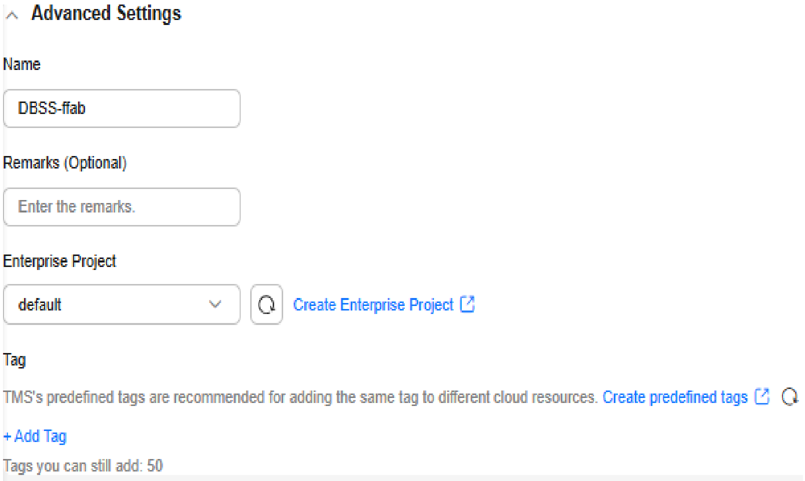
A subnet is a range of IP addresses in your VPC. All resources in a VPC must belong to a specific subnet.

Security Group

Sys-FullAccess

A security group implements access control for associated database audit instances, providing an additional layer of security.

**Figure 2-3** Advanced configuration



Advanced Settings

Name

DBSS-ffab

Remarks (Optional)

Enter the remarks.

Enterprise Project

default

Create Enterprise Project

Tag

TMS's predefined tags are recommended for adding the same tag to different cloud resources. Create predefined tags

+ Add Tag

Tags you can still add: 50

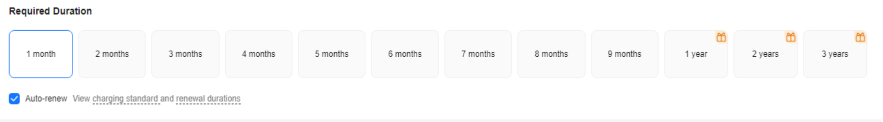
**Table 2-6** Database audit parameters

| 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 project, see **Enterprise Management User Guide**. |

| Parameter | Description |
|---|---|
| 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



Required Duration: 1 month

☑ Auto-renew View charging standard and renewal durations

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 2-7** describes the auto-renewal period.

**Table 2-7** 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.**

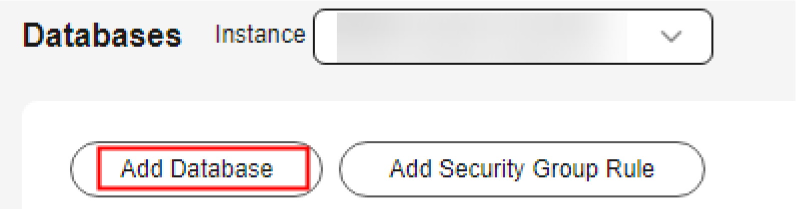
**Step 2** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

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

**Figure 2-5** Adding a database



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

**Table 2-8** 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 |

| Parameter | Description | Example Value |
|---|---|---|
| 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 |
| 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 |

| Parameter | Description | Example Value |
|---|---|---|
| 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>– 8.0.33<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>– 8.1<br>● When **Type** is set to **GaussDB(for MySQL)**, the following versions are available: | 5.0 |

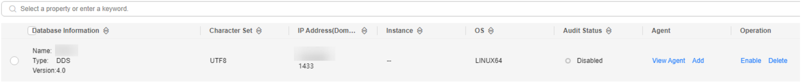
| Parameter | Description | Example Value |
|---|---|---|
| | – When **Database Type** is set to **Self-built database**, you can select the **Mysql 8.0** version.<br>– If **RDS database** is selected, a list of database instances will be displayed for you to choose from. You do not need to install the 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_3.3.0<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 | |

| Parameter | Description | Example Value |
|---|---|---|
| | - When **Type** is set to **MongoDB**, the following version is available:<br>  – v5.0<br>- 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 |

| Parameter | Description | Example Value |
|---|---|---|
| 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



Select a property or enter a keyword.

| | Database Information | Character Set | IP Address(Dom... | Instance | OS | Audit Status | Agent | Operation |
|---|---|---|---|---|---|---|---|---|
| ○ | Name: [redacted]<br>Type: DDS<br>Version:4.0 | UTF8 | [redacted]<br>1433 | -- | LINUX64 | ○ Disabled | View Agent Add | Enable Delete |

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

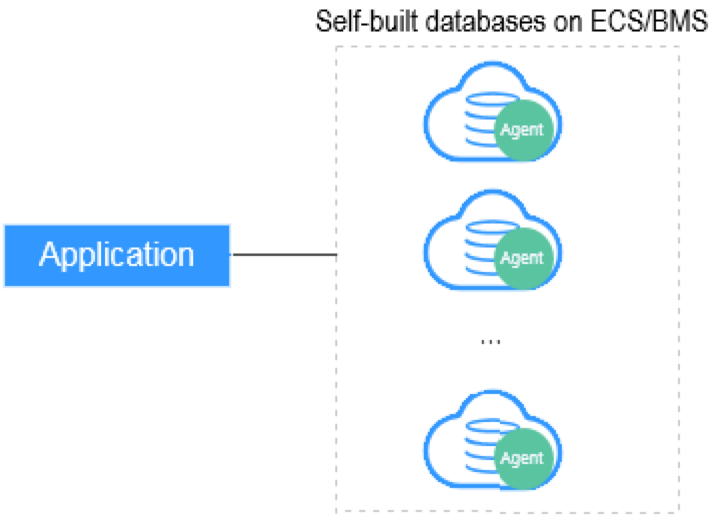
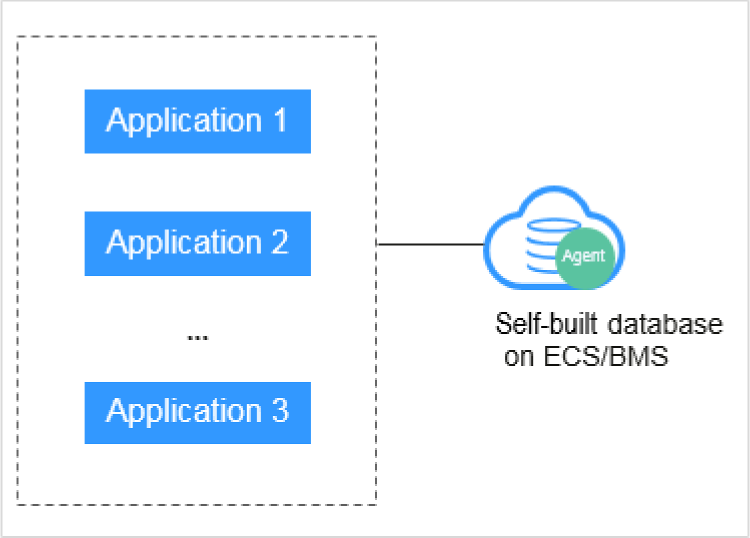


**Figure 2-8** Multiple applications connecting to one database built on ECS/BMS



- 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

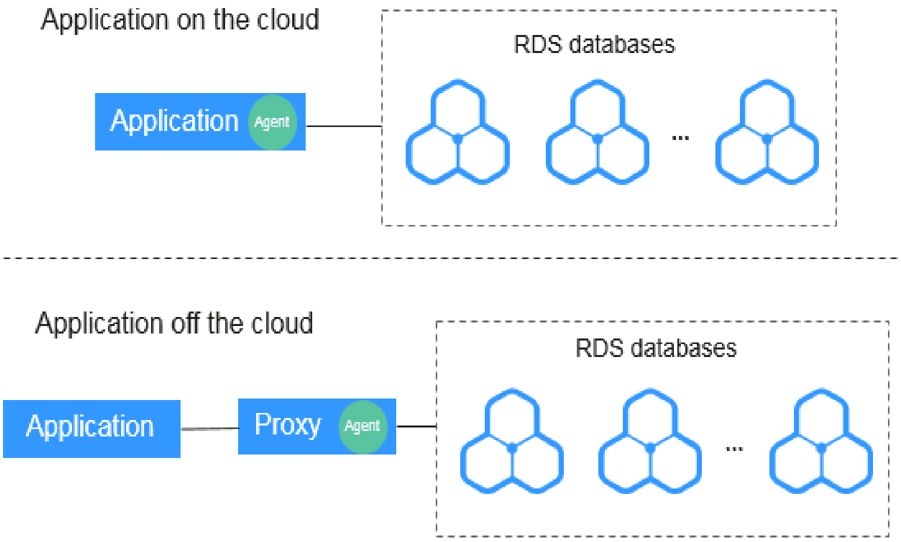


**Figure 2-10** Multiple applications connecting to one RDS database

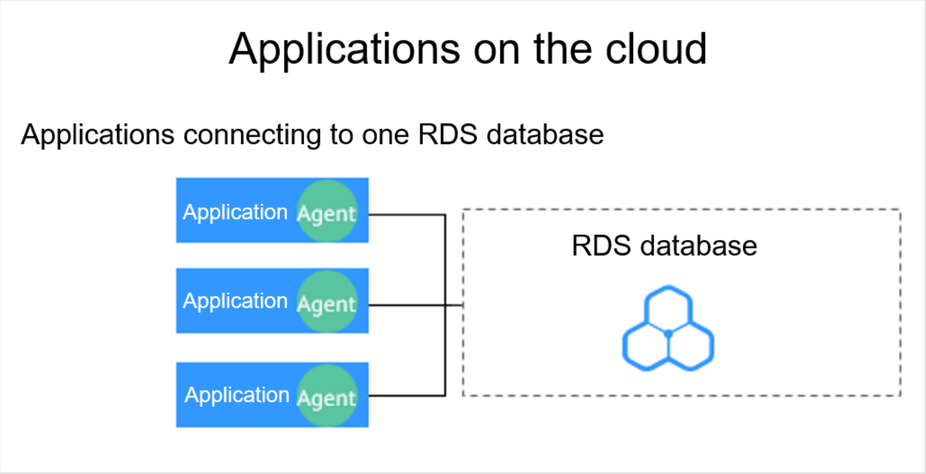

Applications on the cloud
Applications connecting to one RDS database
Application
Agent
Application
Agent
Application
Agent
RDS database

**Table 2-9** 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 2-9** 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. |

| Scenario | Where to Add the Agent | Audit Scope | Description |
|---|---|---|---|
| RDS database | Application (if applications are deployed on the cloud) | Access records of all the databases connected to the application | ● Add the agent on the application side.<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.**

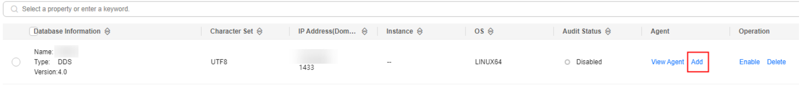
**Step 3** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

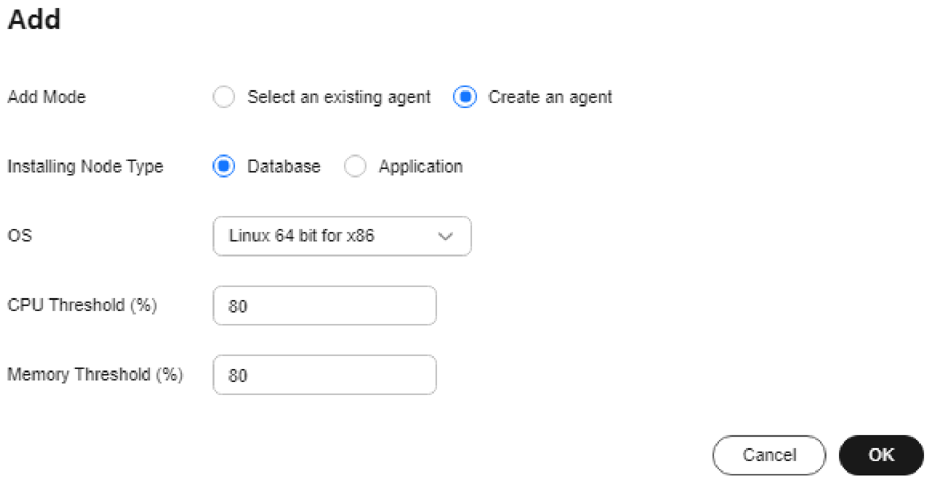


Select a property or enter a keyword.

| | Database Information | Character Set | IP Address(Dom... | Instance | OS | Audit Status | Agent | Operation |
|---|---|---|---|---|---|---|---|---|
| ○ | Name: [redacted]<br>Type: DDS<br>Version:4.0 | UTF8 | [redacted]<br>1433 | -- | LINUX64 | ○ Disabled | View Agent Add | Enable Delete |

**Step 7** In the displayed dialog box, select an add mode, as shown in **Figure 2-12**. For details about related parameters, see **Table 2-10**.

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



Add

Add Mode ○ Select an existing agent ● Create an agent

Installing Node Type ● Database ○ Application

OS Linux 64 bit for x86

CPU Threshold (%) 80

Memory Threshold (%) 80

**Table 2-10** Parameters for adding an agent (user-built databases on ECS/BMS)

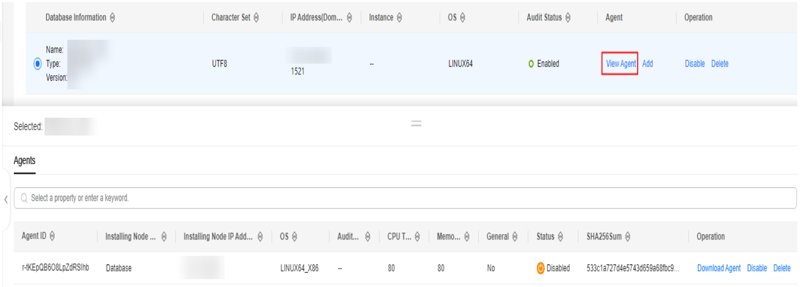
| Parameter | Description | Example Value |
|---|---|---|
| Add Mode | Mode for adding an agent<br>● **Select an existing agent**<br>If an agent has been installed on a database connected to the same application as the desired database, select **Select an existing agent**.<br>● **Create an agent**<br>If 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. | - |
| 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 |

| Parameter | Description | Example Value |
|---|---|---|
| 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



| Database Information | Character Set | IP Address(Dom... | Instance | OS | Audit Status | Agent | Operation |
|---|---|---|---|---|---|---|---|
| ● Name: [redacted]<br>Type:<br>Version: | UTF8 | [redacted]<br>1521 | -- | LINUX64 | ○ Enabled | View Agent Add | Disable Delete |

Selected: [redacted]

Agents

Select a property or enter a keyword.

| Agent ID | Installing Node ... | Installing Node IP Add... | OS | Audit... | CPU T... | Memo... | General | Status | SHA256Sum | Operation |
|---|---|---|---|---|---|---|---|---|---|---|
| r-tKEpQB6O8LpZdRSlhb | Database | [redacted] | LINUX64_X86 | -- | 80 | 80 | No | Disabled | 533c1a727d4e5743d659a68fbc9... | Download Agent Disable Delete |

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.**

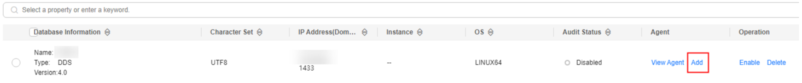
**Step 3** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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



Select a property or enter a keyword.

| | Database Information | Character Set | IP Address(Dom... | Instance | OS | Audit Status | Agent | Operation |
|---|---|---|---|---|---|---|---|---|
| ○ | Name: [redacted]<br>Type: DDS<br>Version:4.0 | UTF8 | [redacted]<br>1433 | -- | LINUX64 | ○ Disabled | View Agent Add | Enable Delete |

**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 2-11**.

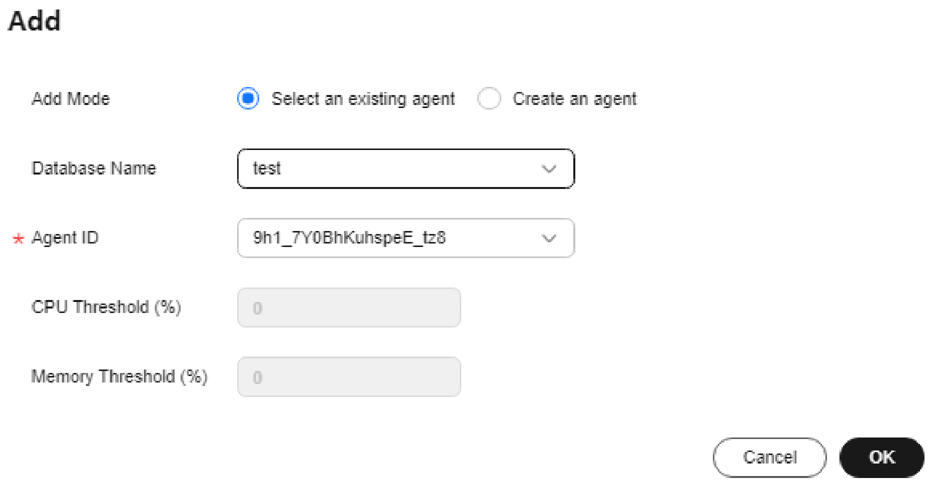
- Select **Select an existing agent** for **Add Mode**.

  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

  Add

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

  Database Name: test

  * Agent ID: 9h1_7Y0BhKuhspeE_tz8

  CPU Threshold (%): 0

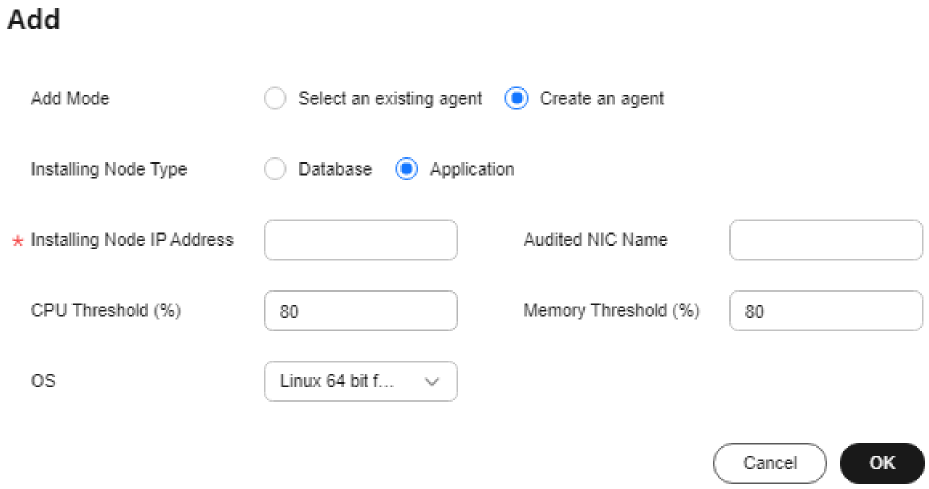
  Memory Threshold (%): 0

- 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



Add

Add Mode ○ Select an existing agent ● Create an agent

Installing Node Type ○ Database ● Application

* Installing Node IP Address:

Audited NIC Name:

CPU Threshold (%): 80

Memory Threshold (%): 80

OS: Linux 64 bit f...

**Table 2-11** Parameters for adding an agent (RDS databases)

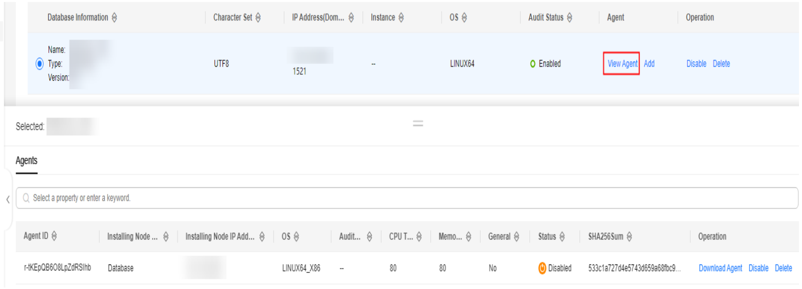
| Parameter | Description | Example Value |
|---|---|---|
| Add Mode | Mode for adding an agent<br>● **Selecting an existing agent**<br>If an agent has been installed on a database connected to the same application as the desired database, select **Select an existing agent**.<br>● **Create an agent**<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 |

| Parameter | Description | Example Value |
|---|---|---|
| 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 |
| 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



| Database Information | Character Set | IP Address(Dom... | Instance | OS | Audit Status | Agent | Operation |
|---|---|---|---|---|---|---|---|
| ● Name: [redacted]<br>Type:<br>Version: | UTF8 | [redacted]<br>1521 | -- | LINUX64 | Enabled | View Agent Add | Disable Delete |

Selected: [redacted]

Agents

Select a property or enter a keyword.

| Agent ID | Installing Node ... | Installing Node IP Add... | OS | Audit... | CPU T... | Memo... | General | Status | SHA256Sum | Operation |
|---|---|---|---|---|---|---|---|---|---|---|
| r-tKEpQB6O8LpZdRSlhb | Database | [redacted] | LINUX64_X86 | -- | 80 | 80 | No | Disabled | 533c1a727d4e5743d659a68fbc9... | Download Agent Disable Delete |

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.**

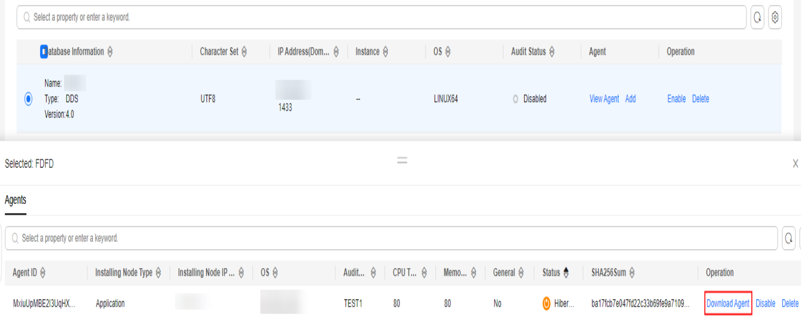
**Step 3** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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



Select a property or enter a keyword.

| | Database Information | Character Set | IP Address(Dom... | Instance | OS | Audit Status | Agent | Operation |
|---|---|---|---|---|---|---|---|---|
| ● | Name: [redacted]<br>Type: DDS<br>Version:4.0 | UTF8 | [redacted]<br>1433 | -- | LINUX64 | ○ Disabled | View Agent Add | Enable Delete |

Selected: FDFD

Agents

Select a property or enter a keyword.

| Agent ID | Installing Node Type | Installing Node IP ... | OS | Audit... | CPU T... | Memo... | General | Status | SHA256Sum | Operation |
|---|---|---|---|---|---|---|---|---|---|---|
| MxiuUpMBE2I3UqHX... | Application | [redacted] | [redacted] | TEST1 | 80 | 80 | No | Hiber... | ba17fcb7e047fd22c33b69fe9a7109... | Download Agent Disable Delete |

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

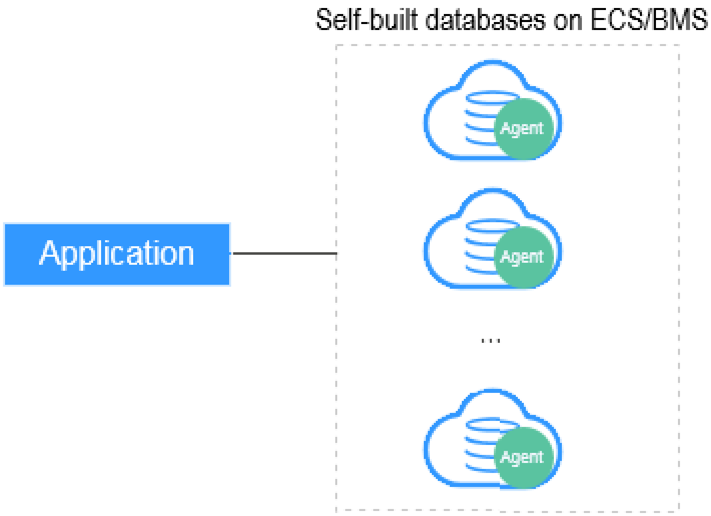
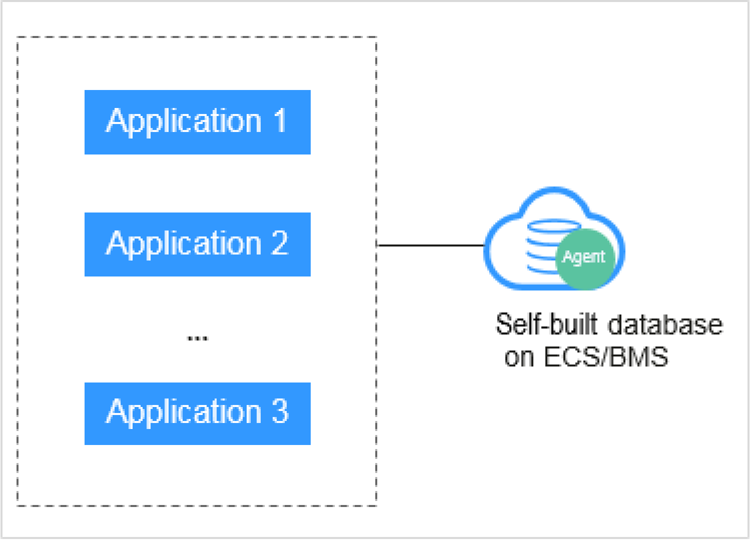


**Figure 2-20** Multiple applications connecting to one database built on ECS/BMS



- 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

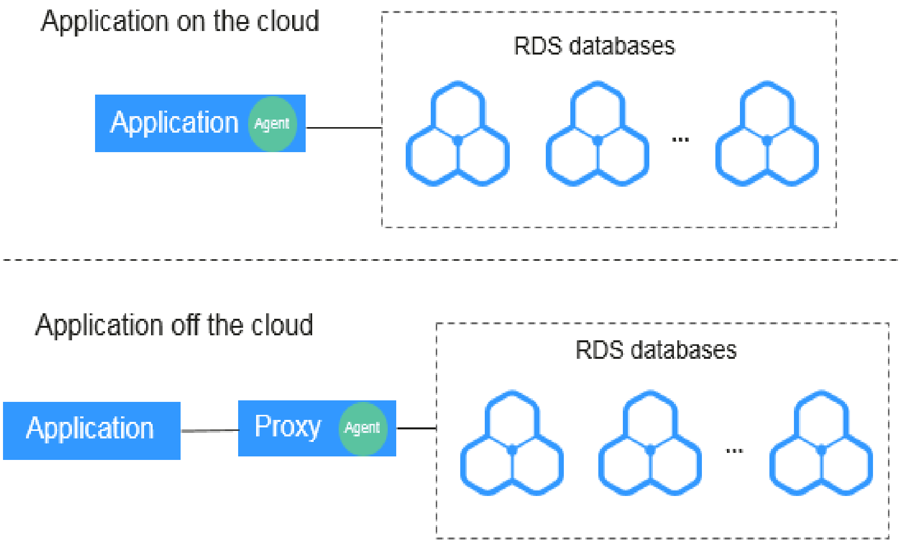


**Figure 2-22** Multiple applications connecting to one RDS database

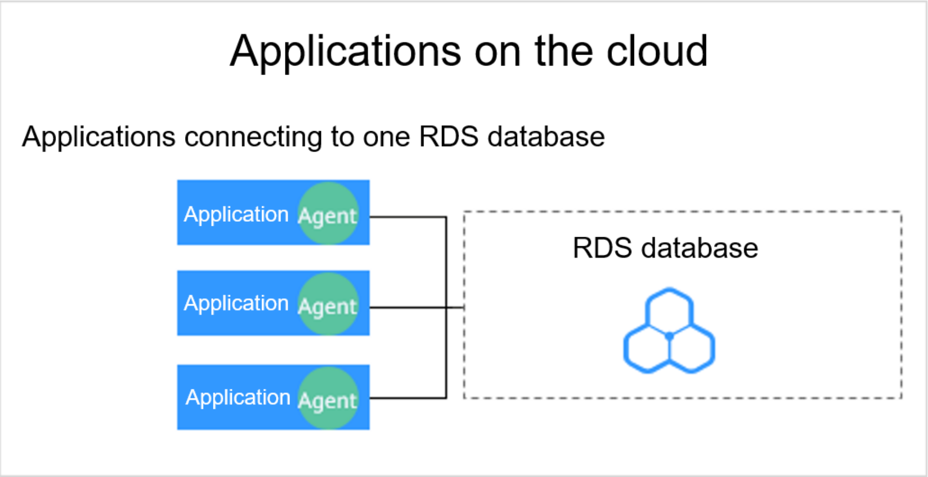

Applications on the cloud
Applications connecting to one RDS database
Application
Agent
Application
Agent
Application
Agent
RDS database

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

**NOTICE**

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

**Table 2-12** Agent installation scenarios

| Scenario | Where to Install Agent | Audit Scope | Description |
|---|---|---|---|
| Self-built database on ECS/BMS | Database | All access records of applications that have accessed the database | - Install the agent on the database side.<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

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**.

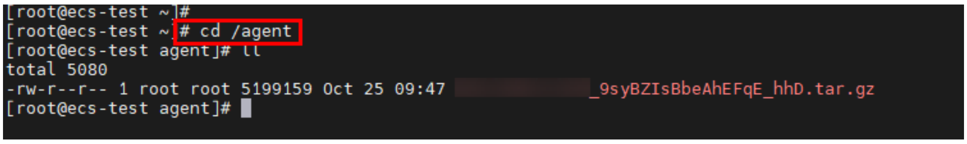
**Step 2** For details about how to obtain the agent installation package of the Linux, see **Downloading an Agent**.

**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:

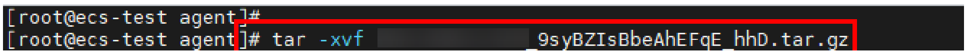
**cd** *Directory_containing_agent_installation_package*



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

**Step 6** Run the following command to decompress the installation package **xxx.tar.gz**:

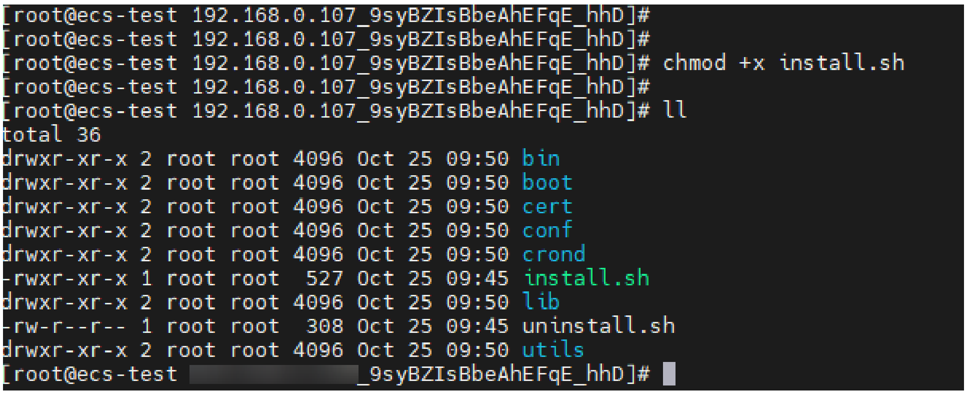
**tar -xvf** *xxx.tar.gz*



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

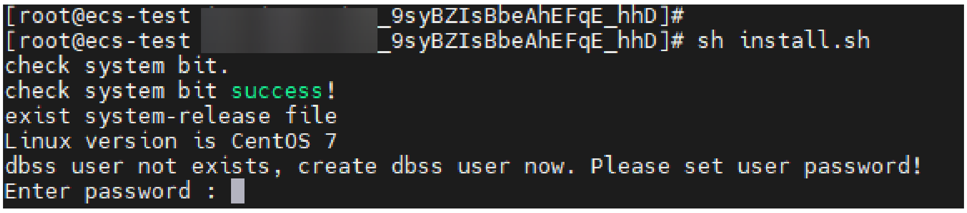
**Step 8** Run the following command to check whether you have the permission for executing the **install.sh** script:

**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 [redacted]_9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test [redacted]_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!
```

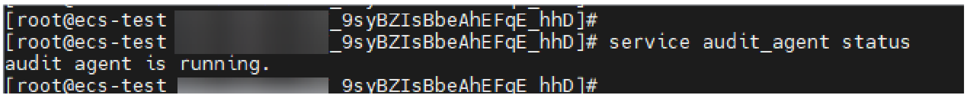
NOTICE

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:



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

```
audit agent is running.
```

**----End**

## Helpful Links

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

# 2.5.3 Installing an Agent (Windows OS)

You can enable database audit only after the agent is installed. This topic describes how to install the agent on a node running a Windows OS. For details about how to install an agent on the Linux OS, see **Installing an Agent (Linux OS)**.

## Prerequisites

- 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

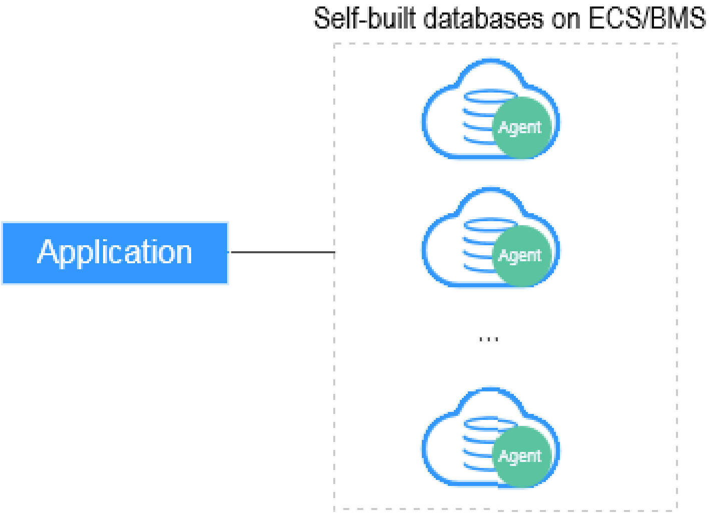
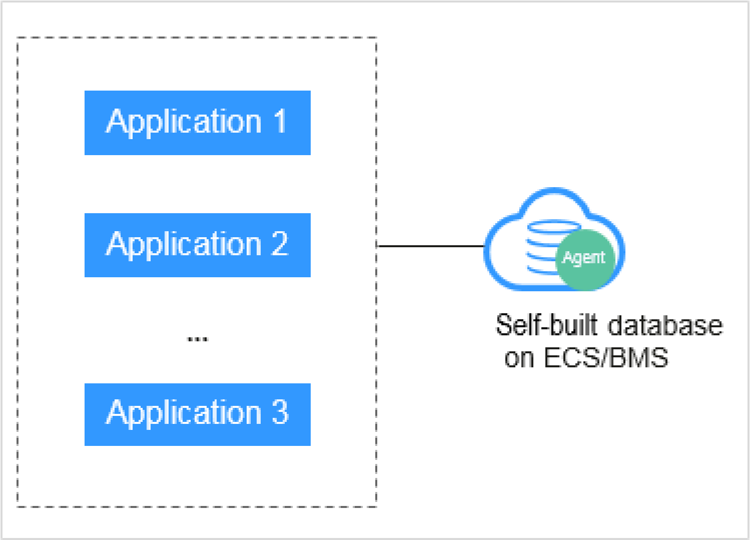
  

  **Figure 2-24** Multiple applications connecting to one database built on ECS/BMS

- 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

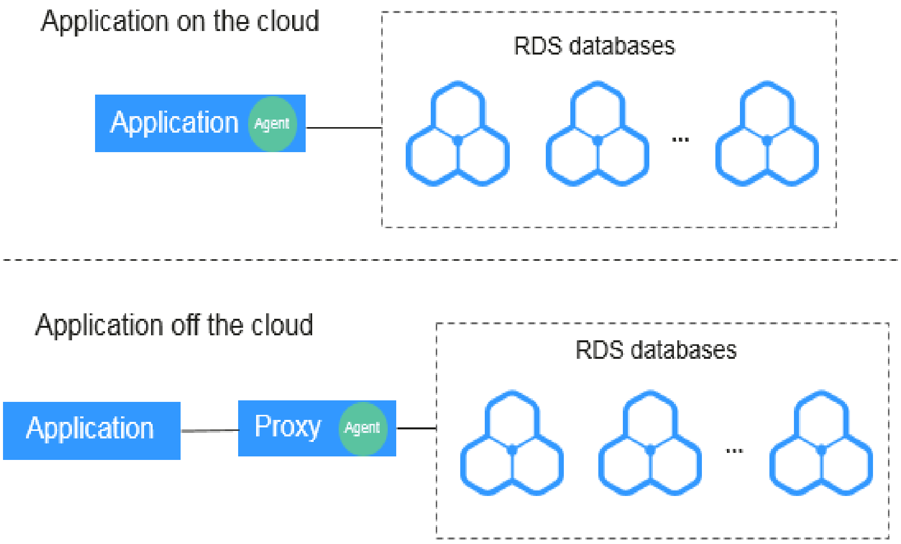


**Figure 2-26** Multiple applications connecting to one RDS database

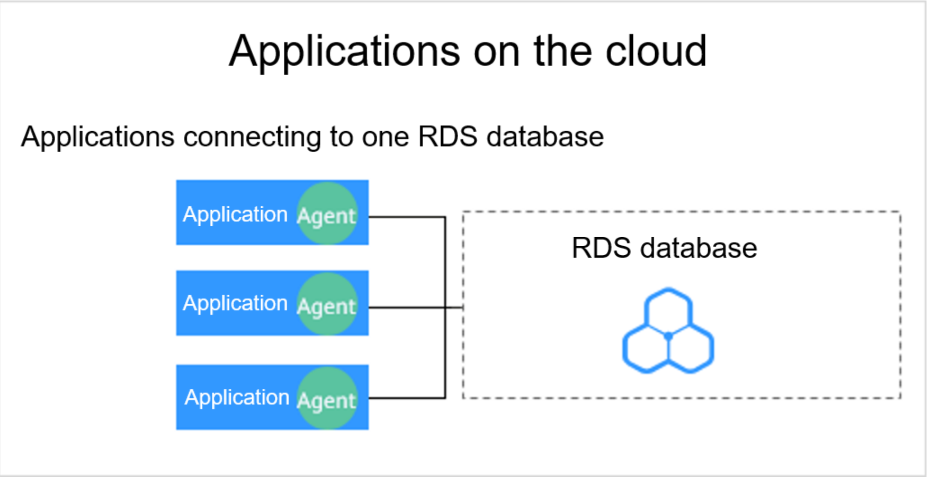

Applications on the cloud
Applications connecting to one RDS database
Application
Agent
Application
Agent
Application
Agent
RDS database

**Table 2-13** 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 2-13** 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

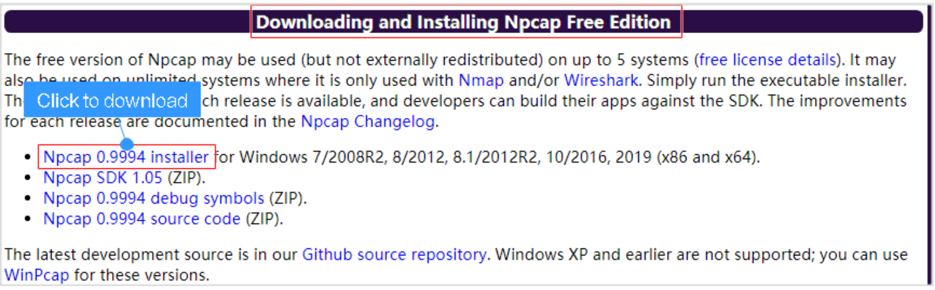
**Step 1** For details about how to add an agent, see **Step 2**.

**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

  **Downloading and Installing Npcap Free Edition**

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

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

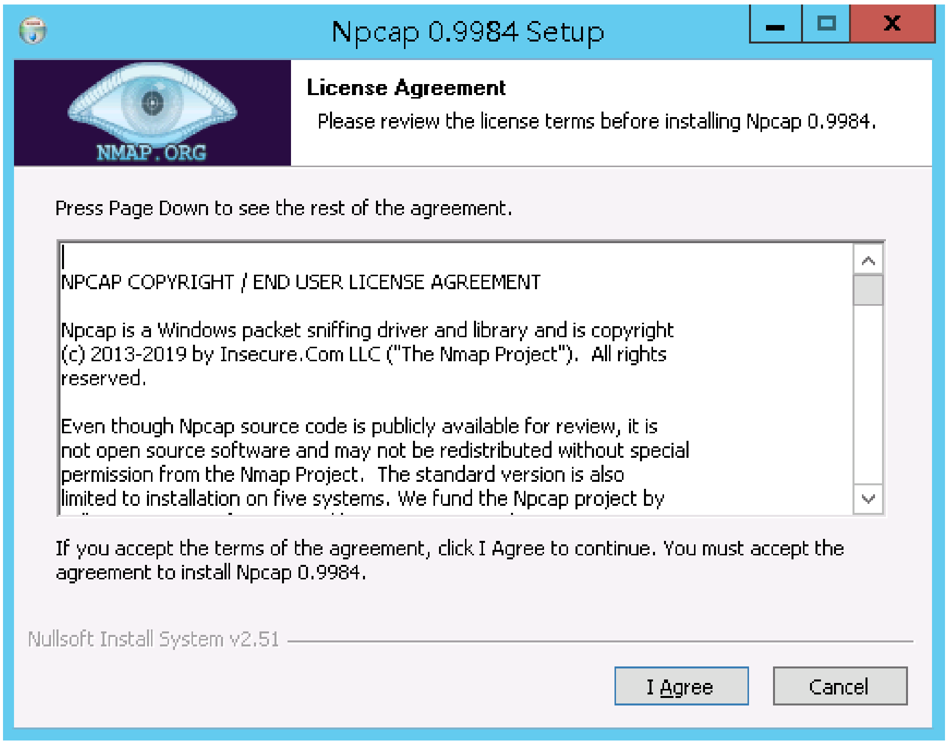
  The latest development source is in our Github source repository. Windows XP and earlier are not supported; you can use WinPcap for these versions.

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

c. Double-click the Npcap installation package.

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

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



**License Agreement**

Please review the license terms before installing Npcap 0.9984.

Press Page Down to see the rest of the agreement.

NPCAP COPYRIGHT / END USER LICENSE AGREEMENT

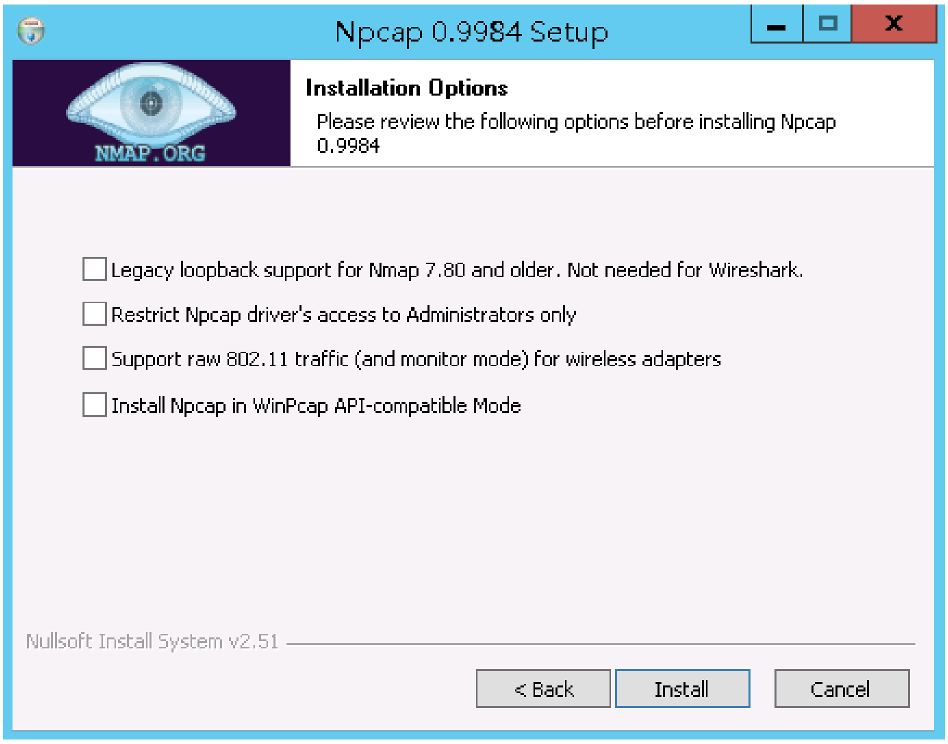
Npcap is a Windows packet sniffing driver and library and is copyright (c) 2013-2019 by Insecure.Com LLC ("The Nmap Project"). All rights reserved.

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

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

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

**Figure 2-29** Installing Npcap



**Installation Options**

Please review the following options before installing Npcap 0.9984

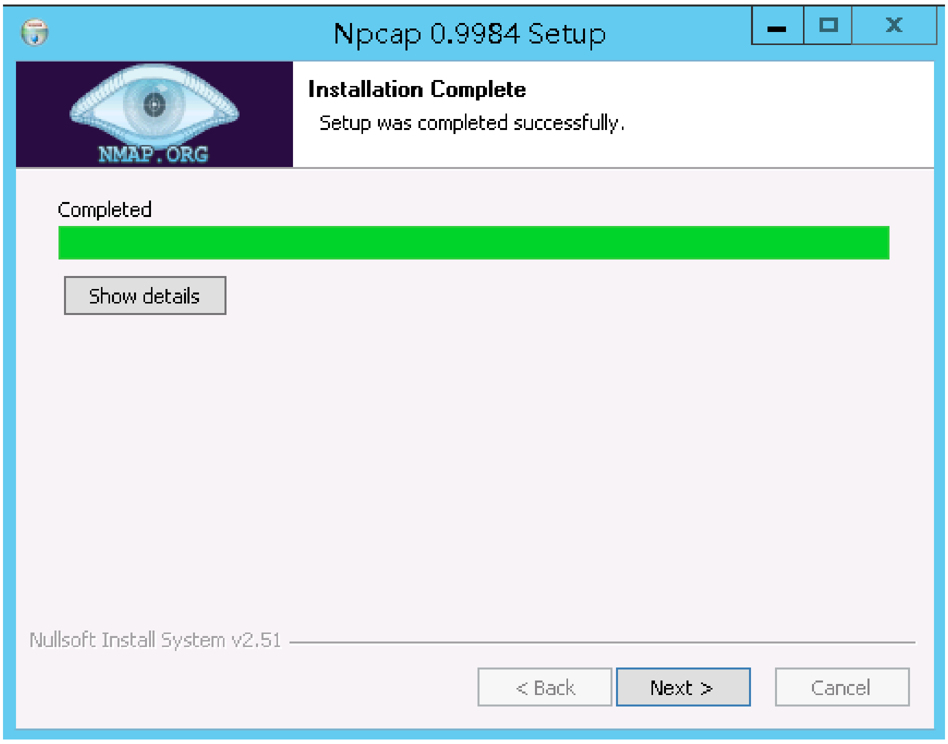
□ Legacy loopback support for Nmap 7.80 and older. Not needed for Wireshark.

□ Restrict Npcap driver's access to Administrators only

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

□ Install Npcap in WinPcap API-compatible Mode

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



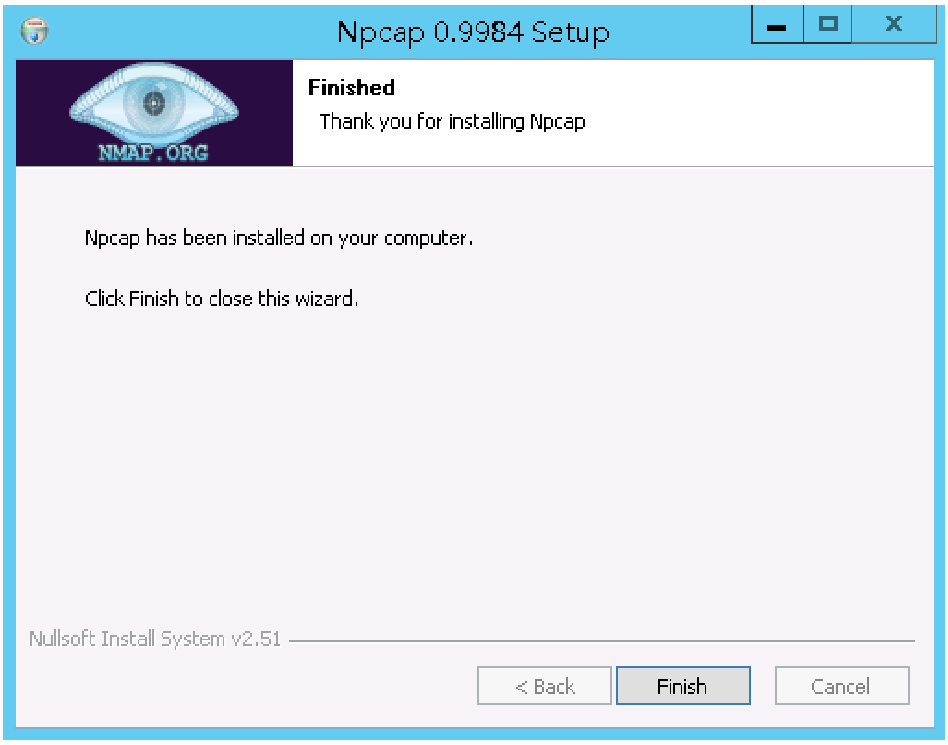
Npcap 0.9984 Setup

**Installation Complete**

Setup was completed successfully.

Completed

g. Click **Finish**.



Npcap 0.9984 Setup

**Finished**

Thank you for installing Npcap

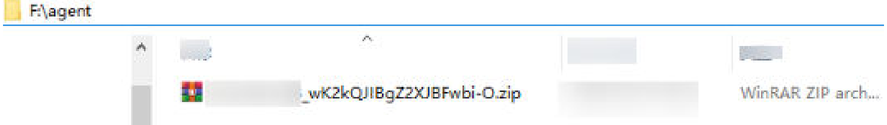
Npcap has been installed on your computer.

Click Finish to close this wizard.

**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



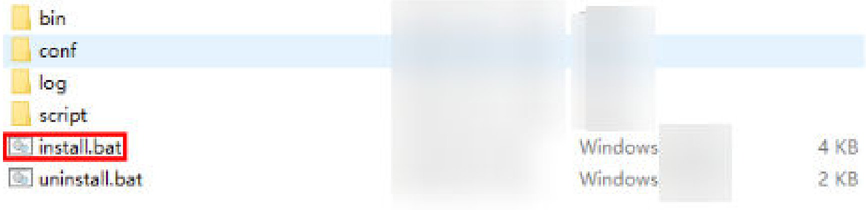
F:\agent

_wK2kQJIBgZ2XJBFwbi-O.zip WinRAR ZIP arch...

**Step 5** Decompress the package.

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

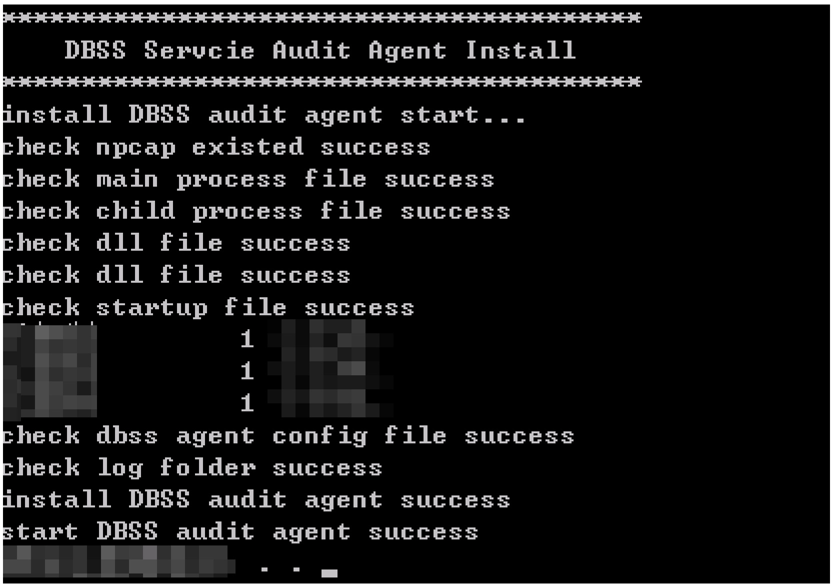
**Figure 2-31** Double-click install.bat



| | | |
|---|---|---|
| bin | | |
| conf | | |
| log | | |
| script | | |
| install.bat | Windows | 4 KB |
| uninstall.bat | Windows | 2 KB |

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

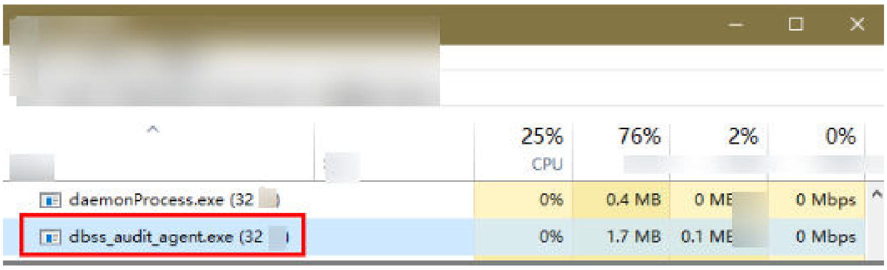
**Figure 2-32** Installation completed



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

**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



| | CPU 25% | 76% | 2% | 0% |
|---|---|---|---|---|
| daemonProcess.exe (32 ) | 0% | 0.4 MB | 0 MB | 0 Mbps |
| dbss_audit_agent.exe (32 ) | 0% | 1.7 MB | 0.1 MB | 0 Mbps |

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

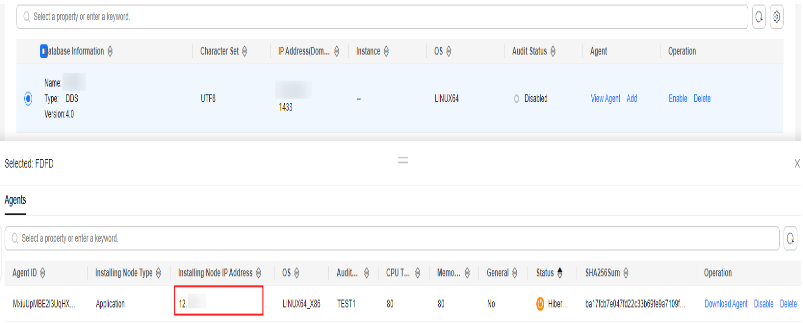
**Step 4** In the navigation tree on the left, choose **Databases**.

**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



Select a property or enter a keyword.

| | Database Information | Character Set | IP Address(Dom... | Instance | OS | Audit Status | Agent | Operation |
|---|---|---|---|---|---|---|---|---|
| ● | Name: [redacted]<br>Type: DDS<br>Version:4.0 | UTF8 | [redacted]<br>1433 | -- | LINUX64 | ○ Disabled | View Agent Add | Enable Delete |

Selected: FDFD

Agents

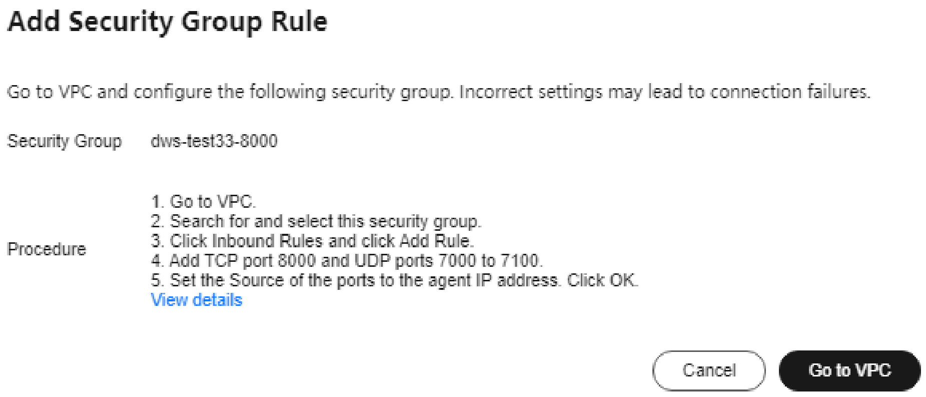
Select a property or enter a keyword.

| Agent ID | Installing Node Type | Installing Node IP Address | OS | Audit... | CPU T... | Memo... | General | Status | SHA256Sum | Operation |
|---|---|---|---|---|---|---|---|---|---|---|
| MxiuUpMBE2I3UqHX... | Application | 12.[redacted] | LINUX64_X86 | TEST1 | 80 | 80 | No | Hiber... | ba17fcb7e047fd22c33b69fe9a7109f... | Download Agent Disable Delete |

**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



## Add Security Group Rule

Go to VPC and configure the following security group. Incorrect settings may lead to connection failures.

Security Group dws-test33-8000

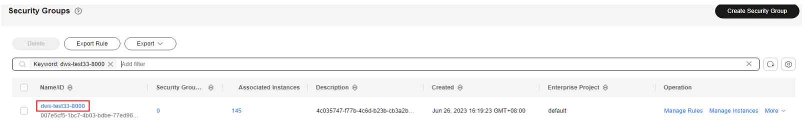
Procedure
1. Go to VPC.
2. Search for and select this security group.
3. Click Inbound Rules and click Add Rule.
4. Add TCP port 8000 and UDP ports 7000 to 7100.
5. Set the Source of the ports to the agent IP address. Click OK.

View details

**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



| | Name/ID | Security Grou... | Associated Instances | Description | Created | Enterprise Project | Operation |
|---|---|---|---|---|---|---|---|
| □ | dws-test33-8000<br>007e5cf5-1bc7-4b03-bdbe-77ed96... | 0 | 145 | 4c035747-f77b-4c6d-b23b-cb3a2b... | Jun 26, 2023 16:19:23 GMT+08:00 | default | Manage Rules Manage Instances More |

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

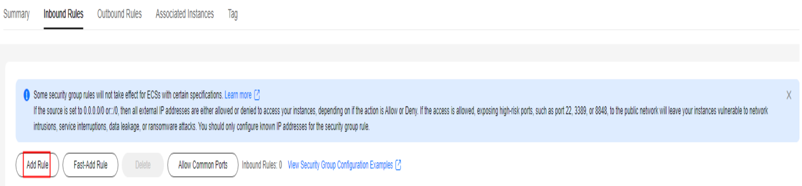
Check whether TCP (port number **8000**) and UDP protocols (port number from **7000** to **7100**) are configured in the inbound rules of the security group for the IP address of the installing node.

- 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



Some security group rules will not take effect for ECSs with certain specifications. Learn more

If the source is set to 0.0.0.0/0 or::/0, then all external IP addresses are either allowed or denied to access your instances, depending on if the action is Allow or Deny. If the access is allowed, exposing high-risk ports, such as port 22, 3389, or 8848, to the public network will leave your instances vulnerable to network intrusions, service interruptions, data leakage, or ransomware attacks. You should only configure known IP addresses for the security group rule.

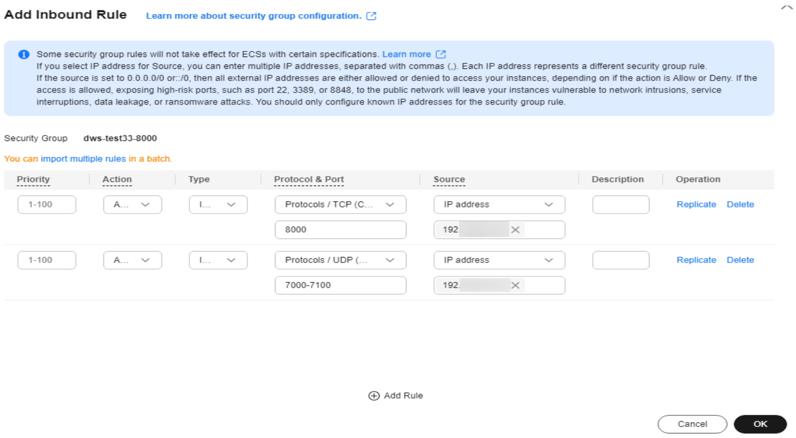
2. In the **Add Inbound Rule** dialog box, add **TCP** (port number **8000**) and **UDP** protocols (port number from **7000** to **7100**).

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



Add Inbound Rule Learn more about security group configuration.

Some security group rules will not take effect for ECSs with certain specifications. Learn more
If you select IP address for Source, you can enter multiple IP addresses, separated with commas (,). Each IP address represents a different security group rule.
If the source is set to 0.0.0.0/0 or::/0, then all external IP addresses are either allowed or denied to access your instances, depending on if the action is Allow or Deny. If the access is allowed, exposing high-risk ports, such as port 22, 3389, or 8848, to the public network will leave your instances vulnerable to network intrusions, service interruptions, data leakage, or ransomware attacks. You should only configure known IP addresses for the security group rule.

Security Group dws-test33-8000

You can import multiple rules in a batch.

| Priority | Action | Type | Protocol & Port | Source | Description | Operation |
|---|---|---|---|---|---|---|
| 1-100 | A... | I... | Protocols / TCP (C...<br>8000 | IP address<br>192 [redacted] |  | Replicate Delete |
| 1-100 | A... | I... | Protocols / UDP (...<br>7000-7100 | IP address<br>192.[redacted] |  | Replicate Delete |

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

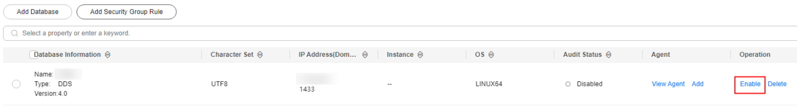
**Step 5** In the navigation tree on the left, choose **Databases**.

**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



| | Database Information | Character Set | IP Address(Dom... | Instance | OS | Audit Status | Agent | Operation |
|---|---|---|---|---|---|---|---|---|
| ○ | Name: [redacted]<br>Type: DDS<br>Version:4.0 | UTF8 | [redacted]<br>1433 | -- | LINUX64 | ○ Disabled | View Agent Add | Enable Delete |

**----End**

## Verifying Audit Results

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

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

**Step 3** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

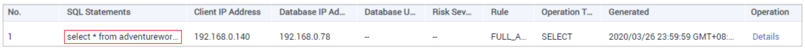
**Step 4** In the navigation tree on the left, choose **Data Reports**. The **Data Reports** page is displayed.

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

**Step 6** Click the **Statements** tab.

**Step 7** 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



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

- 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

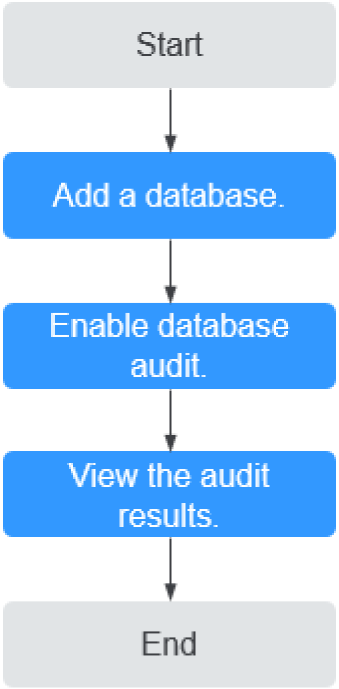


**Table 3-2** Procedure for quickly configuring database audit

| 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. For details, see **DBSS Permission Management** .

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

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

**Step 4** Set **Basic Settings** and **Edition**.

**Table 3-3** Basic settings parameters

| Parameter | Description |
|---|---|
| Service Type | The value is fixed at **Database Audit Service**. |
| Billing Mode | Only the yearly/monthly mode is available. |
| Region | Select the region where the instance is located. Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region. |
| AZ Type | Only general AZs are supported. |
| AZ | An AZ is a physical location that uses an independent power supply and network. AZs in the same region can communicate with each other over an intranet.<br>You can select random allocation or specify an AZ. |

**Table 3-4** Edition specifications

| Parameter | Description |
|---|---|
| Edition specifications | **Basic**, **Standard**, **Professional**, and **Advanced** editions are available.<br>For details about the specifications supported by each edition, see **Table 3-5**. |

**Table 3-5** Database audit editions

| Edition | Specification | Maximum Databases | Performance |
|---|---|---|---|
| Starter | Database audit starter edition | 1 | - Peak QPS: 1,000 queries/second<br>- Database load rate: 1.2 million statements/hour<br>- Online SQL statement storage: 100 million statements |
| Basic | Database audit basic edition | 3 | - Peak QPS: 3,000 queries/second<br>- Database load rate: 3.6 million statements/hour<br>- Online SQL statement storage: 400 million statements |
| Professional | Database audit professional edition | 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 | Database audit advanced edition | 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

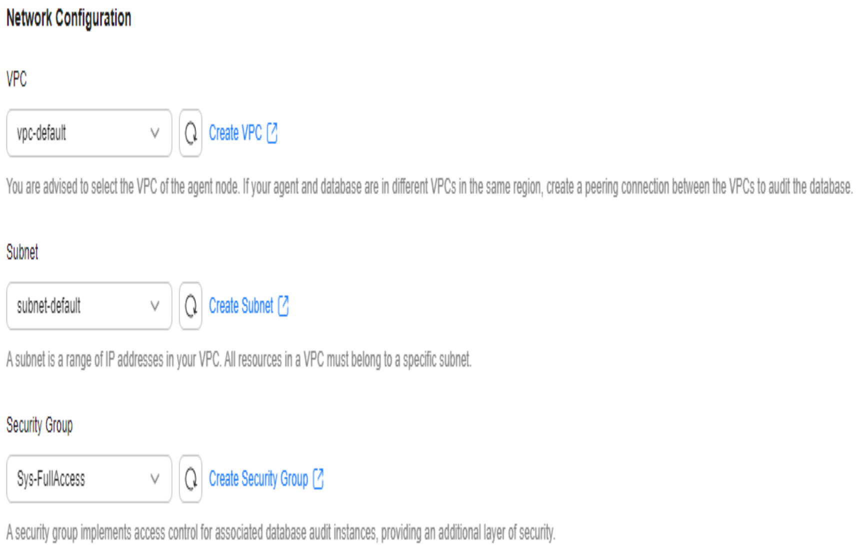
- A database instance is uniquely defined by its **database IP address and port**.

  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 3-6**.

**Figure 3-2** Network configuration



Network Configuration

VPC

vpc-default

You are advised to select the VPC of the agent node. If your agent and database are in different VPCs in the same region, create a peering connection between the VPCs to audit the database.

Subnet

subnet-default

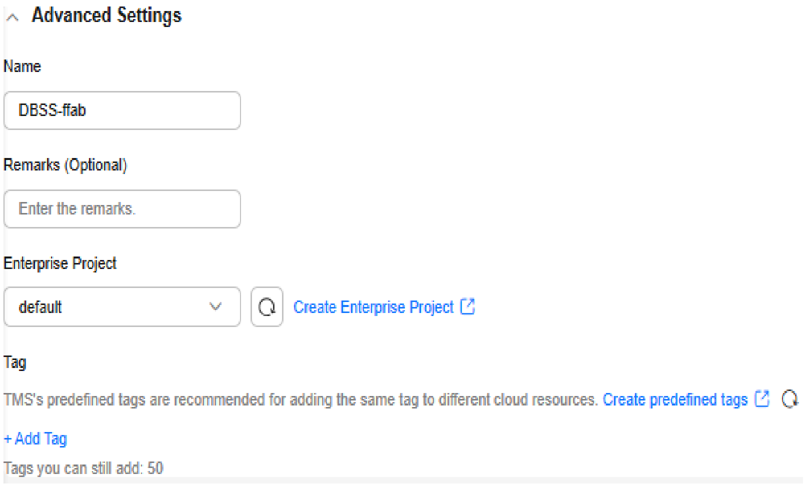
A subnet is a range of IP addresses in your VPC. All resources in a VPC must belong to a specific subnet.

Security Group

Sys-FullAccess

A security group implements access control for associated database audit instances, providing an additional layer of security.

**Figure 3-3** Advanced configuration



Advanced Settings

Name

DBSS-ffab

Remarks (Optional)

Enter the remarks.

Enterprise Project

default

Tag

TMS's predefined tags are recommended for adding the same tag to different cloud resources. Create predefined tags

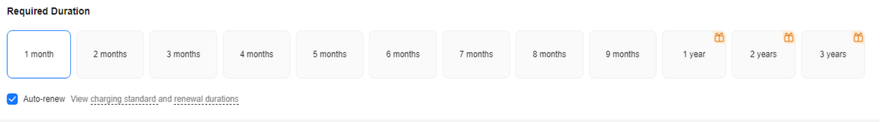
Tags you can still add: 50

**Table 3-6** 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 project, 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



Required Duration

1 month | 2 months | 3 months | 4 months | 5 months | 6 months | 7 months | 8 months | 9 months | 1 year | 2 years | 3 years

☑ Auto-renew View charging standard and renewal durations

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 3-7 describes the auto-renewal period.

**Table 3-7** 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.**

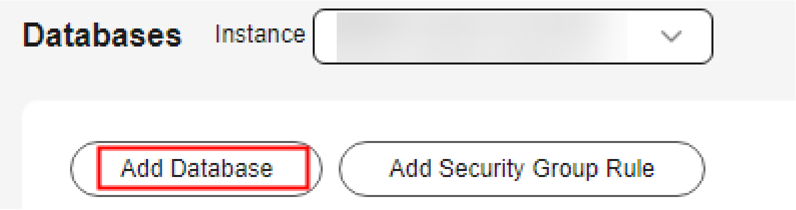
**Step 2** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

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

**Figure 3-5** Adding a database



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

**Table 3-8** 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>– 8.0.33<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>– 8.1<br>● When **Type** is set to **GaussDB(for MySQL)**, the following versions are available: | 5.0 |

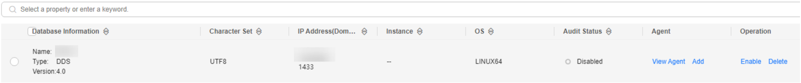
| Parameter | Description | Example Value |
|---|---|---|
| | – When **Database Type** is set to **Self-built database**, you can select the **Mysql 8.0** version.<br>– If **RDS database** is selected, a list of database instances will be displayed for you to choose from. You do not need to install the 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_3.3.0<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 | |

| Parameter | Description | Example Value |
|---|---|---|
| | ● When **Type** is set to **MongoDB**, the following version is available:<br>– v5.0<br>● 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 |

| Parameter | Description | Example Value |
|---|---|---|
| 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



Select a property or enter a keyword.

| Database Information | Character Set | IP Address(Dom... | Instance | OS | Audit Status | Agent | Operation |
|---|---|---|---|---|---|---|---|
| Name: [redacted]<br>Type: DDS<br>Version:4.0 | UTF8 | [redacted]<br>1433 | -- | LINUX64 | ○ Disabled | View Agent Add | Enable Delete |

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

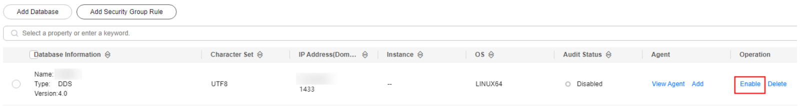
**Step 5** In the navigation tree on the left, choose **Databases**.

**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



Add Database | Add Security Group Rule

Select a property or enter a keyword.

| | Database Information | Character Set | IP Address(Dom... | Instance | OS | Audit Status | Agent | Operation |
|---|---|---|---|---|---|---|---|---|
| ○ | Name: [redacted]<br>Type: DDS<br>Version:4.0 | UTF8 | [redacted]<br>1433 | -- | LINUX64 | ○ Disabled | View Agent Add | Enable Delete |

**----End**

## Verifying Audit Results

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

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

**Step 3** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

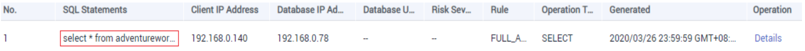
**Step 4** In the navigation tree on the left, choose **Data Reports**. The **Data Reports** page is displayed.

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

**Step 6** Click the **Statements** tab.

**Step 7** 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



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

**----End**

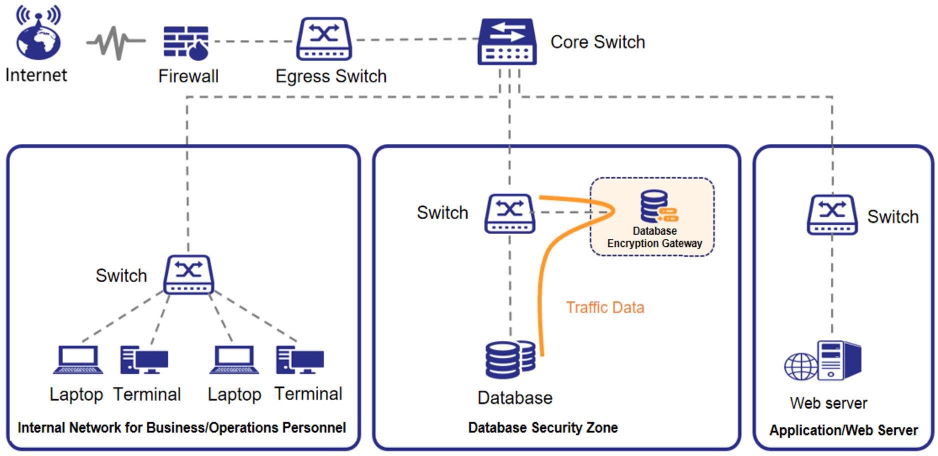
# 4 Enabling and Using Database Security Encryption

## 4.1 Introduction to Database Encryption and Access Control

Database encryption and access control is a security solution that safeguards sensitive data through encryption, utilizing gateway proxy technology.

As a proxy encryption gateway, the system is deployed between the database and client applications. Any access must pass through the gateway to implement data encryption and access control. **Figure 4-1** shows the system networking scenario.

**Figure 4-1** Network Mode



### Encrypting Data

The system supports data encryption and integrity verification, meeting the evaluation requirements of graded protection and sub-protection as well as the evaluation requirements of storage data integrity and confidentiality assurance in the application and security evaluation of commercial cryptographic systems.

- Encryption algorithm: AES
- Integrity check algorithm: AES-GCM

## Access control

The system has an access authorization mechanism independent of the database. Authorized users can access encrypted data, but unauthorized users cannot access encrypted data. This effectively prevents administrators from accessing the database without authorization and hackers from dragging the database.

The system allows system administrators, security administrators, and audit administrators to manage separation of permissions, enhancing database security and compliance.

## Application Scenarios

Database encryption and access control can meet compliance requirements as well as sensitive database data protection requirements.

**Meet the compliance requirements of national assessment.**

The application system processes data based on user permissions. For legacy systems (the old system cannot be upgraded or reconstructed) and personal privacy protection issues required by the Cybersecurity Law are not considered during development, it is too complex to change the code, data privacy protection depends on external technologies.

Database encryption and access control can implement database encryption and comply with various laws and regulations.

**Meets the requirements for protecting sensitive database data.**

Database encryption and access control can effectively prevent data leakage caused by the leakage of high-privilege accounts and passwords of database administrators, such as DBAs. In addition, the system can prevent database files from being downloaded or copied due to external APT attacks or improper internal management, meeting sensitive data protection requirements of databases.

## Functions

This section describes the main functions and related sections of database encryption and access control.

**Table 4-1** Functions

| Feature/ Update | Function | Related Chapters |
|---|---|---|
| Asset Management | Allows users to add, delete, modify, and query database assets, test data source connectivity, and configure database read/write isolation, encryption mode, return value, and account permission detection. | **Adding Data Assets** |

| Feature/ Update | Function | Related Chapters |
|---|---|---|
| Sensitive Data Discovery | Supports sensitive data scanning, sensitive data type management, and sensitive data industry template management. | **Sensitive Data Discovery** |
| Business test | Supports service simulation tests to simulate whether encryption and decryption can be performed properly. Supports service SQL traffic analysis by accessing the network before encryption, locates SQL statements that may be executed abnormally after encryption, and generates analysis reports. | **Simulated Encryption Test**, **Simulated Decryption Test**, **Service Test and Analysis** |
| Encrypting Data | The data encryption module manages encryption and decryption tasks, authorizes client and database users to restrict user access, views and downloads encryption logs, rolls back table structures, manages encryption tables, and downloads bypass plug-ins. | **Data Encryption and Decryption** |
| Dynamic data masking | A masking algorithm can be configured for sensitive data to dynamically mask plaintext data. | **Dynamic Data Masking** |
| Key management | Supports three-level key algorithms, key source configuration, key (DSK) periodic rotation update, KMS interconnection configuration, key record query, and key search. | **Initializing a Key**, **Key Management** |
| Platform management | On the platform management module, you can configure basic network adapters and routes, upgrade the system, back up and restore configuration data, view application access records, and configure security passwords. | **Platform Management** |

| Feature/ Update | Function | Related Chapters |
|---|---|---|
| System management | ● Maintains platform users, including account management, organizational structure management, role management, and account review; and allows users to view and manage various system messages.<br>● Displays the device status, manages devices, diagnoses the usage of the system kernel, CPU, and hard disk, upgrades the system, and manages system security configurations. | **System Management** |
| Log management | Allows users to view and search for logs of all operations in the system. | **Viewing System Operation Logs** |

# 4.2 Step 1: Buy Database Security Encryption

This section describes how to buy a database encryption instance. The instance can be billed on a yearly/monthly basis.

NOTICE

Database encryption is in the open beta test (OBT) phase. To use this function, **submit a service ticket**.

## Limitations and Constraints

Database encryption and access cannot be used across regions. The database to be encrypted and accessed must be in the same region as the purchased instance.

## Procedure

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

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

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

**Step 4** (Optional) Enter the purchase information.

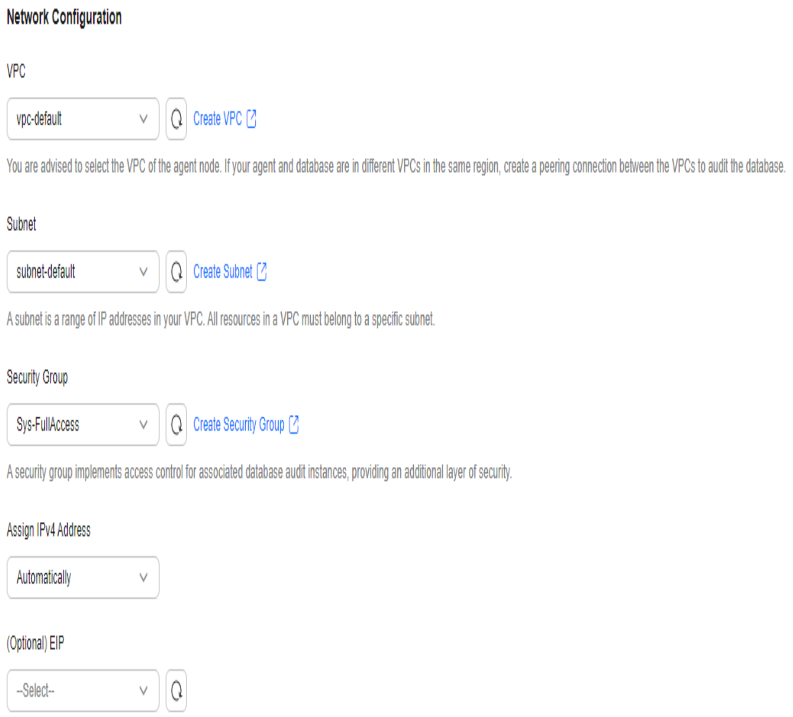
**Table 4-2** Basic configuration parameters

| Parameter | Description |
|---|---|
| Service Type | The value is fixed at **Database Audit Service**. |
| Billing Mode | Only the yearly/monthly mode is available. |
| Region | Select the region where the instance is located. Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region. |
| AZ Type | Only general AZs are supported. |
| AZ | An AZ is a physical location that uses an independent power supply and network. AZs in the same region can communicate with each other over an intranet.<br>You can select random allocation or specify an AZ. |
| Standby AZ | You can select random allocation or specify an AZ. |

**Table 4-3** Edition specifications

| Parameter | Description |
|---|---|
| Edition | Select **Database Audit Encryption Enhanced Edition** under advanced edition.<br>The specifications are as follows:<br>● Asset quantity: A maximum of 10 databases are supported.<br>● System resources:<br>– CPU: 16 vCPUs<br>– Memory: 32 GB<br>● Encryption/decryption performance: 40,000 QPS<br>● Maximum concurrent connections: 3000 |

**Figure 4-2** Network configuration



Network Configuration

VPC

vpc-default

You are advised to select the VPC of the agent node. If your agent and database are in different VPCs in the same region, create a peering connection between the VPCs to audit the database.

Subnet

subnet-default

A subnet is a range of IP addresses in your VPC. All resources in a VPC must belong to a specific subnet.

Security Group

Sys-FullAccess

A security group implements access control for associated database audit instances, providing an additional layer of security.

Assign IPv4 Address

Automatically

(Optional) EIP

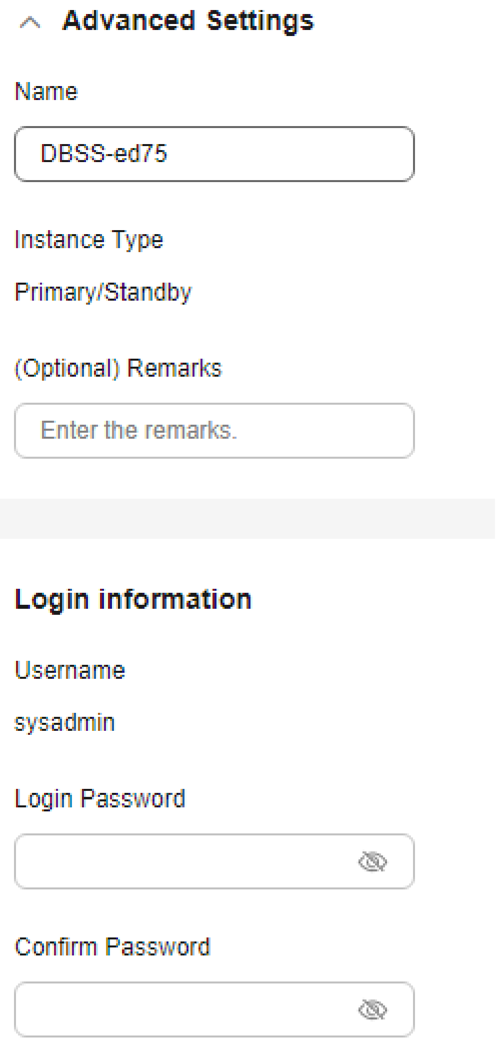
--Select--

**Table 4-4** Network configuration parameters

| Parameter | Description | Example Value |
|---|---|---|
| VPC | Select the VPC to be associated.<br>A VPC facilitates internal network management and configuration, and allows you to perform secure and quick network changes. It is recommended that the VPC be the same as that of the agent node. | - |
| Security Group | This parameter is mandatory when **Deployed Location** is set to **On-cloud**.<br>Security groups are used for access control. | - |

| Parameter | Description | Example Value |
|---|---|---|
| Subnet | A subnet is a range of IP addresses in your VPC. All of the resources in a VPC must be deployed in subnets.<br>**NOTE**<br>Subnets cannot be used across geolocations. A general AZ cannot use the subnet of an edge AZ, and an edge AZ cannot use the subnet of a general AZ. | - |
| Assign IPv4 Address | This parameter is mandatory when **Deployed Location** is set to **On-cloud**.<br>Select an IPv4 address. | Automatically assign IP address |
| (Optional) EIP | This parameter is mandatory when **Deployed Location** is set to **On-cloud**.<br>Select the EIP bound to the instance. | - |
| IP address of the active node | This parameter is mandatory when **Deployed Location** is set to **Off-cloud**.<br>Enter the IP address of the active node. | - |
| IP address of the standby node | This parameter is mandatory when **Deployed Location** is set to **Off-cloud**.<br>Enter the IP address of the standby node. | - |
| Floating IP address | This parameter is mandatory when **Deployed Location** is set to **Off-cloud**.<br>Enter a floating IP address. | - |

**Figure 4-3** Advanced configuration and login information



Advanced Settings

Name

DBSS-ed75

Instance Type

Primary/Standby

(Optional) Remarks

Enter the remarks.

Login information

Username

sysadmin

Login Password

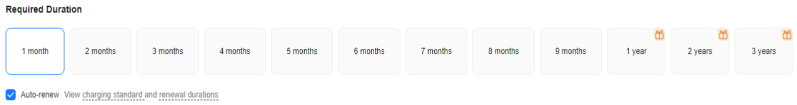
Confirm Password

**Table 4-5** Parameters

| Parameter | Description | Example Value |
|---|---|---|
| Name | The name is automatically generated. You can also customize the name. | - |
| Instance Type | Currently, only the active/ standby mode is supported. | Primary/Standby |
| Remarks (Optional) | Remarks about the instance. | - |
| Username | Default username. | sysadmin |

<table>
<tr><th>Parameter</th><th>Description</th><th>Example Value</th></tr>
<tr><td>Login Password</td><td>Set the password for logging in to the instance.<br>NOTE<br>The password must contain:<br>● Contains 8 to 26 characters.<br>● The password must contain at least two of the following types of characters: uppercase letters, lowercase letters, digits, and the following special characters: ~!@#$%^&*()_+`=-[]{}|;':,".<>?/\<br>● The password should be different from the username or the username spelled backwards.</td><td>-</td></tr>
<tr><td>Confirm Password</td><td>Enter the confirm password, which must be the same as the login password.</td><td>-</td></tr>
</table>

**Figure 4-4** Required duration



☑ Auto-renew

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 4-6** describes the auto-renewal period.

**Table 4-6** 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 5** Confirm the configuration and click **Next**.

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

**Step 6** 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 7** On the displayed page, select a payment method.

- Balance/Online payment

  Use your account balance to pay for your order. If the balance is insufficient, click **Top Up** to recharge your account.

   a. Select **Balance**.
   b. Click **Pay**.
- **Request Online Contract and Pay**
   a. Choose **Request Online Contract and Pay** and click **Create Contract**.
   b. Enter the contract information and click **Create Formal Contract**.

**Step 8** After you pay for your order, you can view the creation status of your instances.

**----End**

# 4.3 Step 2: Logging In to the Instance Web Console

The system administrator can use a web browser to log in to the console of database encryption and access control to manage and maintain it.

Table 4-7 describes the default user names. Obtain the actual user names and passwords from technical support engineers.

**Table 4-7** Default System Account Information

| Default Role | Default Account | Description |
|---|---|---|
| System administrator | sysadmin | Responsible for system configuration and routine system operation and maintenance. The default password is the password set during instance purchase. Reset the password upon the first login.<br>For details, see **System administrator operation guide**. |
| Safety manager | secadmin | Manages system users and system security. The default password is the same as the password of the **sysadmin** user set during instance purchase. Reset the password upon the first login.<br>For details, see **Security Administrator Operation Guide**. |
| AuditManager | audadmin | Audits, traces, analyzes, supervises, and checks the operations of system administrators and security administrators. The default password is the same as the password of the **sysadmin** user set during instance purchase. Reset the password upon the first login.<br>For details, see **Operation Guide for Audit Administrators**. |

## Prerequisites

- You have obtained the username and password from technical support engineers.

- Supporting Browsers
  - Chrome 77 or later.
  - Secret Message Browser 1.0.0.7.

## Procedure

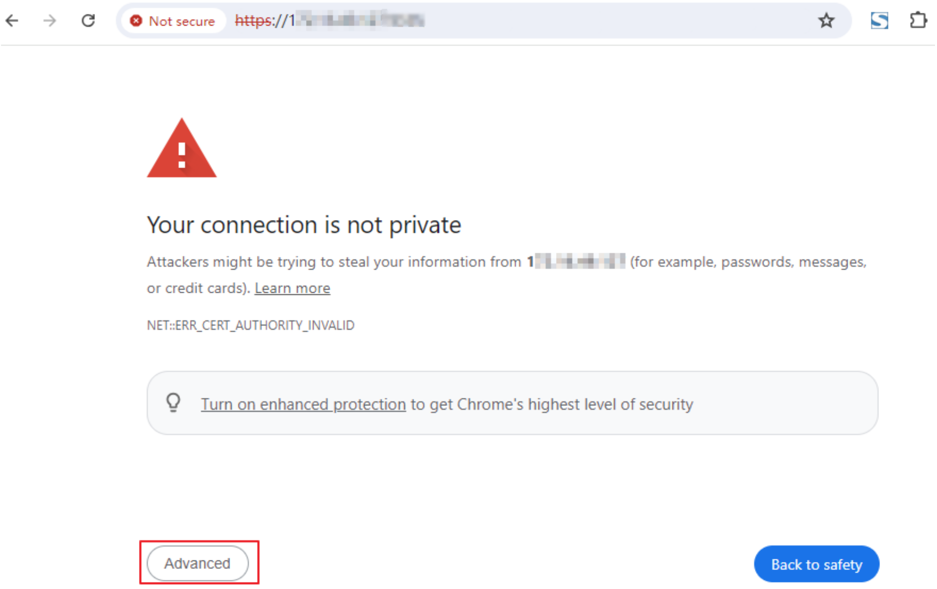
**Step 1** Log in to an instance.

- Method 1: Log in to the service management console, go to the database encryption and access control page, and click in the **Operation** column of the target instance.
- Method 2: Obtain **EIP** from the database encryption and access control page displayed in method 1. Enter the address in the address box of the browser and press **Enter**. The login page is displayed.

  Address: **https://***ServerEIP*:*PortNumber*, for example, **https://100.xx.xx.54:9595**.

**Step 2** On the security warning page, click **Advanced**.

**Figure 4-5** Security



Your connection is not private

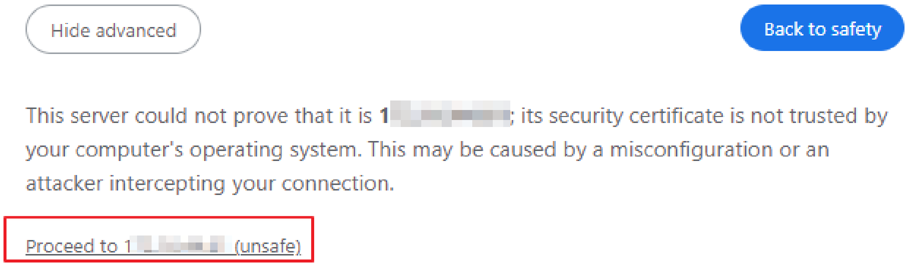
Attackers might be trying to steal your information from 1[redacted] (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

Turn on enhanced protection to get Chrome's highest level of security

**Step 3** Click **Proceed to** *xx.xx.xx.xx* **(unsafe)**.

**Figure 4-6** Continue



This server could not prove that it is 1[redacted]; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

**Step 4** (Optional) Click the drop-down arrow in the upper right corner and select a language.

**Step 5** Enter the username, password, and verification code, and click **Log In**.

**Step 6** After the first login, you need to change the default password. For details, see **Changing the login password**.

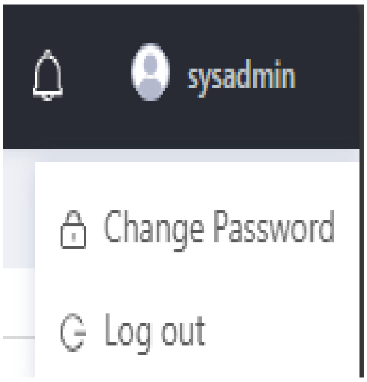
You are advised to change the password periodically to ensure login security.

**----End**

## Changing the login password

**Step 1** On the web console, move the cursor to the username in the upper right corner.

**Figure 4-7** Changing a password



**Step 2** Select **Change Password** from the drop-down list box.

**Step 3** In the dialog box, enter the old password and new password, and click **OK**. **Table 4-8** describes the new password rules.

After the password is changed, you need to log out of the web console and use the new password to log in again.

**Table 4-8** Changing a password

| Parameter | Description |
|---|---|
| Old password | Enter the original login password. |
| New Password | Enter the new password.<br>Password requirements:<br>● Contain 8 to 32 characters.<br>● Contain at least three of the following types: uppercase letters, lowercase letters, numbers, and special characters (!@$%^-_=+[{}]:,./?~#*).<br>● Cannot contain the username or the username spelled backwards. |
| Confirm Password | Enter the new password again. |

**----End**

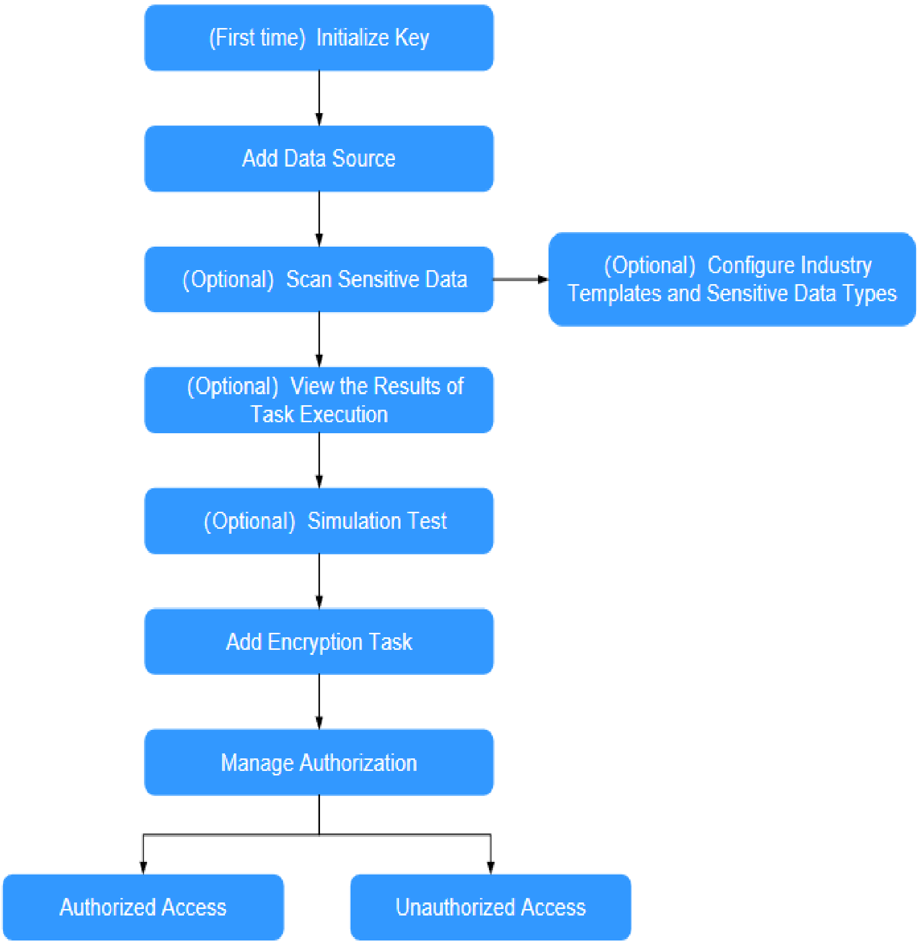
# 4.4 System Function Configuration and Application Scenario Examples

## 4.4.1 Scenario 1: Encryption Process and Typical Encryption Configuration

### Encryption Process

The following figure shows the encryption process of database encryption and access control.

**Figure 4-8** Encryption process


(First time) Initialize Key
Add Data Source
(Optional) Scan Sensitive Data
(Optional) Configure Industry Templates and Sensitive Data Types
(Optional) View the Results of Task Execution
(Optional) Simulation Test
Add Encryption Task
Manage Authorization
Authorized Access
Unauthorized Access

1. Initialize the key for the first time.

   When you use the system for the first time, initialize the key based on the key source. For details, see **Initializing a Key**.

2. Add a data source.

   Before using the data masking function, you need to add data assets to the system. For details, see **Adding Data Assets**.

3. (Optional) Configure the industry template and sensitive data type.

   The system has built-in sensitive data types and common industry templates that meet most requirements. If you have special requirements, you can also customize sensitive data types and industry templates. For details, see **Adding an Industry Template** and **Adding a User-Defined Data Type**.

4. (Optional) Discover sensitive data.

   Automatically scans and identifies sensitive data in data assets through sensitive data discovery tasks. For details, see **Scanning Sensitive Data in Assets**.

5. (Optional) View the task execution result.

   You can view the task execution result to check whether the result meets the sensitive data requirements. For details, see **Viewing the Execution Result of a Scan Task**.

6. (Optional) Perform an emulation encryption test.

   Perform a simulation encryption test to check whether the target supports encryption. For details, see **Simulated Encryption Test**.

7. Create an encryption task.

   You can create an encryption task based on sensitive data information in the result of a sensitive data discovery task. For details, see **Creating an Encrypted Task in the Result** .

   Encryption tasks can also be directly created in the data encryption module. For details, see **Configuring an Encryption Task**.

8. Manage authorizations.

   After encryption is configured, you can view only the encrypted data when accessing the database by default. To ensure the normal running of the application system, you need to obtain the data before encryption. In this case, you need to authorize the application system. For details, see **Managing Authorization**.

9. After the configuration is complete, you can verify the configuration in the following ways:

   - Use the authorized client address and user to access the database in proxy mode. In this case, you can view the plaintext data before encryption.
   - Use an unauthorized client address or user to access the database in proxy mode. In this case, only encrypted data can be viewed.

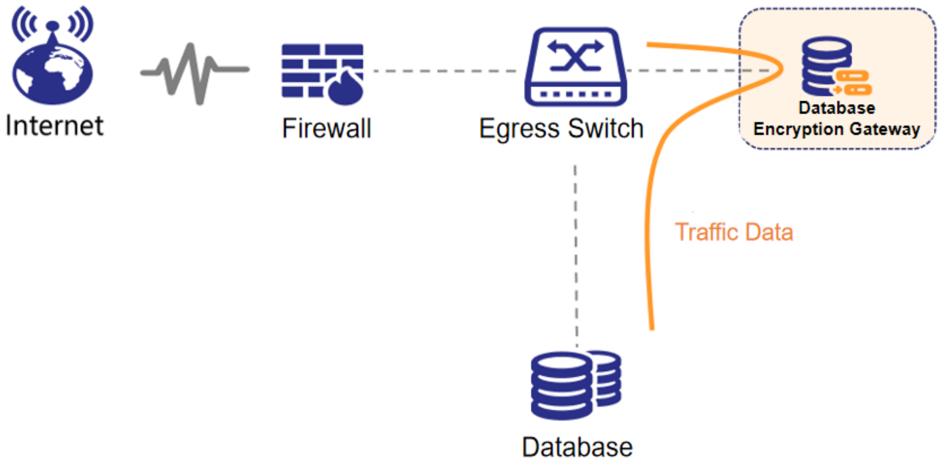
## Typical Configuration of the Encryption Function

Database encryption and access control encrypt sensitive data in the database to ensure data security. This example shows how to encrypt the database.

**Networking description:**

Database encryption and access control use the reverse proxy mode. The following figure shows the typical networking.

**Figure 4-9** Networking



## Prerequisite

- The route between the device and the application system is reachable.
- The route between the device and the database is reachable.

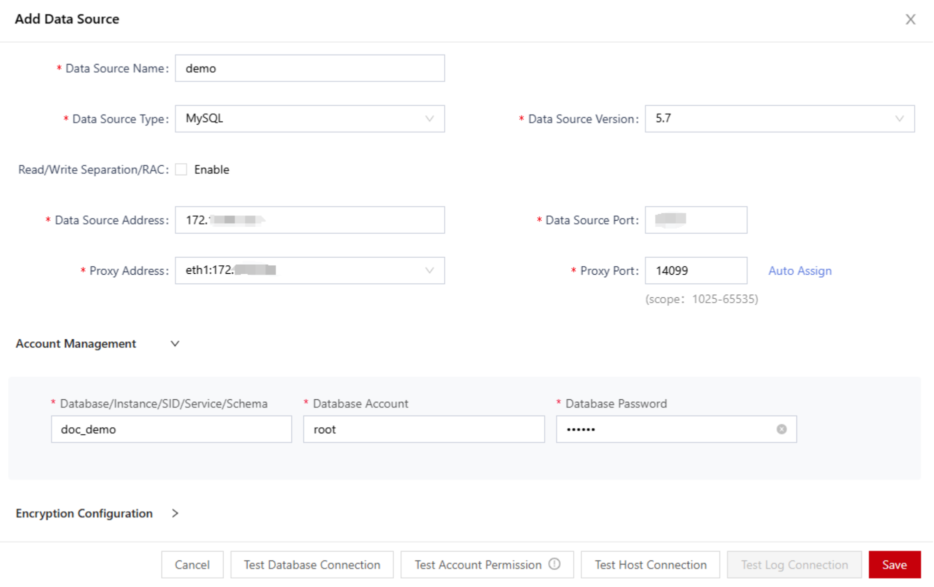
## Step 1: Adding a Data Source

Before using the, you need to add the target database on the Asset Management page.

1. Log in to the instance web console as user sysadmin.
2. In the navigation pane, choose **Assets Management** > **Data Source Management**.
3. Click **Add Data Source** in the upper right corner.
4. In the **Add Data Source** dialog box, configure asset information.

   Host information and log information are optional. The SSH service must be enabled on the database server.

   **Figure 4-10** Adding a data source

   Add Data Source

   * Data Source Name: demo
   * Data Source Type: MySQL
   * Data Source Version: 5.7
   Read/Write Separation/RAC: □ Enable
   * Data Source Address: 172.[redacted]
   * Data Source Port: [redacted]
   * Proxy Address: eth1:172.[redacted]
   * Proxy Port: 14099 Auto Assign
   (scope：1025-65535)

   Account Management

   | * Database/Instance/SID/Service/Schema | * Database Account | * Database Password |
   |---|---|---|
   | doc_demo | root | •••••• |

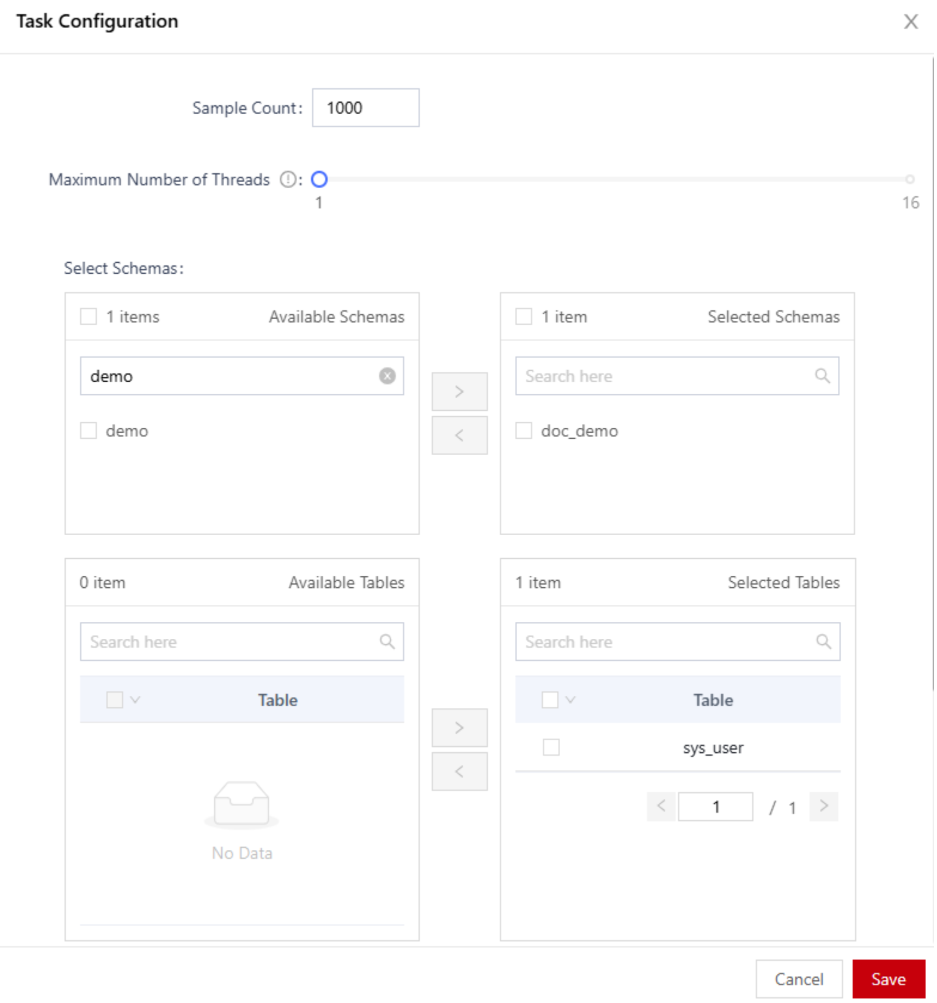
   Encryption Configuration

5. After the configuration is complete, click **Test Database Connection** to check whether the database can be connected.
6. Click **Test Account Permission** to check whether the database account permission meets the encryption requirements.
7. Click **Save**.

**Step 2: Executing a Sensitive Data Discovery Task**

1. **Log in to the web console of the instance** as user **sysadmin**.
2. In the navigation tree on the left, choose **Sensitive Data Discovery** > **Sensitive Data Scan**.
3. Find the target data asset and click **Task Configuration**.
4. In the **Task Configuration** dialog box, set a sensitive data discovery task.

**Figure 4-11** Configuring a sensitive data discovery task



Task Configuration

Sample Count: 1000

Maximum Number of Threads ⓘ: 1 (range 1–16)

Select Schemas:

| Available Schemas (1 items) | Selected Schemas (1 item) |
|---|---|
| demo | doc_demo |

| Available Tables (0 item) | Selected Tables (1 item) |
|---|---|
| No Data | sys_user |

5. Click **Save**.
6. Find the target data asset and click ▷ to execute the sensitive data discovery task.

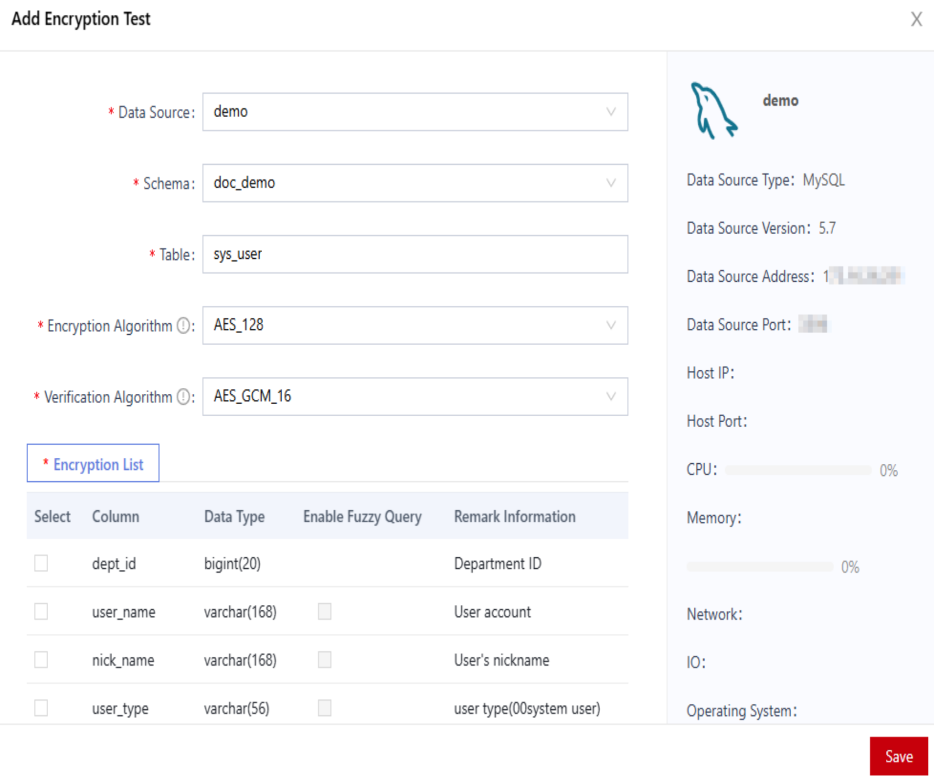
After the execution starts, the system automatically scans and identifies sensitive data. The scan duration depends on the amount of data to be scanned. The larger the amount of data, the longer the scan duration. You can view the scan progress on the page.

### Step 3: Performing a Simulated Encryption Test

Before encrypting a database table, perform a simulation encryption test to check whether the database meets the encryption requirements.

1. Log in to the web console of the instance as user **sysadmin**.
1. In the navigation tree, choose **Service Test** > **Simulation Test**.
2. Click **Add Encryption Test**.
3. In the **Add Encryption Test** dialog box, configure the test target.

**Figure 4-12** Adding an encryption test



Add Encryption Test

* Data Source: demo

* Schema: doc_demo

* Table: sys_user

* Encryption Algorithm: AES_128

* Verification Algorithm: AES_GCM_16

* Encryption List

| Select | Column | Data Type | Enable Fuzzy Query | Remark Information |
|---|---|---|---|---|
| □ | dept_id | bigint(20) | | Department ID |
| □ | user_name | varchar(168) | □ | User account |
| □ | nick_name | varchar(168) | □ | User's nickname |
| □ | user_type | varchar(56) | □ | user type(00system user) |

demo

Data Source Type: MySQL

Data Source Version: 5.7

Data Source Address: [redacted]

Data Source Port: [redacted]

Host IP:

Host Port:

CPU: 0%

Memory: 0%

Network:

IO:

Operating System:

4. Click **Save**.

   After the test is complete, you can view the test result in the list and click **Details** to view the completion status of each node in the encryption process.

   After the test is complete, click **Delete** to delete it.

   NOTE

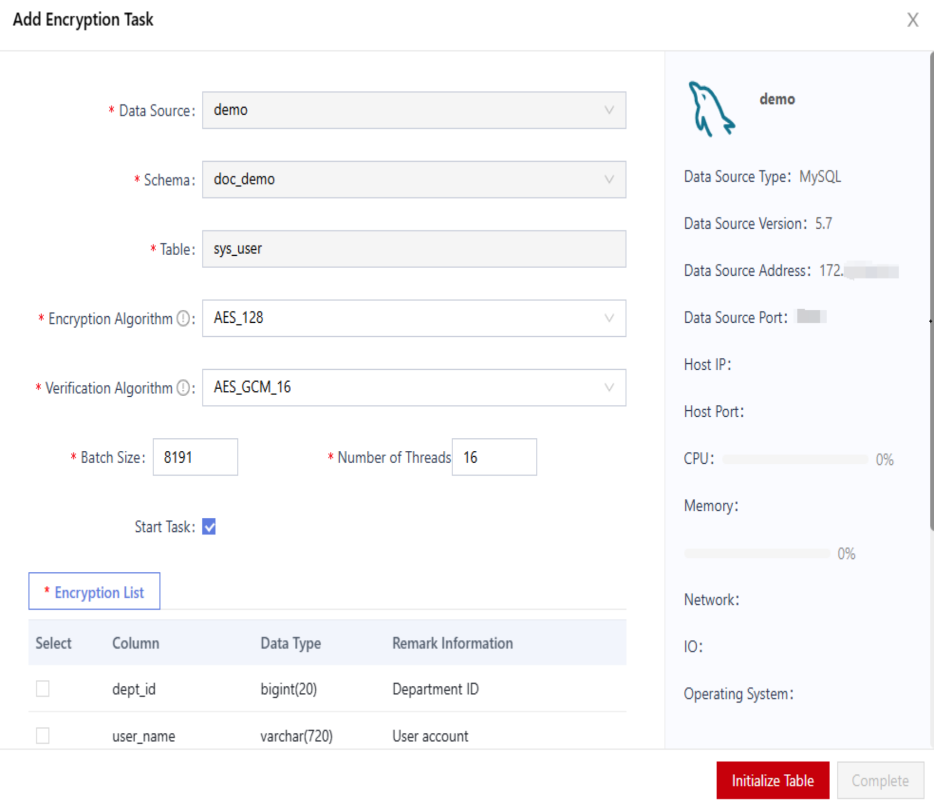
   - If a fault occurs during the simulation test, rectify the fault as prompted.
   - If an encryption task needs to be configured after the test, delete the stimulated encryption test first.

### Step 4: Creating an Encryption Task in the Discovery Result

1. Log in to the web console of the instance as user **sysadmin**.
2. In the navigation tree on the left, choose **Sensitive Data Discovery** > **Sensitive Data Scanning**.

3. On the scan task list page, locate the target data asset and click **View**.
4. On the scan result page, locate the target database table and click **Add Encryption Task**.
5. In the **Add Encryption Task** dialog box, configure encryption information.

**Figure 4-13** Adding an encrypted task



Add Encryption Task

* Data Source: demo
* Schema: doc_demo
* Table: sys_user
* Encryption Algorithm: AES_128
* Verification Algorithm: AES_GCM_16
* Batch Size: 8191
* Number of Threads: 16

Start Task: ☑

* Encryption List

| Select | Column | Data Type | Remark Information |
|---|---|---|---|
| □ | dept_id | bigint(20) | Department ID |
| □ | user_name | varchar(720) | User account |

demo

Data Source Type: MySQL
Data Source Version: 5.7
Data Source Address: 172.[redacted]
Data Source Port: [redacted]
Host IP:
Host Port:
CPU: 0%
Memory: 0%
Network:
IO:
Operating System:

6. Select an encryption algorithm from the Encryption Algorithm drop-down list box.
7. Click the **Encryption List** tab and select the columns to be encrypted.
8. Click **Initialize Table** to initialize the data table.
9. Click **Complete**.

After the encryption task is executed, the encryption results of data will be retrieved when the database is accessed. In this case, you need to authorize the application system (or client) to access the application system (or client) to ensure that the application system (or client) can be used properly.

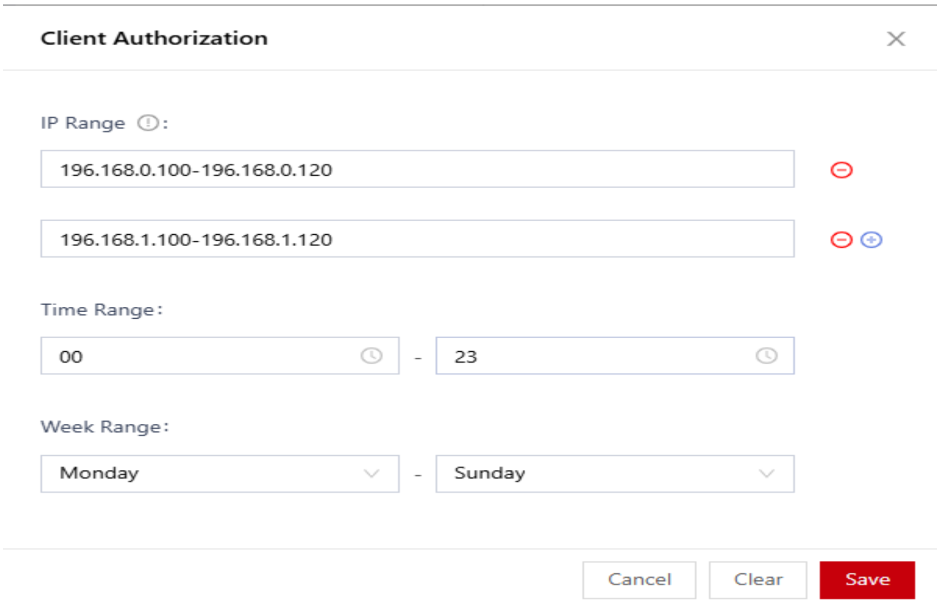
### Step 5: Setting Access Authorization

The authorization management module supports client authorization and user authorization. The intersection of the two authorization modes is used.

1. Log in to the web console of the instance as user **sysadmin**.
2. In the navigation pane, choose **Data Encryption** > **Authorization Management**.
3. In the data source list, click a data source.
4. Locate the target encrypted database table and click **Client Authorization**.

5. In the **Client Authorization** dialog box, set the client IP address range, time range, and week range, and then click **Save**.

**Figure 4-14** Client authorization



Client Authorization

IP Range:

196.168.0.100-196.168.0.120

196.168.1.100-196.168.1.120

Time Range:

00 - 23

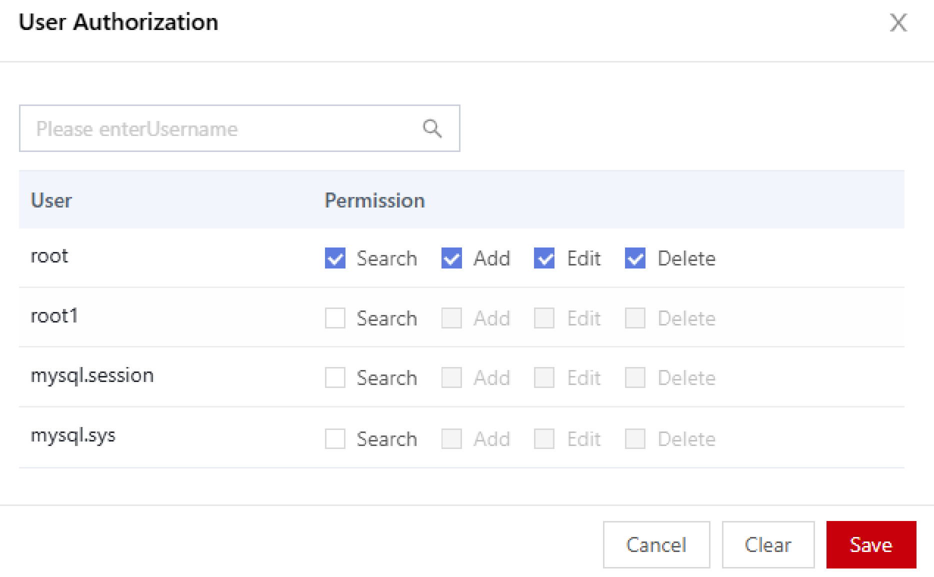
Week Range:

Monday - Sunday

You can set the start IP address and end IP address for an IP address range. You can click ⊕ to add multiple IP address ranges. A maximum of 10 IP address ranges can be set.

6. Locate the target encrypted database table and click **User Authorization**.
7. In the **User Authorization** dialog box, set permissions for the database user and click **Save**.

**Figure 4-15** User authorization



User Authorization

Please enterUsername

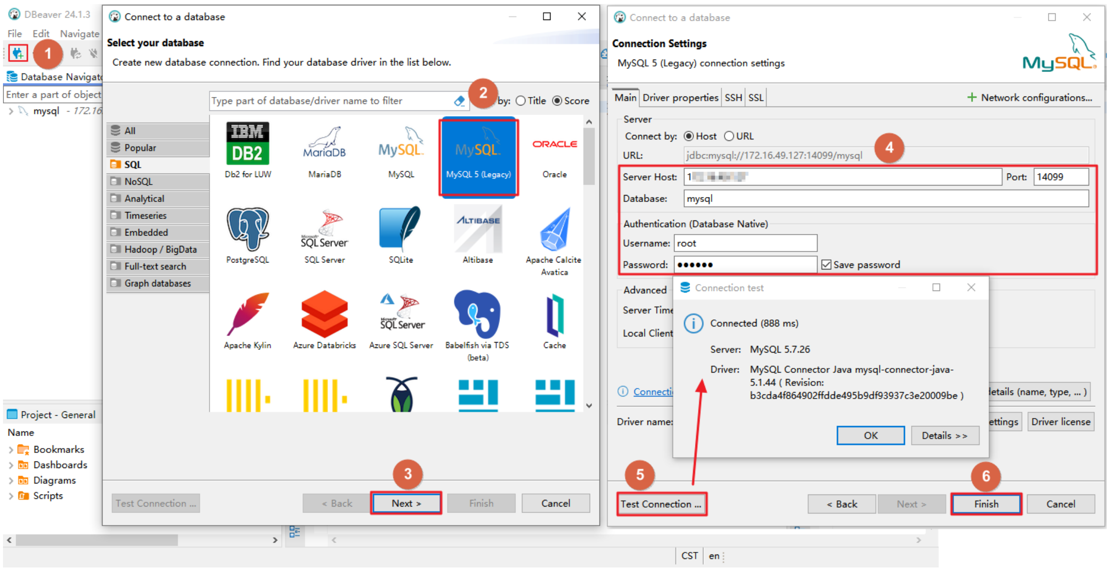
| User | Permission |
|---|---|
| root | ☑ Search ☑ Add ☑ Edit ☑ Delete |
| root1 | □ Search □ Add □ Edit □ Delete |
| mysql.session | □ Search □ Add □ Edit □ Delete |
| mysql.sys | □ Search □ Add □ Edit □ Delete |

**Step 6: Connecting to the Database Through a Proxy**

> **CAUTION**
>
> The DBeaver tool is used as an example. In practice, you need to modify the information about the connection between the application system and the database.

This section uses the DBeaver tool as an example to describe how to connect to the database through a proxy.

**Figure 4-16** Connecting to the database through a proxy



Connect by: ● Host ○ URL

URL: jdbc:mysql://172.16.49.127:14099/mysql

Server Host: [redacted] Port: 14099

Database: mysql

Authentication (Database Native)

Username: root

Password: ●●●●●● ☑ Save password

Connected (888 ms)

Server: MySQL 5.7.26

Driver: MySQL Connector Java mysql-connector-java-5.1.44 ( Revision: b3cda4f864902ffdde495b9df93937c3e20009be )

1. Click .
2. In the **Select your database** dialog box, select MySQL.
3. Click **Next**.
4. In the **Connection Settings** dialog box, configure the connection information.

   The connection information is described as follows:

   – Address: IP address of database encryption and access control. For example, **192.*xx*.*xx*.54**.

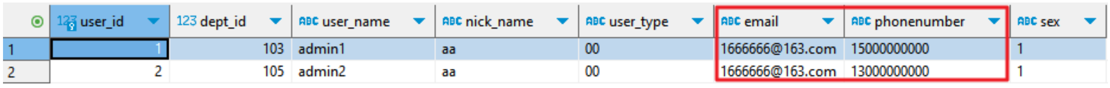
   – Port: Use the proxy port, that is, the proxy port (14099) set during asset creation.
5. Click **Test Connection** to check whether the database can be connected.
6. After the test is passed, click **Next** and perform operations as prompted.

**Step 7: Verifying the Encryption Result**

Connect to the database by referring to Step 6 (Connecting to the Database Through a Proxy) to check whether the authorization is successfully configured.

1. A user whose IP address is 192.168.0.105 (authorized address) can view plaintext data when accessing the database as an authorized user (for example, user root) in proxy mode.

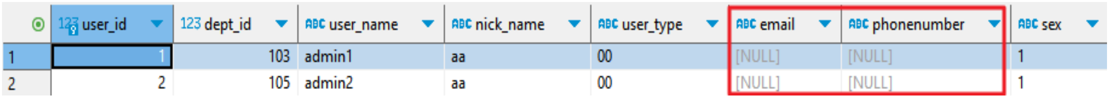
**Figure 4-17** Plaintext data



| | user_id | dept_id | user_name | nick_name | user_type | email | phonenumber | sex |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 103 | admin1 | aa | 00 | 1666666@163.com | 15000000000 | 1 |
| 2 | 2 | 105 | admin2 | aa | 00 | 1666666@163.com | 13000000000 | 1 |

2. A user whose IP address is 192.168.0.105 (authorized address) accesses the database as an unauthorized user (for example, user01) in proxy mode. Only encrypted data can be viewed.

**Figure 4-18** Encrypted data

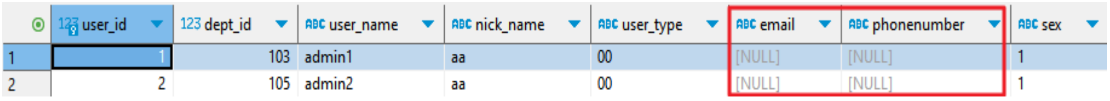


| | user_id | dept_id | user_name | nick_name | user_type | email | phonenumber | sex |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 103 | admin1 | aa | 00 | [NULL] | [NULL] | 1 |
| 2 | 2 | 105 | admin2 | aa | 00 | [NULL] | [NULL] | 1 |

The encryption result is displayed based on the default display parameter of no permission configured during asset adding.

3. The IP address of the user is 192.168.3.105 (an unauthorized address). When the user accesses the database in proxy mode as an authorized user (for example, user root), only encrypted data can be viewed.

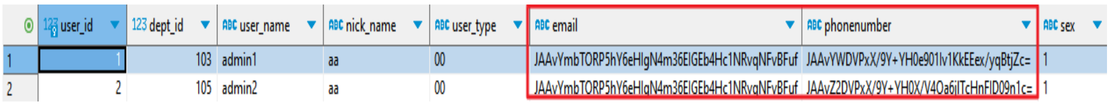
**Figure 4-19** Encrypted data



| | user_id | dept_id | user_name | nick_name | user_type | email | phonenumber | sex |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 103 | admin1 | aa | 00 | [NULL] | [NULL] | 1 |
| 2 | 2 | 105 | admin2 | aa | 00 | [NULL] | [NULL] | 1 |

4. In this case, use the original database address to access the database and view the ciphertext data.

**Figure 4-20** Encrypted data



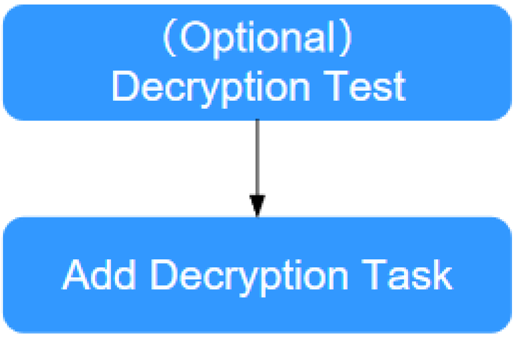
| | user_id | dept_id | user_name | nick_name | user_type | email | phonenumber | sex |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 103 | admin1 | aa | 00 | JAAvYmbTORP5hY6eHIgN4m36ElGEb4Hc1NRvqNFvBFuf | JAAvYWDVPxX/9Y+YH0e901lv1KkEEex/yqBtjZc= | 1 |
| 2 | 2 | 105 | admin2 | aa | 00 | JAAvYmbTORP5hY6eHIgN4m36ElGEb4Hc1NRvqNFvBFuf | JAAvZ2DVPxX/9Y+YH0X/V4Oa6jITcHnFID09n1c= | 1 |

## 4.4.2 Scenario 2: Decryption Process and Typical Decryption Configuration

### Decryption Process

Figure 4-21 shows the decryption process of database encryption and access control.

**Figure 4-21** Decryption process



1. (Optional) Perform an emulation decryption test.

   Perform the simulation decryption test to check whether the target supports decryption. For details, see **Simulated Decryption Test**.

2. Create a decryption task.

   Create a decryption task. For details, see **Configuring a Decryption Task**.

## Typical Configuration of the Decryption Function

After database assets are encrypted, they do not need to be encrypted if services are changed. In this case, you need to restore the database table by using the decryption function and the table structure rollback function. This example shows how to decrypt database tables.

### Prerequisite

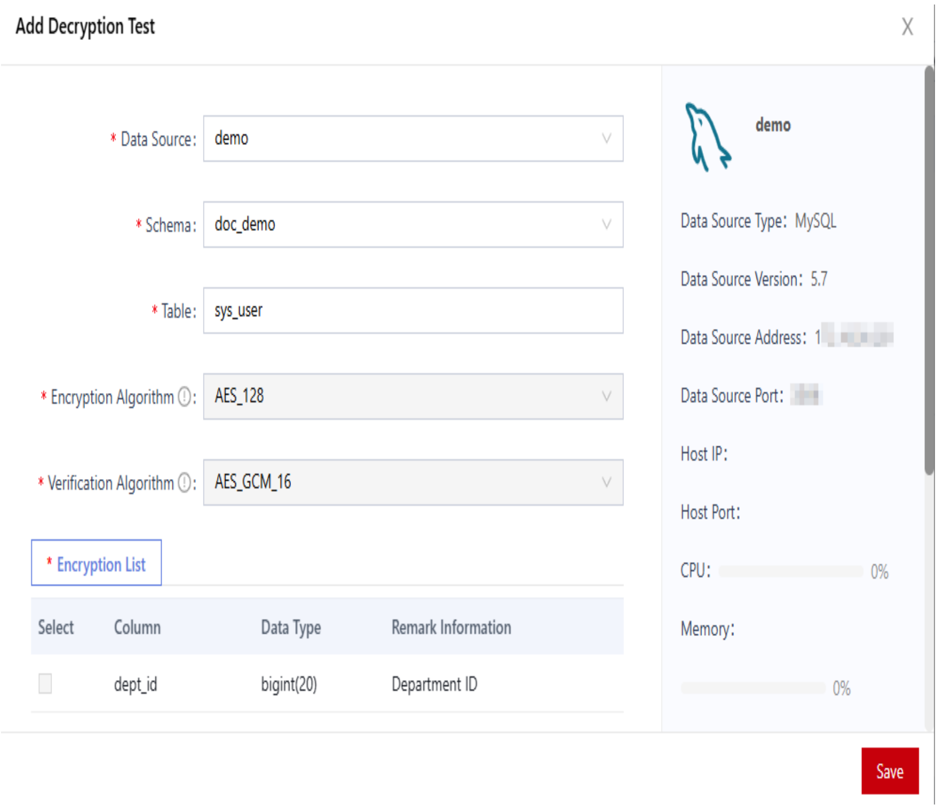
Database tables have been encrypted. For details, see **Scenario 1: Encryption Process and Typical Encryption Configuration**.

### Step 1: Performing a Simulated Decryption Test

Before decrypting a database table, perform a simulation decryption test to check whether the database meets the decryption requirements.

1. **Log in to the web console of the instance** as user **sysadmin**.
2. In the navigation tree, choose **Service Test** > **Simulation Test**.
3. Click **Add Decryption Test**.
4. In the **Add Decryption Test** dialog box, configure the test target.

**Figure 4-22** The decryption test is added.



Add Decryption Test

* Data Source: demo

* Schema: doc_demo

* Table: sys_user

* Encryption Algorithm: AES_128

* Verification Algorithm: AES_GCM_16

* Encryption List

| Select | Column | Data Type | Remark Information |
|---|---|---|---|
| □ | dept_id | bigint(20) | Department ID |

demo

Data Source Type: MySQL

Data Source Version: 5.7

Data Source Address: 1[redacted]

Data Source Port: [redacted]

Host IP:

Host Port:

CPU: 0%

Memory: 0%

5. Click **Save**.

   After the test is complete, you can view the test result in the list and click **Details** to view the completion status of each node in the decryption process.

   If a fault occurs during the simulation test, rectify the fault as prompted.

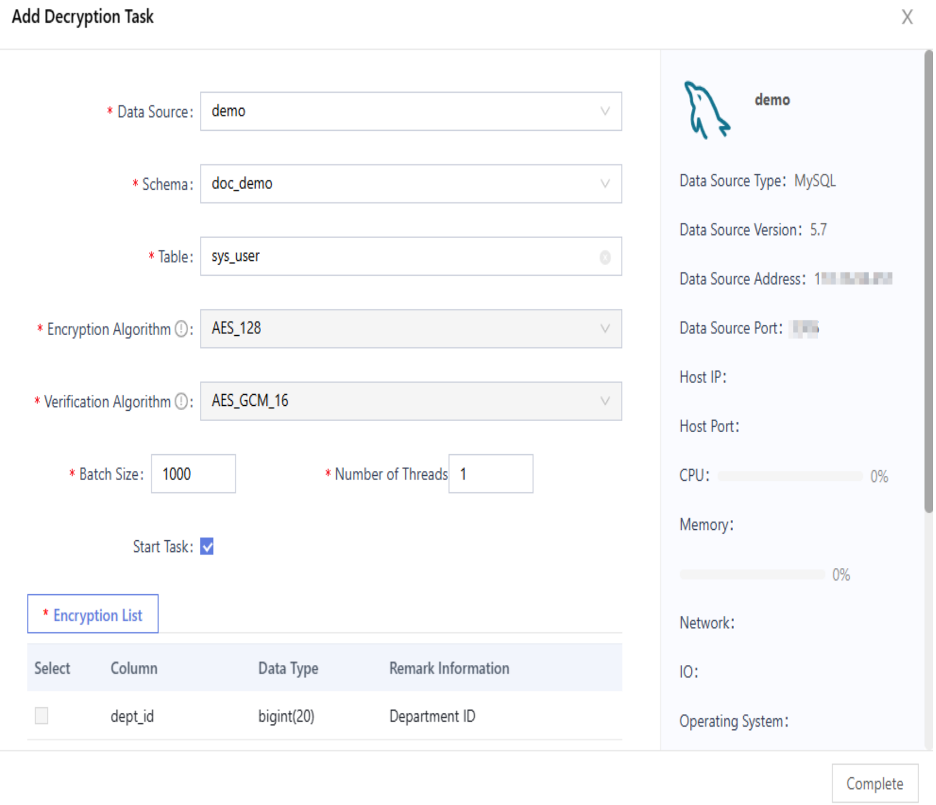
6. After the test is complete, click **Delete** to delete the simulated decryption test.

   If a decryption task needs to be configured after the test, delete the simulated decryption test first.

### Step 2: Creating a Decryption Task

1. **Log in to the web console of the instance** as user **sysadmin**.
2. In the navigation tree on the left, choose **Data Encryption** > **Decryption Task Management**.
3. Click **Add Decryption Task** in the upper right corner.
4. In the **Add Decryption Task** dialog box, set and encrypt the corresponding data information, including the asset name, schema name, and table name.

**Figure 4-23** Adding a decryption task



Add Decryption Task

* Data Source: demo

* Schema: doc_demo

* Table: sys_user

* Encryption Algorithm: AES_128

* Verification Algorithm: AES_GCM_16

* Batch Size: 1000 * Number of Threads 1

Start Task: ☑

* Encryption List

| Select | Column | Data Type | Remark Information |
|---|---|---|---|
| □ | dept_id | bigint(20) | Department ID |

demo

Data Source Type: MySQL

Data Source Version: 5.7

Data Source Address: [redacted]

Data Source Port: [redacted]

Host IP:

Host Port:

CPU: 0%

Memory: 0%

Network:

IO:

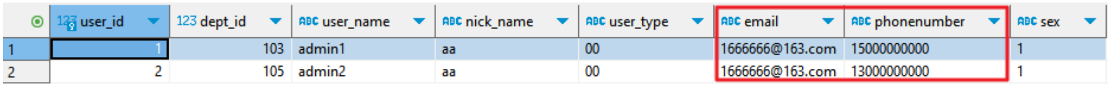
Operating System:

5. Select **Start Task**. After the creation is complete, the decryption task is automatically started.
6. Click **Complete**.

**Step 3: Verifying the Configuration**

After decryption, use the original database address or proxy address to query the database table content. If the following information is displayed, the database table has been restored:

**Figure 4-24** Querying the result through the proxy

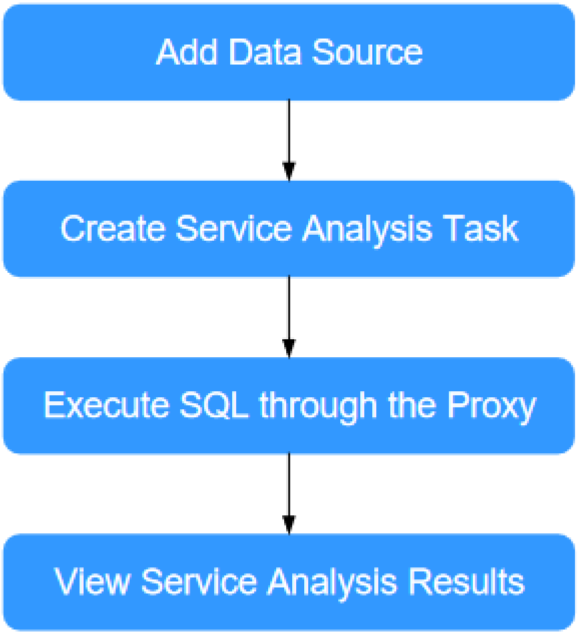


| | user_id | dept_id | user_name | nick_name | user_type | email | phonenumber | sex |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 103 | admin1 | aa | 00 | 1666666@163.com | 15000000000 | 1 |
| 2 | 2 | 105 | admin2 | aa | 00 | 1666666@163.com | 13000000000 | 1 |

## 4.4.3 Scenario 3: Typical Configuration Examples for Service Tests

Database encryption and access control support initial analysis on database assets by using the service analysis function to eliminate service errors that may be caused by encryption. Figure 4-25 shows the service test process.

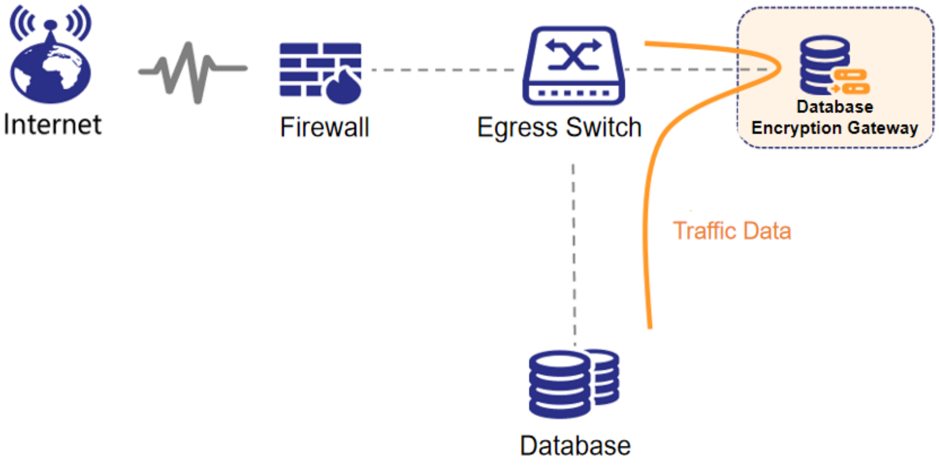
**Figure 4-25** Service test process


Add Data Source
Create Service Analysis Task
Execute SQL through the Proxy
View Service Analysis Results

### Networking Description

Database encryption and access control uses the reverse proxy mode. The following figure shows the typical networking.

**Figure 4-26** Networking



### Prerequisites

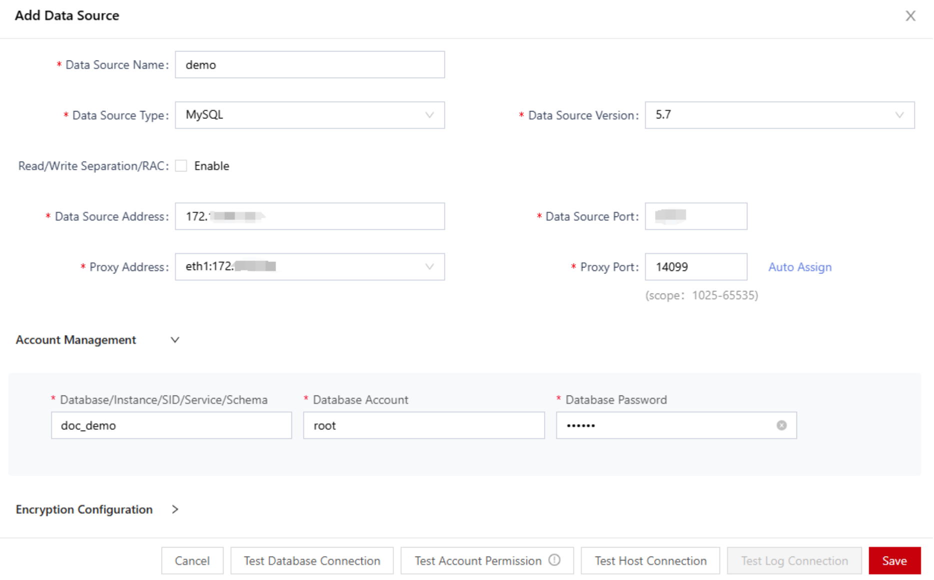
- The route between the device and the application system is reachable.
- The route between the device and the database is reachable.

### Step 1: Adding a Data Source

Add a database on the **Assets Management** page.

1. **Log in to the web console of the instance** as user **sysadmin**.
2. In the navigation pane, choose **Assets Management** > **Data Source Management**.
3. Click **Add Data Source** in the upper right corner.
4. In the **Add Data Source** dialog box, configure asset information.

**Figure 4-27** Adding a data source



Add Data Source

* Data Source Name: demo

* Data Source Type: MySQL

* Data Source Version: 5.7

Read/Write Separation/RAC: □ Enable

* Data Source Address: 172.[redacted]

* Data Source Port: [redacted]

* Proxy Address: eth1:172.[redacted]

* Proxy Port: 14099 Auto Assign

(scope: 1025-65535)

Account Management

| * Database/Instance/SID/Service/Schema | * Database Account | * Database Password |
|---|---|---|
| doc_demo | root | •••••• |

Encryption Configuration

Host information and log information are optional. The SSH service must be enabled on the database server.

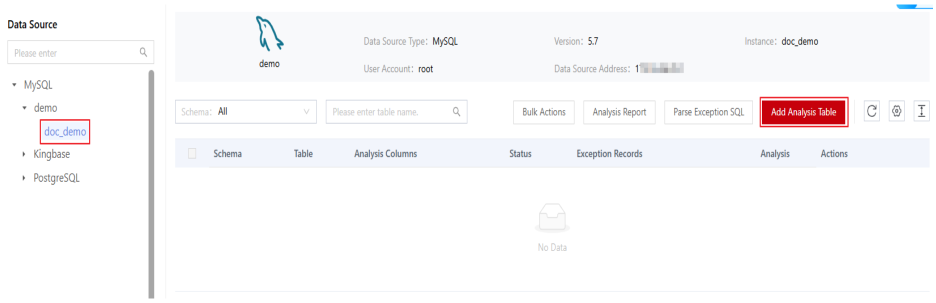
5. After the configuration is complete, click **Test Database Connection** to check whether the database can be connected.
6. Click **Test Account Permission** to check whether the database account permission meets the encryption requirements.
7. Click **Save**.

### Step 2: Creating a Service Analysis Task

Before encryption, create a service analysis task to test whether the service SQL is supported.

1. **Log in to the web console of the instance** as user **sysadmin**.
2. In the navigation tree on the left, choose **Service Test** > **Service Analysis**.
3. In the data source area on the left, click a data source.

**Figure 4-28** Adding a service analysis task



Data Source

Please enter

- MySQL
  - demo
    - doc_demo
  - Kingbase
  - PostgreSQL

demo

Data Source Type: MySQL

Version: 5.7

Instance: doc_demo

User Account: root

Data Source Address: 1[redacted]

Schema: All

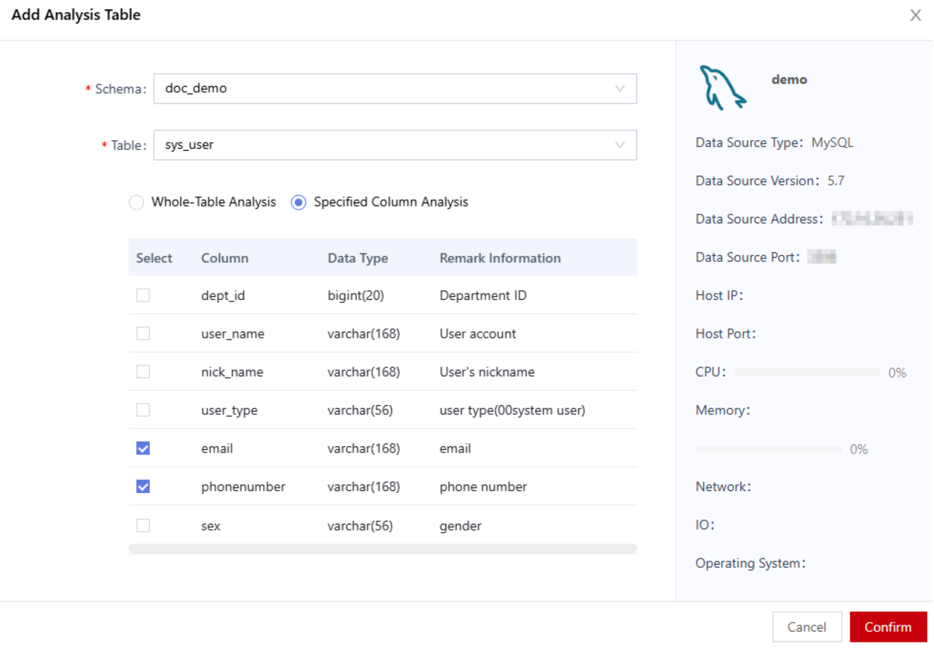
Please enter table name.

| ☐ | Schema | Table | Analysis Columns | Status | Exception Records | Analysis | Actions |
|---|---|---|---|---|---|---|---|

No Data

4. Click **Add Analysis Table**, configure a table, and click **Confirm**.

**Figure 4-29** Configuring a table for analysis



Add Analysis Table

* Schema: doc_demo

* Table: sys_user

○ Whole-Table Analysis ● Specified Column Analysis

| Select | Column | Data Type | Remark Information |
|---|---|---|---|
| ☐ | dept_id | bigint(20) | Department ID |
| ☐ | user_name | varchar(168) | User account |
| ☐ | nick_name | varchar(168) | User's nickname |
| ☐ | user_type | varchar(56) | user type(00system user) |
| ☑ | email | varchar(168) | email |
| ☑ | phonenumber | varchar(168) | phone number |
| ☐ | sex | varchar(56) | gender |

demo

Data Source Type: MySQL

Data Source Version: 5.7

Data Source Address: [redacted]

Data Source Port: [redacted]

Host IP:

Host Port:

CPU: 0%

Memory: 0%

Network:

IO:

Operating System:

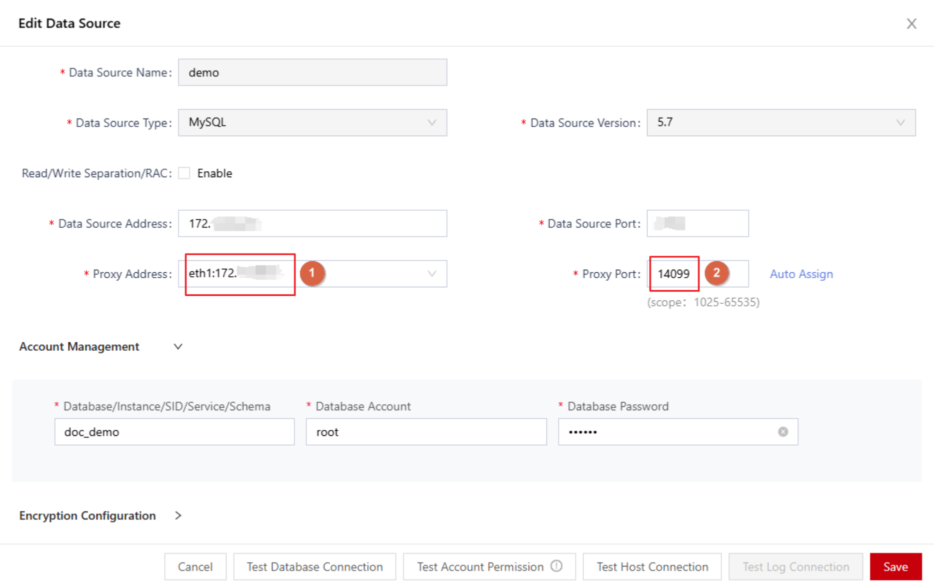
Locate the target table and click the start button ▷.

### Step 3: Running SQL Statements Through the Proxy

Use the proxy address to access the database and run service SQL statements to check whether services are affected after database tables and fields are encrypted.

1. Log in to the web console of the instance as user **sysadmin**.
2. In the navigation pane on the left, choose **Assets Management** > **Data Source Management**, locate the target database, and click **Edit** to view the database proxy IP address and port number.

**Figure 4-30** Viewing the proxy IP address and port number



Edit Data Source

* Data Source Name: demo

* Data Source Type: MySQL

* Data Source Version: 5.7

Read/Write Separation/RAC: □ Enable

* Data Source Address: 172.[redacted]

* Data Source Port: [redacted]

* Proxy Address: eth1:172.[redacted]

* Proxy Port: 14099

(scope: 1025-65535)

Account Management

* Database/Instance/SID/Service/Schema: doc_demo

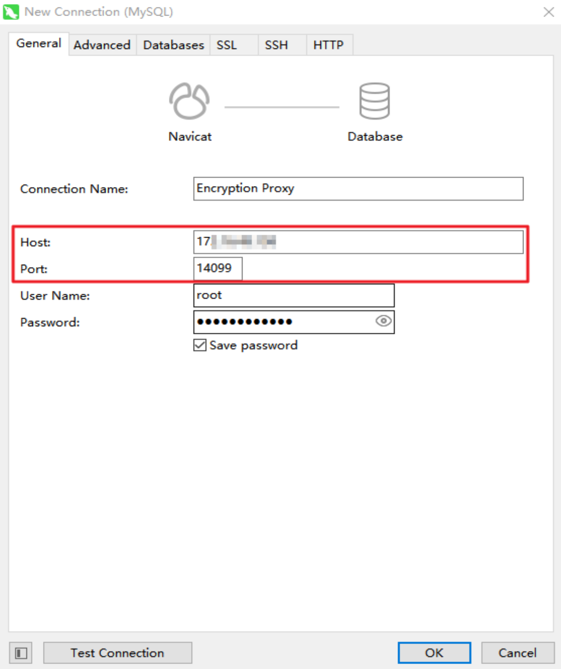
* Database Account: root

* Database Password: ••••••

Encryption Configuration

3. On the database connection tool, use the proxy IP address and port to access the database.

**Figure 4-31** Accessing a database



New Connection (MySQL)

Connection Name: Encryption Proxy

Host: 17[redacted]

Port: 14099

User Name: root

Password: ••••••••••••

☑ Save password

Set the IP address and port number to the proxy IP address and port number obtained in the previous step. Set the username and password to the original username and password of the database.

4. Execute the SQL statement used by the service.

   The preceding SQL statements are only examples. In practice, you need to run the SQL statements used in services to facilitate service analysis.

**Table 4-9** SQL statement examples

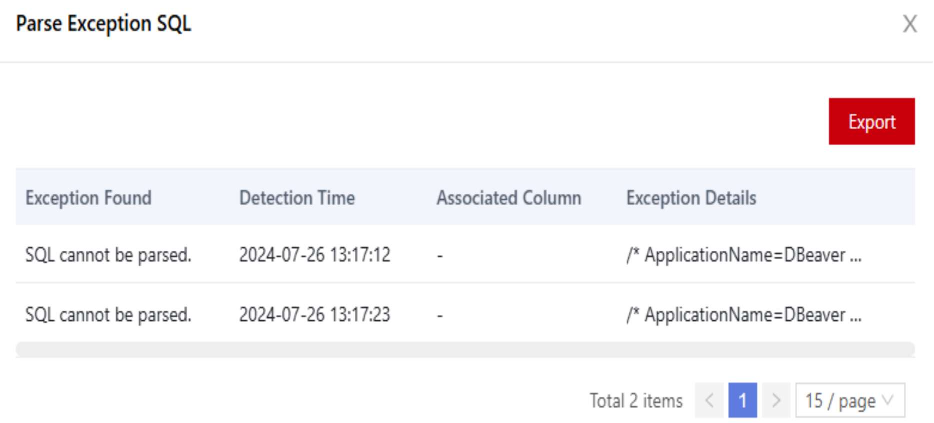
| SQL type. | Example |
|---|---|
| Normal Statement | SELECT * FROM `sys_user`; |
| Exception statements: | SELECT * FROMM `sys_user`; |
| Blocking Statement | RENAME TABLE sys_user to abc; |

### Step 4: Viewing the Service Analysis Result

After service SQL statements are executed, the system records abnormal and blocked SQL statements and analyzes the blocking causes.

1. **Log in to the web console of the instance** as user **sysadmin**.
2. In the navigation tree on the left, choose **Service Test** > **Service Analysis**.
3. In the data source area on the left, click a data source.
4. Click **Parse Exception SQL** to view the abnormal SQL statements.

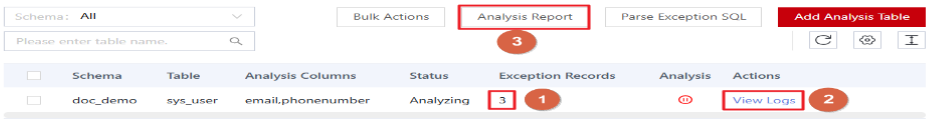
**Figure 4-32** Abnormal SQL statements



| Exception Found | Detection Time | Associated Column | Exception Details |
|---|---|---|---|
| SQL cannot be parsed. | 2024-07-26 13:17:12 | - | /* ApplicationName=DBeaver ... |
| SQL cannot be parsed. | 2024-07-26 13:17:23 | - | /* ApplicationName=DBeaver ... |

5. View blocked SQL statements and system suggestions.

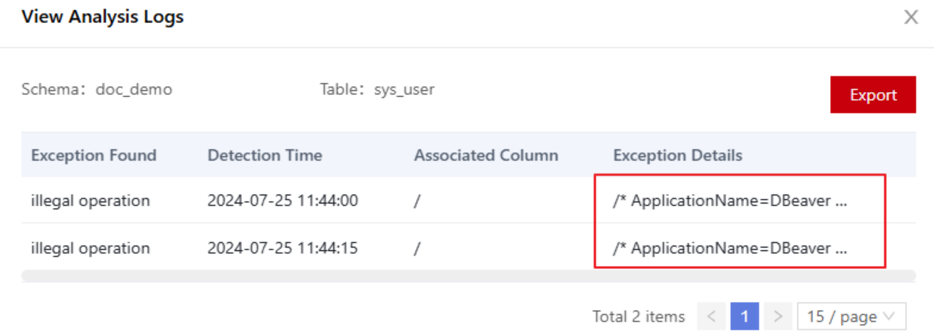
**Figure 4-33** Blocked SQL statements



| Schema | Table | Analysis Columns | Status | Exception Records | Analysis | Actions |
|---|---|---|---|---|---|---|
| doc_demo | sys_user | email,phonenumber | Analyzing | 3 | | View Logs |

6. In the **Exception Records** column, view the number of blocked SQL statements.
7. Click **View Logs** to view the specific blocked SQL statement and error message.

**Figure 4-34** SQL statement blocking log



View Analysis Logs

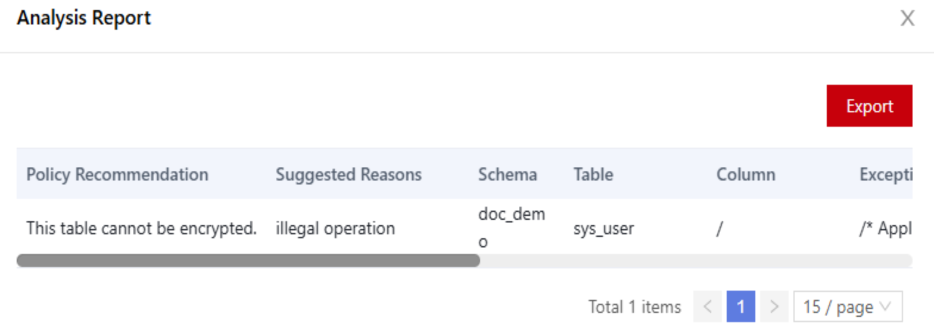
Schema: doc_demo Table: sys_user

| Exception Found | Detection Time | Associated Column | Exception Details |
|---|---|---|---|
| illegal operation | 2024-07-25 11:44:00 | / | /* ApplicationName=DBeaver ... |
| illegal operation | 2024-07-25 11:44:15 | / | /* ApplicationName=DBeaver ... |

Total 2 items

8. Click **Analysis Report** to view the encryption suggestions of the table.

**Figure 4-35** Analysis and suggestions



Analysis Report

| Policy Recommendation | Suggested Reasons | Schema | Table | Column | Excepti |
|---|---|---|---|---|---|
| This table cannot be encrypted. | illegal operation | doc_demo | sys_user | / | /* Appl |

Total 1 items

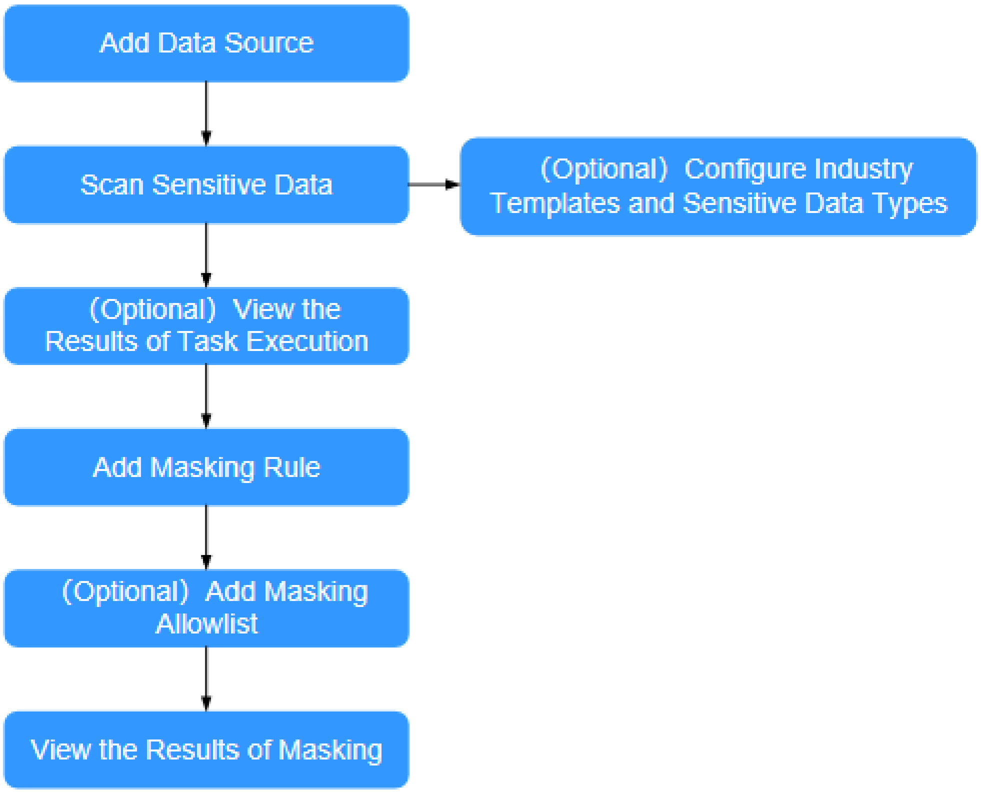
The service test result shows that if the database table is encrypted, the SQL statement running of the service is affected. Therefore, you are not advised to encrypt the database table.

## 4.4.4 Scenario 4: Typical Dynamic Data Masking Configuration

### Dynamic Data Masking Flowchart

With database encryption and access control, you can configure dynamic masking policies to mask plaintext data in database assets. **Figure 4-36** shows the dynamic masking process.

**Figure 4-36** Dynamic masking process


Add Data Source
Scan Sensitive Data
(Optional) Configure Industry Templates and Sensitive Data Types
(Optional) View the Results of Task Execution
Add Masking Rule
(Optional) Add Masking Allowlist
View the Results of Masking

1. Add a data source.

   Before using the data masking function, you need to add data assets to the system. For details, see **Adding Data Assets**.

2. (Optional) Configure the industry template and sensitive data type.

   The system has built-in sensitive data types and common industry templates that meet most requirements. If you have special requirements, you can also customize sensitive data types and industry templates. For details, see **Adding an Industry Template** and **Adding a User-Defined Data Type**.

3. Perform sensitive data discovery.

   A sensitive data discovery task automatically scans and identifies sensitive data in data assets. For details, see **Scanning Sensitive Data in Assets**.

4. (Optional) View the task execution result.

   You can view the matched sensitive data in task execution results. For details, see **Viewing the Execution Result of a Scan Task**.

5. Create a data masking rule.

   You can create an encryption task based on sensitive data information in the result of a sensitive data discovery task. For details, see **Creating a Masking Rule in the Result**.

   You can also directly create masking rules in the dynamic masking module. For details, see **Creating a Data Masking Rule**.

6. (Optional) Configure a masking allowlist.

   After a masking rule is configured and enabled, when you access the plaintext data in the database, you can only view the masking results of data by default. Users in the allowlist can view plaintext data when accessing the database. For details, see Configuring a Data Masking Allowlist.

7. After the configuration is complete, you can use a proxy to access the masking rule to verify the configuration effect.

## Typical Dynamic Masking Configuration

Database encryption and access control support dynamic masking of sensitive plaintext data in the database. This example shows how to dynamically mask plaintext data in the database.

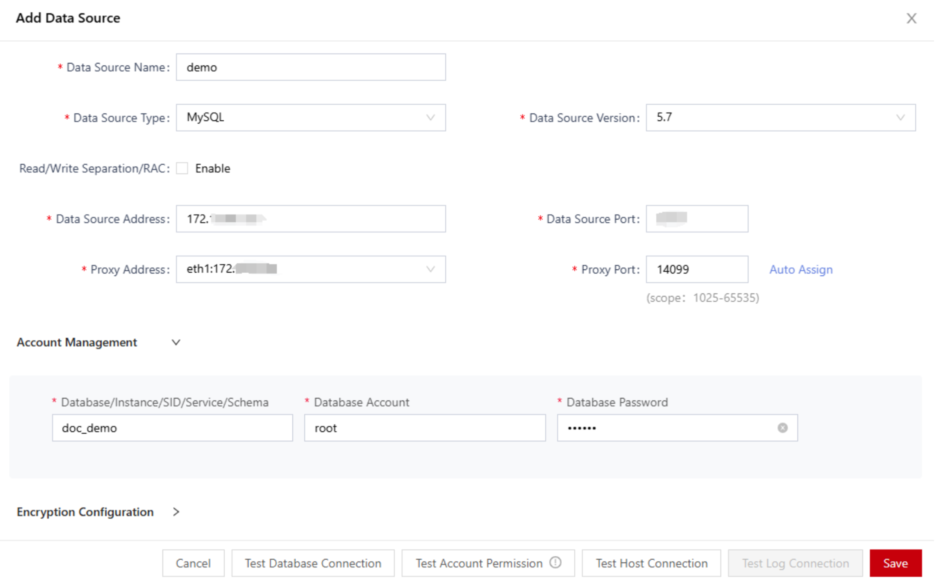
### Step 1: Adding a Data Source

Add a database on the **Assets Management** page.

1. Log in to the web console of the instance as user **sysadmin**.
2. In the navigation pane, choose **Assets Management** > **Data Source Management**.
3. Click **Add Data Source** in the upper right corner.
4. In the **Add Data Source** dialog box, configure asset information.

   Host information and log information are optional. The SSH service must be enabled on the database server.

**Figure 4-37** Adding a data source



Add Data Source

* Data Source Name: demo

* Data Source Type: MySQL

* Data Source Version: 5.7

Read/Write Separation/RAC: □ Enable

* Data Source Address: 172.[redacted]

* Data Source Port: [redacted]

* Proxy Address: eth1:172.[redacted]

* Proxy Port: 14099 Auto Assign

(scope: 1025-65535)

Account Management

* Database/Instance/SID/Service/Schema: doc_demo

* Database Account: root

* Database Password: ••••••

Encryption Configuration

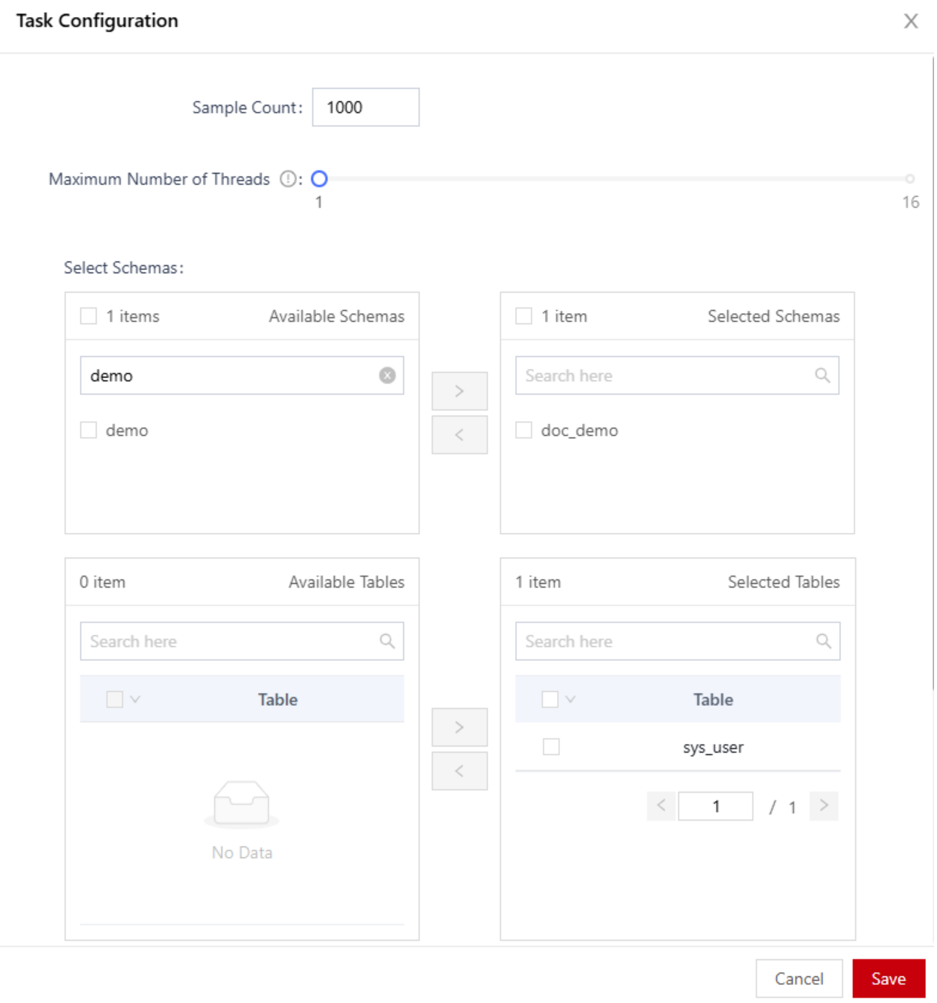
5. After the configuration is complete, click **Test Database Connection** to check whether the database can be connected.
6. Click **Test Account Permission** to check whether the database account permission meets the encryption requirements.
7. Click **Save**.

### Step 2: Executing a Sensitive Data Discovery Task

1. Log in to the web console of the instance as user **sysadmin**.

2. In the navigation tree on the left, choose **Sensitive Data Discovery** > **Sensitive Data Scanning**.
3. Find the target data asset and click **Task Configuration**.
4. In the **Task Configuration** dialog box, set a sensitive data discovery task.

**Figure 4-38** Configuring a sensitive data discovery task



Task Configuration

Sample Count: 1000

Maximum Number of Threads ⓘ: 1 – 16

Select Schemas:

| □ 1 items | Available Schemas |
|---|---|
| demo | |
| □ demo | |

| □ 1 item | Selected Schemas |
|---|---|
| Search here | |
| □ doc_demo | |

| 0 item | Available Tables |
|---|---|
| □ | Table |
| No Data | |

| 1 item | Selected Tables |
|---|---|
| □ | Table |
| □ | sys_user |

1 / 1

Cancel Save

5. Click **Save**.
6. Find the target data asset and click ▷ to execute the sensitive data discovery task.

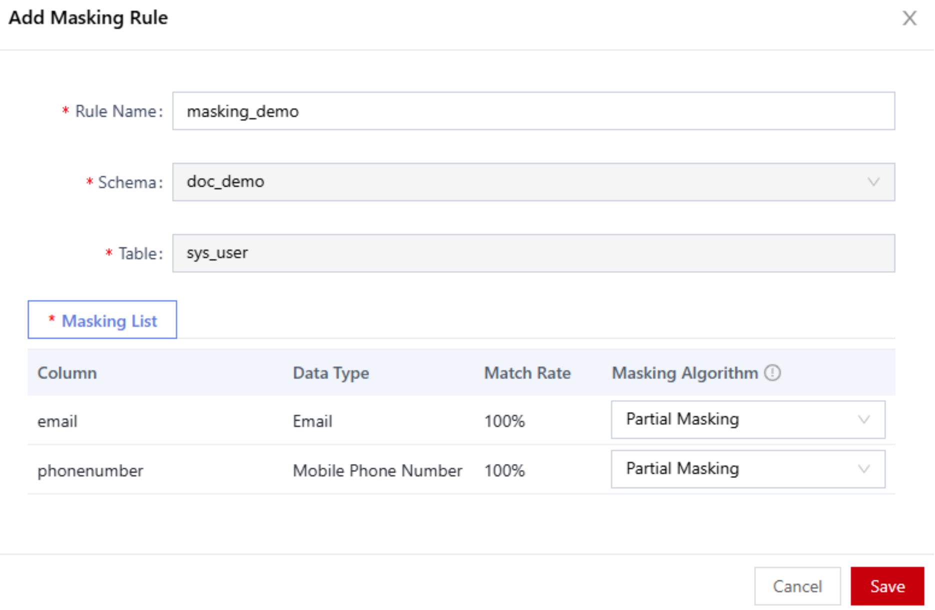
After the execution starts, the system automatically scans and identifies sensitive data. The scan duration depends on the amount of data to be scanned. The larger the amount of data, the longer the scan duration. You can view the scan progress on the page.

**Step 3: Creating a Masking Rule in the Discovery Result**

1. **Log in to the web console of the instance** as user **sysadmin**.
2. In the navigation tree on the left, choose **Sensitive Data Discovery** > **Sensitive Data Scanning**.
3. On the scan task list page, locate the target data asset and click **View**.

4. On the scan result page, locate the target database table and click **Add Masking Rule**.
5. In the **Add Masking Rule** dialog box, configure the masking information.

**Figure 4-39** Adding a masking rule



Add Masking Rule

* Rule Name: masking_demo

* Schema: doc_demo

* Table: sys_user

* Masking List

| Column | Data Type | Match Rate | Masking Algorithm |
|---|---|---|---|
| email | Email | 100% | Partial Masking |
| phonenumber | Mobile Phone Number | 100% | Partial Masking |

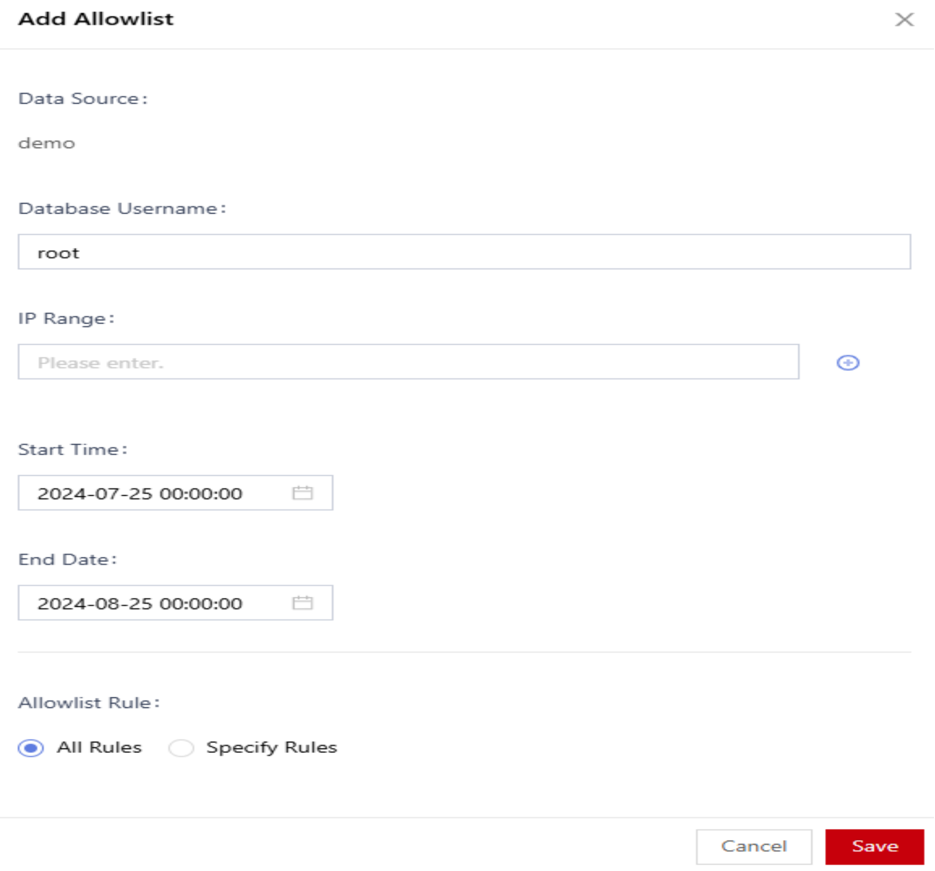
6. Configure the rule name and select the masking algorithm corresponding to the data type from the masking list.
7. Click **Save**.

The masking rule is automatically enabled after being saved. If plaintext data is queried during database access, the masking results of the data will be retrieved. In this case, you can configure a masking allowlist. If data matching the allowlist will not be masked.

**Step 4: Configuring the Masking Allowlist**

1. **Log in to the web console of the instance** as user **sysadmin**.
2. In the navigation pane on the left, choose **Dynamic Data Mask** > **Data Masking Policy**.
3. In the data source list, click a data source.
4. Locate the masking rule list of the target data source and click **Allowlist Rule**.
5. On the allowlist page, click **Add Allowlist**.
6. In the **Add Allowlist** dialog box, set the allowlist range and click **Save**.

**Figure 4-40** Adding an allowlist



Add Allowlist

Data Source:

demo

Database Username:

root

IP Range:

Please enter.

Start Time:

2024-07-25 00:00:00

End Date:

2024-08-25 00:00:00

Allowlist Rule:

● All Rules ○ Specify Rules

The allowlist parameters include the database username, IP address range, start time, and end time. The relationship between the parameters is AND. If multiple parameters are configured, the allowlist takes effect only when all the parameters are matched.

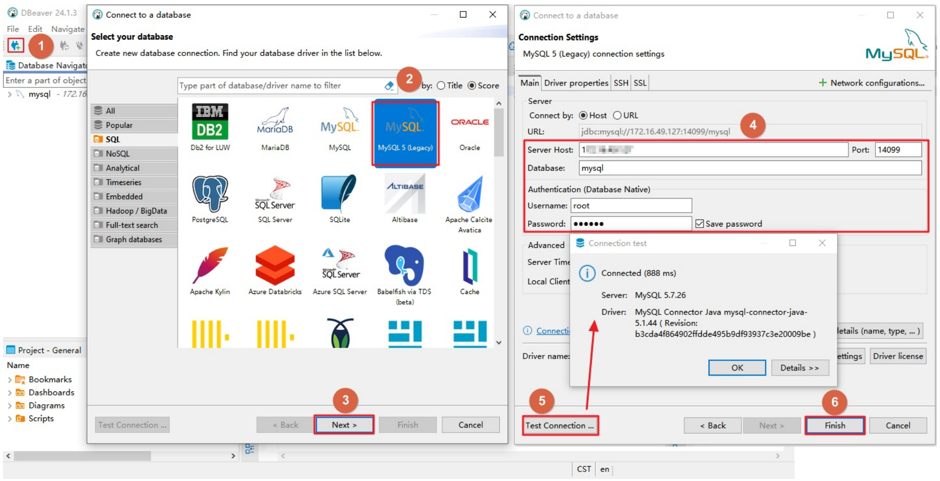
**Step 5: Connecting to the Database Through a Proxy**

⚠ CAUTION

The DBeaver tool is used as an example. In practice, you need to modify the information about the connection between the application system and the database.

This section uses the DBeaver tool as an example to describe how to connect to the database through a proxy.

**Figure 4-41** Connecting to the database through a proxy



Connect to a database

Select your database

Create new database connection. Find your database driver in the list below.

Connect to a database

Connection Settings

MySQL 5 (Legacy) connection settings

Main | Driver properties | SSH | SSL

Server

Connect by: ● Host ○ URL

URL: jdbc:mysql://172.16.49.127:14099/mysql

Server Host: [redacted] Port: 14099

Database: mysql

Authentication (Database Native)

Username: root

Password: •••••• ☑ Save password

Connection test

Connected (888 ms)

Server: MySQL 5.7.26

Driver: MySQL Connector Java mysql-connector-java-5.1.44 ( Revision: b3cda4f864902ffdde495b9df93937c3e20009be )

1. Click .
2. In the **Select your database** dialog box, select MySQL.
3. Click **Next**.
4. In the **Connection Settings** dialog box, configure the connection information.

   The connection information is described as follows:

   – Address: IP address of database encryption and access control Example: **192**.*xx*.*xx*.**54**

   – Port: Use the proxy port, that is, the proxy port (14099) set during asset creation.

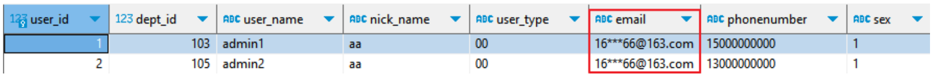
5. Click **Test Connection** to check whether the database can be connected.
6. After the test is passed, click **Next** and perform operations as prompted.

### Step 6: Verifying the Masking Result

Connect to the database by referring to Step 5 (Connecting to the Database Through a Proxy) and check whether the masking rule and masking allowlist are successfully configured.

1. If the IP address of a user is 172.16.215.108 (not in the masking allowlist) and the user accesses the database through a proxy, only the masking results of data will be displayed.

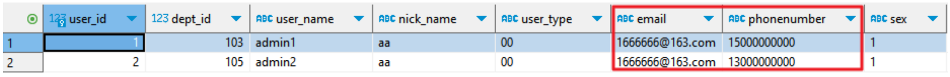
   **Figure 4-42** Masked data

   | user_id | dept_id | user_name | nick_name | user_type | email | phonenumber | sex |
   |---|---|---|---|---|---|---|---|
   | 1 | 103 | admin1 | aa | 00 | 16***66@163.com | 15000000000 | 1 |
   | 2 | 105 | admin2 | aa | 00 | 16***66@163.com | 13000000000 | 1 |

2. If the IP address of a user is 172.16.215.107 (in the masking allowlist) and the user accesses the database through a proxy, the plaintext data will be displayed.

   **Figure 4-43** Plaintext data

   |  | user_id | dept_id | user_name | nick_name | user_type | email | phonenumber | sex |
   |---|---|---|---|---|---|---|---|---|
   | 1 | 1 | 103 | admin1 | aa | 00 | 1666666@163.com | 15000000000 | 1 |
   | 2 | 2 | 105 | admin2 | aa | 00 | 1666666@163.com | 13000000000 | 1 |

# 5 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

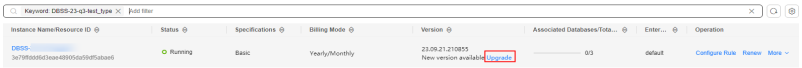
**Step 1** Log in to the management console.

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

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

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

**Figure 5-1** Upgrading the instance version



Keyword: DBSS-23-q3-test_type × Add filter

| Instance Name/Resource ID | Status | Specifications | Billing Mode | Version | Associated Databases/Tota... | Enter... | Operation |
|---|---|---|---|---|---|---|---|
| DBSS-[redacted]<br>3e79ffddd6d3eae48905da59df5abae6 | Running | Basic | Yearly/Monthly | 23.09.21.210855<br>New version available Upgrade | 0/3 | default | Configure Rule Renew More |

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

**----End**

# 6 Configuring Audit Rules

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

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

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

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

NOTE

- By default, database audit complies with a **full audit rule**, which is used to audit all databases that are connected to the database audit instance. This audit rule is enabled by default. You can disable it but cannot delete it.
- 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 6-1** Parameters

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

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

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

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

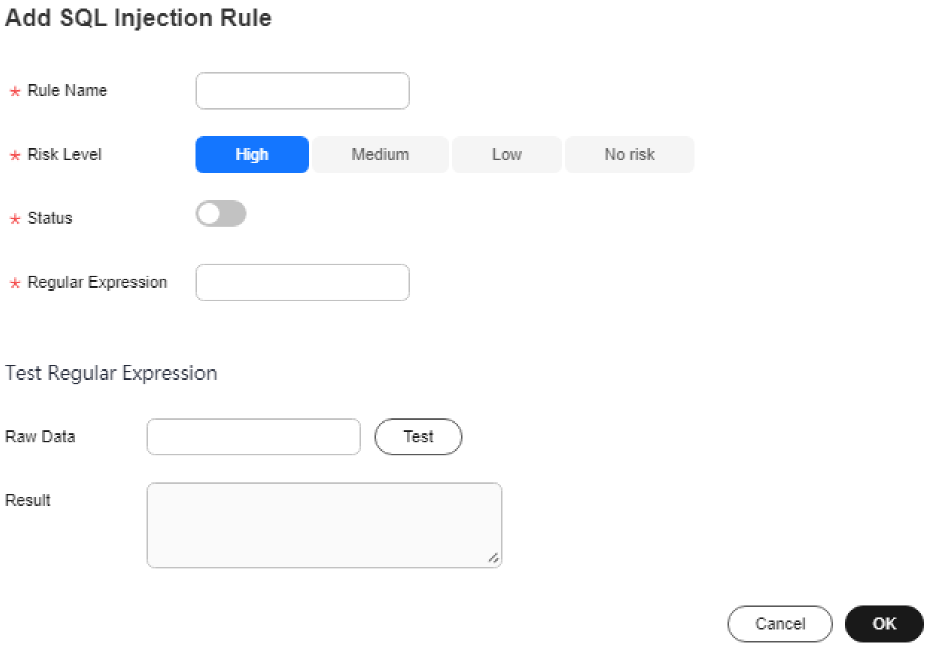
**Step 5** Click the **SQL Injection** tab.

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 6-1** Adding an SQL injection rule



Add SQL Injection Rule

* Rule Name

* Risk Level: [✓ High] Medium Low No risk

* Status

* Regular Expression

Test Regular Expression

Raw Data Test

Result

Cancel OK

**Table 6-2** SQL injection rule parameters

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

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

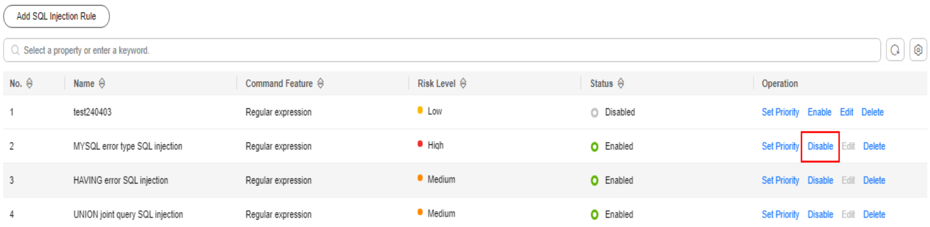
**Step 3** In the navigation tree, choose **Rules**.

**Step 4** In the **Instance** drop-down list, select the instance for which you want to disable SQL injection 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 6-2** Disabling an SQL injection rule



| No. | Name | Command Feature | Risk Level | Status | Operation |
|---|---|---|---|---|---|
| 1 | test240403 | Regular expression | ● Low | ○ Disabled | Set Priority Enable Edit Delete |
| 2 | MYSQL error type SQL injection | Regular expression | ● High | ○ Enabled | Set Priority Disable Edit Delete |
| 3 | HAVING error SQL injection | Regular expression | ● Medium | ○ Enabled | Set Priority Disable Edit Delete |
| 4 | UNION joint query SQL injection | Regular expression | ● Medium | ○ Enabled | Set Priority Disable Edit Delete |

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

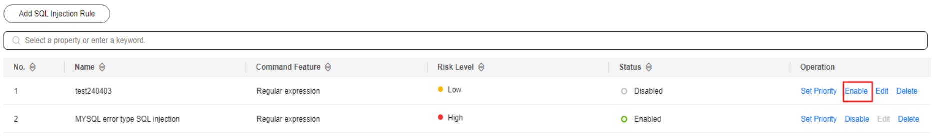
**Step 3** In the navigation tree, choose **Rules**.

**Step 4** In the **Instance** drop-down list, select the instance for which you want to 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 6-3** Enabling an SQL injection rule



| No. | Name | Command Feature | Risk Level | Status | Operation |
|---|---|---|---|---|---|
| 1 | test240403 | Regular expression | ● Low | ○ Disabled | Set Priority Enable Edit Delete |
| 2 | MYSQL error type SQL injection | Regular expression | ● High | ○ Enabled | Set Priority Disable Edit Delete |

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

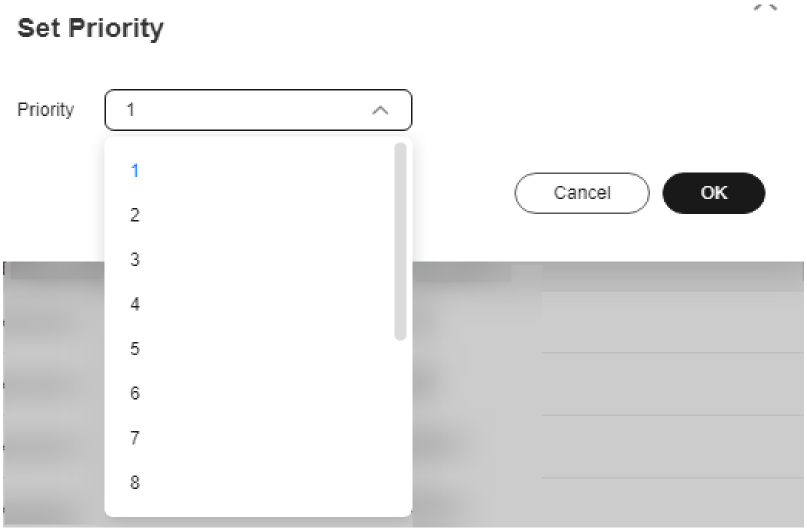
**Step 3** In the navigation tree, choose **Rules**.

**Step 4** In the **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 6-4** Configuring the priority



Set Priority

Priority: 1

**----End**

## Editing an SQL Injection Rule

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

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

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

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

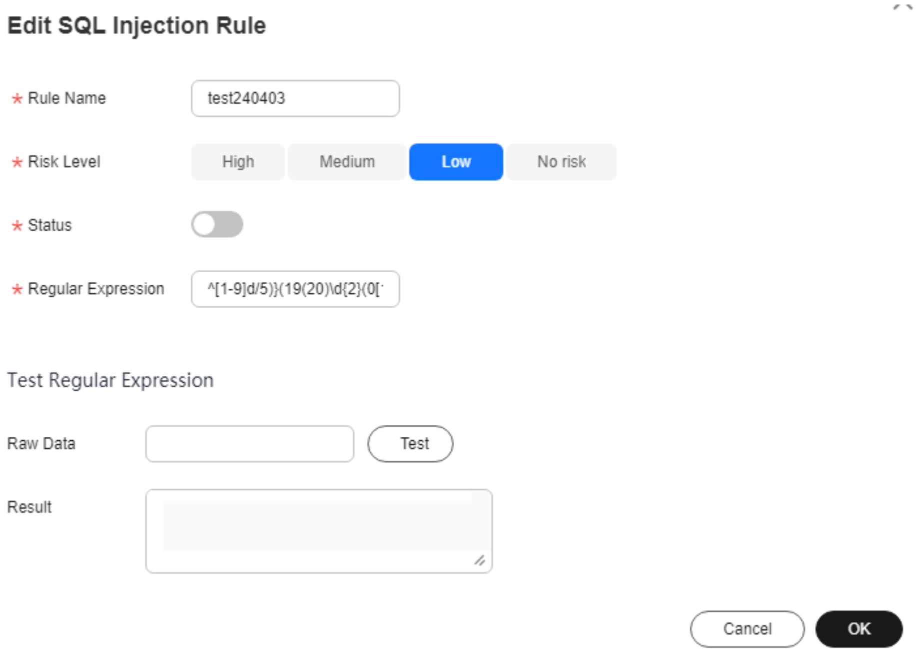
**Step 5** Click the **SQL Injection** tab.

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 6-3**.

**Figure 6-5** Editing an SQL injection rule



Edit SQL Injection Rule

* Rule Name: test240403

* Risk Level: High | Medium | [✓ Low] | No risk

* Status: ○

* Regular Expression: ^[1-9]d/5)}(19(20)\d{2}(0[

Test Regular Expression

Raw Data:

Result:

**Table 6-3** SQL injection rule parameters

| Parameter | Description | Example Value |
|---|---|---|
| Name | Name of an SQL rule. | Postal Code SQL injection Rule |
| Risk Level | Level of risks matching a SQL rule. Its value can be:<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}$ |

| Parameter | Description | Example Value |
|---|---|---|
| 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** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

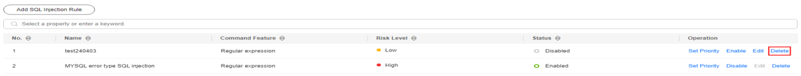
**Step 5** Click the **SQL Injection** tab.

**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 6-6** Deleting SQL injection



| No. | Name | Command Feature | Risk Level | Status | Operation |
|---|---|---|---|---|---|
| 1 | test240403 | Regular expression | Low | Disabled | Set Priority Enable Edit Delete |
| 2 | MYSQL error type SQL injection | Regular expression | High | Enabled | Set Priority Disable Edit Delete |

**----End**

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

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

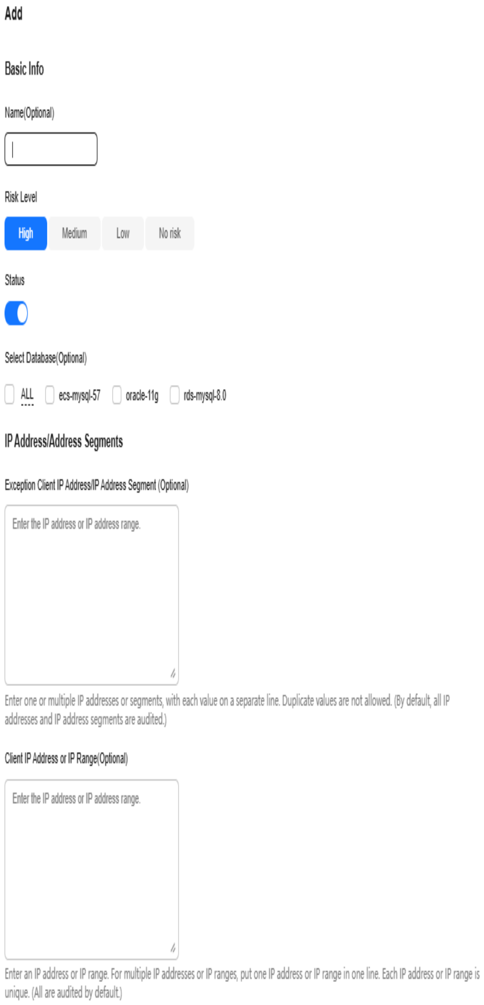
**Step 4** In the **Instance** drop-down list, select an instance to add risky operations.

**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 6-4**.

**Figure 6-7** Configuring basic information and IP addresses or IP address segments



Add

Basic Info

Name(Optional)

Risk Level

High | Medium | Low | No risk

Status

Select Database(Optional)

□ ALL □ ecs-mysql-57 □ oracle-11g □ rds-mysql-8.0

IP Address/Address Segments

Exception Client IP Address/IP Address Segment (Optional)

Enter the IP address or IP address range.

Enter one or multiple IP addresses or segments, with each value on a separate line. Duplicate values are not allowed. (By default, all IP addresses and IP address segments are audited.)

Client IP Address or IP Range(Optional)

Enter the IP address or IP address range.

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

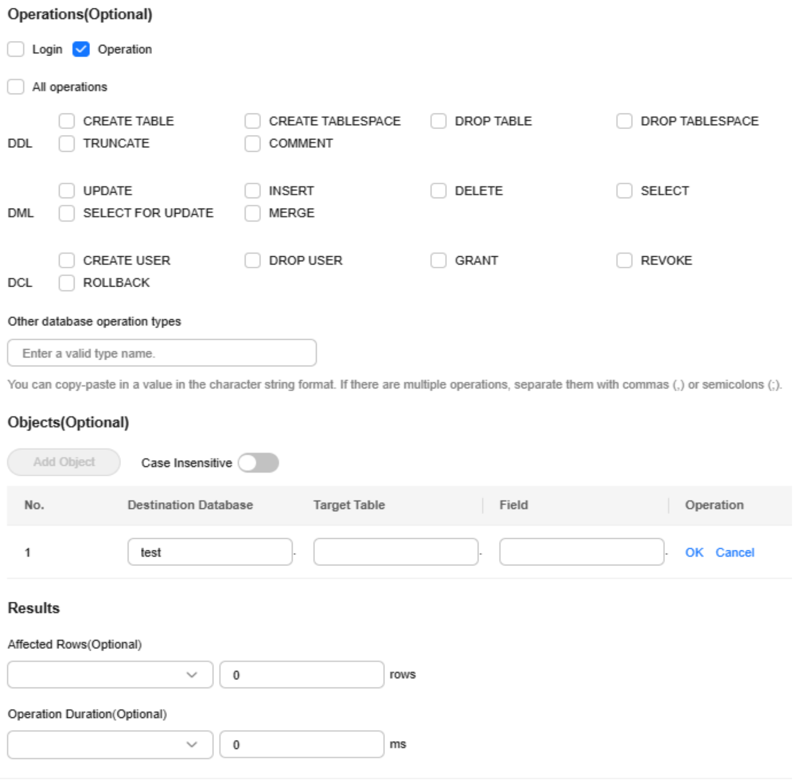
**Table 6-4** Parameters

| 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 |
| Status | Status of a risky operation<br>- ●: enabled<br>- ○: disabled | ● |

| Parameter | Description | Example Value |
|---|---|---|
| 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 6-5**.

**Figure 6-8** Setting the operation type, operation object, and execution result



Operations(Optional)

☐ Login ☑ Operation

☐ All operations

DDL ☐ CREATE TABLE ☐ CREATE TABLESPACE ☐ DROP TABLE ☐ DROP TABLESPACE ☐ TRUNCATE ☐ COMMENT

DML ☐ UPDATE ☐ INSERT ☐ DELETE ☐ SELECT ☐ SELECT FOR UPDATE ☐ MERGE

DCL ☐ CREATE USER ☐ DROP USER ☐ GRANT ☐ REVOKE ☐ ROLLBACK

Other database operation types

Enter a valid type name.

You can copy-paste in a value in the character string format. If there are multiple operations, separate them with commas (,) or semicolons (;).

Objects(Optional)

Add Object  Case Insensitive

| No. | Destination Database | Target Table | Field | Operation |
|---|---|---|---|---|
| 1 | test | | | OK Cancel |

Results

Affected Rows(Optional)

0 rows

Operation Duration(Optional)

0 ms

**Table 6-5** 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**

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

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

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

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

NOTE

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

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

- **Store Result Set**

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

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

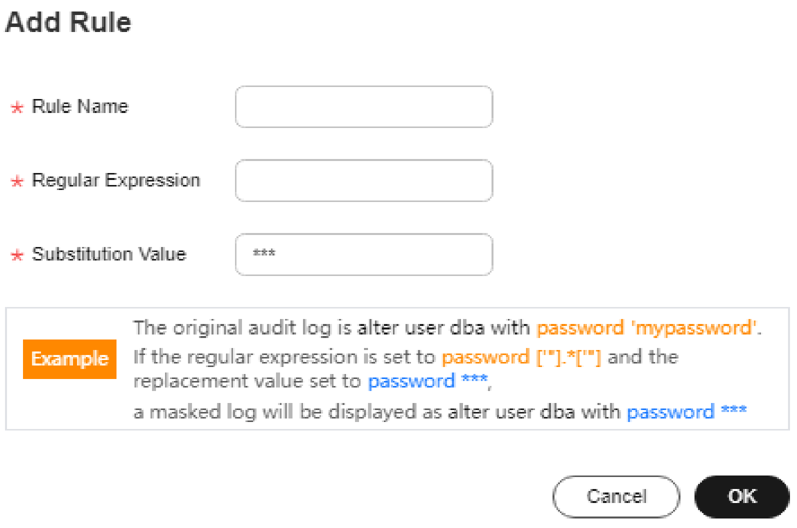
  **Note**: The result set storage supports only the database audit in agent mode.

- **Mask Privacy Data**

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

**Step 7** Click **Add Rule**. In the displayed **Add Rule** dialog box, set the data masking rule, as shown in **Figure 6-9**. For details about related parameters, see **Table 6-6**.

**Figure 6-9** Adding a user-defined rule



Add Rule

* Rule Name

* Regular Expression

* Substitution Value ***

Example

The original audit log is alter user dba with password 'mypassword'.
If the regular expression is set to password ['"].*['"] and the replacement value set to password ***,
a masked log will be displayed as alter user dba with password ***

**Table 6-6** 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.

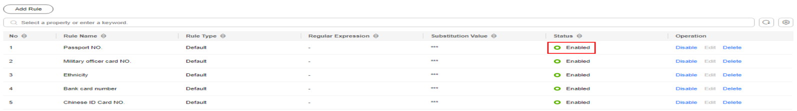
**----End**

## 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 6-10**.

**Figure 6-10** Enabled rule



Add Rule

Select a property or enter a keyword.

| No | Rule Name | Rule Type | Regular Expression | Substitution Value | Status | Operation |
|---|---|---|---|---|---|---|
| 1 | Passport NO. | Default | - | *** | Enabled | Disable Edit Delete |
| 2 | Military officer card NO. | Default | - | *** | Enabled | Disable Edit Delete |
| 3 | Ethnicity | Default | - | *** | Enabled | Disable Edit Delete |
| 4 | Bank card number | Default | - | *** | Enabled | Disable Edit Delete |
| 5 | Chinese ID Card NO. | Default | - | *** | Enabled | Disable Edit Delete |

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

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

**select * from db where HOST=**"*Passport NO.*";

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

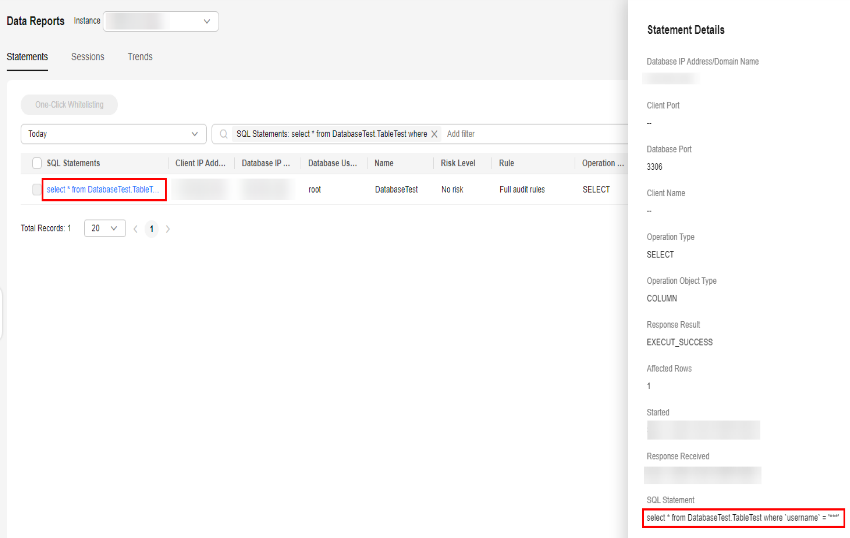
**Step 5** In the navigation tree on the left, choose **Data Reports**. The **Data Reports** page is displayed.

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

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

**Step 8** Click the SQL statement. On the **Statement Details** page, view the SQL statement information. The privacy data masking function is normal, and the masked information is displayed in **SQL Statement**.

**Figure 6-11** Masking privacy data



Data Reports Instance [redacted]

Statements Sessions Trends

One-Click Whitelisting

Today

SQL Statements: select * from DatabaseTest.TableTest where ✕ Add filter

| SQL Statements | Client IP Add... | Database IP ... | Database Us... | Name | Risk Level | Rule | Operation ... |
|---|---|---|---|---|---|---|---|
| select * from DatabaseTest.TableT... | [redacted] | [redacted] | root | DatabaseTest | No risk | Full audit rules | SELECT |

Total Records: 1 20 ‹ 1 ›

Statement Details

Database IP Address/Domain Name
[redacted]

Client Port
--

Database Port
3306

Client Name
--

Operation Type
SELECT

Operation Object Type
COLUMN

Response Result
EXECUT_SUCCESS

Affected Rows
1

Started
[redacted]

Response Received
[redacted]

SQL Statement
select * from DatabaseTest.TableTest where `username` = '***'

**----End**

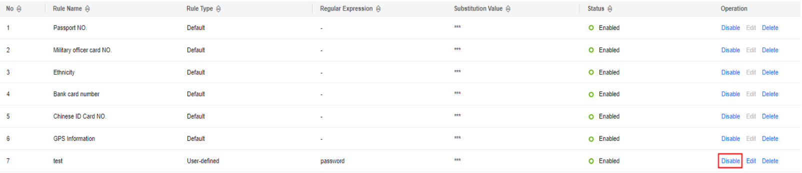
## Common Operations

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 6-12** Disabling a custom masking rule

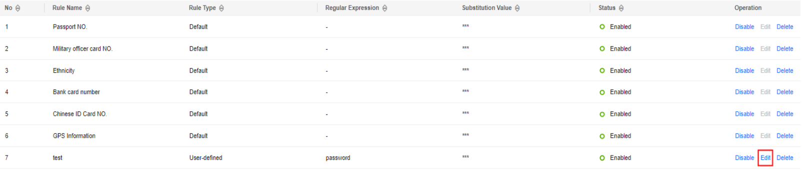
  

  | No | Rule Name | Rule Type | Regular Expression | Substitution Value | Status | Operation |
  |---|---|---|---|---|---|---|
  | 1 | Passport NO. | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 2 | Military officer card NO. | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 3 | Ethnicity | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 4 | Bank card number | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 5 | Chinese ID Card NO. | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 6 | GPS Information | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 7 | test | User-defined | password | *** | ○ Enabled | Disable Edit Delete |

- 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 6-13** Editing a custom masking rule

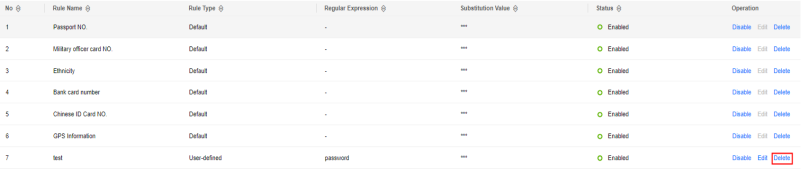
  

  | No | Rule Name | Rule Type | Regular Expression | Substitution Value | Status | Operation |
  |---|---|---|---|---|---|---|
  | 1 | Passport NO. | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 2 | Military officer card NO. | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 3 | Ethnicity | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 4 | Bank card number | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 5 | Chinese ID Card NO. | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 6 | GPS Information | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 7 | test | User-defined | password | *** | ○ Enabled | Disable Edit Delete |

- 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 6-14** Deleting a custom masking rule

  | No | Rule Name | Rule Type | Regular Expression | Substitution Value | Status | Operation |
  |---|---|---|---|---|---|---|
  | 1 | Passport NO. | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 2 | Military officer card NO. | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 3 | Ethnicity | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 4 | Bank card number | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 5 | Chinese ID Card NO. | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 6 | GPS Information | Default | - | *** | ○ Enabled | Disable Edit Delete |
  | 7 | test | User-defined | password | *** | ○ Enabled | Disable Edit Delete |

# 6.6 SQL Whitelist

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

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

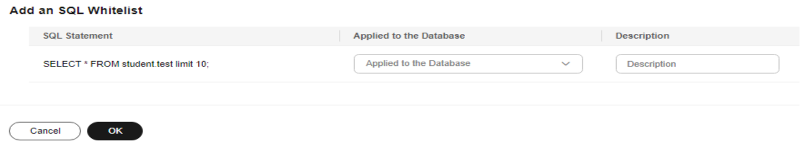
**Step 4** In the **Instance** drop-down list, select the instance whose session information you want to view.

**Step 5** Click the **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 6-15** Adding an SQL whitelist

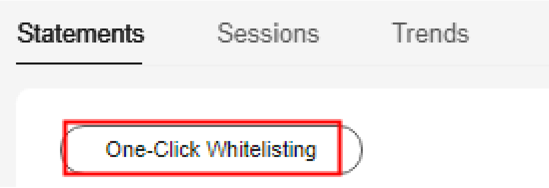


| SQL Statement | Applied to the Database | Description |
|---|---|---|
| SELECT * FROM student.test limit 10; | Applied to the Database | Description |

  c. Click **OK**.

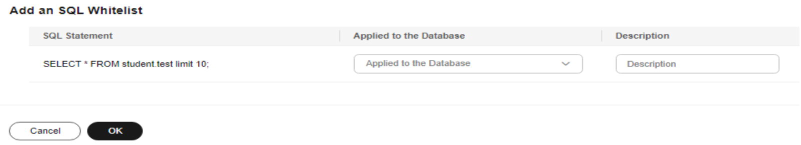
- Add SQL statements in batches.
  a. Select the target SQL statement and click **One-Clink Whitelisting**.

**Figure 6-16** One-click whitelisting



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

**Figure 6-17** Adding an SQL whitelist



| SQL Statement | Applied to the Database | Description |
|---|---|---|
| SELECT * FROM student.test limit 10; | Applied to the Database | Description |

c. Click **OK**.

**----End**

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

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

# 7 Viewing Audit Results

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

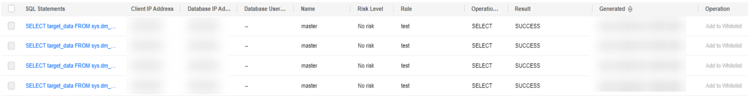
**Step 3** In the navigation tree on the left, choose **Data Reports**. The **Data Reports** page is displayed.

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

**Step 5** Click the **Statements** tab.

**Step 6** View SQL statement information.

**Figure 7-1** Querying SQL statements



| □ | SQL Statements | Client IP Address | Database IP Ad... | Database User... | Name | Risk Level | Rule | Operatio... | Result | Generated | Operation |
|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | SELECT target_data FROM sys.dm_... | [redacted] | [redacted] | -- | master | No risk | test | SELECT | SUCCESS | [redacted] | Add to Whitelist |
| □ | SELECT target_data FROM sys.dm_... | [redacted] | [redacted] | -- | master | No risk | test | SELECT | SUCCESS | [redacted] | Add to Whitelist |
| □ | SELECT target_data FROM sys.dm_... | [redacted] | [redacted] | -- | master | No risk | test | SELECT | SUCCESS | [redacted] | Add to Whitelist |
| □ | SELECT target_data FROM sys.dm_... | [redacted] | [redacted] | -- | master | No risk | test | SELECT | SUCCESS | [redacted] | Add to Whitelist |

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** ), or customize the start time and end time. 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.

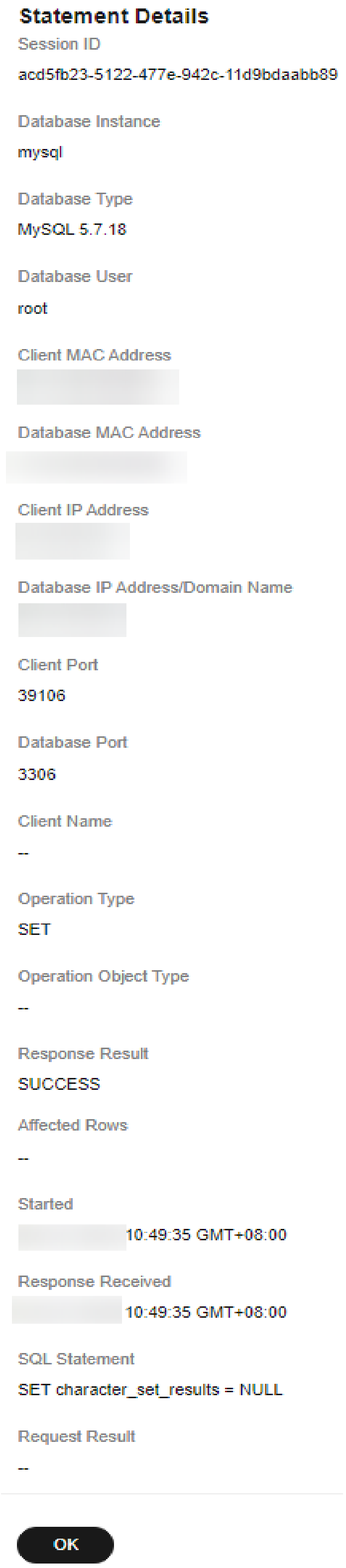
**Step 7** Click the SQL statement.

**Step 8** View the SQL statement information in the **StatementDetails** dialog box. For details about related parameters, see **Table 7-1**.

NOTICE

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

**Figure 7-2 Statement** dialog box



**Statement Details**

Session ID
acd5fb23-5122-477e-942c-11d9bdaabb89

Database Instance
mysql

Database Type
MySQL 5.7.18

Database User
root

Client MAC Address
[redacted]

Database MAC Address
[redacted]

Client IP Address
[redacted]

Database IP Address/Domain Name
[redacted]

Client Port
39106

Database Port
3306

Client Name
--

Operation Type
SET

Operation Object Type
--

Response Result
SUCCESS

Affected Rows
--

Started
[redacted] 10:49:35 GMT+08:00

Response Received
[redacted] 10:49:35 GMT+08:00

SQL Statement
SET character_set_results = NULL

Request Result
--

**Table 7-1** 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?**

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

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

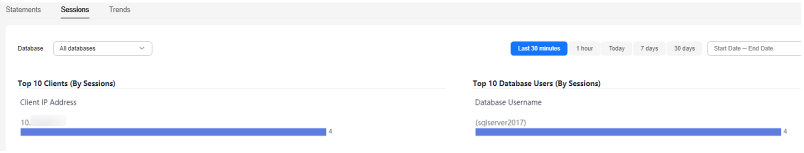
**Step 4** In the **Instance** drop-down list, select the instance whose session information you want to view.

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

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

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

**Figure 7-3** Viewing session distribution



Database: All databases

**----End**

# 7.3 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.**

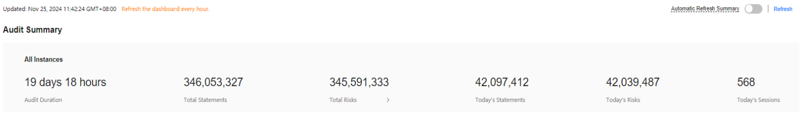
**Step 2** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

**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 7-4** Viewing audit summary

  Updated: Nov 25, 2024 11:42:24 GMT+08:00 Refresh the dashboard every hour.

  Automatic Refresh Summary | Refresh

  Audit Summary

  All Instances

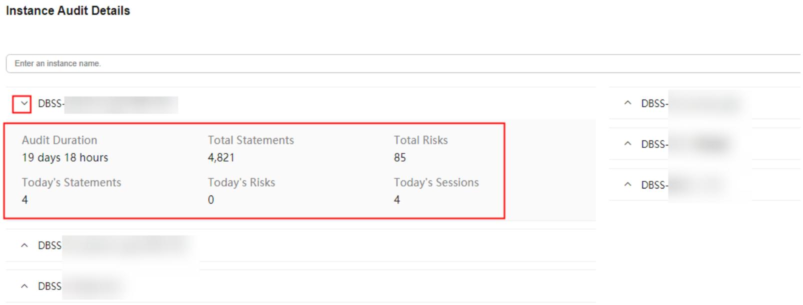
  | 19 days 18 hours | 346,053,327 | 345,591,333 | 42,097,412 | 42,039,487 | 568 |
  |---|---|---|---|---|---|
  | Audit Duration | Total Statements | Total Risks > | Today's Statements | Today's Risks | Today's Sessions |

  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 7-5** Viewing single instance information

  Instance Audit Details

  Enter an instance name.

  ⌄ DBSS-[redacted]

  | Audit Duration | Total Statements | Total Risks |
  |---|---|---|
  | 19 days 18 hours | 4,821 | 85 |
  | **Today's Statements** | **Today's Risks** | **Today's Sessions** |
  | 4 | 0 | 4 |

  ^ DBSS[redacted]

  ^ DBSS[redacted]

  ^ DBSS-[redacted]

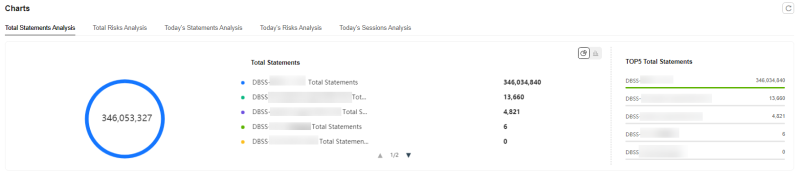
  ^ DBSS-[redacted]

  ^ DBSS-[redacted]

- 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 7-6** Viewing the data analysis chart

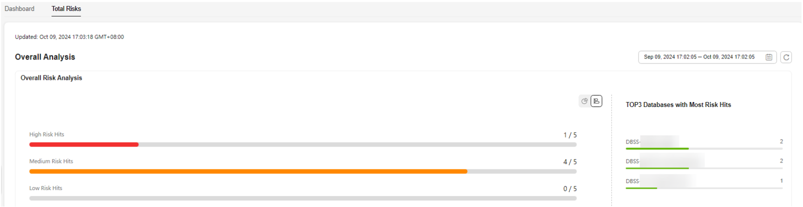


**Step 4** Click **Total Risks**. The **Total Risks** page is displayed. Click 📅 and select a time range to view the risk analysis of all database audit instances in the specified time range.

- 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.

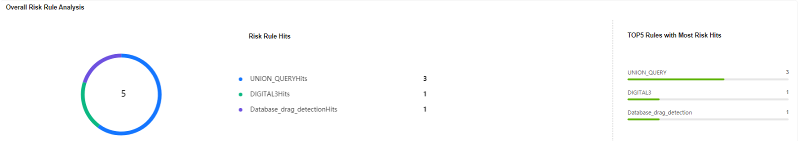
  **Figure 7-7** Overall risk analysis

- Overall risk rule analysis

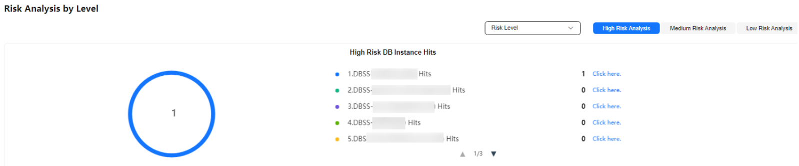
  Displays the number of risk rule hits of all databases and top 5 risk rule hits.

  **Figure 7-8** Overall risk rule analysis

  
  Overall Risk Rule Analysis
Risk Rule Hits
5
UNION_QUERYHits 3
DIGITAL3Hits 1
Database_drag_detectionHits 1
TOP5 Rules with Most Risk Hits
UNION_QUERY 3
DIGITAL3 1
Database_drag_detection 1

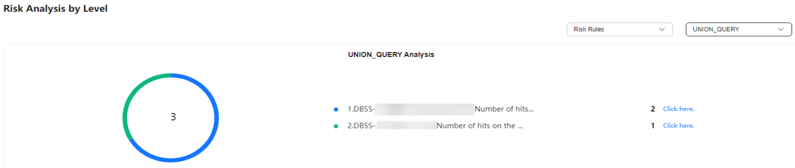
- Risk analysis by level
  - Risk level: displays the high-risk hit analysis, medium-risk hit analysis, and low-risk hit analysis of each database.

    **Figure 7-9** Risk level analysis

    
    Risk Analysis by Level
Risk Level
High Risk Analysis
Medium Risk Analysis
Low Risk Analysis
High Risk DB Instance Hits
1
1.DBSS- Hits 1 Click here.
2.DBSS- Hits 0 Click here.
3.DBSS- Hits 0 Click here.
4.DBSS- Hits 0 Click here.
5.DBS Hits 0 Click here.
1/3

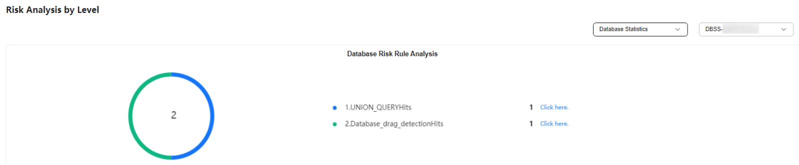
  - Risk rule: displays the analysis when a database is hit by a risk rule.

    **Figure 7-10** Risk rule analysis

    
    Risk Analysis by Level
Risk Rules
UNION_QUERY
UNION_QUERY Analysis
3
1.DBSS- Number of hits... 2 Click here.
2.DBSS- Number of hits on the ... 1 Click here.

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

**Figure 7-11** Database statistics analysis



Risk Analysis by Level

Database Statistics

DBSS-[redacted]

Database Risk Rule Analysis

| | | |
|---|---|---|
| 1.UNION_QUERYHits | 1 | Click here. |
| 2.Database_drag_detectionHits | 1 | Click here. |

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

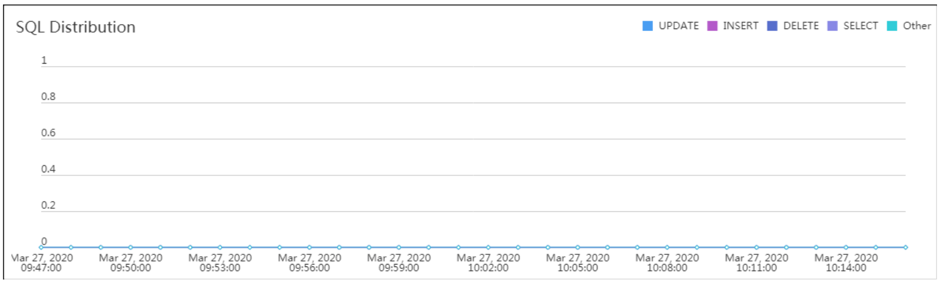
**Step 6** Click the **Trends** tab. The trend analysis page is displayed.

**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 7-12** 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**.

# 7.4 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 7-2** lists the report names. You can **generate reports** and **set report tasks** as needed.

**Table 7-2** 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** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

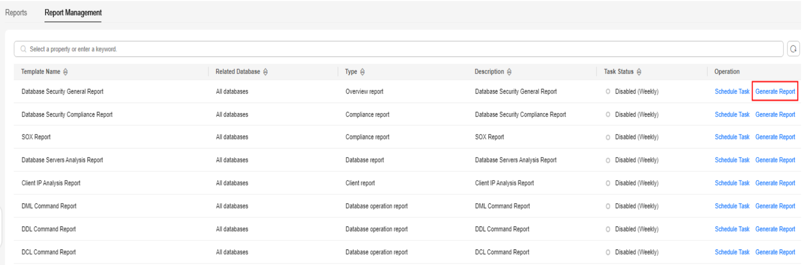
**Step 3** In the navigation tree on the left, choose **Reports**.

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

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

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

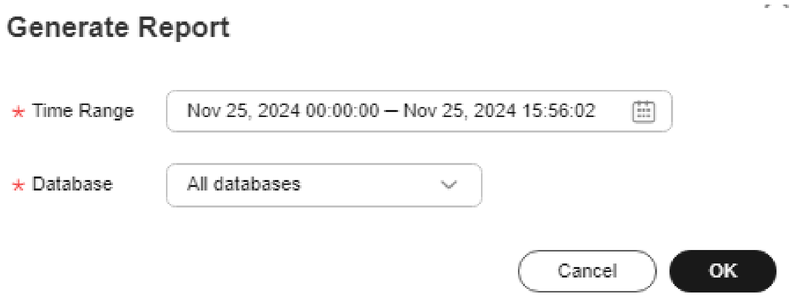
**Figure 7-13** Report template list



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

**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 7-14** Generate Report



Generate Report

* Time Range: Nov 25, 2024 00:00:00 – Nov 25, 2024 15:56:02

* Database: All databases

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

**----End**

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

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

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

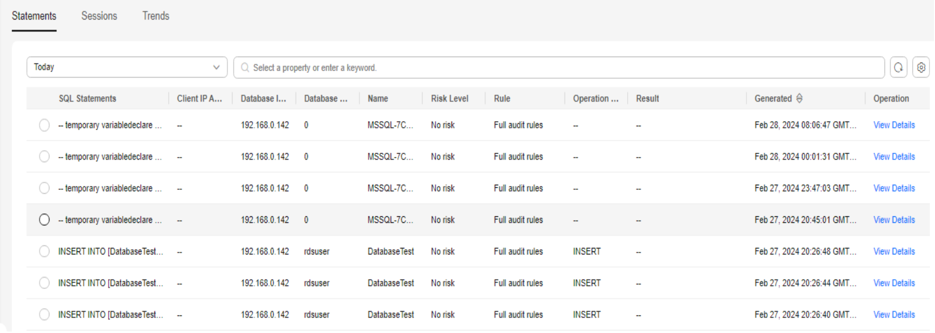
**Step 3** In the navigation tree on the left, choose **Reports**.

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

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

**Step 6** Locate the target template and click **Schedule Task** in the **Operation** column, as shown in **Figure 7-15**.

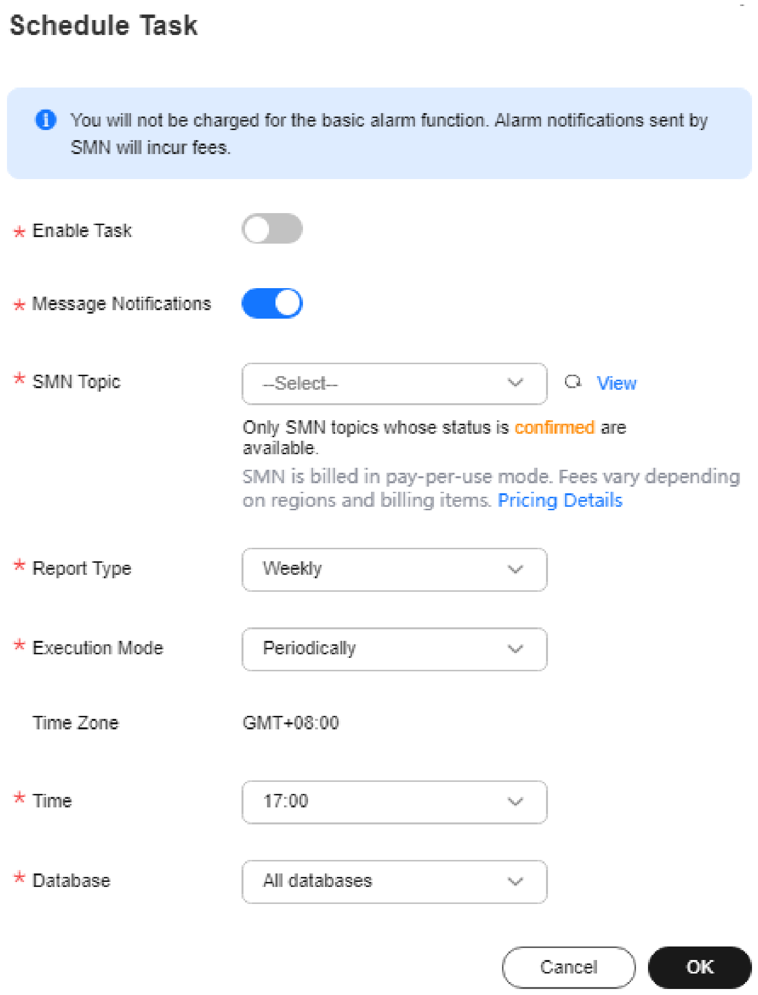
**Figure 7-15** Setting a task



| | SQL Statements | Client IP A... | Database I... | Database ... | Name | Risk Level | Rule | Operation ... | Result | Generated | Operation |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ○ | -- temporary variabledeclare ... | -- | 192.168.0.142 | 0 | MSSQL-7C... | No risk | Full audit rules | -- | -- | Feb 28, 2024 08:06:47 GMT... | View Details |
| ○ | -- temporary variabledeclare ... | -- | 192.168.0.142 | 0 | MSSQL-7C... | No risk | Full audit rules | -- | -- | Feb 28, 2024 00:01:31 GMT... | View Details |
| ○ | -- temporary variabledeclare ... | -- | 192.168.0.142 | 0 | MSSQL-7C... | No risk | Full audit rules | -- | -- | Feb 27, 2024 23:47:03 GMT... | View Details |
| ○ | -- temporary variabledeclare ... | -- | 192.168.0.142 | 0 | MSSQL-7C... | No risk | Full audit rules | -- | -- | Feb 27, 2024 20:45:01 GMT... | View Details |
| ○ | INSERT INTO [DatabaseTest... | -- | 192.168.0.142 | rdsuser | DatabaseTest | No risk | Full audit rules | INSERT | -- | Feb 27, 2024 20:26:48 GMT... | View Details |
| ○ | INSERT INTO [DatabaseTest... | -- | 192.168.0.142 | rdsuser | DatabaseTest | No risk | Full audit rules | INSERT | -- | Feb 27, 2024 20:26:44 GMT... | View Details |
| ○ | INSERT INTO [DatabaseTest... | -- | 192.168.0.142 | rdsuser | DatabaseTest | No risk | Full audit rules | INSERT | -- | Feb 27, 2024 20:26:40 GMT... | View Details |

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

**Figure 7-16** Setting a scheduled task



Schedule Task

You will not be charged for the basic alarm function. Alarm notifications sent by SMN will incur fees.

* Enable Task: ○

* Message Notifications: ◉

* SMN Topic: --Select-- View

Only SMN topics whose status is confirmed are available.

SMN is billed in pay-per-use mode. Fees vary depending on regions and billing items. Pricing Details

* Report Type: Weekly

* Execution Mode: Periodically

Time Zone: GMT+08:00

* Time: 17:00

* Database: All databases

**Table 7-3** 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 Zone | Displays the time zone. | - |
| Time | Time when the report is executed | 10:00 |
| Database | Database for which you want to execute the report task | - |

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

**----End**

## Step 2: Previewing and Downloading Audit Reports

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

NOTICE

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

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

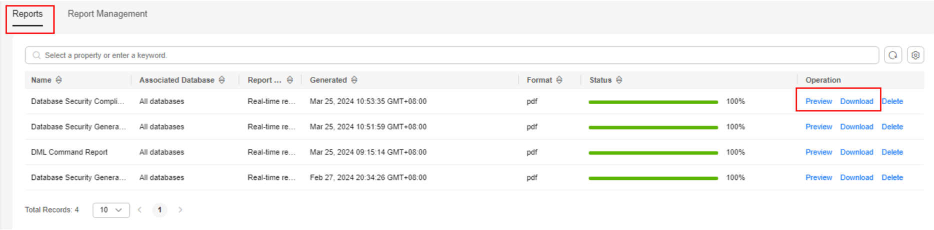
**Step 2** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

**Step 5** Locate the target template, and click **Preview** or **Download** in the **Operation** column to preview or download the report. See **Figure 7-17**..

**Figure 7-17** Previewing or downloading an audit report



| Name | Associated Database | Report ... | Generated | Format | Status | Operation |
|---|---|---|---|---|---|---|
| Database Security Compli... | All databases | Real-time re... | Mar 25, 2024 10:53:35 GMT+08:00 | pdf | 100% | Preview Download Delete |
| Database Security Genera... | All databases | Real-time re... | Mar 25, 2024 10:51:59 GMT+08:00 | pdf | 100% | Preview Download Delete |
| DML Command Report | All databases | Real-time re... | Mar 25, 2024 09:15:14 GMT+08:00 | pdf | 100% | Preview Download Delete |
| Database Security Genera... | All databases | Real-time re... | Feb 27, 2024 20:34:26 GMT+08:00 | pdf | 100% | Preview Download Delete |

Total Records: 4 10 < 1 >

**----End**

## Helpful Links

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

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

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

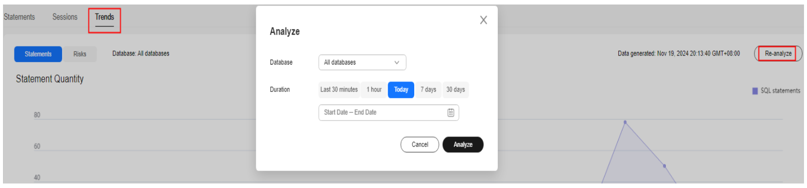
**Step 4** Click the **Trends** tab. The trend analysis page is displayed.

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

**Step 6** View the overall trend of the database.

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

**Figure 7-18** Re-analyze



Database: All databases

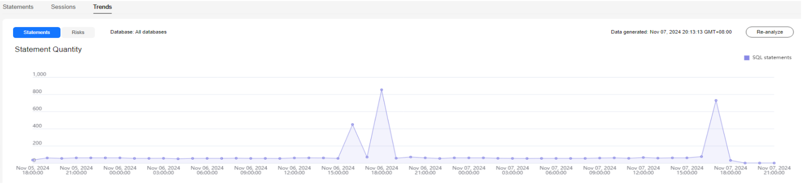
Data generated: Nov 19, 2024 20:13:40 GMT+08:00

Database: All databases

Duration: Today

- 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 7-19** Statement quantity



Database: All databases

Data generated: Nov 07, 2024 20:13:13 GMT+08:00

**Figure 7-20** Session statistics

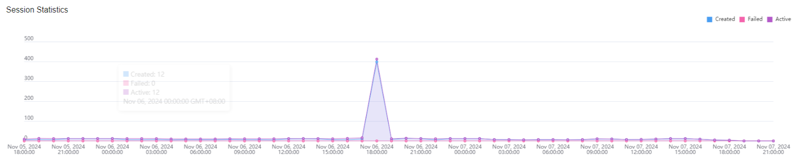


**Figure 7-21** SQL distribution

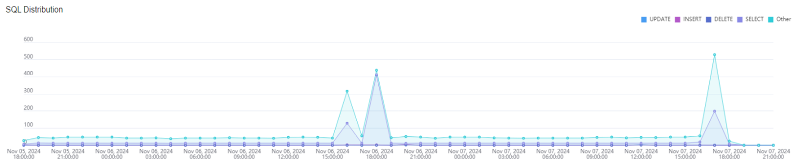
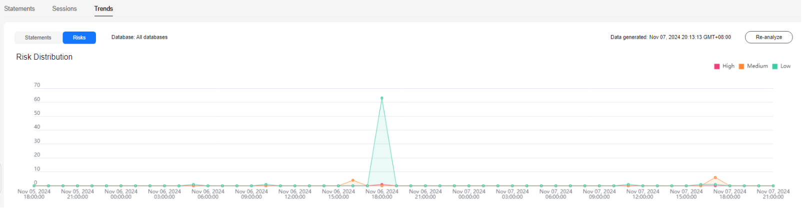


**Figure 7-22** Risk distribution



Database: All databases

Data generated: Nov 07, 2024 20:13:13 GMT+08:00

**Figure 7-23** SQL injections

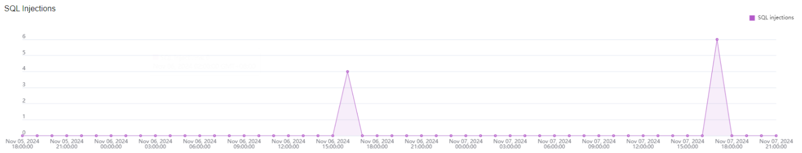
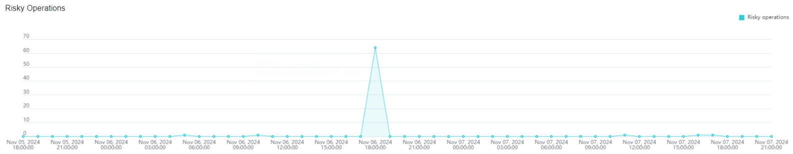


**Figure 7-24** Risky operations



**----End**

# 8 Notification Settings Management

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

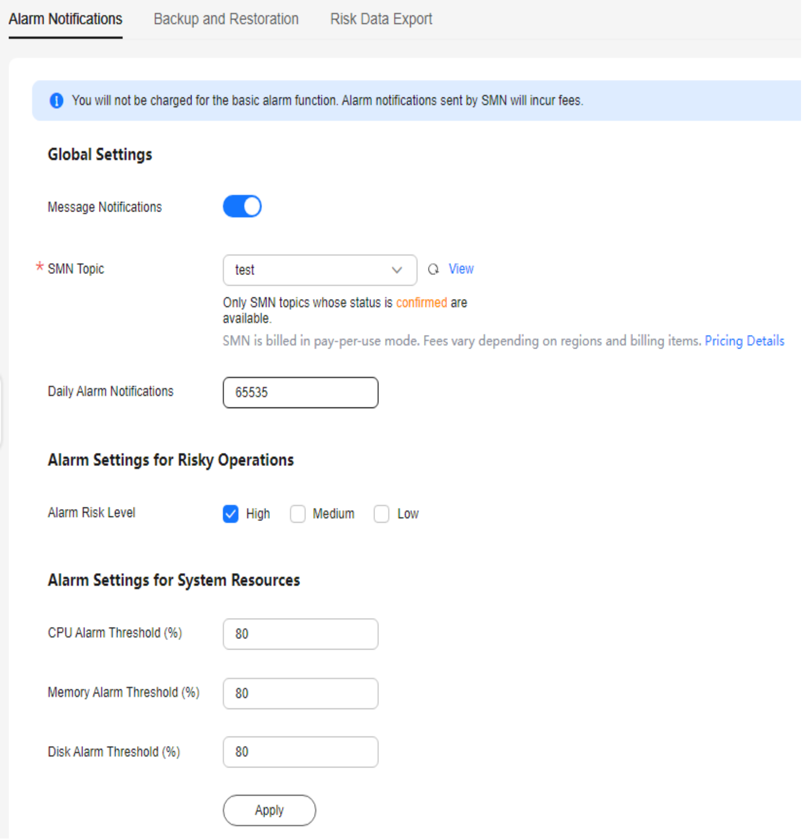
**Step 3** In the navigation tree on the left, choose **Settings**.

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

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

**Step 6** Set alarm notifications. For details about related parameters, see **Table 8-1**.

**Figure 8-1** Configuring alarm notifications



You will not be charged for the basic alarm function. Alarm notifications sent by SMN will incur fees.

Global Settings

Message Notifications: enabled

* SMN Topic: test

View

Only SMN topics whose status is confirmed are available.

SMN is billed in pay-per-use mode. Fees vary depending on regions and billing items. Pricing Details

Daily Alarm Notifications: 65535

Alarm Settings for Risky Operations

Alarm Risk Level: ☑ High □ Medium □ Low

Alarm Settings for System Resources

CPU Alarm Threshold (%): 80

Memory Alarm Threshold (%): 80

Disk Alarm Threshold (%): 80

**Table 8-1** 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**

# 9 Viewing Monitoring Information

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

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

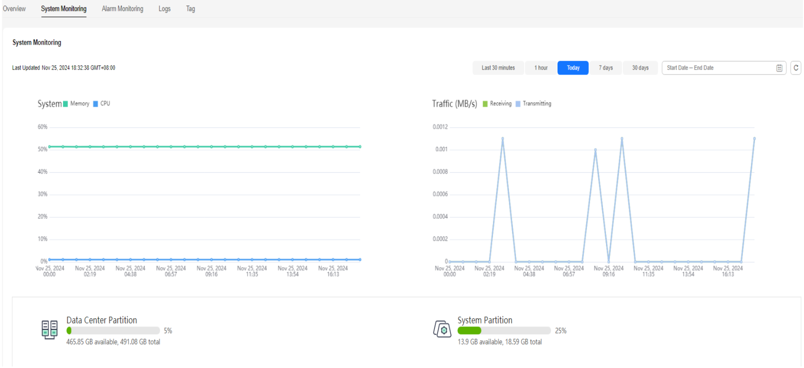
**Step 4** Click the name of the instance for which you want to view the system monitoring. The **Overview** page is displayed.

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

**Step 6** View the system monitoring information.

Select **Last 30 minutes**, **1 hour**, **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 9-1** Viewing the system monitoring



Last Updated Nov 25, 2024 18:32:38 GMT+08:00

Data Center Partition 5%
465.85 GB available, 491.08 GB total

System Partition 25%
13.9 GB available, 18.59 GB total

**----End**

# 9.2 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.**

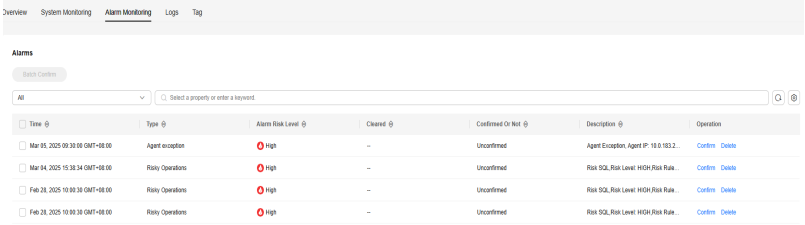
**Step 2** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

**Step 5** View the alarm information, as shown in **Figure 9-2**. For details about related parameters, see **Table 9-1**.

**Figure 9-2** Viewing alarms



| Time | Type | Alarm Risk Level | Cleared | Confirmed Or Not | Description | Operation |
|---|---|---|---|---|---|---|
| Mar 05, 2025 09:30:00 GMT+08:00 | Agent exception | High | -- | Unconfirmed | Agent Exception, Agent IP: 10.0.183.2... | Confirm Delete |
| Mar 04, 2025 15:38:34 GMT+08:00 | Risky Operations | High | -- | Unconfirmed | Risk SQL,Risk Level: HIGH,Risk Rule... | Confirm Delete |
| Feb 28, 2025 10:00:30 GMT+08:00 | Risky Operations | High | -- | Unconfirmed | Risk SQL,Risk Level: HIGH,Risk Rule... | Confirm Delete |
| Feb 28, 2025 10:00:30 GMT+08:00 | Risky Operations | High | -- | Unconfirmed | Risk SQL,Risk Level: HIGH,Risk Rule... | Confirm Delete |

**Table 9-1** 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:

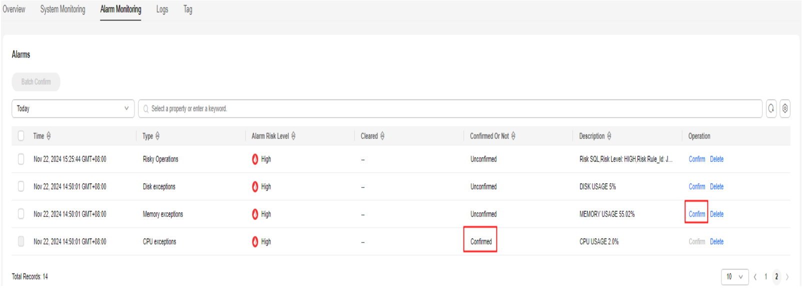
- Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days** from the drop-down list, and click 🔍 to view alarms of the specified time range.
- Select **All**, **High**, **Moderate**, or **Low** for **Risk Severity**. Alarms of specified severity are displayed in the list.
- Select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

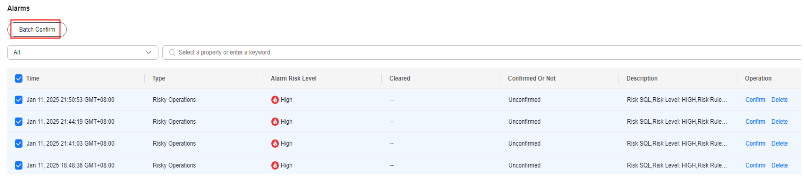
  **Figure 9-3** Confirming an alarm

  | □ | Time | Type | Alarm Risk Level | Cleared | Confirmed Or Not | Description | Operation |
  |---|---|---|---|---|---|---|---|
  | □ | Nov 22, 2024 15:25:44 GMT+08:00 | Risky Operations | High | -- | Unconfirmed | Risk SQL,Risk Level: HIGH,Risk Rule_Id: J... | Confirm Delete |
  | □ | Nov 22, 2024 14:50:01 GMT+08:00 | Disk exceptions | High | -- | Unconfirmed | DISK USAGE 5% | Confirm Delete |
  | □ | Nov 22, 2024 14:50:01 GMT+08:00 | Memory exceptions | High | -- | Unconfirmed | MEMORY USAGE 55.02% | Confirm Delete |
  | □ | Nov 22, 2024 14:50:01 GMT+08:00 | CPU exceptions | High | -- | Confirmed | CPU USAGE 2.0% | Confirm Delete |

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

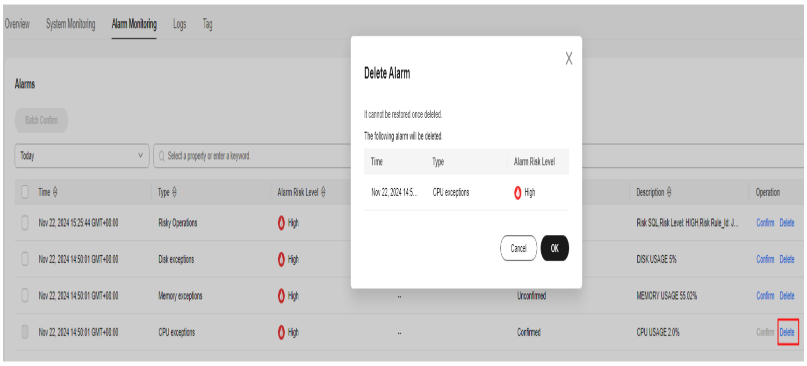
  **Figure 9-4** Confirming alarms in batches

  | ☑ | Time | Type | Alarm Risk Level | Cleared | Confirmed Or Not | Description | Operation |
  |---|---|---|---|---|---|---|---|
  | ☑ | Jan 11, 2025 21:50:53 GMT+08:00 | Risky Operations | High | -- | Unconfirmed | Risk SQL,Risk Level: HIGH,Risk Rule... | Confirm Delete |
  | ☑ | Jan 11, 2025 21:44:19 GMT+08:00 | Risky Operations | High | -- | Unconfirmed | Risk SQL,Risk Level: HIGH,Risk Rule... | Confirm Delete |
  | ☑ | Jan 11, 2025 21:41:03 GMT+08:00 | Risky Operations | High | -- | Unconfirmed | Risk SQL,Risk Level: HIGH,Risk Rule... | Confirm Delete |
  | ☑ | Jan 11, 2025 18:48:36 GMT+08:00 | Risky Operations | High | -- | Unconfirmed | Risk SQL,Risk Level: HIGH,Risk Rule... | Confirm Delete |

- 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 9-5** Deleting an alarm

  Delete Alarm

  It cannot be restored once deleted.

  The following alarm will be deleted.

  | Time | Type | Alarm Risk Level |
  |---|---|---|
  | Nov 22, 2024 14:5... | CPU exceptions | High |

  | □ | Time | Type | Alarm Risk Level | | | Description | Operation |
  |---|---|---|---|---|---|---|---|
  | □ | Nov 22, 2024 15:25:44 GMT+08:00 | Risky Operations | High | | | Risk SQL,Risk Level: HIGH,Risk Rule_Id: J... | Confirm Delete |
  | □ | Nov 22, 2024 14:50:01 GMT+08:00 | Disk exceptions | High | | | DISK USAGE 5% | Confirm Delete |
  | □ | Nov 22, 2024 14:50:01 GMT+08:00 | Memory exceptions | High | -- | Unconfirmed | MEMORY USAGE 55.02% | Confirm Delete |
  | □ | Nov 22, 2024 14:50:01 GMT+08:00 | CPU exceptions | High | -- | Confirmed | CPU USAGE 2.0% | Confirm Delete |

- 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**.

# 10 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**.

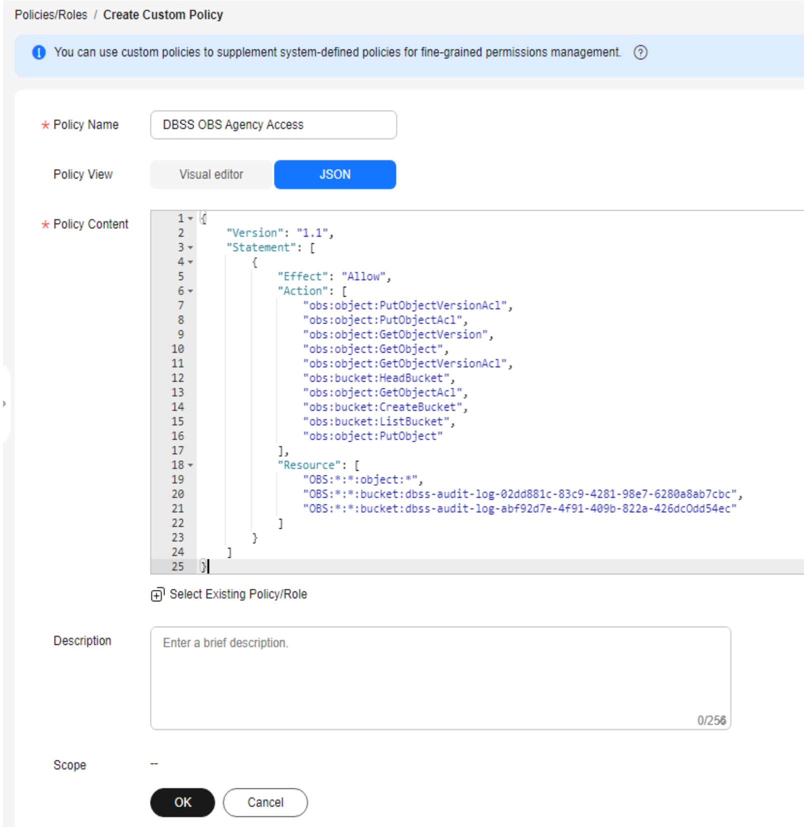
**Step 3** In the navigation pane, choose **Permissions** > **Authorization**. Click **Create Custom Policy**.

**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 10-1**. Click **OK**.

**Figure 10-1** Creating a custom policy



Policies/Roles / Create Custom Policy
You can use custom policies to supplement system-defined policies for fine-grained permissions management.

* Policy Name: DBSS OBS Agency Access

Policy View
Visual editor
JSON

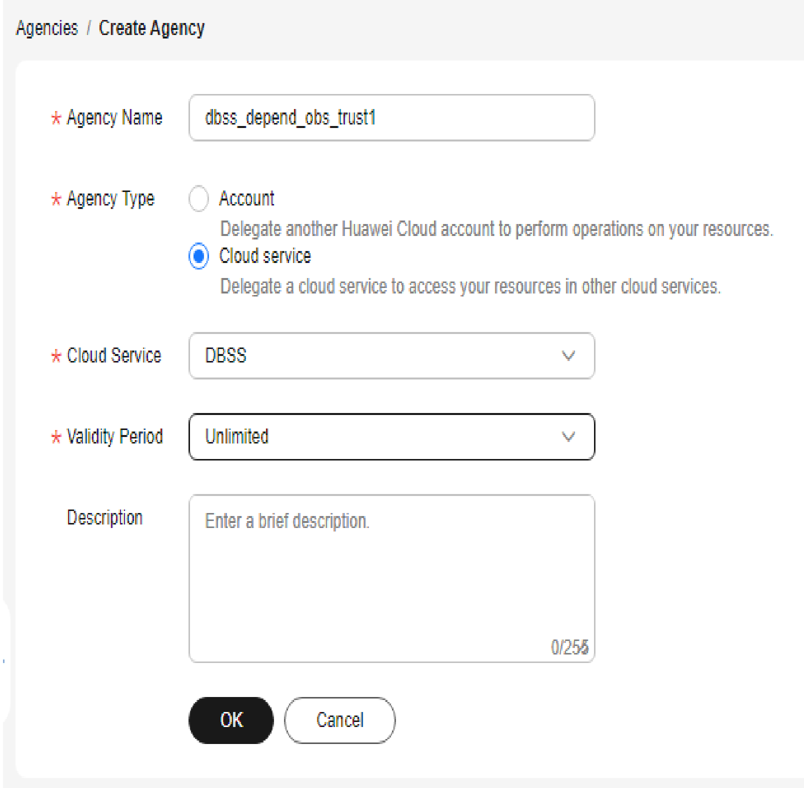
* Policy Content

```
{
    "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:dbss-audit-log-02dd881c-83c9-4281-98e7-6280a8ab7cbc",
                "OBS:*:*:bucket:dbss-audit-log-abf92d7e-4f91-409b-822a-426dc0dd54ec"
            ]
        }
    ]
}
```

**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 10-2**.

**Figure 10-2** Creating an agency



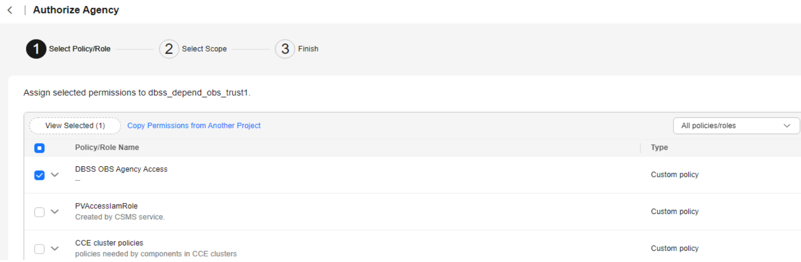
Agencies / Create Agency

* Agency Name: dbss_depend_obs_trust1
* Agency Type:
  ○ Account
  Delegate another Huawei Cloud account to perform operations on your resources.
  ● Cloud service
  Delegate a cloud service to access your resources in other cloud services.
* Cloud Service: DBSS
* Validity Period: Unlimited

Description: Enter a brief description. 0/255

**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 10-3**. Click **Next** in the lower right corner.

**Figure 10-3** Selecting a policy



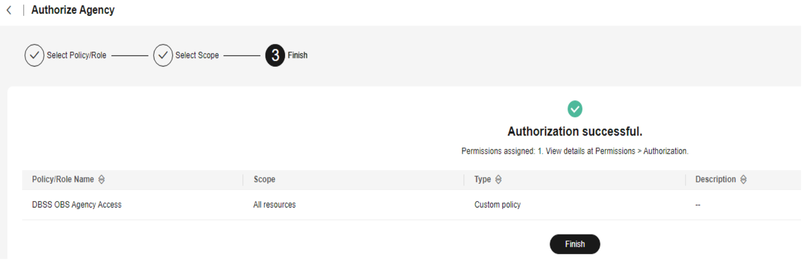
< | Authorize Agency

Assign selected permissions to dbss_depend_obs_trust1.

| ■ | Policy/Role Name | Type |
|---|---|---|
| ☑ | DBSS OBS Agency Access<br>-- | Custom policy |
| □ | PVAccessIamRole<br>Created by CSMS service. | Custom policy |
| □ | CCE cluster policies<br>policies needed by components in CCE clusters | Custom policy |

**Step 8** Set **Scope** to **All resources** and click **OK**. If the message in **Figure 10-4** is displayed, the authorization is successful. Click **Finish**. The authorization will take effect in about 15 minutes.

**Figure 10-4** Authorization completed



Authorize Agency

Authorization successful.

Permissions assigned: 1. View details at Permissions > Authorization.

| Policy/Role Name | Scope | Type | Description |
|---|---|---|---|
| DBSS OBS Agency Access | All resources | Custom policy | -- |

**----End**

## Automatically Backing Up Database Audit Logs

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

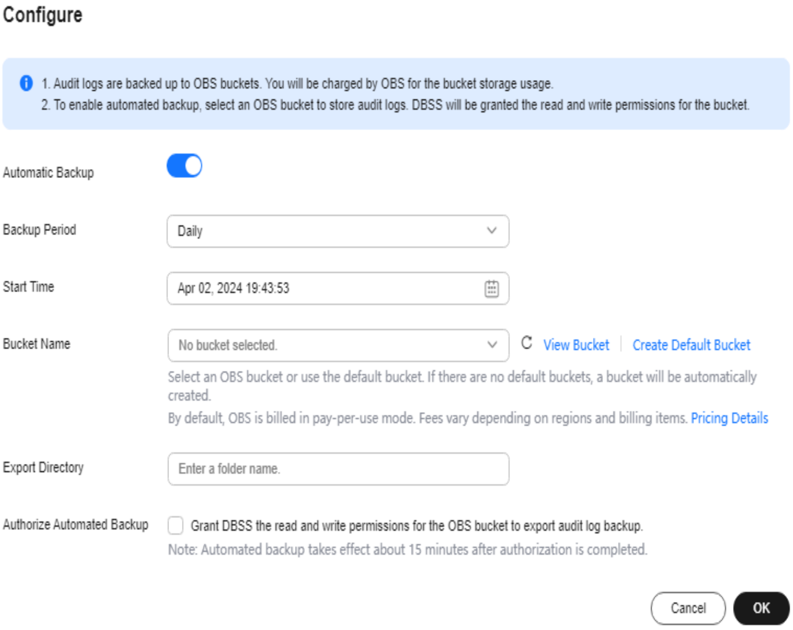
**Step 2** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

**Step 5** Click **Modify Automated Backup Settings**. In the displayed dialog box, set the auto backup parameters. **Table 10-1** describes the parameters.

**Figure 10-5** Configure Automatic Backup dialog box



Configure

1. Audit logs are backed up to OBS buckets. You will be charged by OBS for the bucket storage usage.
2. To enable automated backup, select an OBS bucket to store audit logs. DBSS will be granted the read and write permissions for the bucket.

| | |
|---|---|
| Automatic Backup | ● (on) |
| Backup Period | Daily |
| Start Time | Apr 02, 2024 19:43:53 |
| Bucket Name | No bucket selected. View Bucket \| Create Default Bucket<br>Select an OBS bucket or use the default bucket. If there are no default buckets, a bucket will be automatically created.<br>By default, OBS is billed in pay-per-use mode. Fees vary depending on regions and billing items. Pricing Details |
| Export Directory | Enter a folder name. |
| Authorize Automated Backup | □ Grant DBSS the read and write permissions for the OBS bucket to export audit log backup.<br>Note: Automated backup takes effect about 15 minutes after authorization is completed. |

**Table 10-1** 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.

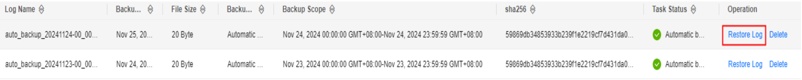
**Step 2** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

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

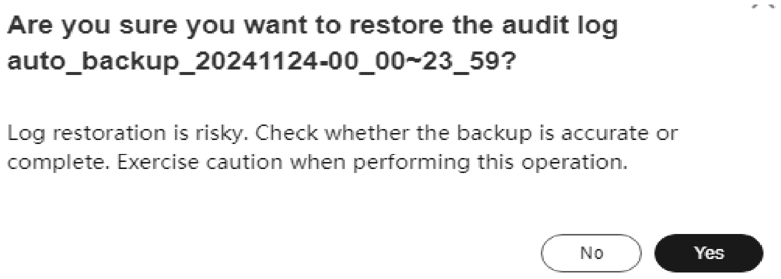
**Figure 10-6** Restoring logs



| Log Name | Backu... | File Size | Backu... | Backup Scope | sha256 | Task Status | Operation |
|---|---|---|---|---|---|---|---|
| auto_backup_20241124-00_00... | Nov 25, 20... | 20 Byte | Automatic ... | Nov 24, 2024 00:00:00 GMT+08:00-Nov 24, 2024 23:59:59 GMT+08:00 | 59869db34853933b239f1e2219cf7d431da0... | ✓ Automatic b... | Restore Log Delete |
| auto_backup_20241123-00_00... | Nov 24, 20... | 20 Byte | Automatic ... | Nov 23, 2024 00:00:00 GMT+08:00-Nov 23, 2024 23:59:59 GMT+08:00 | 59869db34853933b239f1e2219cf7d431da0... | ✓ Automatic b... | Restore Log Delete |

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

**Figure 10-7** Confirming the restoration of audit logs



Are you sure you want to restore the audit log auto_backup_20241124-00_00~23_59?

Log restoration is risky. Check whether the backup is accurate or complete. Exercise caution when performing this operation.

**----End**

## Exporting Risk Data

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

NOTE

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

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

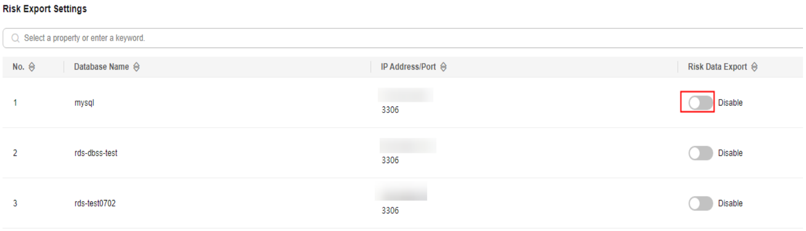
**Step 2** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

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

**Figure 10-8** Enabling risk export



Risk Export Settings

Select a property or enter a keyword.

| No. | Database Name | IP Address/Port | Risk Data Export |
|---|---|---|---|
| 1 | mysql | [redacted]<br>3306 | ○ Disable |
| 2 | rds-dbss-test | [redacted]<br>3306 | ○ Disable |
| 3 | rds-test0702 | [redacted]<br>3306 | ○ Disable |

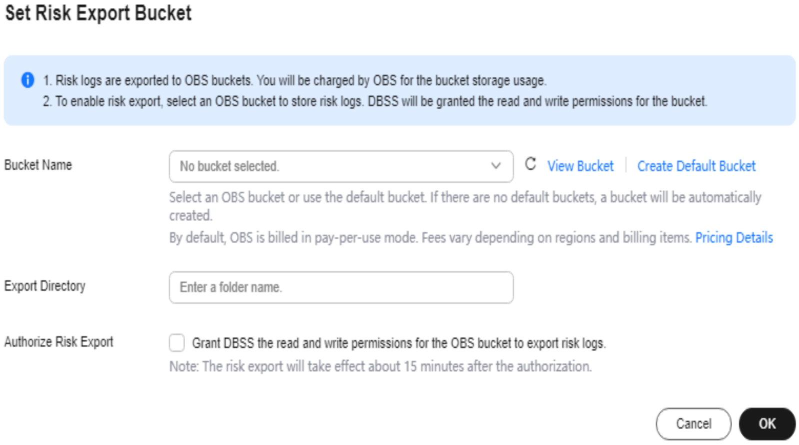
**Step 6** An OBS bucket will be automatically created to store risk logs.

- **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 10-9** Automatically creating an OBS bucket



Set Risk Export Bucket

1. Risk logs are exported to OBS buckets. You will be charged by OBS for the bucket storage usage.
2. To enable risk export, select an OBS bucket to store risk logs. DBSS will be granted the read and write permissions for the bucket.

Bucket Name: No bucket selected.

Select an OBS bucket or use the default bucket. If there are no default buckets, a bucket will be automatically created.

By default, OBS is billed in pay-per-use mode. Fees vary depending on regions and billing items. Pricing Details

Export Directory: Enter a folder name.

Authorize Risk Export: □ Grant DBSS the read and write permissions for the OBS bucket to export risk logs.

Note: The risk export will take effect about 15 minutes after the authorization.

**----End**

# 11 Other Operations

## 11.1 Managing Database Audit Instances

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

### Prerequisites

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

### Viewing the Instance

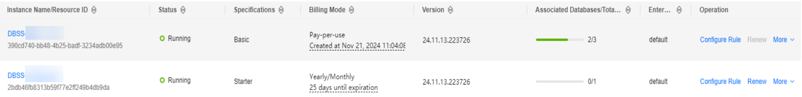
**Step 1** Log in to the management console.

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

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

**Step 4** View the database audit instances information. For details about related parameters, see **Table 11-1**.

**Figure 11-1** Viewing database audit instances



| Instance Name/Resource ID | Status | Specifications | Billing Mode | Version | Associated Databases/Tota... | Enter... | Operation |
|---|---|---|---|---|---|---|---|
| DBSS-[redacted]<br>390cd740-bb48-4b25-badf-3234adb00e95 | ○ Running | Basic | Pay-per-use<br>Created at Nov 21, 2024 11:04:0 | 24.11.13.223726 | 2/3 | default | Configure Rule Renew More ⌄ |
| DBSS-[redacted]<br>2bdb46fb8313b59f77e2ff249b4db9da | ○ Running | Starter | Yearly/Monthly<br>25 days until expiration | 24.11.13.223726 | 0/1 | default | Configure Rule Renew More ⌄ |

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 11-1** 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**

# 11.2 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.**

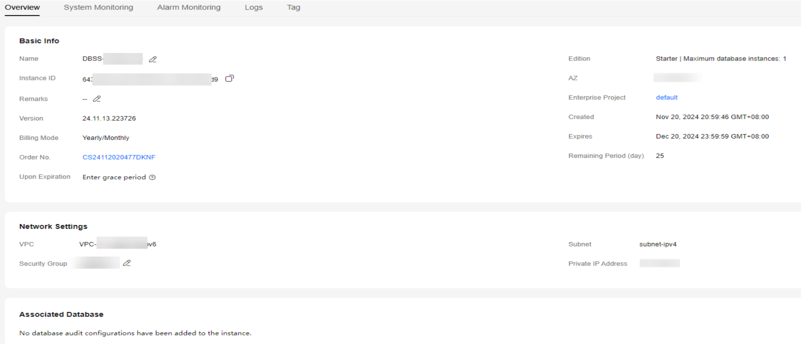
**Step 2** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

**Step 5** View the basic information, network settings, and associated databases about the instance. For details about related parameters, see **Table 11-2**.

**Figure 11-2** Viewing the instance overview



**Basic Info**

Name DBSS-[redacted] ✎

Instance ID 64[redacted]19

Remarks -- ✎

Version 24.11.13.223726

Billing Mode Yearly/Monthly

Order No. CS24112020477DKNF

Upon Expiration Enter grace period

Edition Starter | Maximum database instances: 1

AZ [redacted]

Enterprise Project default

Created Nov 20, 2024 20:59:46 GMT+08:00

Expires Dec 20, 2024 23:59:59 GMT+08:00

Remaining Period (day) 25

**Network Settings**

VPC VPC-[redacted]v6

Security Group [redacted] ✎

Subnet subnet-ipv4

Private IP Address [redacted]

**Associated Database**

No database audit configurations have been added to the instance.

**Table 11-2** 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**

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

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

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

**Step 5** View the database information. For details about related parameters, see **Table 11-3**.

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

**Table 11-3** 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** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

**Step 5** Click ⌄ on the left of the database to expand the agent details. For details about related parameters, see **Table 11-4**.

**Table 11-4** 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**

# 11.4 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**

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

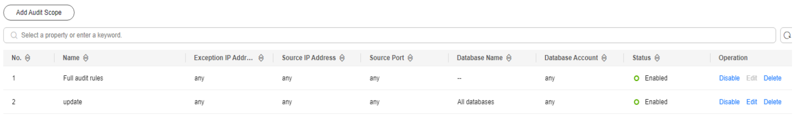
**Step 3** In the navigation tree, choose **Rules**.

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

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

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

**Figure 11-3** Viewing the audit scope



| No. | Name | Exception IP Addr... | Source IP Address | Source Port | Database Name | Database Account | Status | Operation |
|---|---|---|---|---|---|---|---|---|
| 1 | Full audit rules | any | any | any | -- | any | Enabled | Disable Edit Delete |
| 2 | update | any | any | any | All databases | any | Enabled | Disable Edit Delete |

**Table 11-5** 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**

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

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

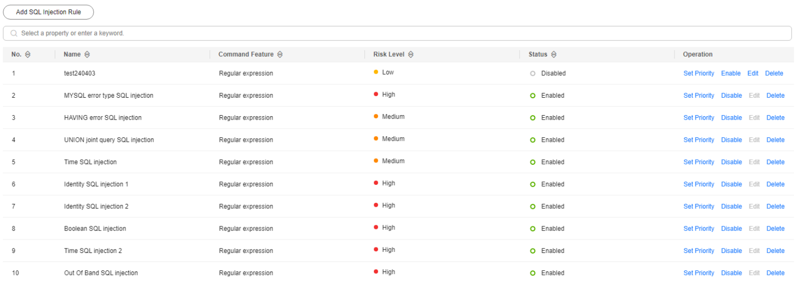
**Step 4** In the **Instance** drop-down list, select the instance for which you want to view SQL injection detection. Click the **SQL Injection** tab.

**Step 5** View information about SQL injection detection. For details about related parameters, see **Table 11-6**.

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 11-4** Viewing information about the SQL injection detection



| No. | Name | Command Feature | Risk Level | Status | Operation |
|---|---|---|---|---|---|
| 1 | test240403 | Regular expression | ● Low | ○ Disabled | Set Priority Enable Edit Delete |
| 2 | MYSQL error type SQL injection | Regular expression | ● High | ○ Enabled | Set Priority Disable Edit Delete |
| 3 | HAVING error SQL injection | Regular expression | ● Medium | ○ Enabled | Set Priority Disable Edit Delete |
| 4 | UNION joint query SQL injection | Regular expression | ● Medium | ○ Enabled | Set Priority Disable Edit Delete |
| 5 | Time SQL injection | Regular expression | ● Medium | ○ Enabled | Set Priority Disable Edit Delete |
| 6 | Identity SQL injection 1 | Regular expression | ● High | ○ Enabled | Set Priority Disable Edit Delete |
| 7 | Identity SQL injection 2 | Regular expression | ● High | ○ Enabled | Set Priority Disable Edit Delete |
| 8 | Boolean SQL injection | Regular expression | ● High | ○ Enabled | Set Priority Disable Edit Delete |
| 9 | Time SQL injection 2 | Regular expression | ● High | ○ Enabled | Set Priority Disable Edit Delete |
| 10 | Out Of Band SQL injection | Regular expression | ● High | ○ Enabled | Set Priority Disable Edit Delete |

**Table 11-6** 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**

# 11.7 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.**

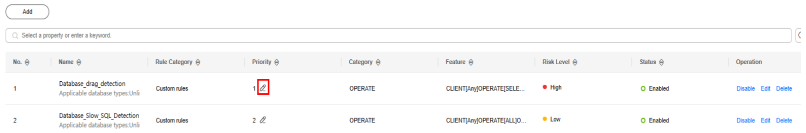
**Step 2** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

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

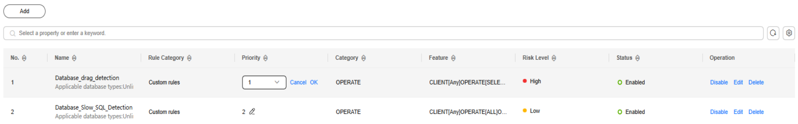
**Figure 11-5** Setting the priority



| No. | Name | Rule Category | Priority | Category | Feature | Risk Level | Status | Operation |
|---|---|---|---|---|---|---|---|---|
| 1 | Database_drag_detection<br>Applicable database types:Unli | Custom rules | 1 ✎ | OPERATE | CLIENT[Any]OPERATE[SELE... | ● High | ○ Enabled | Disable Edit Delete |
| 2 | Database_Slow_SQL_Detection<br>Applicable database types:Unli | Custom rules | 2 ✎ | OPERATE | CLIENT[Any]OPERATE[ALL]O... | ● Low | ○ Enabled | Disable Edit Delete |

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

**Figure 11-6** Setting the priority



| No. | Name | Rule Category | Priority | Category | Feature | Risk Level | Status | Operation |
|---|---|---|---|---|---|---|---|---|
| 1 | Database_drag_detection<br>Applicable database types:Unli | Custom rules | 1 Cancel OK | OPERATE | CLIENT[Any]OPERATE[SELE... | ● High | ○ Enabled | Disable Edit Delete |
| 2 | Database_Slow_SQL_Detection<br>Applicable database types:Unli | Custom rules | 2 | OPERATE | CLIENT[Any]OPERATE[ALL]O... | ● Low | ○ Enabled | Disable Edit Delete |

**----End**

## Viewing the Risky Operation

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

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

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

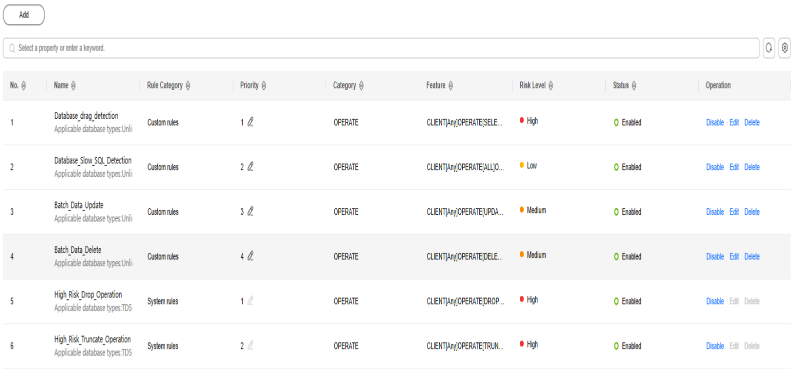
**Step 4** In the **Instance** drop-down list, select an instance to view risky operations.

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

**Step 6** View the risky operation information. For details about related parameters, see **Table 11-7**.

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

**Figure 11-7** Viewing risky operations



| No. | Name | Rule Category | Priority | Category | Feature | Risk Level | Status | Operation |
|---|---|---|---|---|---|---|---|---|
| 1 | Database_drag_detection<br>Applicable database types:Unli | Custom rules | 1 | OPERATE | CLIENT[Any]OPERATE[SELE... | ● High | ○ Enabled | Disable Edit Delete |
| 2 | Database_Slow_SQL_Detection<br>Applicable database types:Unli | Custom rules | 2 | OPERATE | CLIENT[Any]OPERATE[ALL]O... | ● Low | ○ Enabled | Disable Edit Delete |
| 3 | Batch_Data_Update<br>Applicable database types:Unli | Custom rules | 3 | OPERATE | CLIENT[Any]OPERATE[UPDA... | ● Medium | ○ Enabled | Disable Edit Delete |
| 4 | Batch_Data_Delete<br>Applicable database types:Unli | Custom rules | 4 | OPERATE | CLIENT[Any]OPERATE[DELE... | ● Medium | ○ Enabled | Disable Edit Delete |
| 5 | High_Risk_Drop_Operation<br>Applicable database types:TDS | System rules | 1 | OPERATE | CLIENT[Any]OPERATE[DROP... | ● High | ○ Enabled | Disable Edit Delete |
| 6 | High_Risk_Truncate_Operation<br>Applicable database types:TDS | System rules | 2 | OPERATE | CLIENT[Any]OPERATE[TRUN... | ● High | ○ Enabled | Disable Edit Delete |

**Table 11-7** 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 |

| Parameter | Description |
|---|---|
| Priority | Priority of a risky operation. |
| Category | Category of the risky operation |
| Feature | Feature of the risky operation |
| Risk Severity | Risk severity of the risky operation. The options are as follows:<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**

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

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

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

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

NOTE

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

**Step 6** View the rules. For details about related parameters, see **Table 11-8**.

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.

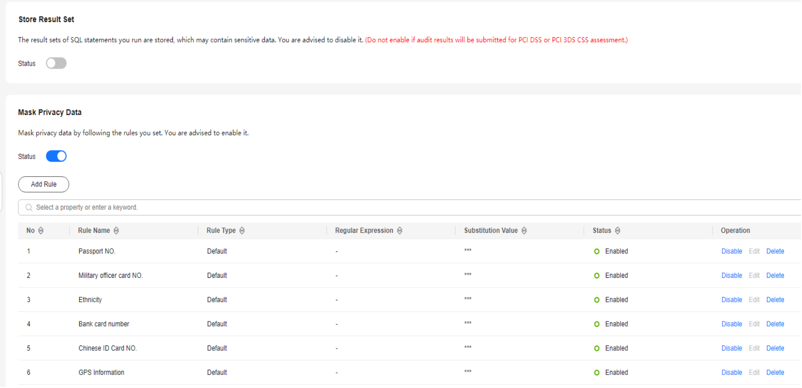
  Do not enable this function if you want to prepare for PCI DSS/PCI 3DS CSS certification.

  **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 11-8** Masking rule information



**Store Result Set**

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

Status ○

**Mask Privacy Data**

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

Status ●

| No | Rule Name | Rule Type | Regular Expression | Substitution Value | Status | Operation |
|---|---|---|---|---|---|---|
| 1 | Passport NO. | Default | - | *** | Enabled | Disable Edit Delete |
| 2 | Military officer card NO. | Default | - | *** | Enabled | Disable Edit Delete |
| 3 | Ethnicity | Default | - | *** | Enabled | Disable Edit Delete |
| 4 | Bank card number | Default | - | *** | Enabled | Disable Edit Delete |
| 5 | Chinese ID Card NO. | Default | - | *** | Enabled | Disable Edit Delete |
| 6 | GPS Information | Default | - | *** | Enabled | Disable Edit Delete |

**Table 11-8** Masking rule parameters

| Parameter | Description |
|---|---|
| Rule Name | Rule name |

| Parameter | Description |
|---|---|
| Rule Type | Rule type.<br>● Default<br>● User-defined |
| Regular Expression | Regular expression that specifies the sensitive data pattern |
| Substitution Value | Value used to replace sensitive data specified by the regular expression |
| Status | Status of a rule. Its value can be:<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**

# 11.9 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.**

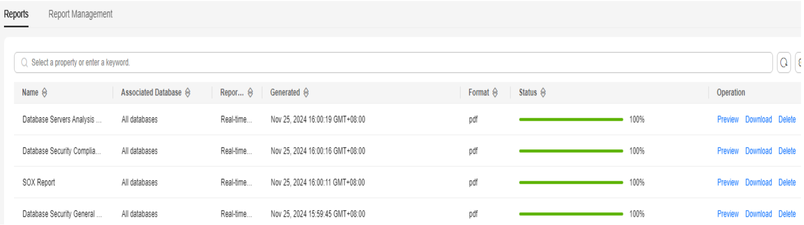
**Step 2** Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

**Step 5** Viewing reports

**Figure 11-9** Viewing a report



| Name | Associated Database | Repor... | Generated | Format | Status | Operation |
|---|---|---|---|---|---|---|
| Database Servers Analysis ... | All databases | Real-time... | Nov 25, 2024 16:00:19 GMT+08:00 | pdf | 100% | Preview Download Delete |
| Database Security Complia... | All databases | Real-time... | Nov 25, 2024 16:00:16 GMT+08:00 | pdf | 100% | Preview Download Delete |
| SOX Report | All databases | Real-time... | Nov 25, 2024 16:00:11 GMT+08:00 | pdf | 100% | Preview Download Delete |
| Database Security General ... | All databases | Real-time... | Nov 25, 2024 15:59:45 GMT+08:00 | pdf | 100% | Preview Download Delete |

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

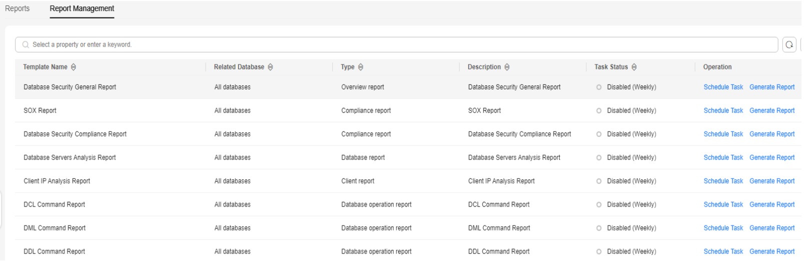
**Step 3** In the navigation tree on the left, choose **Reports**.

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

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

**Step 6** View the report template.

**Figure 11-10** Viewing the template list



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

NOTE

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

**----End**

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

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

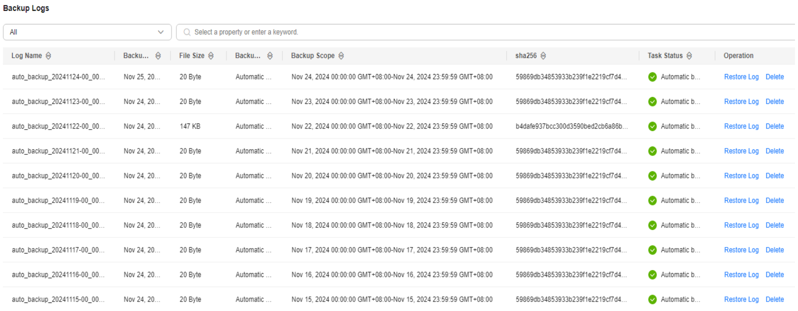
**Step 4** In the **Instance** drop-down list, select the instance whose log template you want to view.

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

**Step 6** View the backup audit log information. For details about related parameters, see **Table 11-9**.

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 11-11** Viewing backup audit logs



Backup Logs

All

Select a property or enter a keyword.

| Log Name | Backu... | File Size | Backu... | Backup Scope | sha256 | Task Status | Operation |
|---|---|---|---|---|---|---|---|
| auto_backup_20241124-00_00... | Nov 25, 20... | 20 Byte | Automatic ... | Nov 24, 2024 00:00:00 GMT+08:00-Nov 24, 2024 23:59:59 GMT+08:00 | 59869db34853933b239f1e2219cf7d4... | ✓ Automatic b... | Restore Log Delete |
| auto_backup_20241123-00_00... | Nov 24, 20... | 20 Byte | Automatic ... | Nov 23, 2024 00:00:00 GMT+08:00-Nov 23, 2024 23:59:59 GMT+08:00 | 59869db34853933b239f1e2219cf7d4... | ✓ Automatic b... | Restore Log Delete |
| auto_backup_20241122-00_00... | Nov 24, 20... | 147 KB | Automatic ... | Nov 22, 2024 00:00:00 GMT+08:00-Nov 22, 2024 23:59:59 GMT+08:00 | b4dafe937bcc300d3590bed2cb6a86b... | ✓ Automatic b... | Restore Log Delete |
| auto_backup_20241121-00_00... | Nov 24, 20... | 20 Byte | Automatic ... | Nov 21, 2024 00:00:00 GMT+08:00-Nov 21, 2024 23:59:59 GMT+08:00 | 59869db34853933b239f1e2219cf7d4... | ✓ Automatic b... | Restore Log Delete |
| auto_backup_20241120-00_00... | Nov 24, 20... | 20 Byte | Automatic ... | Nov 20, 2024 00:00:00 GMT+08:00-Nov 20, 2024 23:59:59 GMT+08:00 | 59869db34853933b239f1e2219cf7d4... | ✓ Automatic b... | Restore Log Delete |
| auto_backup_20241119-00_00... | Nov 24, 20... | 20 Byte | Automatic ... | Nov 19, 2024 00:00:00 GMT+08:00-Nov 19, 2024 23:59:59 GMT+08:00 | 59869db34853933b239f1e2219cf7d4... | ✓ Automatic b... | Restore Log Delete |
| auto_backup_20241118-00_00... | Nov 24, 20... | 20 Byte | Automatic ... | Nov 18, 2024 00:00:00 GMT+08:00-Nov 18, 2024 23:59:59 GMT+08:00 | 59869db34853933b239f1e2219cf7d4... | ✓ Automatic b... | Restore Log Delete |
| auto_backup_20241117-00_00... | Nov 24, 20... | 20 Byte | Automatic ... | Nov 17, 2024 00:00:00 GMT+08:00-Nov 17, 2024 23:59:59 GMT+08:00 | 59869db34853933b239f1e2219cf7d4... | ✓ Automatic b... | Restore Log Delete |
| auto_backup_20241116-00_00... | Nov 24, 20... | 20 Byte | Automatic ... | Nov 16, 2024 00:00:00 GMT+08:00-Nov 16, 2024 23:59:59 GMT+08:00 | 59869db34853933b239f1e2219cf7d4... | ✓ Automatic b... | Restore Log Delete |
| auto_backup_20241115-00_00... | Nov 24, 20... | 20 Byte | Automatic ... | Nov 15, 2024 00:00:00 GMT+08:00-Nov 15, 2024 23:59:59 GMT+08:00 | 59869db34853933b239f1e2219cf7d4... | ✓ Automatic b... | Restore Log Delete |

**Table 11-9** 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**

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

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

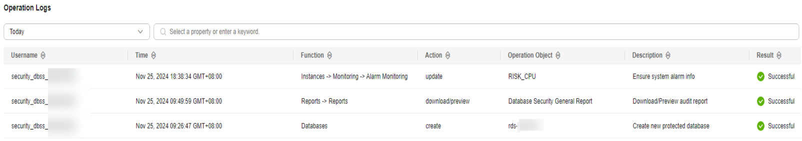
**Step 4** Click the name of the instance whose operation logs you want to view. The **Overview** page is displayed.

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

**Step 6** View operation logs. For details about related parameters, see **Table 11-10**.

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 11-12** Viewing operation logs



Operation Logs

| Username | Time | Function | Action | Operation Object | Description | Result |
|---|---|---|---|---|---|---|
| security_dbss_[redacted] | Nov 25, 2024 18:38:34 GMT+08:00 | Instances -> Monitoring -> Alarm Monitoring | update | RISK_CPU | Ensure system alarm info | ✓ Successful |
| security_dbss_[redacted] | Nov 25, 2024 09:49:59 GMT+08:00 | Reports -> Reports | download/preview | Database Security General Report | Download/Preview audit report | ✓ Successful |
| security_dbss_[redacted] | Nov 25, 2024 09:26:47 GMT+08:00 | Databases | create | rds-[redacted] | Create new protected database | ✓ Successful |

**Table 11-10** 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**

# 12 Key Operations Recorded by CTS

## 12.1 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

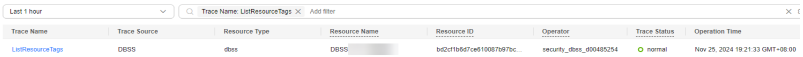
**Step 1** Log in to the management console.

**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 12-1** Trace list

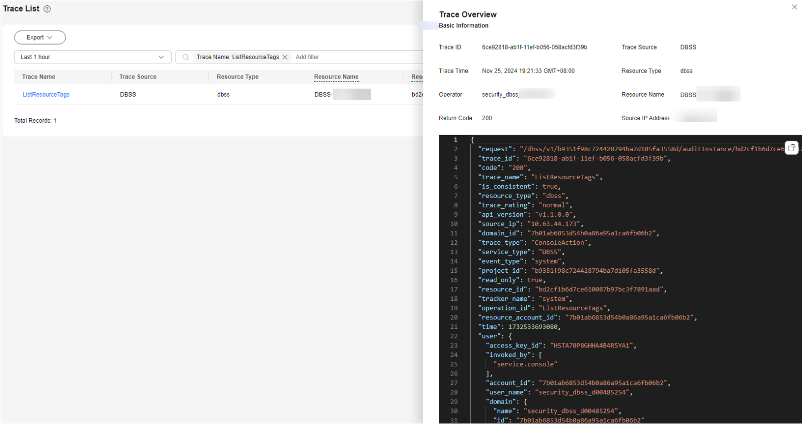


Last 1 hour | Trace Name: ListResourceTags | Add filter

| Trace Name | Trace Source | Resource Type | Resource Name | Resource ID | Operator | Trace Status | Operation Time |
|---|---|---|---|---|---|---|---|
| ListResourceTags | DBSS | dbss | DBSS[redacted] | bd2cf1b6d7ce610087b97bc... | security_dbss_d00485254 | ○ normal | Nov 25, 2024 19:21:33 GMT+08:00 |

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

**Figure 12-2** Viewing traces



Trace List

Export

Last 1 hour

Trace Name: ListResourceTags ✕ Add filter

| Trace Name | Trace Source | Resource Type | Resource Name | Res |
|---|---|---|---|---|
| ListResourceTags | DBSS | dbss | DBSS-[redacted] | bd2c |

Total Records: 1

Trace Overview

Basic Information

| | | | |
|---|---|---|---|
| Trace ID | 6ce92818-ab1f-11ef-b056-058acfd3f39b | Trace Source | DBSS |
| Trace Time | Nov 25, 2024 19:21:33 GMT+08:00 | Resource Type | dbss |
| Operator | security_dbss_[redacted] | Resource Name | DBSS[redacted] |
| Return Code | 200 | Source IP Address | [redacted] |

```
{
  "request": "/dbss/v1/b9351f98c724428794ba7d105fa3558d/auditInstance/bd2cf1b6d7ce6
  "trace_id": "6ce92818-ab1f-11ef-b056-058acfd3f39b",
  "code": "200",
  "trace_name": "ListResourceTags",
  "is_consistent": true,
  "resource_type": "dbss",
  "trace_rating": "normal",
  "api_version": "v1.1.0.0",
  "source_ip": "10.63.44.173",
  "domain_id": "7b01ab6853d54b0a86a95a1ca6fb06b2",
  "trace_type": "ConsoleAction",
  "service_type": "DBSS",
  "event_type": "system",
  "project_id": "b9351f98c724428794ba7d105fa3558d",
  "read_only": true,
  "resource_id": "bd2cf1b6d7ce610087b97bc3f7891aad",
  "tracker_name": "system",
  "operation_id": "ListResourceTags",
  "resource_account_id": "7b01ab6853d54b0a86a95a1ca6fb06b2",
  "time": 1732533693080,
  "user": {
    "access_key_id": "HSTA70P8GHHA4B4RSYA1",
    "invoked_by": [
      "service.console"
    ],
    "account_id": "7b01ab6853d54b0a86a95a1ca6fb06b2",
    "user_name": "security_dbss_d00485254",
    "domain": {
      "name": "security_dbss_d00485254",
      "id": "7b01ab6853d54b0a86a95a1ca6fb06b2"
```

**----End**

## 12.2 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 12-1** lists DBSS operations recorded by CTS.

**Table 12-1** 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 |

# 13 Monitoring

## 13.1 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 13-1** 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 |

# 13.2 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.**

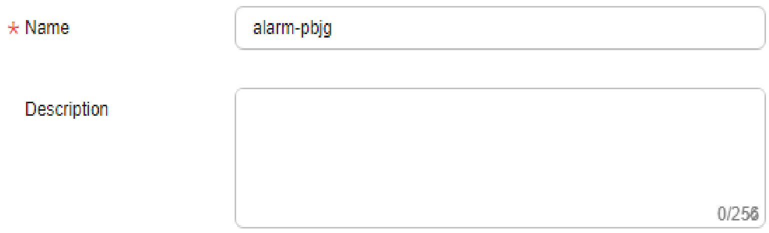
**Step 2** Click ☰ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

**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 13-1** Setting the alarm rule name



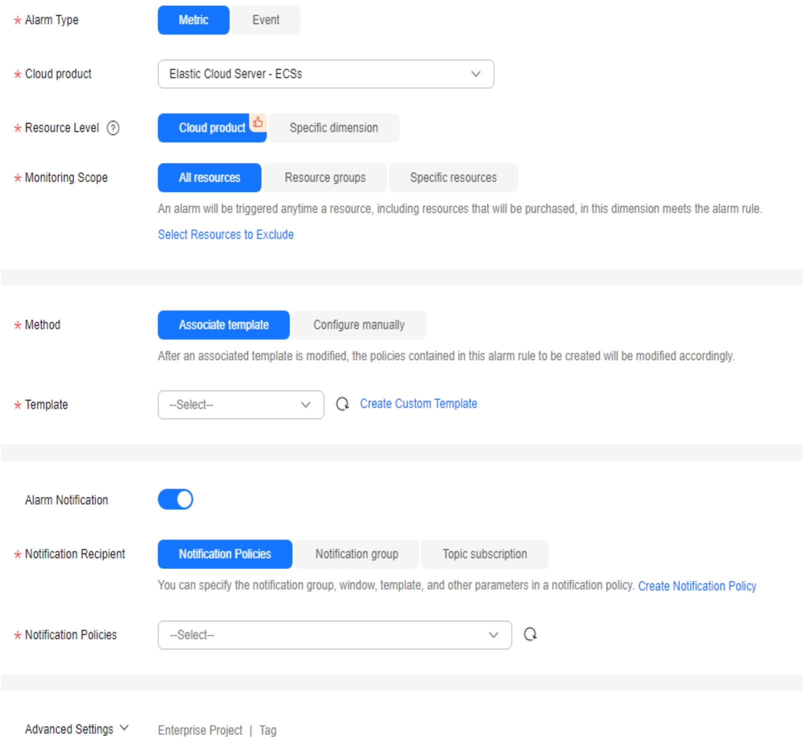
* Name: alarm-pbjg

Description:

0/256

**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 13-2.

**Figure 13-2** Configuring a DBSS alarm monitoring rule



* Alarm Type: Metric | Event

* Cloud product: Elastic Cloud Server - ECSs

* Resource Level: Cloud product | Specific dimension

* Monitoring Scope: All resources | Resource groups | Specific resources

An alarm will be triggered anytime a resource, including resources that will be purchased, in this dimension meets the alarm rule.

Select Resources to Exclude

* Method: Associate template | Configure manually

After an associated template is modified, the policies contained in this alarm rule to be created will be modified accordingly.

* Template: --Select-- Create Custom Template

Alarm Notification

* Notification Recipient: Notification Policies | Notification group | Topic subscription

You can specify the notification group, window, template, and other parameters in a notification policy. Create Notification Policy

* Notification Policies: --Select--

Advanced Settings Enterprise Project | Tag

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

**----End**

# 13.3 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

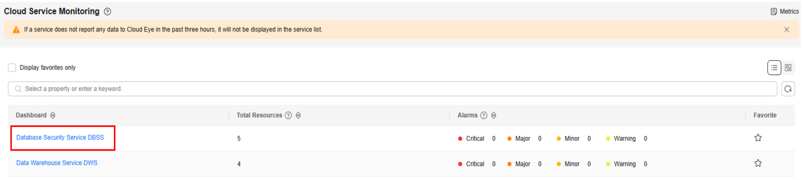
**Step 1** **Log in to the management console.**

**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 13-3** Cloud service monitoring



Cloud Service Monitoring ⓘ — Metrics

If a service does not report any data to Cloud Eye in the past three hours, it will not be displayed in the service list.

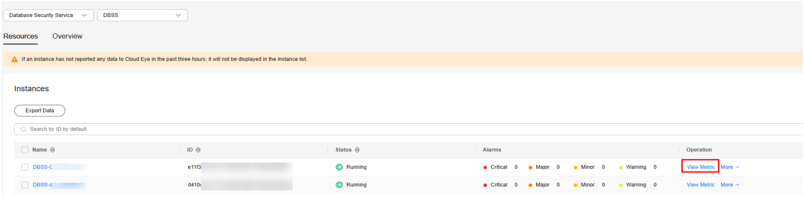
□ Display favorites only

Select a property or enter a keyword.

| Dashboard | Total Resources | Alarms | Favorite |
|---|---|---|---|
| Database Security Service DBSS | 5 | ● Critical 0 ● Major 0 ● Minor 0 ● Warning 0 | ☆ |
| Data Warehouse Service DWS | 4 | ● Critical 0 ● Major 0 ● Minor 0 ● Warning 0 | ☆ |

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

**Figure 13-4** Viewing monitoring metrics



Database Security Service | DBSS

Resources | Overview

If an instance has not reported any data to Cloud Eye in the past three hours, it will not be displayed in the instance list.

Instances

Export Data

Search by ID by default.

| □ Name | ID | Status | Alarms | Operation |
|---|---|---|---|---|
| □ DBSS-C[redacted] | e11f3[redacted] | Running | ● Critical 0 ● Major 0 ● Minor 0 ● Warning 0 | View Metric More |
| □ DBSS-s[redacted] | d410[redacted] | Running | ● Critical 0 ● Major 0 ● Minor 0 ● Warning 0 | View Metric More |

**----End**

# 14 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.

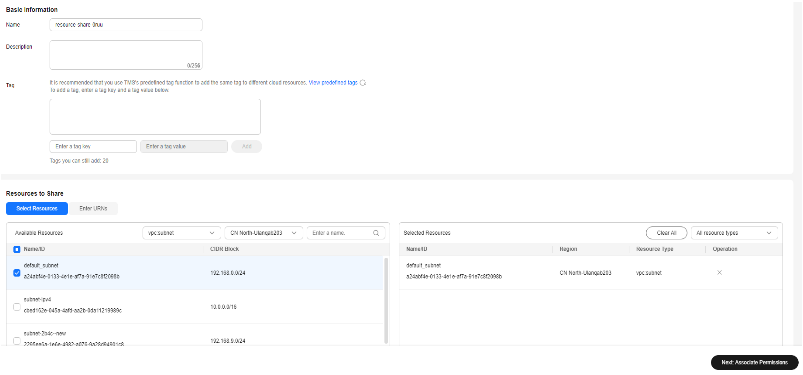
**Step 2** Click ☰ in the upper left corner, choose **Management & Governance** > **Resource Access Manager**, and go to the resource access management page.

**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 14-1** Specifying shared resources



Basic Information

Name: resource-share-0ruu

Description: 0/256

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags
To add a tag, enter a tag key and a tag value below.

Enter a tag key | Enter a tag value | Add

Tags you can still add: 20

Resources to Share

Select Resources | Enter URNs

Available Resources: vpc:subnet | CN North-Ulanqab203 | Enter a name.

| ☑ Name/ID | CIDR Block |
|---|---|
| ☑ default_subnet<br>a24abf4e-0133-4e1e-af7a-91e7c8f2098b | 192.168.0.0/24 |
| □ subnet-ipv4<br>cbed162e-045a-4afd-aa2b-0da11219989c | 10.0.0.0/16 |
| □ subnet-2b4c--new<br>2295ee6a-1e6e-4982-a076-9a28d94901c8 | 192.168.9.0/24 |

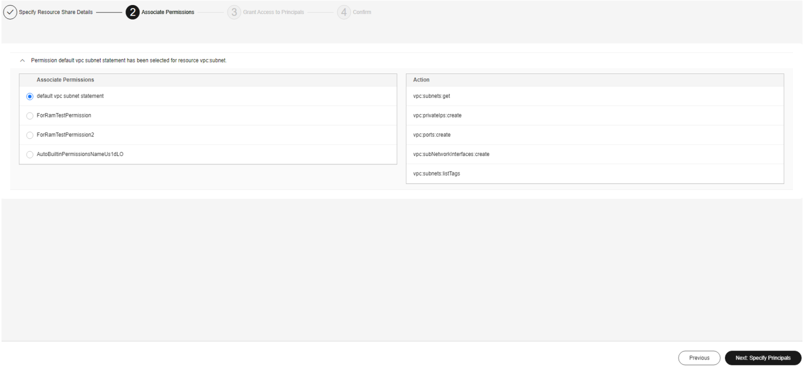
Selected Resources: Clear All | All resource types

| Name/ID | Region | Resource Type | Operation |
|---|---|---|---|
| default_subnet<br>a24abf4e-0133-4e1e-af7a-91e7c8f2098b | CN North-Ulanqab203 | vpc:subnet | × |

Next: Associate Permissions

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

**Figure 14-2** Configuring permissions

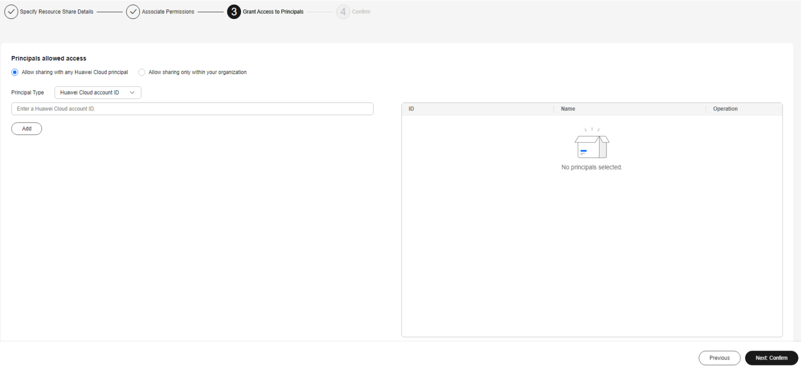


Permission default vpc subnet statement has been selected for resource vpc:subnet.

| Associate Permissions | Action |
|---|---|
| ● default vpc subnet statement | vpc:subnets:get |
| ○ ForRamTestPermission | vpc:privateIps:create |
| ○ ForRamTestPermission2 | vpc:ports:create |
| ○ AutoBuiltinPermissionsNameUs1dLO | vpc:subNetworkInterfaces:create |
| | vpc:subnets:listTags |

**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 14-3** Specifying principals



Principals allowed access

● Allow sharing with any Huawei Cloud principal ○ Allow sharing only within your organization

Principal Type: Huawei Cloud account ID

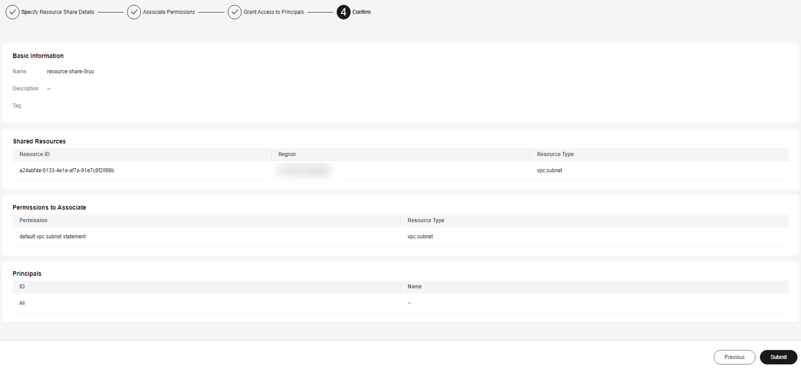
Enter a Huawei Cloud account ID.

**Table 14-1** 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 14-4** Confirming configurations



Basic Information

Name resource-share-0ruu

Description --

Tag

Shared Resources

| Resource ID | Region | Resource Type |
|---|---|---|
| a24abf4e-0133-4e1e-af7a-91e7c8f2098b | [redacted] | vpc:subnet |

Permissions to Associate

| Permission | Resource Type |
|---|---|
| default vpc subnet statement | vpc:subnet |

Principals

| ID | Name |
|---|---|
| as | -- |

**----End**

## Using a VPC

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

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

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

**Step 4** Set **Basic Settings** and **Edition**.

**Table 14-2** Basic settings parameters

| Parameter | Description |
|---|---|
| Service Type | The value is fixed at **Database Audit Service**. |
| Billing Mode | Only the yearly/monthly mode is available. |
| Region | Select the region where the instance is located. Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region. |
| AZ Type | Only general AZs are supported. |
| AZ | An AZ is a physical location that uses an independent power supply and network. AZs in the same region can communicate with each other over an intranet.<br>You can select random allocation or specify an AZ. |

**Table 14-3** Edition specifications

| Parameter | Description |
|---|---|
| Edition specifications | **Basic**, **Standard**, **Professional**, and **Advanced** editions are available.<br>For details about the specifications supported by each edition, see **Table 14-4**. |

**Table 14-4** Database audit editions

| Edition | Specification | Maximum Databases | Performance |
|---|---|---|---|
| Starter | Database audit starter edition | 1 | - Peak QPS: 1,000 queries/second<br>- Database load rate: 1.2 million statements/hour<br>- Online SQL statement storage: 100 million statements |
| Basic | Database audit basic edition | 3 | - Peak QPS: 3,000 queries/second<br>- Database load rate: 3.6 million statements/hour<br>- Online SQL statement storage: 400 million statements |
| Professional | Database audit professional edition | 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 | Database audit advanced edition | 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

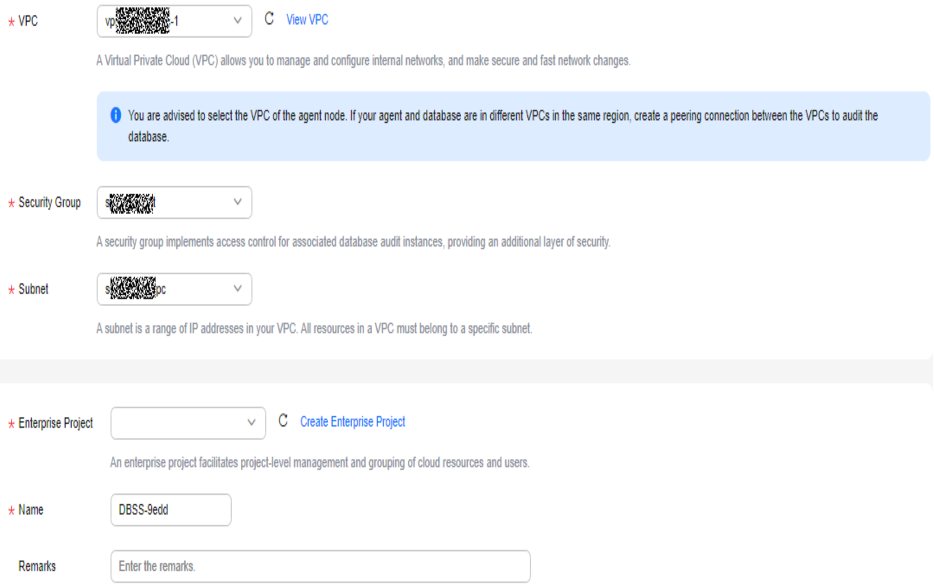
- A database instance is uniquely defined by its **database IP address and port**.

  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** Select the VPC and subnet for database audit. For details about related parameters, see **Table 14-5**.

**Figure 14-5** Setting database audit parameters



* VPC: vp[redacted]-1

A Virtual Private Cloud (VPC) allows you to manage and configure internal networks, and make secure and fast network changes.

You are advised to select the VPC of the agent node. If your agent and database are in different VPCs in the same region, create a peering connection between the VPCs to audit the database.

* Security Group: s[redacted]t

A security group implements access control for associated database audit instances, providing an additional layer of security.

* Subnet: s[redacted]pc

A subnet is a range of IP addresses in your VPC. All resources in a VPC must belong to a specific subnet.

* Enterprise Project:

An enterprise project facilitates project-level management and grouping of cloud resources and users.

* Name: DBSS-9edd

Remarks: Enter the remarks.

**Table 14-5** 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*. |

| Parameter | Description |
|---|---|
| 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**

# 15 Database Security Encryption Management

## 15.1 Instance Management

### 15.1.1 Enabling an Instance

The instance needs to be started in the following scenarios:

- When the **running status** of an instance is **Disable**, you need to start the instance if you want to log in to the instance using database encryption and access control.
- If the **running status** of an instance is **Abnormal**, you can start the instance if you need to log in to the instance using database encryption and access control.

#### Procedure

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

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

**Step 3** In the navigation pane on the left, click ☰ and choose **Security & Compliance** > **Data Security Center**.

**Step 4** Locate the row that contains the desired instance, and click in the **Operation** column.

**----End**

### 15.1.2 Disabling an Instance

You can stop an instance when its **running status** is Running. After the instance is stopped, you cannot log in to the database encryption and access control instance.

## Procedure

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

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

**Step 3** In the navigation tree on the left, click ☰. Choose **Security & Compliance** > **Data Security Center**.

**Step 4** In the row containing the desired instance, choose in the **Operation** column.

**Step 5** In the displayed dialog box, click **OK**. After the instance is stopped, its Running Status changes to Stopped.

> NOTE
>
> To forcibly stop an instance, select the **Forcibly stop** check box in the displayed dialog box. Forcibly stopping an instance may cause data loss. Ensure that all data files have been saved before performing this operation.

**----End**

## 15.1.3 Restarting an Instance

For maintenance purposes, if the system is abnormal, you can reboot a DB instance to restore it to the Available state.

- You can restart a database encryption and access control instance only when it is running.
- Restarting an instance will interrupt system services for about 5 minutes. During this period, the status of the instance is **Restarting**.
- During the restart, the DB encryption and access control instance is unavailable.

## Procedure

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

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

**Step 3** In the navigation pane on the left, click ☰ and choose **Security & Compliance** > **Data Security Center**.

**Step 4** In the row containing the instance to be restarted, choose in the **Operation** column.

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

**Step 6** The restart takes about 5 to 10 minutes, and the instance status changes to **Restarting**.

If the instance status changes to **Running**, the restart is complete and the system can be used properly.

NOTE

In the Restart Instance dialog box, you can select **to forcibly restart the**. Forcibly restarting the instance may cause data loss. Ensure that all data files have been saved and no operation is performed in the system.

**----End**

## 15.1.4 Unbinding an EIP

To rebind or release an EIP, you need to unbind the EIP from the instance first. After an EIP is unbound from an instance, you cannot use the EIP to log in to database encryption and access control.

### Procedure

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

**Step 2** Click in the upper left corner and select a region or project.

**Step 3** In the navigation pane on the left, click and choose **Security & Compliance** > **Data Security Center**.

**Step 4** Locate the row that contains the desired instance and choose in the **Operation** column.

**Step 5** In the displayed Unbind EIP dialog box, click **OK**.

**----End**

# 15.2 Database Security Encryption Instance Management

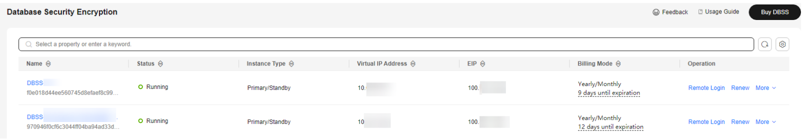
On the management console, you can restart, disable, and unbind EIP from database instances.

**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** Choose **Database Security Encryption** to view the database security encryption instances.

**Figure 15-1** Database security encryption instance



Database Security Encryption

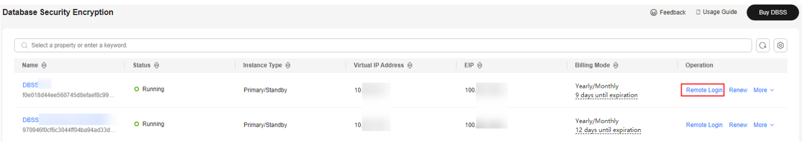
| Name | Status | Instance Type | Virtual IP Address | EIP | Billing Mode | Operation |
|---|---|---|---|---|---|---|
| DBSS [redacted]<br>f0e018d44ee560745d8efaef8c99... | Running | Primary/Standby | 10.[redacted] | 100.[redacted] | Yearly/Monthly<br>9 days until expiration | Remote Login Renew More |
| DBSS [redacted]<br>970946f0cf6c3044ff04ba94ad33d... | Running | Primary/Standby | 10[redacted] | 100.[redacted] | Yearly/Monthly<br>12 days until expiration | Remote Login Renew More |

**----End**

## Remote Login

**Step 1** Locate the target instance and click **Remote Login** in the **Operation** column.

**Figure 15-2** Remotely logging in to a database encryption instance


Database Security Encryption
Feedback
Usage Guide
Buy DBSS
Select a property or enter a keyword.

| Name | Status | Instance Type | Virtual IP Address | EIP | Billing Mode | Operation |
|---|---|---|---|---|---|---|
| DBSS [redacted]<br>f0e018d44ee560745d8efaef8c99... | Running | Primary/Standby | 10. [redacted] | 100. [redacted] | Yearly/Monthly<br>9 days until expiration | Remote Login Renew More |
| DBSS [redacted]<br>970946f0cf6c3044ff04ba94ad33d... | Running | Primary/Standby | 10. [redacted] | 100. [redacted] | Yearly/Monthly<br>12 days until expiration | Remote Login Renew More |

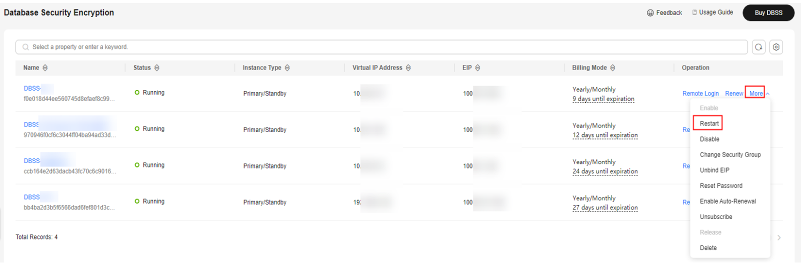
**Step 2** On the displayed login page, enter the username and password of the instance and click **Log In**. The database encryption console is displayed.

**----End**

## Restarting an Instance

**Step 1** In the **Operation** column of the target instance, choose **More** > **Restart**.

**Figure 15-3** Restarting a database encryption instance



| Name | Status | Instance Type | Virtual IP Address | EIP | Billing Mode | Operation |
|---|---|---|---|---|---|---|
| DBSS- [redacted]<br>f0e018d44ee560745d8efaef8c99... | Running | Primary/Standby | 10. [redacted] | 100 [redacted] | Yearly/Monthly<br>9 days until expiration | Remote Login Renew More |
| DBSS [redacted]<br>970946f0cf6c3044ff04ba94ad33d... | Running | Primary/Standby | 10. [redacted] | 100 [redacted] | Yearly/Monthly<br>12 days until expiration | Re |
| DBSS- [redacted]<br>ccb164e2d63dacb43fc70c6c9016... | Running | Primary/Standby | 10. [redacted] | 100 [redacted] | Yearly/Monthly<br>24 days until expiration | Re |
| DBSS [redacted]<br>bb4ba2d3b5f6566dad6fef801d3c... | Running | Primary/Standby | 19 [redacted] | 100 [redacted] | Yearly/Monthly<br>27 days until expiration | Re |

Total Records: 4

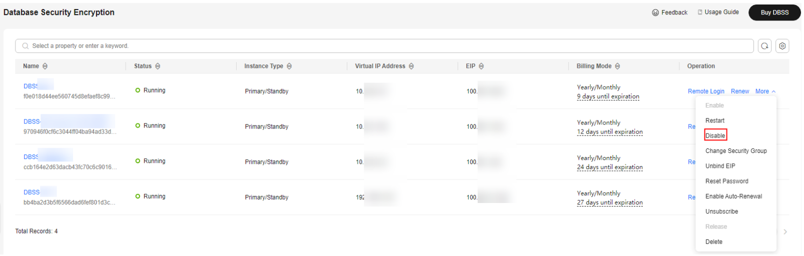
**Step 2** In the displayed dialog box, click **OK**. The instance automatically restarts.

**----End**

## Stopping an Instance

**Step 1** In the **Operation** column of the target instance, choose **More** > **Disable**.

**Figure 15-4** Disabling a database encryption instance



| Name | Status | Instance Type | Virtual IP Address | EIP | Billing Mode | Operation |
|---|---|---|---|---|---|---|
| DBS [redacted]<br>f0e018d44ee560745d8efaef8c99... | Running | Primary/Standby | 10. [redacted] | 100. [redacted] | Yearly/Monthly<br>9 days until expiration | Remote Login Renew More |
| DBSS- [redacted]<br>970946f0cf6c3044ff04ba94ad33d... | Running | Primary/Standby | 10. [redacted] | 100. [redacted] | Yearly/Monthly<br>12 days until expiration | Re |
| DBS [redacted]<br>ccb164e2d63dacb43fc70c6c9016... | Running | Primary/Standby | 10. [redacted] | 100. [redacted] | Yearly/Monthly<br>24 days until expiration | Re |
| DBSS- [redacted]<br>bb4ba2d3b5f6566dad6fef801d3c... | Running | Primary/Standby | 192 [redacted] | 100. [redacted] | Yearly/Monthly<br>27 days until expiration | Re |

Total Records: 4

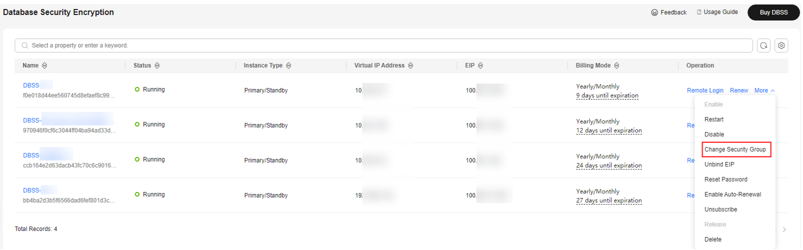
**Step 2** In the displayed dialog box, click **OK**. The instance is automatically disabled.

**----End**

## Modifying a Security Group

**Step 1** In the **Operation** column of the target instance, choose **More** > **Change Security Group**.

**Figure 15-5** Modifying the security group



| Name | Status | Instance Type | Virtual IP Address | EIP | Billing Mode | Operation |
|---|---|---|---|---|---|---|
| DBSS[redacted]<br>f0e018d44ee560745d8efaef8c99... | Running | Primary/Standby | 10.[redacted] | 100.[redacted] | Yearly/Monthly<br>9 days until expiration | Remote Login Renew More |
| DBSS-[redacted]<br>970946f0cf6c3044ff04ba94ad33d... | Running | Primary/Standby | 10.[redacted] | 100.[redacted] | Yearly/Monthly<br>12 days until expiration | Re |
| DBSS[redacted]<br>ccb164e2d63dacb43fc70c6c9016... | Running | Primary/Standby | 10.[redacted] | 100.[redacted] | Yearly/Monthly<br>24 days until expiration | Re |
| DBSS-[redacted]<br>bb4ba2d3b5f6566dad6fef801d3c... | Running | Primary/Standby | 19[redacted] | 100.[redacted] | Yearly/Monthly<br>27 days until expiration | Re |

Total Records: 4

**Step 2** In the displayed dialog box, select a security group and click **OK**.

NOTE

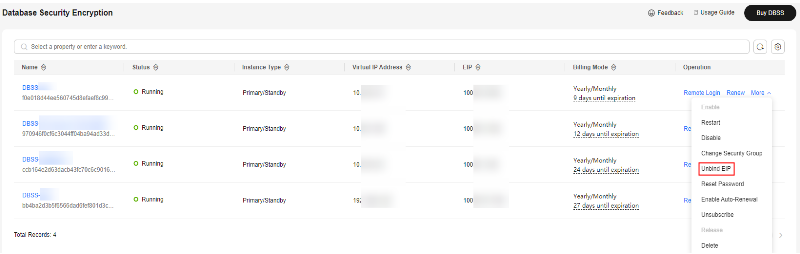
Only existing security groups can be selected.

**----End**

## Unbinding an EIP

**Step 1** In the **Operation** column of the target instance, choose **More** > **Unbind EIP**.

**Figure 15-6** Unbinding an EIP



| Name | Status | Instance Type | Virtual IP Address | EIP | Billing Mode | Operation |
|---|---|---|---|---|---|---|
| DBSS[redacted]<br>f0e018d44ee560745d8efaef8c99... | Running | Primary/Standby | 10.[redacted] | 100.[redacted] | Yearly/Monthly<br>9 days until expiration | Remote Login Renew More |
| DBSS-[redacted]<br>970946f0cf6c3044ff04ba94ad33d... | Running | Primary/Standby | 10.[redacted] | 100.[redacted] | Yearly/Monthly<br>12 days until expiration | Re |
| DBSS[redacted]<br>ccb164e2d63dacb43fc70c6c9016... | Running | Primary/Standby | 10.[redacted] | 100.[redacted] | Yearly/Monthly<br>24 days until expiration | Re |
| DBSS-[redacted]<br>bb4ba2d3b5f6566dad6fef801d3c... | Running | Primary/Standby | 19[redacted] | 100.[redacted] | Yearly/Monthly<br>27 days until expiration | Re |

Total Records: 4

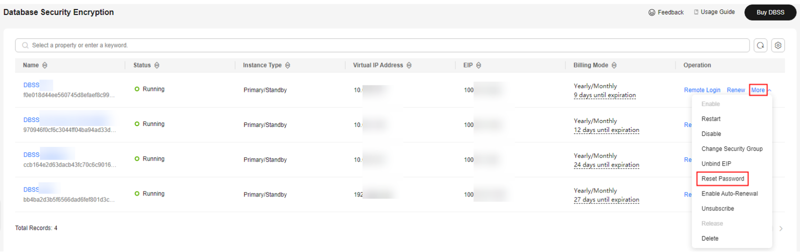
**Step 2** In the displayed dialog box, click **OK**. The EIP will be unbound from the instance.

**----End**

## Resetting a Password

**Step 1** In the **Operation** column of the target instance, choose **More** > **Reset Password**.

**Figure 15-7** Resetting the password



| Name | Status | Instance Type | Virtual IP Address | EIP | Billing Mode | Operation |
|---|---|---|---|---|---|---|
| DBSS[redacted]<br>f0e018d44ee560745d8efaef8c99... | Running | Primary/Standby | 10.[redacted] | 100.[redacted] | Yearly/Monthly<br>9 days until expiration | Remote Login Renew More |
| DBSS[redacted]<br>970946f0cf6c3044ff04ba94ad33d... | Running | Primary/Standby | 10.[redacted] | 100.[redacted] | Yearly/Monthly<br>12 days until expiration | Re |
| DBSS[redacted]<br>ccb164e2d63dacb43fc70c6c9016... | Running | Primary/Standby | 10.[redacted] | 100.[redacted] | Yearly/Monthly<br>24 days until expiration | Re |
| DBSS[redacted]<br>bb4ba2d3b5f6566dad6fef801d3c... | Running | Primary/Standby | 192.[redacted] | 100.[redacted] | Yearly/Monthly<br>27 days until expiration | Re |

Total Records: 4

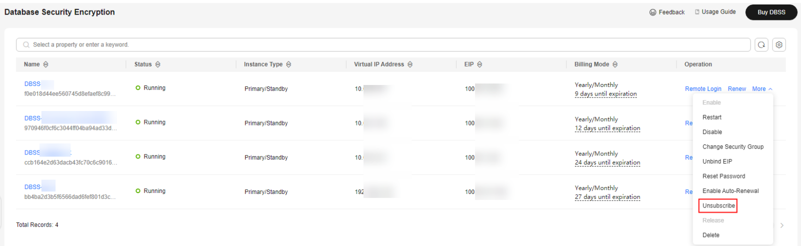
**Step 2** In the dialog box that is displayed, enter the new password and click **OK**.

**----End**

## Unsubscribing

**Step 1** In the **Operation** column of the target instance, choose **More** > **Unsubscribe**.

**Figure 15-8** Unsubscribing from an instance



Database Security Encryption

Select a property or enter a keyword.

| Name | Status | Instance Type | Virtual IP Address | EIP | Billing Mode | Operation |
|---|---|---|---|---|---|---|
| DBSS [redacted]<br>f0e018d44ee560745d8efaef8c99... | Running | Primary/Standby | 10. [redacted] | 100 [redacted] | Yearly/Monthly<br>9 days until expiration | Remote Login Renew More |
| DBSS- [redacted]<br>970946f0cf6c3044ff04ba94ad33d... | Running | Primary/Standby | 10. [redacted] | 100 [redacted] | Yearly/Monthly<br>12 days until expiration | Re |
| DBSS [redacted]<br>ccb164e2d63dacb43fc70c6c9016... | Running | Primary/Standby | 10. [redacted] | 100 [redacted] | Yearly/Monthly<br>24 days until expiration | Re |
| DBSS- [redacted]<br>bb4ba2d3b5f6566dad6fef801d3c... | Running | Primary/Standby | 192 [redacted] | 100 [redacted] | Yearly/Monthly<br>27 days until expiration | Re |

Total Records: 4

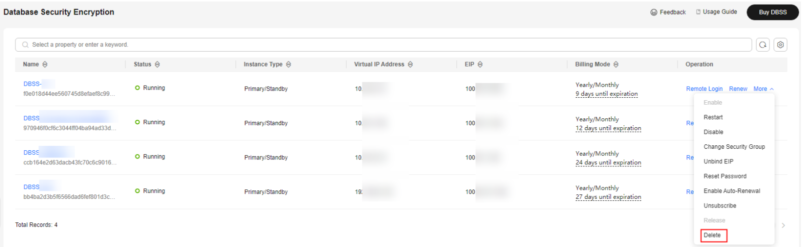
**Step 2** Confirm the unsubscription and click **Yes**.

**----End**

## Deleting

**Step 1** In the **Operation** column of the target instance, choose **More** > **Delete**.

**Figure 15-9** Deleting an instance



Database Security Encryption

Select a property or enter a keyword.

| Name | Status | Instance Type | Virtual IP Address | EIP | Billing Mode | Operation |
|---|---|---|---|---|---|---|
| DBSS- [redacted]<br>f0e018d44ee560745d8efaef8c99... | Running | Primary/Standby | 10 [redacted] | 100 [redacted] | Yearly/Monthly<br>9 days until expiration | Remote Login Renew More |
| DBSS [redacted]<br>970946f0cf6c3044ff04ba94ad33d... | Running | Primary/Standby | 10 [redacted] | 100 [redacted] | Yearly/Monthly<br>12 days until expiration | Re |
| DBSS [redacted]<br>ccb164e2d63dacb43fc70c6c9016... | Running | Primary/Standby | 10 [redacted] | 100 [redacted] | Yearly/Monthly<br>24 days until expiration | Re |
| DBSS [redacted]<br>bb4ba2d3b5f6566dad6fef801d3c... | Running | Primary/Standby | 19 [redacted] | 100 [redacted] | Yearly/Monthly<br>27 days until expiration | Re |

Total Records: 4

**Step 2** In the displayed dialog box, confirm the deletion information and click **OK**.

**----End**

# 15.3 System administrator operation guide

## 15.3.1 Platform Management

Before using database encryption and access control for the first time, you need to complete the basic configurations described in this section.

### 15.3.1.1 Configuring the Network

Configure the network interface card (NIC), DNS server, and routing policy information.

- NIC information: Configure the network IP address and gateway address. NIC information needs to be configured during **initial installation** or **network environment change**.
- DNS Server: Configure a DNS server address. If the asset is a domain name, the DNS server must be configured.
- Routing policy information: If a device has multiple NICs, configure the routing policy information based on the network plan.

⚠ CAUTION

- Configure the network information of a device based on the network environment plan. If the network configuration is incorrect, the device may fail to be accessed through a web browser. In this case, you need to directly connect to the device and reconfigure the network information.
- Before modifying route information, ensure that you understand the impact of the route modifications on the network. To avoid network disconnection, exercise caution when performing this operation.
- The NIC IP address can only be configured on this page. Do not directly modify the NIC configuration file in the background. Otherwise, the IP address of the SSH service (port 22) will be incorrectly bound.

## Prerequisites

You have obtained the network information such as the IP address to be configured for the device.

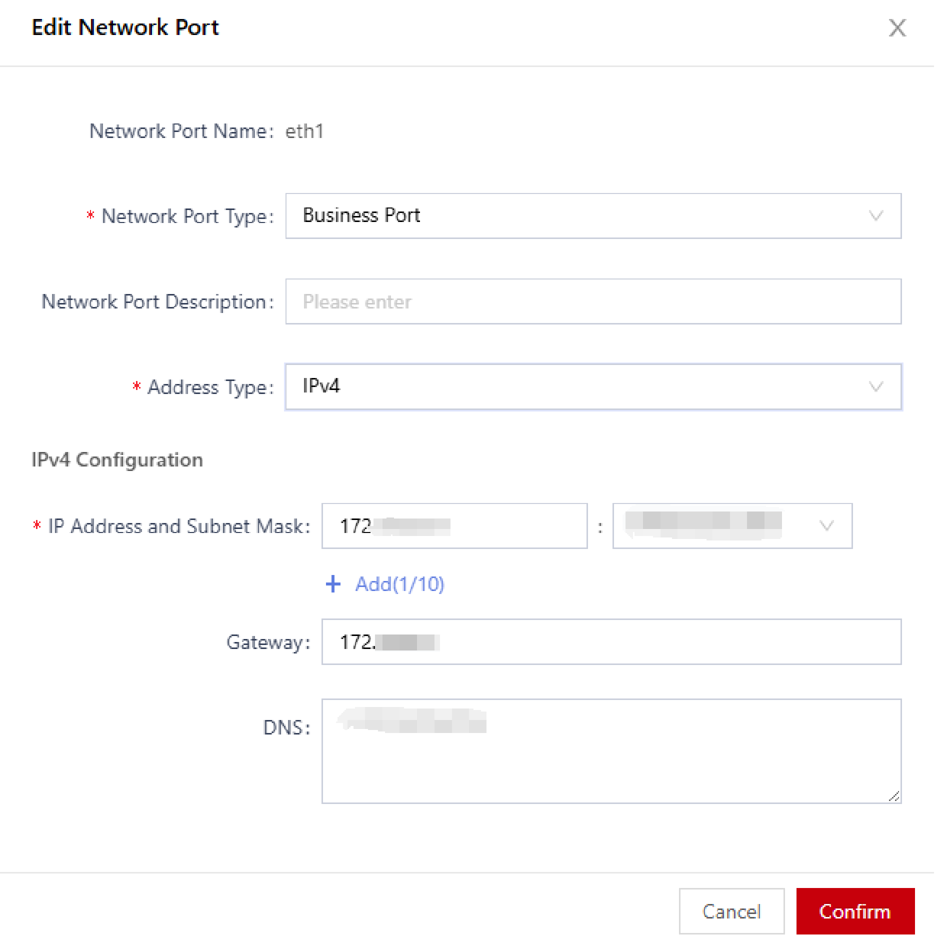
## Configuring NIC Information

**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

**Step 2** In the navigation tree on the left, choose **System Management** > **Network Management**. Go to the network port management page.

**Step 3** Click **Edit** in the **Actions** column of an NIC. The **Edit Network Port** dialog box is displayed, as shown in **Figure 15-10**.

**Figure 15-10** Editing a network port



Edit Network Port

Network Port Name: eth1

* Network Port Type: Business Port

Network Port Description: Please enter

* Address Type: IPv4

IPv4 Configuration

* IP Address and Subnet Mask: 172[redacted] : [redacted]

Gateway: 172.[redacted]

DNS: [redacted]

**Step 4** Configure NIC information. For details, see **Table 15-1**.

**Table 15-1** Configuring NIC Information

| Parameter | Description |
|---|---|
| Network Port Name | Default network port name, which cannot be changed. |
| Network Port Type | Select a network port type. The network port types are as follows:<br>● **Management Port**<br>● **Business Port** |
| Network Port Description | Enter the description as required. |

| Parameter | Description |
|---|---|
| Address Type | Select an address type. Its value can be:<br>● **Unconfigured Address**<br>● IPv4<br>● IPv6<br>● IPv4 & IPv6 |
| IP Address and Subnet Mask | **IP Address**: IP address of a device. Set it based on your network plan. It needs to communicate with data assets such as databases.<br>**Subnet Mask**: A subnet mask. Set this parameter based on your network plan. |
| Gateway | Gateway address. |
| DNS | Set the domain name server to be used. |

**Step 5** Click **Confirm**.

**----End**

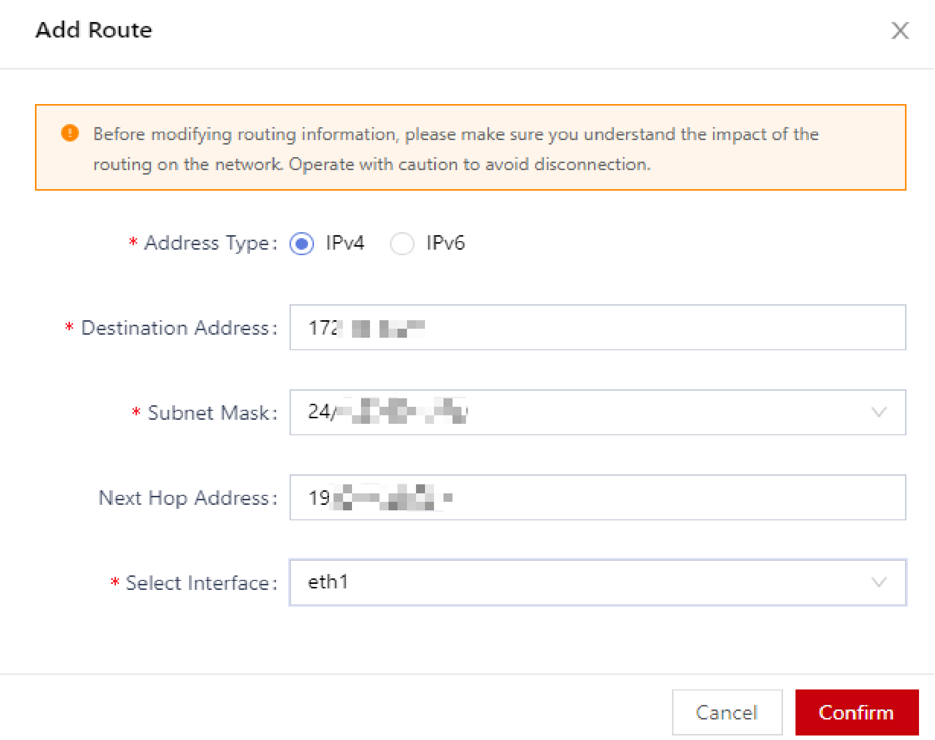
## Configuring Route Information

**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

**Step 2** In the navigation tree on the left, choose **System Management** > **Network Management**. Go to the route management page.

**Step 3** Choose **Add Route**.

**Figure 15-11** Adding a route



Add Route

Before modifying routing information, please make sure you understand the impact of the routing on the network. Operate with caution to avoid disconnection.

* Address Type: ● IPv4 ○ IPv6

* Destination Address: 172[redacted]

* Subnet Mask: 24/[redacted]

Next Hop Address: 19[redacted]

* Select Interface: eth1

**Step 4** Configure route information. For details, see **Table 15-2**.

**Table 15-2** Configuring route information

| Parameter | Description |
|---|---|
| Address Type | The options are as follows:<br>● IPv4<br>● IPv6 |
| Destination Address | IP address of the destination network. |
| Subnet Mask (IPv4) | Subnet mask of the destination IP address. |
| Prefix Length (IPv6) | Prefix length of the destination address. |
| Next Hop Address | Next hop address, which is usually the gateway address. |
| Select Interface | Manually select a NIC for sending traffic. |

**Step 5** Click **Confirm**.

**----End**

### 15.3.1.2 Upgrading the System

You can upgrade the system to a later version.

Common upgrade scenarios include:

- The old version has functionality and security issues. You need to upgrade the version to fix the issues.
- You need to upgrade to a new version to use new functions.

📖 NOTE

To perform upgrade in the two-node HA scenario, choose **System Management** > **HA Management**, disable data synchronization, disable HA on standby server B (in dual-active mode, disable HA on either of the servers), and upgrade server B. After the upgrade is successful, enable HA on server B, disable HA on server A, and then upgrade server A. After the upgrade is complete, enable HA on server A and then enable data synchronization. This step minimizes the impact on services during the HA upgrade.

## Prerequisites

If the cryptographic algorithm or key is updated in the new version, direct upgrade may cause data decryption errors. Before the upgrade, you are advised to decrypt all tables.

⚠ CAUTION

Before the upgrade, you are advised to manually back up the system configuration. For details, see **Backing Up and Restoring Configurations**.

## Procedure

**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

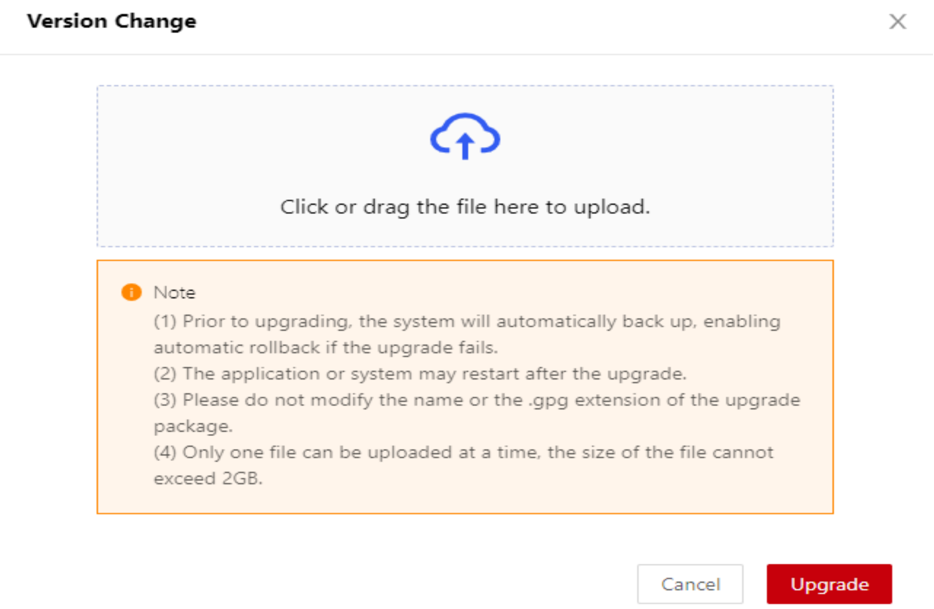
**Step 2** In the navigation pane on the left, choose **System Management** > **System O&M**.

**Step 3** Click **System Upgrade**.

**Step 4** Click **Uploading Upgrade Script**.

**Step 5** In the **Version Change** dialog box, click **Click or drag the file here to upload.** and upload the upgrade package. To obtain the upgrade package, contact technical support.

**Figure 15-12** Uploading an upgrade package



Note

(1) Prior to upgrading, the system will automatically back up, enabling automatic rollback if the upgrade fails.

(2) The application or system may restart after the upgrade.

(3) Please do not modify the name or the .gpg extension of the upgrade package.

(4) Only one file can be uploaded at a time, the size of the file cannot exceed 2GB.

**Step 6** After the upgrade is successful, view the upgrade records in the version change history.

**----End**

### 15.3.1.3 Backing Up and Restoring Configurations

Database encryption and access control support manual and automatic backup of system configuration files to facilitate data restoration in case of faults.

## Backing Up Configurations

Configuration backup involves all configurations, including system configuration, asset management, sensitive data discovery, and key management information. For disaster recovery purposes, you are advised to periodically back up system configurations.

**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

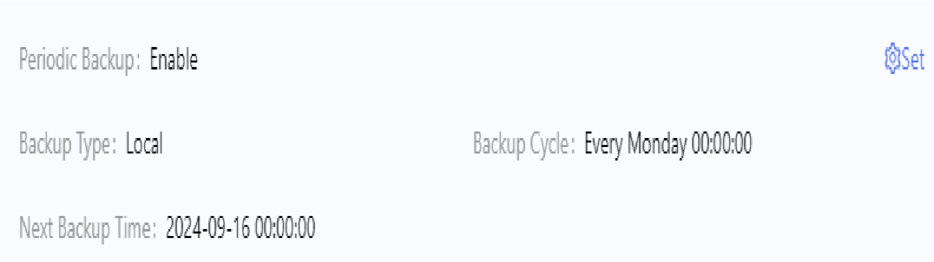
**Step 2** In the navigation tree on the left, choose **System Management** > **Backup and Restore**.

**Step 3** Click the **Backup** tab and select **Manual Backup** or **Periodic Backup**.

- Manual backup: Backup information is directly stored on the server.
  a. In the **Backup Now** area, click **Backup Now**.
  b. In the **Select Backup Method** dialog box, select a backup storage location from the drop-down list.
  c. Click **Confirm**.
- Periodic automatic backup:

a. In the **Periodic Backup** area, click **Set**.

**Figure 15-13** Configuring automatic backup



Periodic Backup: Enable

Backup Type: Local

Backup Cycle: Every Monday 00:00:00

Next Backup Time: 2024-09-16 00:00:00

b. In the **Set Periodic Backup** dialog box, configure the periodic backup information. For details about the configuration information, see **Table 15-3**.

**Table 15-3** Backup description

| Parameter | Description |
|---|---|
| Backup Type | You can select **Local backup**. |
| Backup Cycle | Backup period. The options are as follows:<br>▪ **None**: No periodic backup is performed.<br>▪ **Daily**: The data is backed up once a day.<br>▪ **Weekly**: The data is backed up once a week.<br>▪ **Monthly**: The data is backed up once a month. |
| Backup Time | Configure the backup time based on the backup period. |

c. Click **Save**.

d. In the backup file list, you can view the backup information and click ⭳ to download the backup file to the local PC.

The downloaded backup file can be used to restore the system configurations. For details, see **Restoring Configurations**.

**----End**

## Restoring Configurations

By importing a configuration file, you can restore the configurations to a backup time point. Generally, this operation is performed for fault recovery or device migration.

**Prerequisites**

- The database encryption and access control server to be restored must be in the initialized state after reinstallation, that is, there should be no data asset configured on the server.
- The configuration backup file has been generated and downloaded. For details, see **Backing Up Configurations**.

**Step 1** Log in to database encryption and access control.

**Step 2** In the navigation tree on the left, choose **System Management** > **Backup and Restore**.

**Step 3** Click the **Recovery** tab.

**Step 4** Click **Restore Now** in the upper right corner.

**Step 5** In the displayed dialog box, you can select **Local File Recovery**, enter the security password, and upload the backup file. You can also select **OBS Recovery**, enter the security password, OBS endpoint, bucket name, and backup storage path.

**Step 6** Click **Confirm**.

**----End**

### 15.3.1.4 Viewing Platform Information

When you use the product for the first time, contact technical support engineers for system authorization. You can use the product only after being authorized.

After the authorization, you can choose **System Management** > **Platform Information** to view the remaining time and validity period of the authorization. If the authorization expires, contact technical support for re-authorization.

**Table 15-4** Platform information

| Category | Parameter | Description |
|---|---|---|
| Basic Information | Product Name | Product name |
| | System Version | Product version |
| | Engine Version | Engine version |
| | System Time | System time |
| | Boot Time | Server startup time |
| Authorization Information | Machine Model | Device model |
| | Asset Count | Allowed number of assets that can be added |
| | Number of Columns Encrypted/ Recommended Maximum Encrypted Columns | Number of encrypted columns and the allowed maximum |

| Category | Parameter | Description |
|---|---|---|
| | Number of Columns Masked/ Recommended Maximum Masked Columns | Maximum number of masked columns and the current number of masked columns |
| | Bypass Plugin Count | Allowed number of bypass services |

### 15.3.1.5 Viewing HA Information

If your system is deployed in HA mode, you can choose **System Management** > **HA Management** and view HA information, including the IP addresses and virtual IP addresses (VIP addresses) of the active and standby nodes, running time of the active and standby nodes, and metrics.

For a single server group deployed in HA mode and having data assets, pay attention to the following:

- If a VIP address is added, you need to manually change the proxy addresses of all existing data sources to the VIP address.
- If the VIP address is set to the original physical IP address of the single-node system during HA configuration, you do not need to change the proxy address of each data source.

NOTE

To perform upgrade in the two-node HA scenario, choose **System Management** > **High Availability**, disable data synchronization, disable HA on standby server B (in dual-active mode, disable HA on either of the servers), and upgrade server B. After the upgrade is successful, enable HA on server B, disable HA on server A, and then upgrade server A. After the upgrade is complete, enable HA on server A and then enable data synchronization. This step minimizes the impact on services during the HA upgrade.

## 15.3.2 Changing the Security Password

To protect keys, the system verifies the security password before users create, edit, or modify a key. For system security purposes, keep the password secure. This section describes how to change it.

During operations such as key initialization, the default security password message is displayed. You are advised to change the default password before using the device. You are also advised to periodically change the security password.

To obtain the default password, **submit a service ticket**.

### Procedure

**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

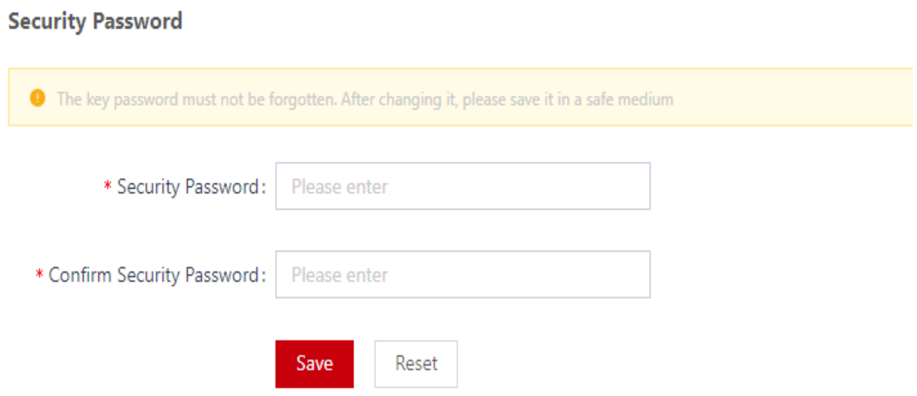
**Step 2** In the navigation tree on the left, choose **System Management** > **System Settings**. On the displayed **General Settings** page, click **Secure Password Setting**. The **Security Password** page is displayed.

**Step 3** Click **Security Password**.

**Step 4** Enter a new security password in the text box and click **Save**.

Properly keep the password. After changing the password, save it in a secure medium.

**Figure 15-14** Changing the security password



Security Password

The key password must not be forgotten. After changing it, please save it in a safe medium

* Security Password: Please enter

* Confirm Security Password: Please enter

**Step 5** In the **Password Verification** text box, enter the old security password and click **Confirm**.

**----End**

## 15.3.3 Initializing a Key

Before using encryption for the first time, you need to initialize keys.

Keys for database encryption and access control include root keys (RKs), data source keys (DSKs), and data encryption keys (DEKs). For details, see **Initializing a Key**.

**Table 15-5** Key types

| Type | Description |
|---|---|
| Root key (RK) | Generated after a key is initialized. It is not exposed externally. |
| Data source key (DSK) | Generated when a data source is added. It is encrypted by RK for storage. |
| Data encryption key (DEK) | Generated during initialization when an encryption task is added. It is encrypted by DSK for storage. |

## Procedure

**Step 1** Log in to database encryption and access control.

**Step 2** In the navigation pane on the left, choose **Key Management** > **Key Configuration**.

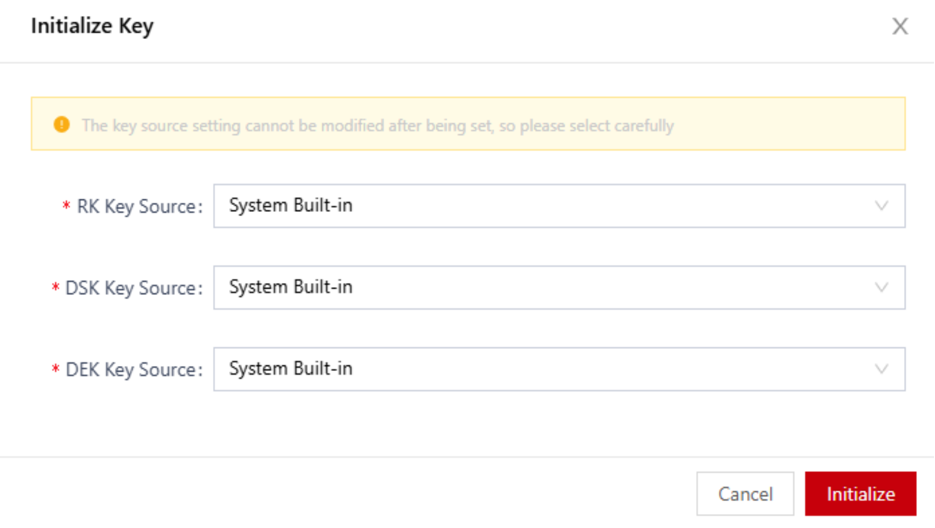
**Step 3** Click **Initialize Key**. In the displayed dialog box, enter the security password and click OK.

**Step 4** In the password verification dialog box, enter the security password and click **Confirm**.

For details about how to change the security password, see **Changing the Security Password**.

**Step 5** In the **Initialize Key** dialog box, set the key sources. For details about the parameters, see **Table 15-6**.

**Figure 15-15** Initializing a key



Initialize Key

The key source setting cannot be modified after being set, so please select carefully

* RK Key Source: System Built-in

* DSK Key Source: System Built-in

* DEK Key Source: System Built-in

**Table 15-6** Initializing a key

| Parameter | Description |
|---|---|
| RK Key Source | RK source. The following sources are supported:<br>- **System Built-in**: fixed key built in the system, which is used only for tests.<br>- **KEY_Service**: key platform connected to the system. For details about how to configure a key platform, see **Interconnecting with KMS**.<br>After the configuration, select a platform vendor.<br>**NOTE**<br>KMS requires the KMS CMKFullAccess permission. |

| Parameter | Description |
|---|---|
| DSK Key Source | DSK source. The following sources are supported:<br>● **System Built-in**: fixed key built in the system, which is used only for tests.<br>● **KEY_Service**: key platform connected to the system. For details about how to configure the key platform, see **Interconnecting with KMS**.<br>After the configuration, select a platform vendor.<br>**NOTE**<br>KMS requires the KMS CMKFullAccess permission. |
| DEK Key Source | DEK source. The following sources are supported:<br>● **System Built-in**: fixed key built in the system, which is used only for tests.<br>● **KEY_Service**: key platform connected to the system. For details about how to configure the key platform, see **Interconnecting with KMS**.<br>After the configuration, select a platform vendor.<br>**NOTE**<br>KMS requires the KMS CMKFullAccess permission. |

**Step 6** Click **Initialize**.

**----End**

## 15.3.4 Adding Data Assets

After data assets (databases) are added to the system, you can identify, encrypt, decrypt, and mask sensitive data in the databases.

This section uses the MySQL database as an example. Add data assets based on the site requirements.

### Constraint

**Table 15-7** Data sources and versions that can be managed by database encryption

| Database | Version |
|---|---|
| MySQL | 5.5, 5.6, 5.7, 8.0, 8.0.13+ |
| Oracle | 11.1, 11.2, 12c, 19c |
| SQLServer | 2012, 2016 |
| PostgreSQL | 9.4, 11.5 |
| DM | 6, 7.6, 8.1 |
| Kingbase | V8 R3, V8 R6 |

| Database | Version |
|---|---|
| MariaDB | 10.2 |
| GaussDB | A |
| TDSQL | 5.7 |
| TBASE | V2.15.17.3 |
| RDS_MYSQL | 5.6, 5.7, 8.0 |
| RDS_PostgreSQL | 11 |
| HotDB | 2.5.6 |
| HighGO | 4.5 |
| DWS | 8.1 |

**Table 15-8** Database account permissions for database encryption

| Database | System Catalog Requiring the SELECT Permission | Database Account Permission |
|---|---|---|
| MySQL | mysql.user<br>performance_schema.* | select<br>insert<br>create<br>update<br>delete<br>drop<br>alter<br>index |
| RDS_MYSQL | mysql.user<br>performance_schema.* | select<br>insert<br>create<br>update<br>delete<br>drop<br>alter<br>index |

| Database | System Catalog Requiring the SELECT Permission | Database Account Permission |
|---|---|---|
| TDSQL | mysql.user<br>performance_schema.* | select<br>insert<br>create<br>update<br>delete<br>drop<br>alter<br>index |
| MariaDB | mysql.user<br>performance_schema.* | select<br>insert<br>create<br>update<br>delete<br>drop<br>alter<br>index |
| DM | SYS.ALL_SUBPART_KEY_COLUMNS<br>SYS.ALL_USERS<br>SYS.ALL_CONS_COLUMNS<br>SYS.ALL_CONSTRAINTS<br>SYS.ALL_TABLES<br>SYS.ALL_TABLE_COLUMNS<br>SYS.ALL_COL_COMMENTS<br>SYS.ALL_PART_KEY_COLUMNS<br>SYS.ALL_IND_COLUMNS<br>SYS.ALL_INDEXS<br>V$VERSION<br>V$LOCK<br>SYS.DBMS_LOB<br>SYS.DBMS_METADATA | The user role must be **dba**. |

| Database | System Catalog Requiring the SELECT Permission | Database Account Permission |
|---|---|---|
| postgreSQL | pg_catalog.pg_class<br>pg_catalog.pg_index<br>pg_catalog.pg_user<br>pg_catalog.pg_indexes<br>information_schema.columns<br>information_schema.sequences<br>information_schema.tables<br>pg_catalog.pg_sequence | The user must be the table owner or the **dba** role. |
| RDS_PostgreSQL | pg_catalog.pg_class<br>pg_catalog.pg_index<br>pg_catalog.pg_user<br>pg_catalog.pg_indexes<br>information_schema.columns<br>information_schema.sequences<br>information_schema.tables<br>pg_catalog.pg_sequence | The user must be the table owner or the **dba** role. |
| TBASE | pg_catalog.pg_class<br>pg_catalog.pg_index<br>pg_catalog.pg_user<br>pg_catalog.pg_indexes<br>information_schema.columns<br>information_schema.sequences<br>information_schema.tables<br>pg_catalog.pg_sequence | The user must be the table owner or the **dba** role. |
| GAUSSDB | pg_catalog.pg_class<br>pg_catalog.pg_index<br>pg_catalog.pg_user<br>pg_catalog.pg_indexes<br>information_schema.columns<br>information_schema.sequences<br>information_schema.tables<br>pg_catalog.pg_sequence | The user must be the table owner or the **dba** role. |

| Database | System Catalog Requiring the SELECT Permission | Database Account Permission |
|---|---|---|
| Kingbase 8.6 (pg) | pg_catalog.pg_class<br>pg_catalog.pg_index<br>pg_catalog.pg_user<br>pg_catalog.pg_indexes<br>information_schema.columns<br>information_schema.sequences<br>information_schema.tables<br>pg_catalog.pg_sequence<br>pg_catalog.pg_matviews | The user must be the table owner or the **dba** role. |
| KINGBASE 8.3 | sys_catalog.sys_class<br>sys_catalog.sys_index<br>sys_catalog.sys_user<br>sys_catalog.sys_indexes<br>information_schema.columns<br>information_schema.sequences<br>information_schema.tables<br>sys_catalog.sys_sequence<br>sys_catalog.sys_matviews | The user must be the table owner or the **dba** role. |
| Oracle | SYS.ALL_SUBPART_KEY_COLUMNS<br>SYS.DUAL<br>SYS.ALL_USERS<br>SYS.ALL_CONS_COLUMNS<br>SYS.ALL_CONSTRAINTS<br>SYS.ALL_TABLES<br>SYS.ALL_TABLE_COLUMNS<br>SYS.ALL_COL_COMMENTS<br>SYS.ALL_PART_KEY_COLUMNS<br>SYS.ALL_IND_COLUMNS<br>SYS.ALL_INDEXS<br>SYS.V_$INSTANCE<br>SYS.DBMS_LOB<br>SYS.DBMS_METADATA<br>DBA_TABLES<br>DBA_TAB_COLS | The user role must be **dba**. |

| Database | System Catalog Requiring the SELECT Permission | Database Account Permission |
|---|---|---|
| SQLserver | sys.tables<br>sys.indexes<br>sys.index_columns<br>sys.default_constraints<br>sys.systypes<br>sys.extended_properties<br>sys.foreign_key_columns<br>sys.check_constraints<br>sys.foreign_keys<br>sys.columns<br>sys.objects<br>sys.all_columns<br>sys.types<br>sys.syslogins<br>sys.all_objects<br>sys.schemas<br>sys.key_constraints<br>sys.computed_columns<br>sys.triggers<br>sys.partition_schemes<br>sys.dm_sql_referencing_entities | schemaSelect<br>schemaInsert<br>schemaUpdate<br>schemaAlter<br>createTable<br>VIEW SERVER STATE<br>SELECT permission of the encrypted table<br>INSERT permission of the encrypted table<br>ALTER permission of the encrypted table |
| HighGO | pg_catalog.pg_class<br>pg_catalog.pg_index<br>pg_catalog.pg_user<br>pg_catalog.pg_indexes<br>information_schema.columns<br>information_schema.sequences<br>information_schema.tables<br>pg_catalog.pg_sequence | The user must be the table owner or the **dba** role. |
| DWS | pg_catalog.pg_class<br>pg_catalog.pg_index<br>pg_catalog.pg_user<br>pg_catalog.pg_indexes<br>information_schema.columns<br>information_schema.sequences<br>information_schema.tables<br>pg_catalog.pg_sequence | The user must be the table owner or the **dba** role. |

## Procedure

**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation pane, choose **Assets Management** > **Data Source Management**.

**Step 3** Click **Add Data Source** in the upper right corner.

**Step 4** In the **Add Data Source** dialog box, configure asset information. For details, see Table 15-9.

**Table 15-9** Parameters for adding a data source

| Parameter | Description |
|---|---|
| **Database Information** | |
| Data Source | Customized data asset name. |
| Data Source Type | Select a database type from the drop-down list box. For details about supported database versions, see **Constraint**. |
| Data Source Version | Select a database version from the drop-down list box. |
| Read/Write Separation/RAC | If the database is deployed in read/write isolation mode, select this option and configure information about the secondary database node. |
| Data Source Address | IP address of the database. |
| Data Source Port | Connection port of the database. |
| Proxy Address | Select a proxy address from the drop-down list box, that is, the IP address for accessing and controlling the database. |
| Proxy Port | Set a proxy port. O&M personnel access the database through the proxy IP address and proxy port.<br>● The value range is 1025 to 65535.<br>● You can set any idle port within the range. Ports that have been used by other data assets cannot be used. For example, if data asset A uses port 14000, data asset B cannot use this port.<br>You can click **Auto Assign** to let the system automatically assign idle proxy ports. |
| Database/Instance/SID/Service/Schema | Set the database, instance name, SID, service name, or schema. |

| Parameter | Description |
|---|---|
| Database Account | Database login user. |
| Database Password | Password for logging in to the database. |
| **Encryption Parameters** | |
| Encryption Mode | ● Asset encryption mode. The options are as follows:<br>– **One Key Per Asset**: The DEKs of assets are the same. Connection query and cross-database query are supported.<br>– **One Key Per Column**: The DEKs of assets are different. Join query and cross-database query are not supported. |
| Default Display without Permission | ● Set what is displayed to the users who do not have the permissions to access the database. The options are as follows:<br>– **Ciphertext**: Ciphertext is displayed. The encoding format is Base64 or hexadecimal. For details, see **Setting Encryption Parameters**.<br>– **Default Data**: Default data is displayed. You need to set the default data of the string type.<br>– NULL: The content is blank. |
| **(Optional) Host Information**<br>After the monitoring threshold is configured, the system encrypts data in batches only within the monitoring threshold of the database server. If the resource usage exceeds the threshold, the system stops encrypting data to reduce the impact on services. You are advised to set the following parameters if possible. | |
| Host IP | Host IP address. |
| Host Port | SSH service port of the host. The default SSH service port is 22. |
| Username | Username for logging in to the host. |
| Password | Password for logging in to the host. |
| Character Set | Character set used by the host, which is automatically obtained after the host is connected. |
| Host Operating System | Host OS, which is automatically obtained after the host is connected. |
| Kernel | Host kernel, which is automatically obtained after the host is connected. |

| Parameter | Description |
|---|---|
| Monitoring Threshold | Thresholds for host monitoring metrics (CPU, memory, I/O, and network). The system encrypts database data only within the threshold to reduce the impact on services. |
| **Log Information** | |
| Database Log File Name | Path and name of the database log file. Example: **/usr/local/mysql/binlogs/mysql-bin.000060** |

**Step 5** (Optional) After the configuration is complete, click **Test Database Connection** and check whether the database can be connected.

**Step 6** (Optional) Click **Test Account Permission** to check whether the database account permission meets the encryption requirements.

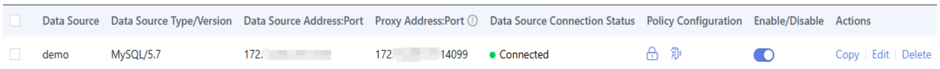
If the database account permission does not meet the encryption requirements, configure the database account permission by referring to **Table 15-8**.

**Step 7** (Optional) If the host information is configured, click **Test Host Connection**. Check whether the host can be connected and whether its character set and OS can be automatically obtained.

**Step 8** Click **Save** to save the data asset configuration.

After the asset is added, you can view its information in the data source list, as shown in **Figure 15-16**.

**Figure 15-16** Data source list



| □ | Data Source | Data Source Type/Version | Data Source Address:Port | Proxy Address:Port | Data Source Connection Status | Policy Configuration | Enable/Disable | Actions |
|---|---|---|---|---|---|---|---|---|
| □ | demo | MySQL/5.7 | 172.[redacted] | 172[redacted]14099 | ● Connected | 🔒 | ● | Copy \| Edit \| Delete |

**Step 9** In the list, click ○ to enable the database proxy.

After this function is enabled, you can access the database through the proxy IP address and proxy port.

**----End**

## Related Operations

- Click 🔒 in the **Policy Configuration** column of the data source list. The encryption task configuration page is displayed. You are advised to identify sensitive data before configuring an encryption task. For details, see **Scanning Sensitive Data in Assets**.
- Click in the **Policy Configuration** column of the data source list. The masking rule configuration page is displayed. You are advised to identify sensitive data before configuring a masking rule. For details, see **Scanning Sensitive Data in Assets**.
- Click **Edit** in the **Actions** column of the data source list to modify data asset information.

- Click **Delete** in the **Actions** column of the data source list to delete unnecessary data assets.

  NOTE

  If a message is displayed, indicating that the table structure of the current database is not rolled back, perform the operations in **Rolling Back the Table Structure** or **Configuring a Decryption Task** based on site requirements.

## 15.3.5 Service Test and Analysis

Before encryption, you are advised to test the database to check whether the SQL statements used in services can be used in the encryption environment. In this way, service errors that may be result from encryption can be eliminated, reducing service test costs. After data is encrypted, the data will be changed from Chinese characters, English letters, or numbers to hexadecimal strings. As a result, some SQL statements that can be executed before may fail to be executed after data encryption.

For example, fuzzy query of strings, calculation of values, and range search may fail.

Before encryption, analyze the SQL statements run by users to determine whether tables can be encrypted.

- Abnormal SQL statements: SQL statements that cannot be parsed, for example, incorrect SQL statements or SQL statements that are too complex to be parsed.
- Blocked SQL statements: SQL statements that are not supported by database encryption and access control.

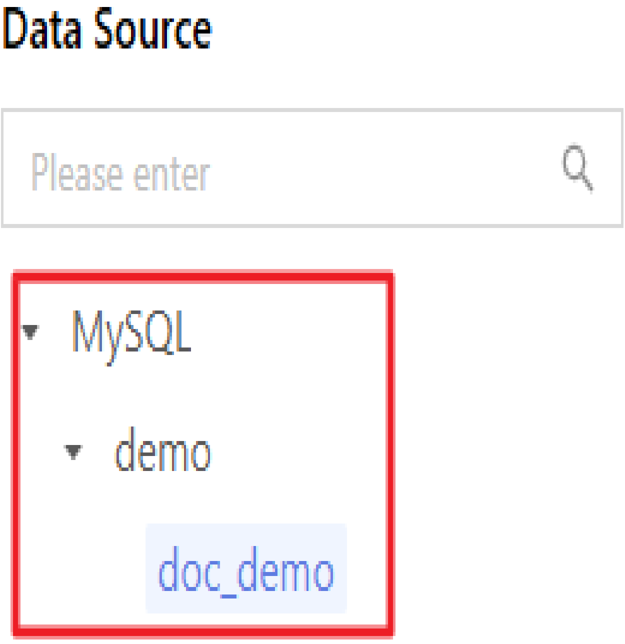
### Procedure

**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

**Step 2** Create a service analysis task.

1. In the navigation tree on the left, choose **Service Test** > **Service Analysis**.
2. In the data source area on the left, click a data source.

**Figure 15-17** Selecting a data source



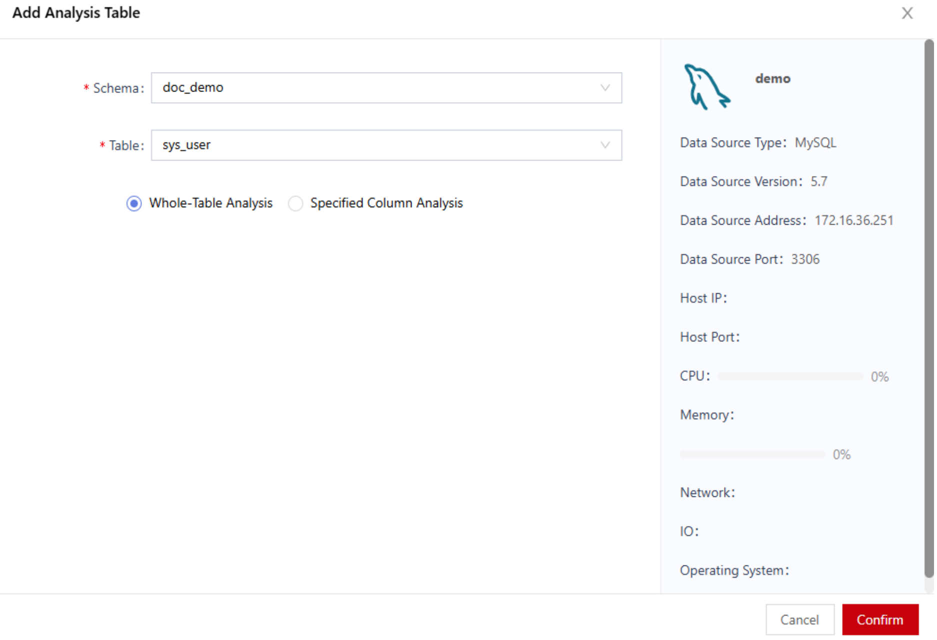
Data Source

Please enter

- MySQL
  - demo
    - doc_demo

3. Click **Add Analysis Table**, configure a table, and click **OK**.

**Figure 15-18** Adding a table



Add Analysis Table

* Schema: doc_demo

* Table: sys_user

● Whole-Table Analysis ○ Specified Column Analysis

demo

Data Source Type: MySQL

Data Source Version: 5.7

Data Source Address: 172.16.36.251

Data Source Port: 3306

Host IP:

Host Port:

CPU: 0%

Memory: 0%

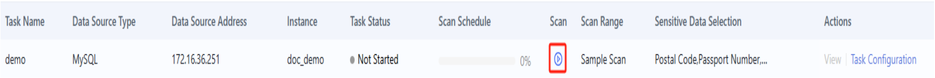
Network:

IO:

Operating System:

4. Click the icon in the **Start** column of the table.

**Figure 15-19** Start



| Task Name | Data Source Type | Data Source Address | Instance | Task Status | Scan Schedule | Scan | Scan Range | Sensitive Data Selection | Actions |
|---|---|---|---|---|---|---|---|---|---|
| demo | MySQL | 172.16.36.251 | doc_demo | ● Not Started | 0% | ▷ | Sample Scan | Postal Code,Passport Number,... | View \| Task Configuration |

**Step 3** Use the proxy address to access the database and run a SQL statement.

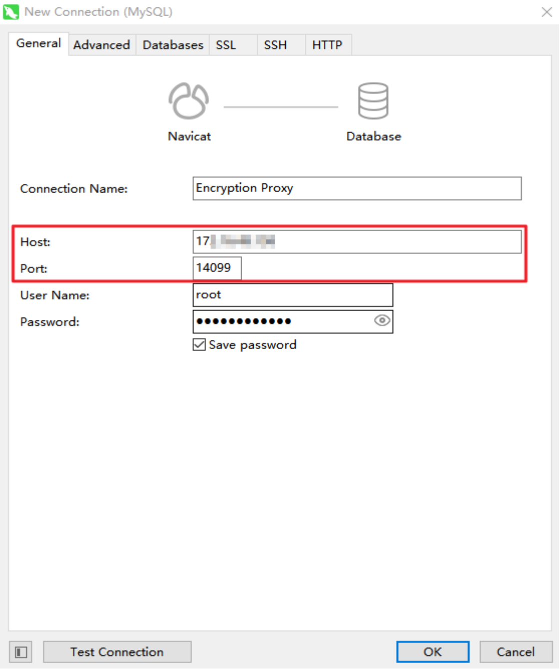
1. Choose **Asset Management** > **Data Source Management** and obtain the proxy address.

   The IP address is that of database encryption and access control, and the proxy port is that configured when the data asset is added.

2. Configure the access proxy address on the database tool and connect to the database.

   For details about the host and port number, see the preceding steps. Set the username and password based on site requirements. The following figure is only an example. Configure the proxy access connection based on the specific database tool.

   **Figure 15-20** Configuring the proxy address

   Connection Name: Encryption Proxy

   Host: 17[redacted]

   Port: 14099

   User Name: root

   Password: ●●●●●●●●●●●●

   ☑ Save password

3. Run an abnormal SQL statement on the database tool.

   For example, run the following statements:

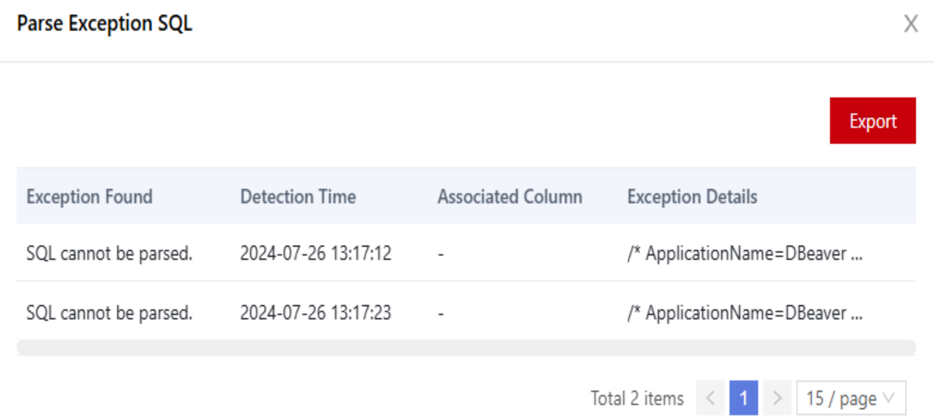
   **Table 15-10** Exception examples

   | Type | Statement |
   |---|---|
   | Abnormal SQL statement | select * fform table |
   | Blocked SQL statement | RENAME TABLE sys_user to abc |

**Step 4** View the logs of the abnormal SQL statements on the web console.

1. In the navigation tree on the left, choose **Service Test** > **Service Analysis**.
2. In the data source area on the left, click a data source.
3. Click **Parse Exception SQL** to view the abnormal SQL statements.

**Figure 15-21** Abnormal SQL statements



Parse Exception SQL

Export

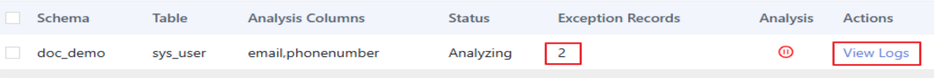
| Exception Found | Detection Time | Associated Column | Exception Details |
|---|---|---|---|
| SQL cannot be parsed. | 2024-07-26 13:17:12 | - | /* ApplicationName=DBeaver ... |
| SQL cannot be parsed. | 2024-07-26 13:17:23 | - | /* ApplicationName=DBeaver ... |

Total 2 items 1 15 / page

**Step 5** On the web console, view the analysis results of blocked SQL statements.

1. In the navigation tree on the left, choose **Service Test** > **Service Analysis**.
2. In the data source area on the left, click a data source.
3. You can view the number of abnormal records in the list.

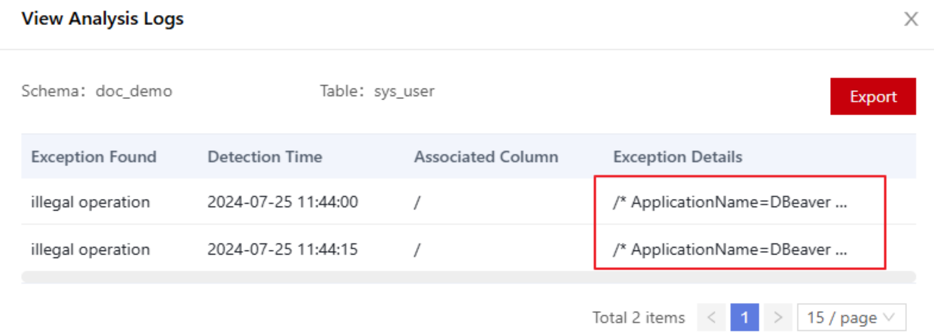
**Figure 15-22** Viewing the number of blocked SQL statements



| □ | Schema | Table | Analysis Columns | Status | Exception Records | Analysis | Actions |
|---|---|---|---|---|---|---|---|
| □ | doc_demo | sys_user | email,phonenumber | Analyzing | 2 | ⊙ | View Logs |

4. Click **View Log** to view the records of blocked SQL statements.

**Figure 15-23** Viewing blocked SQL statements



View Analysis Logs

Schema: doc_demo Table: sys_user

Export

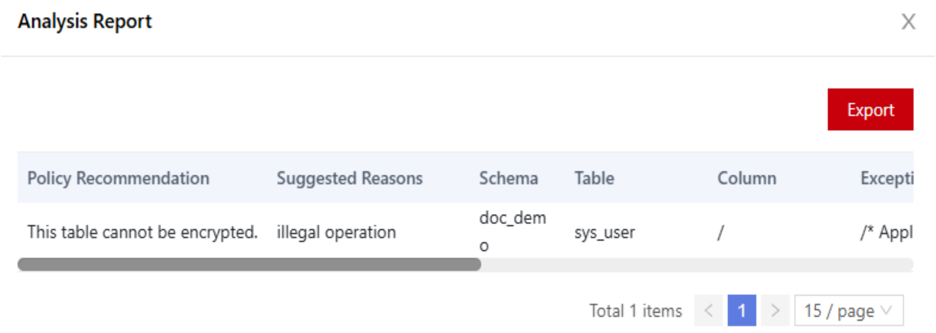
| Exception Found | Detection Time | Associated Column | Exception Details |
|---|---|---|---|
| illegal operation | 2024-07-25 11:44:00 | / | /* ApplicationName=DBeaver ... |
| illegal operation | 2024-07-25 11:44:15 | / | /* ApplicationName=DBeaver ... |

Total 2 items 1 15 / page

5. Click **Analysis Report** to view the encryption suggestions of the table.

   As shown in **Figure 15-24**, if you have renamed a database table, you are not advised to encrypt the table.

**Figure 15-24** Analysis and suggestions



Analysis Report

| Policy Recommendation | Suggested Reasons | Schema | Table | Column | Excepti |
|---|---|---|---|---|---|
| This table cannot be encrypted. | illegal operation | doc_demo | sys_user | / | /* Appl |

**----End**

# 15.3.6 Sensitive Data Discovery

## 15.3.6.1 Scanning Sensitive Data in Assets

A sensitive data discovery task automatically obtains sensitive data table information in data assets.

### Procedure

**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation tree on the left, choose **Sensitive Data Discovery** > **Sensitive Data Scanning**.

**Step 3** Find the target data asset and click **Task Configuration**. In the **Task Configuration** dialog box, set a sensitive data discovery task.

**Table 15-11** Parameters for a sensitive data discovery task

| Parameter | Description |
|---|---|
| Sample Count | Set the number of scanned samples.<br>Sampling scanning refers to extracting a certain amount of data from a dataset for identification. The more samples, the more accurate the recognition. The fewer samples, the faster the scanning speed. |
| Maximum Number of Threads | Set the maximum number of threads used by a task.<br>The sensitive data discovery task can use multiple threads. The more threads, the higher the scanning efficiency and the more device resources. |

| Parameter | Description |
|---|---|
| Select Schemas | Select the database schema to be encrypted.<br>In the **Available Schemas** area on the left, select the target mode and click **>** to move the mode to the selected mode. |
| Select Table | After a schema is selected, all tables in the schema are automatically selected. If you select only a single schema, you can adjust the number of tables in the schema as required.<br>If some tables do not need to be scanned, select the target objects in the selected tables on the right and click **<** to move the target objects to available tables. |
| Sensitive Data Selection | Select an industry template from the drop-down list box. After you select an industry template, the system scans the data types set in the template.<br>The system has built-in common industry templates. You can also customize industry templates. For details, see **Adding an Industry Template**.<br>If you select do not use a template, manually set the types of data to be scanned in **Data Types to Discover** module. |
| Data Types to Discover | Manually select the types of data to be scanned.<br>This parameter is available only when **Sensitive Data Selection** is set to no template. |

**Step 4** Click **Save**.

**Step 5** Find the target data asset and click ▷ to execute the sensitive data discovery task. After the execution starts, the system automatically scans and identifies sensitive data. The scan duration depends on the amount of data to be scanned. The larger the amount of data, the longer the scan duration. You can view the scan progress on the page. After the execution is complete, the **Task Status** is **Scan Finished**.

**----End**

## 15.3.6.2 Viewing the Execution Result of a Scan Task

After a sensitive data discovery task is executed, the system scans and identifies sensitive data in data assets. You can view the sensitive data in the execution result.

## Procedure

**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

**Step 2** In the navigation tree on the left, choose **Sensitive Data Discovery** > **Sensitive Data Scanning**.

**Step 3** (Optional) Set search criteria and click search icon to query specified data assets.

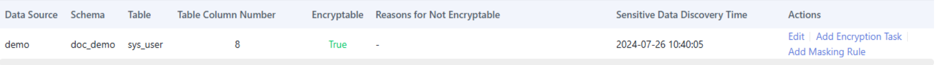
**Step 4** Find the target data asset and click **View**.

**Step 5** On the scan result page, view all scan results.

**Table 15-12** Scan result

| Parameter | Description |
|---|---|
| Data Source | Name of the data asset where sensitive information is located. |
| Schema | Mode of sensitive information. |
| Table | Name of the table or view where sensitive information is stored. |
| Table Column Number | Number of columns in a database table. |
| Encryptable | Whether the database table supports encryption. |
| Reasons for Not Encryptable | If the table cannot be encrypted, the system displays the reason why the table cannot be encrypted. |
| Sensitive Data Discovery | Time when sensitive data is discovered. |

**Figure 15-25** Scan result

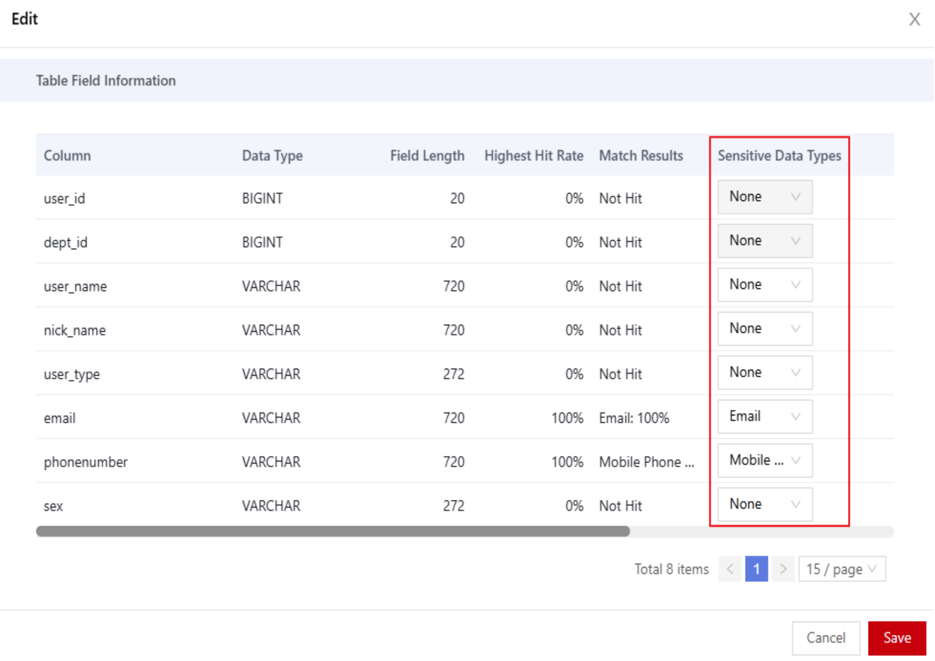


| Data Source | Schema | Table | Table Column Number | Encryptable | Reasons for Not Encryptable | Sensitive Data Discovery Time | Actions |
|---|---|---|---|---|---|---|---|
| demo | doc_demo | sys_user | 8 | True | - | 2024-07-26 10:40:05 | Edit \| Add Encryption Task \| Add Masking Rule |

**Step 6** For a database table, you can click **Edit** to view the table field information.

As shown in **Figure 15-26**, the column information and the sensitive data types are displayed in the **Table Field Information**. If the scanning result does not match the actual situation, you can modify the sensitive data type information.

**Figure 15-26** Editing table field information



Edit

Table Field Information

| Column | Data Type | Field Length | Highest Hit Rate | Match Results | Sensitive Data Types |
|---|---|---|---|---|---|
| user_id | BIGINT | 20 | 0% | Not Hit | None |
| dept_id | BIGINT | 20 | 0% | Not Hit | None |
| user_name | VARCHAR | 720 | 0% | Not Hit | None |
| nick_name | VARCHAR | 720 | 0% | Not Hit | None |
| user_type | VARCHAR | 272 | 0% | Not Hit | None |
| email | VARCHAR | 720 | 100% | Email: 100% | Email |
| phonenumber | VARCHAR | 720 | 100% | Mobile Phone ... | Mobile ... |
| sex | VARCHAR | 272 | 0% | Not Hit | None |

**----End**

### 15.3.6.3 Creating an Encrypted Task in the Result

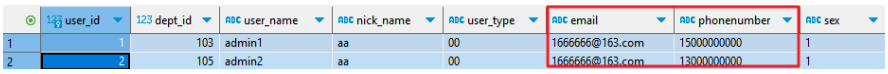
You can create an encryption task based on the sensitive data discovery result. This section describes how to create an encryption task in the result.

Before configuring the encryption task, you are advised to perform a simulated encryption test to check whether any problem occurs during the process. Rectify the fault.

You can also create an encryption task in data encryption module. For details, see **Configuring an Encryption Task**.

Before the encryption, the data table information is plaintext information, as shown in **Figure 15-27**.

**Figure 15-27** Query result before encryption



| | user_id | dept_id | user_name | nick_name | user_type | email | phonenumber | sex |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 103 | admin1 | aa | 00 | 1666666@163.com | 15000000000 | 1 |
| 2 | 2 | 105 | admin2 | aa | 00 | 1666666@163.com | 13000000000 | 1 |

## Prerequisites

Before creating an encrypted task, you have created a key.

## Creating an Encryption Task

**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

**Step 2** In the navigation tree on the left, choose **Sensitive Data Discovery** > **Sensitive Data Scan**.

**Step 3** On the scan task list page, locate the target data asset and click **View**.

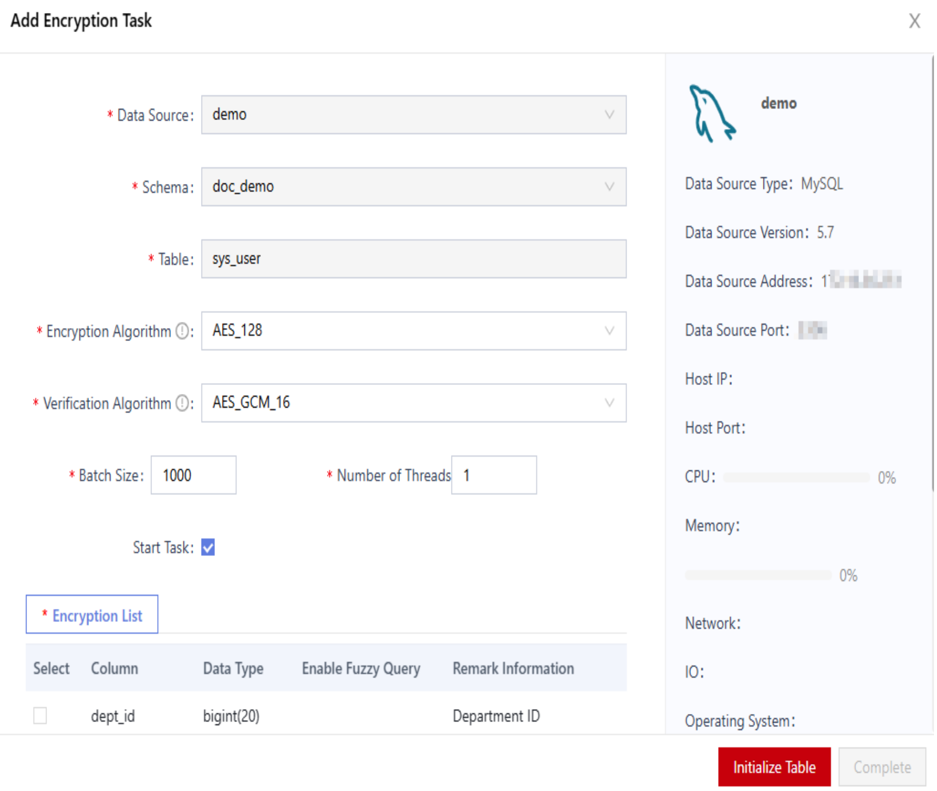
**Step 4** On the scan result page, locate the target database table and click **Add Encryption Task**.

**Step 5** In the displayed dialog box, set encryption information. **Table 15-13** describes the configuration information.

**Table 15-13** Adding an encrypted task

| Parameter | Description |
|---|---|
| Data Source | Name of a data asset. |
| Schema | Name of the schema of the asset. |
| Table | Name of the table of an asset. |
| Encryption Algorithm | Select an encryption algorithm from the drop-down list box.<br>You can view the supported algorithm types on the **Checking the Encryption Algorithm** page. |
| Verificatio n Algorithm | Select a verification algorithm from the drop-down list.<br>The verification algorithm is used to verify the integrity of important data. You can view the supported algorithm types on the **Checking the Encryption Algorithm** page. |
| Batch Size | The amount of data processed by each batch of encryption task. |
| Number of Threads | Number of threads occupied by the encryption task. |
| Start Task | If this parameter is selected, the task is automatically started after being created. |

**Figure 15-28** Adding an encrypted task



Add Encryption Task

* Data Source: demo

* Schema: doc_demo

* Table: sys_user

* Encryption Algorithm: AES_128

* Verification Algorithm: AES_GCM_16

* Batch Size: 1000 * Number of Threads 1

Start Task: ☑

* Encryption List

| Select | Column | Data Type | Enable Fuzzy Query | Remark Information |
|---|---|---|---|---|
| □ | dept_id | bigint(20) | | Department ID |

demo

Data Source Type: MySQL

Data Source Version: 5.7

Data Source Address: 1[redacted]

Data Source Port: [redacted]

Host IP:

Host Port:

CPU: 0%

Memory: 0%

Network:

IO:

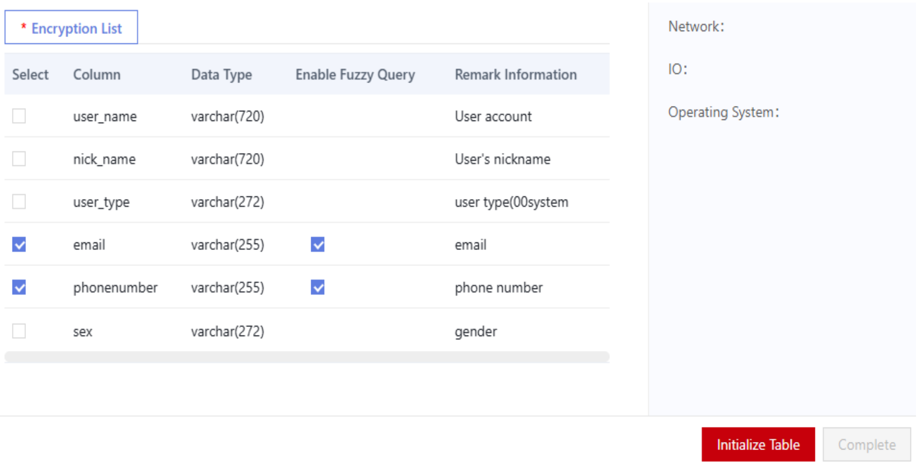
Operating System:

**Step 6** Click the **Encryption List** tab, select columns to be encrypted, and set whether to enable fuzzy search.

After encryption, fuzzy search cannot be performed by default. If the following conditions are met, select **Enable Fuzzy Search**. Fuzzy search supports **%** and _.

- The ciphertext is encoded in hexadecimal format and does not support BASE64 encoding. For details, see **Setting Encryption Parameters**.
- The field is of the string type (varchar). Other types are not supported.

**Figure 15-29** Selecting encrypted column



* Encryption List

| Select | Column | Data Type | Enable Fuzzy Query | Remark Information |
|---|---|---|---|---|
| □ | user_name | varchar(720) | | User account |
| □ | nick_name | varchar(720) | | User's nickname |
| □ | user_type | varchar(272) | | user type(00system |
| ☑ | email | varchar(255) | ☑ | email |
| ☑ | phonenumber | varchar(255) | ☑ | phone number |
| □ | sex | varchar(272) | | gender |

Network:

IO:

Operating System:

**Step 7** Click **Initialize Table** to initialize the data table.

**Step 8** Click **Complete**.

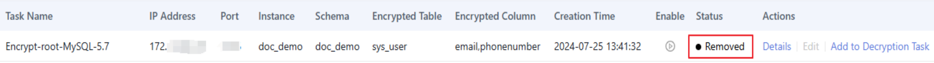
**----End**

## Upgrade Verification

**Step 1** After the encryption task is created, choose **Data Encryption** > **Encryption Task Management** to view and manage the new task.

**Step 2** The encryption task is automatically removed after inventory data is encrypted. In this case, the task is removed, but the system continues to encrypt data.

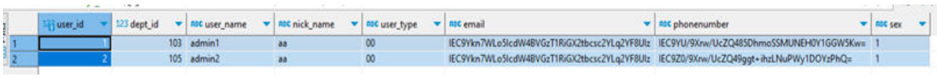
**Figure 15-30** Full encryption mode



| Task Name | IP Address | Port | Instance | Schema | Encrypted Table | Encrypted Column | Creation Time | Enable | Status | Actions |
|---|---|---|---|---|---|---|---|---|---|---|
| Encrypt-root-MySQL-5.7 | 172.[redacted] | [redacted] | doc_demo | doc_demo | sys_user | email,phonenumber | 2024-07-25 13:41:32 | ⊙ | ● Removed | Details \| Edit \| Add to Decryption Task |

**Step 3** Query the database table again. The query result is encrypted data, as shown in **Figure 15-31**.

**Figure 15-31** Encrypted data



| | user_id | dept_id | user_name | nick_name | user_type | email | phonenumber | sex |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 103 | admin1 | aa | 00 | IEC9Ykn7WLo5lcdW4BVGzT1RiGX2tbcsc2YLq2YF8Ulz | IEC9YU/9Xrw/UcZQ485DhmoSSMUNEH0Y1GGW5Kw= | 1 |
| 2 | 2 | 105 | admin2 | aa | 00 | IEC9Ykn7WLo5lcdW4BVGzT1RiGX2tbcsc2YLq2YF8Ulz | IEC9Z0/9Xrw/UcZQ49ggt+ihzLNuPWy1DOYzPhQ= | 1 |

**----End**

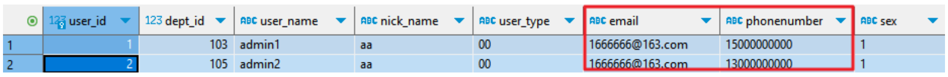
## 15.3.6.4 Creating a Masking Rule in the Result

You can create a masking rule based on the sensitive data discovery result. This section describes how to create a masking rule in the result.

You can also create masking rules in the dynamic masking module. For details, see **Creating a Masking Rule**.

The data table information is plaintext information (data is not encrypted or user authorization is performed after encryption) before masking, as shown in **Figure 15-32**.

**Figure 15-32** Query result before masking



| | user_id | dept_id | user_name | nick_name | user_type | email | phonenumber | sex |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 103 | admin1 | aa | 00 | 1666666@163.com | 15000000000 | 1 |
| 2 | 2 | 105 | admin2 | aa | 00 | 1666666@163.com | 13000000000 | 1 |

## Creating a Data Masking Rule

**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

**Step 2** In the navigation tree on the left, choose **Sensitive Data Discovery** > **Sensitive Data Scan**.

**Step 3** On the scan task list page, locate the target data asset and click **View**.

**Step 4** On the scan result page, locate the target database table and click **Add Masking Rule**.

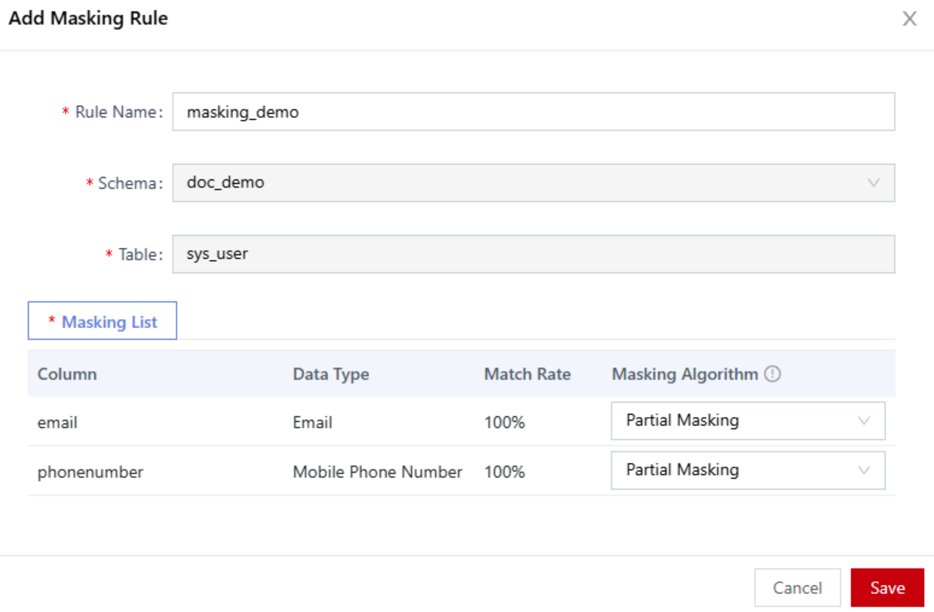
You can also click **Add Desensitization Rules in Batch** on the scan result list page to generate masking rules in batches based on the industry template used for scanning sensitive data. For details about how to configure an industry template, see **Adding an Industry Template**.

**Step 5** In the **Add Masking Rule** dialog box, set masking information, as shown in **Table 15-14**.

**Table 15-14** Adding a masking rule

| Parameter | Description |
|---|---|
| Rule Name | Enter a masking rule name. |
| Schema | Name of the schema of the asset. |
| Table Name | Table name of an asset. |
| Masking List | Configure the masking algorithm in the masking list. |

**Figure 15-33** Adding a masking rule



Add Masking Rule

* Rule Name: masking_demo

* Schema: doc_demo

* Table: sys_user

* Masking List

| Column | Data Type | Match Rate | Masking Algorithm |
|---|---|---|---|
| email | Email | 100% | Partial Masking |
| phonenumber | Mobile Phone Number | 100% | Partial Masking |

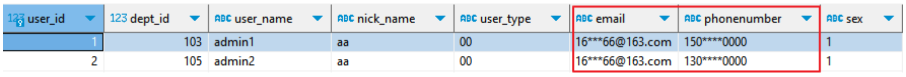
**Step 6** Click **Save**.

**----End**

## Upgrade Verification

1. After the masking rule is created, choose **Dynamic Data Mask** > **Data Masking Policy** to view and manage the new masking rule.
2. Use the proxy to query the database table again. The query result is the masked data, as shown in **Figure 15-34**.

**Figure 15-34** Masked data



| user_id | dept_id | user_name | nick_name | user_type | email | phonenumber | sex |
|---|---|---|---|---|---|---|---|
| 1 | 103 | admin1 | aa | 00 | 16***66@163.com | 150****0000 | 1 |
| 2 | 105 | admin2 | aa | 00 | 16***66@163.com | 130****0000 | 1 |

### 15.3.6.5 Adding a User-Defined Data Type

If the default data types cannot meet service requirements, you can create custom data types.

Regular expressions are patterns used to match strings, check if a string contains a certain substring, replace matching substrings, or extract substrings that meet certain criteria.

## Procedure

**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation tree on the left, choose **Sensitive Data Discovery > Data Type Management**.

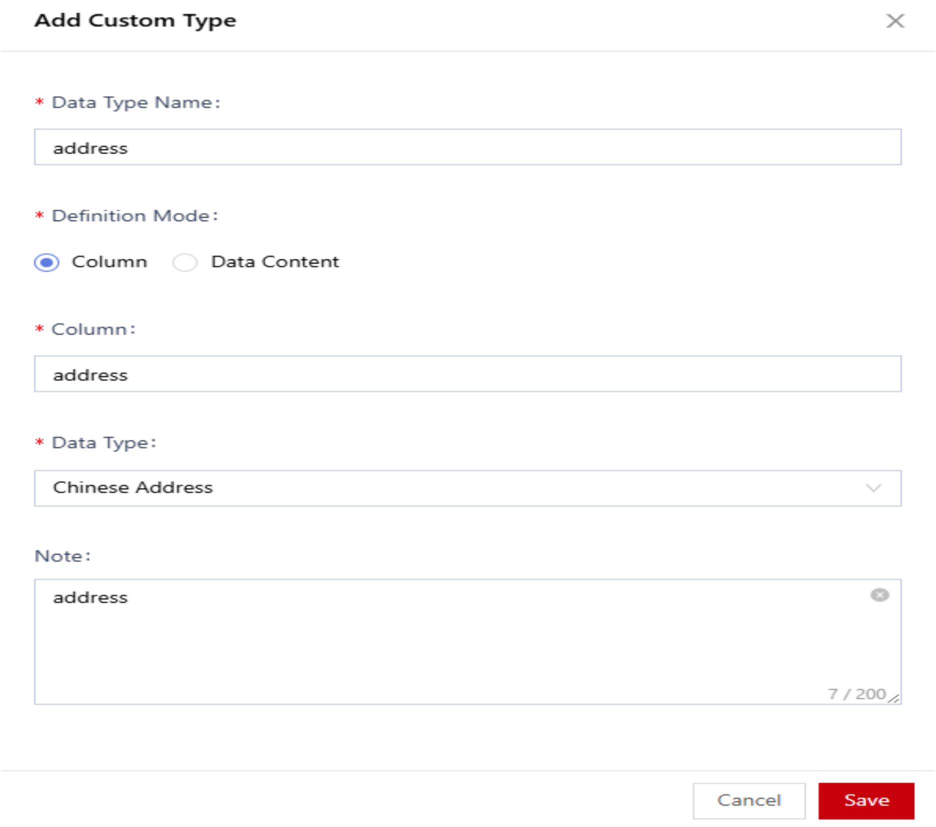
**Step 3** On the **Data Type List** page, click **Add Custom Type** in the upper right corner.

**Step 4** In the displayed dialog box, configure the custom data type.

You can create user-defined data types by matching **Column** or **Data Content**.

- Matching column

**Figure 15-35** Matching column



Add Custom Type

* Data Type Name: address

* Definition Mode: ● Column ○ Data Content

* Column: address

* Data Type: Chinese Address

Note: address

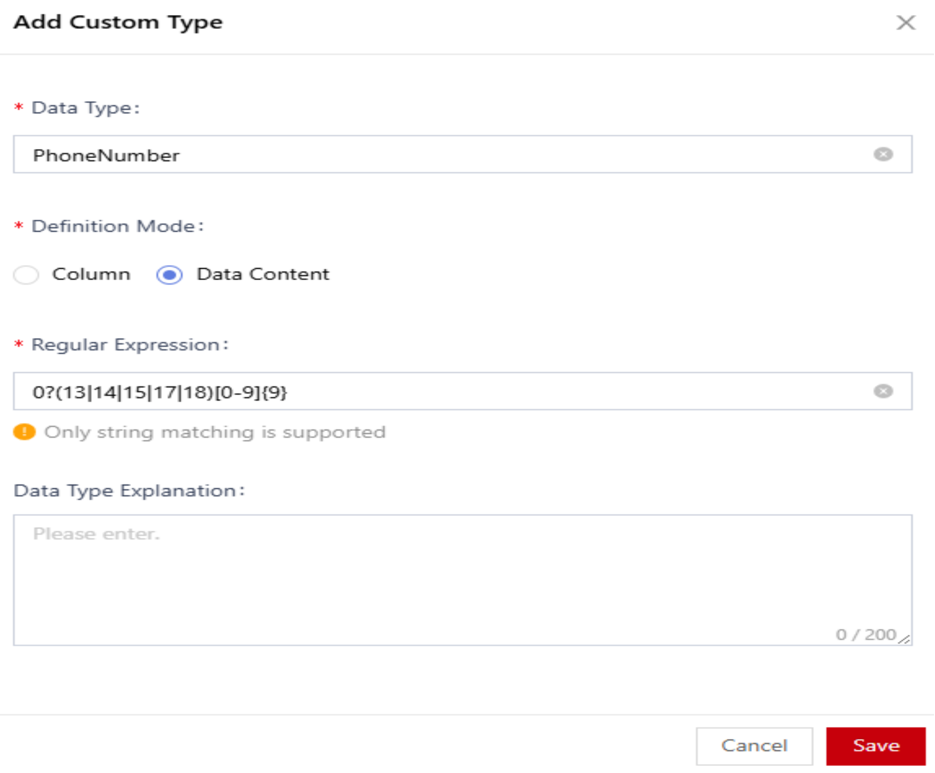
7 / 200

**Table 15-15** Matching column

| Parameter | Description |
|---|---|
| Data Type | Set a custom data type name for further management. |
| Definition Mode | Select a column name. |
| Column | Enter a keyword or a regular expression.<br>Note: If a column name contains a keyword or matches a regular expression, the column name is matched. |
| Data Type | Select the corresponding data type.<br>Built-in types include numbers, strings, address groups, ID card numbers, email addresses, ID card numbers, mobile numbers, and dates. |
| Data Type Explanation | Enter the description about the data type. |

- Matching data content

**Figure 15-36** Matching data content



Add Custom Type

* Data Type: PhoneNumber

* Definition Mode: ○ Column ● Data Content

* Regular Expression: 0?(13|14|15|17|18)[0-9]{9}

Only string matching is supported

Data Type Explanation: Please enter. 0 / 200

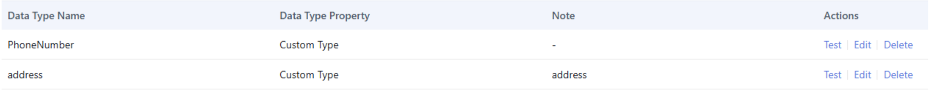
**Table 15-16** Matching data content

| Parameter | Description |
|---|---|
| Data Type | Set a custom data type name for further management. |
| Definition Mode | Set **Definition Mode** to **Data Content**. |
| Regular Expression | Set the regular expression for matching user-defined data.<br>For example, the regular expression of a mobile number is as follows:<br>0?(13\|14\|15\|17\|18)[0-9]{9} |
| Data Type Explanation | Enter the description about the data type. |

**Step 5** Click **Save**.

Then, you can view the added custom data type in the data type list.

**Figure 15-37** Custom data type



| Data Type Name | Data Type Property | Note | Actions |
|---|---|---|---|
| PhoneNumber | Custom Type | - | Test \| Edit \| Delete |
| address | Custom Type | address | Test \| Edit \| Delete |

**Step 6** (Optional) Click **Test** and enter the test data to check whether the custom type meets the expected result.

**----End**

## Related Operations

You can perform the following operations on the data type list page as required.

- Editing a user-defined data type: Click **Edit** to modify the custom data type.
- Deleting a user-defined data type: Click **Delete** to delete unused custom data types.

## 15.3.6.6 Adding an Industry Template

An industry template is a collection of sensitive data types. You can add multiple data types (such as vehicle identification number, military certificate number, and unified social credit code) to an industry template. You can customize an industry template based on industry characteristics. When executing a sensitive data discovery task, you can directly reference the industry template.

## Procedure

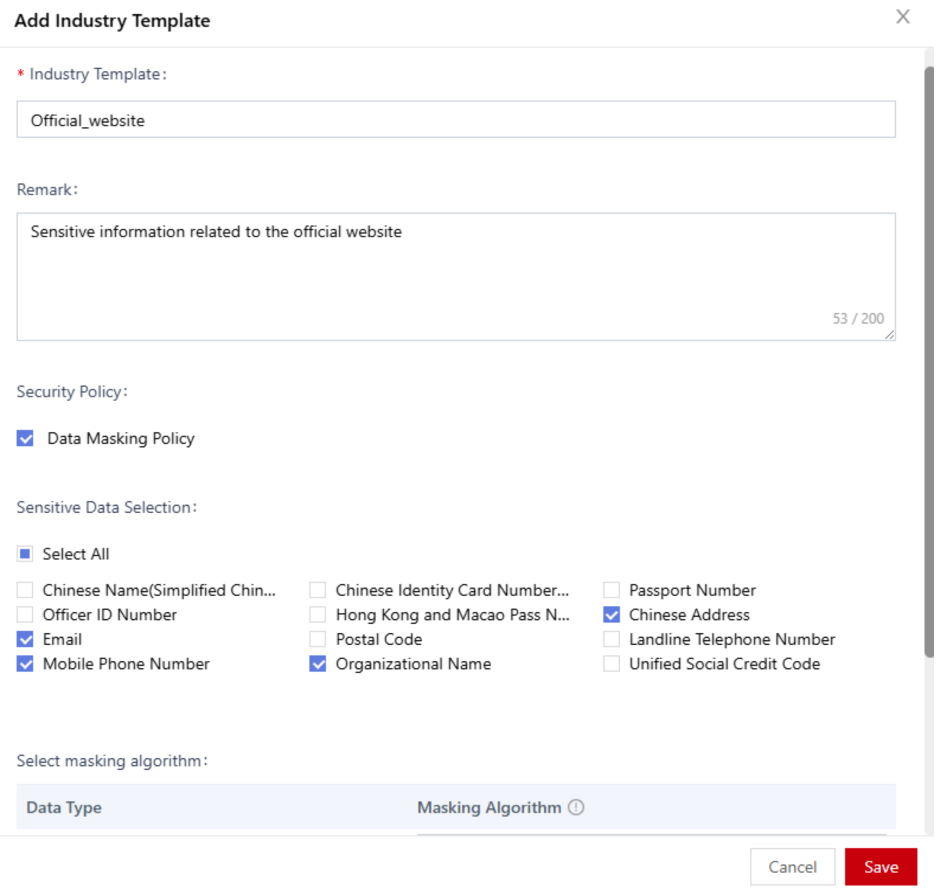
**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation tree on the left, choose **Sensitive Data Discovery > Industry Template**.

**Step 3** On the **Template List** page, click **Add Industry Template** in the upper right corner.

**Step 4** In the displayed dialog box, configure template information, as shown in **Table 15-17**.

**Figure 15-38** Adding a template



Add Industry Template

* Industry Template: Official_website

Remark: Sensitive information related to the official website 53 / 200

Security Policy:

☑ Data Masking Policy

Sensitive Data Selection:

■ Select All

| | | |
|---|---|---|
| □ Chinese Name(Simplified Chin... | □ Chinese Identity Card Number... | □ Passport Number |
| □ Officer ID Number | □ Hong Kong and Macao Pass N... | ☑ Chinese Address |
| ☑ Email | □ Postal Code | □ Landline Telephone Number |
| ☑ Mobile Phone Number | ☑ Organizational Name | □ Unified Social Credit Code |

Select masking algorithm:

| Data Type | Masking Algorithm ⓘ |
|---|---|

**Table 15-17** Parameters for configuring a template

| Parameter | Description |
|---|---|
| Industry Template | Set the name of the industry template. |
| Remarks | Description of an industry template. |
| Security Policy | After **Data Masking Policy** is selected, the industry template contains the masking policy. You need to select a data masking algorithm in the lower part. |

| Parameter | Description |
|---|---|
| Sensitive Data Selection | Type of sensitive data contained in a template. The options are as follows:<br>● **Select All**: Select all data types, including built-in data types and customized data types.<br>● Built-in data type: built-in data type of the system.<br>● User-defined data type: Data types manually created by users. |
| Select Masking Algorithm | Configure a masking algorithm for the selected sensitive data.<br>When the industry template is called to scan sensitive data and masking rules are created in batches in the sensitive data scanning result, you can use the masking algorithm configured. |

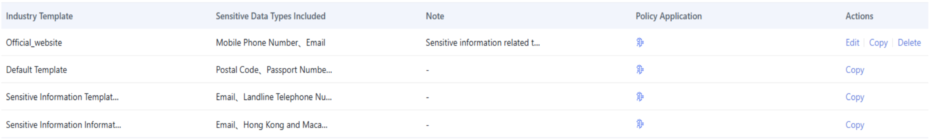
**Step 5** Click **Save** to add an industry template.

**----End**

## Related Operations

- After the template is created, you can view the new industry template on the **Template List** page.

**Figure 15-39** Adding template successfully



| Industry Template | Sensitive Data Types Included | Note | Policy Application | Actions |
|---|---|---|---|---|
| Official_website | Mobile Phone Number、Email | Sensitive information related t... | ⚙ | Edit \| Copy \| Delete |
| Default Template | Postal Code、Passport Numbe... | - | ⚙ | Copy |
| Sensitive Information Templat... | Email、Landline Telephone Nu... | - | ⚙ | Copy |
| Sensitive Information Informat... | Email、Hong Kong and Maca... | - | ⚙ | Copy |

- Table 15-18 shows the template management operations.

**Table 15-18** Management operations

| Operation | Description |
|---|---|
| Click **Edit**. | Modify a custom industry template. |
| Click **Delete**. | Delete unused custom industry templates. |
| Click **Copy**. | Quickly copy and modify an industry template. |

# 15.3.7 Data Encryption and Decryption

## 15.3.7.1 Setting Encryption Parameters

Set ciphertext encoding mode after encryption. The encoding mode can be hexadecimal or BASE64. If you want to support fuzzy search, the encryption parameter must be set to hexadecimal format.

## Constraint

You can change the ciphertext encoding mode only when no asset is configured in the system.

## Procedure

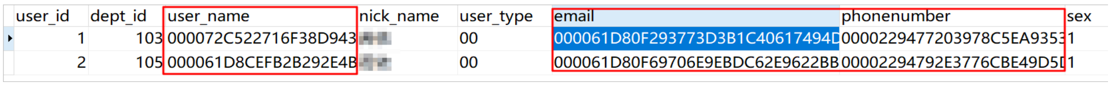
**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation tree on the left, choose **Data Encryption** > **Encryption Parameter**.

**Step 3** On the **Encryption Parameter** page, you can select **Hexadecimal** or **BASE64** from the **Ciphertext Encoding Mode** drop-down list box.

**Step 4** The ciphertext of the encryption table is displayed as a hexadecimal or BASE64 string. For example, Figure 15-40.

**Figure 15-40** Example of ciphertext in hexadecimal mode



| user_id | dept_id | user_name | nick_name | user_type | email | phonenumber | sex |
|---|---|---|---|---|---|---|---|
| 1 | 103 | 000072C522716F38D943 | [redacted] | 00 | 000061D80F293773D3B1C40617494D | 0000229477203978C5EA9353 | 1 |
| 2 | 105 | 000061D8CEFB2B292E4B | [redacted] | 00 | 000061D80F69706E9EBDC62E9622BB | 00002294792E3776CBE49D5 | 1 |

**----End**

## 15.3.7.2 Checking the Encryption Algorithm

After a key is initialized, the system generates the corresponding encryption algorithm. You can view the encryption algorithms supported by the system on the **View Algorithm** page.

## Prerequisites

Ensure that the key has been initialized. For details, see section Initializing a Key.

## Procedure

**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation tree on the left, choose **Data Encryption** > **Algorithm View**.

**Step 3** On the displayed page, view the algorithm details.

**----End**

## 15.3.7.3 Simulated Encryption Test

Before configuring the encryption task, you are advised to perform a simulated encryption test to check whether the encryption is normal.

## Procedure

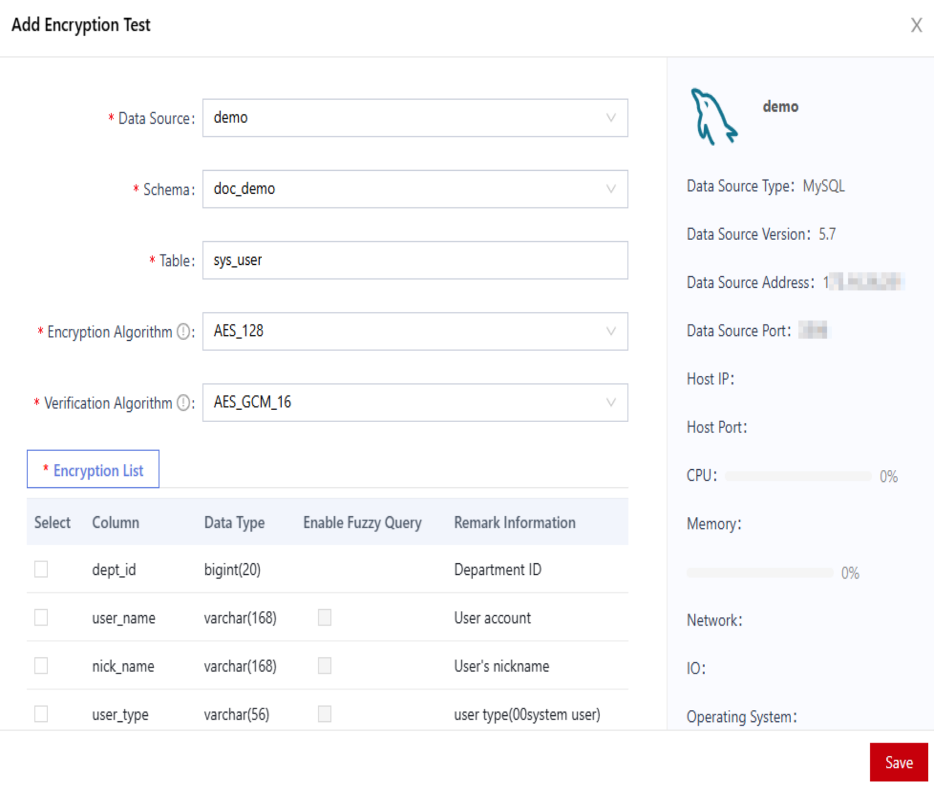
**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation tree, choose **Service Test** > **Simulation Test**.

**Step 3** Click **Add Encryption Test**.

**Step 4** In the displayed dialog box, configure the test target. For details about the related parameters, see **Table 15-19**.

**Figure 15-41** Adding an encryption test



Add Encryption Test

* Data Source: demo
* Schema: doc_demo
* Table: sys_user
* Encryption Algorithm: AES_128
* Verification Algorithm: AES_GCM_16

* Encryption List

| Select | Column | Data Type | Enable Fuzzy Query | Remark Information |
|---|---|---|---|---|
| □ | dept_id | bigint(20) | | Department ID |
| □ | user_name | varchar(168) | □ | User account |
| □ | nick_name | varchar(168) | □ | User's nickname |
| □ | user_type | varchar(56) | □ | user type(00system user) |

demo

Data Source Type: MySQL

Data Source Version: 5.7

Data Source Address: [redacted]

Data Source Port: [redacted]

Host IP:

Host Port:

CPU: 0%

Memory: 0%

Network:

IO:

Operating System:

**Table 15-19** Simulation test

| Parameter | Description |
|---|---|
| Data Source | Name of an asset. |
| Schema | Name of the schema of the asset. |
| Table | Table name of an asset. |
| Encryption Algorithm | Select an encryption algorithm from the drop-down list box.<br>You can view the supported algorithm types on the **Checking the Encryption Algorithm** page. |
| Verification Algorithm | Select a verification algorithm from the drop-down list.<br>The verification algorithm is used to verify the integrity of important data. You can view the supported algorithm types on the **Checking the Encryption Algorithm** page. |

**Step 5** Click the **Encryption List** tab and select the columns to be encrypted.

**Step 6** Click **Save**.

After the test is complete, you can view the test result in the list and click **Details** to view the completion status of each node in the encryption process.

**Step 7** After the test is complete, click **Delete** to delete it.

⚠ CAUTION

If an encryption task needs to be configured after the test, delete the stimulated encryption test first.

**----End**

### 15.3.7.4 Configuring an Encryption Task

- If you are familiar with the database table structure, add it on the **Encryption Task Management** page. After encryption is configured, unauthorized users can view only the ciphertext when querying the database information.
- If you are not familiar with sensitive data distribution, you can use the **Sensitive Data Discovery** function to scan your database, create an encryption task in the result, and encrypt database tables. For details, see **Creating an Encrypted Task in the Result** .

## Prerequisites

Before configuring the encryption task, you are advised to perform a simulation encryption test to check whether any problem occurs during the process. Rectify the fault. For details, see **Simulated Encryption Test**.

## Procedure

**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

**Step 2** In the navigation tree on the left, choose **Data Encryption** > **Encryption Task Management**.

**Step 3** Click **Add Encryption Task** in the upper right corner.

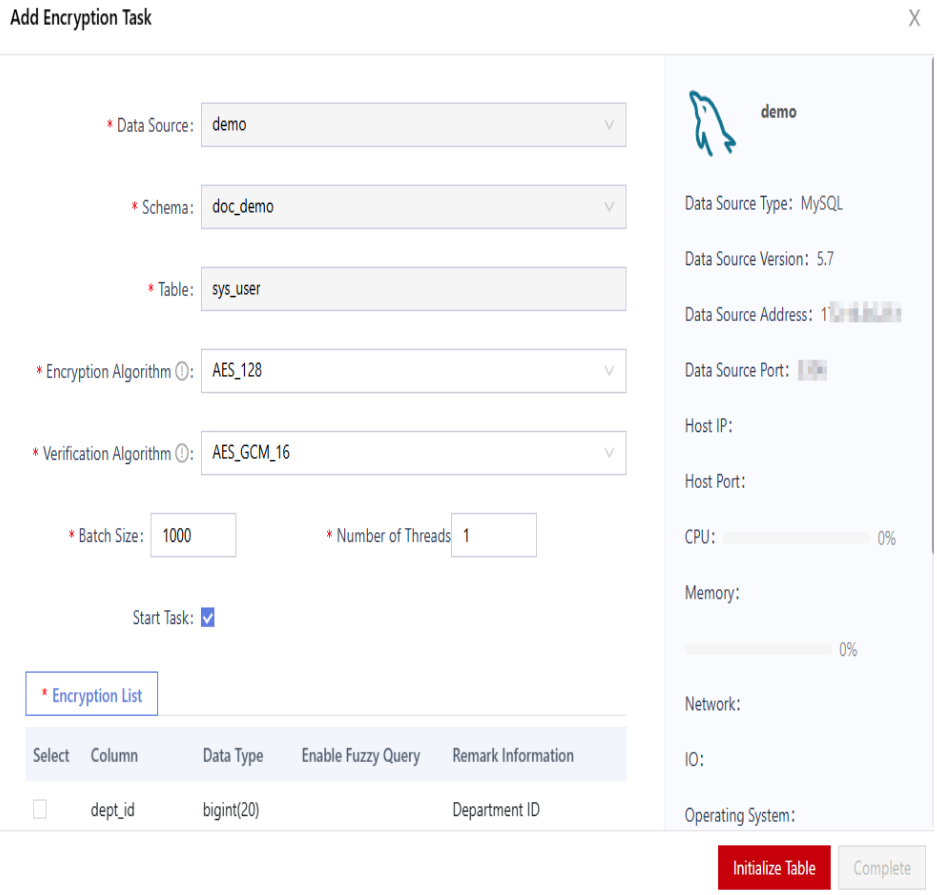
**Step 4** In the displayed dialog box, set encryption information. For details about the related parameters, see **Table 15-20**.

**Table 15-20** Adding an encrypted task

| Parameter | Description |
|---|---|
| Data Source Name | Name of an asset. |
| Schema | Name of the schema of the asset. |
| Table | Table name of an asset. |

| Parameter | Description |
|---|---|
| Encryption Algorithm | Select an encryption algorithm from the drop-down list box.<br>You can view the supported algorithm types on the **Checking the Encryption Algorithm** page. |
| Verification Algorithm | Select a verification algorithm from the drop-down list.<br>The verification algorithm is used to verify the integrity of important data. You can view the supported algorithm types on the **Checking the Encryption Algorithm** page. |
| Batch Size | Set the amount of data processed of each batch in the encryption task. |
| Number of Threads | Number of threads occupied by the encryption task. |
| Start Task | If this parameter is selected, the task is automatically started after being created. |

**Figure 15-42** Adding an encrypted task



Add Encryption Task

* Data Source: demo

* Schema: doc_demo

* Table: sys_user

* Encryption Algorithm: AES_128

* Verification Algorithm: AES_GCM_16

* Batch Size: 1000    * Number of Threads: 1

Start Task: ☑

* Encryption List

| Select | Column | Data Type | Enable Fuzzy Query | Remark Information |
|---|---|---|---|---|
| □ | dept_id | bigint(20) | | Department ID |

demo

Data Source Type: MySQL

Data Source Version: 5.7

Data Source Address: 1[redacted]

Data Source Port: [redacted]

Host IP:

Host Port:

CPU: 0%

Memory: 0%

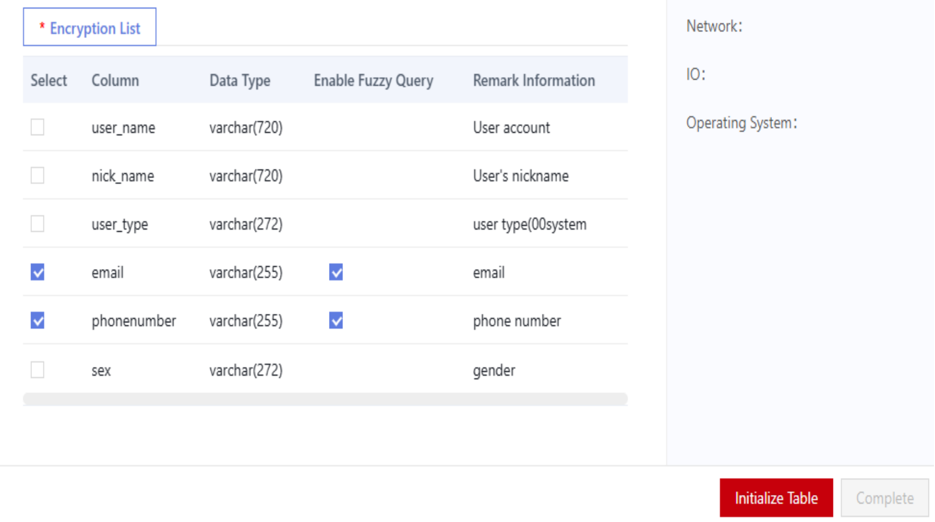
Network:

IO:

Operating System:

**Step 5** Click the **Encryption List** tab, select columns to be encrypted, and set whether to enable fuzzy search.

**Figure 15-43** Selecting encrypted column



* Encryption List

| Select | Column | Data Type | Enable Fuzzy Query | Remark Information |
|---|---|---|---|---|
| □ | user_name | varchar(720) | | User account |
| □ | nick_name | varchar(720) | | User's nickname |
| □ | user_type | varchar(272) | | user type(00system |
| ☑ | email | varchar(255) | ☑ | email |
| ☑ | phonenumber | varchar(255) | ☑ | phone number |
| □ | sex | varchar(272) | | gender |

Network:

IO:

Operating System:

After encryption, fuzzy search cannot be performed by default. In the following cases, you can select **Enable Fuzzy Query** to perform fuzzy search, which supports **%** and _ characters.

- The ciphertext is encoded in hexadecimal format and does not support BASE64 encoding. For details, see **Setting Encryption Parameters**.
- The field is of the string type, for example, varchar and text. Other types are not supported.

**Step 6** Click **Initialize Table** to initialize the data table.

**Step 7** Click **Complete**.

**Step 8** If **Start Task** is not selected during the configuration, click ⓟ to start encryption.

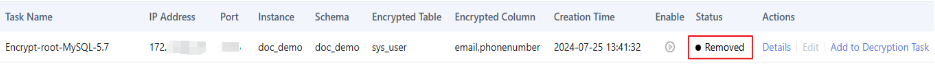
If the encryption is interrupted, you can click ⓟ to continue the encryption.

**----End**

## Operation Result

- After the encryption task is created, you can view and manage it in the list. The encryption task is automatically removed after inventory data is encrypted. In this case, the task is in the **Removed** state, but the system continues to encrypt data.

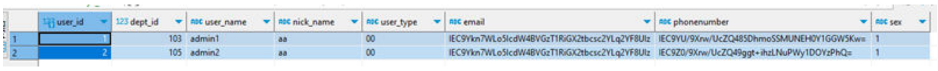
**Figure 15-44** Encryption task



| Task Name | IP Address | Port | Instance | Schema | Encrypted Table | Encrypted Column | Creation Time | Enable | Status | Actions |
|---|---|---|---|---|---|---|---|---|---|---|
| Encrypt-root-MySQL-5.7 | 172.[redacted] | [redacted] | doc_demo | doc_demo | sys_user | email,phonenumber | 2024-07-25 13:41:32 | ⓟ | ● Removed | Details \| Edit \| Add to Decryption Task |

- After the encryption is complete, only encrypted data can be queried by unauthorized users.

**Figure 15-45** Encrypted data



| | user_id | dept_id | user_name | nick_name | user_type | email | phonenumber | sex |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 103 | admin1 | aa | 00 | IEC9Ykn7WLo5lcdW4BVGzT1RiGX2tbcsc2YLq2YF8Ulz | IEC9YU/9Xrw/UcZQ485DhmoSSMUNEH0Y1GGW5Kw= | 1 |
| 2 | 2 | 105 | admin2 | aa | 00 | IEC9Ykn7WLo5lcdW4BVGzT1RiGX2tbcsc2YLq2YF8Ulz | IEC9Z0/9Xrw/UcZQ49ggt+ihzLNuPWy1DOYzPhQ= | 1 |

## Related Operations

In the task list, you can manage encrypted tasks.

- Click **Details** to view **Encryption Task State**, **Task Name**, **Encrypted Table**, **Encrypted Column**, and **Encryption Algorithm**.
- Click **Edit** to modify information such as **Encrypted Column**.

## 15.3.7.5 Managing Authorization

You can grant permissions to clients and database users who access the database on the **Authorization Management** page.

The authorization management module supports client and user authorization. Obtain the intersection of client and user authorization. For details, see **Authorizing Clients** and **Authorizing Users**.

The management authorization example is described as follows:

**Table 15-21** Configuration example description

| Parameter | Example Value |
|---|---|
| Client Authorization | IP address range:<br>● 192.168.0.100~192.168.0.120<br>● 192.168.1.100~192.168.1.120 |
| User Authorization | The WordPress user can query, add, and modify permissions. |

The configuration result is as follows:

- A user whose IP address is 192.168.0.105 can view plaintext data when accessing the database uses WordPress in proxy mode.
- A user whose IP address is 192.168.0.105 can only view encrypted data when accessing the database uses non-WordPress in proxy mode.
- A user whose IP address is 192.168.3.105 can only view encrypted data when accessing the database uses WordPress in proxy mode.

## Authorizing Clients

Grant permissions to control clients access to database.

**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

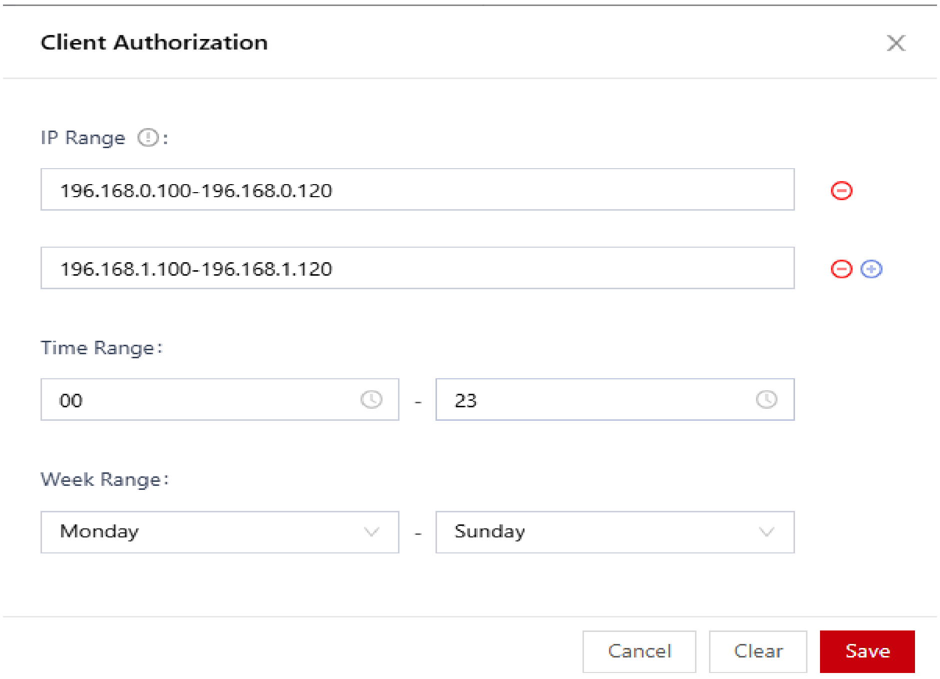
**Step 2** In the navigation pane, choose **Data Encryption** > **Authorization Management**.

**Step 3** In the data source list, click a data source.

**Step 4** Locate the target encrypted database table and click **Client Authorization**.

**Step 5** In the **Client Authorization** dialog box, set the client IP address range, time range, and week range.

**Figure 15-46** Client authorization



Client Authorization

IP Range:

196.168.0.100-196.168.0.120

196.168.1.100-196.168.1.120

Time Range:

00 - 23

Week Range:

Monday - Sunday

NOTE

- You can set the start IP address and end IP address for an IP address range. You can click ⊕ to add multiple IP address ranges. A maximum of 10 IP address ranges can be set.
- The value ranges from 00 to 23. The value indicates the hour. For example, the value **10** indicates 10:00-10:59, including 10:00 and 10:59. If the time range is set to 08-18, the time range is 08:00-18:59, including 08:00 and 18:59.

**Step 6** Click **Save**.

**----End**

## Authorizing Users

Grant permissions to control user access to database.

**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

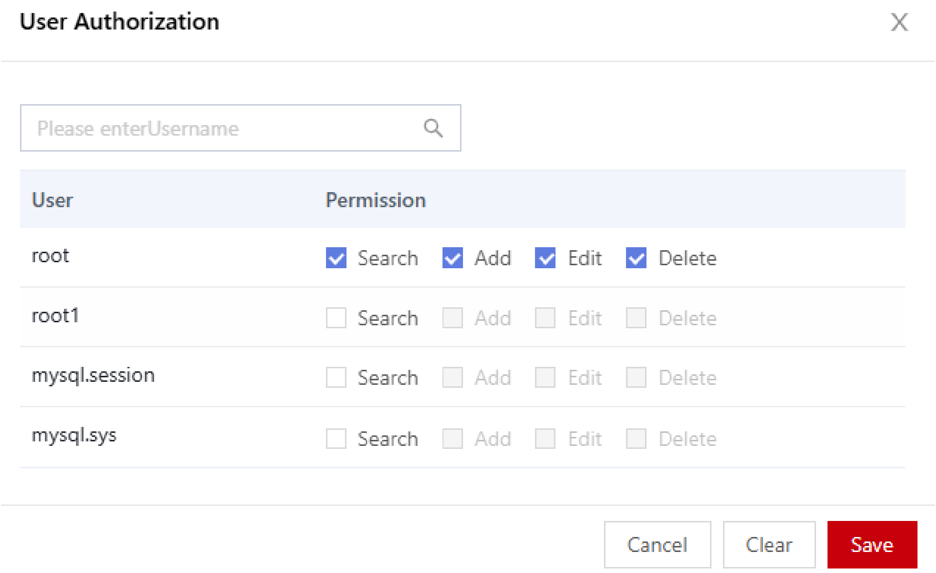
**Step 2** In the navigation pane, choose **Data Encryption** > **Authorization Management**.

**Step 3** In the data source list, click a data source.

**Step 4** Locate the target encrypted database table and click **User Authorization**.

**Step 5** In the displayed dialog box, set the database user to be authorized.

**Figure 15-47** User authorization



| User | Permission |
|---|---|
| root | ☑ Search ☑ Add ☑ Edit ☑ Delete |
| root1 | □ Search □ Add □ Edit □ Delete |
| mysql.session | □ Search □ Add □ Edit □ Delete |
| mysql.sys | □ Search □ Add □ Edit □ Delete |

**Step 6** Click **Save**.

**----End**

## 15.3.7.6 Simulated Decryption Test

Before configuring a decryption task, you are advised to perform a simulated decryption test to verify the decryption function.

### Prerequisites

The table to be decrypted has been encrypted in the encryption task, that is, **Configuring an Encryption Task** has been completed.

### Procedure

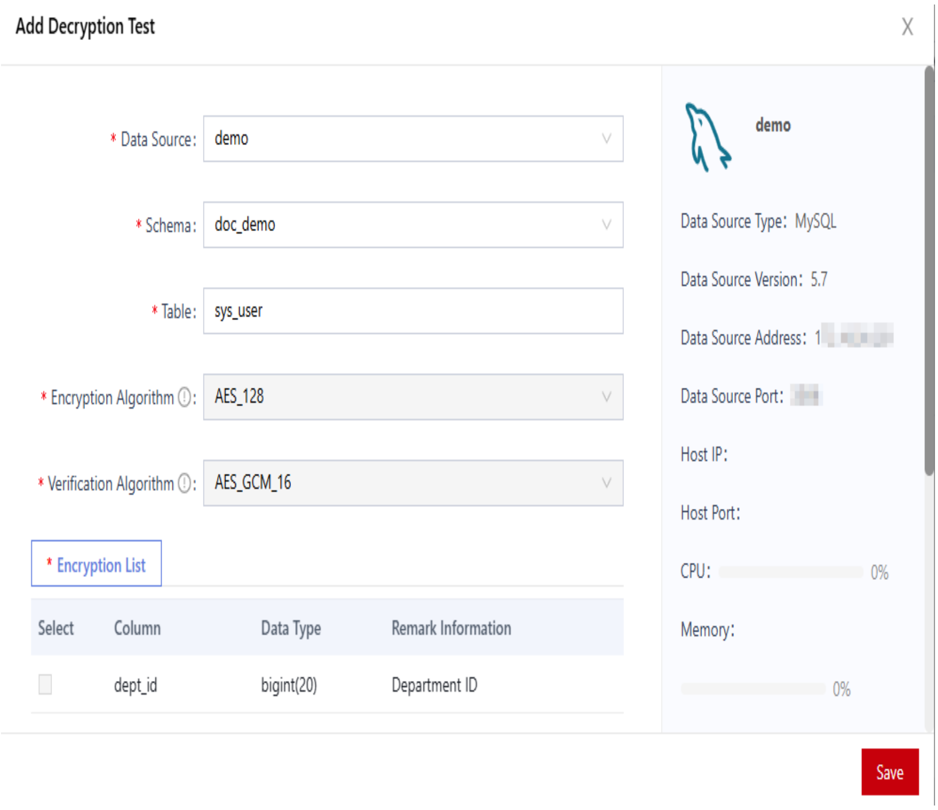
**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

**Step 2** In the navigation tree, choose **Service Test** > **Simulation Test**.

**Step 3** Click **Add Decryption Test**.

**Step 4** In the displayed dialog box, configure the test target.

**Figure 15-48** Adding a decryption test



Add Decryption Test

* Data Source: demo

* Schema: doc_demo

* Table: sys_user

* Encryption Algorithm: AES_128

* Verification Algorithm: AES_GCM_16

* Encryption List

| Select | Column | Data Type | Remark Information |
|---|---|---|---|
| □ | dept_id | bigint(20) | Department ID |

demo

Data Source Type: MySQL

Data Source Version: 5.7

Data Source Address: [redacted]

Data Source Port: [redacted]

Host IP:

Host Port:

CPU: 0%

Memory: 0%

**Step 5** Click **Save**.

After the test is complete, you can view the test result in the list and click **Details** to view the completion status of each node in the decryption process.

**Step 6** After the test is complete, click **Delete** to delete the simulated decryption test.

If a decryption task needs to be configured after the test, delete the simulated decryption test first.

**----End**

## 15.3.7.7 Configuring a Decryption Task

If the database does not need to be encrypted, you can configure a decryption task. After decryption is configured, the information in the corresponding database column changes to the plaintext data.

You can find the target encryption task on the **Encryption Task Management** page and click **Add to Decryption Task** to create a decryption task. You can also create a decryption task on the **Decryption Task Management** page.

The following describes how to create a decryption task on the **Decryption Task Management** page.

### Prerequisites

Before configuring the decryption task, you are advised to perform a simulated decryption test to check whether any problem occurs during decryption. For details, see **Simulated Decryption Test**.

## Procedure

**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

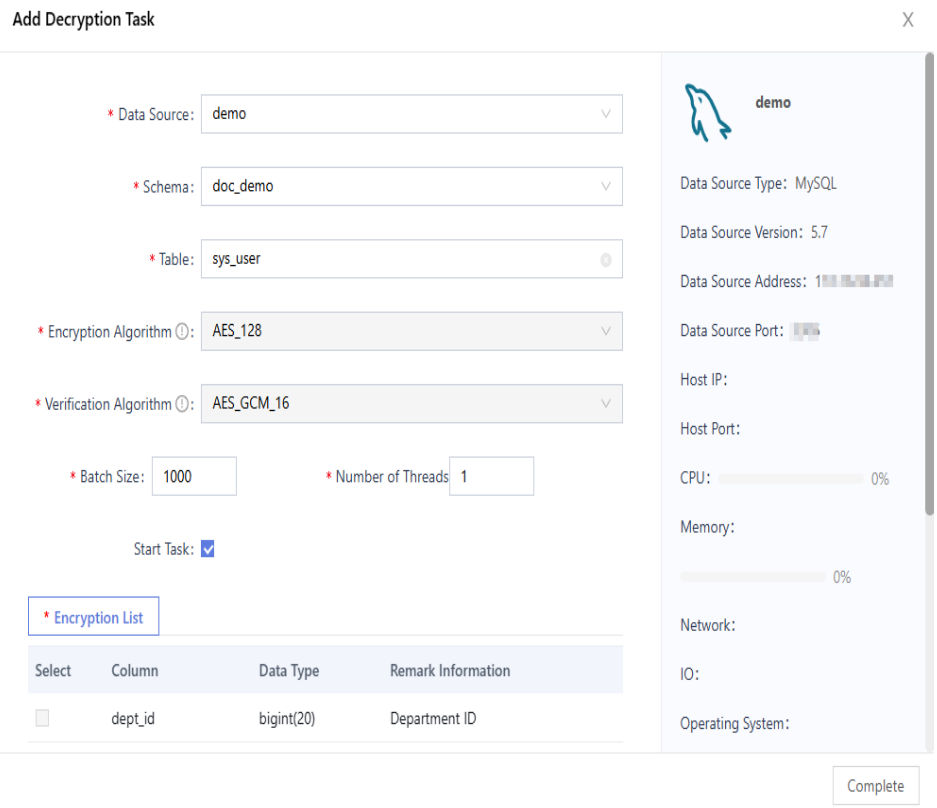
**Step 2** In the navigation tree on the left, choose **Data Encryption** > **Decryption Task Management**.

**Step 3** Click **Add Decryption Task** in the upper right corner.

**Step 4** In the displayed dialog box, set the information about the data to be decrypted.

- The data information includes the data source name, schema name, and table name. You can select a value from the drop-down list box.
- If no encrypted table exists in the destination database schema, the table name cannot be selected. In this case, encrypt the table first. For details about how to encrypt a table, see **Configuring an Encryption Task**.

**Figure 15-49** Adding a decrypted task



Add Decryption Task

* Data Source: demo

* Schema: doc_demo

* Table: sys_user

* Encryption Algorithm: AES_128

* Verification Algorithm: AES_GCM_16

* Batch Size: 1000 * Number of Threads 1

Start Task: ☑

* Encryption List

| Select | Column | Data Type | Remark Information |
|---|---|---|---|
| □ | dept_id | bigint(20) | Department ID |

demo

Data Source Type: MySQL

Data Source Version: 5.7

Data Source Address: [redacted]

Data Source Port: [redacted]

Host IP:

Host Port:

CPU: 0%

Memory: 0%

Network:

IO:

Operating System:

**Step 5** Select **Start Task**. After the creation is complete, the decryption task is automatically started.

**Step 6** Click **Complete**.

After the decryption is complete, the data in the corresponding column of the database table has been decrypted. The data in the database column is restored to the plaintext state.

**----End**

### 15.3.7.8 Encryption Table Management

For encrypted tables, functions such as **Edit Index** and **Edit Non-encrypted Column** are supported on the web page.

## Editing Index

When the data volume is large (for example, more than 10 million rows), querying encrypted columns is time-consuming. You can add indexes to improve the efficiency. You can add an index on the database asset or on the system. This section describes how to add indexes to encrypted columns in the system.

**Step 1** **Log in to a database encryption and access control system** as the **sysadmin** user.

**Step 2** In the navigation tree on the left, choose **Data Encryption** > **Encryption Table Management**.

**Step 3** Choose **Data Source > Asset Name**.

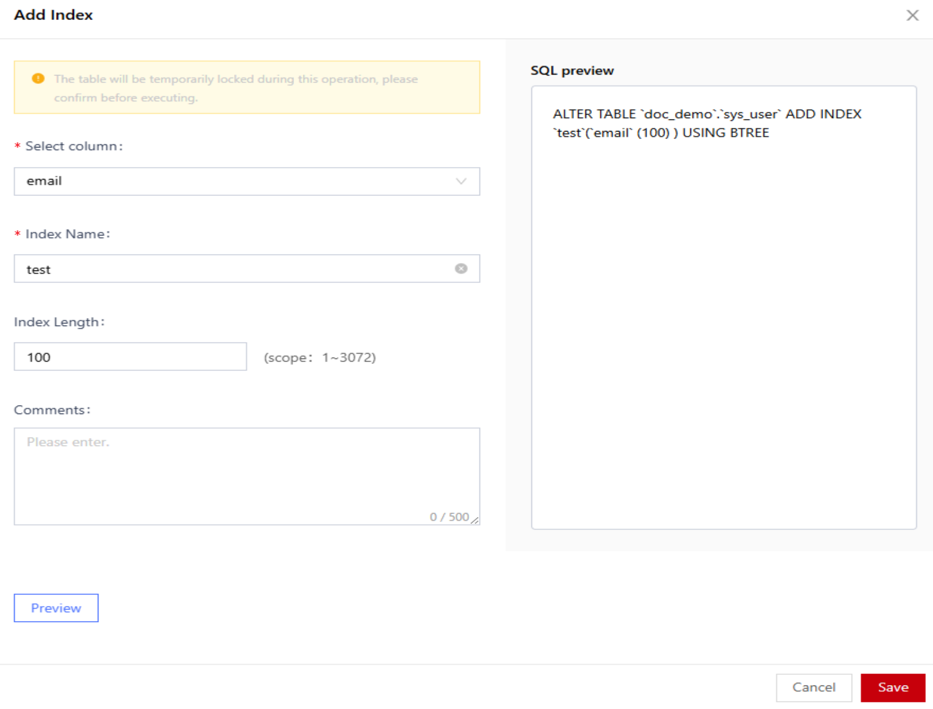
**Step 4** In the list, view the list of encrypted tables. You can search for the target encrypted table by schema and table name.

**Step 5** Find the target encrypted table and click **Edit Index**. The index list page is displayed.

**Step 6** Click **Add Index**.

**Step 7** In the displayed dialog box, set index parameters. Select a column, set the index name and index length, and click **Preview** to view the SQL statement for adding the index.

**Figure 15-50** Adding an index



Add Index

The table will be temporarily locked during this operation, please confirm before executing.

* Select column: email

* Index Name: test

Index Length: 100 (scope: 1~3072)

Comments: Please enter. 0 / 500

SQL preview

```
ALTER TABLE `doc_demo`.`sys_user` ADD INDEX
`test`(`email` (100) ) USING BTREE
```

**Step 8** Click **Save**.

**----End**

## Editing Non-encrypted Column

After database tables in data assets are encrypted, users cannot directly add columns to the database. You need to fully decrypt the encrypted table before adding columns. Services on the live network need to be stopped, which greatly affects user services.

With the function of editing non-encrypted columns, you can add columns without full decryption. The encrypted table is locked only when is executed, which has minimized impact on the live network.

**NOTE**

If you want to modify a large number of columns in an encrypted table, you still need to decrypt all columns in the encrypted table before modifying them.

**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

**Step 2** In the navigation tree on the left, choose **Data Encryption** > **Encryption Table Management**.

**Step 3** Choose **Data Source** > **Asset Name**.

**Step 4** In the list, view the list of encrypted tables. You can search for the target encrypted table by schema and table name.

**Step 5** Locate the target encrypted table and click **Edit Non-encrypted Column**.

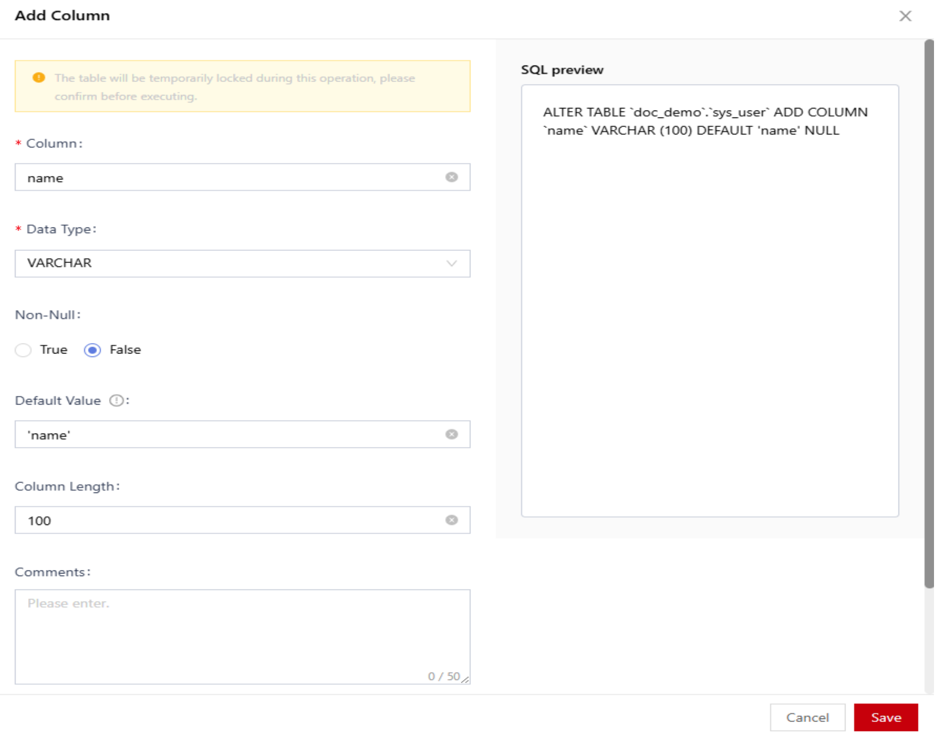
**Step 6** In the displayed page, click **Add Column**.

**Step 7** In the **Add Column** dialog box, configure column parameters, including the **Column**, **Data Type**, **Non-Null**, **Default Value**, and **Column Length**. Click **Preview** to view the SQL statement for adding a column.

**NOTE**

The default value cannot contain single or double quotation marks.

**Figure 15-51** Adding a column



Add Column

The table will be temporarily locked during this operation, please confirm before executing.

* Column: name

* Data Type: VARCHAR

Non-Null: ○ True ● False

Default Value: 'name'

Column Length: 100

Comments: Please enter. 0 / 50

SQL preview

```
ALTER TABLE `doc_demo`.`sys_user` ADD COLUMN
`name` VARCHAR (100) DEFAULT 'name' NULL
```

**Step 8** Click **Save**.

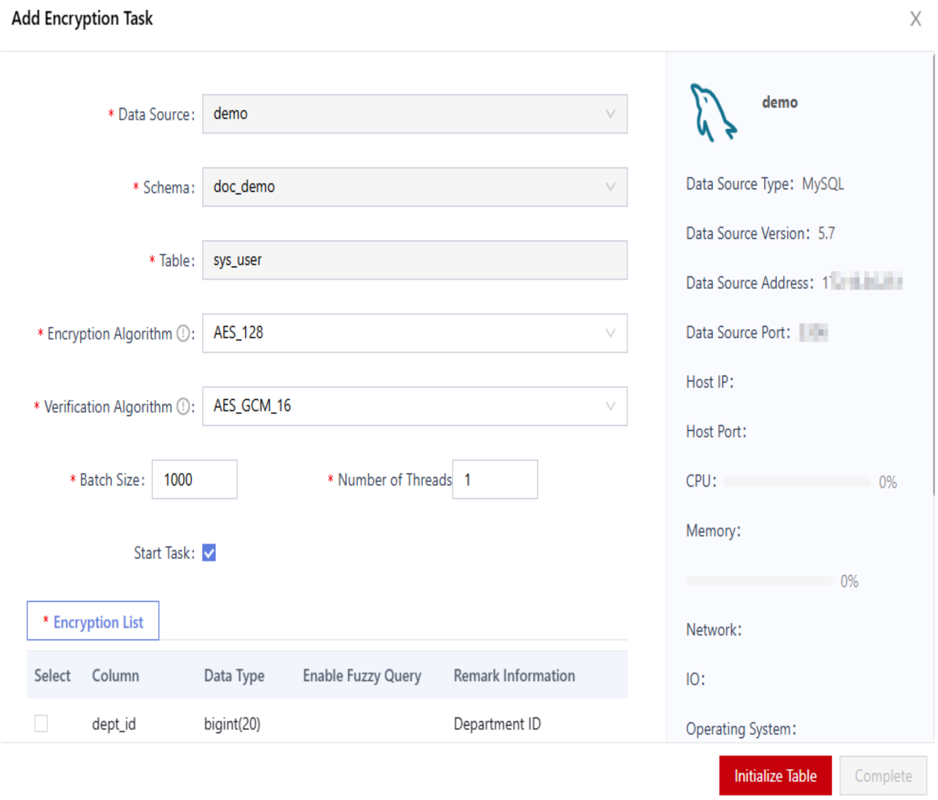
**----End**

## 15.3.7.9 Rolling Back the Table Structure

After the database table is initialized, the system modifies the table structure. You are advised to roll back the table structure if the table needs to restored to the original state.

Scenario: After the database table is initialized and before encryption, you need to manually roll back the table structure to the original state.

**Figure 15-52** Initializing a table



Add Encryption Task

* Data Source: demo

* Schema: doc_demo

* Table: sys_user

* Encryption Algorithm: AES_128

* Verification Algorithm: AES_GCM_16

* Batch Size: 1000

* Number of Threads: 1

Start Task: ☑

* Encryption List

| Select | Column | Data Type | Enable Fuzzy Query | Remark Information |
|---|---|---|---|---|
| □ | dept_id | bigint(20) | | Department ID |

demo

Data Source Type: MySQL

Data Source Version: 5.7

Data Source Address: 1[redacted]

Data Source Port: [redacted]

Host IP:

Host Port:

CPU: 0%

Memory: 0%

Network:

IO:

Operating System:

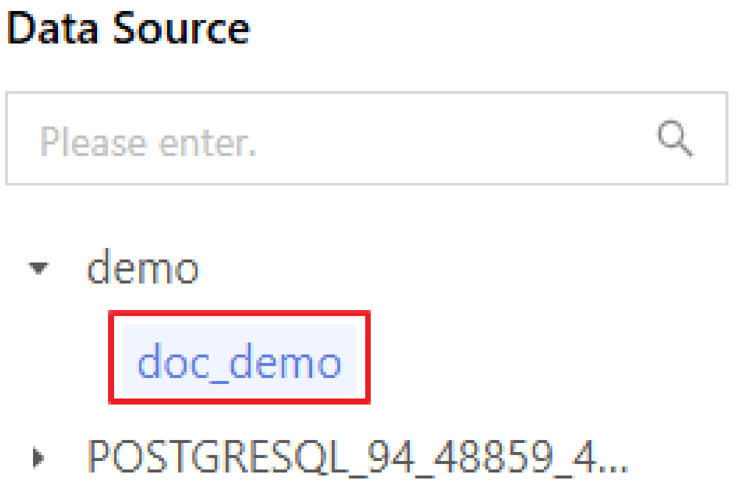
## Procedure

**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation tree on the left, choose **Data Encryption** > **Rollback Table Structure**.

**Step 3** Click **Data Source** and select the asset name and pattern name, as shown in **Figure 15-53**.

**Figure 15-53** Selecting a mode



**Step 4** In the list, select a database table and click **Check Associate Task**.

**Step 5** Click **Restore Table Structure**.

**Step 6** Click **Restore Column**.

After all tables in the data asset are rolled back, you can go to the data source management page and perform operations such as deleting the data asset.

**----End**

### 15.3.7.10 Installing the Bypass Plug-in

If a single point of failure (SPOF) occurs after data encryption, the ciphertext restoration tool takes a long time to decrypt a large amount of data. In this scenario, the bypass plug-in can be used to encrypt and decrypt customers' ciphertext data in real time when a single point of failure (SPOF) occurs on the encryption device, ensuring quick service recovery.

You are advised to deploy the bypass plug-in in advance to cope with single points of failure (SPOFs) on encryption devices.

## Constraint

- MySQL database is supported.
- The escape plug-in can be installed only in the JRE 8 or later and Linux x86 environment.

## Plug-in Status

The plug-in is deployed on the customer's application system. The plug-in can be in any of the following states:

- online: The plug-in is in the ready state. The status can be detected through heartbeat messages. The encryption system periodically pushes the corresponding encryption configuration and key file to the plug-in. Wait until the encryption system is faulty and then switch to the active state.

- bypass: The plug-in is activated and in normal state. The plug-in has detected that the encryption system is abnormal. The plug-in starts to work, modifies the application connection from the gateway proxy to the directly connected database, and encrypts and decrypts the data in the JDBC request.

  When the application is connected to the gateway encryption proxy address and the application cannot communicate with the gateway encryption proxy address, the plug-in switches to the bypass state.

## Procedure

**Step 1** Log in to database encryption and access control.

**Step 2** In the navigation tree on the left, choose **Data Encryption > Bypass**.

**Step 3** Click **Plug-in Download** in the upper right corner of the page to download the plug-in package **gde-agent.tar.gz**.

**Step 4** After the plug-in is downloaded, install the plug-in based on the deployment scenario of the customer's application system.

**----End**

## Operation Results

After the plug-in is installed, the plug-in information is displayed in the plug-in list. If a single point of failure occurs on the encryption device, the plug-in starts to work.

### 15.3.7.11 Querying Application Access Records

After an application accesses the database through a proxy, the system automatically records the access. The administrator can periodically check and audit the access record list.

## Prerequisites

The device records only the information about the application's access to the database through a proxy.

## Procedure

**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation tree on the left, choose **Data Encryption** > **Application Access Logs**. The **Access Records List** page is displayed.

**Step 3** In the access record list, view the application access information, including the data source name, data source IP address, proxy IP address, and application IP address.

You can set the asset type and name to filter access records.

**----End**

# 15.3.8 Dynamic Data Masking

## 15.3.8.1 Adding a Custom Masking Algorithm

The system provides multiple algorithms for sensitive data masking. You can create a custom masking algorithm if the existing algorithms cannot meet your requirements.

### Procedure

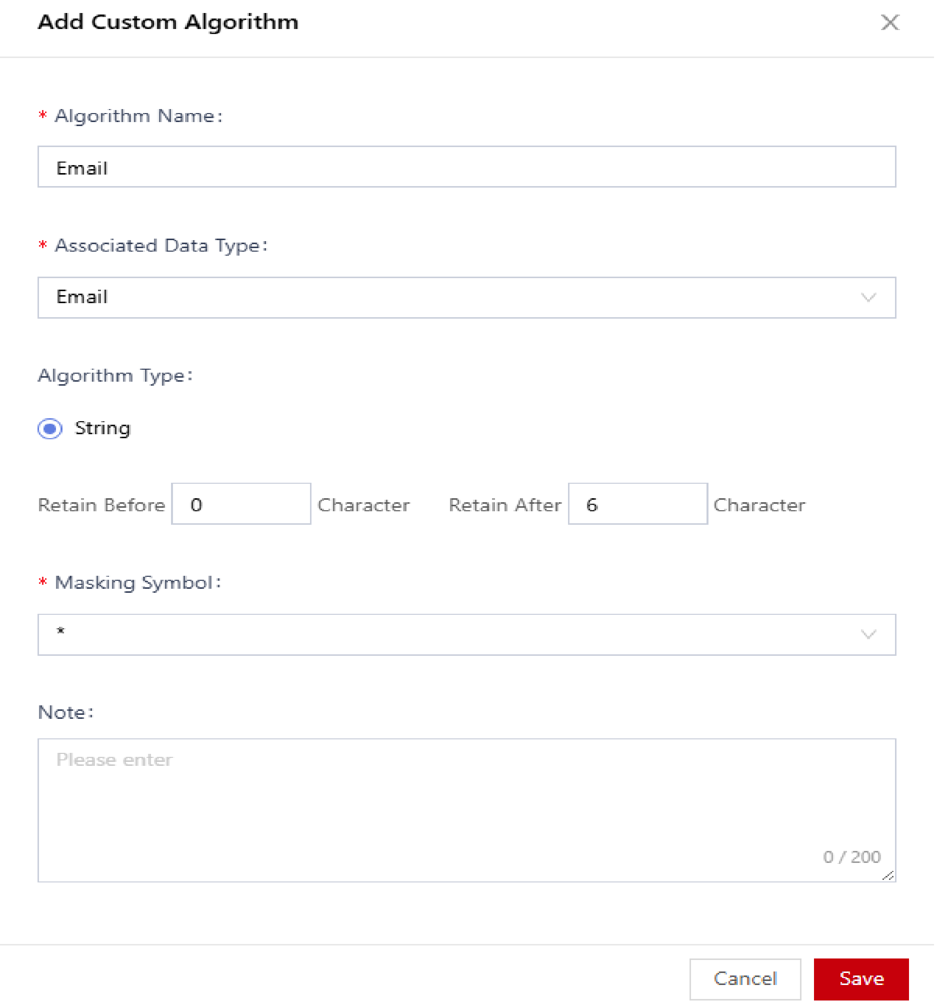
**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation pane on the left, choose **Dynamic Data Mask** > **Desensitization Algorithm**.

**Step 3** On the **Data Masking Algorithm List** page, click **Add Custom Algorithm** in the upper right corner.

**Step 4** Configure the parameters in the displayed dialog box.

**Figure 15-54** Adding a custom algorithm



Add Custom Algorithm

* Algorithm Name: Email

* Associated Data Type: Email

Algorithm Type: ● String

Retain Before 0 Character Retain After 6 Character

* Masking Symbol: *

Note: Please enter 0 / 200

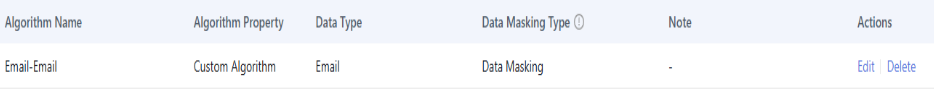
**Table 15-22** Adding a custom algorithm

| Parameter | Description |
|---|---|
| Algorithm Name | Set a custom algorithm name for further management. |
| Associated Data Type | Select the type of the sensitive data to be associated with the algorithm. |
| Algorithm Type | Set the number of retained characters at the beginning and the end of the string. |
| Masking Symbol | Select the symbol used for masking. |
| Algorithm Description | Enter the description about the algorithm. |

**Step 5** Click **Save**.

Then, you can view the added custom masking algorithm in the data type list.

**Figure 15-55** Custom masking algorithm



| Algorithm Name | Algorithm Property | Data Type | Data Masking Type | Note | Actions |
|---|---|---|---|---|---|
| Email-Email | Custom Algorithm | Email | Data Masking | - | Edit \| Delete |

**----End**

## Related Operations

You can perform the following operations on the **Data Masking Algorithm List** page:

- Editing: Locate the target algorithm and click **Edit** in the **Actions** column.
- Deleting: Locate the target algorithm and click **Delete** in the **Actions** column.

### 15.3.8.2 Creating a Data Masking Rule

You can create a masking rule for the plaintext data in the database to ensure security.

- If you are familiar with the database table structure, add a data masking rule on the **Data Masking Policy** page. After the rule is created, users who are not in the whitelist can view only masked data when querying database information.
- If you are not familiar with the sensitive data distribution, scan your database by referring to **Sensitive Data Discovery**. Then, create a masking rule in the result. For details, see **Creating a Masking Rule in the Result**.

If the data in the data table is encrypted and also masked, the following will occur based on different scenarios:

- If the user is authorized, the masked data is returned.
- If the user is not authorized, the ciphertext data which is not masked is returned.

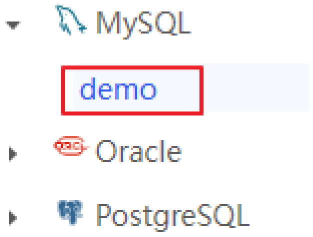
## Procedure

**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation pane on the left, choose **Dynamic Data Mask** > **Data Masking Policy**.

**Step 3** Choose **Data Type** > **Asset Name**.

**Figure 15-56** Selecting a data source



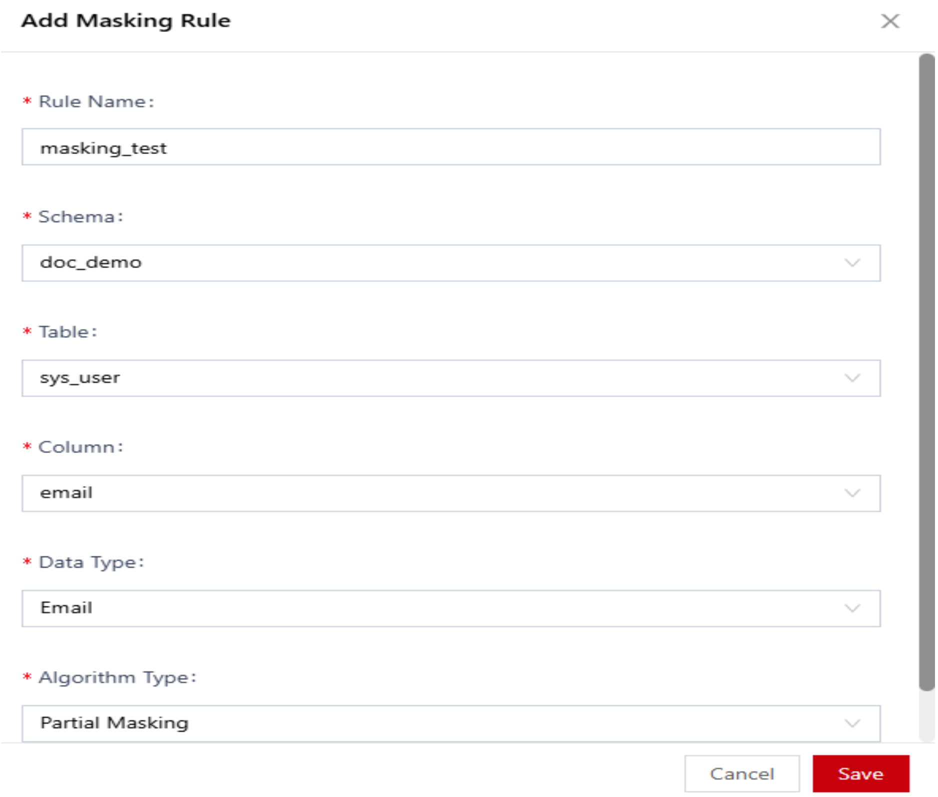
**Step 4** On the masking rule list page of the target data source, click **Add Custom Rule**.

**Step 5** In the displayed **Add Masking Rule** dialog box, configure the parameters. Table 15-23 lists the parameters.

**Table 15-23** Adding a masking rule

| Parameter | Description |
|---|---|
| Rule Name | Set a masking rule name. |
| Schema | Select a data asset mode. |
| Table | Select a data asset table. |
| Column | Select the column to be masked.<br>For details about supported algorithm types, see **Checking the Encryption Algorithm**. |
| Data Type | Select the data type of the selected column.<br>You can add a custom data type. For details, see **Adding a User-Defined Data Type**. |
| Masking Rule | Select the masking rule to be used.<br>You can add a custom masking rule. For details, see **Adding a Custom Masking Algorithm**. |

**Figure 15-57** Adding a masking rule



Add Masking Rule

* Rule Name: masking_test

* Schema: doc_demo

* Table: sys_user

* Column: email

* Data Type: Email

* Algorithm Type: Partial Masking

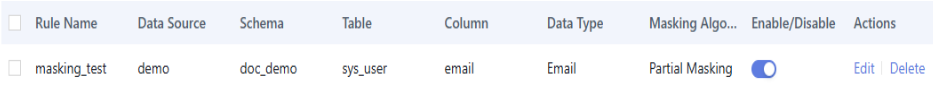
**Step 6** Click **Save**.

**----End**

## Operation Result

- You can view and manage the created masking rule in the masking rule list. The created masking rule is enabled automatically.

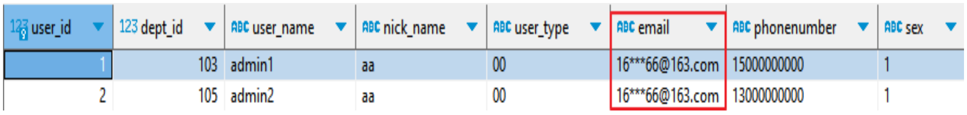
  **Figure 15-58** Masking rule

  | □ | Rule Name | Data Source | Schema | Table | Column | Data Type | Masking Algo... | Enable/Disable | Actions |
  |---|---|---|---|---|---|---|---|---|---|
  | □ | masking_test | demo | doc_demo | sys_user | email | Email | Partial Masking | ● | Edit \| Delete |

- After the data is masked, users who are not in the whitelist can view only masked data when querying the plaintext data.

  **Figure 15-59** Masked data

  | user_id | dept_id | user_name | nick_name | user_type | email | phonenumber | sex |
  |---|---|---|---|---|---|---|---|
  | 1 | 103 | admin1 | aa | 00 | 16***66@163.com | 15000000000 | 1 |
  | 2 | 105 | admin2 | aa | 00 | 16***66@163.com | 13000000000 | 1 |

## Related Operations

You can manage the masking rules as follows:

- Enabling or disabling: Locate the target rule and click the button in the **Enable/Disable** column.

- Editing: Locate the target rule and click **Edit** in the **Actions** column.
- Deleting: Locate the target rule and click **Delete** in the **Actions** column.
- Batch operations: Select the target rules and choose batch enabling, disabling, or delete from the **Bulk Actions** drop-down list.

### 15.3.8.3 Configuring a Data Masking Allowlist

You can add an allowlist on the **Allowlist** page by configuring **Database Username**, **IP Range**, **Start Time**, and **End Date**. The relationship between the parameters is AND. If multiple parameters are configured, only those who meet all conditions are added to the allowlist. Users in the allowlist can view the unmasked plaintext data.

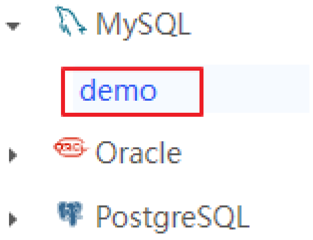
## Procedure

**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation pane on the left, choose **Dynamic Data Mask** > **Data Masking Policy**.

**Step 3** Choose **Data Type** > **Asset Name**.

**Figure 15-60** Data source



**Step 4** In the masking rule list, locate the target data source and click **Allowlist Rule**.

**Step 5** On the **Allowlist** page, click **Add Allowlist**.

**Step 6** Configure the parameters in the displayed **Add Allowlist** dialog box. **Table 15-24** describes the parameters.

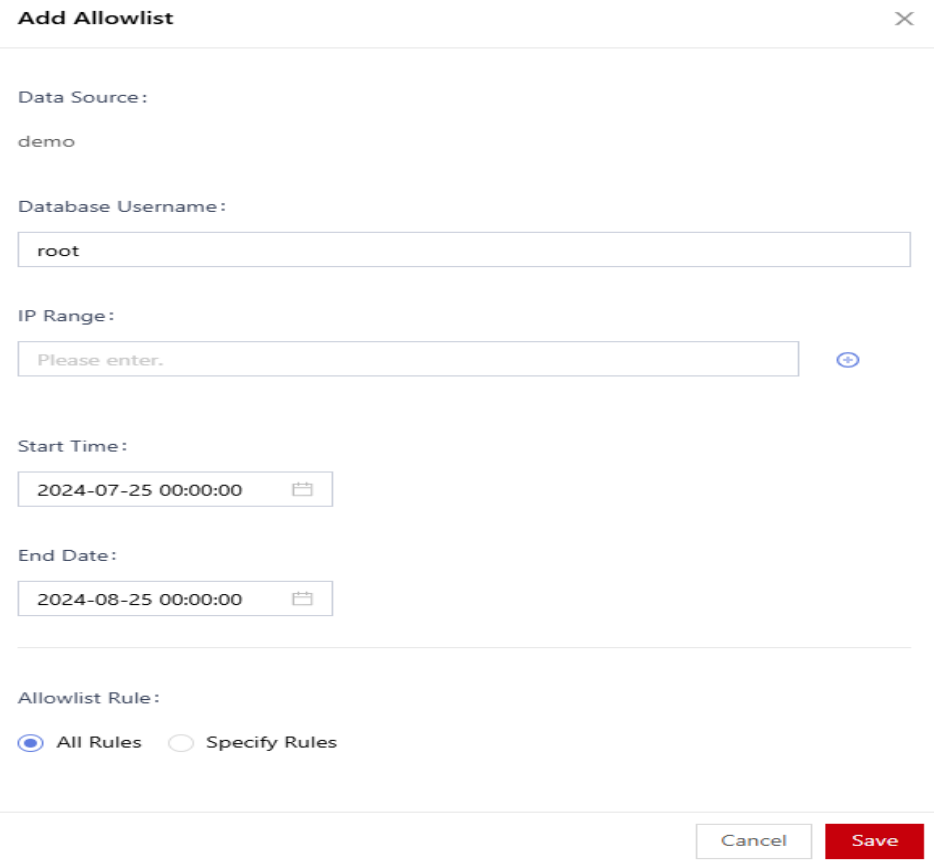
The relationship between the parameters is AND. If multiple parameters are configured, only those who meet all conditions are added to the allowlist.

**Table 15-24** Adding an allowlist

| Parameter | Description |
|---|---|
| Data Source | Data source name |
| Database Username | Database username to be added to the allowlist |
| IP Range | IP addresses to be added to the allowlist |

| Parameter | Description |
|---|---|
| Authorization Start Time | Time when the allowlist starts to take effect |
| Authorization End Time | Time when the allowlist stops to take effect |
| Allowlist Rule | ● **All Rules**: All masking rules are added to the allowlist.<br>● **Specify Rules**: Only specified rules are added to the allowlist. |

**Figure 15-61** Adding an allowlist


Add Allowlist

Data Source:

demo

Database Username:

root

IP Range:

Please enter.

Start Time:

2024-07-25 00:00:00

End Date:

2024-08-25 00:00:00

Allowlist Rule:

● All Rules ○ Specify Rules

**Step 7** Click **Save**.

**----End**

# 15.3.9 Key Management

## 15.3.9.1 Updating a Data Source Key

You can manually or periodically update a data source key (DSK) to ensure service security.

## Prerequisites

The key has been initialized. For details, see **Initializing a Key**.

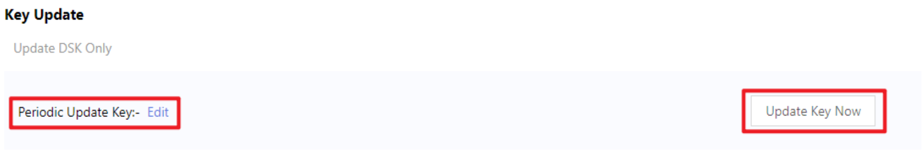
## Procedure

**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

**Step 2** In the navigation pane on the left, choose **Key Management** > **Key Configuration**.

**Step 3** In the **Key Update** area, edit a periodic update task or update the DSK now.

**Figure 15-62** Key update



Key Update

Update DSK Only

Periodic Update Key:- Edit

Update Key Now

**Step 4** To manually update the DSK, perform the following operations:

1. Click **Update Key Now**.
2. In the displayed **Password Verification** dialog box, enter the security password, and click **Confirm**.

**Step 5** To periodically update the DSK, perform the following operations:

1. Click **Edit** next to **Periodic Update Key**.
2. In the displayed **Modify Key Update Cycle** dialog box, configure the update time. **Table 15-25** describes the parameters.

**Table 15-25** Configuring key update cycle

| Parameter | Description |
|---|---|
| Update Cycle | Key update period. The options are as follows:<br>– **None**: No periodic updates are performed.<br>– **Daily**: The data is updated once a day.<br>– **Weekly**: The data is updated once a week.<br>– **Monthly**: The data is updated once a month. |
| Update Time | Configure the key update time based on the key update period. |

**Step 6** Click **Save**.

**----End**

## Follow-up Operations

After the DSK is updated, the system destroys the original DSK and generates a new DSK. You can view the key changing status by referring to **Viewing Key Details**.

## 15.3.9.2 Interconnecting with KMS

You can obtain the key sources from Key Management Service (KMS). Currently, Huawei Cloud is supported.

KMS is a cryptographic platform that provides key management services for third-party cryptographic applications.

## Procedure

**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

**Step 2** In the navigation pane on the left, choose **Key Management** > **KMS Management**.

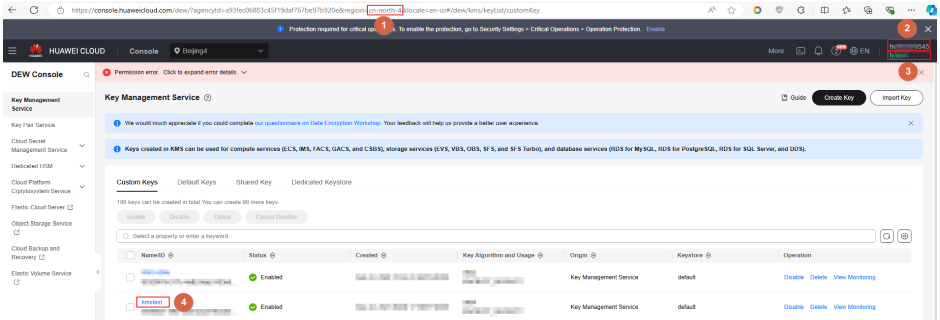
**Step 3** Click the **Huawei Cloud** tab.

**Step 4** Configure the parameters for interconnecting with KMS. For details, see **Table 15-26**.

**Table 15-26** Parameters

| Parameter | Description |
|---|---|
| Region | Region of Huawei Cloud. You can obtain it from the URL of the KMS console, as shown in **Figure 15-63**. |
| Username | IAM username |
| User Password | IAM user password |
| Primary User Account | IAM tenant name, that is, the account to which the IAM user belongs. |
| Key Name | Alias of the KMS key |

**Figure 15-63** KMS console parameters



https://console.huaweicloud.com/dew/?agencyId=a93fec06883c45f19daf767be97b920e&region=cn-north-4&locale=en-us#/dew/kms/keyList/customKey

Protection required for critical op[redacted]s. To enable the protection, go to Security Settings > Critical Operations > Operation Protection. Enable

Permission error. Click to expand error details.

Key Management Service

We would much appreciate if you could complete our questionnaire on Data Encryption Workshop. Your feedback will help us provide a better user experience.

Keys created in KMS can be used for compute services (ECS, IMS, FACS, GACS, and CSBS), storage services (EVS, VBS, OBS, SFS, and SFS Turbo), and database services (RDS for MySQL, RDS for PostgreSQL, RDS for SQL Server, and DDS).

100 keys can be created in total.You can create 98 more keys.

| Name/ID | Status | Created | Key Algorithm and Usage | Origin | Keystore | Operation |
|---|---|---|---|---|---|---|
| [redacted] | Enabled | [redacted] | [redacted] | Key Management Service | default | Disable Delete View Monitoring |
| kmstest [redacted] | Enabled | [redacted] | [redacted] | Key Management Service | default | Disable Delete View Monitoring |

**Step 5** Click **Connection Test**.

**Step 6** After KMS is interconnected, click **Save**.

**----End**

## Follow-up Operations

After the configuration, you can select it by clicking **KEY_Service** when initializing a key. For details, see **Initializing a Key**.

### 15.3.9.3 Viewing Key Details

The system records information such as the ID and type of the created key.

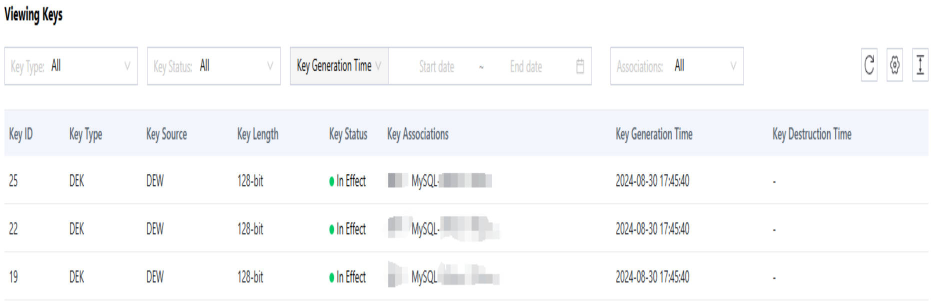
## Procedure

**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

**Step 2** In the navigation pane on the left, choose **Key Management** > **Viewing Keys**.

**Step 3** Search for and view the key information.

**Figure 15-64** Viewing key details



Viewing Keys

Key Type: All

Key Status: All

Key Generation Time: Start date ~ End date

Associations: All

| Key ID | Key Type | Key Source | Key Length | Key Status | Key Associations | Key Generation Time | Key Destruction Time |
|---|---|---|---|---|---|---|---|
| 25 | DEK | DEW | 128-bit | ● In Effect | MySQL-[redacted] | 2024-08-30 17:45:40 | - |
| 22 | DEK | DEW | 128-bit | ● In Effect | MySQL-[redacted] | 2024-08-30 17:45:40 | - |
| 19 | DEK | DEW | 128-bit | ● In Effect | MySQL[redacted] | 2024-08-30 17:45:40 | - |

**----End**

# 15.3.10 System Management

### 15.3.10.1 Creating an Account

By default, the system creates the system administrator **sysadmin**, audit administrator **audadmin**, and security administrator **secadmin** for an account. If multiple employees need to use the system, create separate accounts for each employee for easier management.

The permissions of an account depend on the role. The system creates the system administrator, audit administrator, and security administrator for a role.

## Procedure

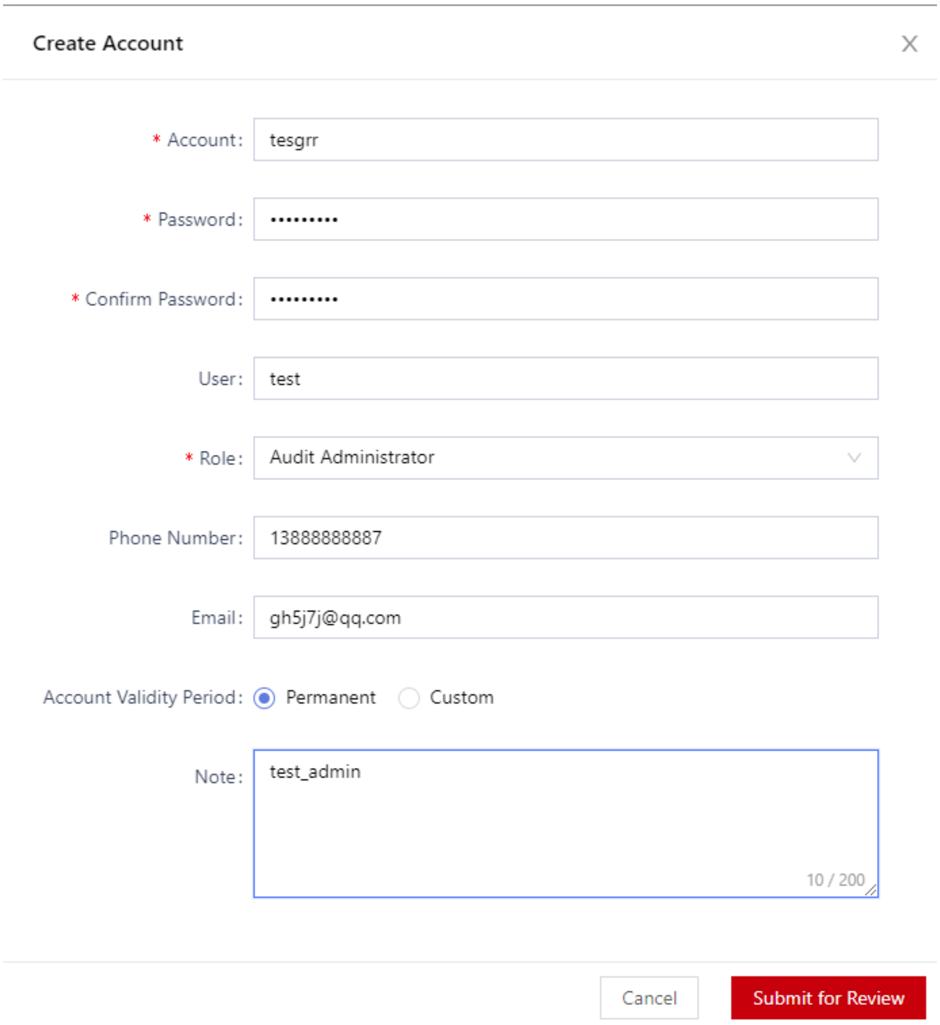
**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

**Step 2** In the navigation pane on the left, choose **System Management** > **Account Management**.

**Step 3** Click **Create Account** in the upper right corner.

**Step 4** Configure the parameters in the displayed dialog box. **Table 15-27** describes the parameters.

**Figure 15-65** Creating an account



Create Account

* Account: tesgrr

* Password: •••••••••

* Confirm Password: •••••••••

User: test

* Role: Audit Administrator

Phone Number: 13888888887

Email: gh5j7j@qq.com

Account Validity Period: ● Permanent ○ Custom

Note: test_admin

10 / 200

**Table 15-27** Creating an account

| Parameter | Description |
|---|---|
| Account | Enter the username. |
| Password/ Confirm Password | Set and confirm the password.<br>Change the password upon the first login and periodically update the password to avoid information breach. |
| User | Set the user. |

| Parameter | Description |
|---|---|
| Role | Select a role from the drop-down list box.<br>● Security Administrator<br>● Audit Administrator<br>● System Administrator |
| Phone Number | Enter the phone number. |
| Email | Enter the email address. |
| Account Validity Period | Select a validity period.<br>● **Permanent**: The account is permanently valid.<br>● **Custom**: The account is valid until the configured expiration date. |
| Time Limit | ● This parameter is available when you set **Service lifetime** to **Define The Deadline**.<br>● The account is available after being created and becomes invalid after the expiration time. Then, the account cannot be used to log in to the system. |
| Note | Enter the description about the account. |

**Step 5** Click **Submit for Review**.

**Step 6** Locate the created account in the list and enable it.

NOTE

The created account is not reviewed. After it is reviewed, you can use it to log in to the system. For details, see **Reviewing an Account**.

**----End**

## Related Operations

You can manage the account as described in the following table.

**Table 15-28** Management operations

| Operation | Description |
|---|---|
| Click **Edit**. | Edit the account information. |
| Click **Delete**. | Delete accounts that are no longer used. |
| Click **Enable**. | Enable an account. |
| Click **Disable**. | Disable an account. After the account is disabled, it cannot be used to log in to the system. |

| Operation | Description |
|---|---|
| Click **Reset Password**. | Set password, which must meet the password requirements. |

## 15.3.10.2 Organization Management

You can manage the organization and the members in it on the **Organization Management** page.

### 15.3.10.2.1 Creating an Organization

An organization can manage the members in it. Create an organization as needed for better management.

## Procedure

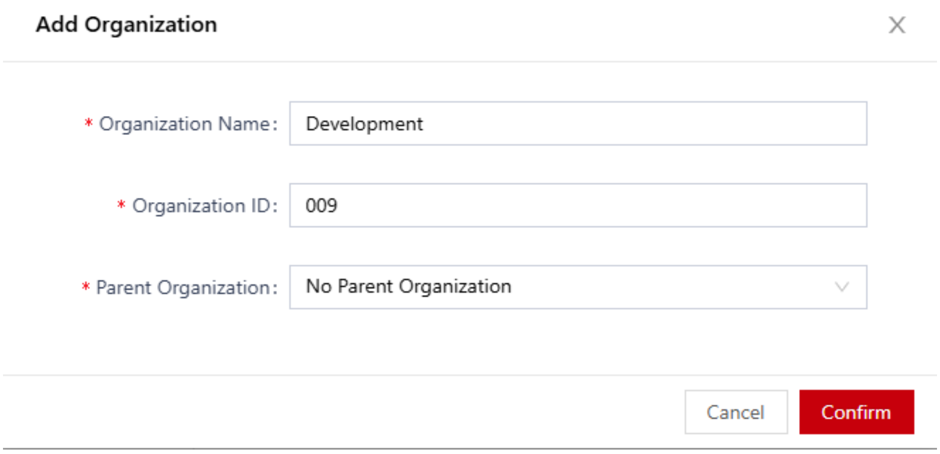
**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation pane on the left, choose **System Management** > **Organization Management**.

**Step 3** Click **Add Organization** on the left.

**Step 4** Configure the parameters in the displayed dialog box.

**Figure 15-66** Parameters for adding an organization



Add Organization

* Organization Name: Development

* Organization ID: 009

* Parent Organization: No Parent Organization

**Table 15-29** Parameters for adding an organization

| Parameter | Description |
|---|---|
| Organization Name | Set the organization name. |
| Organization ID | Set the internal code. |

| Parameter | Description |
|---|---|
| Parent Organization | Choose the parent department from the drop-down list.<br>If this parameter is not configured, the created organization is the level-1 department by default. |

**Step 5** Click **Confirm**.

**----End**

### 15.3.10.2.2 Creating a Member

You can add members for better management. Create members based on the personnel management requirements of the company.

## Prerequisites

An organization has been created for member management. For details, see **Creating an Organization**.

## Procedure

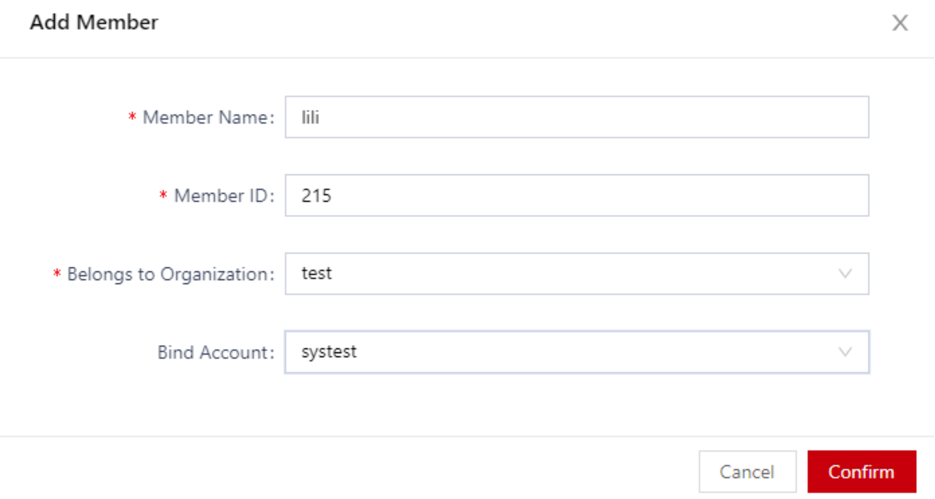
**Step 1** **Log in to a database encryption and access control instance** as the **sysadmin** user.

**Step 2** In the navigation pane on the left, choose **System Management** > **Organization Management**.

**Step 3** Click **Add Member**.

**Step 4** Configure the parameters in the displayed dialog box.

**Figure 15-67** Parameters for adding a member


Add Member

* Member Name: lili

* Member ID: 215

* Belongs to Organization: test

Bind Account: systest

**Table 15-30** Parameters for adding a member

| Parameter | Description |
|---|---|
| Member Name | Set the member name. |
| Member ID | Set the ID. Use information that can identify the employee, such as employee ID.<br>The ID must be unique. |
| Belongs to Organization | Choose the organization from the drop-down list. |
| Bind Account | Select the target member account from the drop-down list. |

**Step 5** Click **Confirm**. You can view the added member on the organization page.

**----End**

## Related Operations

You can manage the member as described in the following table.

**Table 15-31** Management operations

| Operation | Description |
|---|---|
| Click **Edit**. | Edit member details. |
| Click **Delete**. | Delete members that do not need to be managed. |

## 15.3.10.3 System O&M

### 15.3.10.3.1 Viewing the System Monitoring

You can easily troubleshoot issues by viewing the device status and monitoring the system's resource usage.

## Procedure

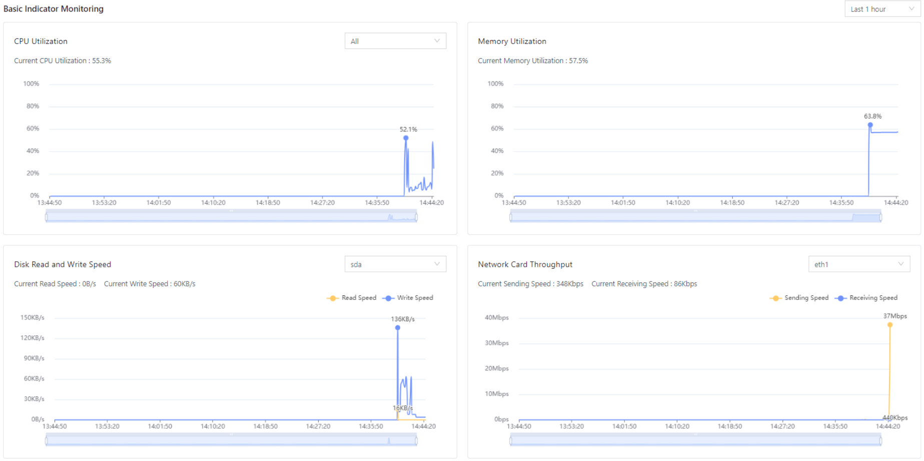
**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation pane on the left, choose **System Management** > **System O&M**.

**Step 3** Click the **System Monitoring** tab.

**Step 4** On the displayed page, view real-time and historical information about your system's performance, including CPU utilization, memory utilization, disk read and write speed, and NIC throughput. You can also see current disk partitions and the status of critical services.

**Figure 15-68** Basic device indicator monitoring



Basic Indicator Monitoring

Last 1 hour

CPU Utilization

All

Current CPU Utilization : 55.3%

Memory Utilization

Current Memory Utilization : 57.5%

Disk Read and Write Speed

sda

Current Read Speed : 0B/s    Current Write Speed : 60KB/s

Network Card Throughput

eth1

Current Sending Speed : 348Kbps    Current Receiving Speed : 86Kbps

**Table 15-32** Parameter descriptions

| Parameter | Description |
|---|---|
| Hardware | Displays system hardware details, including CPU, memory, and disk specifications and usage. |
| CPU Utilization | Displays CPU usage over the past hour, current day, or a custom time period selected by the user. |
| Memory Utilization | Displays memory usage over the past hour, current day, or a custom time period selected by the user. |
| Disk Read and Write Speed | Displays displays changes in disk read/write speeds over the last hour, current day, or a custom time period selected by the user. |
| NIC Throughput | Displays network interface card (NIC) throughput for the past hour, current day, or a custom time period selected by the user. |
| Disk Partition Usage | Displays the status and usage of each partition. |
| Critical Service Monitoring | Displays the running status and resource usage of critical services. |

**Step 5** (Optional) You can restart the service and restart or disable the device in the upper right corner.

⚠ CAUTION

These operations will affect the running of asset management services. Perform the operations during off-peak hours.

**----End**

### 15.3.10.3.2 System Diagnosis

View the resources, such as CPU, memory, disk, and NIC.

## Procedure

**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation pane, choose **System Management > System O&M**. Click **System Diagnostics**.

**Step 3** Select the service to be diagnosed from the **Diagnose Command** drop-down list.

The diagnosis items include the CPU, memory, disk, NIC, and ping.

**Step 4** Click **Execute**.

**----End**

### 15.3.10.3.3 Log Collection

On the one-click collection page, you can set the default log level and collect background logs to facilitate troubleshooting.

## Procedure

**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

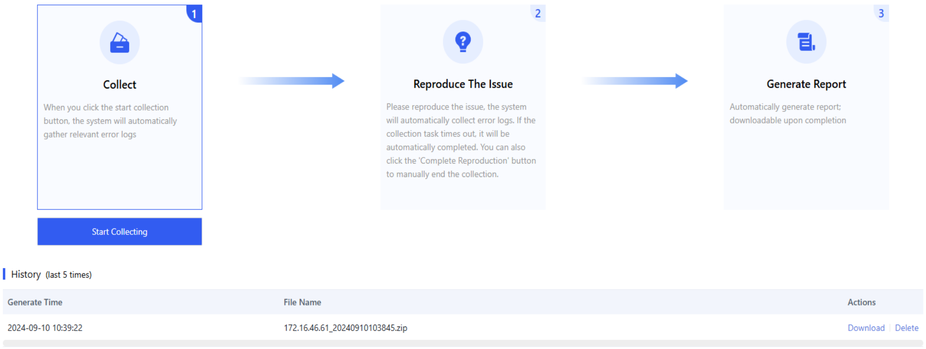
**Step 2** In the navigation pane, choose **System Management > System O&M**. Click **System Diagnostics** > **One-click Collect**.

**Step 3** Click **Start Collecting**.

**Step 4** Click **Complete Reproduction** to wait for the report to be generated.

**Step 5** In the **History** area, select **Download** from the **Operation** drop-down list and provide the downloaded file to related personnel.

**Figure 15-69** Log collection



1 Collect

When you click the start collection button, the system will automatically gather relevant error logs

2 Reproduce The Issue

Please reproduce the issue, the system will automatically collect error logs. If the collection task times out, it will be automatically completed. You can also click the 'Complete Reproduction' button to manually end the collection.

3 Generate Report

Automatically generate report; downloadable upon completion

History (last 5 times)

| Generate Time | File Name | Actions |
|---|---|---|
| 2024-09-10 10:39:22 | 172.16.46.61_20240910103845.zip | Download \| Delete |

**----End**

### 15.3.10.3.4 System Cleanup

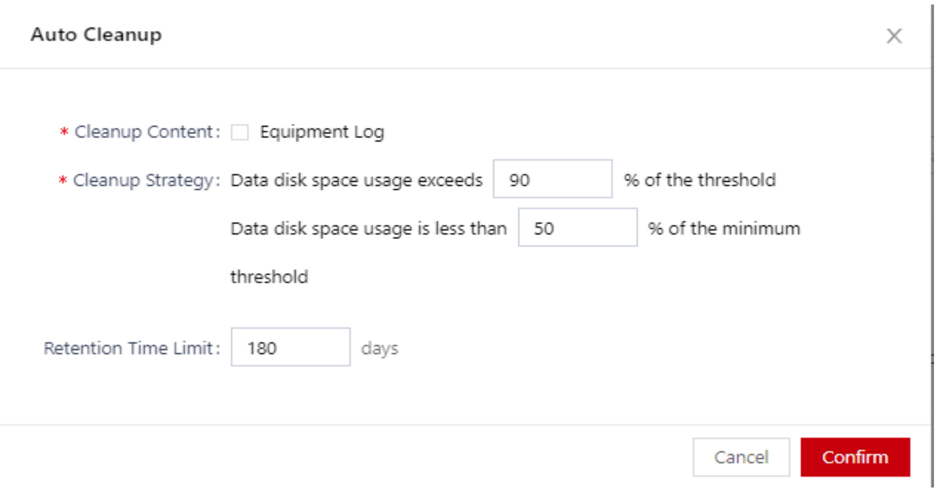
## Automatically Clearing Business Data

**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation pane on the left, choose **System Management** > **System O&M** > **System Clean**.

**Step 3** In the **Auto Cleanup** area, click **Set** next to **Auto Cleanup**. In the dialog box that is displayed, set the parameters for automatically clearing service data.

**Figure 15-70** Setting automatic cleanup



Auto Cleanup

* Cleanup Content: □ Equipment Log

* Cleanup Strategy: Data disk space usage exceeds 90 % of the threshold

Data disk space usage is less than 50 % of the minimum threshold

Retention Time Limit: 180 days

**Table 15-33** Parameter description

| Parameter | Description |
|---|---|
| Retention time limit | Sets the automatic cleanup time for timed-out business data. |
| Maximum threshold for data disk space | Sets the maximum threshold for data disk space. When the disk space usage of the mount point where business data is located exceeds the threshold, an alarm will be triggered and data will be automatically cleaned up. |
| Minimum threshold for data disk space | Sets the minimum threshold for data disk space. When the disk space usage of the mount point where business data is located is below the threshold, data cleanup will be stopped. |

NOTE

The cleanup based on timeout and the cleanup based on storage threshold are independent of each other, and either one can trigger automatic data cleanup.

**Step 4** Click **OK**.

**Step 5** Click ○ to enable automatic cleanup.

**----End**

## Manually Clearing Business Data

**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation pane on the left, choose **System Management** > **System O&M** > **System Clean**.

**Step 3** In the **Manual Cleanup** area, set the date and content to be cleaned, and click **Cleanup**.

**----End**

## 15.3.10.4 View Message Notifications

On the **Message Center** page, you can view system notifications and alarms, configure the message type, template, and recipient roles.

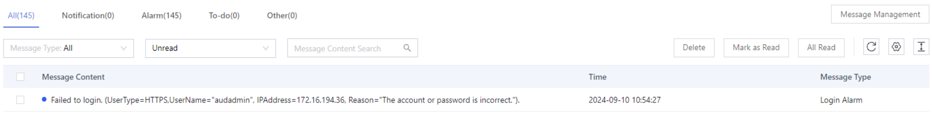
## Procedure

**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

**Step 2** In the navigation pane on the left, choose **System O&M** > **Message Notice**.

**Step 3** View the notifications and alarms in the **All**, **Notification**, **Alarm**, **To-do**, and **Other** tabs.

**Figure 15-71** Message center



Message Type: All

Unread

| □ | Message Content | Time | Message Type |
|---|---|---|---|
| □ | ● Failed to login. (UserType=HTTPS,UserName="audadmin", IPAddress=172.16.194.36, Reason="The account or password is incorrect."). | 2024-09-10 10:54:27 | Login Alarm |

**----End**

## 15.3.10.5 System Settings

### 15.3.10.5.1 General Settings

You can switch the default system language between Chinese and English on the **General Settings** page.

## Procedure

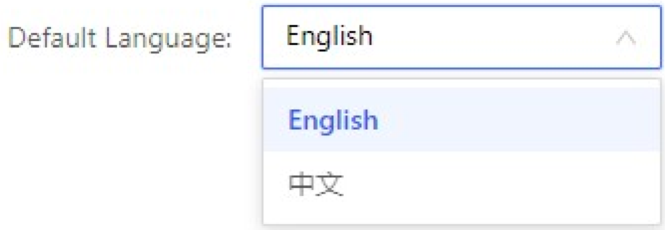
**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

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

**Step 3** Click the **General Settings** tab.

**Step 4** Select a language (Chinese or English) from the **Default Language** drop-down list box.

**Figure 15-72** Selecting the default language



Default Language: English

**----End**

### 15.3.10.5.2 Time Settings

The system enables you to either manually adjust the server time or synchronize it with the network time.

Adjusting or synchronizing the time may invalidate the current browser session. After making changes, please log in to the web console again.

## Procedure

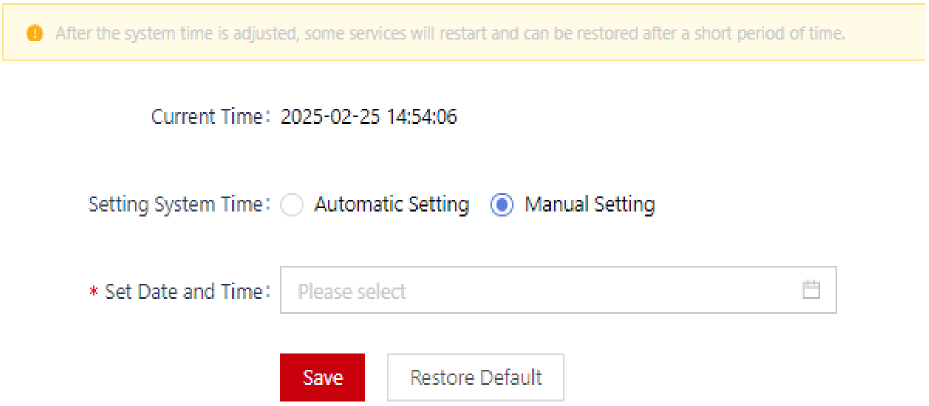
**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

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

**Step 3** Click the **Time Settings** tab.

**Step 4** To manually change the system time, perform the following steps:

**Figure 15-73** Manually changing the system time



After the system time is adjusted, some services will restart and can be restored after a short period of time.

Current Time: 2025-02-25 14:54:06

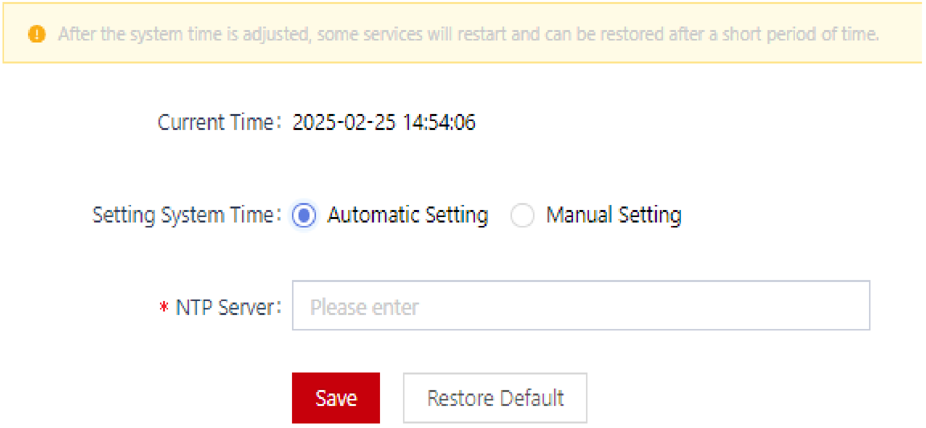
Setting System Time: ○ Automatic Setting ● Manual Setting

* Set Date and Time: Please select

1. Click the drop-down list box of **Set Date and Time**. In the dialog box that is displayed, select the date and time, and click **OK**.
2. Click **Save**. The message "Please restart the service after modifying the system time, otherwise some functions will not take effect." is displayed. Click **Confirm**. The system time is changed.

**Step 5** To automatically set the system time, perform the following steps:

**Figure 15-74** Automatically setting the system time



After the system time is adjusted, some services will restart and can be restored after a short period of time.

Current Time: 2025-02-25 14:54:06

Setting System Time: ● Automatic Setting ○ Manual Setting

* NTP Server: Please enter

1. Enter the IP address or domain name of the time server in the **NTP Server** text box.
2. Click **Save**. The message "Are you sure you want to change it?" is displayed. Click **Confirm**. The system time is changed.

**----End**

### 15.3.10.5.3 Alarm Settings

You can set the trigger value, severity level, and notification frequency.

## Procedure

**Step 1** Log in to a database encryption and access control instance as the **sysadmin** user.

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

**Step 3** Click the **Alarm Settings** tab.

**Step 4** Click **Edit** of the alarm to be modified. In the displayed dialog box, modify the **Threshold Value**, **Level**, and **Frequency** of the alarm.

**Step 5** Click **Confirm**.

**----End**

# 15.4 Security Administrator Operation Guide

## 15.4.1 System Management

### 15.4.1.1 Viewing a Role

By default, the system creates roles such as the system administrator, audit administrator, and security administrator.

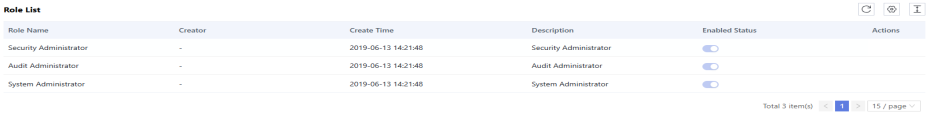
## Procedure

**Step 1** Log in to a database encryption and access control instance as the **secadmin** user.

**Step 2** In the navigation pane on the left, choose **System Management** > **Role Management**.

**Step 3** View the built-in roles, as shown in Figure 15-75.

**Figure 15-75** Viewing the roles



Role List

| Role Name | Creator | Create Time | Description | Enabled Status | Actions |
|---|---|---|---|---|---|
| Security Administrator | - | 2019-06-13 14:21:48 | Security Administrator | | |
| Audit Administrator | - | 2019-06-13 14:21:48 | Audit Administrator | | |
| System Administrator | - | 2019-06-13 14:21:48 | System Administrator | | |

Total 3 item(s) < 1 > 15 / page

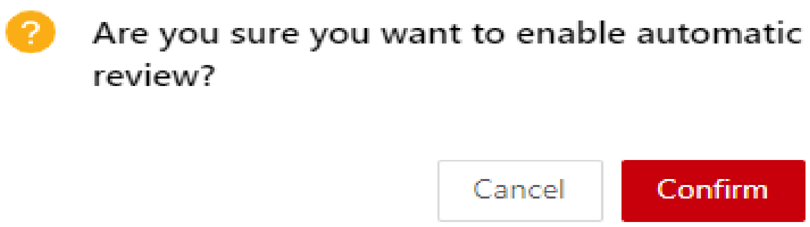
**----End**

### 15.4.1.2 Reviewing an Account

After an account is created, it is available only after being approved by the security administrator. You can choose **Manual Review** or **Automatic Review**.

By default, the security administrator needs to review the account manually.

**Figure 15-76** Automatic review



Are you sure you want to enable automatic review?

## Prerequisites

An account has been created.

## Procedure

**Step 1** Log in to a database encryption and access control instance as the **secadmin** user.

**Step 2** In the navigation pane on the left, choose **System Management** > **Account Review**.

**Step 3** Locate the target account and click **Approve**.

**Step 4** Click **Confirm**.

**----End**

### 15.4.1.3 Configuring Security Settings

To ensure system security, the security administrator can configure the security settings of platform login, account, and network access.

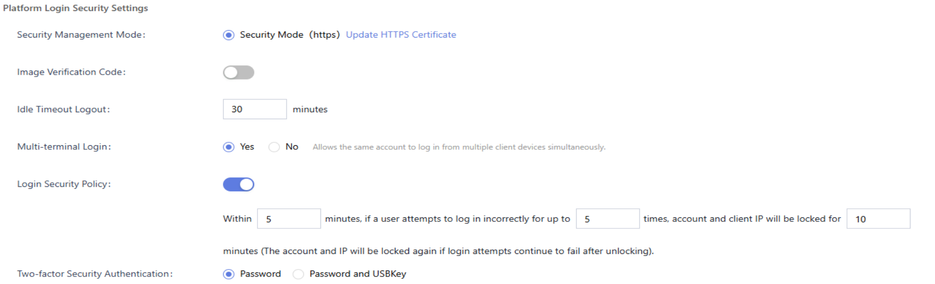
## Procedure

**Step 1** Log in to a database encryption and access control instance as the **secadmin** user.

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

**Step 3** In the **Platform Login Security Settings** area, configure the parameters.

**Figure 15-77** Platform login security settings



Platform Login Security Settings

Security Management Mode: ● Security Mode (https) Update HTTPS Certificate

Image Verification Code:

Idle Timeout Logout: 30 minutes

Multi-terminal Login: ● Yes ○ No Allows the same account to log in from multiple client devices simultaneously.

Login Security Policy:

Within 5 minutes, if a user attempts to log in incorrectly for up to 5 times, account and client IP will be locked for 10 minutes (The account and IP will be locked again if login attempts continue to fail after unlocking).

Two-factor Security Authentication: ● Password ○ Password and USBKey

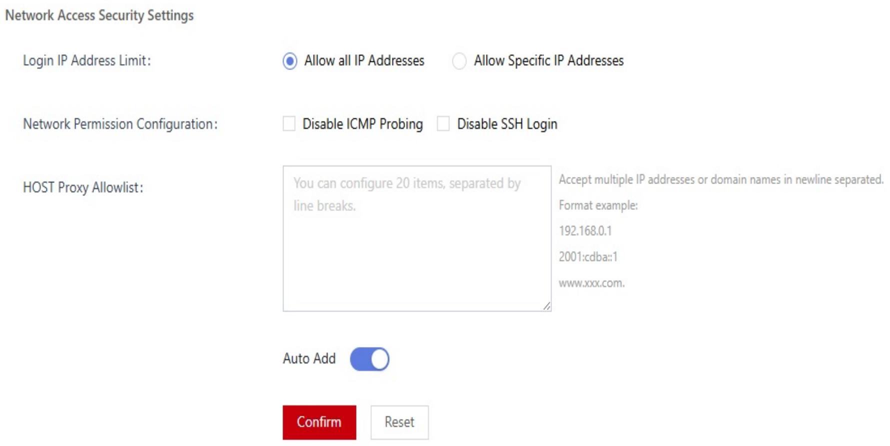
**Table 15-34** Parameters of platform login security settings

| Parameter | Description |
|---|---|
| Security Management Mode | HTTPS security mode is supported with updatable certificates. |
| Image Verification Code | ● You can choose whether to enable this function.<br>● Once enabled, an image verification code is required for system login to prevent brute-force attacks. |
| Idle Timeout Logout | Set the automatic logout interval. |
| Multi-terminal Login | You can choose whether to enable this function.<br>● **Yes**: An account can be logged in at different places.<br>● **No**: An account cannot be logged in at different places. |
| Login Security Policy | ● You can choose whether to enable this function to prevent brute-force attacks.<br>● For example, if the login information is incorrect for three consecutive times within 3 minutes, the account is locked for 5 minutes. |
| Two-factor Security Authentication | Configure the login authentication mode.<br>● **Password**: Only password is required for login.<br>● **Password and USBKey**: You need to enter the password and insert the USBKey with the certificate to the device. |

**Step 4** In the **Account and Password Security Settings** area, set the password validity period.

**Step 5** In the **Network Access Security Settings** area, set the access restrictions.

**Figure 15-78** Network access security settings



Network Access Security Settings

Login IP Address Limit: ● Allow all IP Addresses ○ Allow Specific IP Addresses

Network Permission Configuration: □ Disable ICMP Probing □ Disable SSH Login

HOST Proxy Allowlist: You can configure 20 items, separated by line breaks.

Accept multiple IP addresses or domain names in newline separated.
Format example:
192.168.0.1
2001:cdba::1
www.xxx.com.

Auto Add

**Table 15-35** Parameters of network access security settings

| Parameter | Description |
|---|---|
| Login IP Address Limit | Whether to restrict the access source.<br>● **Accept All IP Addresses**: All IP addresses can access the system.<br>● **Allow Specific IP Addresses**: Only IP addresses in the allowlist can access the console of database encryption and access control. |
| Allowed Login IP Addresses | Enter the allowed IP addresses and separate them with line breaks. |
| Network Permission Configuration | You choose whether to disable ICMP probing and SSH login.<br>● **Disable ICMP Probing**: If you enable this function, other devices cannot ping the system.<br>● **Disable SSH Login**: SSH login is disabled.<br>**NOTE**<br>If **Disable SSH Login** is enabled, O&M engineers cannot access the server background through SSH. |
| Host Proxy Whitelist | Enter the host proxy whitelist. The value can be an IP address or a domain name. |

**Step 6** Click **Confirm**.

**----End**

# 15.5 Operation Guide for Audit Administrators

## 15.5.1 Viewing System Operation Logs

The system stores all operation records. The audit administrator can periodically check the system logs to ensure system security and compliance.

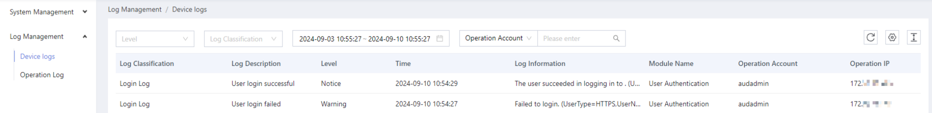
### Procedure

**Step 1** Log in to a database encryption and access control system as the **audadmin** user.

**Step 2** In the navigation pane on the left, choose **Log Management** > **Device Logs**.

**Step 3** (Optional) Set the filtering criteria and search for the related audit logs.

**Figure 15-79** Search settings



| Log Classification | Log Description | Level | Time | Log Information | Module Name | Operation Account | Operation IP |
|---|---|---|---|---|---|---|---|
| Login Log | User login successful | Notice | 2024-09-10 10:54:29 | The user succeeded in logging in to . (U... | User Authentication | audadmin | 172.[redacted] |
| Login Log | User login failed | Warning | 2024-09-10 10:54:27 | Failed to login. (UserType=HTTPS,UserN... | User Authentication | audadmin | 172.[redacted] |

**Step 4** View the logs in the list.

**----End**

## 15.5.2 Viewing System Device Logs

The system stores all device messages. The audit administrator can periodically check the device logs to ensure system security and compliance.

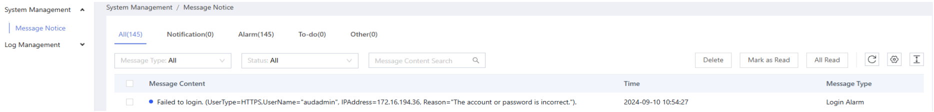
### Procedure

**Step 1** Log in to a database encryption and access control system as the **audadmin** user.

**Step 2** In the navigation pane on the left, choose **Log Management** > **Device Logs**.

**Step 3** (Optional) Set the filtering criteria and search for the related device logs.

**Figure 15-80** Setting filter criteria



Message Type: All
Status: All

| | Message Content | Time | Message Type |
|---|---|---|---|
| □ | ● Failed to login. (UserType=HTTPS,UserName="audadmin", IPAddress=172.16.194.36, Reason="The account or password is incorrect."). | 2024-09-10 10:54:27 | Login Alarm |

**Step 4** View the logs in the list.

**----End**

# 16 Permission Control

## 16.1 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 16-1**).

### Prerequisites

Before authorizing permissions to a user group, you need to know which DBSS permissions can be added to the user group. **Table 16-1** describes the policy details. For details about system permissions supported by DBSS, see **DBSS Permissions**.

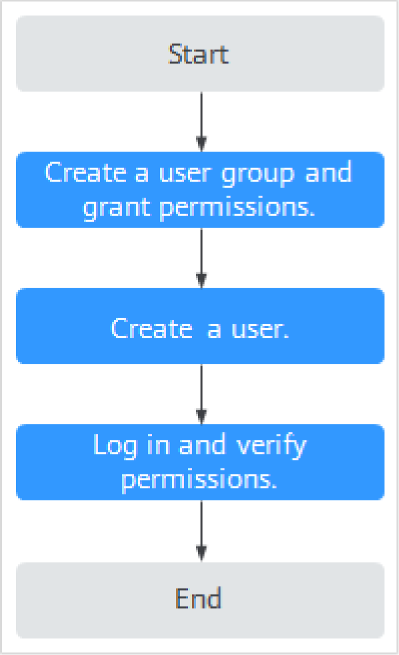
**Table 16-1** System permissions

| 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 16-1** Process for granting permissions


Start
Create a user group and grant permissions.
Create  a user.
Log in and verify permissions.
End

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.

# 16.2 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"
            ]
        }
    ]
}
```

# 16.3 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 16-2** lists the API actions supported by DBSS.

**Table 16-2** 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 |

# 16.4 Configuring FullAccess Sensitive Permissions

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

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

For details about sensitive permissions, see **Table 16-3**. The permission details are as follows:

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

**Table 16-3** Description of sensitive permissions

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

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