Database Security Service (DBSS)

User Guide

Issue	01
Date	2025-12-19

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions


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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 1-1**).

Prerequisites

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

Table 1-1 System permissions

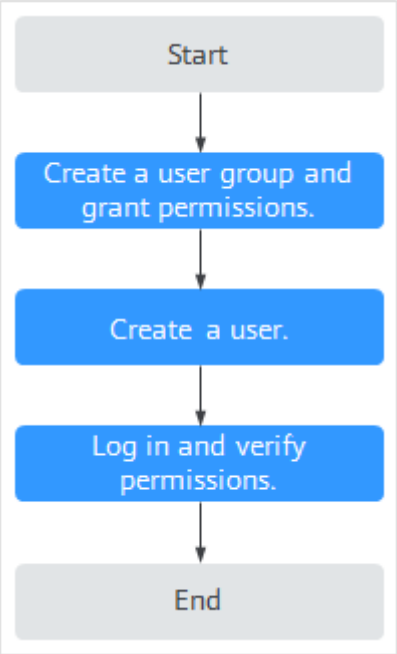
Role/Policy Name	Description	Type	Dependency
DBSS Audit Administrator	DBSS audit administrator, who has the permissions to check DBSS security logs.	System-defined role	None
DBSS FullAccess	Full permissions for DBSS	System-defined policy	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Role/Policy Name	Description	Type	Dependency
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 1-1 Process for granting permissions



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

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

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

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

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

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2 Purchasing DBSS

This section describes how to purchase DBSS. DBSS charges yearly or monthly.

Constraints

- DBSS cannot be used across regions and the database must be in the same region as the instance you purchased.
- 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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

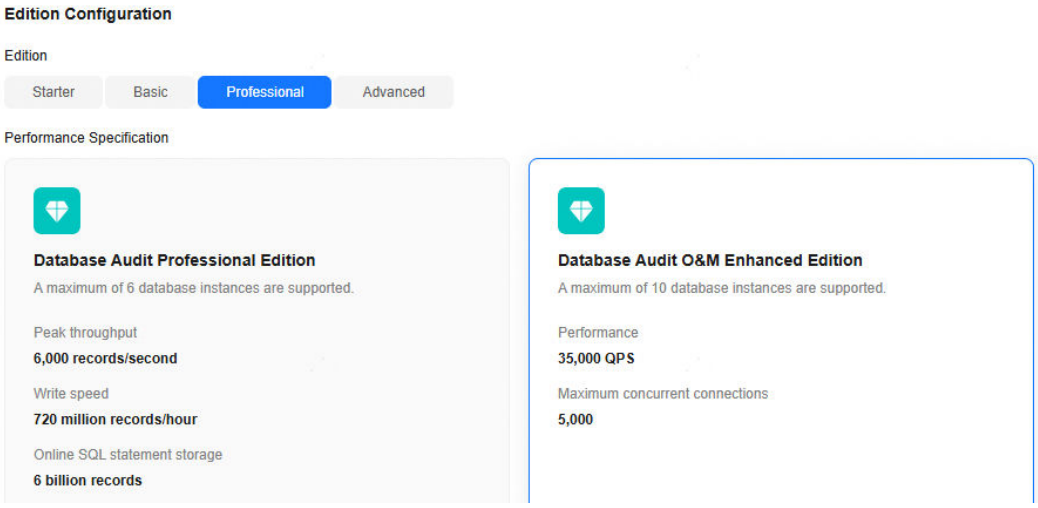
Step 3 In the upper right corner, click **Buy DBSS**.

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

When **Edition** is set to **Professional**, you can select **Database Audit and O&M Enhanced Edition**, as shown in Figure 2-1.

When **Edition** is set to **Advanced**, you can select **Database Audit Encryption Enhanced Edition**, as shown in Figure 2-2.

Figure 2-1 Buying database audit O&M enhanced edition



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 2-2 Buying database audit encryption enhanced edition

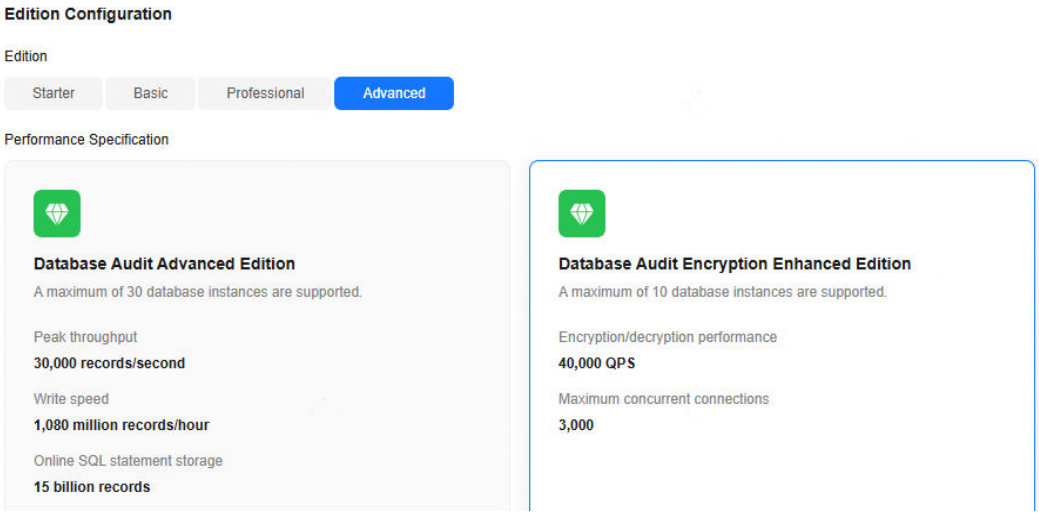


Table 2-1 Basic configuration parameters

Parameter	Description
Service Type	The value is fixed at **Database Audit Service**.
Billing Mode	Only the yearly/monthly mode is available.
Category	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. You can select random allocation or specify an AZ.
Standby AZ	This parameter is displayed when **Edition** is set to **Advanced** > **Database Audit Encryption Enhanced Edition**. Instances can be deployed in one AZ.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 2-2 DBSS editions

Edition	Specification	Maximum Databases	System Resource	Performance
Starter	Database audit starter edition	1	-	• Peak QPS: 1,000 queries/second • Database load rate: 1.2 million statements/hour • Online SQL statement storage: 100 million statements
Basic	Database audit basic edition	3	-	• Peak QPS: 3,000 queries/second • Database load rate: 3.6 million statements/hour • Online SQL statement storage: 400 million statements
Professional	Database audit professional edition	6	-	• Peak QPS: 6,000 queries/second • Database load rate: 7.2 million statements/hour • Online SQL statement storage: 600 million statements
	Database audit O&M enhanced edition	10	• CPU: 8 vCPUs • Memory: 16 GB	• Performance: 35,000 QPS • Maximum concurrent connections: 5000

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Edition	Specification	Maximum Databases	System Resource	Performance
Advanced	Database audit advanced edition	30	-	• Peak QPS: 30,000 queries/second • Database load rate: 10.8 million records/hour • Online SQL statement storage: 1.5 billion statements
	Database audit encryption enhanced edition	10	• CPU: 16 vCPUs • Memory: 32 GB	• Encryption/decryption performance: 40,000 QPS • Maximum concurrent connections: 3000

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 described in **Table 2-3**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 2-3 Network configuration

Figure 2-4 Advanced configuration

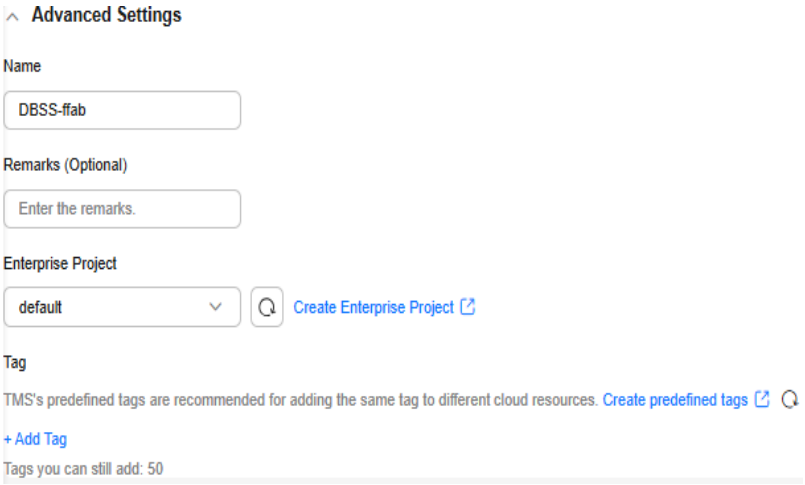


Table 2-3 Database audit parameters

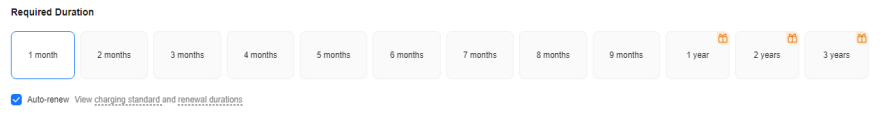
Parameter	Description
VPC	You can select an existing VPC, or click **View VPC** to create one on the VPC console. **NOTE** • Select the VPC of the node (application or database side) where you plan to install the agent. For more information, see **How Do I Determine Where to Install an Agent?** • To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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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. 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. An enterprise project groups cloud resources, so you can manage resources and members by project. The default project is **default**. 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 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 2-5**.

Figure 2-5 Setting the required duration



After you select **Auto-renew**, the system automatically renews the instance upon expiry if your account balance is sufficient. You can continue to use the instance. **Table 2-4** describes the auto-renewal period.

Table 2-4 Auto-renewal period description

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Required Duration	Auto-renewal Period
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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3 Database Audit

3.1 Viewing the Database Audit Overview

After the added database is connected to the database audit instance, you can enable scheduled database audit update on the overview page to view the audit information of each instance and the audit information about statements, risks, and sessions of all instances.

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.**

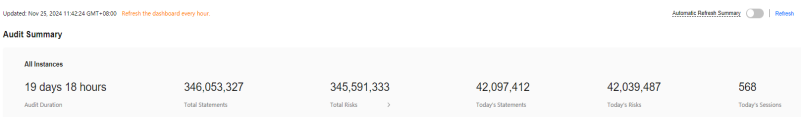
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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 3-1 Viewing audit summary



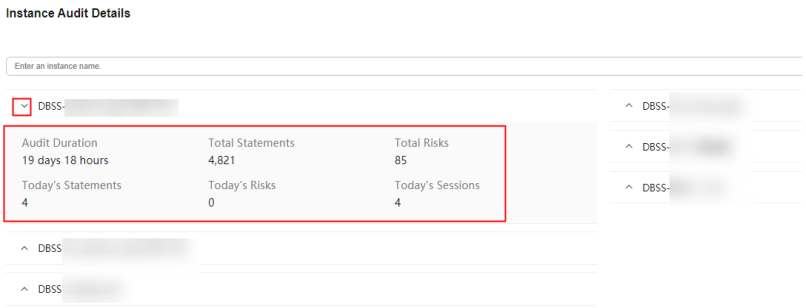
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

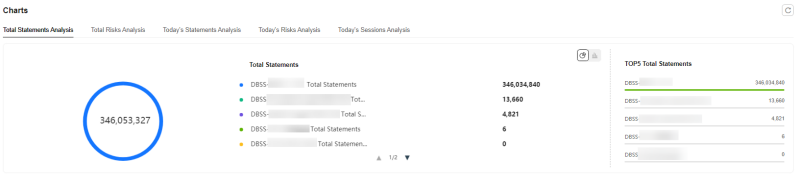
  Figure 3-2 Viewing single instance information

- Data analysis charts

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

  Figure 3-3 Viewing the data analysis chart

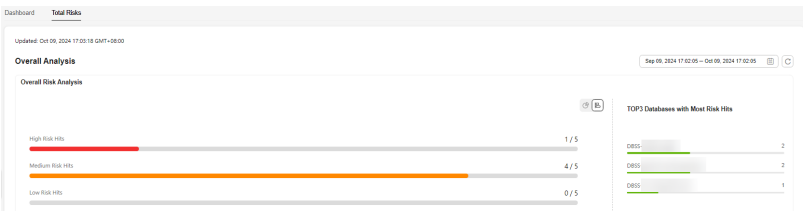
  

Step 4 Click **Total Risks**. The **Total Risks** page is displayed. Click  and select a time range to view the risk analysis of all database audit instances in the specified time range.

- 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 3-4 Overall risk analysis

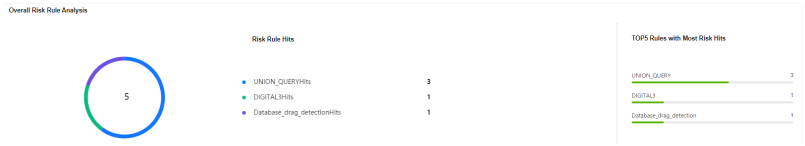
  

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- Overall risk rule analysis

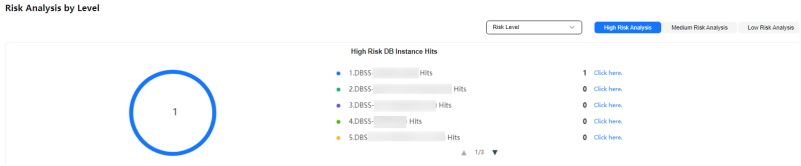
  Displays the number of risk rule hits of all databases and top 5 risk rule hits.

  Figure 3-5 Overall risk rule analysis

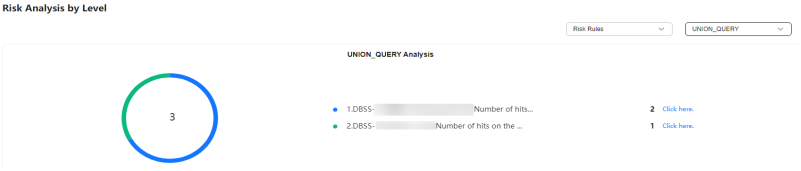
- Risk analysis by level
  - Risk level: displays the high-risk hit analysis, medium-risk hit analysis, and low-risk hit analysis of each database.

    Figure 3-6 Risk level analysis

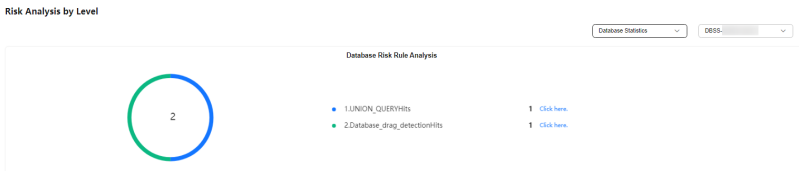
  - Risk rule: displays the analysis when a database is hit by a risk rule.

    Figure 3-7 Risk rule analysis

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

    Figure 3-8 Database statistics analysis

----End

Related Operations

- 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 **Configuring Audit Rules**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3.2 Configuring and Enabling Database Audit

3.2.1 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 to be 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?**

Configuring Database Audit

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-9 Configuring database audit without installing agent

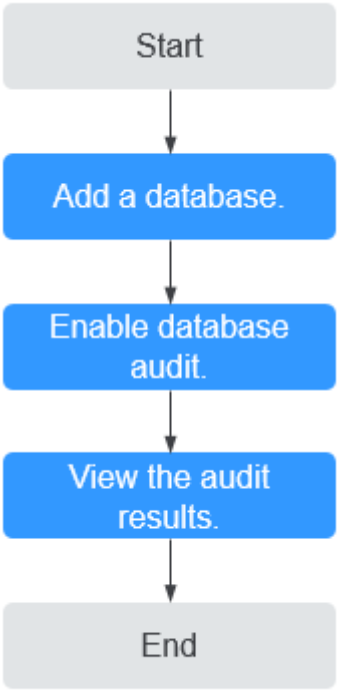
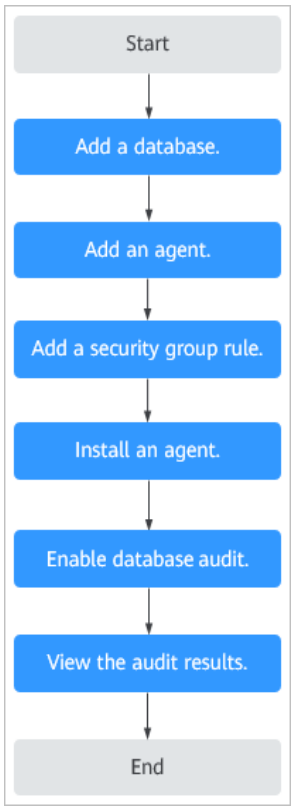


Figure 3-10 Process



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 3-1 Procedure of configuring database audit without installing agent

Step	Configuration	Description
1	**Step 1: Add a Database**	After purchasing DBSS, you need to add the database to be audited to the instance.
2	**Step 5: Enable Database Audit**	Enable database audit and connect the added database to the database audit instance.
3	**Viewing Audit Data**	By default, database audit complies with a **full audit rule**, which is used to audit all databases that are connected to the database audit instance. You can view the audit result on the database audit page. **NOTICE** You can set database audit rules as required. For details about how to configure an audit rule, see **Configuring an Audit Scope Rule**.

Table 3-2 Procedure of configuring database audit by installing the agent

Step	Configuration	Description
1	**Step 1: Add a Database**	Purchase database audit. Add a database to the database audit instance and enable audit for the database.
2	**Step 2: Add an Agent**	Select an agent add mode. Database audit supports auditing databases built on ECS, BMS, and RDS on Huawei Cloud. Select an agent add mode based on your database deployed on Huawei Cloud.
3	**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.
4	• **Installing an Agent (Linux OS)** • **Installing an Agent (Windows OS)**	Download and then install the agent on the database or application based on the add mode you chose.
5	**Step 5: Enable Database Audit**	Enable database audit and connect the added database to the database audit instance.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step	Configuration	Description
6	Viewing Audit Data	By default, database audit complies with a **full audit rule**, which is used to audit all databases that are connected to the database audit instance. You can view the audit result on the database audit page. **NOTICE** You can set database audit rules as required. For details about how to configure an audit rule, see **Configuring an Audit Scope Rule**.

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.

3.2.2 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.

Supported Database Types and Versions in Agent Installation-Free Mode

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 3-3 Agent-free relational databases

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

Supported Database Types and Versions in Agent Installation Mode

For a database whose type and version are listed in **Table 3-4**, you need to install an agent to enable the database audit.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 3-4 Database types and editions supported by database audit

Database Type	Version
MySQL **NOTICE** The database versions supported by the agent-free mode are different from those supported by the agent mode. For details, see **Constraints**.	• 5.0, 5.1, 5.5, 5.6, and 5.7 • 8.0 (8.0.11 and earlier) • 8.0.30 • 8.0.33 • 8.0.35 • 8.1.0 • 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 • 12c 12.1.0.2.0, 12.2.0.1.0 • 19c
PostgreSQL	• 7.4 • 8.0, 8.1, 8.2, 8.3, and 8.4 • 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, and 9.6 • 10.0, 10.1, 10.2, 10.3, 10.4, and 10.5 • 11 • 12 • 13 • 14
SQL Server	• 2008 • 2012 • 2014 • 2016 • 2017
TaurusDB	8.0
DWS	• 1.5 • 8.1
DAMENG	DM8
KINGBASE	V8
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8
Gbase XDM Cluster	V8.0

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-11 Adding a database

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

Table 3-5 Parameters

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
Version	Supported database versions **NOTICE** The database versions supported by the agent-free mode are different from those supported by the agent mode. For details, see **Constraints**. • When **Type** is set to **MySQL**, the following versions are available: – 5.0, 5.1, 5.5, 5.6, and 5.7 – 8.0 (8.0.11 and earlier) – 8.0.30 – 8.0.35 – 8.1.0 – 8.2.0 • When **Type** is set to **ORACLE**, the following versions are available: – 11g – 12c – 19c • When **Type** is set to **PostgreSQL**, the following versions are available: – 7.4 – 8.0, 8.1, 8.2, 8.3, and 8.4 – 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, and 9.6 – 10.0, 10.1, 10.2, 10.3, 10.4, and 10.5 – 11.0 – 12.0 – 13.0 – 14.0 • When **Type** is set to **SQLServer**, the following versions are available: – 2008 – 2012 – 2014 – 2016 – 2017 • When **Type** is set to **DWS**, the following versions are available: – 1.5 – 8.1	5.0

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
	• When **Type** is set to **GaussDB(for MySQL)**, the following versions are available: – When **Database Type** is set to **Self-built database**, you can select the **Mysql 8.0** version. – If **RDS database** is selected, a list of database instances will be displayed for you to choose from. You do not need to install the agent. • When **Type** is set to **TaurusDB**, the following edition is available: – When **Database Type** is set to **Self-built database**, you can select the **Mysql 8.0** version. – If **RDS database** is selected, a list of database instances will be displayed for you to choose from. You do not need to install the agent. • When **Type** is set to **GaussDB**, the following version is available: – 1.4 Enterprise Edition – 1.3 Enterprise Edition – 2.8 Enterprise Edition – 3.223 Enterprise Edition • When **Type** is set to **DAMENG**, the following version is available: – DM8 • When **Type** is set to **KINGBASE**, the following version is available: – V8 • When **Type** is set to **HBase**, the following versions are available: – 1.3.1 – 2.2.3 • When **Type** is set to **SHENTONG**, the following version is available: – 7.0 • When **Type** is set to **GBase 8a**, the following version is available: – 8.5 • When **Type** is set to **GBase XDM Cluster**, the following version is available:	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

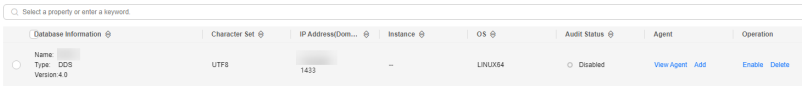
Parameter	Description	Example Value
	– 8.0 • When **Type** is set to **GBase 8s**, the following version is available: – v8.8 • When **Type** is set to **Greenplum**, the following version is available: – v6.0 • When **Type** is set to **HighGo**, the following version is available: – v6.0 • When **Type** is set to **MongoDB**, the following version is available: – v5.0 • When **Type** is set to **MariaDB**, the following version is available: – 10.6 • When **Type** is set to **Hive**, the following versions are available: – 1.2.2 – 2.3.9 – 3.1.2 – 3.1.3 • When **Type** is set to **TDSQL**, the following version is available: – 10.3.17.3.0 • When **Type** is set to **Vastbase**, the following edition is available: – G100 V2.2 • When **Type** is set to **TiDB**, the following editions are available: – V4 – V5 – V6 – V7 – V8	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
Instance	Instance name of the database to be audited **NOTE** • If you do not configure the **Instance** field, database audit will audit all instances in the database. • If you enter an instance name, database audit will audit the entered instance. Enter a maximum of five instance names and use semicolons (;) to separate instance names.	-
Character Set	Encoding format of the database character set. The options are as follows: • UTF-8 • GBK	UTF-8
OS	OS of the added database. The options are as follows: • LINUX64 • WINDOWS64	LINUX64

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

Figure 3-12 Successfully adding a database



NOTE

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

----End

3.2.3 Step 2: Add an Agent

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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**.

- TaurusDB
- 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

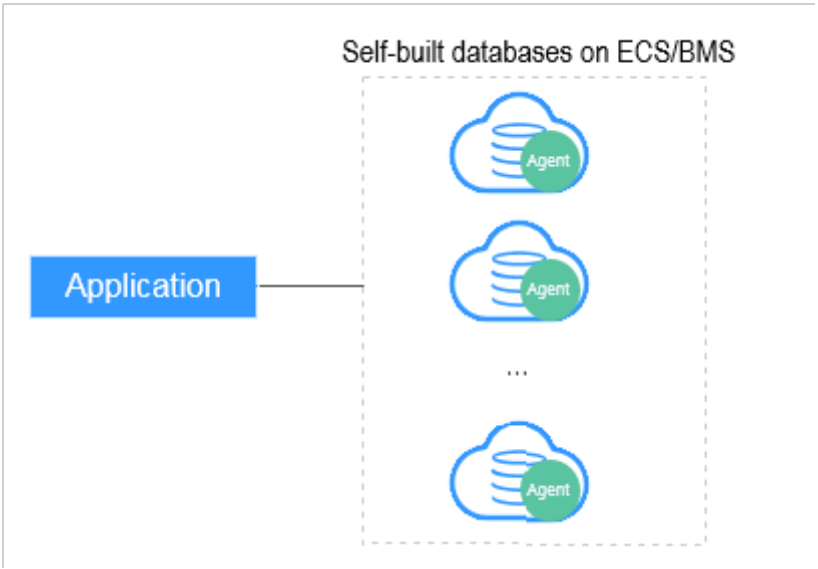
The database audit instance is in the **Running** state.

Scenarios

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

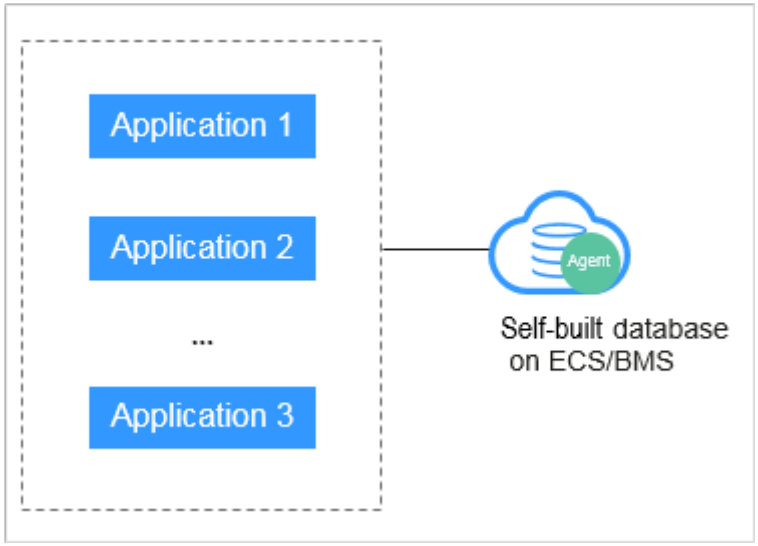
- Deploy DBSS for databases built on ECS/BMS. For details, see **Figure 3-13** and **Figure 3-14**.

  Figure 3-13 One application connecting to multiple databases built on ECS/BMS



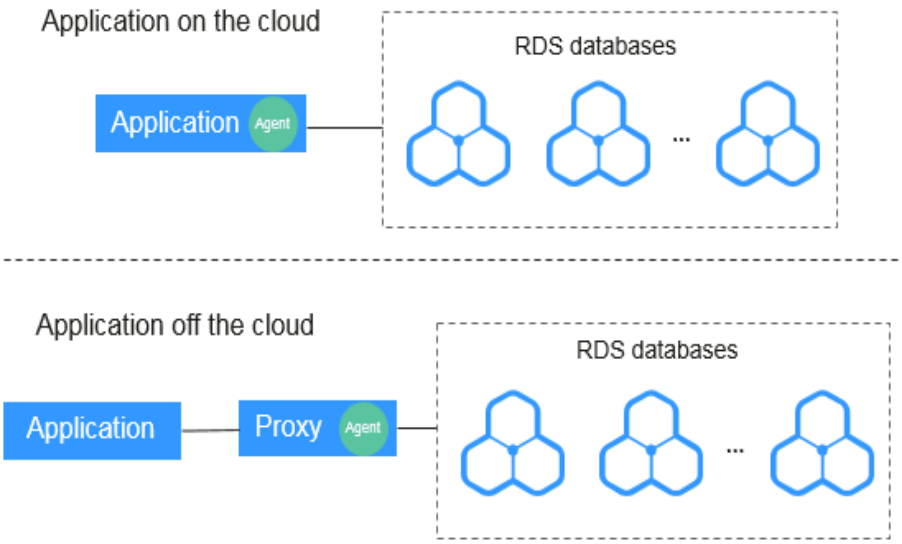
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-14 Multiple applications connecting to one database built on ECS/BMS



- Deploy DBSS for RDS databases. For details, see **Figure 3-15** and **Figure 3-16**.

Figure 3-15 One application connecting to multiple RDS databases



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-16 Multiple applications connecting to one RDS database

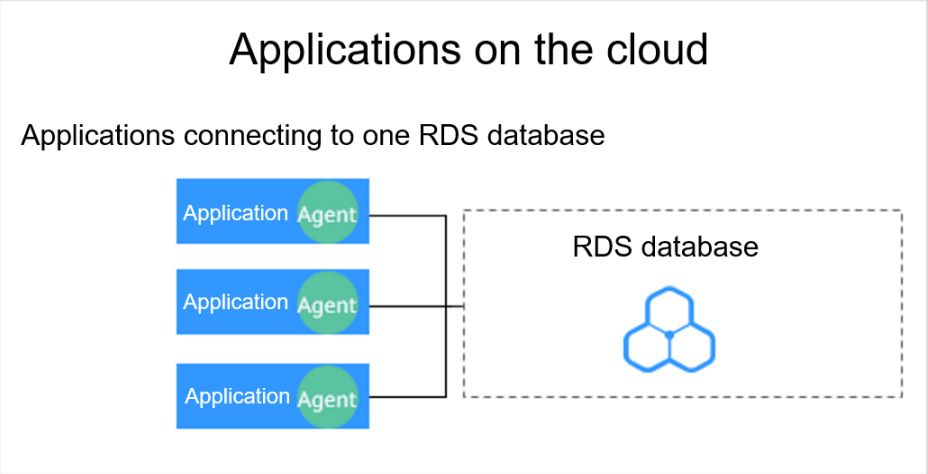


Table 3-6 provides more details.

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 3-6 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. • If an application connects to multiple databases built on ECS/BMS, the agent must be added on all these databases.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Scenario	Where to Add the Agent	Audit Scope	Description
RDS database	Application (if applications are deployed on the cloud)	Access records of all the databases connected to the application	• Add the agent on the application side. • If an application connects to multiple RDS databases, add an agent on each of the databases. Set **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**. • 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. • **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.**

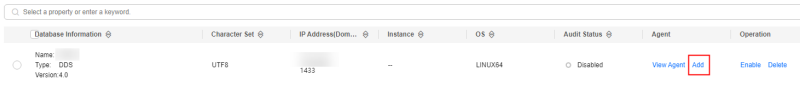
Step 3 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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 3-17 Adding an agent



Step 7 In the displayed dialog box, select an add mode, as shown in **Figure 3-18**. For details about related parameters, see **Table 3-7**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-18 Adding an agent to a database

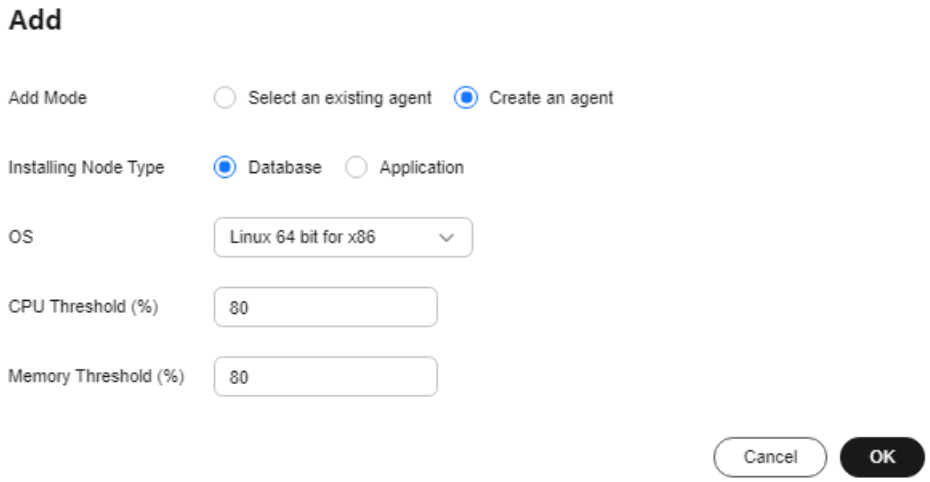


Table 3-7 Parameters for adding an agent (user-built databases on ECS/BMS)

Parameter	Description	Example Value
Add Mode	Mode for adding an agent • **Select an existing agent** If an agent has been installed on a database connected to the same application as the desired database, select **Select an existing agent**. • **Create an agent** If no agent is available, select **Create an agent** to create one.	Create an agent
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**. 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**. When auditing user-installed databases on ECS/BMS, select **Database** or **Application** for **Installing Node Type**.	Database

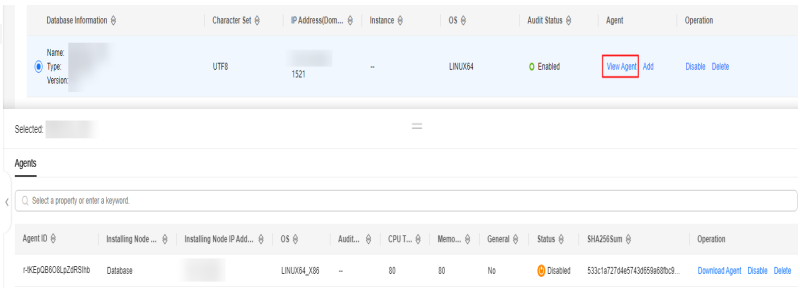
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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. 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**. OS of the database to be audited. The value can be **LINUX64_x86 , LINUX64_Arm,** or **WINDOWS64**. **NOTE** 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 3-19 Successfully adding an agent



NOTE

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

----End

Adding an Agent (RDS Databases)

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- 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.**

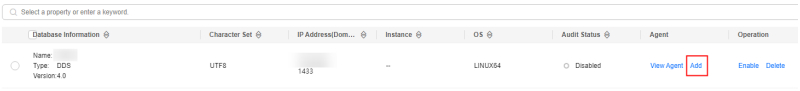
Step 3 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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 3-20 Adding an agent



Step 7 In the displayed dialog box, select an add mode, as shown in **Figure 3-21** and **Figure 3-22**. For details about related parameters, see **Table 3-8**.

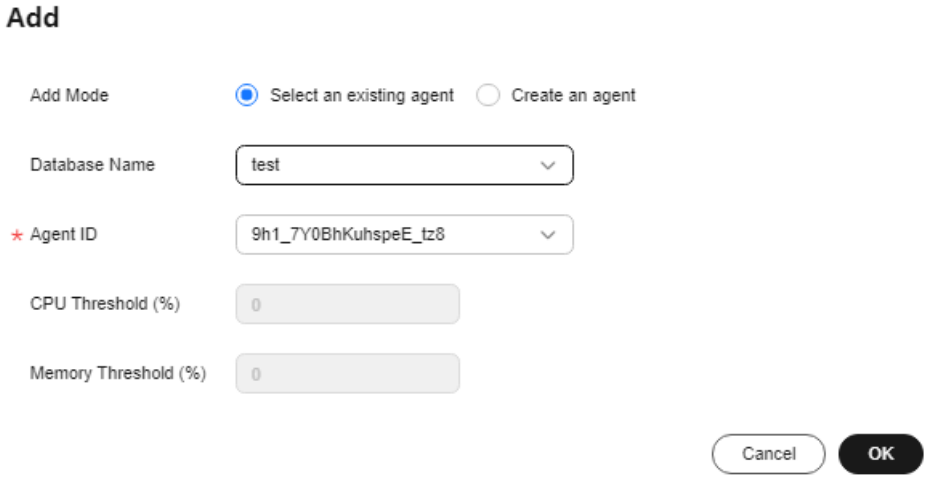
- Select **Select an existing agent** for **Add Mode**.

  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 3-21 Selecting an existing agent



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

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

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-22 Adding an agent to an application

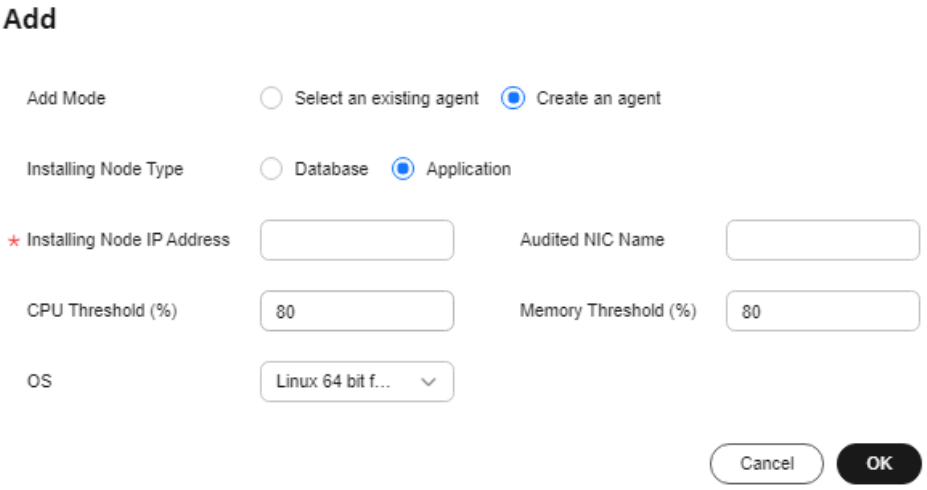


Table 3-8 Parameters for adding an agent (RDS databases)

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

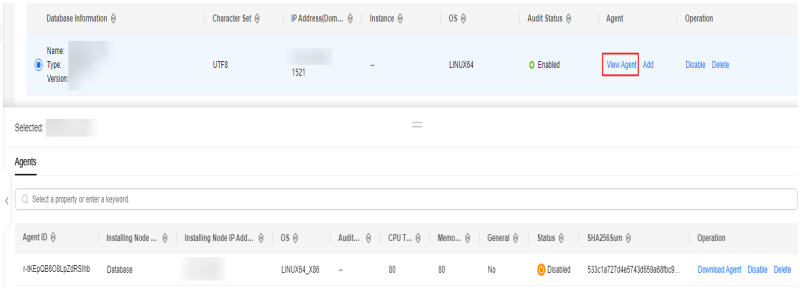
Parameter	Description	Example Value
Installing Node IP Address	This parameter is mandatory when **Installing Node Type** is set to **Application**. IP address of the application node to be audited. You can enter only one IP address. The IP address must be the internal IP address of the application node. IPv4 and IPv6 formats are both supported. **NOTICE** To audit an RDS database connected to an off-cloud application, set this parameter to the IP address of the proxy.	192.168.1.1
Audited NIC Name	Optional. This parameter is configurable if **Installing Node Type** is set to **Application**. Name of the network interface card (NIC) of the application node to be audited	-
CPU Threshold (%)	Optional. This parameter is configurable if **Installing Node Type** is set to **Application**. CPU threshold of the application node to be audited. The default value is **80**. **NOTICE** If the CPU usage of a server exceeds the threshold, the agent on the server will stop running.	80
Memory Threshold (%)	Optional. This parameter is configurable if **Installing Node Type** is set to **Application**. Memory threshold of the application node to be audited. The default value is **80**. **NOTICE** If the memory usage of your server exceeds the threshold, the agent will stop running.	80
OS	Optional. This parameter is configurable if **Installing Node Type** is set to **Application**. OS of the application node to be audited. The value can be **LINUX64_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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-23 Successfully adding an agent



NOTE

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

----End

Follow-Up Procedure

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

3.2.4 Step 3: Download and Install the Agent

3.2.4.1 Downloading an Agent

Download and then install the agent on the database or application, as required by the add mode you chose.

NOTE

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

Prerequisites

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.

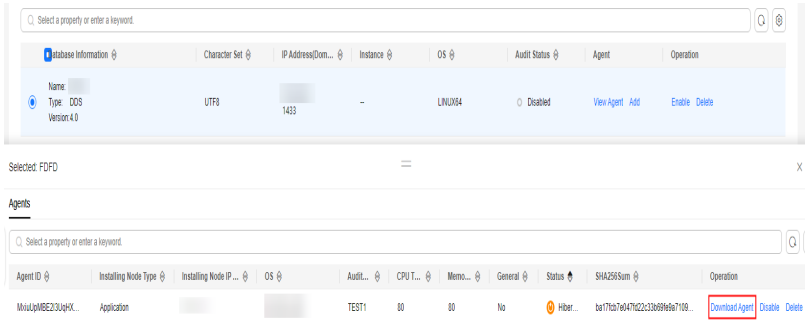
Step 4 In the navigation tree on the left, choose **Databases**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 3-24 Downloading an Agent



Download the agent installation package suitable for your OS.

- Linux OS

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

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

----End

3.2.4.2 Installing an Agent (Linux OS)

You can enable database audit only after the agent is installed. This topic describes how to install the agent on a node running a Linux OS. 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 3-25** and **Figure 3-26**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-25 One application connecting to multiple databases built on ECS/BMS

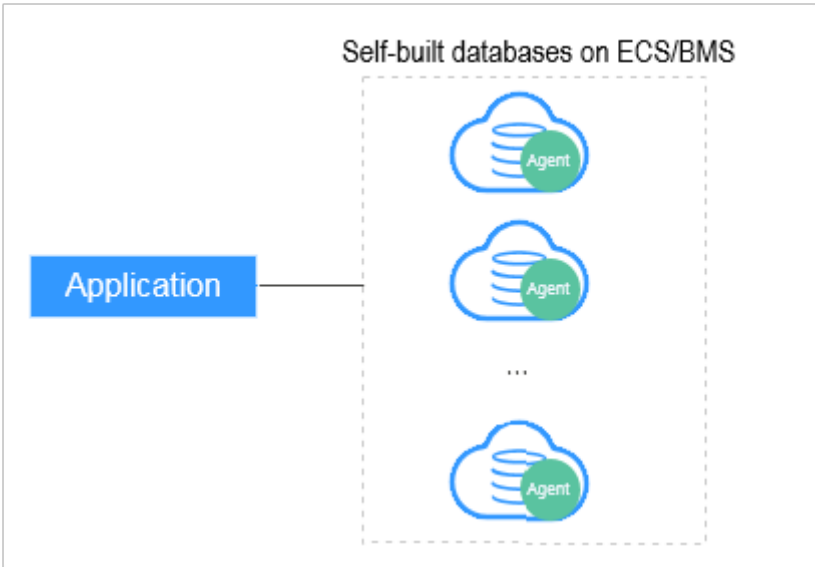
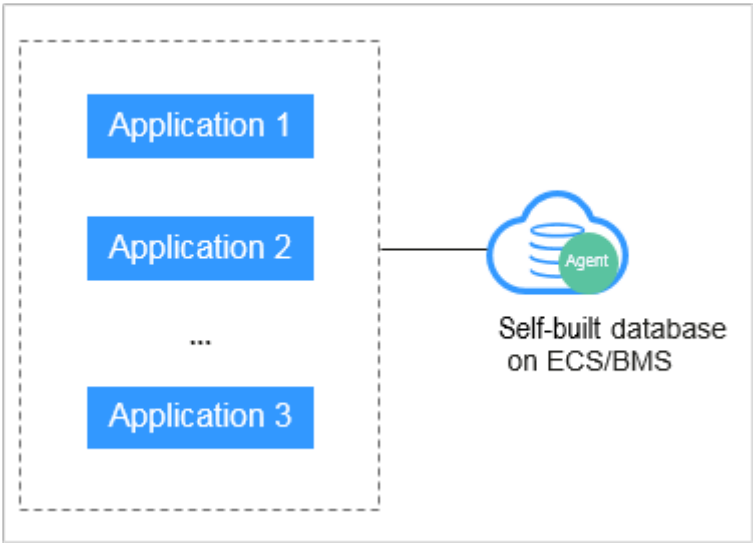


Figure 3-26 Multiple applications connecting to one database built on ECS/BMS



- Deploy DBSS for RDS databases. For details, see **Figure 3-27** and **Figure 3-28**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-27 One application connecting to multiple RDS databases

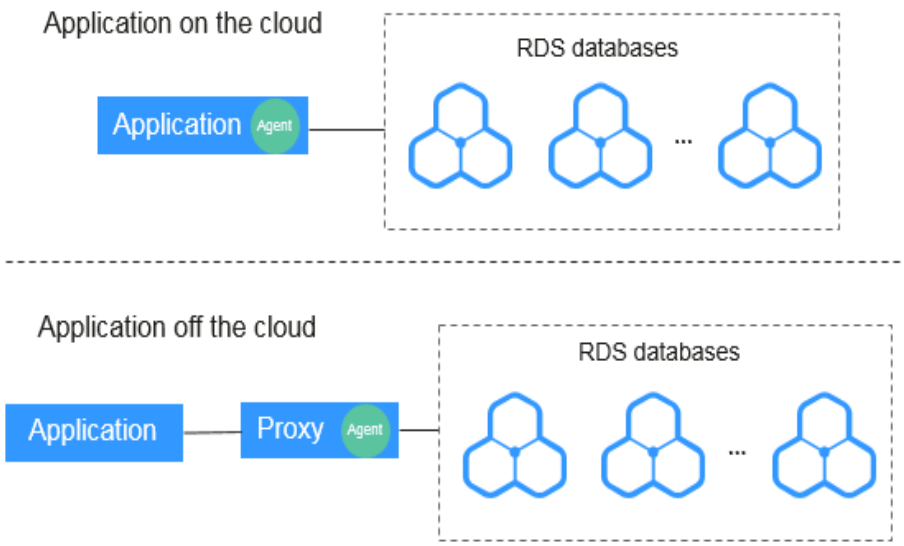


Figure 3-28 Multiple applications connecting to one RDS database

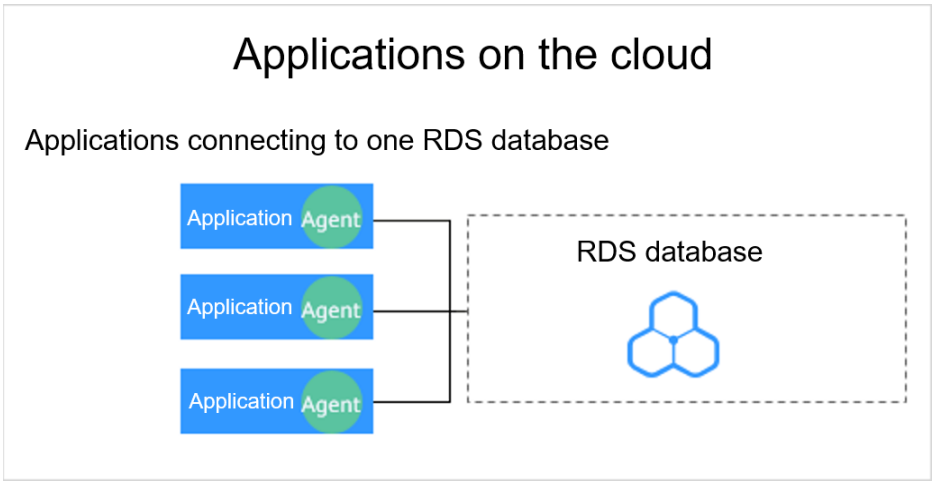


Table 3-9 describes where to install the agent in the preceding scenarios.

NOTICE

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 3-9 Agent installation scenarios

Scenario	Where to Install Agent	Audit Scope	Description
Self-built database on ECS/BMS	Database	All access records of applications that have accessed the database	• Install the agent on the database side. • If an application connects to multiple databases built on ECS/BMS, the agent must be installed on all these databases.
RDS database	Application side (if applications are deployed on the cloud)	Access records of all the databases connected to the application	• Install the agent on the application side. • If multiple applications are connected to the same RDS database, the agent must be installed on all these applications.
RDS database	Proxy side (if applications are deployed off the cloud)	Only the access records between the proxy and database. Those between the applications and database cannot be audited.	Install the agent on the proxy side.

Installing an Agent

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*

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
[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 :
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

NOTE

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

----End

Helpful Links

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

3.2.4.3 Installing an Agent (Windows OS)

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

Prerequisites

- 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?**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 3-29** and **Figure 3-30**.

  Figure 3-29 One application connecting to multiple databases built on ECS/BMS

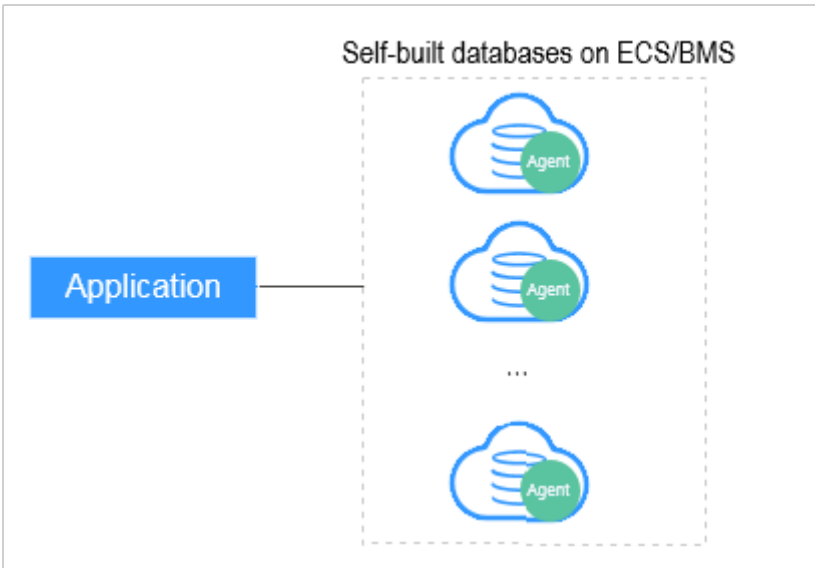
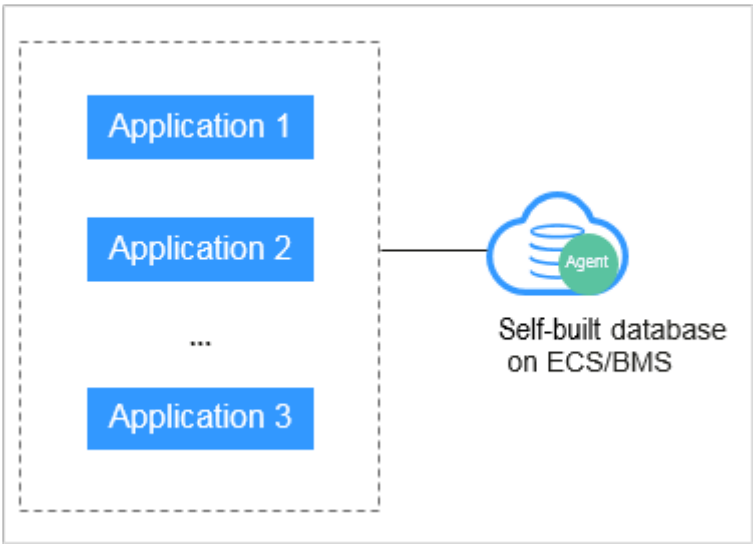
  

  Figure 3-30 Multiple applications connecting to one database built on ECS/BMS

- Deploy DBSS for RDS databases. For details, see **Figure 3-31** and **Figure 3-32**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-31 One application connecting to multiple RDS databases

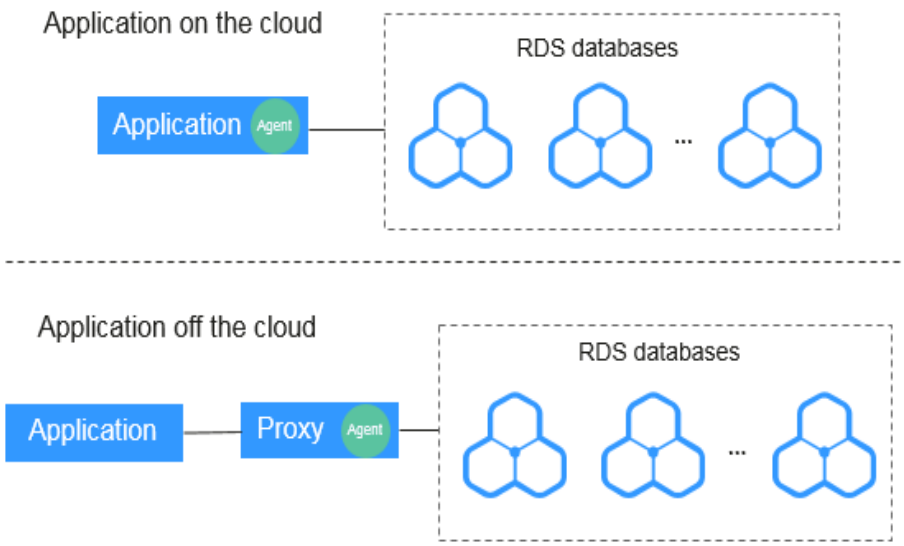


Figure 3-32 Multiple applications connecting to one RDS database

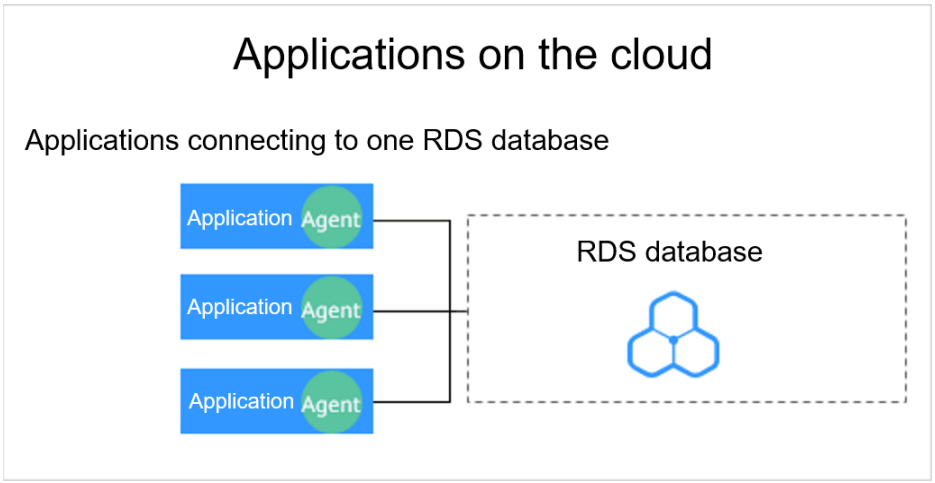


Table 3-10 describes where to install the agent in the preceding scenarios.

NOTICE

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 3-10 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. • If an application connects to multiple databases built on ECS/BMS, the agent must be installed on all these databases.
RDS database	Application side (if applications are deployed on the cloud)	Access records of all the databases connected to the application	• Install the agent on the application side. • If multiple applications are connected to the same RDS database, the agent must be installed on all these applications.
RDS database	Proxy side (if applications are deployed off the cloud)	Only the access records between the proxy and database. Those between the applications and database cannot be audited.	Install the agent on the proxy side.

Installing an Agent

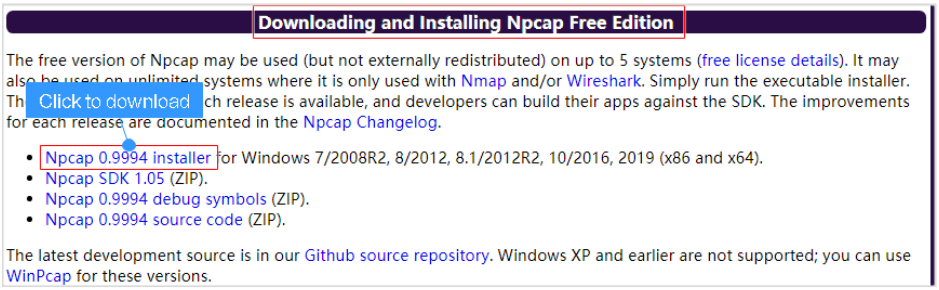
Step 1 For details about how to add an agent, see **Step 2**.

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 3-33 Downloading Npcap

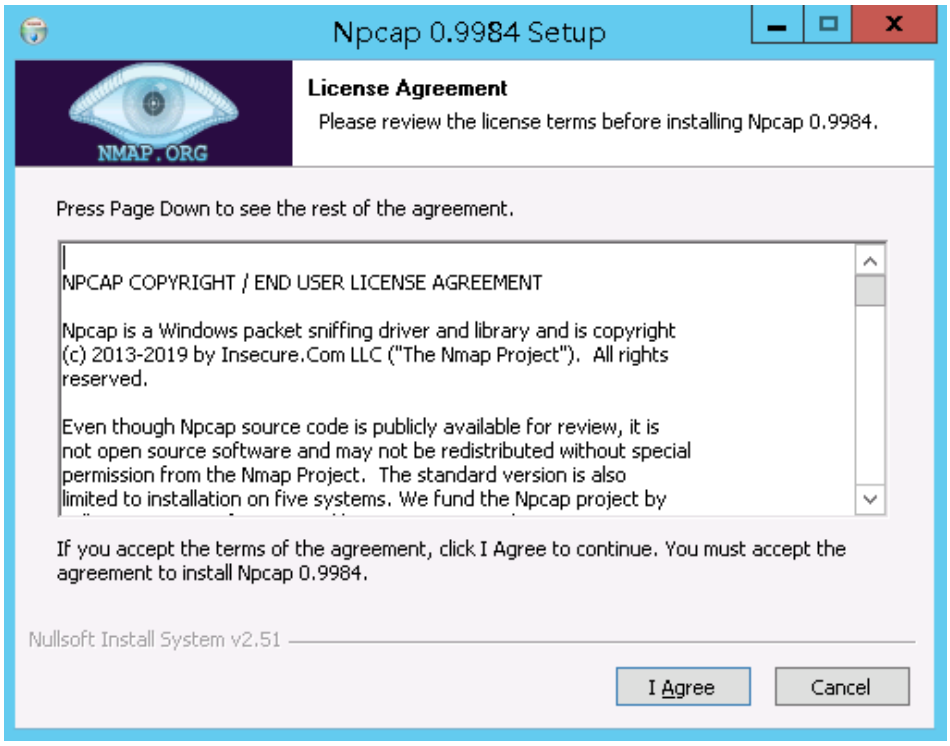
  b. Upload the **npcap-*xxxx*.exe** software installation package to the VM where the agent is to be installed.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

c. Double-click the Npcap installation package.

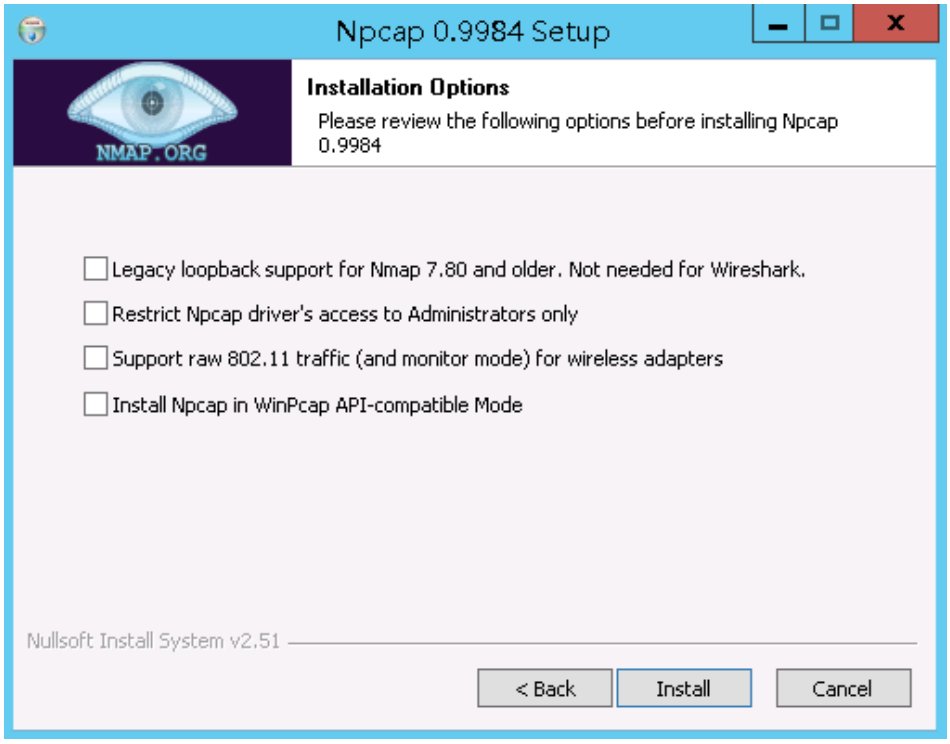
d. In the displayed dialog box, click **I Agree**, as shown in **Figure 3-34**.

Figure 3-34 Agreeing to install Npcap



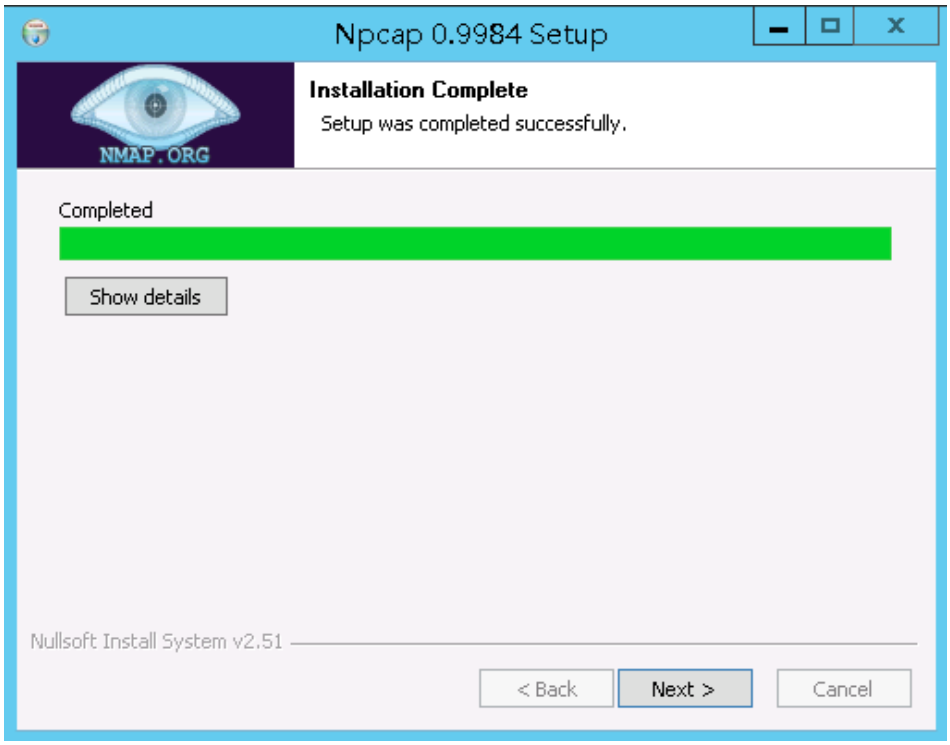
e. In the displayed dialog box, leave all the check boxes unselected and click **Install**, as shown in **Figure 3-35**.

Figure 3-35 Installing Npcap

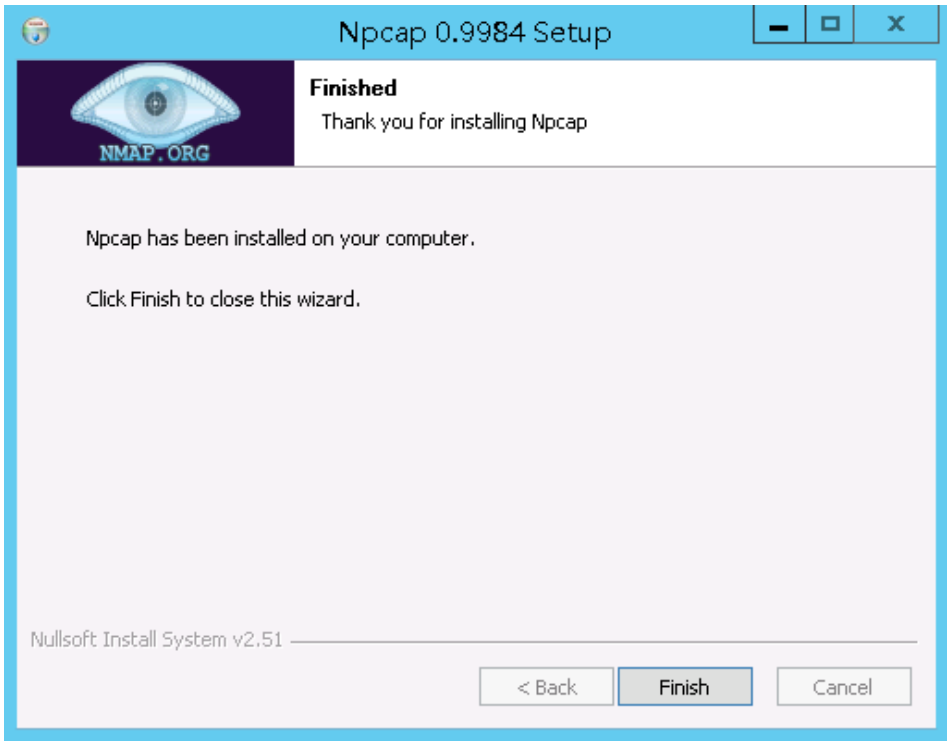


 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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



g. Click **Finish**.

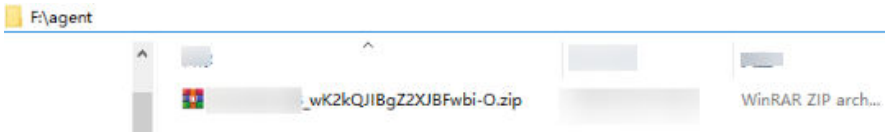


Step 3 For details about how to obtain the agent installation package of the Windows, see **Downloading an Agent**.

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-36 Agent installation package



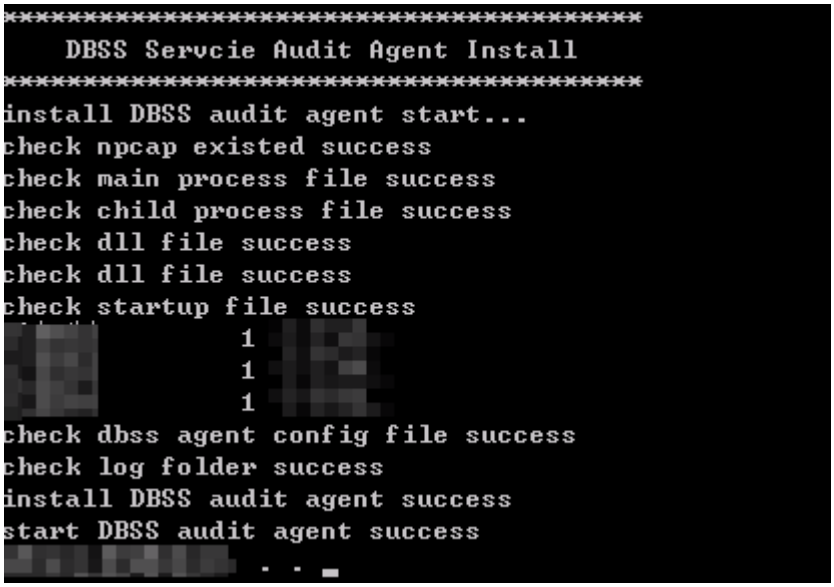
Step 5 Decompress the package.

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

Figure 3-37 Double-click install.bat

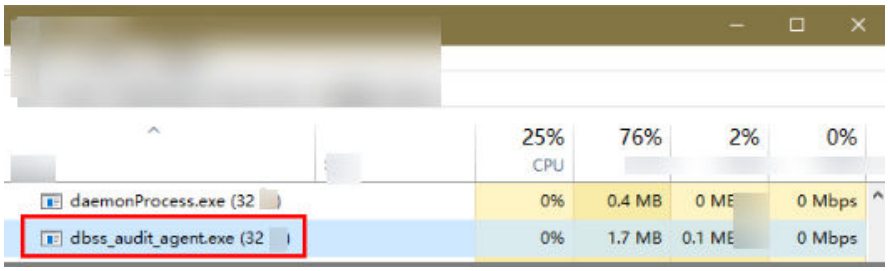
Step 7 Press any key to complete installation after the output shown in **Figure 3-38** is displayed.

Figure 3-38 Installation completed



Step 8 Check the installation result. If the dbss_audit_agent process can be found in the Windows Task Manager, the installation succeeded, as shown in the **Figure 3-39**.

Figure 3-39 Checking the dbss_audit_agent process



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

If it is not found, install the agent again.

----End

3.2.5 Step 4: Add a Security Group Rule

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

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

NOTE

You can configure security group rules before 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.

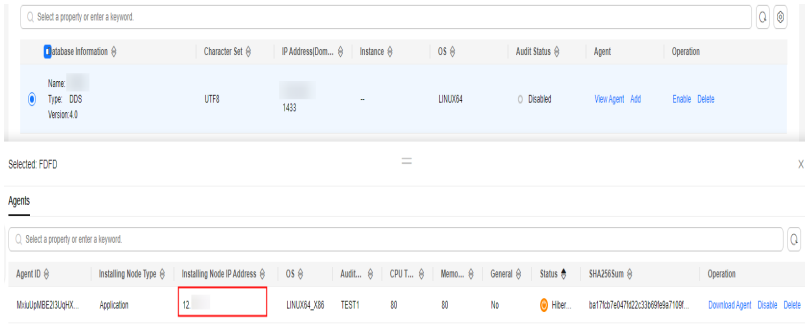
Step 4 In the navigation tree on the left, choose **Databases**.

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 3-40 Installing Node IP Address

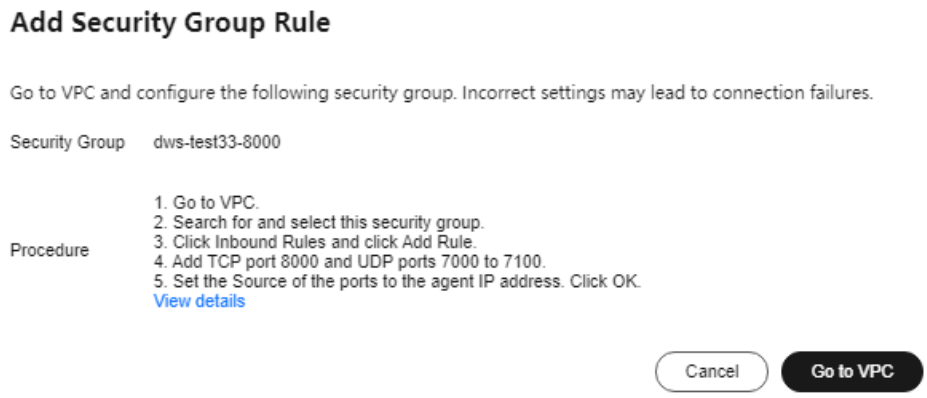


Step 7 Click **Add Security Group Rule**.

Step 8 In the displayed dialog box, record the security group name (for example, **default**) of the database audit instance, as shown in **Figure 3-41**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-41 Adding a security group rule



Step 9 Click **Go to VPC**.

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

Figure 3-42 Security group

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

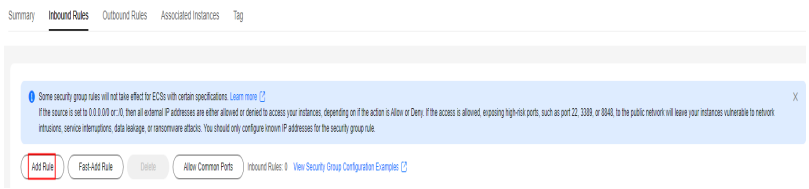
Check whether TCP (port number **8000**) and UDP protocols (port number from **7000** to **7100**) are configured in the inbound rules of the security group for the IP address of the installing node.

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

Step 12 Add an inbound rule for the installing node.

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

   Figure 3-43 Adding rules

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

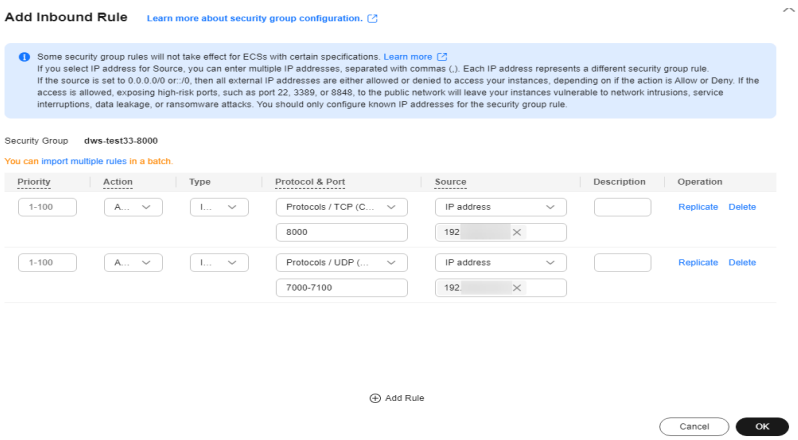
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 3-44 Add Inbound Rule dialog box



3. Click **OK**.

----End

3.2.6 Step 5: Enable Database Audit

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

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**.

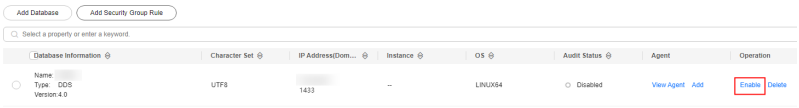
Step 6 Select a database audit instance from the **Instance** drop-down list.

Step 7 In the database list, click **Enable** in the **Operation** column of the database you want to audit.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

Figure 3-45 Enabling database audit



----End

Verifying Audit Results

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

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

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

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

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

Step 6 Click the **Statements** tab.

Step 7 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 3-46 Viewing SQL statements

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

----End

3.3 Managing Database Audit Instances

3.3.1 Viewing Database Instance Details

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 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 the instance whose information you want to view. The **Overview** page is displayed.

----End

Viewing the Instance Overview

Click the **Overview** tab to view instance information. For details about the parameters, see **Table 3-11**.

Table 3-11 Parameters of the instance overview

Category	Parameter	Description
Instance information	ID	Instance ID, which is automatically generated
	Status	Status of the instance.
Basic Info	Name	Name of an instance. You can click  next to **Name** to change it.
	ID	Instance ID, which is automatically generated
	Remarks	Remarks about an instance. You can click  next to **Remarks** to modify it.
	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. Impact scope of DBSS instance versions: • Supported database types • Supported database versions
	Billing Mode	The billing mode is yearly/monthly.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Category	Parameter	Description
	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: • Auto-renewal • Enter grace period
	Edition	Edition of an instance
	AZ	Availability Zone (AZ) where an instance resides
	Enterprise Project	Enterprise project name of the instance
	Created	Time when an instance is created
	Expiration	Time when an instance expires
	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 Click **Manage Database**, and the **Databases** page is displayed. For details about how to add a database, see **Step 1: Add a Database**.

Viewing System Monitoring Information of an Instance

Step 1 Click the **System Monitoring** tab. The **System Monitoring** page is displayed.

Step 2 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-47 Viewing the system monitoring

----End

Viewing the Alarm Monitoring Information of an Instance

Step 1 Choose **Monitoring**. The alarm monitoring page is displayed.

Step 2 View alarm information. For details about related parameters, see **Table 3-12**.

Figure 3-48 Viewing alarms

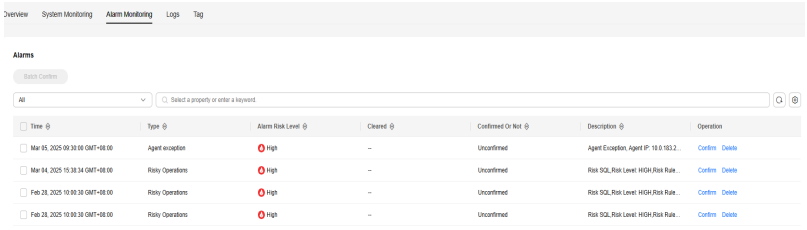


Table 3-12 Parameters of alarms

Parameter	Description
Time	Time when an alarm occurred.
Type	Alarm type. The options are as follows: • Audit traffic exceeds threshold • CPU exceptions • Memory exceptions • Disk exceptions • Insufficient audit log storage • Log backup to OBS failed • Agent exceptions • Risky operations

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description
Alarm Risk Severity	Risk severity of an alarm. The options are as follows: • **High** • **Moderate** • **Low**
Cleared	Time when an alarm is cleared
Confirmed Or Not	Confirmation status of an alarm.
Description	Description of an alarm
Operation	Operations supported by alarms, including: • Confirm • Deleting • 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

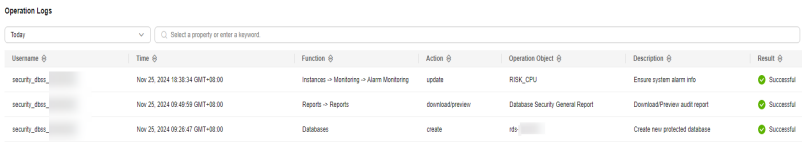
Viewing Operation Logs of an Instance

Step 1 Click the **Logs** tab. The log list page is displayed.

Step 2 View operation logs. For details about related parameters, see **Table 3-13**.

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 3-49 Viewing Operation Logs



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 3-13 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
Objects	Object of the operation
Description	Description of the operation
Result	Result of the operation

----End

3.3.2 Starting an Instance

You can manually enable an instance.

Prerequisites

The **Status** of the target audit instance is **Disabled**.

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 **More** > **Enable** in the **Operation** column of the target instance.

Step 5 In the displayed dialog box, confirm the information and click **Yes**. After the instance is enabled, check whether **Status** of the target instance is **Running**. If yes, the instance is running properly.

----End

3.3.3 Disabling an Instance

You can manually disable an instance.

Prerequisites

The **Status** of the target audit instance is **Running**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 **More** > **Disable** in the **Operation** column of the target instance.

Step 5 In the displayed dialog box, confirm the information and click **Yes**. After the instance is disabled, check that **Status** of the target instance is **Disabled**, indicating that the instance has stopped running.

NOTE

- Audit will be disabled for the database.
- A stopped instance still incurs changes. You are advised to keep it running or delete it to save costs.

----End

3.3.4 Restarting an Instance

You can manually restart an instance.

Prerequisites

The **Status** of the target audit instance is **Running**.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 Click **More** > **Restart** in the **Operation** column of the target instance.

Step 5 In the displayed dialog box, confirm the restart information. If the information is correct, click **Yes**. After the instance is restarted, check whether **Status** of the target instance is **Running**. If yes, the instance is restarted successfully.

NOTE

It takes 1 to 3 minutes to restart an instance. During this period, database audit is stopped.

----End

3.3.5 Enabling or Modifying Auto Renewal

You can manually enable or modify auto-renewal for database audit instances.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Constraints and Limitations

- The **Pay-per-use** mode is not supported. The **Billing Mode** of the target audit instance must be **Yearly/Monthly**.
- Auto-renewal can be enabled only for instances that have not enabled auto-renewal.
- Auto-renewal can be modified only for instances that have enabled auto-renewal.

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 Renewal operations

- Auto-renewal is not enabled.
  a. Click **More** > **Enable Auto-Renewal** in the **Operation** column of the target DB instance.
  b. In the displayed dialog box, confirm the instance information and click **Yes**.
- Auto-renewal enabled.
  a. Click **More** > **Modify Auto-Renewal** in the **Operation** column of the target DB instance.
  b. On the displayed page, confirm the instance information and select a renewal mode.
     - Auto-renewal: You need to select the renewal duration and set the number of renewal cycles.
     - Manual renewal: Disable auto-renewal. You need to manually renew the subscription every month.
  c. Confirm the information and click **OK**.

----End

3.3.6 Unsubscribing from an Instance

You can manually unsubscribe from an instance.

Constraints and Limitations

The **Status** of the target audit instance is **Running** and the **Billing Mode** is **Yearly/Monthly**.

Procedure

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 **More** > **Unsubscribe** in the **Operation** column of the target instance.

Step 5 In the displayed dialog box, confirm the unsubscription information and click **Yes** to initiate the unsubscription process. After unsubscription, the target instance will not be displayed in the database audit instance list.

NOTE

After the instance is unsubscribed, the database information, audit configuration information, and audit data added to the target instance will be cleared and cannot be restored.

----End

3.3.7 Releasing an Instance

You can manually release an instance.

Constraints and Limitations

The **Status** of the target instance must be **Frozen** or **Billing Mode** must be **Expired**.

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 Choose **More** > **Release** in the **Operation** column of the target instance.

Step 5 In the displayed dialog box, confirm the release information. If the information is correct, click **Yes** to initiate the release process. After the release is complete, the target instance is not displayed in the database audit instance list.

NOTE

After the instance is released, the database information, audit configuration information, and audit data added to the target instance will be cleared and cannot be restored.

----End

3.3.8 Deleting an Instance

You can delete idle instances.

Deleted audit instances cannot be restored. After an audit instance is deleted, the database audit configuration and audit data added to the instance are also deleted.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 Choose **More** > **Delete** in the **Operation** column of the target instance.

Step 5 In the displayed dialog box, confirm the instance information, enter **DELETE**, and click **OK**.

NOTE

Before deleting an instance, ensure that the instance is idle. After the instance is deleted, the database information, audit configuration information, and audit data added to the instance will be cleared and cannot be restored.

----End

3.3.9 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

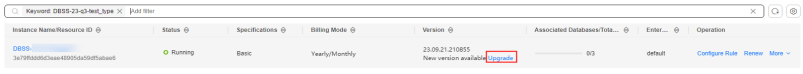
Step 1 Log in to the management console.

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 3-50 Upgrading the instance version



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

----End

3.3.10 Managing Instance Tags

You can add tags to database audit instances for easy management.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Prerequisites

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

Adding Tags to an 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 Click the name of an instance. On the displayed page, click the **Tag** tab.

Step 5 Click **Add Tag** in the upper left corner. In the dialog box that is displayed, enter the tag key and tag value.

NOTE

Up to 10 tags can be added to each DB instance.

Step 6 Click **OK**.

In the **Operation** column of the target tag, click **Edit** or **Delete** to manage the tag.

----End

3.3.11 Handling Instance Alarm Information

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.

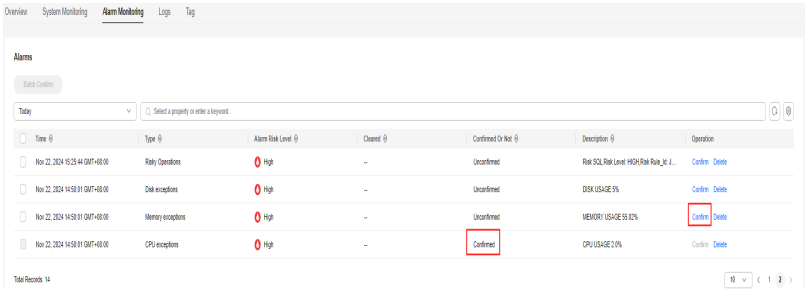
Step 3 In the navigation tree on the left, choose **Instances**.

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

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

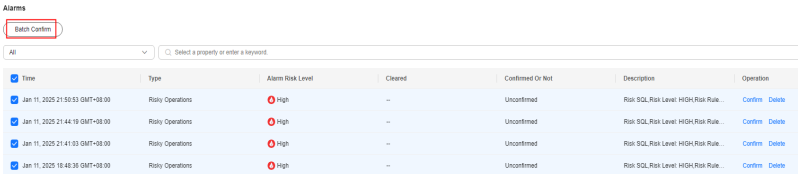
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-51 Confirming an alarm



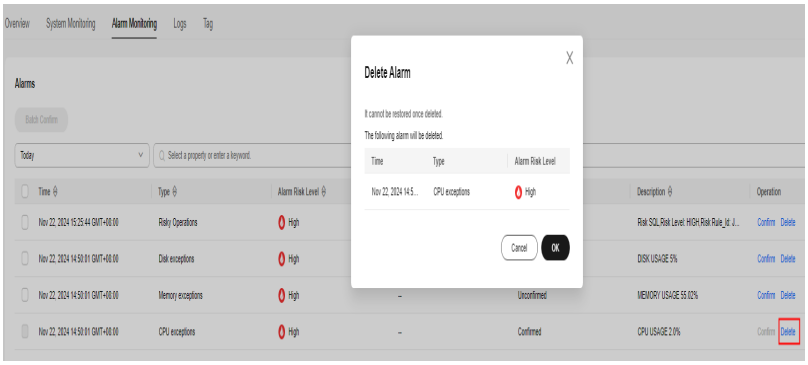
You can select multiple alarms to be confirmed and click **Batch Confirm** to batch confirm alarms.

Figure 3-52 Confirming alarms in batches



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

Figure 3-53 Deleting an alarm



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

----End

3.4 Configuring Audit Rules

3.4.1 Configuring an Audit Scope Rule

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.
- 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**.

Adding an Audit Scope Rule

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

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

Step 3 In the navigation tree on the left, choose **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, as shown in **Figure 3-54**. For details about related parameters, see **Table 3-14**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-54 Add Audit Scope dialog box

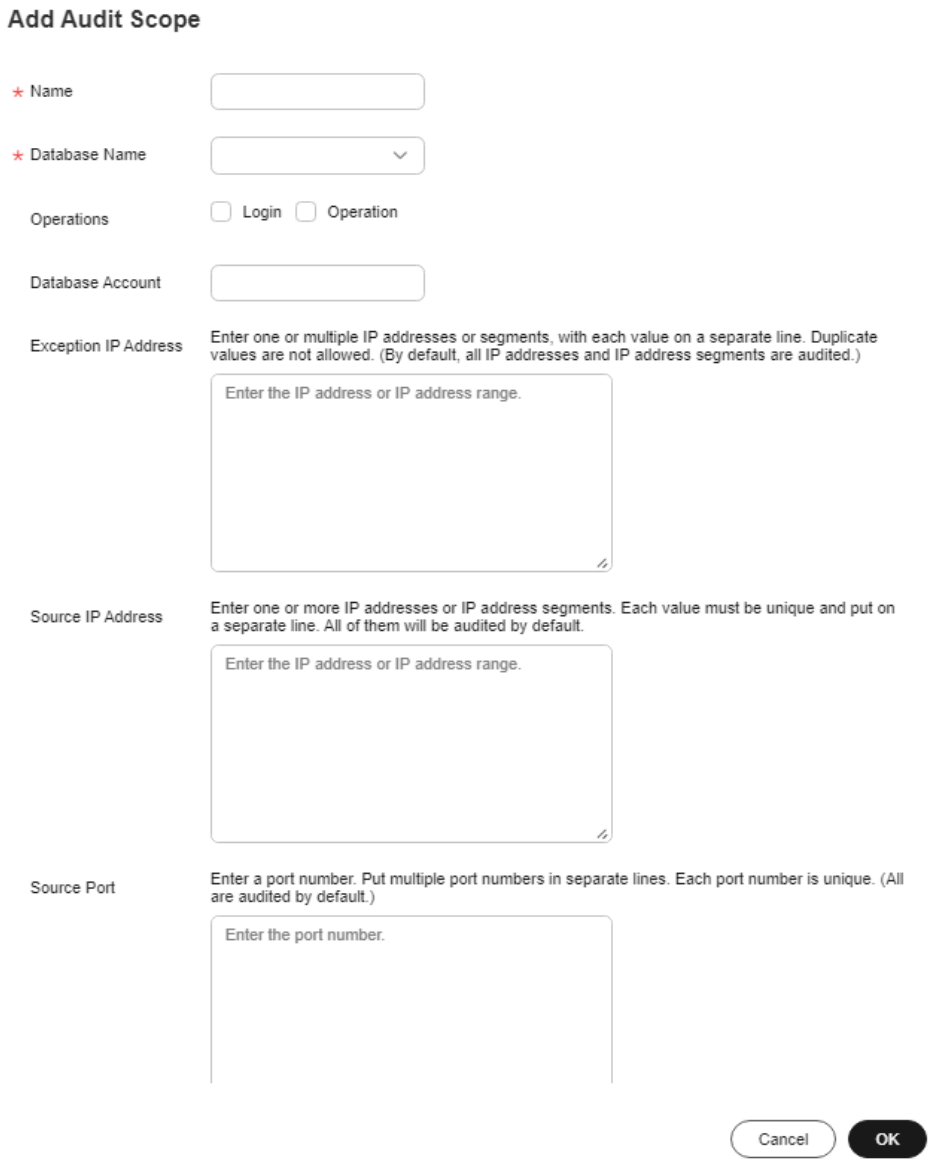


Table 3-14 Parameters

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

Step 7 Click **OK**.

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

----End

Managing Audit 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 on the left, 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 3-15**.

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-55 Viewing the audit scope

Table 3-15 Parameters

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

NOTE

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

- Enable

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

- Edit (supported in customized audit scopes only)

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

- Disable

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

- Delete (supported in customized audit scopes only)

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

----End

3.4.2 Configuring SQL Injection Rules

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3.4.2.1 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.

Constraints and Limitations

- 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.

Adding 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 on the left, choose **Audit Rules**.

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

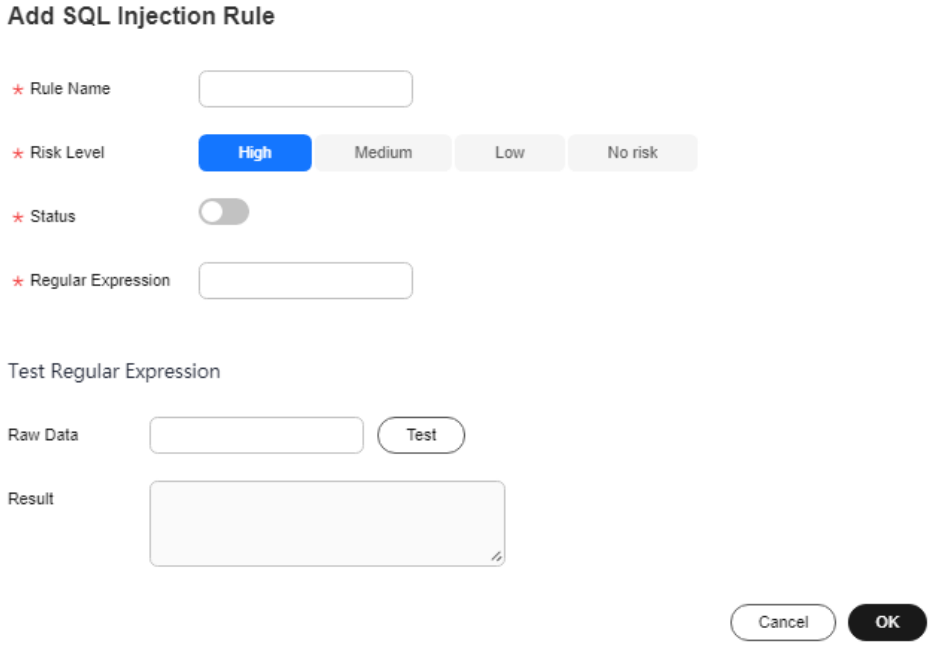
Step 5 Click the **SQL Injection** tab.

NOTE

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

Step 6 Click **Add SQL Injection Rule** and configure parameters.

Figure 3-56 Adding an SQL injection rule



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 3-16 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: • **High** • **Medium** • **Low** • **No risk**	**Medium**
Status	Enables or disables an SQL injection rule. •  : enabled •  : disabled	
Regular Expression	Regular expression that checks for content in certain pattern.	^\d{6}$
Raw Data	Content that matches the regular expression. Enter content and click **Test** to verify that the regular expression works properly.	628307
Result	Test result. It can be: • Hit • Miss **NOTE** – If the test result is **Hit**, the regular expression is correct. – If the test result is **Miss**, the regular expression is incorrect.	Hit

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

----End

Viewing 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 3-17**.

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 3-57 Viewing information about the SQL injection detection

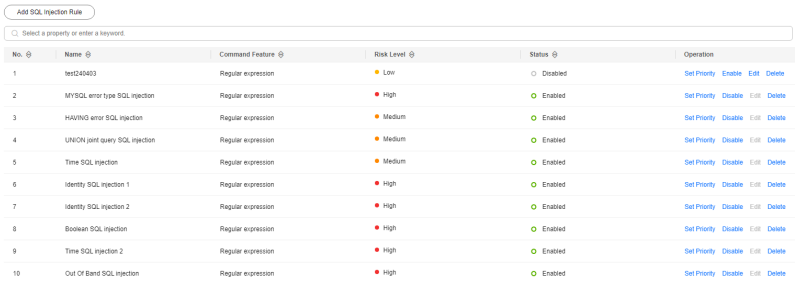


Table 3-17 Parameters

Parameter	Description
Name	Name of the SQL injection detection
Command Feature	Command features of the SQL injection detection
Risk Severity	Risk level of the SQL injection detection. The options are as follows: • **High** • **Medium** • **Low** • **No risks**
Status	Status of the SQL injection detection. The options are as follows: • Enabled • Disabled
Operation	Operations on an SQL injection rule. The options are as follows: • **Set Priority** • **Disable** • **Edit** • **Delete**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

----End

3.4.2.2 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.

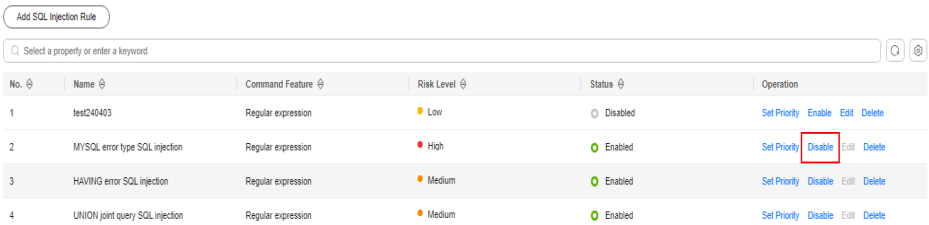
Step 3 In the navigation tree, choose **Rules**.

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 3-58 Disabling an SQL injection rule



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

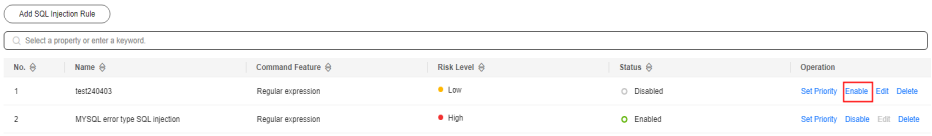
Step 3 In the navigation tree, choose **Rules**.

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 3-59 Enabling an SQL injection rule



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

----End

Setting the Priority of SQL Injection Rules

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

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

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

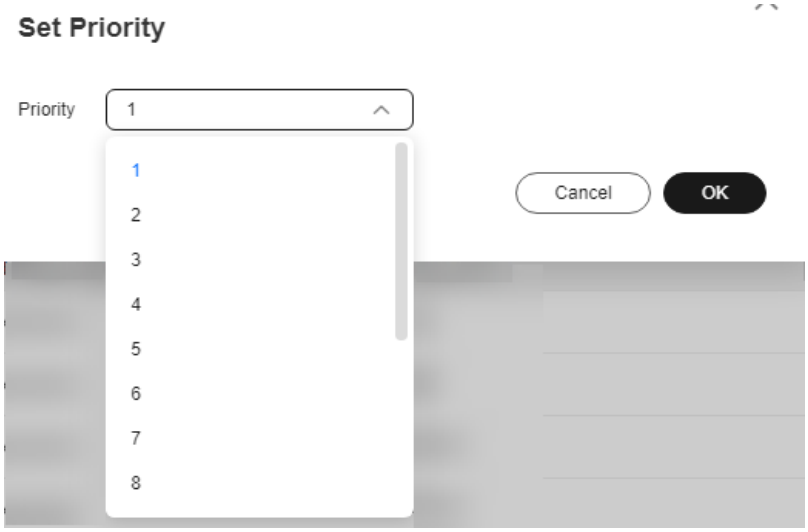
Step 4 In the **Select Instance** drop-down list, select the instance for which you want to set the priority for the SQL injection rule.

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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-60 Configuring the priority



----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 3-18**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-61 Editing an SQL injection rule

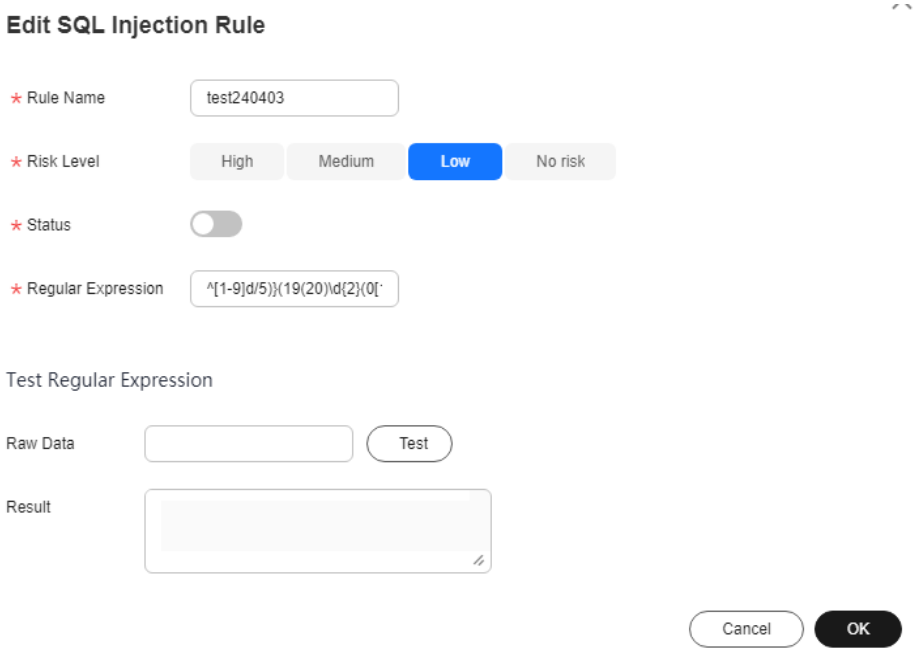


Table 3-18 SQL injection rule parameters

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

Step 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.

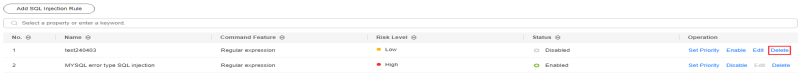
Step 5 Click the **SQL Injection** tab.

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 3-62 Deleting SQL injection



----End

3.4.3 Configuring Risky Operation Rules

Database audit has four built-in detection rules, including database reduction detection, slow SQL statements detection, batch data tampering detection, and

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

Constraints and Limitations

- Before enabling the risky operation, ensure that its status is **Disabled**.
- Before disabling the risky operation, ensure that its status is **Enabled**.
- If the risky operation is a system rule, setting priorities, editing, or deleting operations are not supported.

Adding a Risky Operation 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 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 3-19**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-63 Configuring basic information and IP addresses or IP address segments

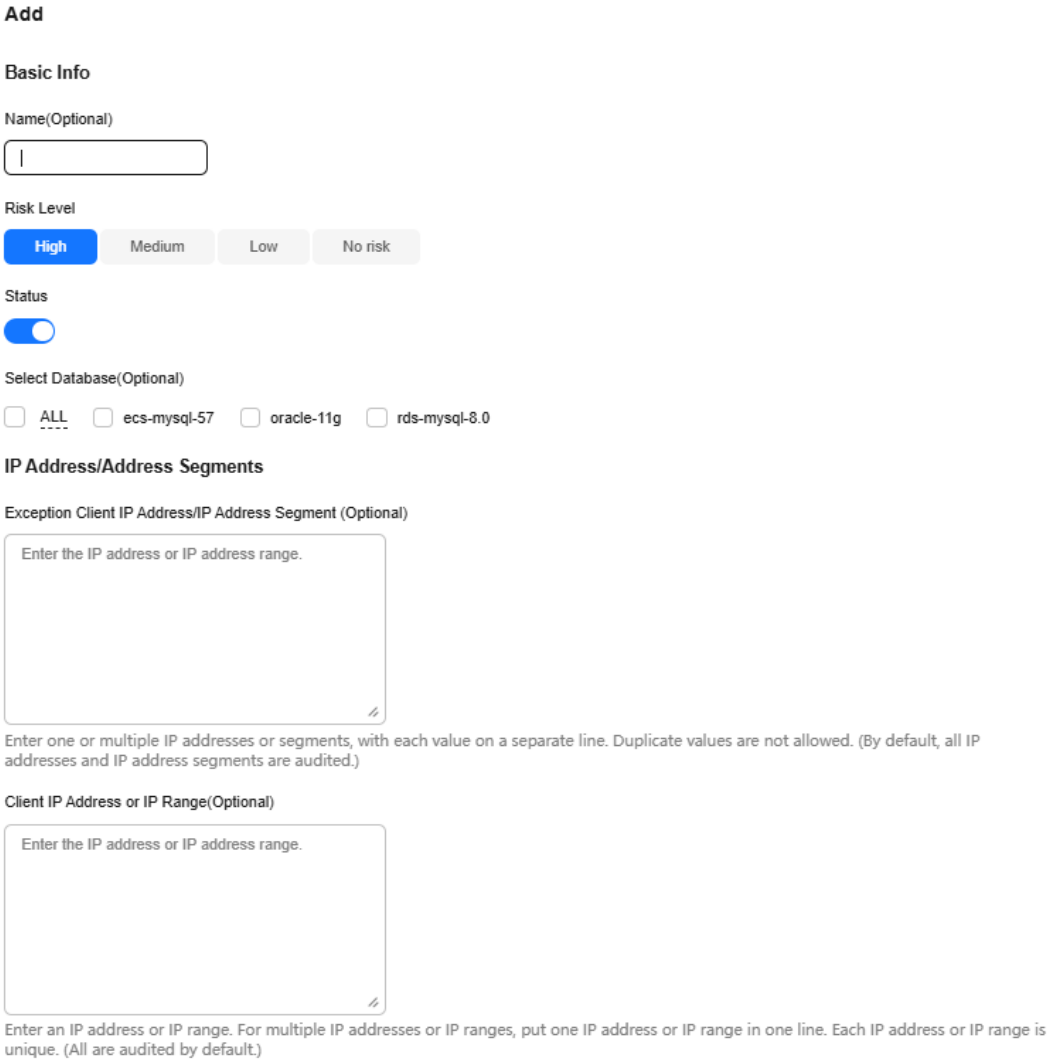


Table 3-19 Parameters

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description	Example Value
Status	Status of a risky operation •  : enabled •  : disabled	
Select Database	Database that the risky operation will be applied to You can select **ALL** or a specific database.	-
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. 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 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 3-20**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-64 Setting the operation type, operation object, and execution result

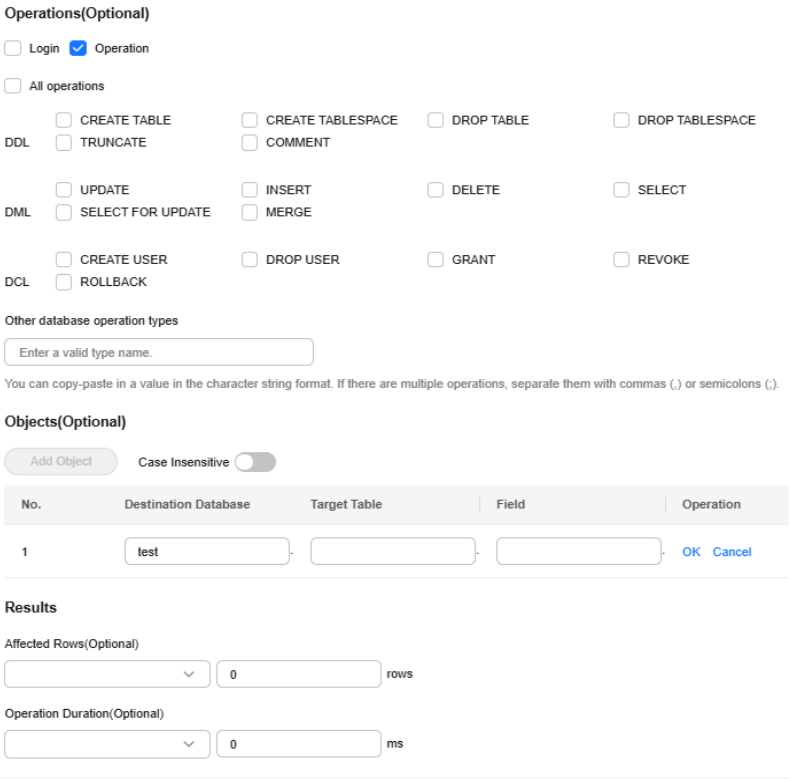


Table 3-20 Parameters for adding a risk rule

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

Step 9 Click **Save**.

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Viewing Risk Operation 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 risky operations.

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

Step 6 View the risky operation information. For details about related parameters, see Table 3-21.

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

Figure 3-65 Viewing the risky operation

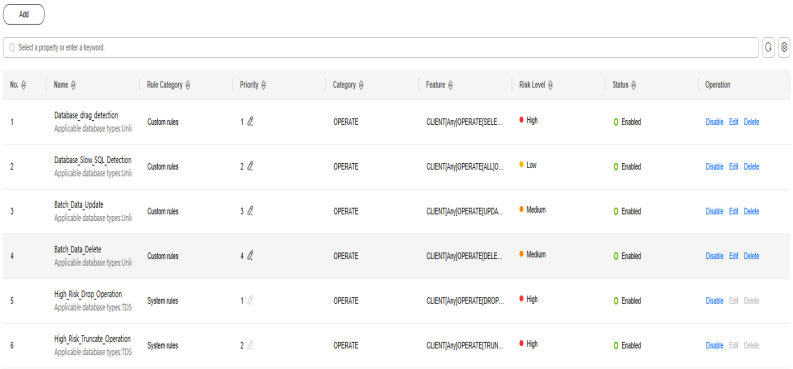


Table 3-21 Parameters

Parameter	Description
Name	Name of the risky operation
Rule Category	Risky operation type. The options are as follows: • Custom rules • System rules
Priority	Priority of a risky operation.
Category	Category of the risky operation
Feature	Feature of the risky operation
Risk Level	Risk level of a risky operation. The options are as follows: • **High** • **Medium** • **Low** • **No risks**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description
Status	Status of the risky operation. The options are as follows: • **Enabled** • **Disabled**

NOTE

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

- Enable

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

- Edit

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

- Disable

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

- Deleting

  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

Setting the Risk Rule Priority

Step 1 Log in to the management console.

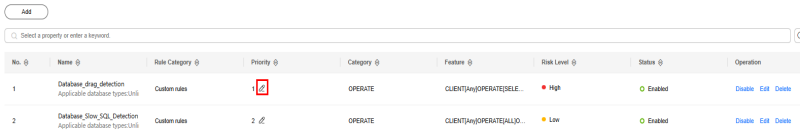
Step 2 Select a region, click , and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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.

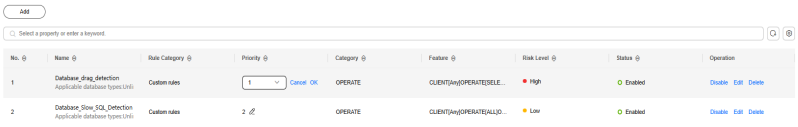
Figure 3-66 Setting the priority



Step 6 Click **OK**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-67 Setting the priority



----End

3.4.4 Configuring Privacy Data Protection Rules

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

Prerequisites

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

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 on the left, choose **Audit 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 3-22**.

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-68 Masking rule information

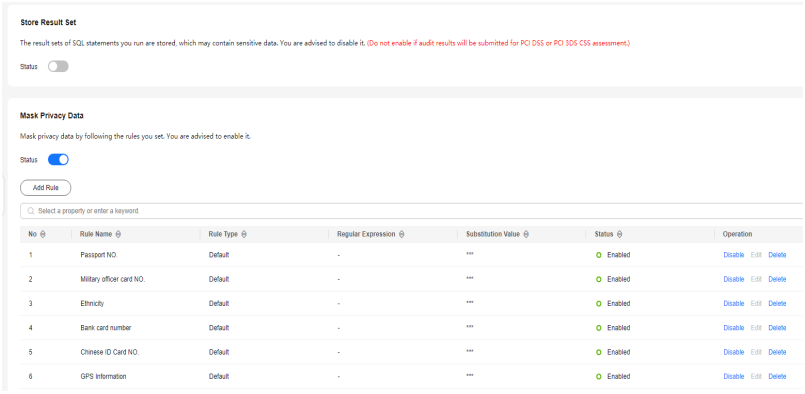


Table 3-22 Masking rule parameters

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

NOTE

You can perform the following operations on a rule:

- Disable

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

- Edit

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

- Deleting

  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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Adding a Custom Privacy Data 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 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.

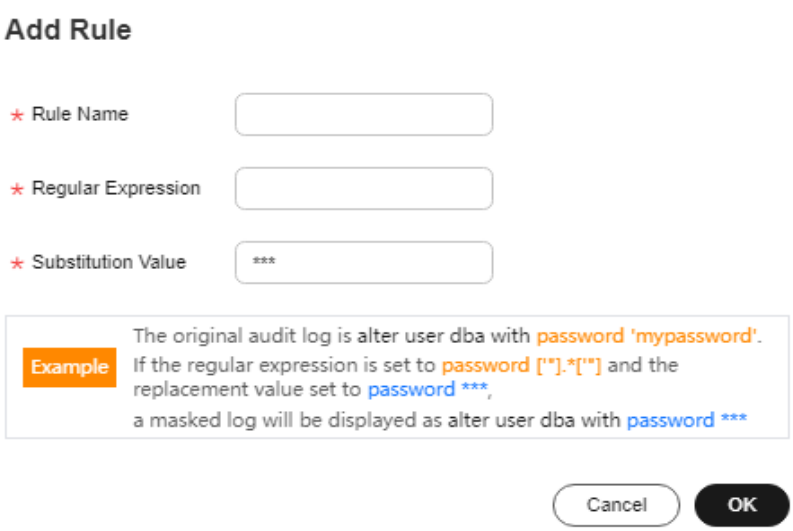
  Note: The result set storage supports only the database audit in agent mode.

- **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 3-69**. For details about related parameters, see **Table 3-23**.

Figure 3-69 Adding a user-defined rule



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 3-23 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.

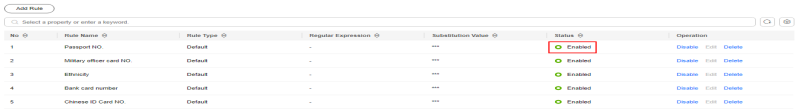
----End

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 3-70**.

Figure 3-70 Enabled rule



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

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

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

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

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

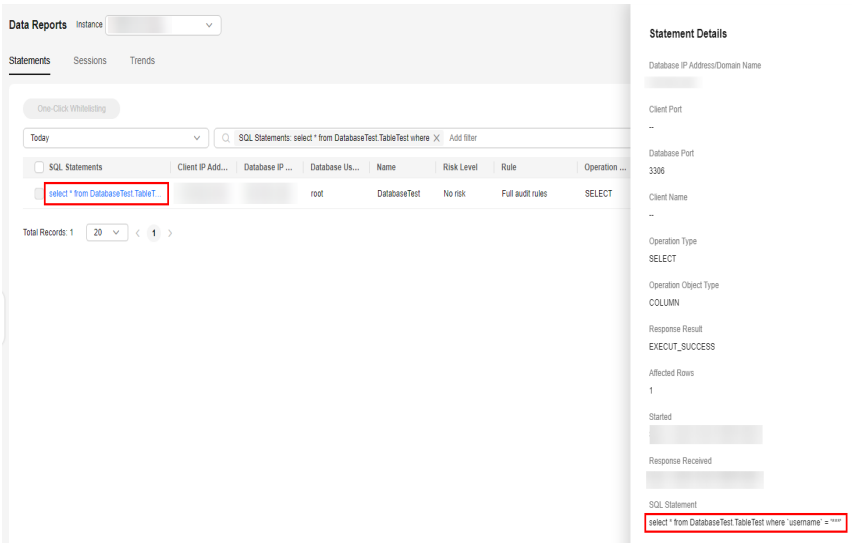
Step 6 In the **Instance** drop-down list, select the instance whose SQL statement information you want to view. Click the **Statements** tab.

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

Step 8 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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-71 Masking privacy data



----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.

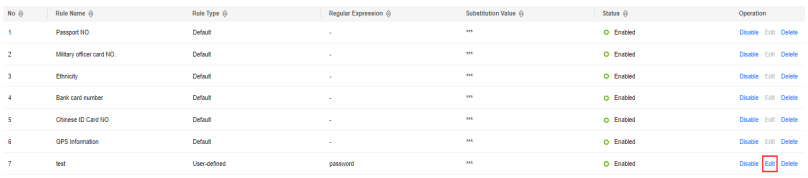
  Figure 3-72 Disabling a custom masking rule

- Edit

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

  Figure 3-73 Editing a custom masking rule

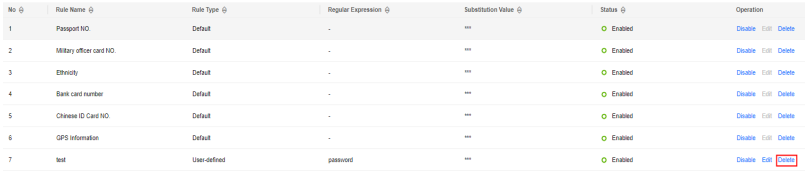
  

- Delete

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-74 Deleting a custom masking rule



3.4.5 Configuring SQL Whitelist Rules

3.4.5.1 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.

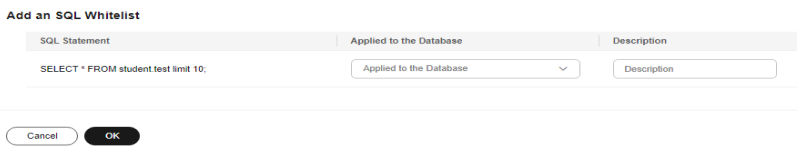
Step 4 In the **Instance** drop-down list, select the instance whose session information you want to view.

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.

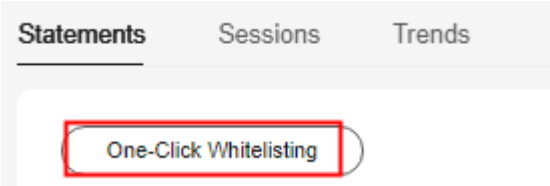
  Figure 3-75 Adding an SQL whitelist

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

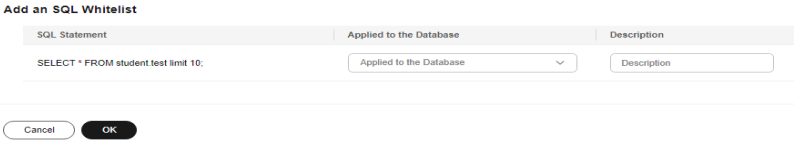
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-76 One-click whitelisting



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

Figure 3-77 Adding an SQL whitelist



c. Click **OK**.

----End

3.4.5.2 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- 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

3.5 Viewing Audit Data

3.5.1 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.

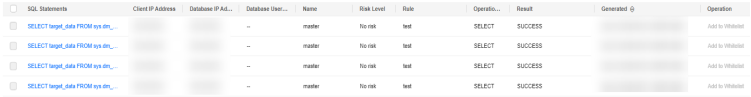
Step 3 In the navigation tree on the left, choose **Data Reports**. The **Data Reports** page is displayed.

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 3-78 Querying SQL statements



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

- Select the time range (**All** time, **Last 30 minutes**, **1 hour**, **Today**, **7 days**, or **30 days**), or customize the start time and end time. Click , the SQL statements in the time period are displayed in the list.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- 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.

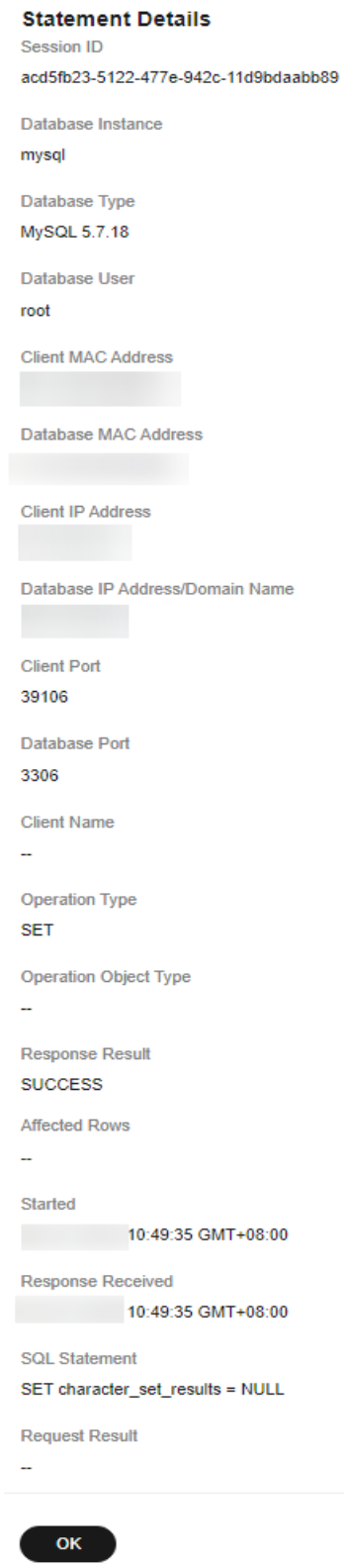
Step 8 View the SQL statement information in the **StatementDetails** dialog box. For details about related parameters, see **Table 3-24**.

NOTICE

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-79 Statement dialog box



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 3-24 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?**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- 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?**

3.5.2 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.

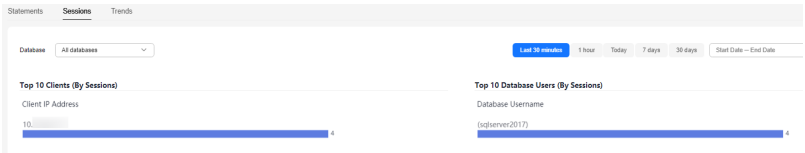
Step 4 In the **Instance** drop-down list, select the instance whose session information you want to view.

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 3-80 Viewing session distribution



----End

3.5.3 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).

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

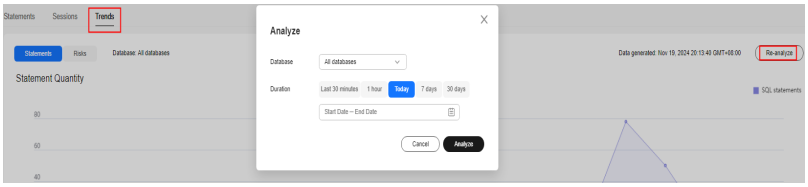
Step 4 Click the **Trends** tab. The trend analysis page is displayed.

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 3-81 Re-analyze



- 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 3-82 Statement quantity

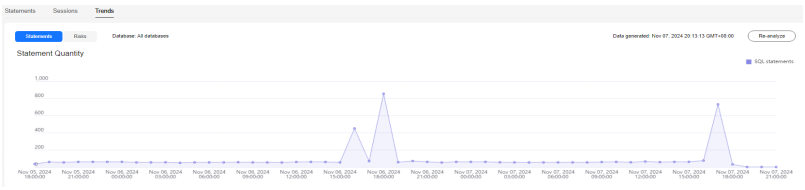
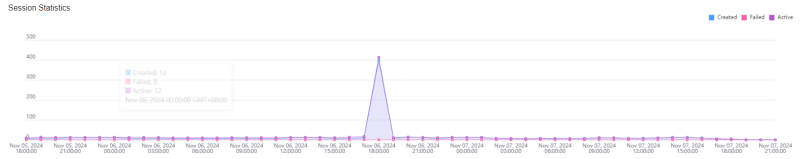


Figure 3-83 Session statistics



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-84 SQL distribution

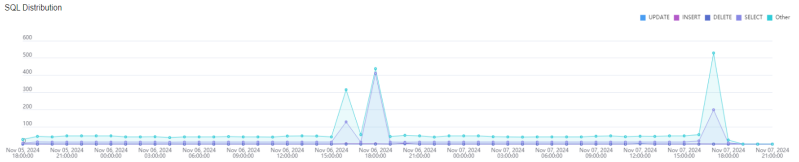


Figure 3-85 Risk distribution

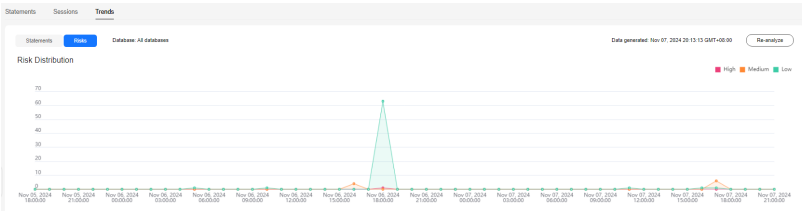


Figure 3-86 SQL injections

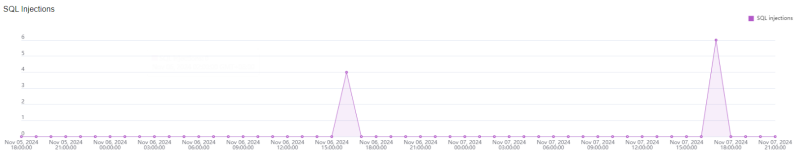
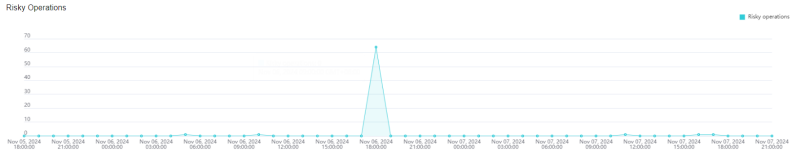


Figure 3-87 Risky operations



----End

3.6 Report Center

3.6.1 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 3-25** lists the report names. You can **generate reports** and **set report tasks** as needed.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 3-25 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**.

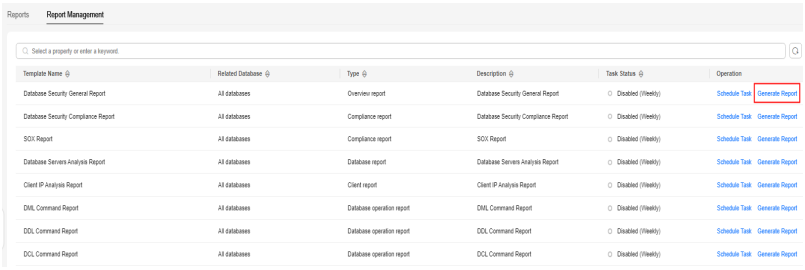
Step 4 In the **Instance** drop-down list, select the instance whose instance report you want to generate.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

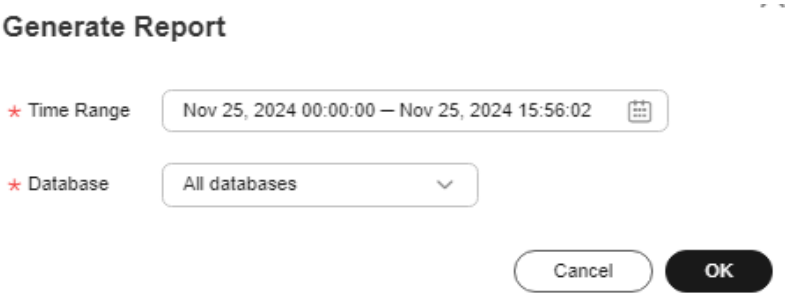
Step 6 In the **Operation** column of a report template, click **Generate Report**.

Figure 3-88 Report template list



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

Figure 3-89 Generate Report



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**.

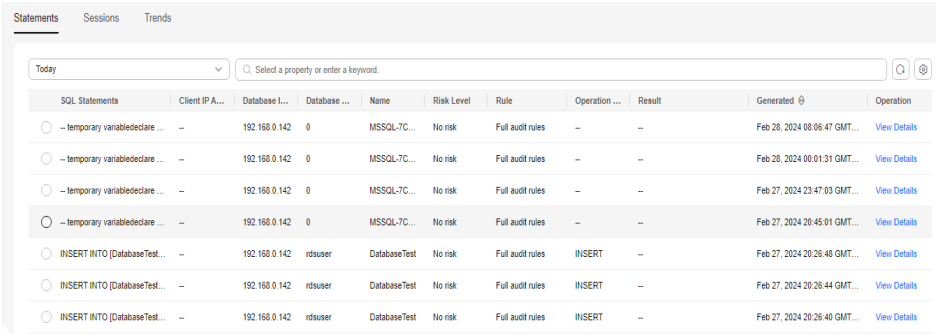
Step 4 In the **Instance** drop-down list, select the instance for which you want to set a report task.

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 3-90**.

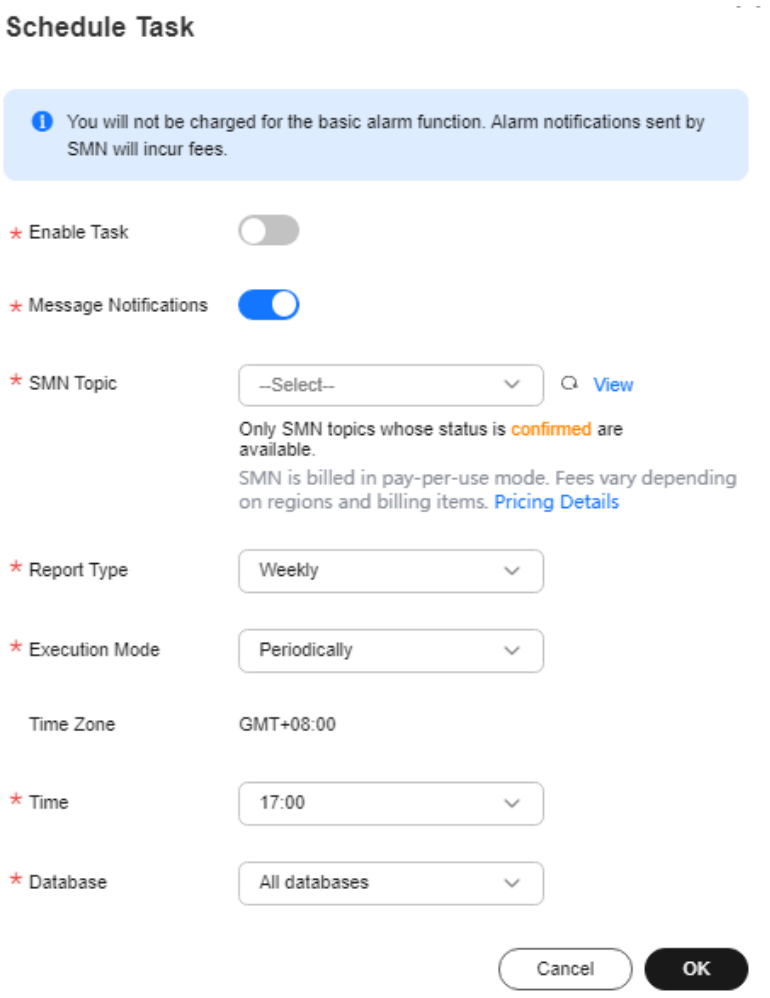
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-90 Setting a task



Step 7 In the displayed dialog box, set the parameters of the scheduled task, as shown in **Figure 3-91**. For details about related parameters, see **Table 3-26**.

Figure 3-91 Setting a scheduled task



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 3-26 Parameters for setting a task

Parameter	Description	Example Value
Enable Task	Status of a scheduled task. •  : enabled •  : disabled	
Message Notifications	Enables or disables notifications. Notifications are sent and billed by SMN in pay-per-use mode. Fees vary depending on regions and billing items. For details, see **SMN Pricing Details**. •  : enabled •  : disabled	
SMN Topic	• Select an existing topic from the drop-down list or click **View** to create a topic. For details, see **Creating a Topic**. • You can add multiple subscriptions to a topic and select multiple subscription endpoints (such as SMS messages and emails). For details, see **Adding a Subscription**. For details about topics and subscriptions, see *Simple Message Notification User Guide*.	-
Report Type	Type of a report. The options are as follows: • **Daily** • **Weekly** • **Monthly**	Weekly
Execution Mode	Execution mode of the report. The options are as follows: • **Once** • **Periodically**	Periodically
Time	Time when the report is executed	10:00
Database	Database for which you want to execute the report task	-

Step 8 Click **OK**.

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

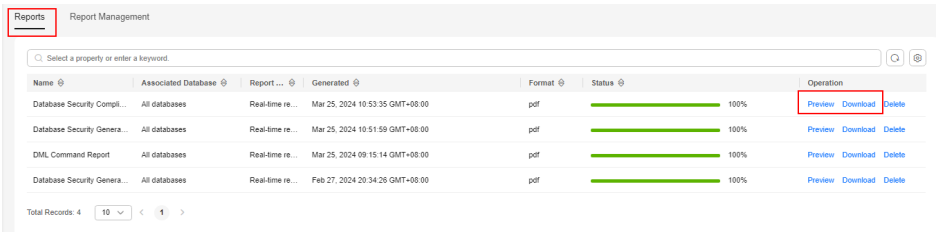
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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 3-92**..

Figure 3-92 Previewing or downloading an audit report



----End

Helpful Links

Why I Cannot Preview the Database Security Audit Report Online?

3.6.2 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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Viewing a Report

Step 1 Log in to the management console.

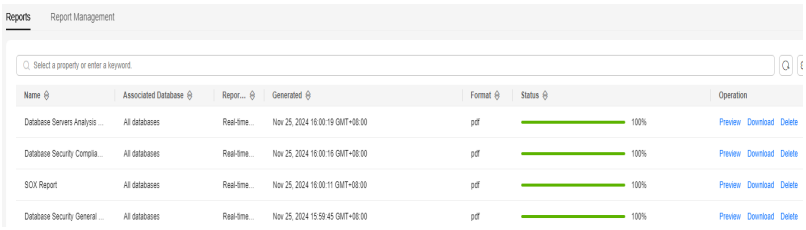
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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 3-93 Viewing a report



NOTE

- You can select an attribute from the search box above the list or enter a keyword to search for a specified report.
- A real-time report is automatically generated in PDF format.
- Locate the row that contains the report to be deleted, click **Delete** in the **Operation** column, and click **OK** in the displayed dialog box. When a report is deleted, you need to manually generate a report if you want to view the report result.

----End

Viewing a Report Template

Step 1 Log in to the management console.

Step 2 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**.

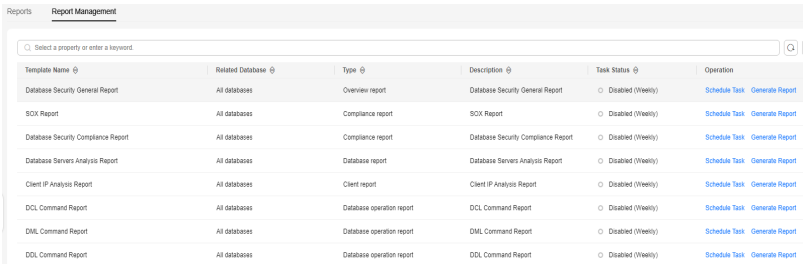
Step 4 In the **Instance** drop-down list, select the instance whose report template you want to view.

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

Step 6 View the report template.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-94 Viewing the template list



NOTE

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

----End

3.7 Audit System Management

3.7.1 Configuring Alarm Notifications

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

- Alarm notifications may be mistakenly blocked. If you have enabled notifications but not received any, check whether they have been blocked as spam.
- The system collects alarm statistics every 5 minutes and sends alarm notifications (if any).
- Database audit alarm notifications are sent by SMN and will incur fees. See **SMN Pricing Details**.

Prerequisites

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

Procedure

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

Step 2 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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 3-27**.

Figure 3-95 Configuring alarm notifications

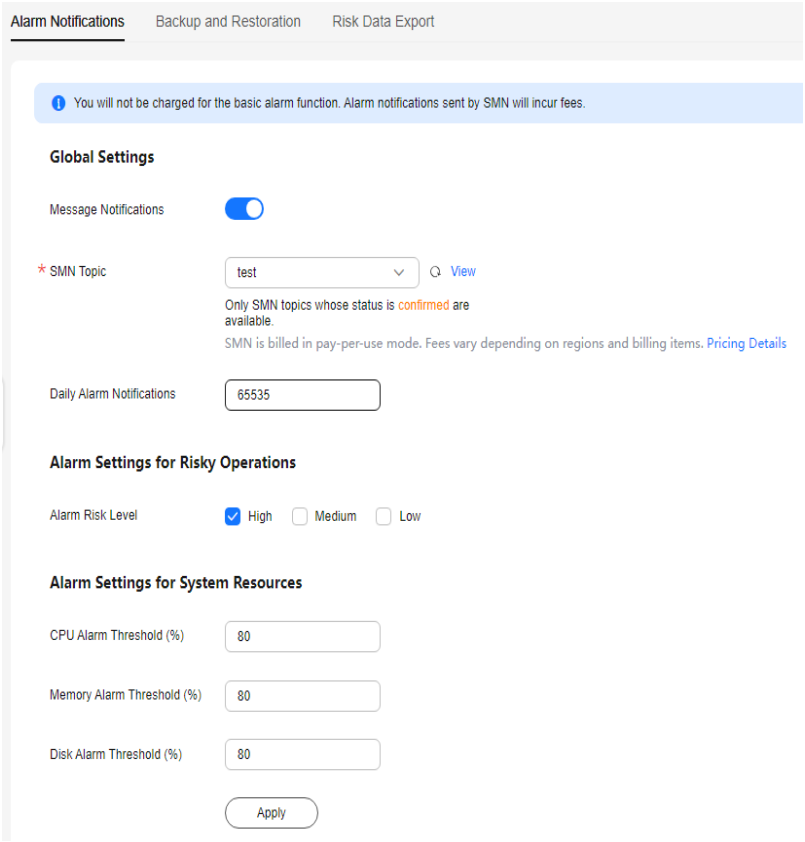


Table 3-27 Alarm notification parameters

Parameter	Description	Example Value
Message Notifications	Enables or disables notifications. Database audit alarm notifications are sent by SMN and will probably incur a small fee. See **SMN Pricing Details**. •  : disabled •  : enabled	

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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**. • You can add multiple subscriptions to a topic and select multiple subscription endpoints (such as SMS messages and emails). For details, see **Adding a Subscription**. **NOTE** Before selecting a topic, ensure that the subscription status of the topic is **Confirmed**. Otherwise, alarm notifications may not be received. For details about topics and subscriptions, see *Simple Message Notification User Guide*.	-
Daily Alarm Notifications	Total number of alarms allowed to be sent every day **NOTICE** • If the number of alarms exceeds this value on a day, no more notification will be sent on that day. • There is no fixed time point for sending alarm notifications. The system collects statistics every 5 minutes and sends alarm notifications (if any).	30
Alarm Risk Severity	Risk severity of the risk log. The options are as follows: • **High** • **Moderate** • **Low**	High
CPU Alarm Threshold (%)	CPU alarm threshold of an audit instance. When the threshold is exceeded, an alarm notification is generated.	80
Memory Alarm Threshold (%)	Memory alarm threshold of an audit instance. When the threshold is exceeded, an alarm notification is generated.	80
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

3.7.2 Managing Backup and Restoration

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

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 3-28**.

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 3-96 Viewing backup audit logs

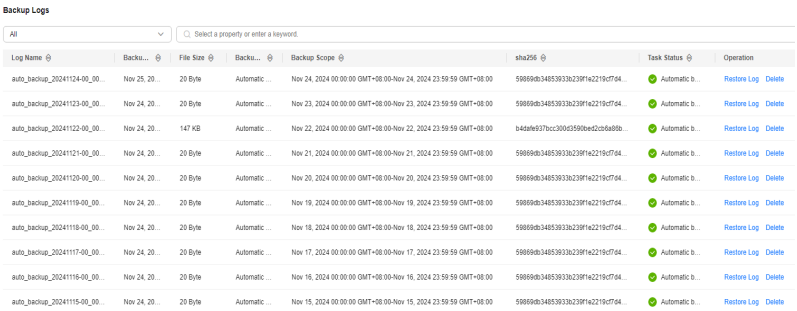


Table 3-28 Parameters of audit logs

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description
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

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**.

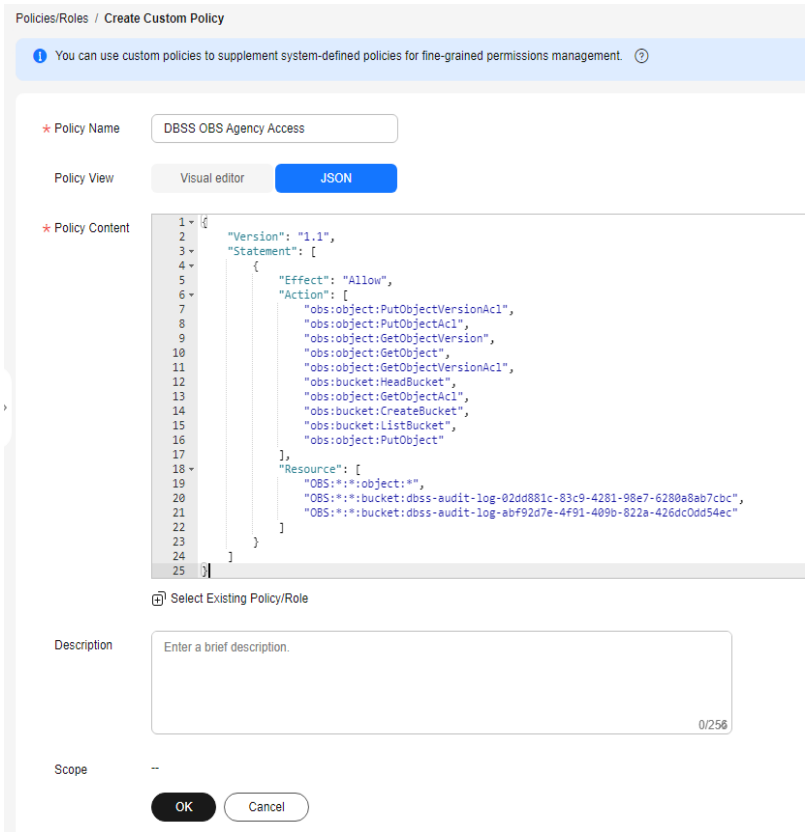
Step 4 Configure policy parameters. Set **Policy Name** to **DBSS OBS Agency Access**. Set **Policy View** to **JSON**. The policy content is as follows:

```
{
   "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 3-97**. Click **OK**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-97 Creating a custom policy

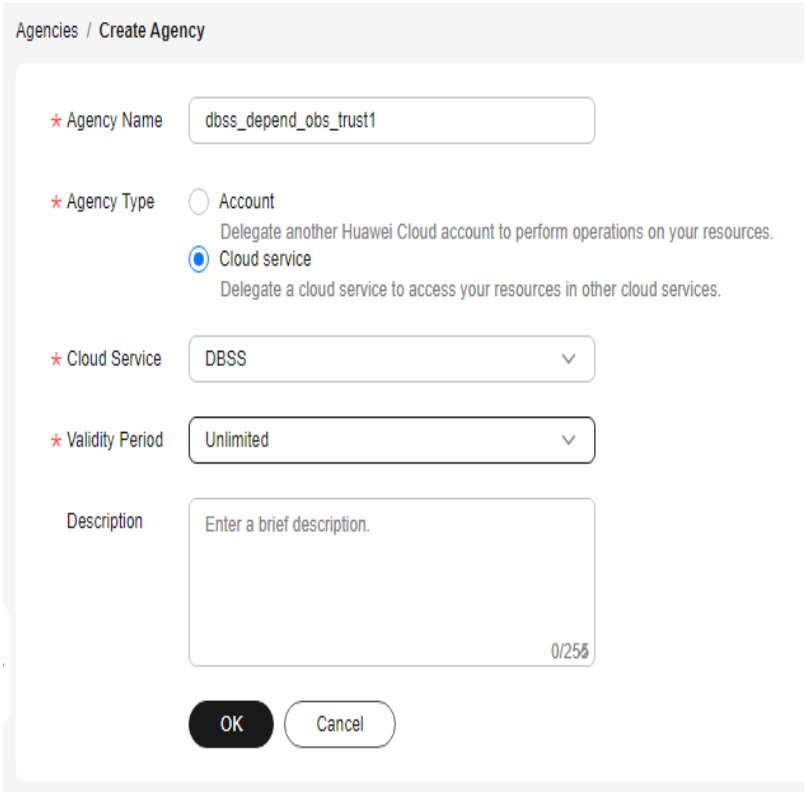


Step 5 In the navigation pane, choose **Agencies** and then click **Create Agency** in the upper right corner.

Step 6 Configure agency parameters. Set **Agency Name** to **dbss_depend_obs_trust**. Set **Agency Type** to **Cloud service**. Set **Cloud Service** to **DBSS**. See **Figure 3-98**.

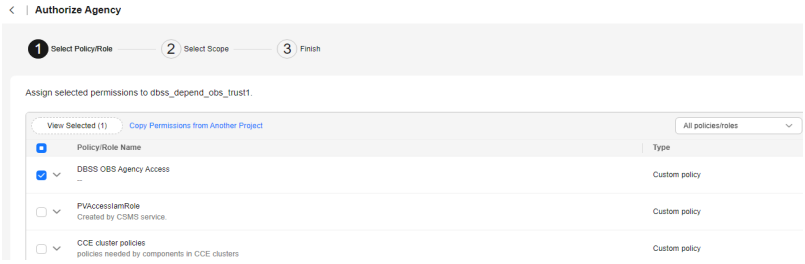
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-98 Creating an agency



Step 7 Click **Next**. Select the custom policy created in **Step 4**, and add the permission **DBSS OBS Agency Access** to the agency **dbss_depend_obs_trust**, as shown in **Figure 3-99**. Click **Next** in the lower right corner.

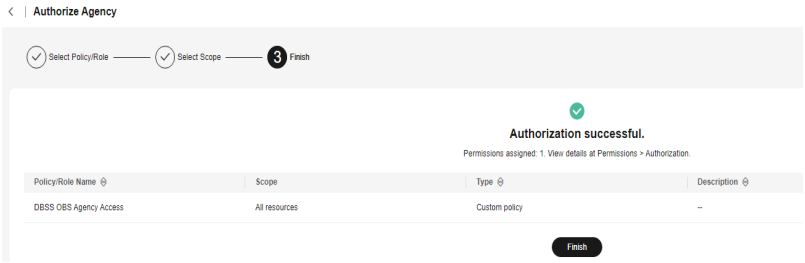
Figure 3-99 Selecting a policy



Step 8 Set **Scope** to **All resources** and click **OK**. If the message in **Figure 3-100** is displayed, the authorization is successful. Click **Finish**. The authorization will take effect in about 15 minutes.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-100 Authorization completed



----End

Automatically Backing Up Database Audit Logs

Step 1 Log in to the management console.

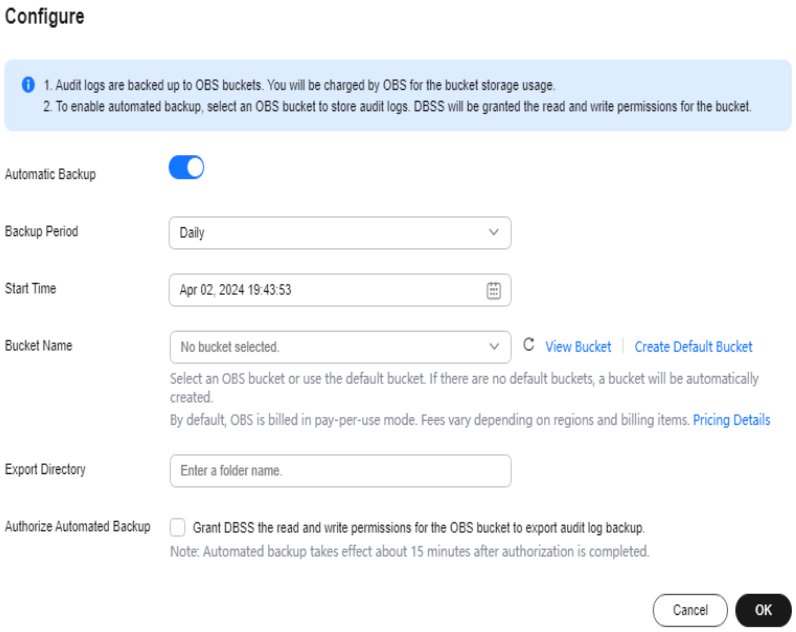
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 Click **Modify Automated Backup Settings**. In the displayed dialog box, set the auto backup parameters. **Table 3-29** describes the parameters.

Figure 3-101 Configure Automatic Backup dialog box



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 3-29 Parameters

Parameter	Description	Example Value
Automatic Backup	Status of automatic backup •  : enabled •  : disabled	
Backup Period	Automatic backup period. Its options are as follows: • **Daily** • **Hourly**	Daily
Started	Start time of the backup. Click  to configure.	2020/01/14 20:27:08
Bucket Name	Name of the OBS bucket used for backup. Its options are as follows: • Create Default Bucket • Select Bucket **NOTE** • If you click **Create Default Bucket**, you will be prompted to authorize OBS for exporting audit log backups. • Audit logs can be exported only to the bucket created by DBSS.	20f18-7a5a-4042
Export Directory	Directory for storing backup files in the OBS bucket.	test
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. **CAUTION** 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

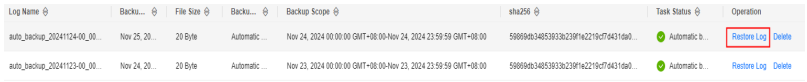
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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.

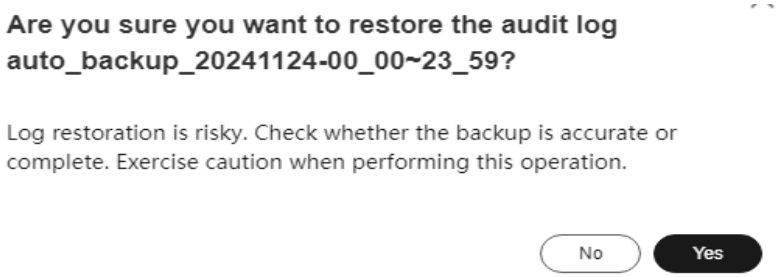
Step 5 In the **Operation** column of the backup log to be restored, click **Restore Log**.

Figure 3-102 Restoring logs



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

Figure 3-103 Confirming the restoration of audit logs



----End

Exporting Risk Data

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

NOTE

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

Step 1 Log in to the management console.

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

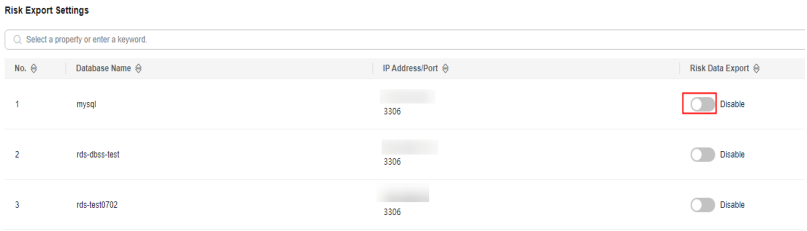
Step 3 In the navigation tree on the left, choose **Settings**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 3-104 Enabling risk export



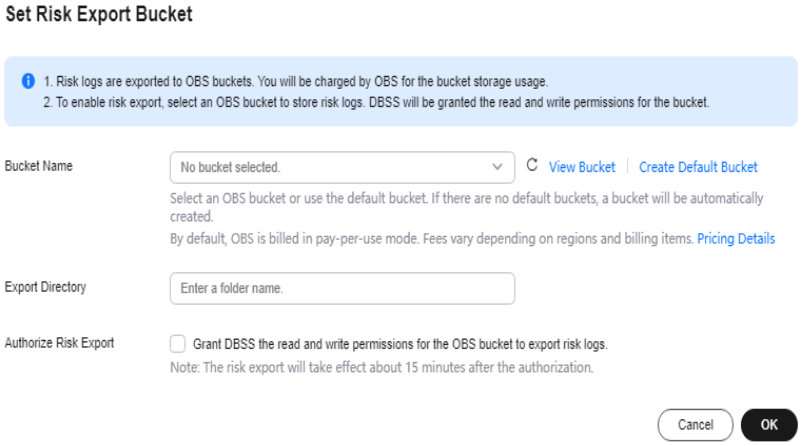
Step 6 An OBS bucket will be automatically created to store risk logs.

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

CAUTION

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

Figure 3-105 Automatically creating an OBS bucket



----End

3.7.3 Managing Database Assets and Agents

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3.7.3.1 Agent Management

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.

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 3-30**.

Table 3-30 Parameters of an agent

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description
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

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
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
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

3.7.3.2 Asset Management

After a database is added, you can view, close, and delete the database.

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 3-31**.

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

Table 3-31 Parameters

Parameter	Description
Database Information	Name, type, and version of a database
Character Set	Encoding character set of the database

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description
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: • Enabled • 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

3.8 Key Operations Recorded by CTS

3.8.1 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.

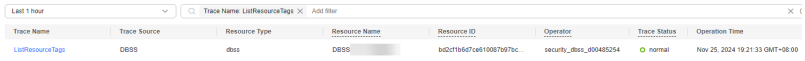
Step 2 In the navigation pane on the left, click ☰ and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.

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.

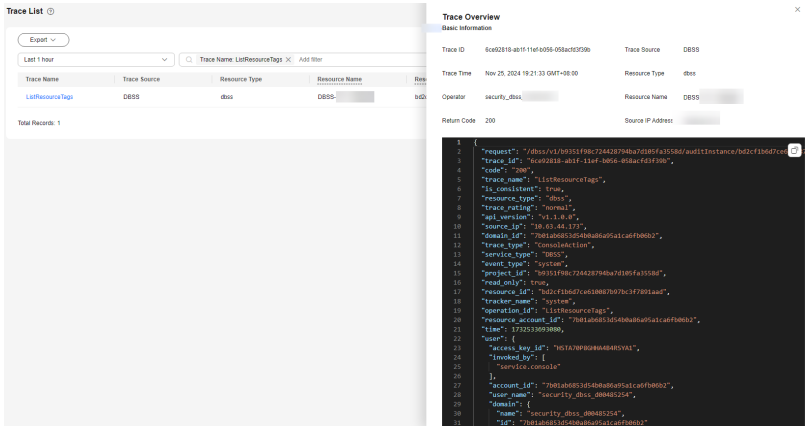
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 3-106 Trace list



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

Figure 3-107 Viewing traces



----End

3.8.2 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 3-32 lists DBSS operations recorded by CTS.

Table 3-32 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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

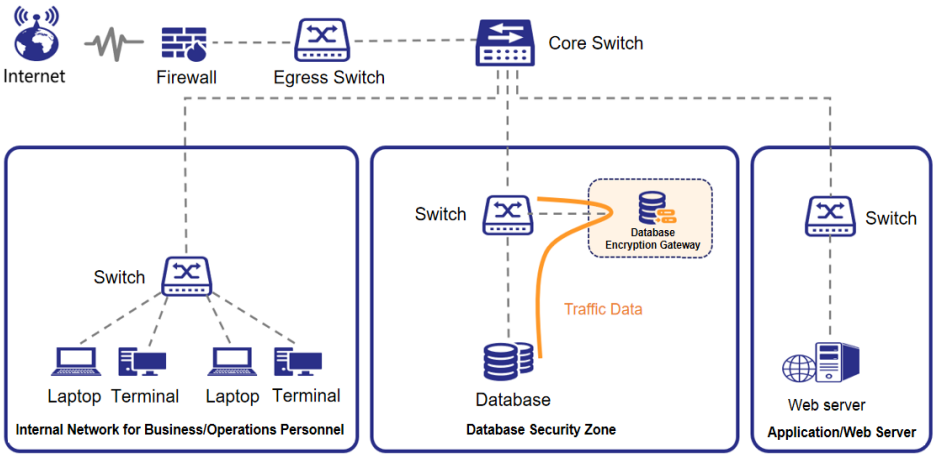
4 Database Encryption

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- 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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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**

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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. • 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 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 4-2 describes the default user names. Obtain the actual user names and passwords from technical support engineers.

Table 4-2 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. 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. For details, see **Security Administrator Operation Guide**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Default Role	Default Account	Description
Audit administrator	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. 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.

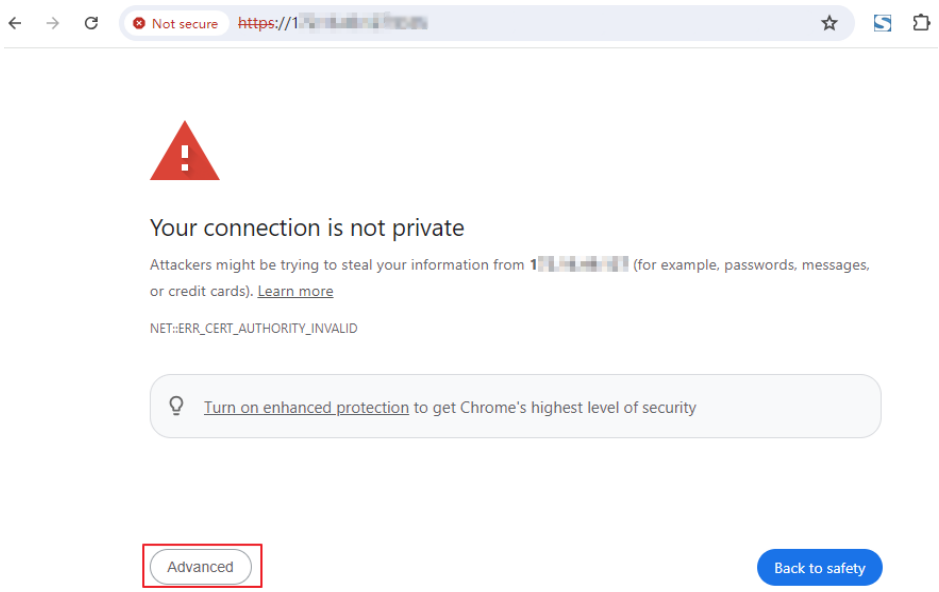
- Method 1: Log in to the service management console, go to the database encryption and access control page, and click in the **Operation** column of the target instance.
- Method 2: Obtain **EIP** from the database encryption and access control page displayed in method 1. Enter the address in the address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

  Address: **https://***<server-EIP>***:***<port-number>*, for example, **https://100.xx.xx.54:9595**.

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

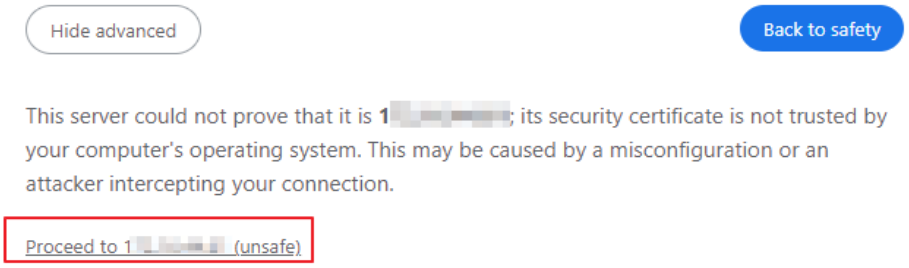
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-2 Security warning



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

Figure 4-3 Continue



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.

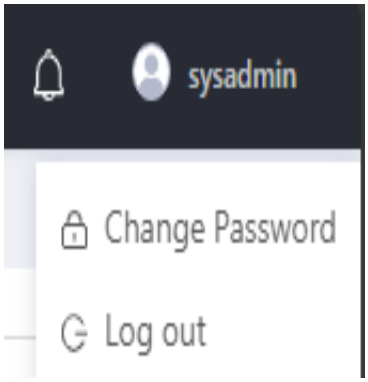
----End

Changing the Login Password

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-4 Changing a password



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

Step 3 In the dialog box, enter the old password and new password, and click **OK**. **Table 4-3** 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 4-3 Changing a password

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

----End

4.3 System Function Configuration and Application Scenario Examples

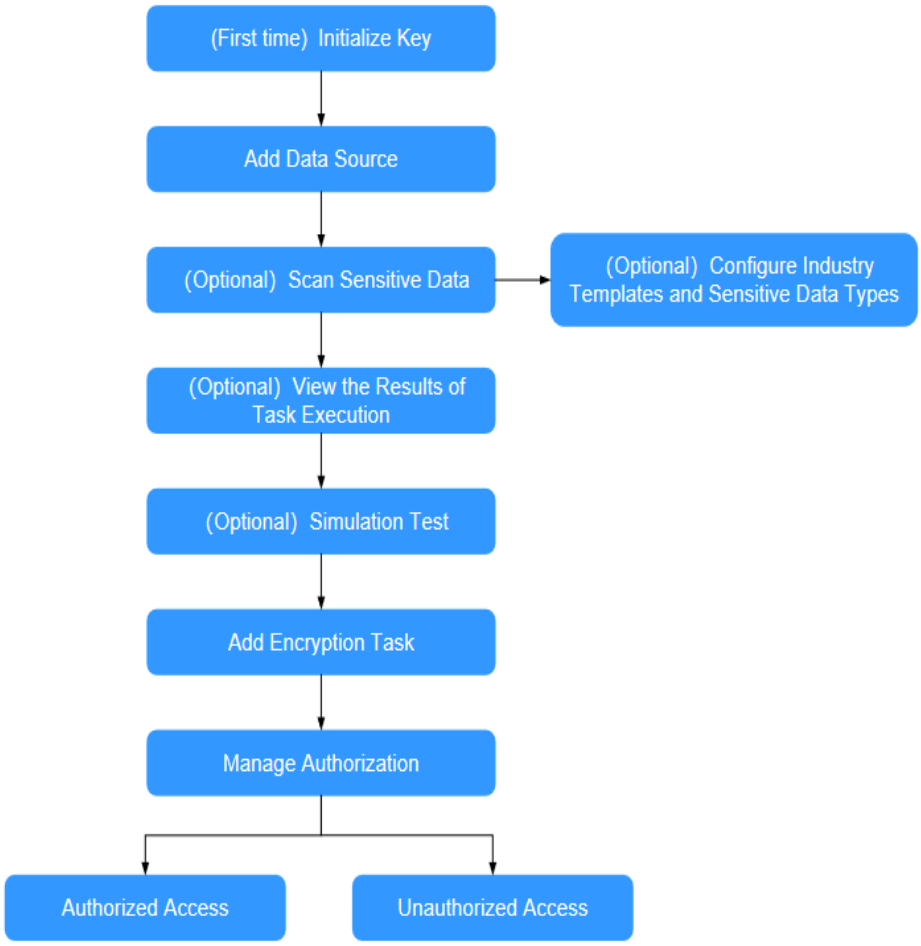
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.3.1 Scenario 1: Encryption Process and Typical Encryption Configuration

Encryption Process

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

Figure 4-5 Encryption process



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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 Encryption 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

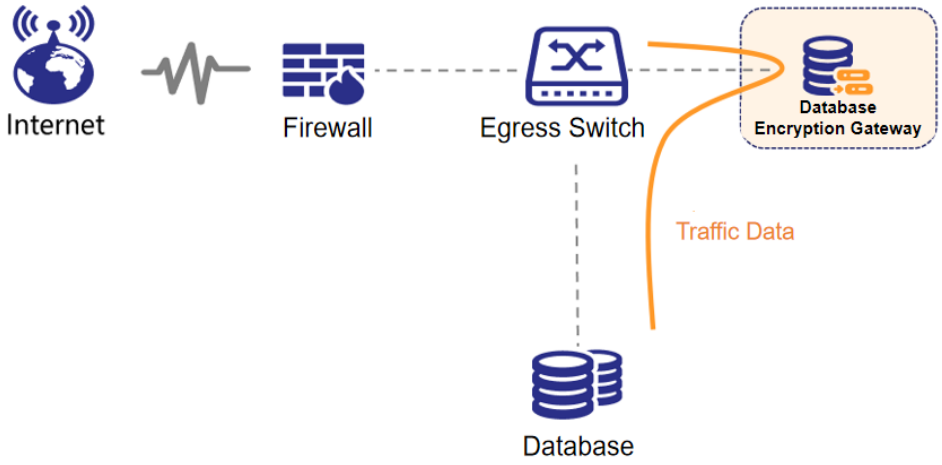
Database encryption and access control encrypt sensitive data in the database to ensure data security. This example shows how to encrypt the database.

Networking description:

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-6 Networking



Prerequisite

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

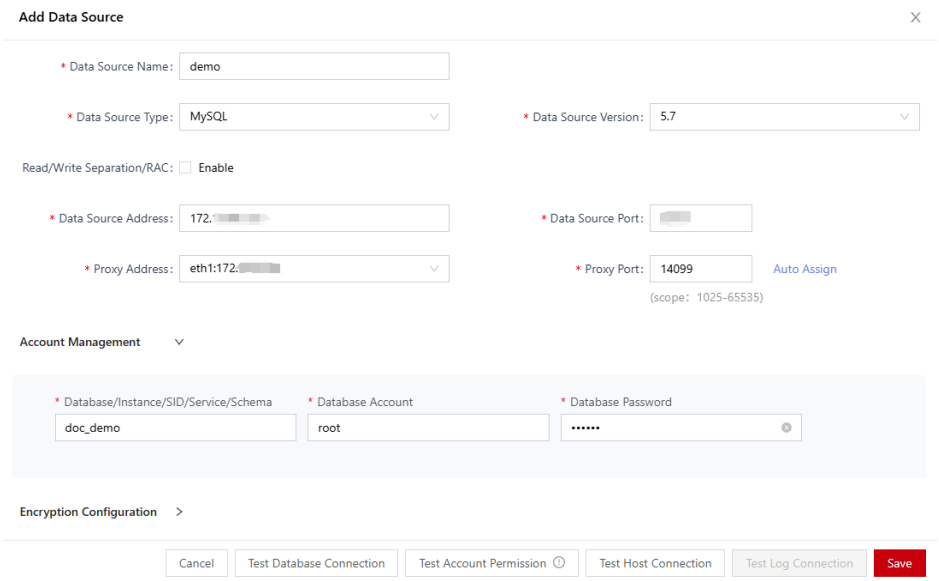
Step 1: Adding a Data Source

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 4-7 Adding a data source



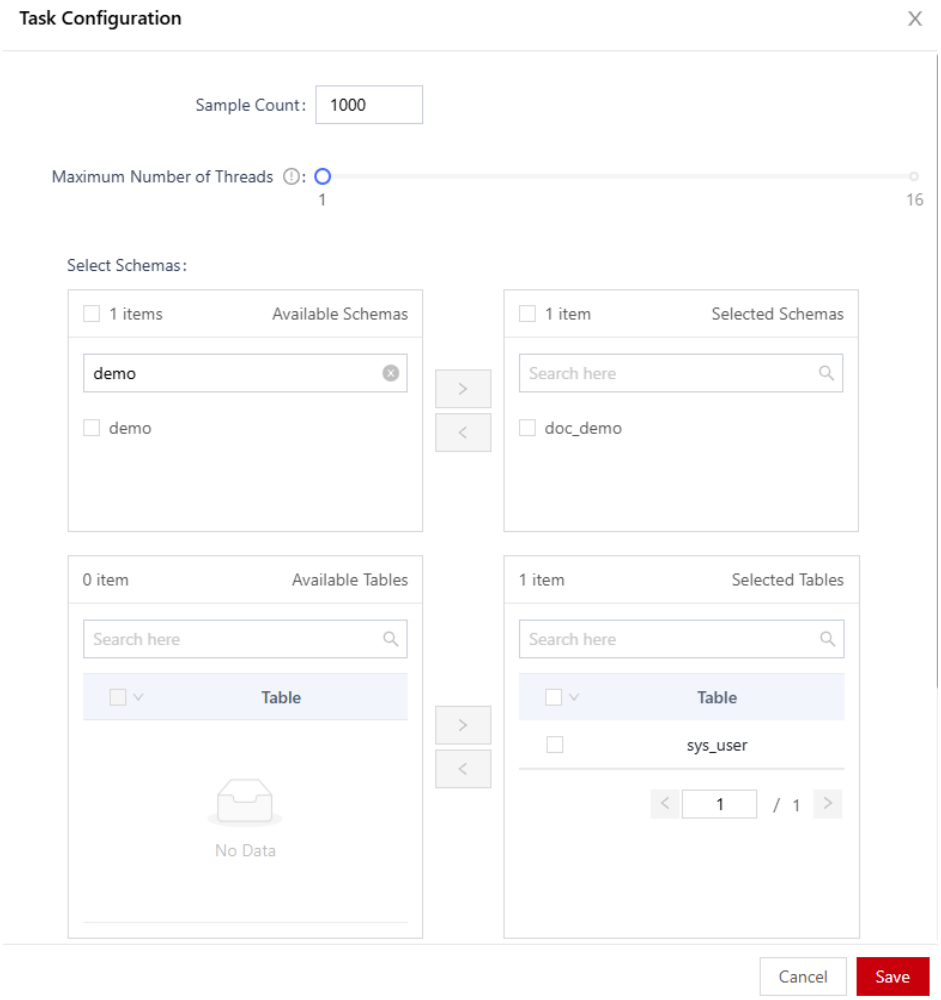
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 4-8 Configuring a sensitive data discovery task



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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

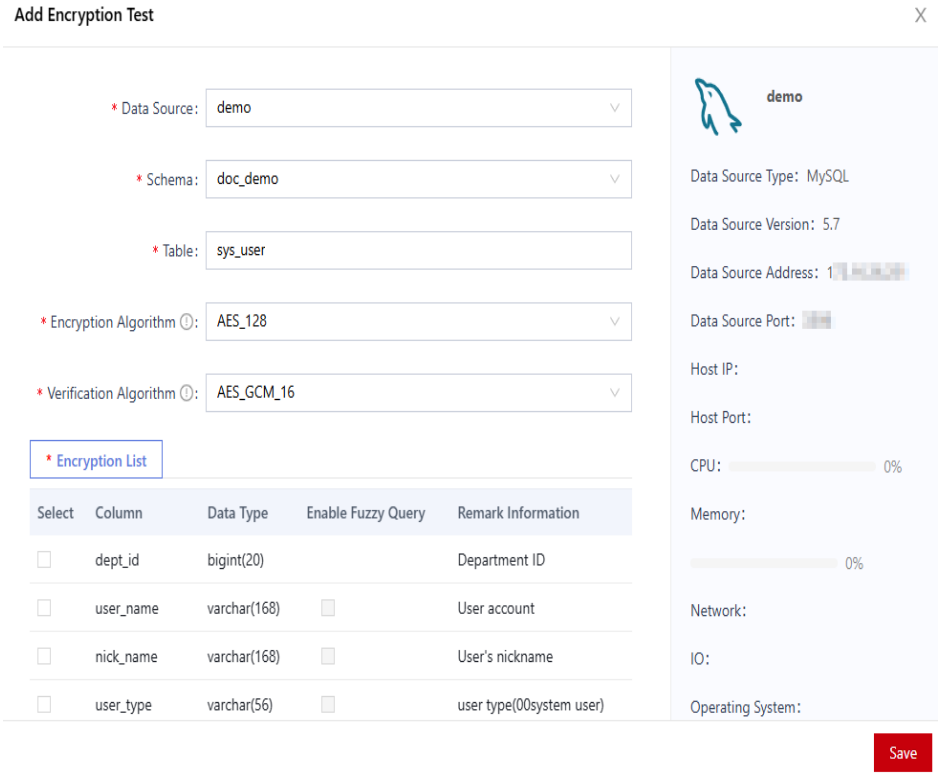
the amount of data, the longer the scan duration. You can view the scan progress on the page.

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 4-9 Adding an encryption test



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.

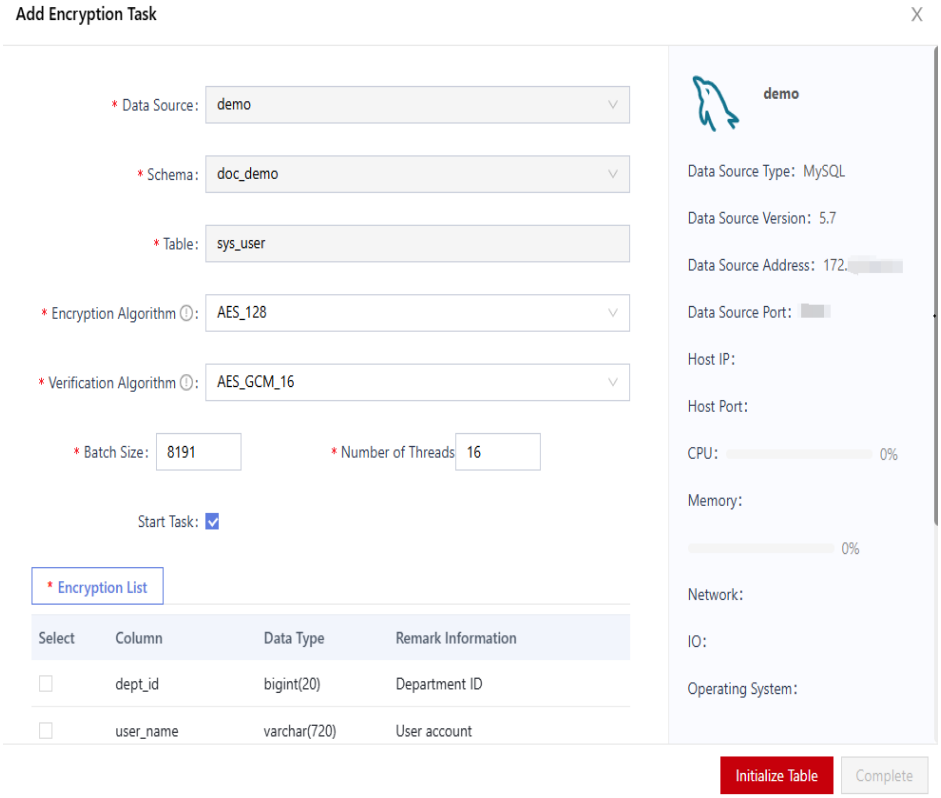
Step 4: Creating an Encryption Task in the Discovery Result

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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 4-10 Adding an encrypted task



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

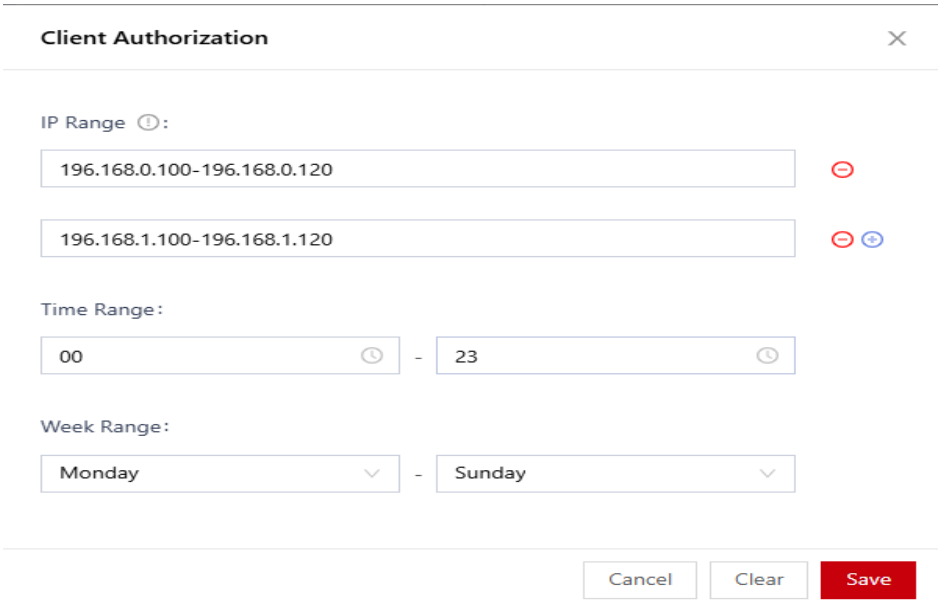
The authorization management module supports client authorization and user authorization. The intersection of the two authorization modes is used.

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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

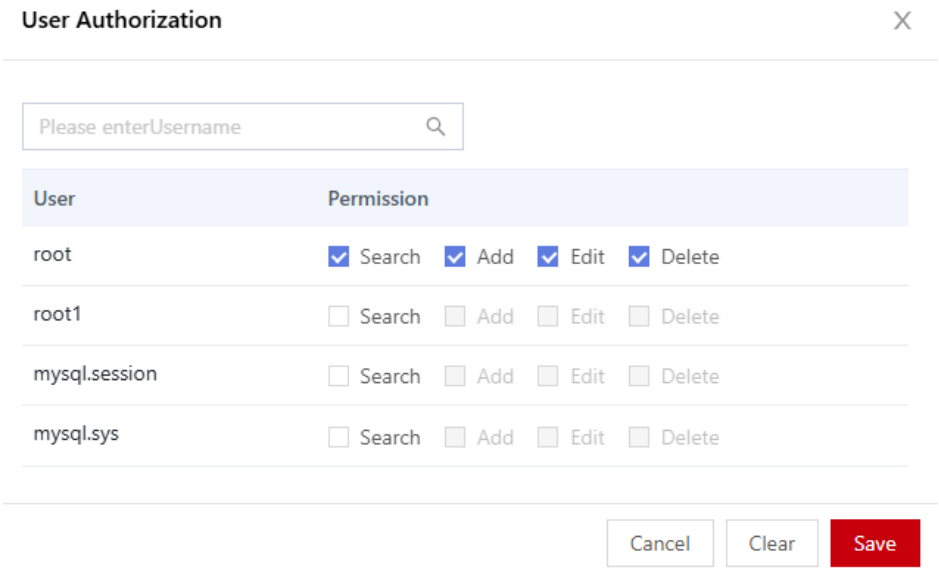
Figure 4-11 Client authorization



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 4-12 User authorization



Step 6: Connecting to the Database Through a Proxy

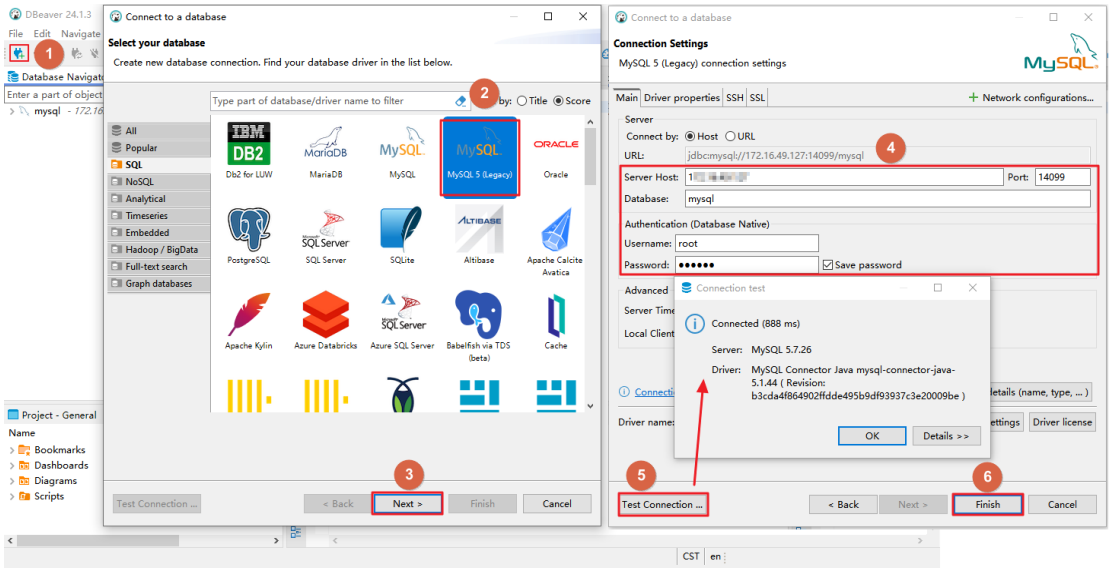
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 4-13 Connecting to the database through a proxy



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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-14 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 4-15 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 4-16 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 4-17 Encrypted data

	user_id	dept_id	user_name	nick_name	user_type	email	phonenumber	sex
1	1	103	admin1	aa	00	JAAvYmbTORP5hY6eHlgN4m36EIGEb4Hc1NRvqNFvBFuf	JAAvYWDVPxX/9Y+YH0e901lv1KkEEex/yqBtjZc=	1
2	2	105	admin2	aa	00	JAAvYmbTORP5hY6eHlgN4m36EIGEb4Hc1NRvqNFvBFuf	JAAvZ2DVPxX/9Y+YH0X/V4Oa6iiITcHnFlD09n1c=	1

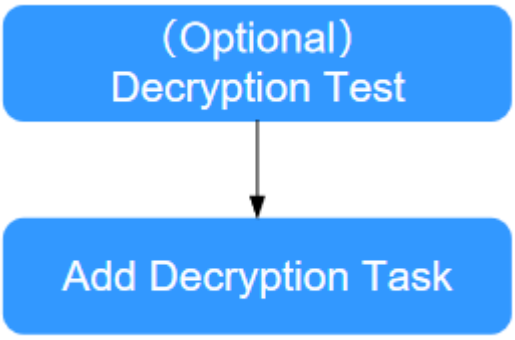
4.3.2 Scenario 2: Decryption Process and Typical Decryption Configuration

Decryption Process

Figure 4-18 shows the decryption process of database encryption and access control.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-18 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**.

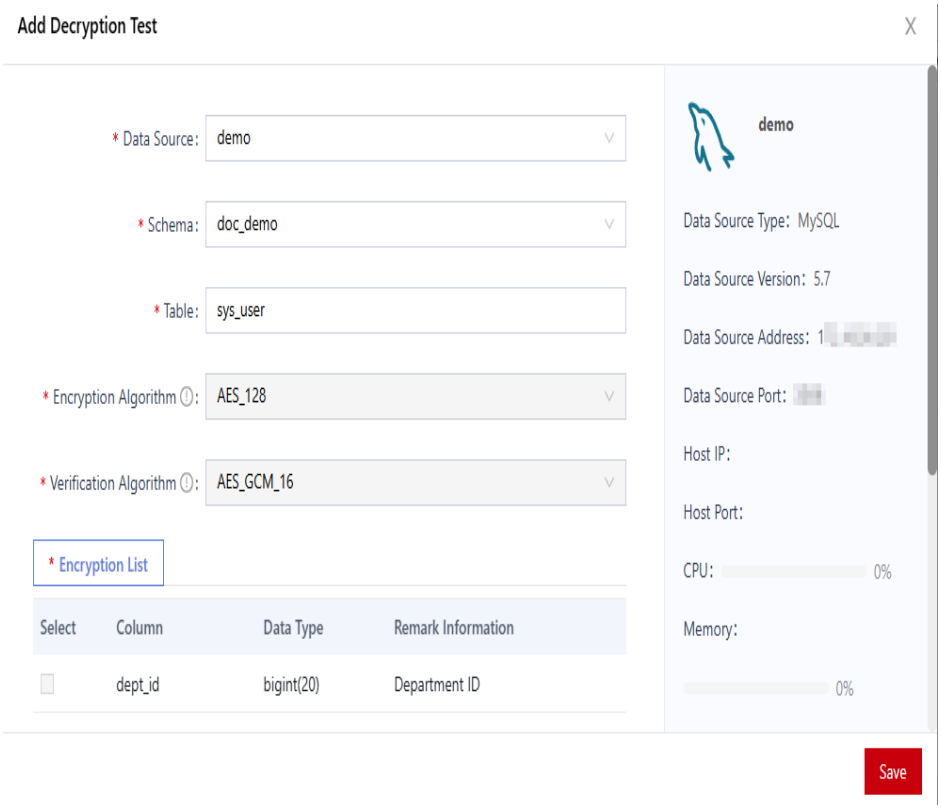
Step 1: Performing a Simulated Decryption Test

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-19 The decryption test is added.



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.

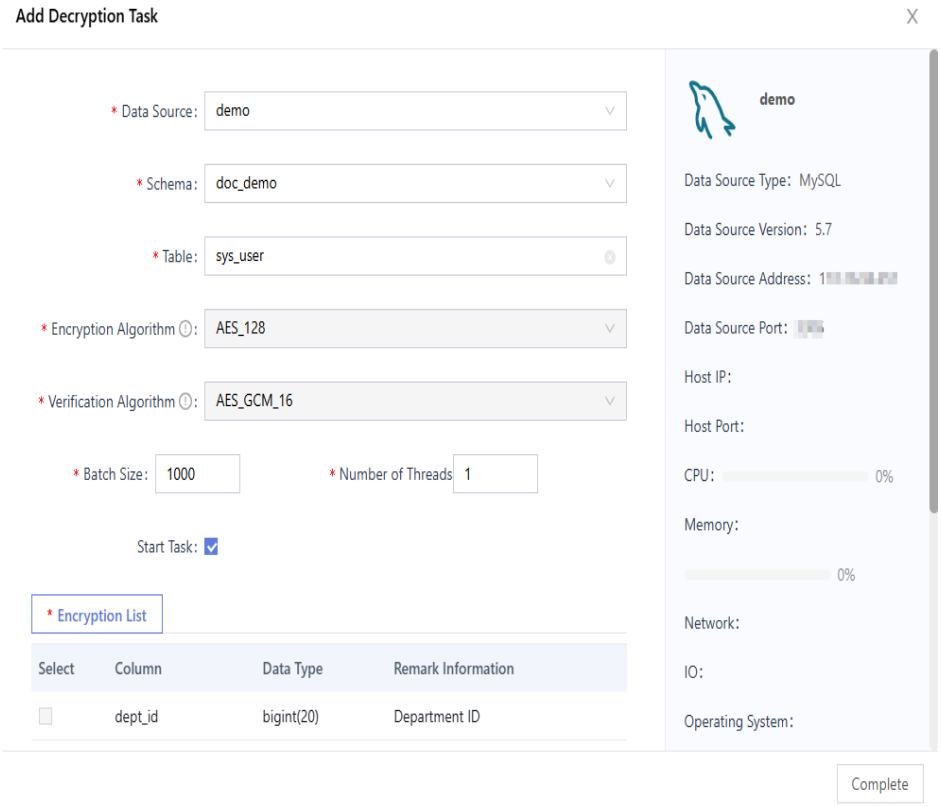
   If a decryption task needs to be configured after the test, delete the simulated decryption test first.

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-20 Adding a decryption task



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 4-21 Querying the result through the proxy

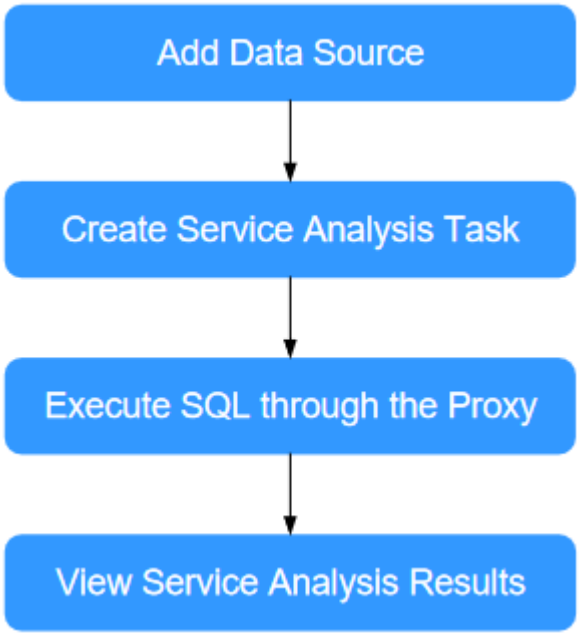
	user_id	dept_id	user_name	nick_name	user_type	email	phonenumber	sex
1	1	103	admin1	aa	00	1666666@163.com	15000000000	1
2	2	105	admin2	aa	00	1666666@163.com	13000000000	1

4.3.3 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 4-22** shows the service test process.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

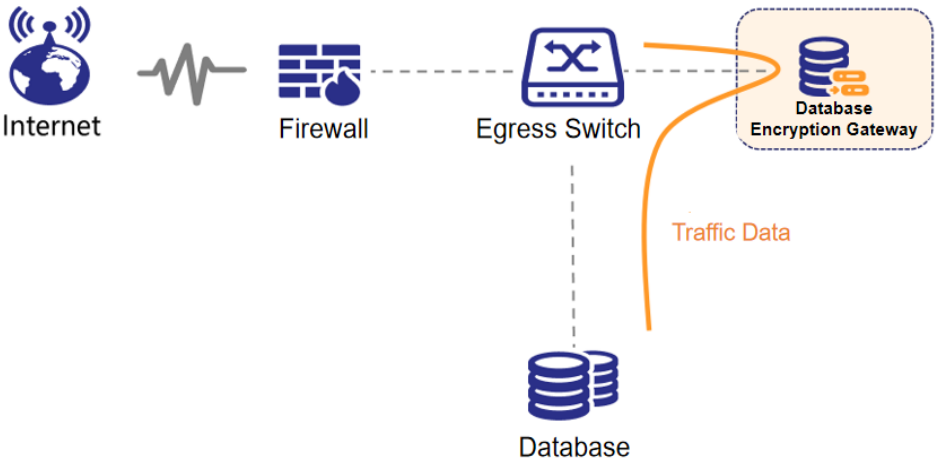
Figure 4-22 Service test process



Networking Description

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

Figure 4-23 Networking



Prerequisites

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

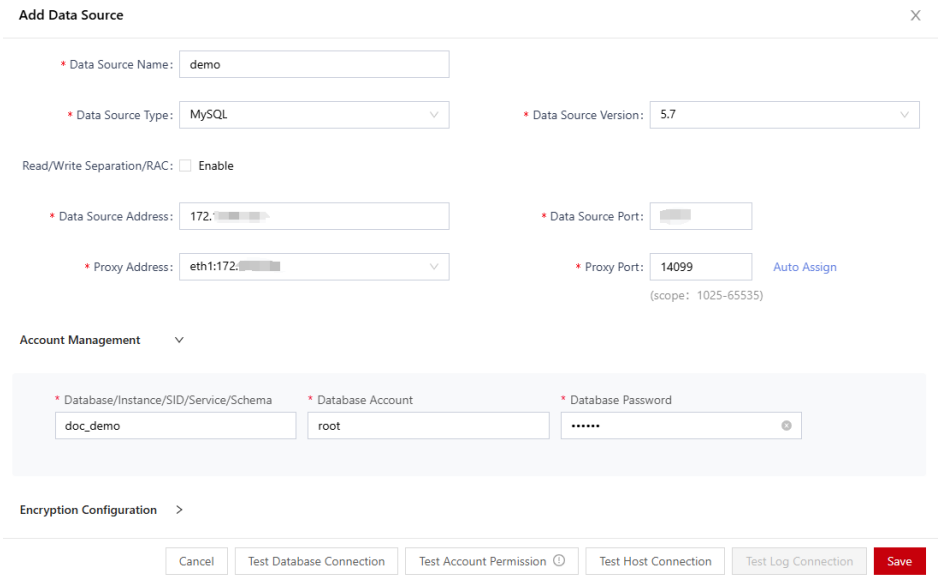
Step 1: Adding a Data Source

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 4-24 Adding a data source

   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**.

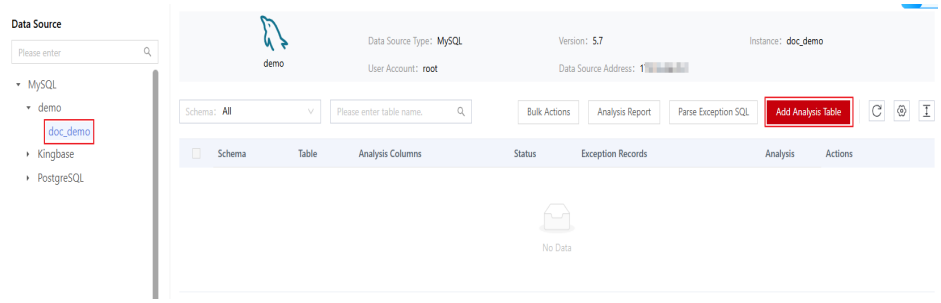
Step 2: Creating a Service Analysis Task

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.

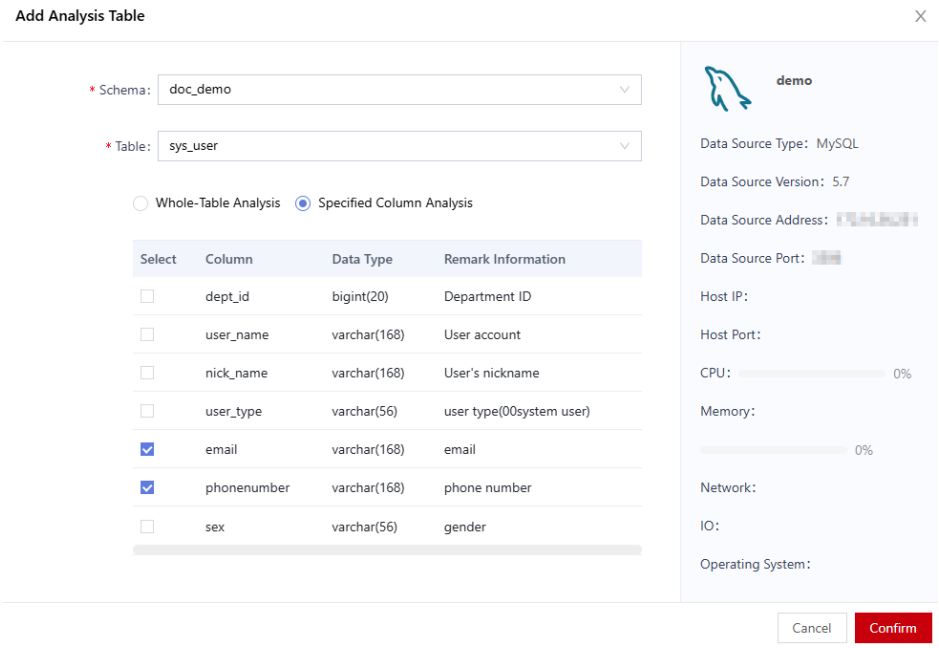
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-25 Adding a service analysis task



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

Figure 4-26 Configuring a table for analysis



Locate the target table and click the start button .

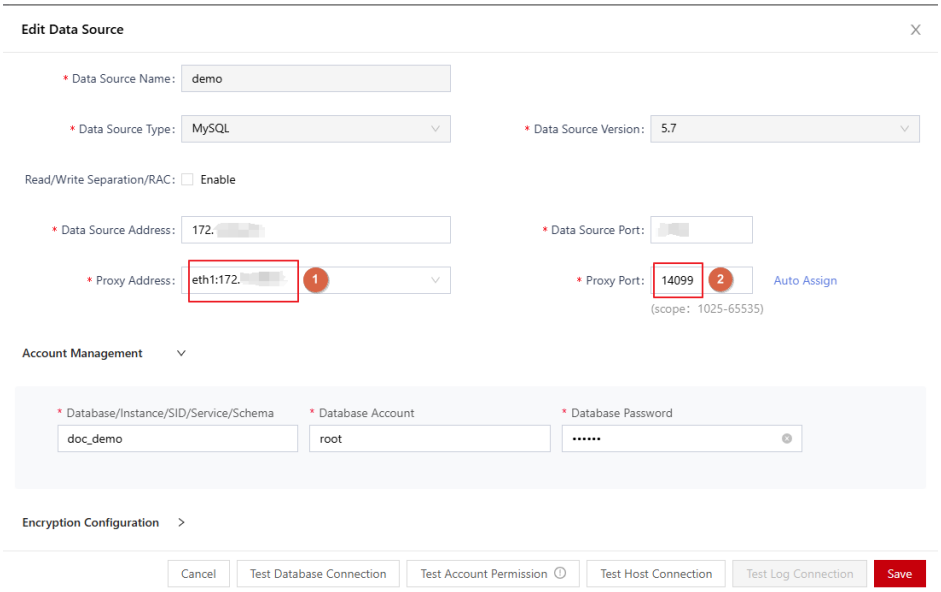
Step 3: Running SQL Statements Through the Proxy

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.

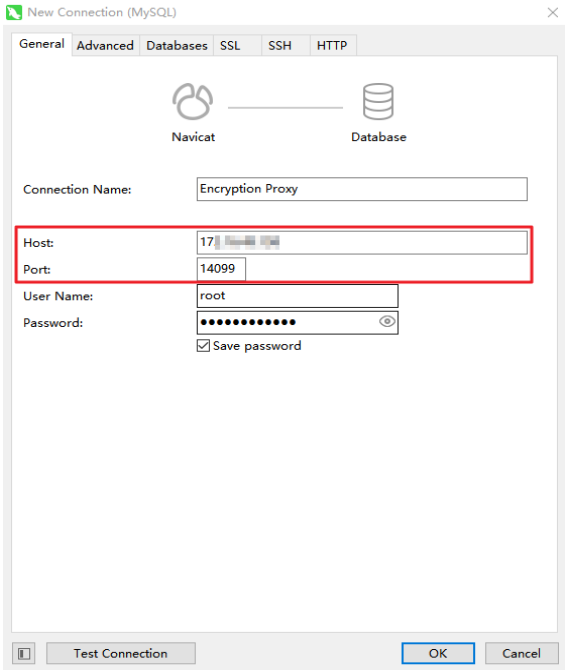
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-27 Viewing the proxy IP address and port number



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

Figure 4-28 Accessing a database



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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-4 SQL statement examples

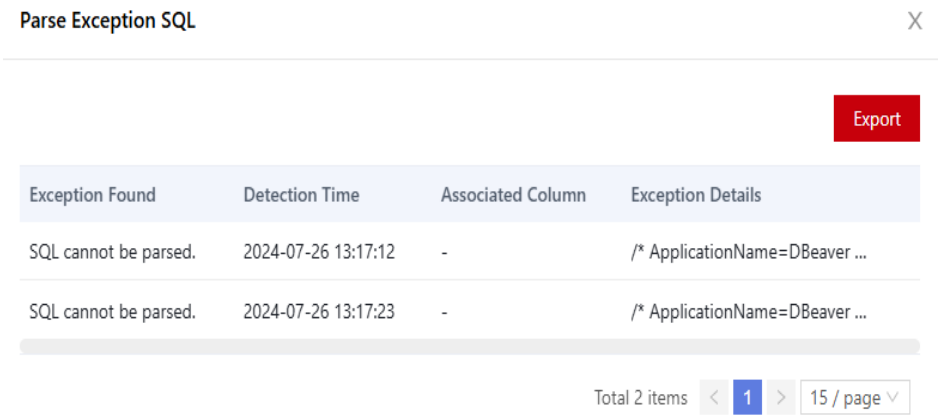
SQL type.	Example
Normal Statement	SELECT * FROM `sys_user`;
Exception statements:	SELECT * FROMM `sys_user`;
Blocking Statement	RENAME TABLE sys_user to abc;

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.

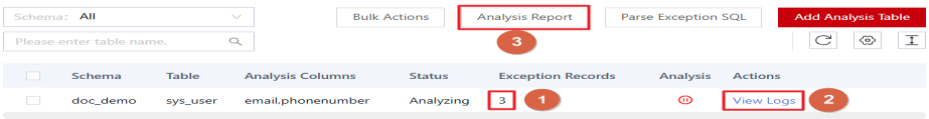
1. **Log in to the web console of the instance** as user **sysadmin**.
2. In the navigation tree on the left, choose **Service Test** > **Service Analysis**.
3. In the data source area on the left, click a data source.
4. Click **Parse Exception SQL** to view the abnormal SQL statements.

Figure 4-29 Abnormal SQL statements



5. View blocked SQL statements and system suggestions.

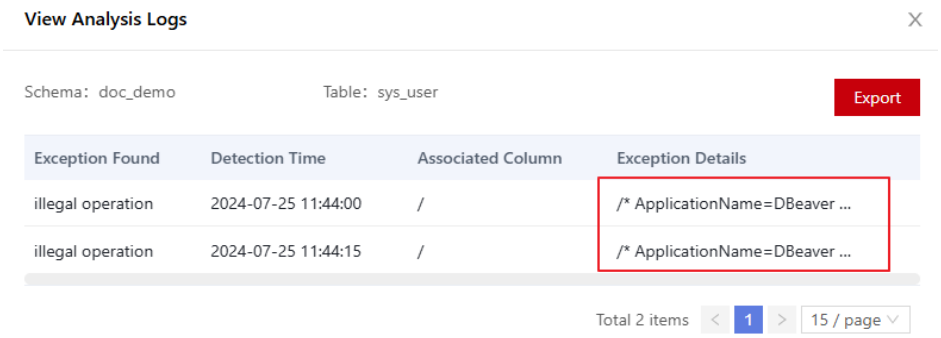
Figure 4-30 Blocked SQL statements



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.

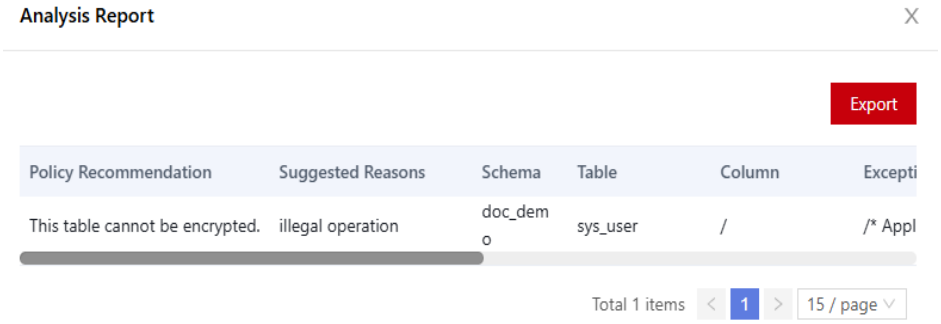
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-31 SQL statement blocking log



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

Figure 4-32 Analysis and suggestions



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.

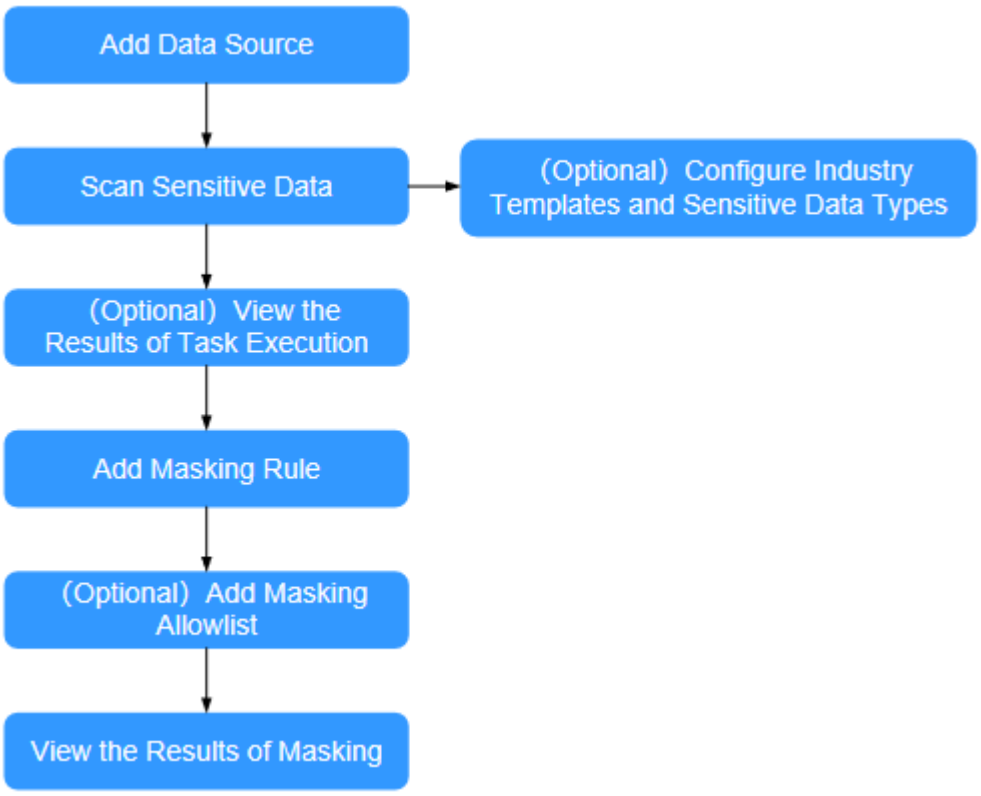
4.3.4 Scenario 4: Typical Dynamic Data Masking Configuration

Dynamic Data Masking Flowchart

With database encryption and access control, you can configure dynamic masking policies to mask plaintext data in database assets. **Figure 4-33** shows the dynamic masking process.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-33 Dynamic masking process



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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

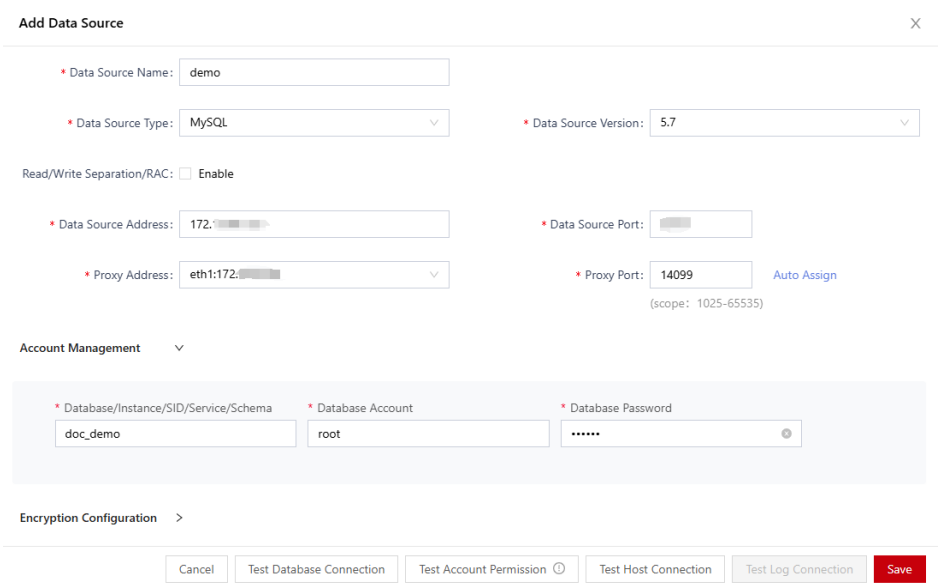
Step 1: Adding a Data Source

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 4-34 Adding a data source



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**.

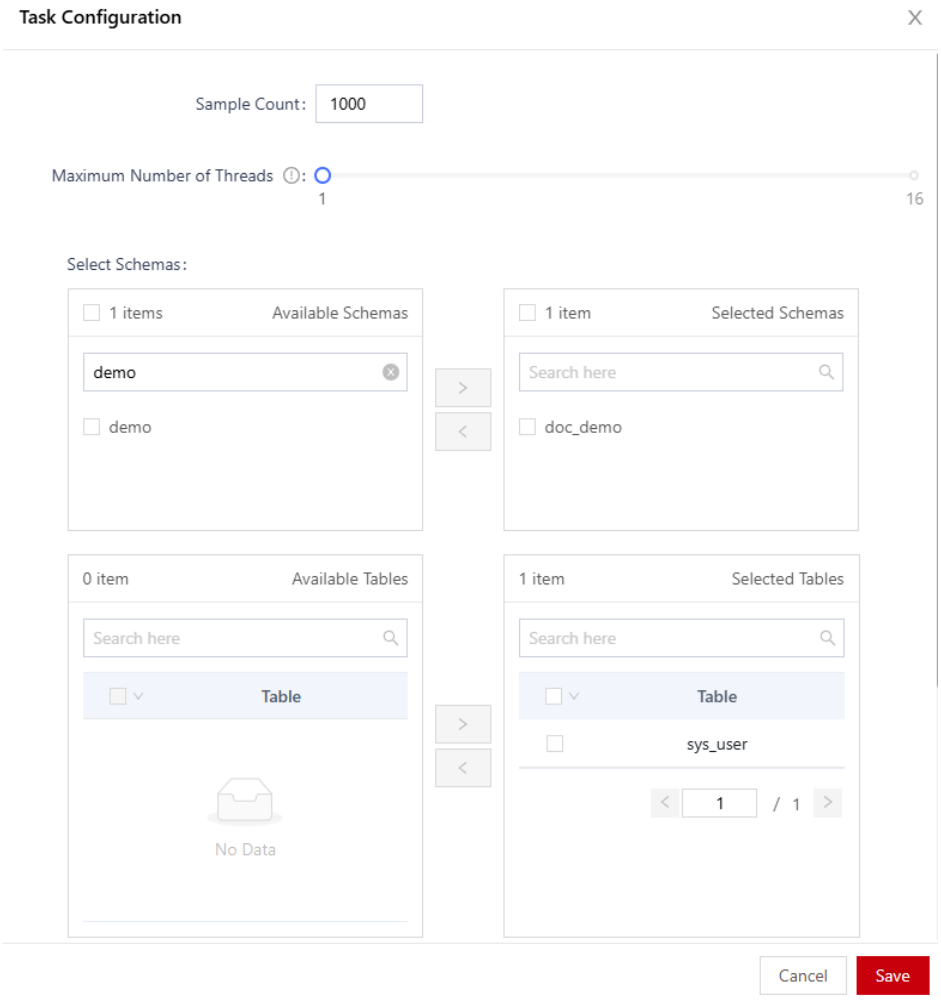
Step 2: Executing a Sensitive Data Discovery Task

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 4-35 Configuring a sensitive data discovery task



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.

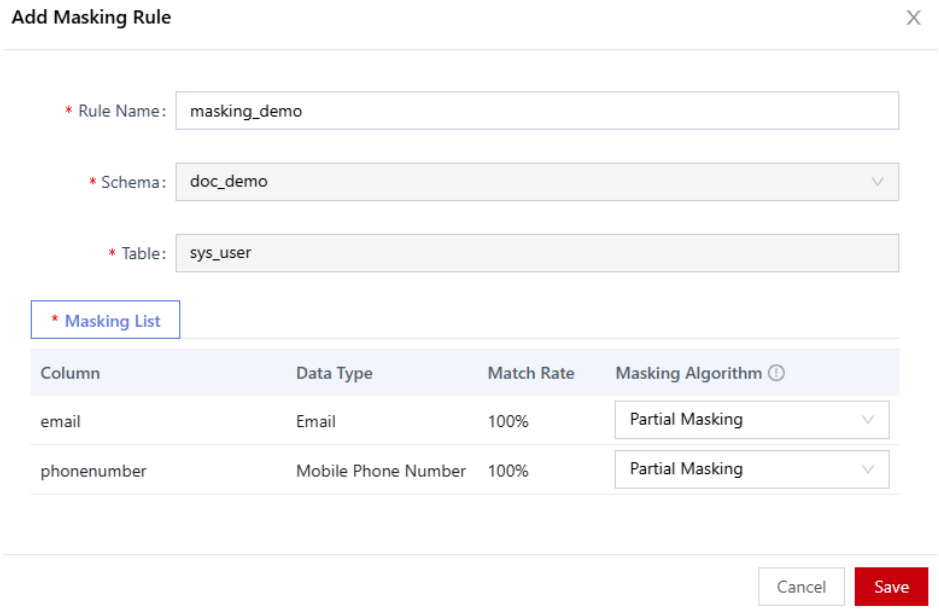
Step 3: Creating a Masking Rule in the Discovery Result

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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 4-36 Adding a masking rule



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

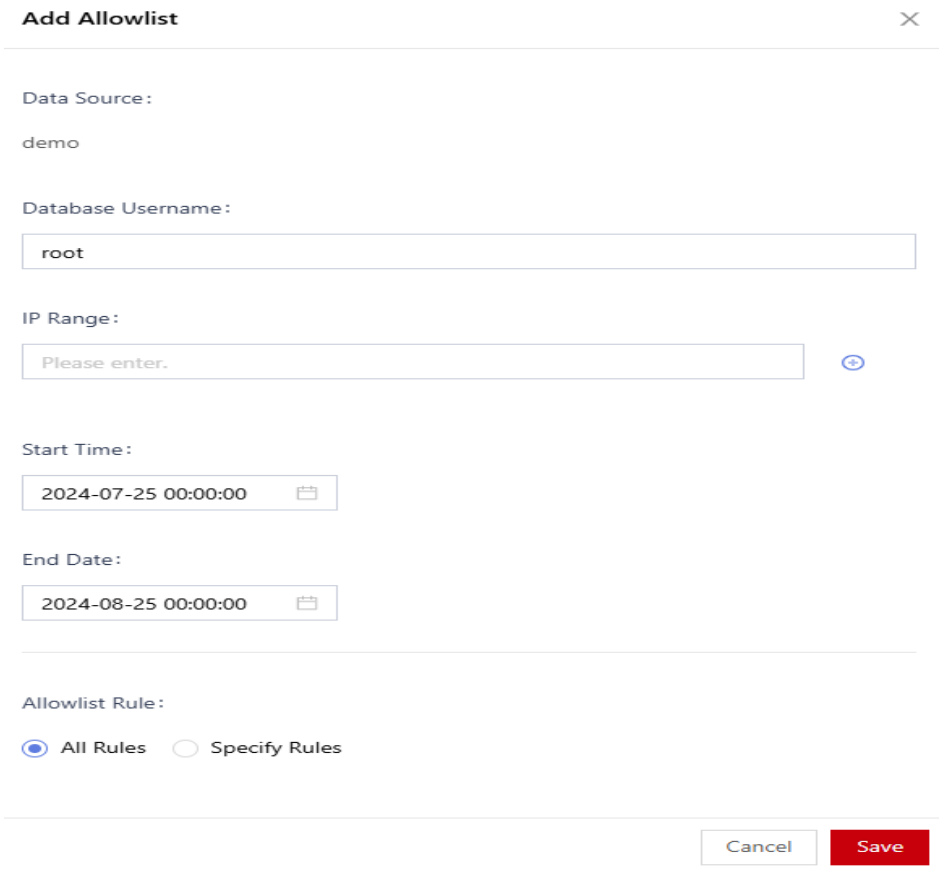
The masking rule is automatically enabled after being saved. If plaintext data is queried during database access, the masking results of the data will be retrieved. In this case, you can configure a masking allowlist. If data matching the allowlist will not be masked.

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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-37 Adding an allowlist



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

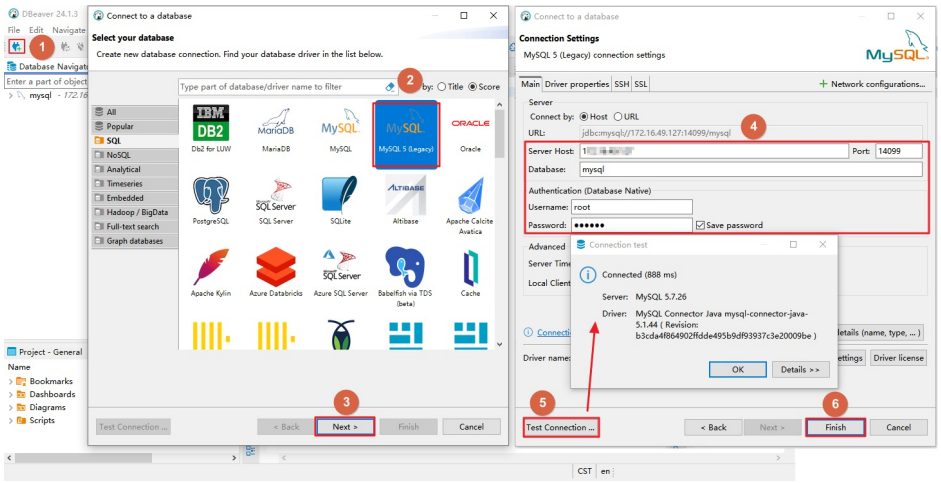
CAUTION

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-38 Connecting to the database through a proxy



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 4-39 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 4-40 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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.4 Instance Management

4.4.1 Enabling an Instance

The instance needs to be started in the following scenarios:

- When the **running status** of an instance is **Disabled**, 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 DSC console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Locate the target instance, and choose in the **Operation** column.

----End

4.4.2 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 DSC console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Locate the target instance and choose in the **Operation** column.

Step 4 In the displayed dialog box, click **OK**. After the instance is stopped, its status changes to **Disabled**.

NOTE

To forcibly stop an instance, select **Force Stop** in the **Stop Instance** dialog box. Forcibly stopping an instance may cause data loss. Ensure that all data files have been saved before performing this operation.

----End

4.4.3 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- 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 DSC console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Locate the target instance and choose in the **Operation** column.

Step 4 In the displayed dialog box, click **OK**.

Step 5 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

To forcibly restart an instance, select **Force Restart** in the **Restart Instance** dialog box. Forcibly stopping an instance may cause data loss. Ensure that all data files have been saved before performing this operation and no operations are performed in the system.

----End

4.4.4 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 DSC console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Locate the target instance and choose **More** > **Unbind EIP** in the **Operation** column.

Step 4 In the displayed **Unbind EIP** dialog box, click **OK**.

----End

4.5 Database Security Encryption Instance Management

On the management console, you can restart, disable, and unbind EIP from database instances.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

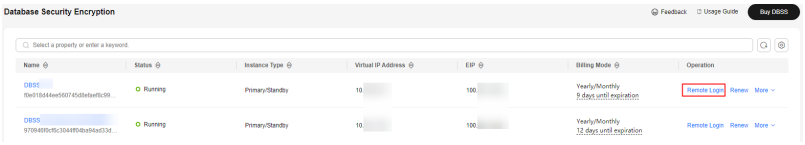
Figure 4-41 Database security encryption instance

----End

Remote Login

Step 1 Locate the target instance and click **Remote Login** in the **Operation** column.

Figure 4-42 Remotely logging in to a database encryption instance



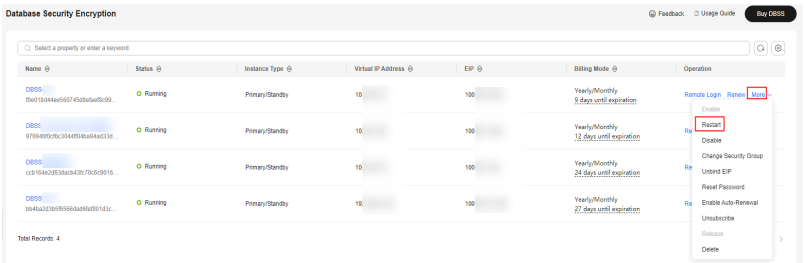
Step 2 On the displayed login page, enter the username and password of the instance and click **Log In**. The database encryption console is displayed.

----End

Restarting an Instance

Step 1 In the **Operation** column of the target instance, choose **More** > **Restart**.

Figure 4-43 Restarting a database encryption instance



Step 2 In the displayed dialog box, click **OK**. The instance automatically restarts.

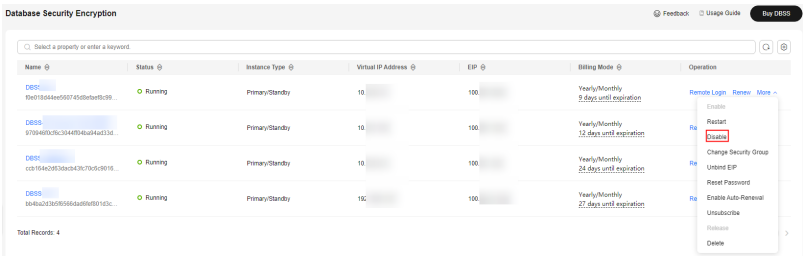
----End

Stopping an Instance

Step 1 In the **Operation** column of the target instance, choose **More** > **Disable**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-44 Disabling a database encryption instance



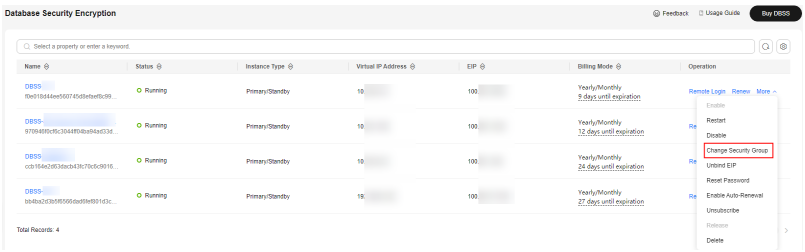
Step 2 In the displayed dialog box, click **OK**. The instance is automatically disabled.

----End

Modifying a Security Group

Step 1 In the **Operation** column of the target instance, choose **More** > **Change Security Group**.

Figure 4-45 Modifying the security group



Step 2 In the displayed dialog box, select a security group and click **OK**.

NOTE

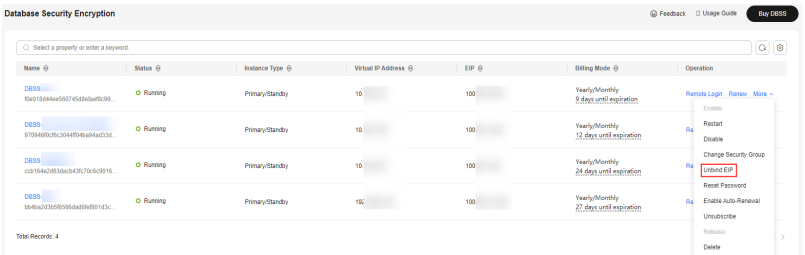
Only existing security groups can be selected.

----End

Unbinding an EIP

Step 1 In the **Operation** column of the target instance, choose **More** > **Unbind EIP**.

Figure 4-46 Unbinding an EIP



Step 2 In the displayed dialog box, click **OK**. The EIP will be unbound from the instance.

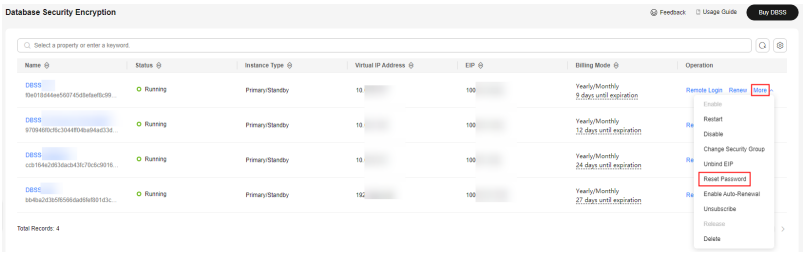
----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Resetting a Password

Step 1 In the **Operation** column of the target instance, choose **More** > **Reset Password**.

Figure 4-47 Resetting the password



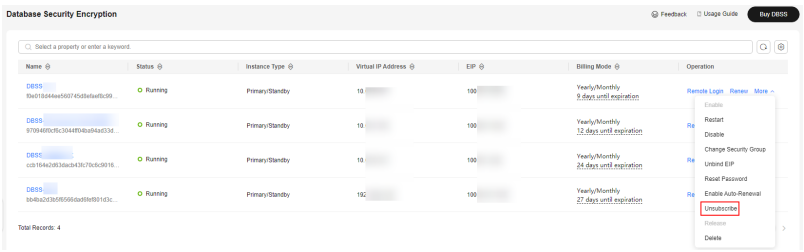
Step 2 In the dialog box that is displayed, enter the new password and click **OK**.

----End

Unsubscribing

Step 1 In the **Operation** column of the target instance, choose **More** > **Unsubscribe**.

Figure 4-48 Unsubscribing from an instance



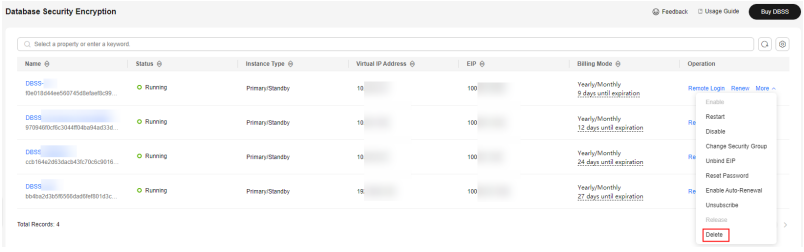
Step 2 Confirm the unsubscription and click **Yes**.

----End

Deleting

Step 1 In the **Operation** column of the target instance, choose **More** > **Delete**.

Figure 4-49 Deleting an instance



Step 2 In the displayed dialog box, confirm the deletion information and click **OK**.

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.6 System Administrator Operation Guide

4.6.1 Platform Management

Before using database encryption and access control for the first time, you need to complete the basic configurations described in this section.

4.6.1.1 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

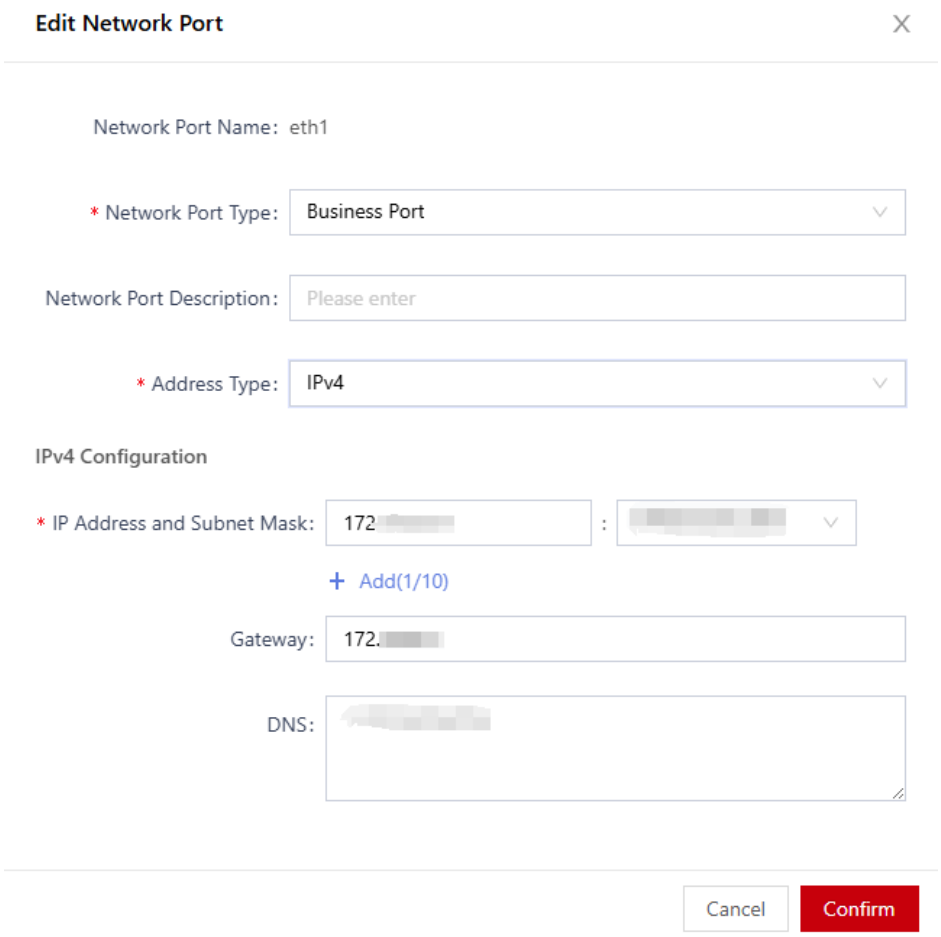
Step 1 Log in to a database encryption and access control instance as the **sysadmin** user.

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 4-50**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-50 Editing a network port



Step 4 Configure NIC information. For details, see **Table 4-5**.

Table 4-5 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: • **Management Port** • **Business Port**
Network Port Description	Enter the description as required.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description
Address Type	Select an address type. Its value can be: • **Unconfigured Address** • IPv4 • IPv6 • 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. **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

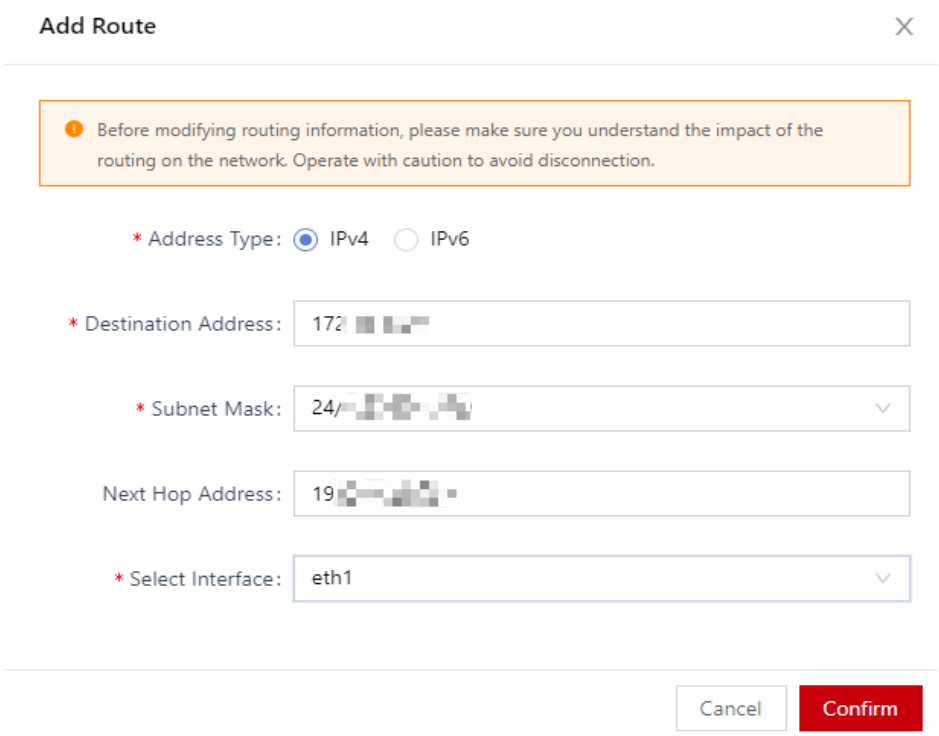
Step 1 **Log in to a database encryption and access control instance** as the **sysadmin** user.

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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-51 Adding a route



Step 4 Configure route information. For details, see **Table 4-6**.

Table 4-6 Configuring route information

Parameter	Description
Address Type	The options are as follows: • IPv4 • 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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.6.1.2 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**.

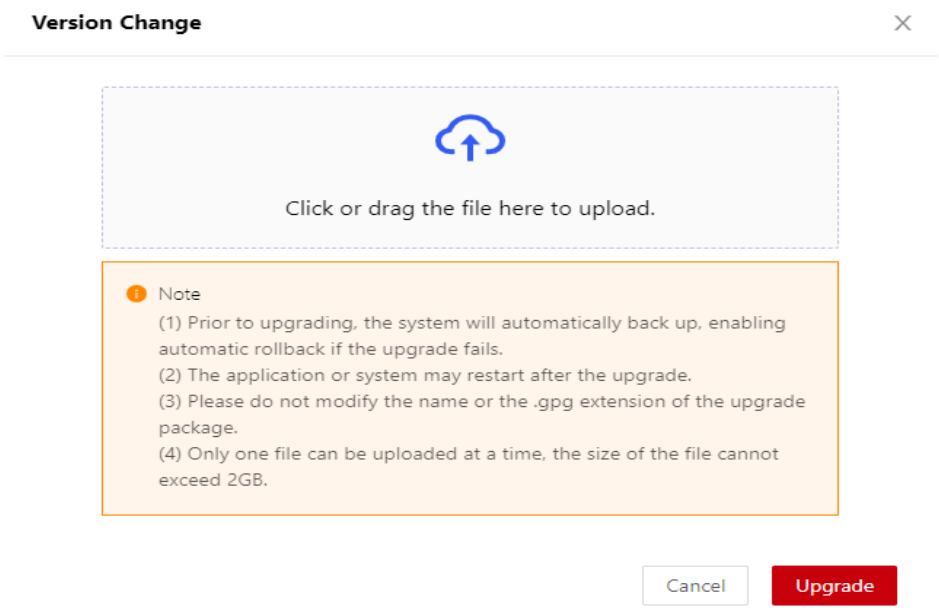
Step 3 Click **System Upgrade**.

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-52 Uploading an upgrade package



Step 6 After the upgrade is successful, view the upgrade records in the version change history.

----End

4.6.1.3 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:

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

a. In the **Periodic Backup** area, click **Set**.

Figure 4-53 Configuring automatic backup

b. In the **Set Periodic Backup** dialog box, configure the periodic backup information. For details about the configuration information, see **Table 4-7**.

Table 4-7 Backup description

Parameter	Description
Backup Type	You can select **Local backup**.
Backup Cycle	Backup period. The options are as follows: ▪ **None**: No periodic backup is performed. ▪ **Daily**: The data is backed up once a day. ▪ **Weekly**: The data is backed up once a week. ▪ **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

4.6.1.4 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 4-8 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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

4.6.1.5 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.

4.6.2 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

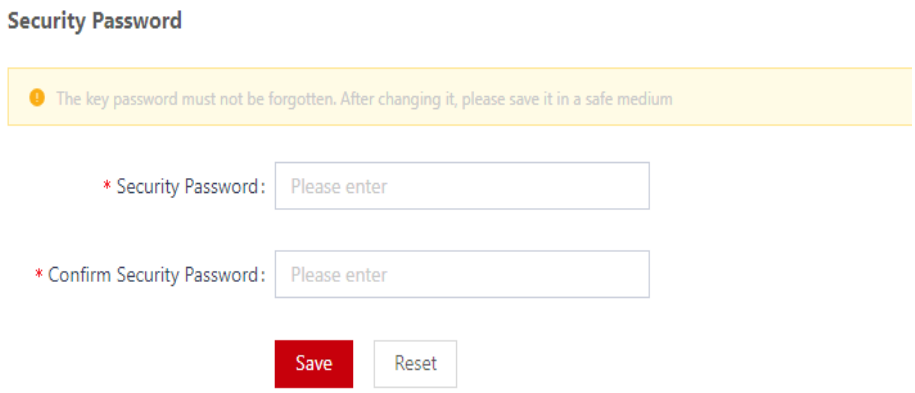
Step 2 In the navigation tree on the left, choose **System Management** > **System Settings**. On the displayed **General Settings** page, click **Secure Password Setting**. The **Security Password** page is displayed.

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 4-54 Changing the security password



Step 5 In the **Password Verification** text box, enter the old security password and click **Confirm**.

----End

4.6.3 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 4-9 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 4-10**.

Figure 4-55 Initializing a key

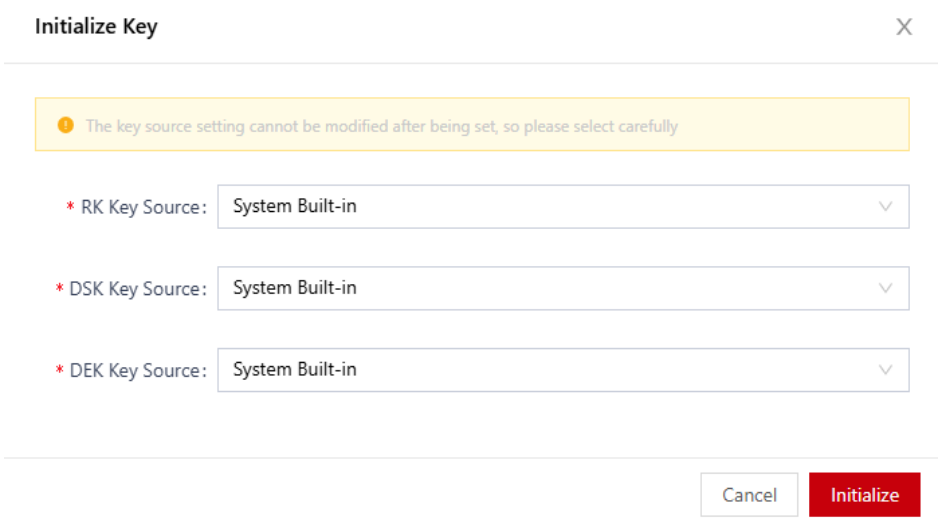


Table 4-10 Initializing a key

Parameter	Description
RK Key Source	RK source. The following sources are supported: • **System Built-in**: fixed key built in the system, which is used only for tests. • **KEY_Service**: key platform connected to the system. For details about how to configure a key platform, see **Interconnecting with KMS**. After the configuration, select a platform vendor. **NOTE** KMS requires the KMS CMKFullAccess permission.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description
DSK Key Source	DSK source. The following sources are supported: • **System Built-in**: fixed key built in the system, which is used only for tests. • **KEY_Service**: key platform connected to the system. For details about how to configure the key platform, see **Interconnecting with KMS**. After the configuration, select a platform vendor. **NOTE** KMS requires the KMS CMKFullAccess permission.
DEK Key Source	DEK source. The following sources are supported: • **System Built-in**: fixed key built in the system, which is used only for tests. • **KEY_Service**: key platform connected to the system. For details about how to configure the key platform, see **Interconnecting with KMS**. After the configuration, select a platform vendor. **NOTE** KMS requires the KMS CMKFullAccess permission.

Step 6 Click **Initialize**.

----End

4.6.4 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 4-11 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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 4-12 Database account permissions for database encryption

Database	System Catalog Requiring the SELECT Permission	Database Account Permission
MySQL	mysql.user performance_schema.*	select insert create update delete drop alter index
RDS_MYSQL	mysql.user performance_schema.*	select insert create update delete drop alter index

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Database	System Catalog Requiring the SELECT Permission	Database Account Permission
TDSQL	mysql.user performance_schema.*	select insert create update delete drop alter index
MariaDB	mysql.user performance_schema.*	select insert create update delete drop alter index
DM	SYS.ALL_SUBPART_KEY_COLUMNS SYS.ALL_USERS SYS.ALL_CONS_COLUMNS SYS.ALL_CONSTRAINTS SYS.ALL_TABLES SYS.ALL_TABLE_COLUMNS SYS.ALL_COL_COMMENTS SYS.ALL_PART_KEY_COLUMNS SYS.ALL_IND_COLUMNS SYS.ALL_INDEXS V$VERSION V$LOCK SYS.DBMS_LOB SYS.DBMS_METADATA	The user role must be **dba**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Database	System Catalog Requiring the SELECT Permission	Database Account Permission
postgreSQL	pg_catalog.pg_class pg_catalog.pg_index pg_catalog.pg_user pg_catalog.pg_indexes information_schema.columns information_schema.sequences information_schema.tables pg_catalog.pg_sequence	The user must be the table owner or the **dba** role.
RDS_PostgreSQL	pg_catalog.pg_class pg_catalog.pg_index pg_catalog.pg_user pg_catalog.pg_indexes information_schema.columns information_schema.sequences information_schema.tables pg_catalog.pg_sequence	The user must be the table owner or the **dba** role.
TBASE	pg_catalog.pg_class pg_catalog.pg_index pg_catalog.pg_user pg_catalog.pg_indexes information_schema.columns information_schema.sequences information_schema.tables pg_catalog.pg_sequence	The user must be the table owner or the **dba** role.
GAUSSDB	pg_catalog.pg_class pg_catalog.pg_index pg_catalog.pg_user pg_catalog.pg_indexes information_schema.columns information_schema.sequences information_schema.tables pg_catalog.pg_sequence	The user must be the table owner or the **dba** role.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Database	System Catalog Requiring the SELECT Permission	Database Account Permission
Kingbase 8.6 (pg)	pg_catalog.pg_class pg_catalog.pg_index pg_catalog.pg_user pg_catalog.pg_indexes information_schema.columns information_schema.sequences information_schema.tables pg_catalog.pg_sequence pg_catalog.pg_matviews	The user must be the table owner or the **dba** role.
KINGBASE 8.3	sys_catalog.sys_class sys_catalog.sys_index sys_catalog.sys_user sys_catalog.sys_indexes information_schema.columns information_schema.sequences information_schema.tables sys_catalog.sys_sequence sys_catalog.sys_matviews	The user must be the table owner or the **dba** role.
Oracle	SYS.ALL_SUBPART_KEY_COLUMNS SYS.DUAL SYS.ALL_USERS SYS.ALL_CONS_COLUMNS SYS.ALL_CONSTRAINTS SYS.ALL_TABLES SYS.ALL_TABLE_COLUMNS SYS.ALL_COL_COMMENTS SYS.ALL_PART_KEY_COLUMNS SYS.ALL_IND_COLUMNS SYS.ALL_INDEXS SYS.V_$INSTANCE SYS.DBMS_LOB SYS.DBMS_METADATA DBA_TABLES DBA_TAB_COLS	The user role must be **dba**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Database	System Catalog Requiring the SELECT Permission	Database Account Permission
SQLserver	sys.tables sys.indexes sys.index_columns sys.default_constraints sys.systypes sys.extended_properties sys.foreign_key_columns sys.check_constraints sys.foreign_keys sys.columns sys.objects sys.all_columns sys.types sys.syslogins sys.all_objects sys.schemas sys.key_constraints sys.computed_columns sys.triggers sys.partition_schemes sys.dm_sql_referencing_entities	schemaSelect schemaInsert schemaUpdate schemaAlter createTable VIEW SERVER STATE SELECT permission of the encrypted table INSERT permission of the encrypted table ALTER permission of the encrypted table
HighGO	pg_catalog.pg_class pg_catalog.pg_index pg_catalog.pg_user pg_catalog.pg_indexes information_schema.columns information_schema.sequences information_schema.tables pg_catalog.pg_sequence	The user must be the table owner or the **dba** role.
DWS	pg_catalog.pg_class pg_catalog.pg_index pg_catalog.pg_user pg_catalog.pg_indexes information_schema.columns information_schema.sequences information_schema.tables pg_catalog.pg_sequence	The user must be the table owner or the **dba** role.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 4-13**.

Table 4-13 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. • The value range is 1025 to 65535. • 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. 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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: – **One Key Per Asset**: The DEKs of assets are the same. Connection query and cross-database query are supported. – **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: – **Ciphertext**: Ciphertext is displayed. The encoding format is Base64 or hexadecimal. For details, see **Setting Encryption Parameters**. – **Default Data**: Default data is displayed. You need to set the default data of the string type. – NULL: The content is blank.
(Optional) Host Information 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

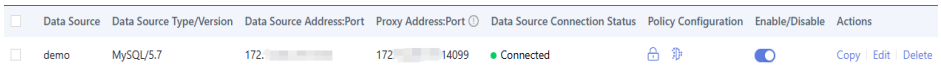
If the database account permission does not meet the encryption requirements, configure the database account permission by referring to **Table 4-12**.

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 4-56**.

Figure 4-56 Data source list



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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- 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.

4.6.5 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

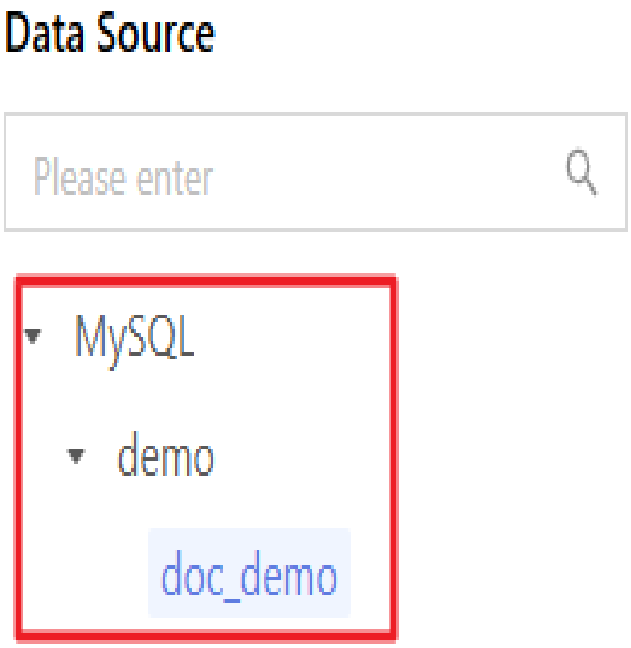
Step 1 **Log in to a database encryption and access control instance** as the **sysadmin** user.

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.

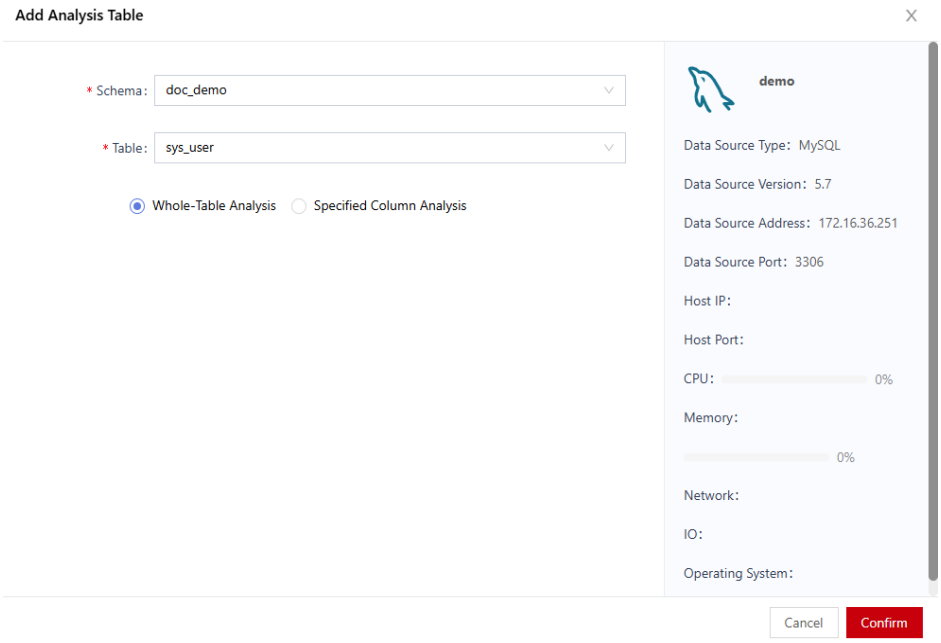
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-57 Selecting a data source



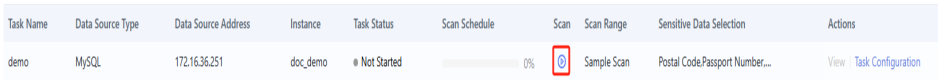
3. Click **Add Analysis Table**, configure a table, and click **OK**.

Figure 4-58 Adding a table



4. Click the icon in the **Start** column of the table.

Figure 4-59 Start



Step 3 Use the proxy address to access the database and run a SQL statement.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

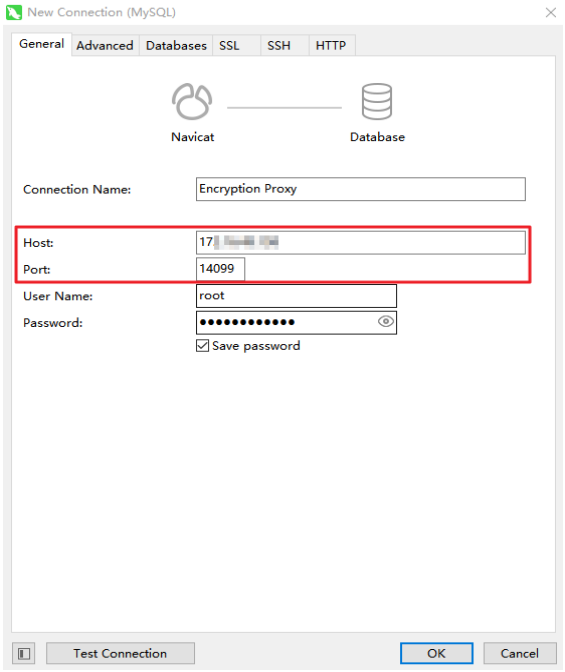
1. Choose **Asset Management** > **Data Source Management** and obtain the proxy address.

   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 4-60 Configuring the proxy address



3. Run an abnormal SQL statement on the database tool.

   For example, run the following statements:

   Table 4-14 Exception examples

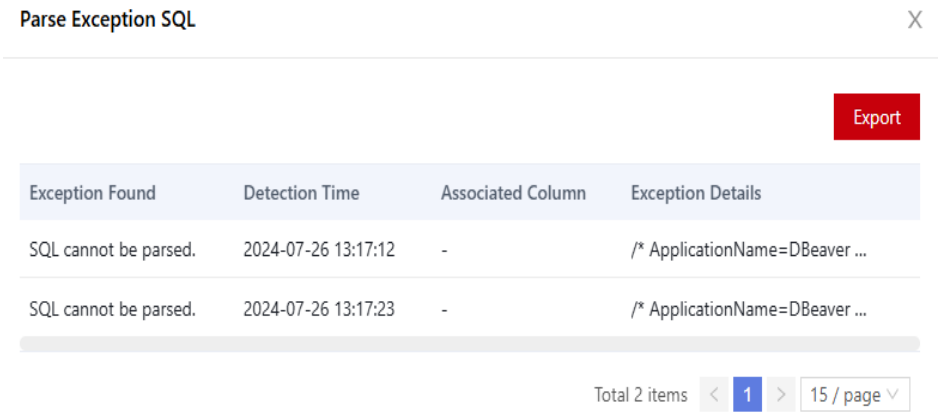
Type	Statement
Abnormal SQL statement	select * form table
Blocked SQL statement	RENAME TABLE sys_user to abc

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

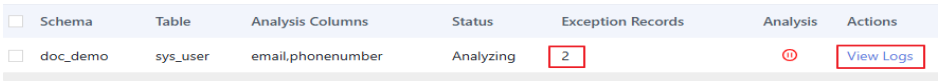
Figure 4-61 Abnormal SQL statements



Step 5 On the web console, view the analysis results of blocked SQL statements.

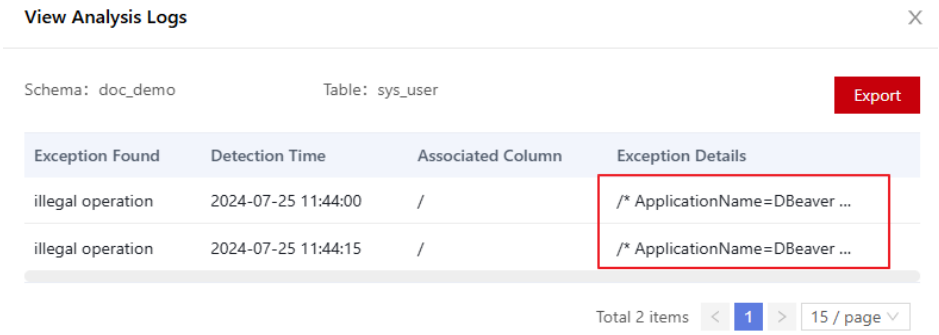
1. In the navigation tree on the left, choose **Service Test** > **Service Analysis**.
2. In the data source area on the left, click a data source.
3. You can view the number of abnormal records in the list.

Figure 4-62 Viewing the number of blocked SQL statements



4. Click **View Log** to view the records of blocked SQL statements.

Figure 4-63 Viewing blocked SQL statements

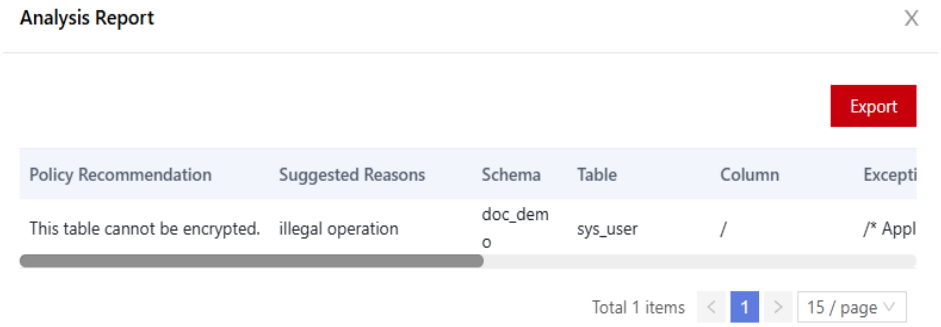


5. Click **Analysis Report** to view the encryption suggestions of the table.

   As shown in **Figure 4-64**, if you have renamed a database table, you are not advised to encrypt the table.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-64 Analysis and suggestions



----End

4.6.6 Sensitive Data Discovery

4.6.6.1 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 4-15 Parameters for a sensitive data discovery task

Parameter	Description
Sample Count	Set the number of scanned samples. 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. The sensitive data discovery task can use multiple threads. The more threads, the higher the scanning efficiency and the more device resources.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description
Select Schemas	Select the database schema to be encrypted. 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. 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. Then, the system scans the data types set in the template. The system has built-in common industry templates. You can also customize industry templates. For details, see **Adding an Industry Template**. 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. 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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.6.6.2 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.

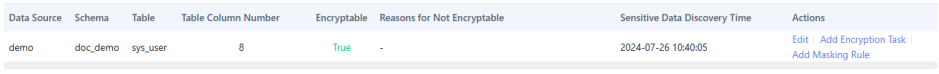
Step 4 Find the target data asset and click **View**.

Step 5 On the scan result page, view all scan results.

Table 4-16 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 4-65 Scan result

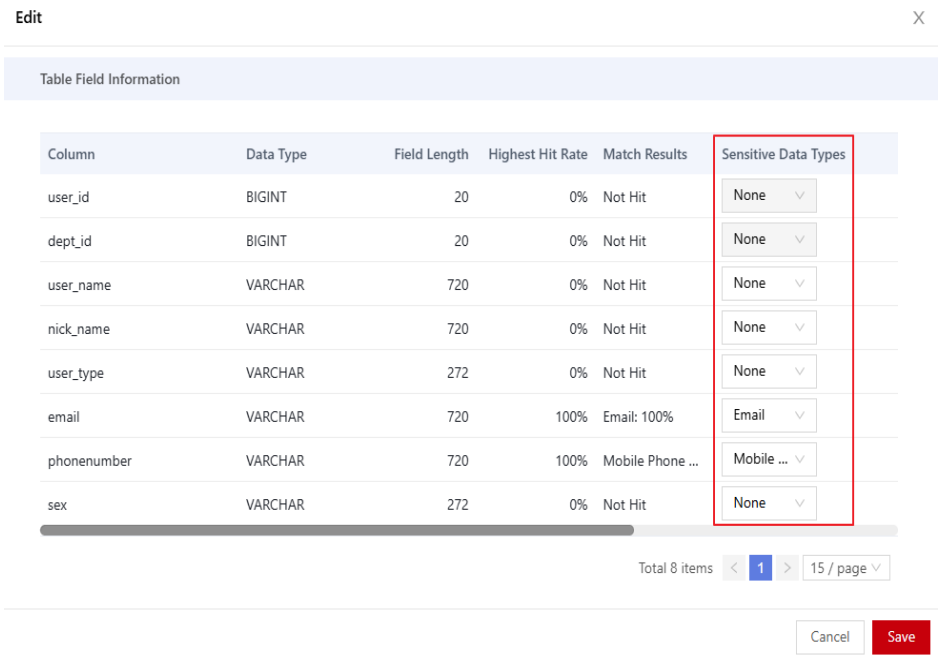


Step 6 For a database table, you can click **Edit** to view the table field information.

As shown in **Figure 4-66**, 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-66 Editing table field information



----End

4.6.6.3 Creating an Encryption Task in the Result

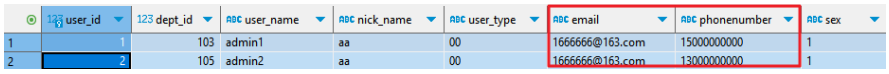
You can create an encryption task based on the sensitive data discovery result. This section describes how to create an encryption task in the result.

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 4-67**.

Figure 4-67 Querying the result before encryption



Prerequisites

Before creating an encryption 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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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**.

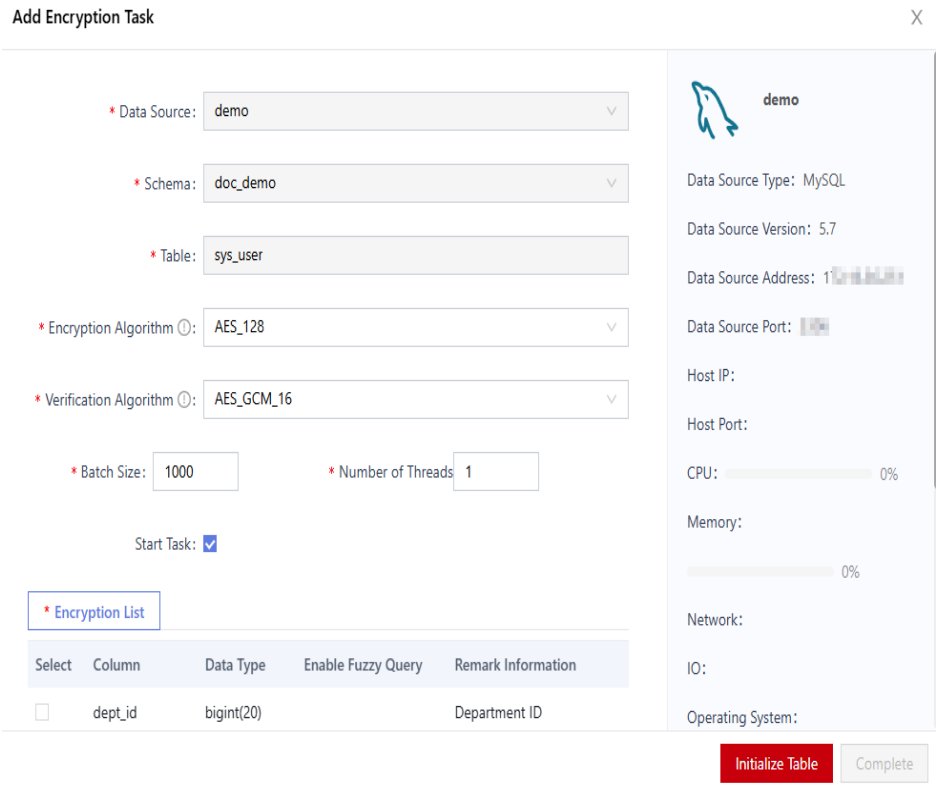
Step 5 In the displayed dialog box, set encryption information. **Table 4-17** describes the configuration information.

Table 4-17 Adding an encryption 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. 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. 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-68 Adding an encryption task

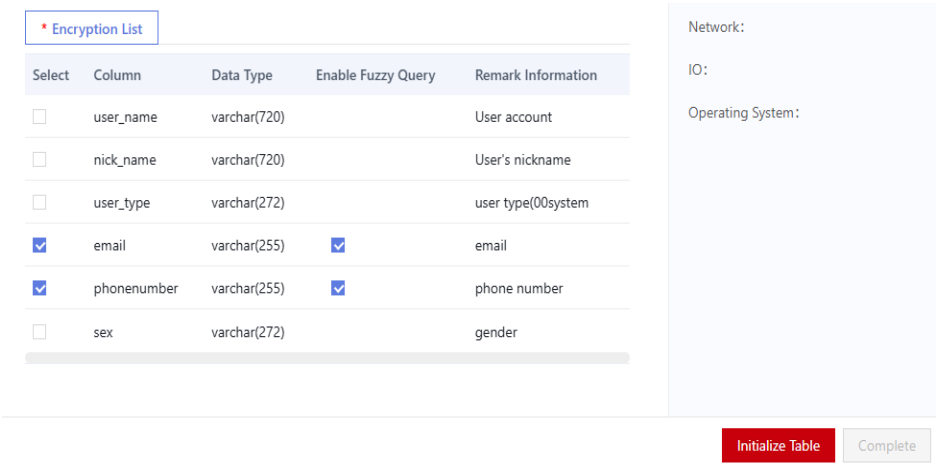


Step 6 Click the **Encryption List** tab, select columns to be encrypted, and set whether to enable fuzzy search.

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 4-69 Selecting columns to be encrypted



Step 7 Click **Initialize Table** to initialize the data table.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 8 Click **Complete**.

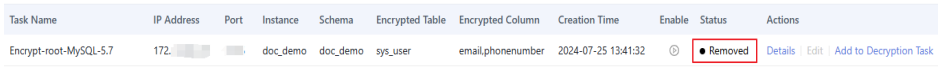
----End

Upgrade Verification

Step 1 After the encryption task is created, choose **Data Encryption** > **Encryption Task Management** to view and manage the new task.

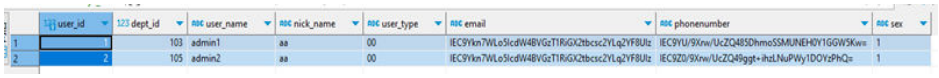
Step 2 The encryption task is automatically removed after inventory data is encrypted. In this case, the task is removed, but the system continues to encrypt data.

Figure 4-70 Full encryption mode



Step 3 Query the database table again. The query result is encrypted data, as shown in **Figure 4-71**.

Figure 4-71 Encrypted data



----End

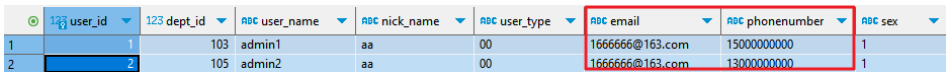
4.6.6.4 Creating a Masking Rule in the Result

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 4-72**.

Figure 4-72 Querying the result before masking



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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

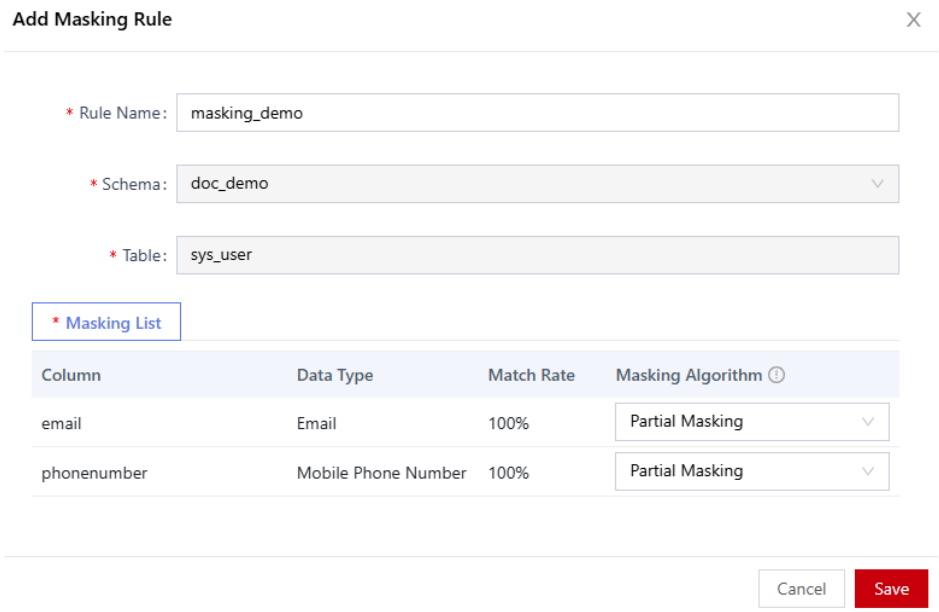
You can also click **Add Desensitization Rules in Batch** on the scan result list page to generate masking rules in batches based on the industry template used for scanning sensitive data. For details about how to configure an industry template, see **Adding an Industry Template**.

Step 5 In the **Add Masking Rule** dialog box, set masking information, as shown in **Table 4-18**.

Table 4-18 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 4-73 Adding a masking rule



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 4-74**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-74 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

4.6.6.5 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**.

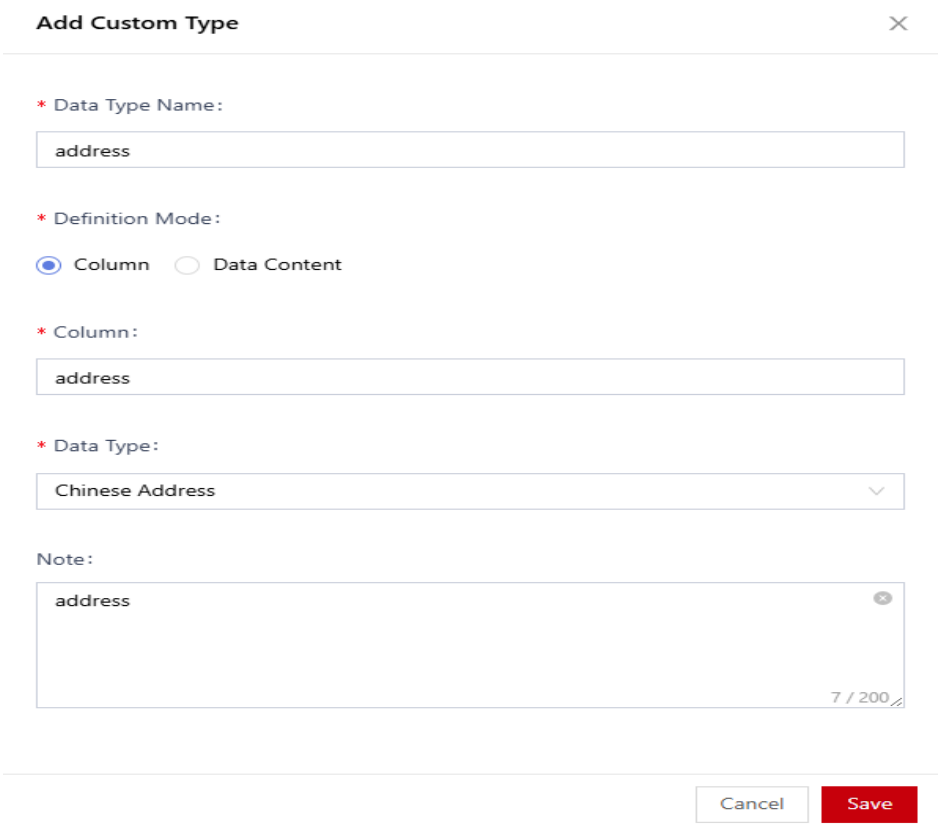
Step 3 On the **Data Type List** page, click **Add Custom Type** in the upper right corner.

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 4-75 Matching column



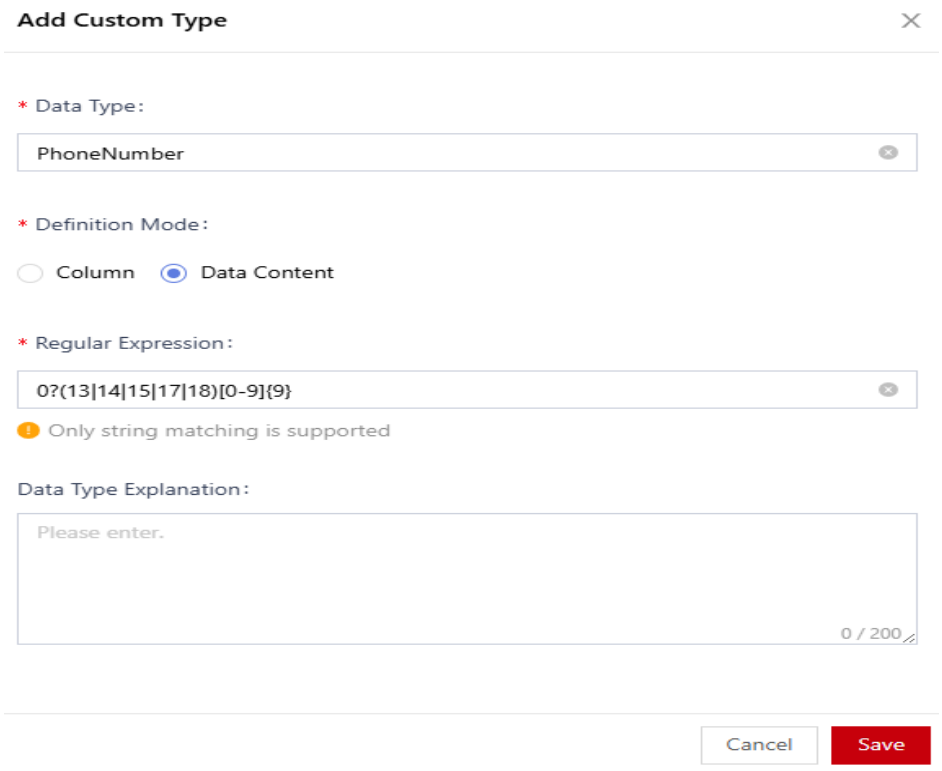
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-19 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. 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. 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 4-76 Matching data content



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-20 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. For example, the regular expression of a mobile number is as follows: 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 4-77 Custom data type

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.

4.6.6.6 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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 4-21**.

Figure 4-78 Adding a template

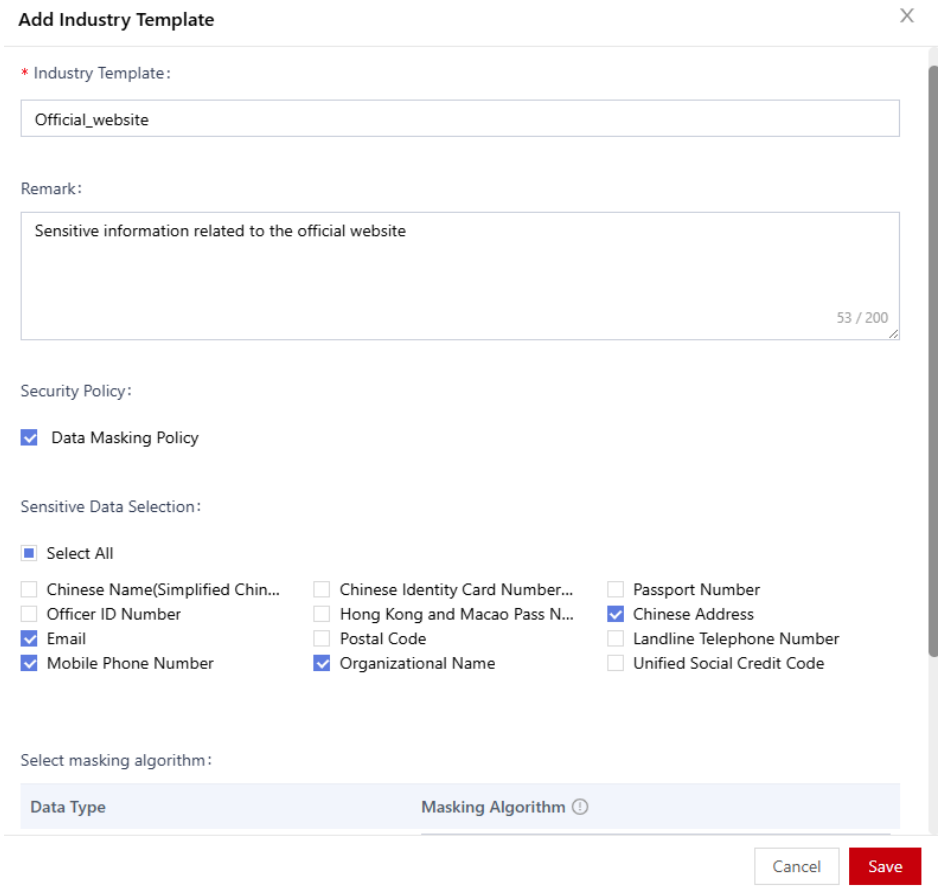


Table 4-21 Parameters for configuring a template

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description
Sensitive Data Selection	Type of sensitive data contained in a template. The options are as follows: • **Select All**: Select all data types, including built-in data types and customized data types. • Built-in data type: built-in data type of the system. • User-defined data type: Data types manually created by users.
Select Masking Algorithm	Configure a masking algorithm for the selected sensitive data. 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.

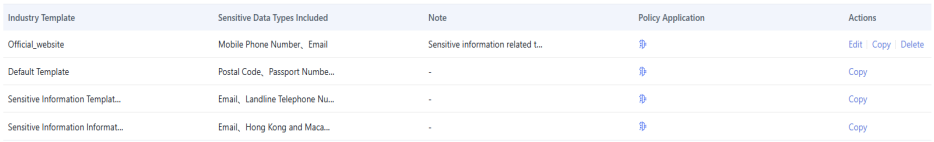
Step 5 Click **Save** to add an industry template.

----End

Related Operations

- After the template is created, you can view the new industry template on the **Template List** page.

  Figure 4-79 Adding template successfully

- Table 4-22 shows the template management operations.

  Table 4-22 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.

4.6.7 Data Encryption and Decryption

4.6.7.1 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 4-80**.

Figure 4-80 Example of ciphertext in hexadecimal mode

user_id	dept_id	user_name	nick_name	user_type	email	phonenumber	sex
1	103	000072C522716F38D943		00	000061D80F293773D3B1C40617494D	00002294772039 78C5EA93531	
2	105	000061D8CEFB2B292E4B		00	000061D80F69706E9EBDC62E9622BB	00002294792E3776CBE49D501	

----End

4.6.7.2 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

4.6.7.3 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 4-23**.

Figure 4-81 Adding an encryption test

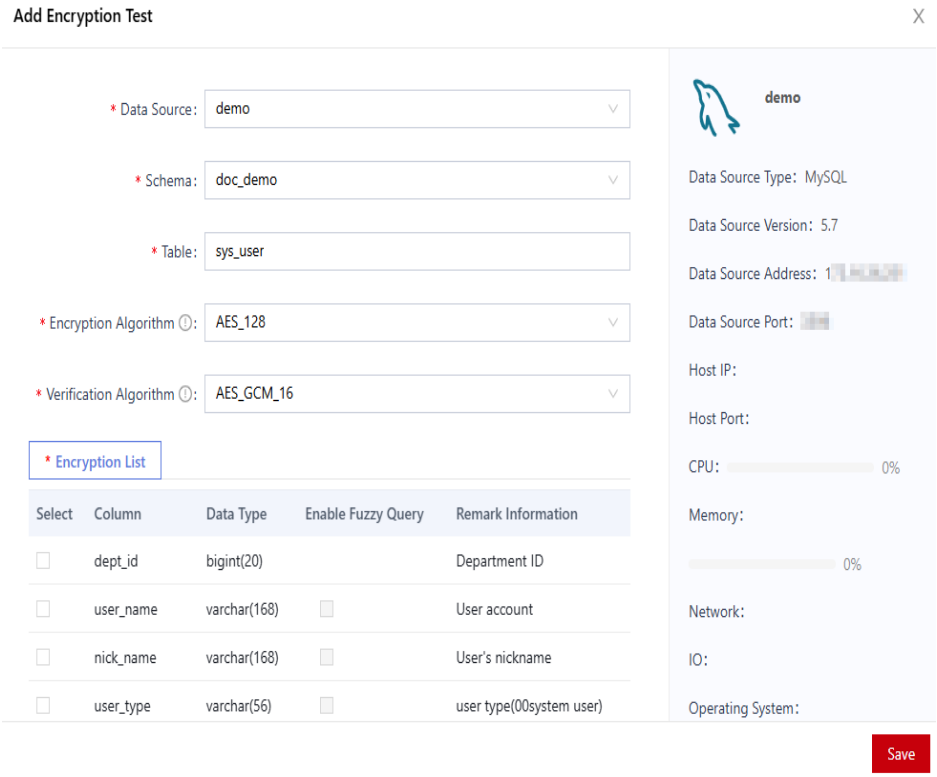


Table 4-23 Simulation test

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. 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. 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

4.6.7.4 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 Encryption 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 4-24**.

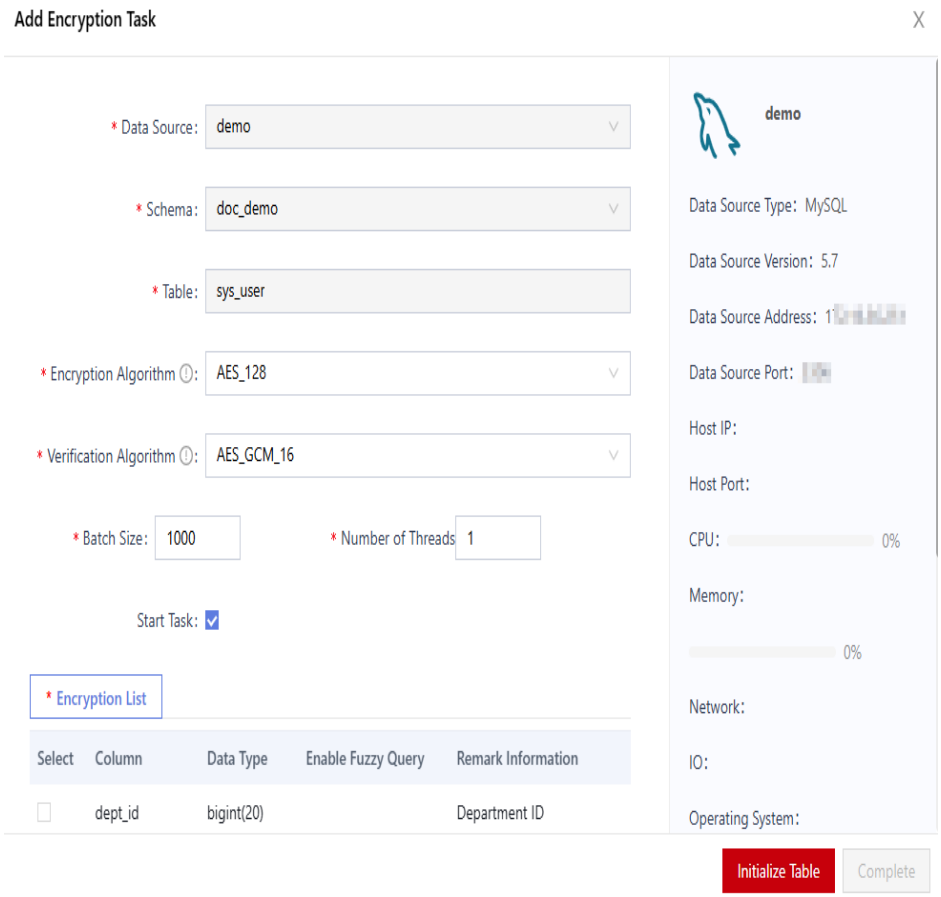
Table 4-24 Adding an encrypted task

Parameter	Description
Data Source Name	Name of an asset.
Schema	Name of the schema of the asset.
Table	Table name of an asset.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description
Encryption Algorithm	Select an encryption algorithm from the drop-down list box. 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. 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.

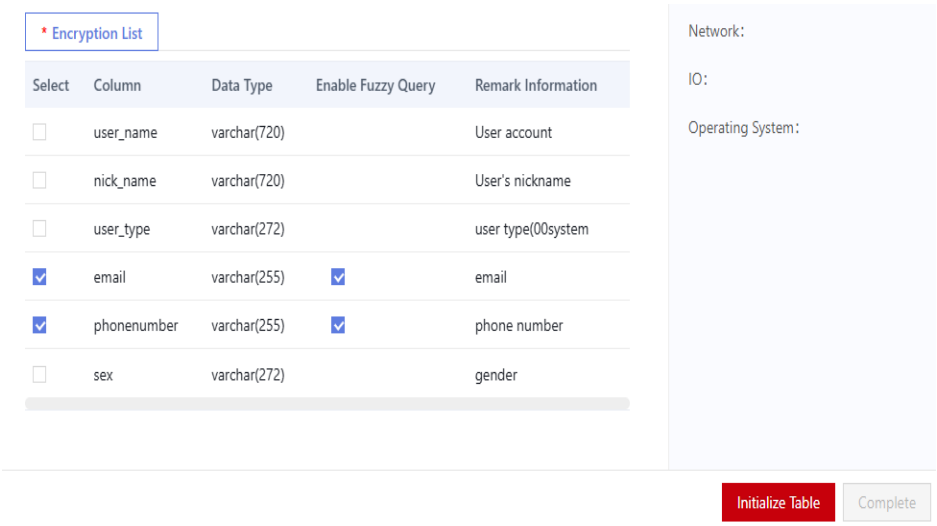
Figure 4-82 Adding an encrypted task



Step 5 Click the **Encryption List** tab, select columns to be encrypted, and set whether to enable fuzzy search.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-83 Selecting encrypted column



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.

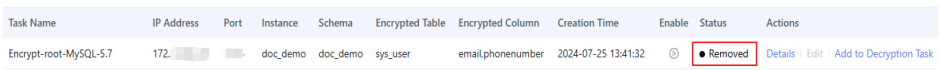
If the encryption is interrupted, you can click to continue the encryption.

----End

Operation Result

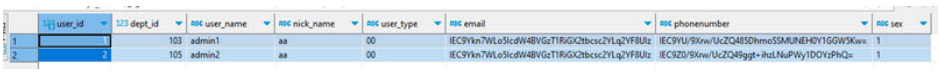
- After the encryption task is created, you can view and manage it in the list. The encryption task is automatically removed after inventory data is encrypted. In this case, the task is in the **Removed** state, but the system continues to encrypt data.

  Figure 4-84 Encryption task



- After the encryption is complete, only encrypted data can be queried by unauthorized users.

  Figure 4-85 Encrypted data



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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**.

4.6.7.5 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 4-25 Configuration example description

Parameter	Example Value
Client Authorization	IP address range: • 192.168.0.100~192.168.0.120 • 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**.

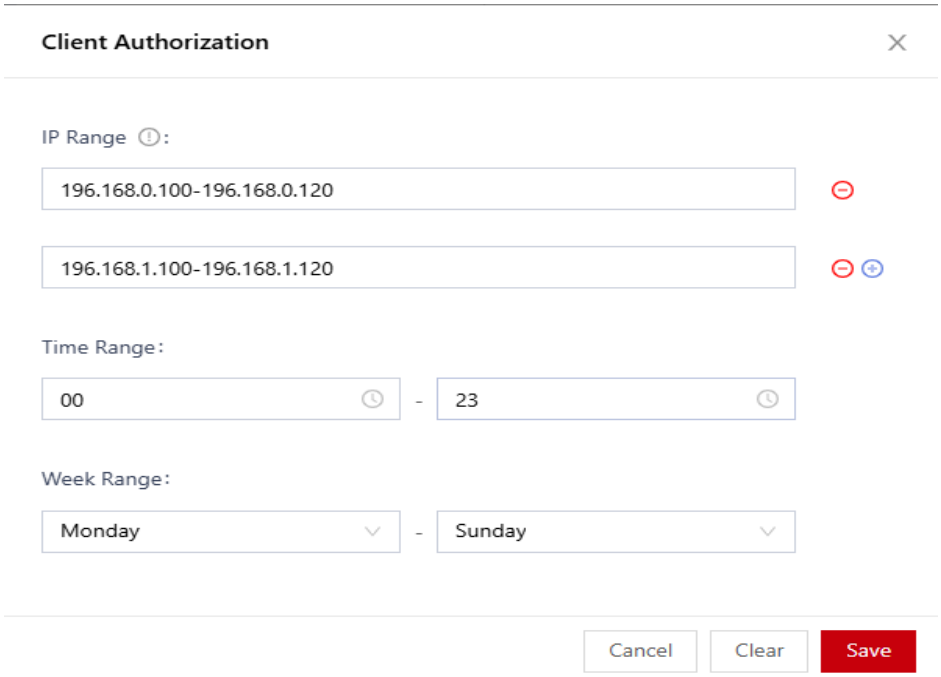
Step 3 In the data source list, click a data source.

Step 4 Locate the target encrypted database table and click **Client Authorization**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

Figure 4-86 Client authorization



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**.

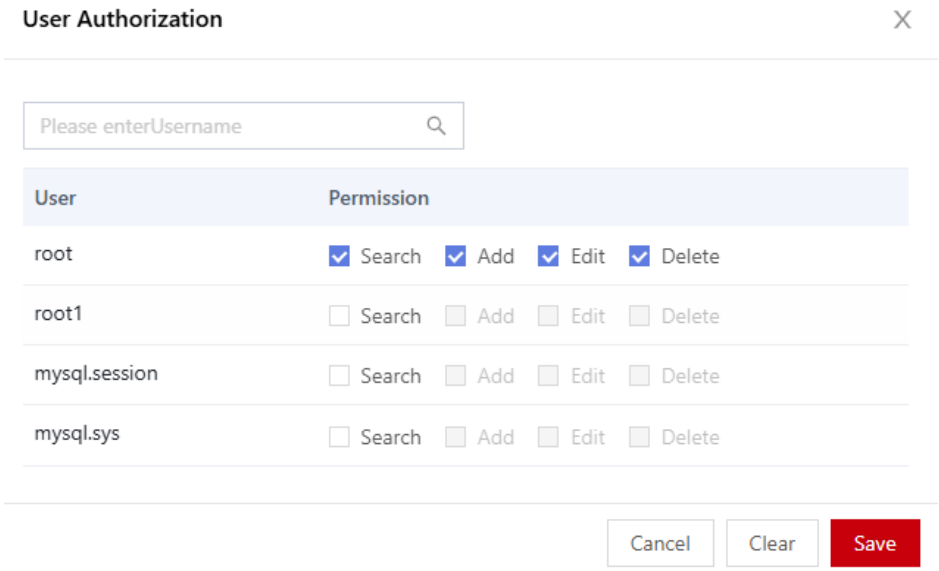
Step 3 In the data source list, click a data source.

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-87 User authorization



Step 6 Click **Save**.

----End

4.6.7.6 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.

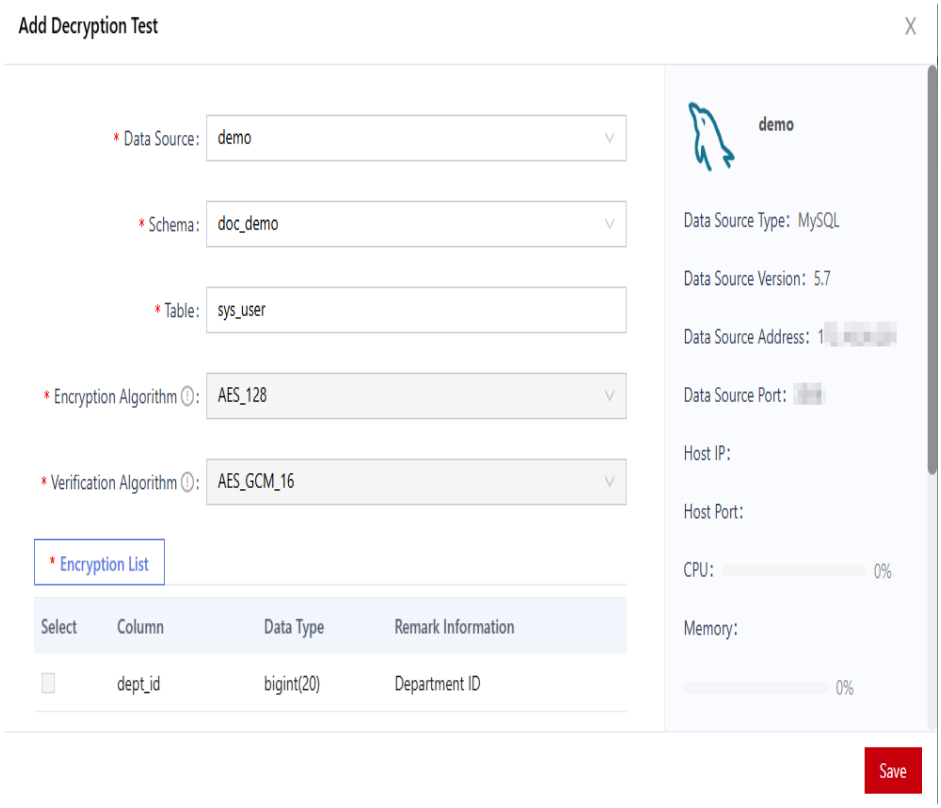
Step 2 In the navigation tree, choose **Service Test** > **Simulation Test**.

Step 3 Click **Add Decryption Test**.

Step 4 In the displayed dialog box, configure the test target.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-88 Adding a decryption test



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

4.6.7.7 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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Procedure

Step 1 **Log in to a database encryption and access control instance** as the **sysadmin** user.

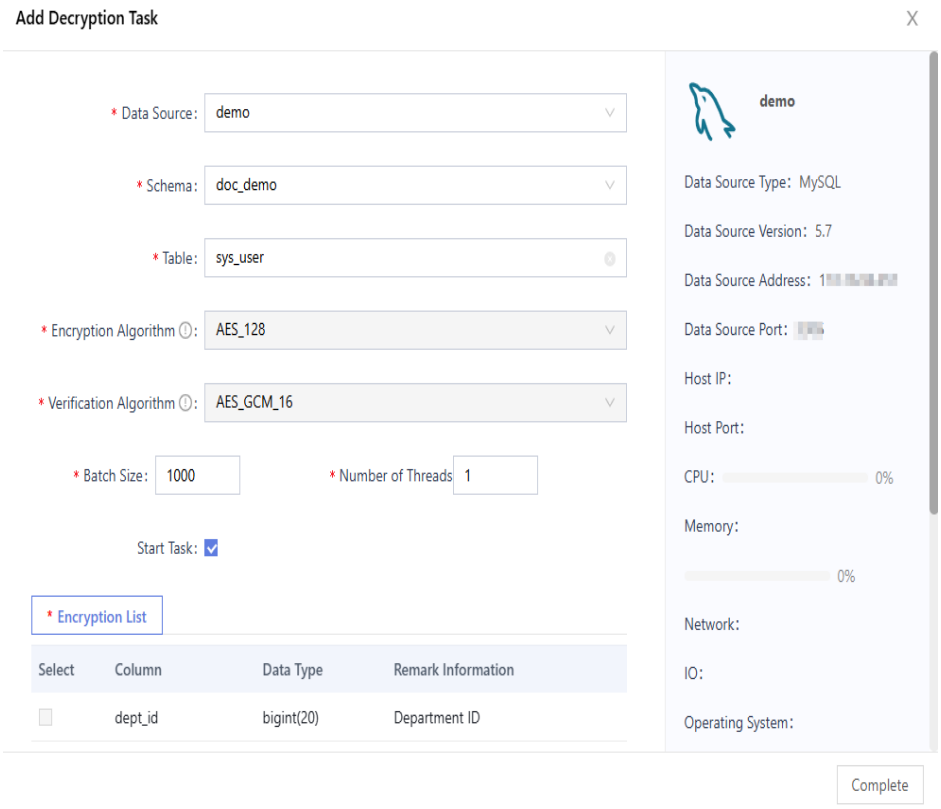
Step 2 In the navigation tree on the left, choose **Data Encryption** > **Decryption Task Management**.

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 4-89 Adding a decrypted task



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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.6.7.8 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**.

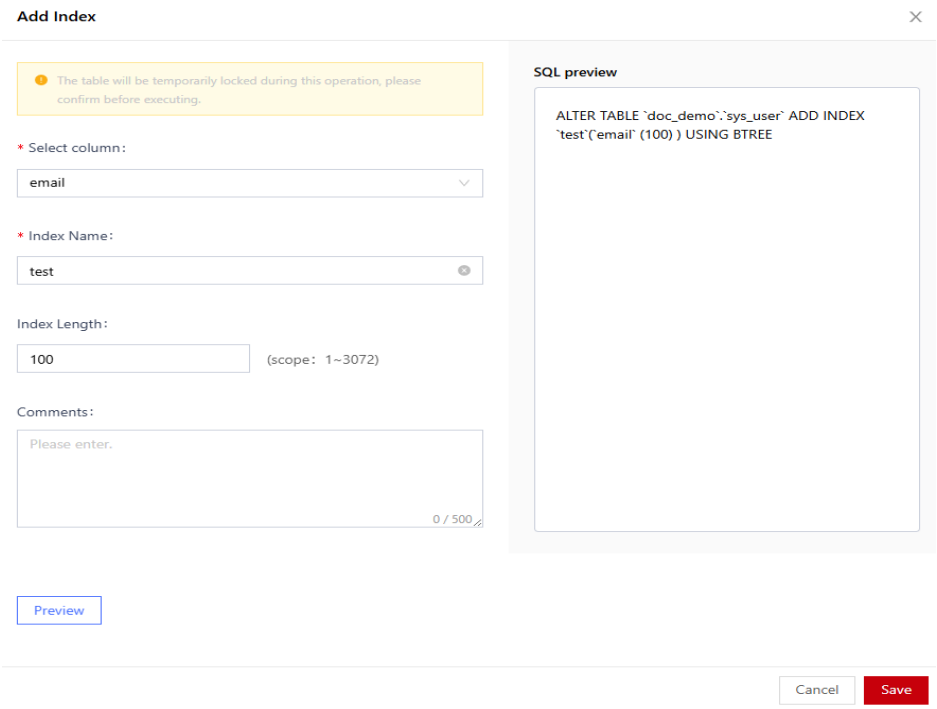
Step 4 In the list, view the list of encrypted tables. You can search for the target encrypted table by schema and table name.

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 4-90 Adding an index



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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**.

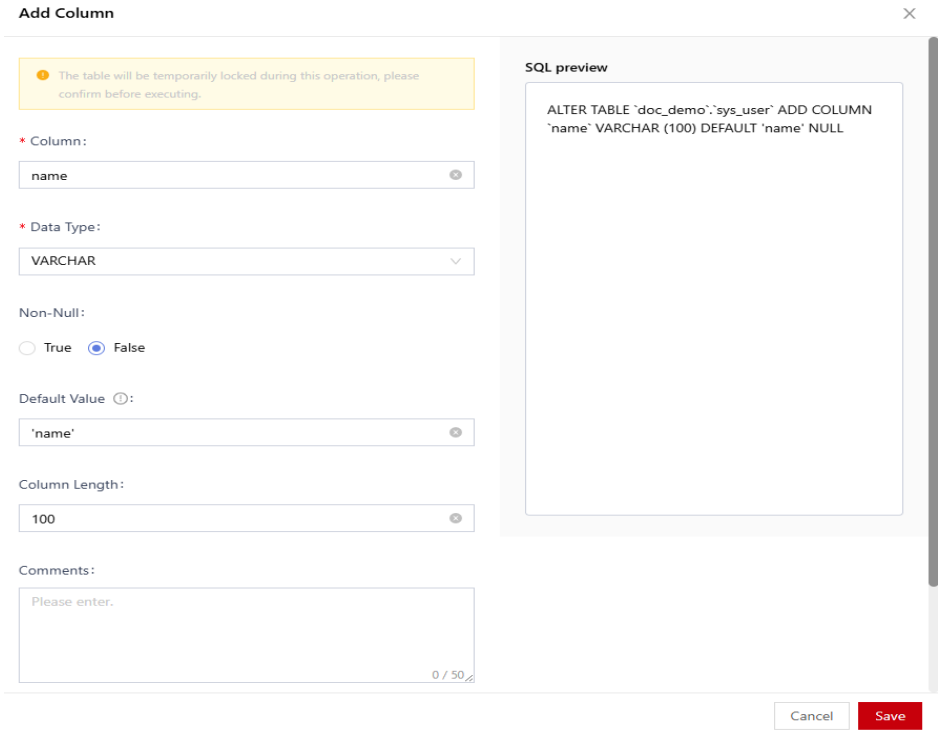
Step 7 In the **Add Column** dialog box, configure column parameters, including the **Column**, **Data Type**, **Non-Null**, **Default Value**, and **Column Length**. Click **Preview** to view the SQL statement for adding a column.

NOTE

The default value cannot contain single or double quotation marks.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-91 Adding a column



Step 8 Click **Save**.

----End

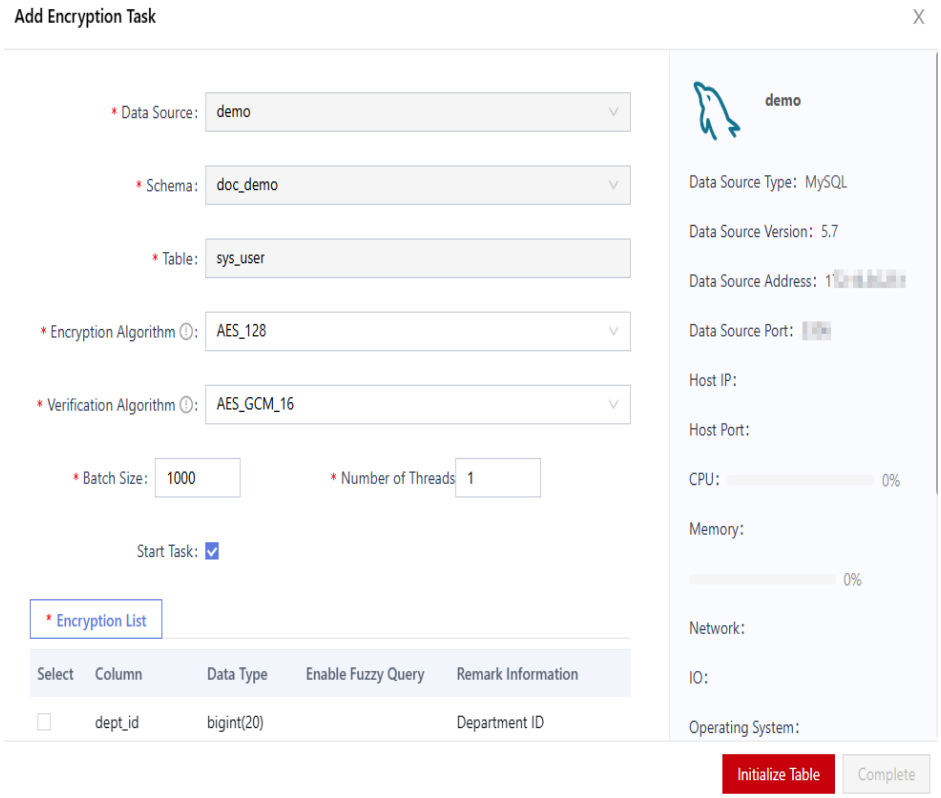
4.6.7.9 Rolling Back the Table Structure

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-92 Initializing a table



Procedure

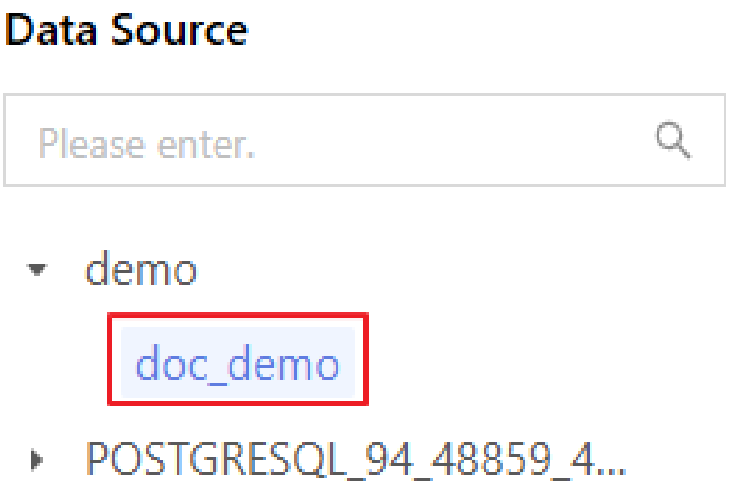
Step 1 Log in to a database encryption and access control instance as the **sysadmin** user.

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 4-93.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-93 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

4.6.7.10 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- 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.

4.6.7.11 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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.6.8 Dynamic Data Masking

4.6.8.1 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

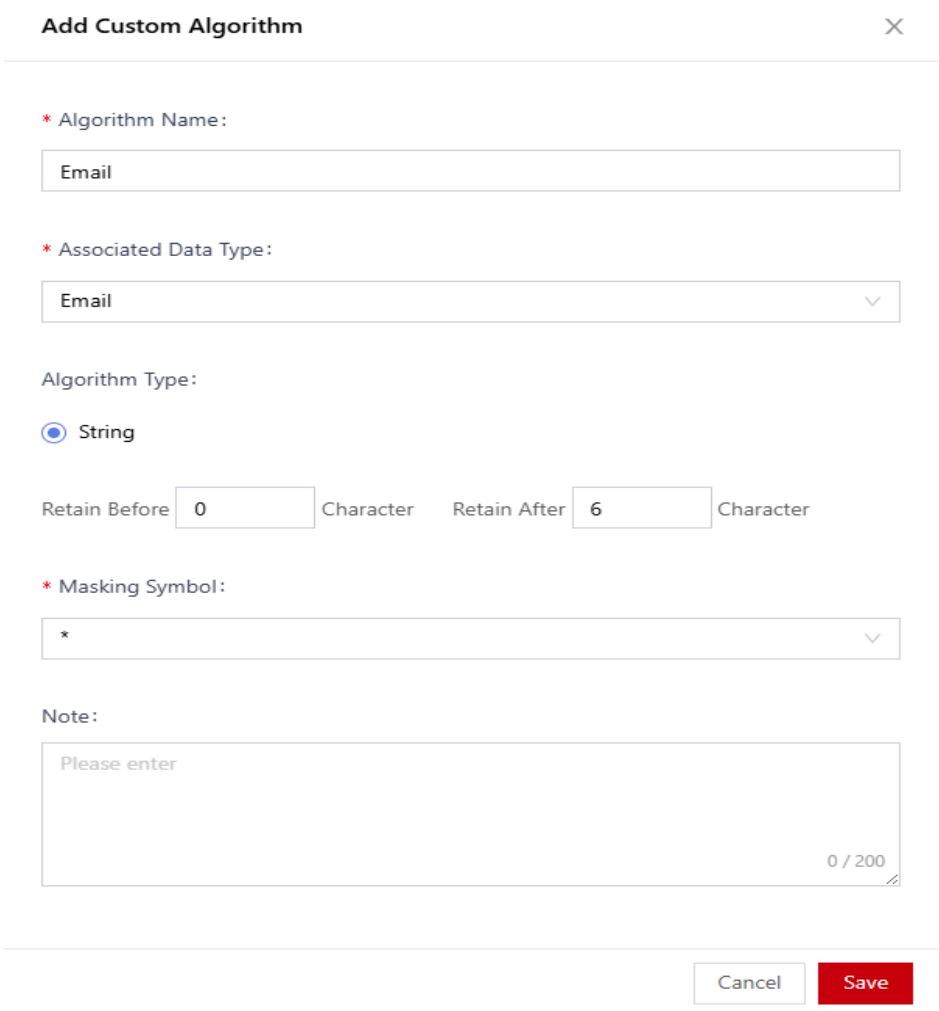
Step 1 Log in to a database encryption and access control instance as the **sysadmin** user.

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 4-94 Adding a custom algorithm



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-26 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 4-95 Custom masking algorithm

----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.

4.6.8.2 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:

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- 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.

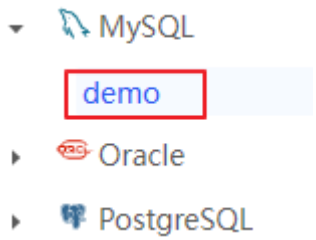
Procedure

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 4-96 Selecting a data source



Step 4 On the masking rule list page of the target data source, click **Add Custom Rule**.

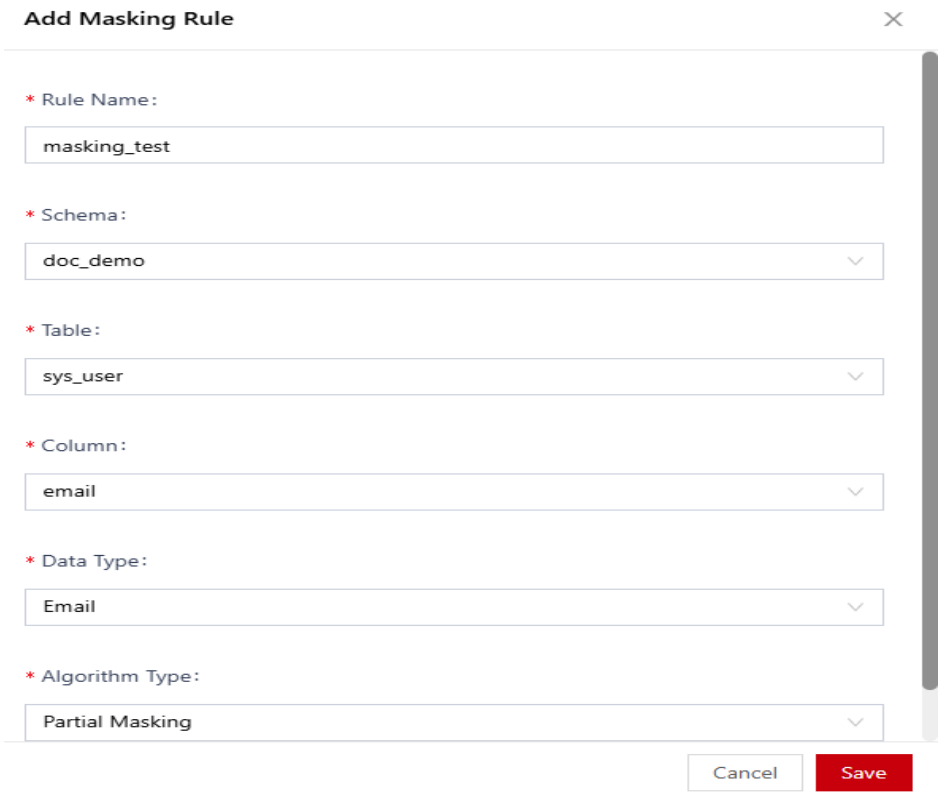
Step 5 In the displayed **Add Masking Rule** dialog box, configure the parameters. **Table 4-27** lists the parameters.

Table 4-27 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. For details about supported algorithm types, see **Checking the Encryption Algorithm**.
Data Type	Select the data type of the selected column. 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. You can add a custom masking rule. For details, see **Adding a Custom Masking Algorithm**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-97 Adding a masking rule



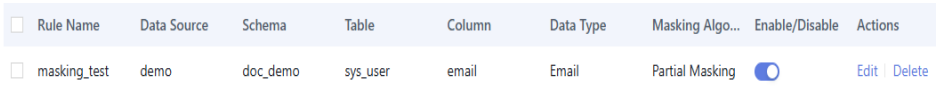
Step 6 Click **Save**.

----End

Operation Result

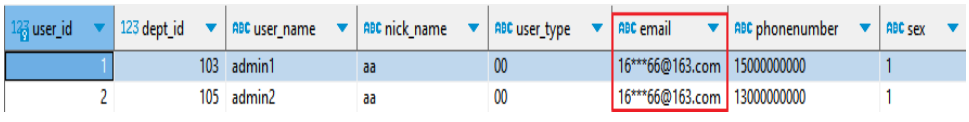
- You can view and manage the created masking rule in the masking rule list. The created masking rule is enabled automatically.

  Figure 4-98 Masking rule

- After the data is masked, users who are not in the whitelist can view only masked data when querying the plaintext data.

  Figure 4-99 Masked data

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- 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.

4.6.8.3 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.

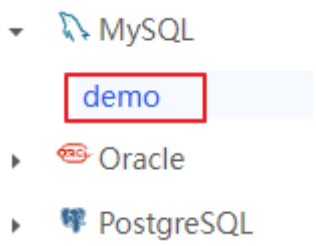
Procedure

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 4-100 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 4-28 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.

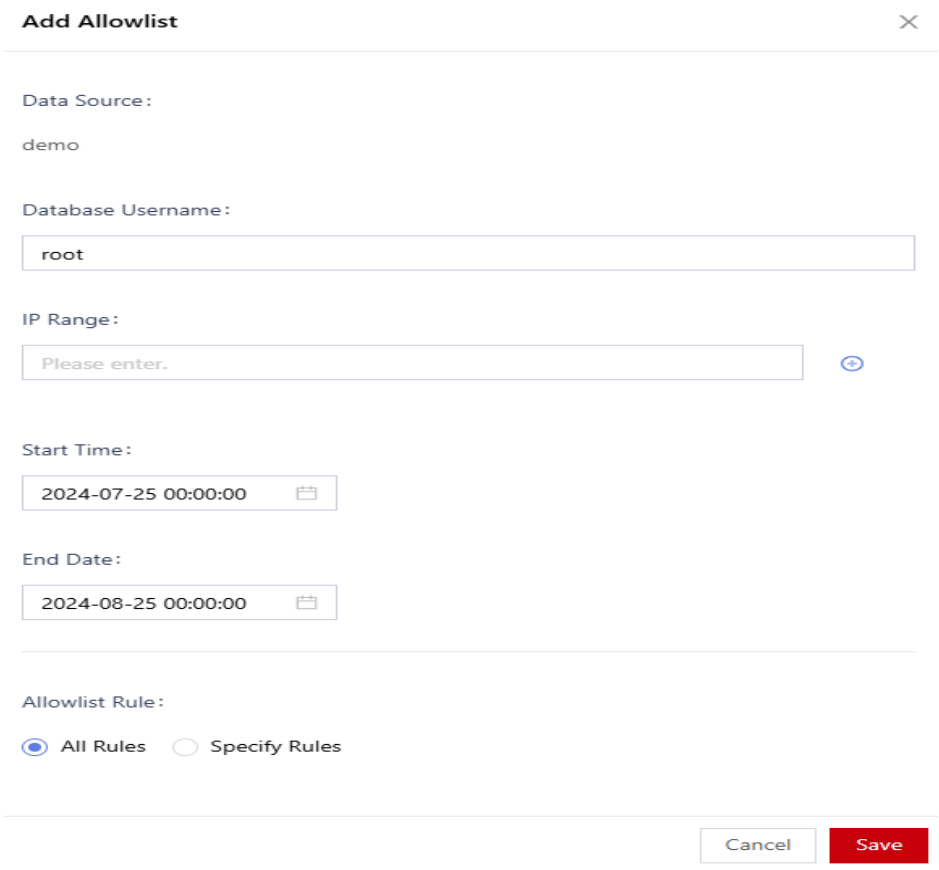
Table 4-28 Adding an allowlist

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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. • **Specify Rules**: Only specified rules are added to the allowlist.

Figure 4-101 Adding an allowlist



Step 7 Click **Save**.

----End

4.6.9 Key Management

4.6.9.1 Updating a Data Source Key

You can manually or periodically update a data source key (DSK) to ensure service security.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Prerequisites

The key has been initialized. For details, see **Initializing a Key**.

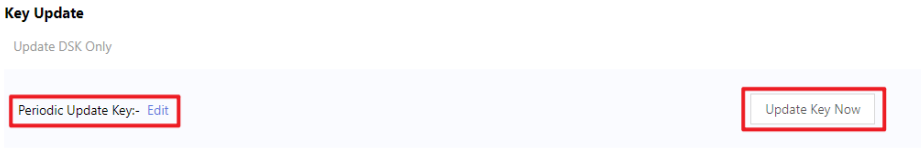
Procedure

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 4-102 Key update



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 4-29** describes the parameters.

Table 4-29 Configuring key update cycle

Parameter	Description
Update Cycle	Key update period. The options are as follows: – **None**: No periodic updates are performed. – **Daily**: The data is updated once a day. – **Weekly**: The data is updated once a week. – **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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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**.

4.6.9.2 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**.

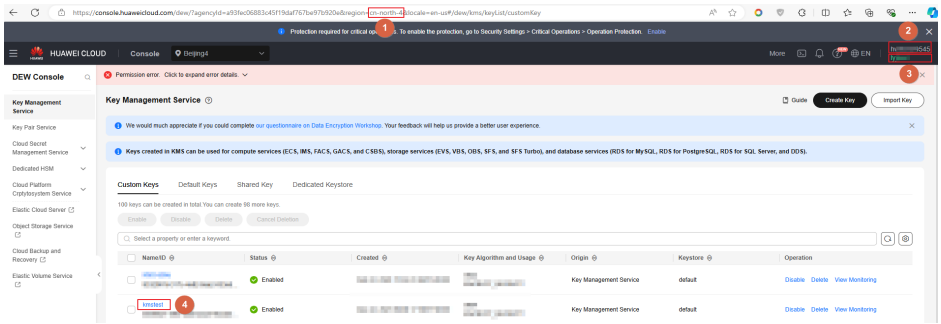
Step 3 Click the **Huawei Cloud** tab.

Step 4 Configure the parameters for interconnecting with KMS. For details, see **Table 4-30**.

Table 4-30 Parameters

Parameter	Description
Region	Region of Huawei Cloud. You can obtain it from the URL of the KMS console, as shown in **Figure 4-103**.
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 4-103 KMS console parameters



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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**.

4.6.9.3 Viewing Key Details

The system records information such as the ID and type of the created key.

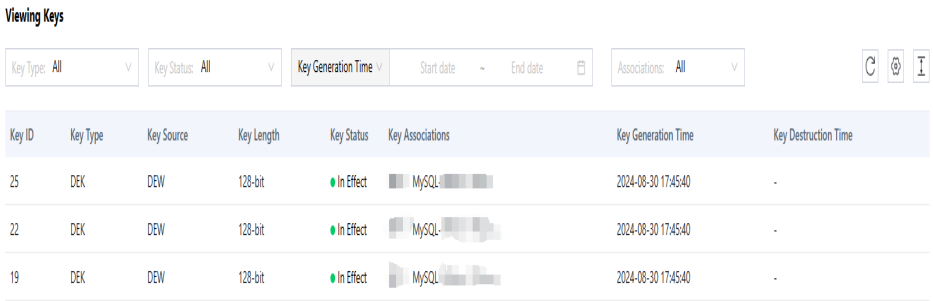
Procedure

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 4-104 Viewing key details



----End

4.6.10 System Management

4.6.10.1 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 4-31** describes the parameters.

Figure 4-105 Creating an account

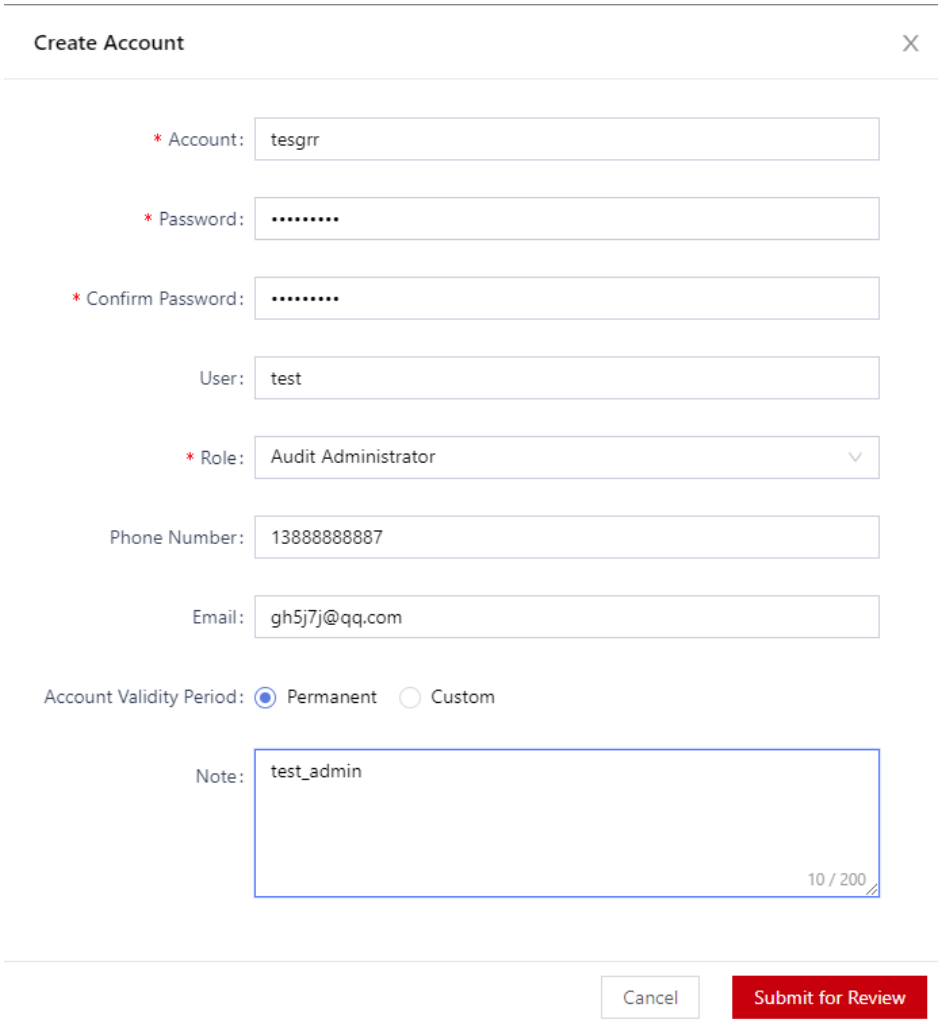


Table 4-31 Creating an account

Parameter	Description
Account	Enter the username.
Password/ Confirm Password	Set and confirm the password. Change the password upon the first login and periodically update the password to avoid information breach.
User	Set the user.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description
Role	Select a role from the drop-down list. • Security Administrator • Audit Administrator • System Administrator
Phone Number	Enter the phone number.
Email	Enter the email address.
Account Validity Period	Select a validity period. • **Permanent**: The account is permanently valid. • **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**. • 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 4-32 Management operations

Operation	Description
Clicking **Edit**	Edit the account information.
Clicking **Delete**	Delete accounts that are no longer used.
Clicking **Enable**	Enable an account.
Clicking **Disable**	Disable an account. After the account is disabled, it cannot be used to log in to the system.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Operation	Description
Clicking **Reset Password**	Set password, which must meet the password requirements.

4.6.10.2 Organization Management

You can manage the organization and the members in it on the **Organization Management** page.

4.6.10.2.1 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 4-106 Parameters for adding an organization

Table 4-33 Parameters for adding an organization

Parameter	Description
Organization Name	Set the organization name.
Organization ID	Set the internal code.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description
Parent Organization	Choose the parent department from the drop-down list. If this parameter is not configured, the created organization is the level-1 department by default.

Step 5 Click **Confirm**.

----End

4.6.10.2.2 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

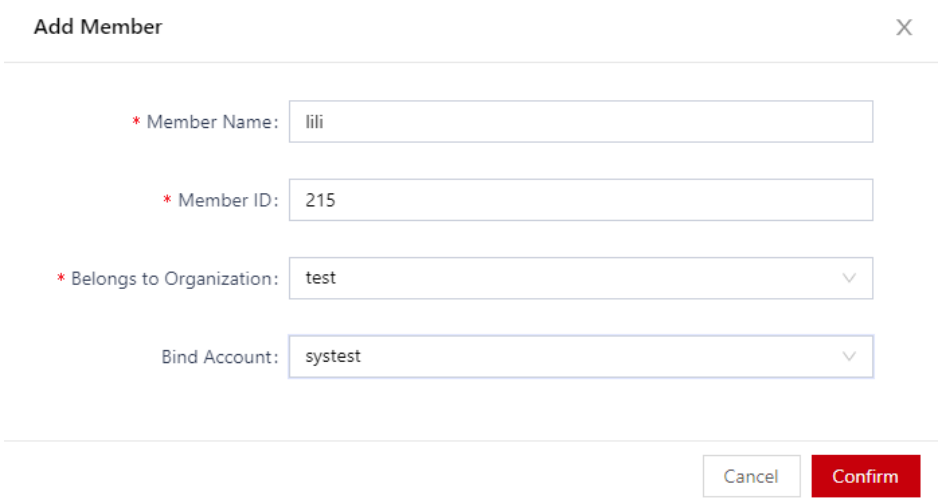
Step 1 **Log in to a database encryption and access control instance** as the **sysadmin** user.

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 4-107 Parameters for adding a member



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Table 4-34 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. 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 4-35 Management operations

Operation	Description
Click **Edit**.	Edit member details.
Click **Delete**.	Delete members that do not need to be managed.

4.6.10.3 System O&M

4.6.10.3.1 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 4-108 Basic device indicator monitoring

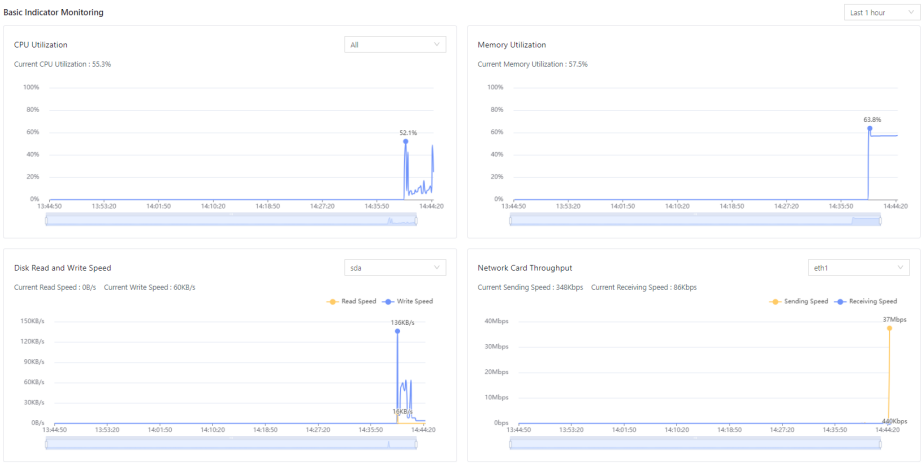


Table 4-36 Parameter descriptions

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.6.10.3.2 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

4.6.10.3.3 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.

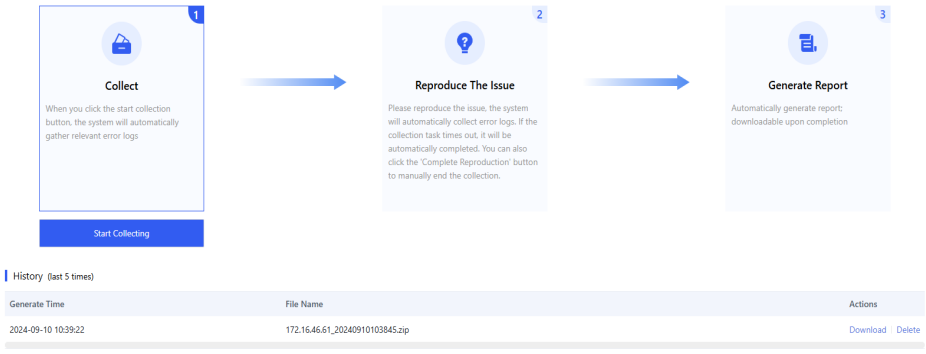
Step 2 In the navigation pane, choose **System Management** > **System O&M**. Click **System Diagnostics** > **One-click Collect**.

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 4-109 Log collection



----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.6.10.3.4 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 4-110 Setting automatic cleanup

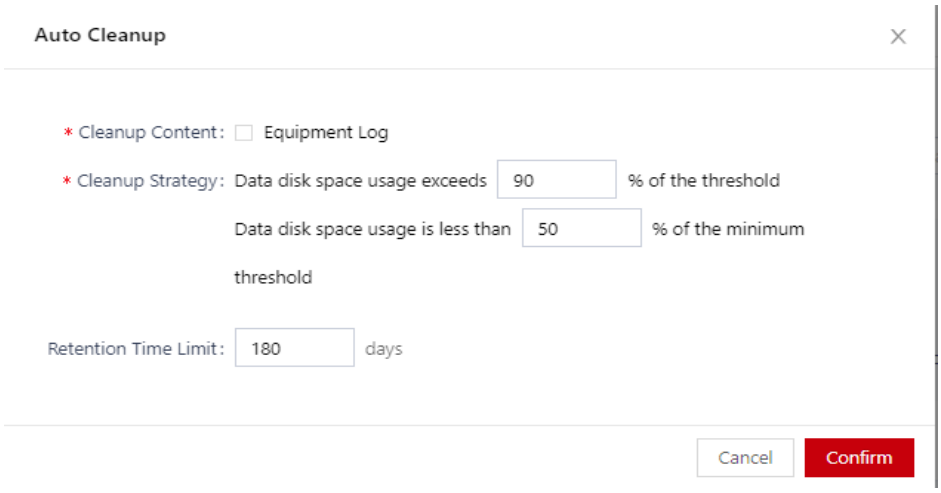


Table 4-37 Parameter description

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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

4.6.10.4 View Message Notifications

On the **Message Center** page, you can view system notifications and alarms, configure the message type, template, and recipient roles.

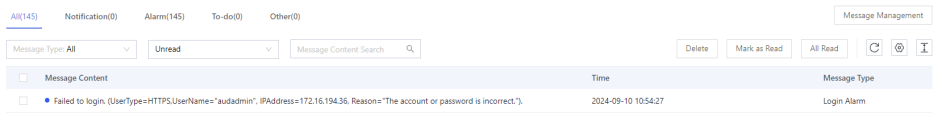
Procedure

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 4-111 Message center



----End

4.6.10.5 System Settings

4.6.10.5.1 General Settings

You can switch the default system language between Chinese and English on the **General Settings** page.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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.

----End

4.6.10.5.2 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

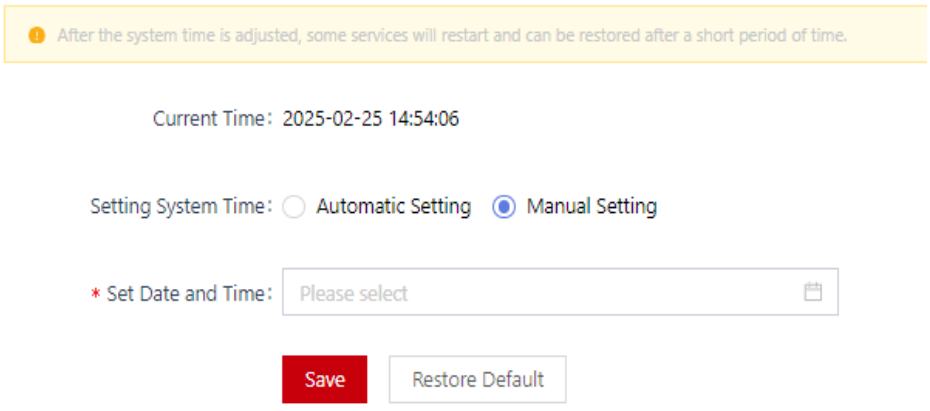
Step 1 Log in to a database encryption and access control instance as the **sysadmin** user.

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 4-112 Manually changing the system time

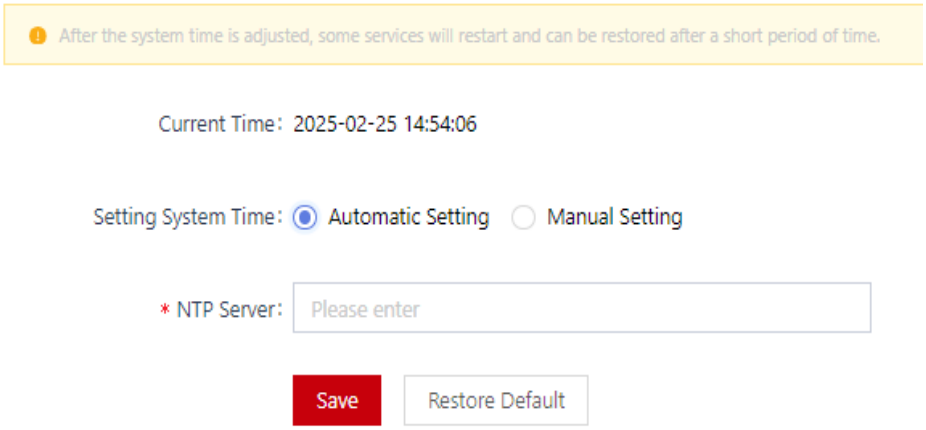


1. Click the drop-down list box of **Set Date and Time**. In the dialog box that is displayed, select the date and time, and click **OK**.
2. Click **Save**. The message "Please restart the service after modifying the system time, otherwise some functions will not take effect." is displayed. Click **Confirm**. The system time is changed.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 5 To automatically set the system time, perform the following steps:

Figure 4-113 Automatically setting the system time



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

4.6.10.5.3 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

4.7 Security Administrator Operation Guide

4.7.1 System Management

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4.7.1.1 Viewing a Role

By default, the system creates roles such as the system administrator, audit administrator, and security administrator.

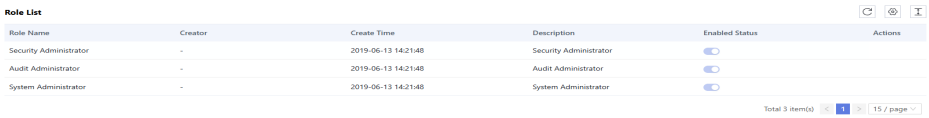
Procedure

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 4-114.

Figure 4-114 Viewing the roles



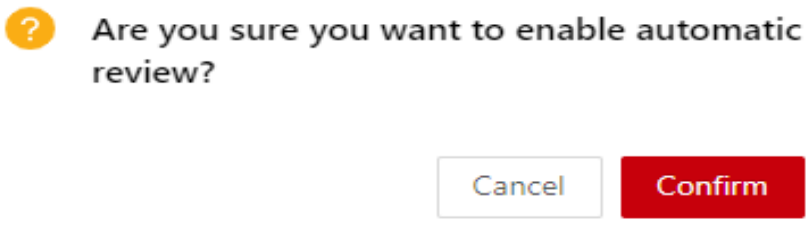
----End

4.7.1.2 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 4-115 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**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Step 3 Locate the target account and click **Approve**.

Step 4 Click **Confirm**.

----End

4.7.1.3 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 4-116 Platform login security settings

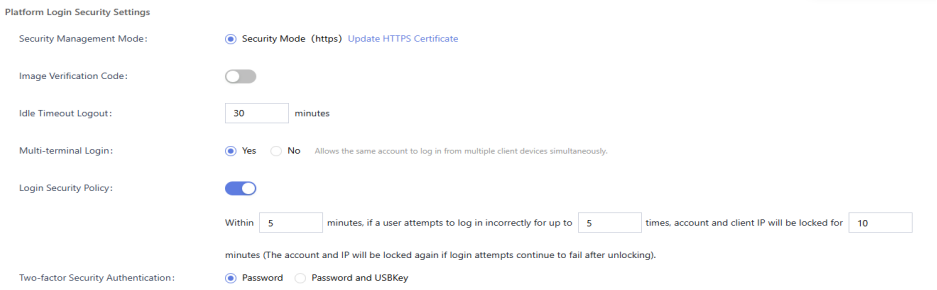


Table 4-38 Parameters of platform login security settings

Parameter	Description
Security Management Mode	HTTPS security mode is supported with updatable certificates.
Image Verification Code	• You can choose whether to enable this function. • 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. • **Yes**: An account can be logged in at different places. • **No**: An account cannot be logged in at different places.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description
Login Security Policy	• You can choose whether to enable this function to prevent brute-force attacks. • 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. • **Password**: Only password is required for login. • **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 4-117 Network access security settings

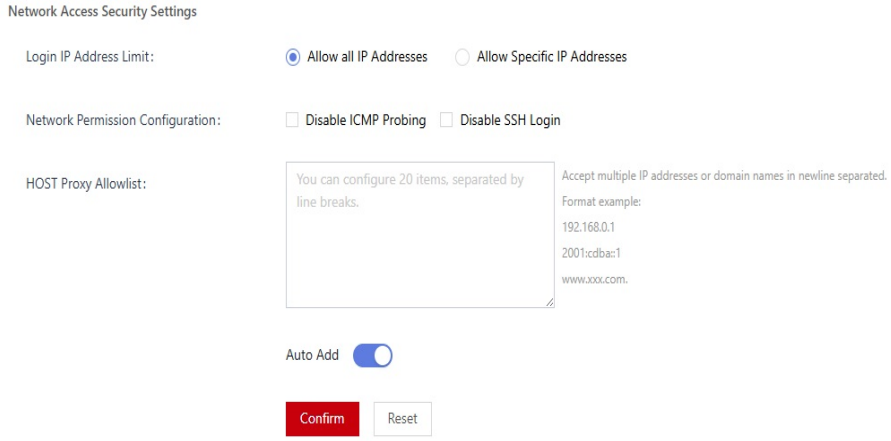


Table 4-39 Parameters of network access security settings

Parameter	Description
Login IP Address Limit	Whether to restrict the access source. • **Accept All IP Addresses**: All IP addresses can access the system. • **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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Parameter	Description
Network Permission Configuration	You choose whether to disable ICMP probing and SSH login. • **Disable ICMP Probing**: If you enable this function, other devices cannot ping the system. • **Disable SSH Login**: SSH login is disabled. **NOTE** 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

4.8 Operation Guide for Audit Administrators

4.8.1 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.

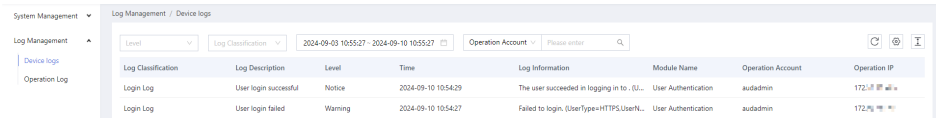
Procedure

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 4-118 Search settings



Step 4 View the logs in the list.

----End

4.8.2 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

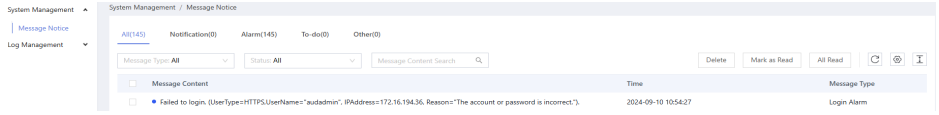
Procedure

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 4-119 Setting filter criteria



Step 4 View the logs in the list.

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5 Monitoring

5.1 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Metrics

Table 5-1 DBSS metrics

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Dimension	Monitored Object	Monitoring Interval (Raw Data)
cpu_util	CPU Usage	CPU consumed by the monitored object Unit: % Collection method: 100% minus idle CPU usage percentage	0 to 100% Value type: Float	%	N/A	audit_id	Database audit instance	1 minute
mem_util	Memory Usage	Memory usage of the monitored object Unit: % Collection method: 100% minus idle memory percentage	0 to 100% Value type: Float	%	N/A	audit_id	Database audit instance	1 minute
disk_util	Disk usage	Disk usage of the monitored object Unit: % Collection method: 100% minus idle disk space percentage	0 to 100% Value type: Float	%	N/A	audit_id	Database audit instance	1 minute

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Dimension	Monitored Object	Monitoring Interval (Raw Data)
hx_process_status	Protected Instance Process Status	The process status of a protected instance. **NOTE** This protected instance is no longer maintained.	0/1 • **0**: The process status is abnormal. • **1**: The process status is normal.	N/A	N/A	-	Database audit instance	1 minute

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Dimension	Monitored Object	Monitoring Interval (Raw Data)
hx_active_connections_num	Protected Instance Active Connections	The number of active connections of a protected instance. **NOTE** This protected instance is no longer maintained.	≥0	Count	N/A	-	Database audit instance	1 minute

Dimension

Key	Value
audit_id	Audit instance ID. You can obtain the value by referring to **Querying Audit Instances**.

5.2 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**.

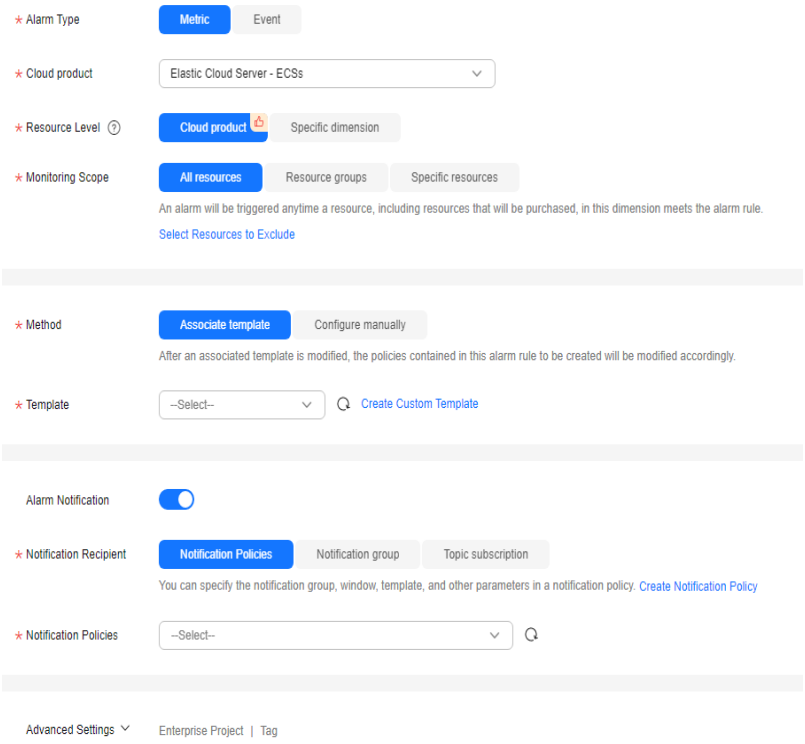
Step 5 Set the alarm rule name.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 5-1 Setting the alarm rule name

Step 6 Select **Metric** for **Alarm Type**, select **DBSS** from the **Cloud Product** drop-down list, and set the **Resource Level**, **Monitoring Scope**, **Method**, **Template**, **Alarm Notification**, **Notification Recipient**, and **Notification Policies**, as shown in **Figure 5-2**.

Figure 5-2 Configuring a DBSS alarm monitoring rule



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

----End

5.3 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.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Prerequisites

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

Procedures

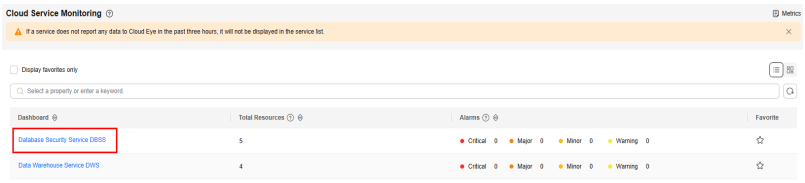
Step 1 **Log in to the management console.**

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**.

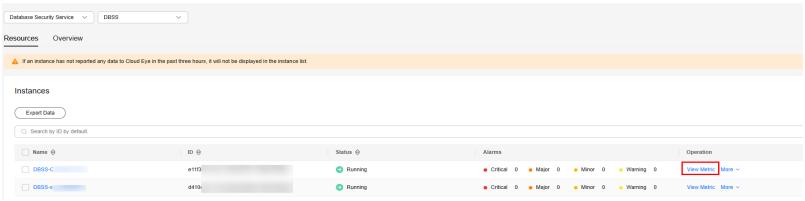
Step 4 Click the dashboard name **Database Security Service DBSS**.

Figure 5-3 Cloud service monitoring



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

Figure 5-4 Viewing monitoring metrics



----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

6 Sharing

6.1 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.**

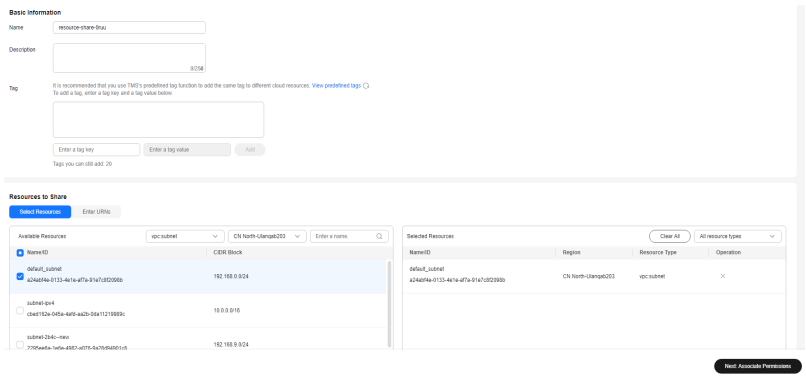
Step 2 Click ☰ in the upper left corner, choose **Management & Governance** > **Resource Access Manager**, and go to the resource access management page.

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**.

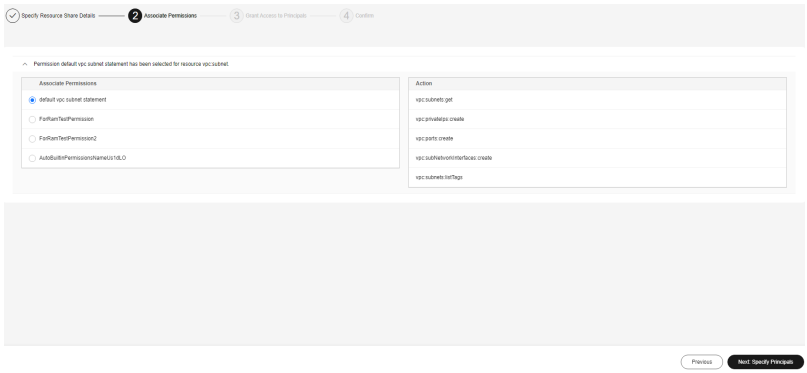
Figure 6-1 Specifying shared resources



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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 6-2 Configuring permissions



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

Figure 6-3 Specifying principals

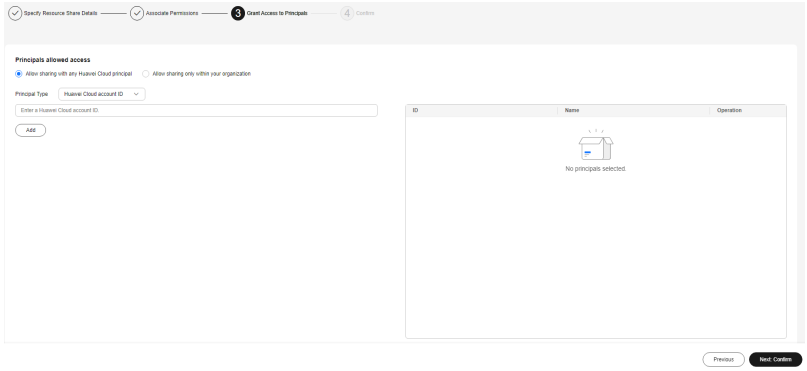


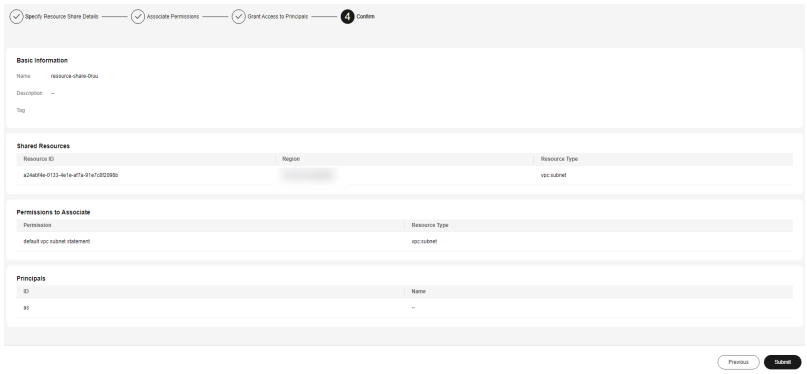
Table 6-1 Parameter descriptions

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

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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 6-4 Confirming configurations



----End

Using a VPC

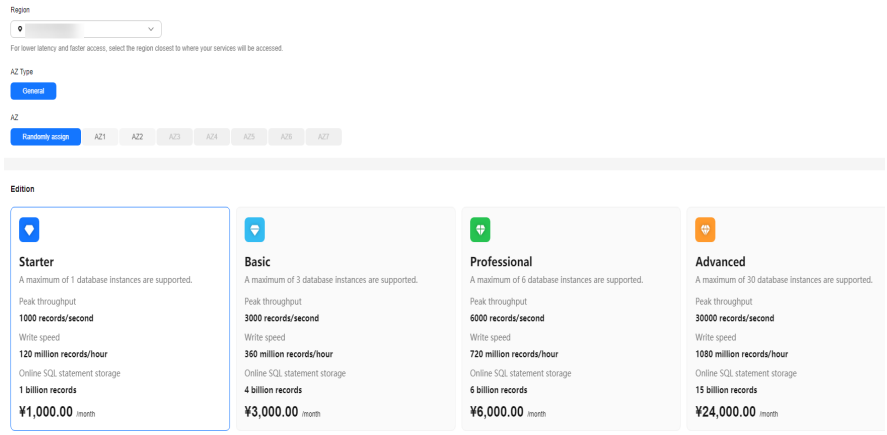
Step 1 **Log in to the management console.**

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 Select a region, an AZ type, an AZ, and an edition.

Figure 6-5 Selecting an AZ and an edition



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

Table 6-2 describes the database audit editions.

Table 6-2 DBSS editions

Edition	Maximum Databases	Performance
Professional	6	• Peak QPS: 6,000 queries/second • Database load rate: 7.2 million statements/hour • Online SQL statement storage: 600 million statements
Advanced	30	• Peak QPS: 30,000 queries/second • Database load rate: 10.8 million records/hour • Online SQL statement storage: 1.5 billion statements

NOTE

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

  The number of database instances equals the number of database ports. If a database IP address has N database ports, there are N database instances.

  Example: A user has two database IP addresses, IP_1 and IP_2. IP_1 has a database port. IP_2 has three database ports. IP_1 and IP_2 have four database instances in total. To audit all of them, select professional edition DBSS, which supports a maximum of six database instances.
- To change the edition of a DBSS instance, unsubscribe from it and purchase a new one.
- The table above lists the system resources consumed by a database audit instance. Ensure your system has the required configurations before purchasing database audit instances.
- Online SQL statements are counted based on the assumption that the capacity of an SQL statement is 1 KB.

Step 5 Select the VPC and subnet for database audit. For details about related parameters, see **Table 6-3**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 6-6 Setting database audit parameters

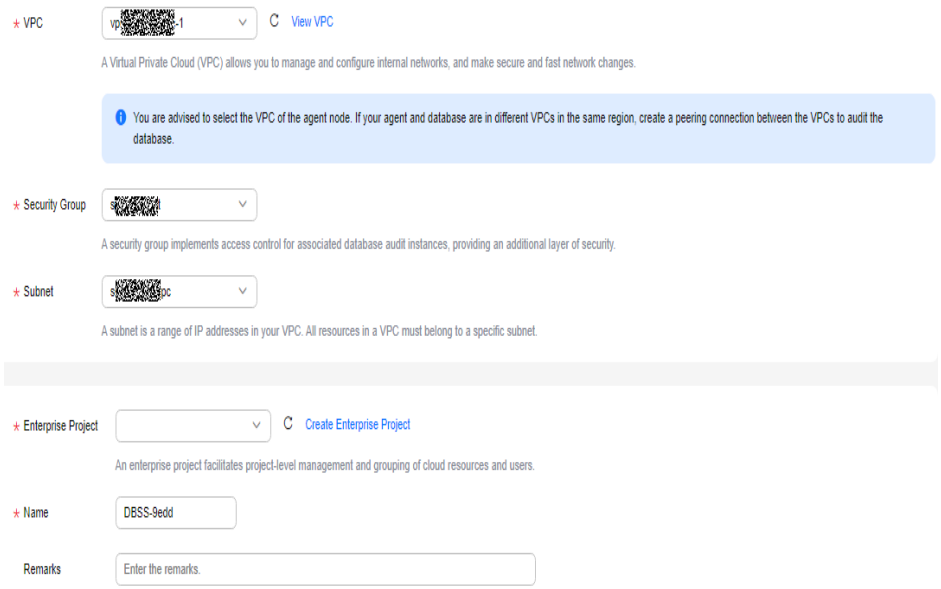


Table 6-3 Database audit instance parameters

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

----End

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

7 Using IAM to Grant Access to DBSS

7.1 Using IAM Roles or Policies to Grant Access to DBSS

Role/policy-based permission provided by **Identity and Access Management (IAM)** let you control access to DBSS. With IAM, you can:

- Create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing DBSS resources.
- Grant users only the permissions required to perform a given task based on their job responsibilities.
- Entrust an 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 how to assign permissions based on roles and policies. **Figure 7-1** shows the authorization process.

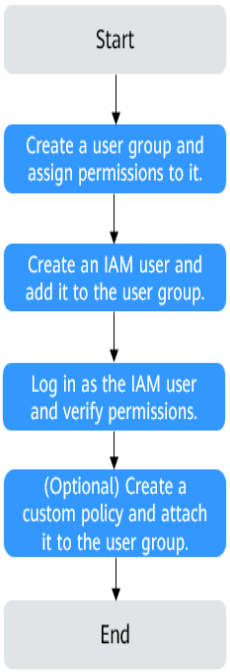
Prerequisites

Before assigning permissions to a user group, you need to understand the DBSS permissions. For details, see **Role and Policy Permission Management**. For details about the permissions of other services, see **System-defined Permissions**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Process Flow

Figure 7-1 Process of granting DBSS permissions



1. On the IAM console, **create a user group and grant it permissions** (*ECS ReadOnlyAccess* as an example).

   Create a user group on the IAM console, and assign the DBSS ReadOnlyAccess permission to the group.

2. **Create an IAM user and add it to the created user group**.

   On the IAM console, create an IAM user and add it to the user group created in **1**.

3. **Log in as the IAM user** and verify permissions.

   In the authorized region, perform the following operations:

   - Choose **Database Security Service** in the service list and click **Buy DBSS** on the DBSS console. If you cannot buy DBSS (assuming that the current permissions include only **DBSS ReadOnlyAccess**), the **DBSS ReadOnlyAccess** policy has already taken effect.
   - Choose another service from **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **DBSS ReadOnlyAccess** policy is in effect.

Examples of Custom Policies

Custom policies can be created to supplement the system-defined policies of DBSS. Then, you can add actions in custom policies. For details, see **Actions Supported by Identity Policies**.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

To create a custom policy, choose either visual editor or JSON.

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit policies from scratch or based on an existing policy in JSON format.

For details, see **Creating a Custom Policy**. The following lists examples of common DBSS 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 policy with only "Deny" permissions must be used together with other policies. If the policies assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  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: Creating a custom policy containing multiple actions.

  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": [
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

```
            "hss:accountCracks:unblock",
            "hss:commonIPs:set"
        ]
    }
  ]
}
```

7.2 Using IAM Identity Policies to Grant Access to DBSS

With **IAM**, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing DBSS resources.
- Grant users only the permissions required to perform a given task based on their job responsibilities.
- Entrust an account or cloud service to perform professional and efficient O&M on your DBSS resources.

If your account meets your permissions requirements, you can skip this section.

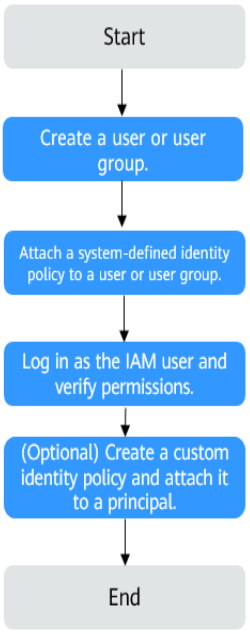
Figure 7-2 shows the process flow of identity policy-based authorization.

Prerequisites

Before granting permissions, learn about the DBSS permissions and select them as required. For details about the system-defined identity policies supported by DBSS, see **Role/Policy-based Permissions Management**. For details about the permissions of other services, see **System-defined Permissions**.

Process Flow

Figure 7-2 Process of granting DBSS permissions



 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1. On the IAM console, **create an IAM user** or **create a user group**.

   Create a user or user group on the IAM console.

2. **Attach a system-defined identity policy** (*CBRReadOnlyPolicy* as an example) to the user or user group.

   Grant the DBSS system-defined identity policy **DBSSReadOnlyPolicy** to a user or user group, or add the policy to the user or user group.

3. **Log in as the IAM user** and verify permissions.

   In the authorized region, perform the following operations:

   - Choose **Database Security Service** in the service list and click **Buy DBSS** on the DBSS console. If you cannot buy DBSS (assuming that the current permissions include only **DBSSReadOnlyPolicy**), the **DBSSReadOnlyPolicy** policy has already taken effect.
   - Choose another service from **Service List**. (The current policy contains only DBSSReadOnlyPolicy.) If a message is displayed, indicating insufficient permissions to access the service, the DBSSReadOnlyPolicy policy has already taken effect.

DBSS Example Custom Identity Policies

If the system-defined policies of DBSS cannot meet your needs, you can create custom identity policies. Then, you can add actions in custom identity policies. For details, see **Actions Supported by Identity Policies**.

You can create custom identity policies on Huawei Cloud in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit policies from scratch or based on an existing policy in JSON format.

For details, see **Creating a Custom Identity Policy and Attaching It to a Principal**.

When creating a custom identity policy, use the **Resource** element to specify the resources the policy applies to and use the **Condition** element (condition keys) to control when the policy is in effect. For details about the supported resource types and condition keys, see **Actions Supported by Identity Policy-based Authorization**. The following provides examples of custom identity 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

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

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

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: Creating a custom policy containing multiple actions.

  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"
         ]
      }
   ]
}
```

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.