Database Security Service

Best Practices

Issue	15
Date	2022-11-18

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks 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 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.

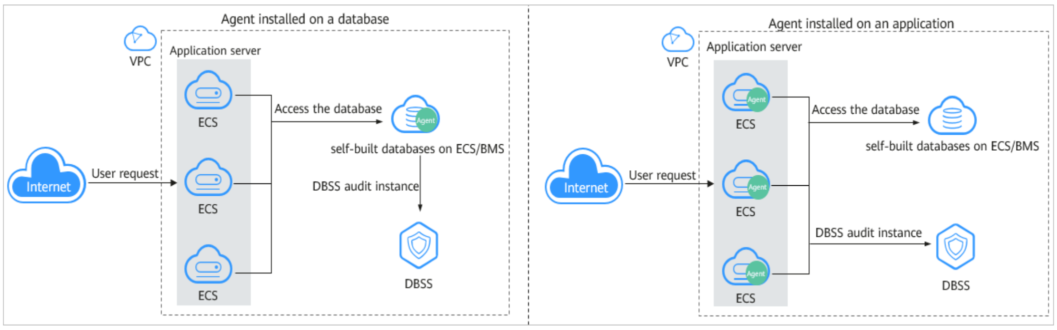
Contents

1 Auditing a User-built Database on ECS

Database audit is deployed in out-of-path mode. The database audit agent is deployed on the database or application server to obtain access traffic, upload traffic data to the audit system, receive audit system configuration commands, and report database monitoring results, implementing security audit on databases built on ECS or BMS.

The following figure shows the architecture used for auditing a user-built database on ECS or BMS.

Figure 1-1 Auditing user-built databases on ECS and BMS



Scenario

Assume you have created a database on Elastic Cloud Server (ECS). **Table 1-1** describes its details. You need to locate and track internal violations and improper operations in the database to meet compliance requirements. This section describes how to install an agent on the database, enable the database audit function, and check audit results.

Table 1-1 ECS database information

Database Type	MySQL
Database Version	5.7
IP Address	192.168.1.5

Port	3306
OS	LINUX64

Limitations and Constraints

- Disable SSL for a database before auditing it.
- The database audit instance and the database to be audited must be in the same region.
- For connection purposes, ensure the VPC of the database audit instance is the same as that of the agent node.

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

Step 1: Purchase Database Audit

Configure and purchase the database audit service. For details, see **Purchasing Database Audit**.

NOTE

For connection purposes, ensure the VPC of the database audit instance is the same as that of the agent node.

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

Step 2: Add a Database and Enable Audit

After purchasing database audit, add the example database to the database audit instance and enable the database audit function for the database.

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

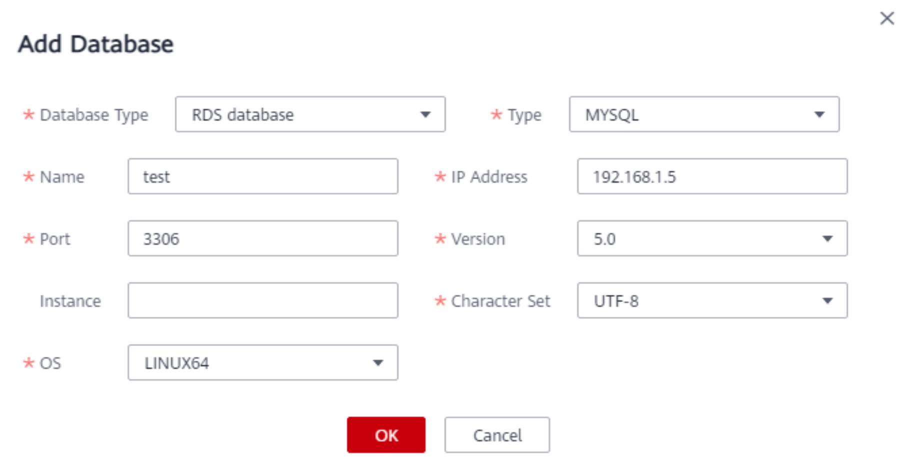
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation pane, choose **Databases**.

Step 4 Select an instance from the **Instance** drop-down list. Click **Add Database**.

Step 5 In the displayed dialog box, set database parameters described in **Table 1-1**, as shown in **Figure 1-2**.

Figure 1-2 Add Database dialog box



Add Database

* Database Type: RDS database
* Type: MYSQL
* Name: test
* IP Address: 192.168.1.5
* Port: 3306
* Version: 5.0
Instance:
* Character Set: UTF-8
* OS: LINUX64

Step 6 Click **OK**. The database will be displayed in the database list and its **Audit Status** will be **Disabled**.

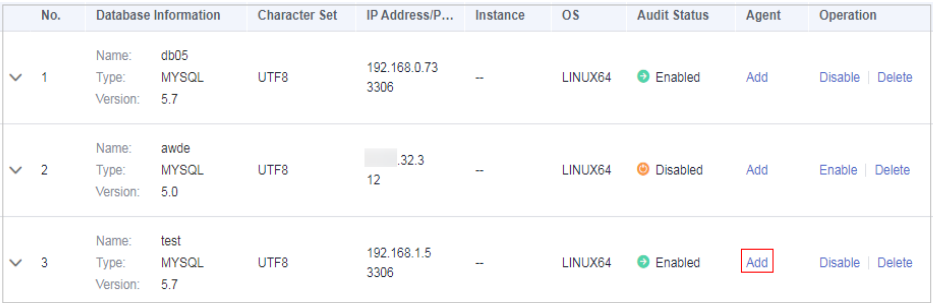
Step 7 In the **Operation** column of the database, click **Enable**.

----End

Step 3: Add an Agent

Step 1 In the **Agent** column of the database, click **Add**, as shown in **Figure 1-3**.

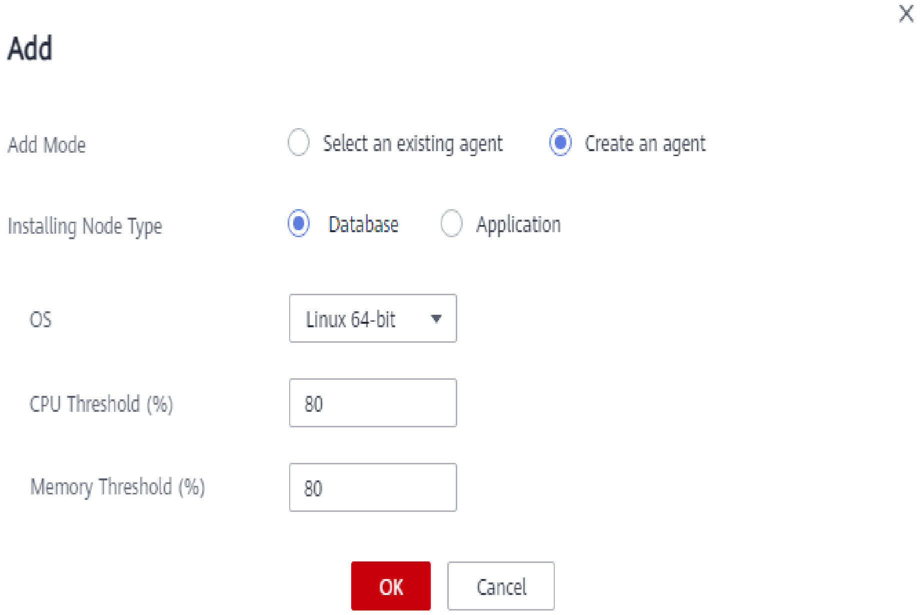
Figure 1-3 Adding an agent



	No.	Database Information	Character Set	IP Address/P...	Instance	OS	Audit Status	Agent	Operation
∨	1	Name: db05 Type: MYSQL Version: 5.7	UTF8	192.168.0.73 3306	--	LINUX64	● Enabled	Add	Disable | Delete
∨	2	Name: awde Type: MYSQL Version: 5.0	UTF8	[redacted].32.3 12	--	LINUX64	● Disabled	Add	Enable | Delete
∨	3	Name: test Type: MYSQL Version: 5.7	UTF8	192.168.1.5 3306	--	LINUX64	● Enabled	Add	Disable | Delete

Step 2 In the displayed dialog box, select an addition mode.

Figure 1-4 Adding an agent to a database



Add

Add Mode ○ Select an existing agent ● Create an agent

Installing Node Type ● Database ○ Application

OS: Linux 64-bit

CPU Threshold (%): 80

Memory Threshold (%): 80

Step 3 Click **OK**.

----End

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.

- If the inbound rules of the security group have been configured for the installing node, go to **Step 5: Install an Agent**.
- If no inbound rules have been configured, perform the following operations.

NOTE

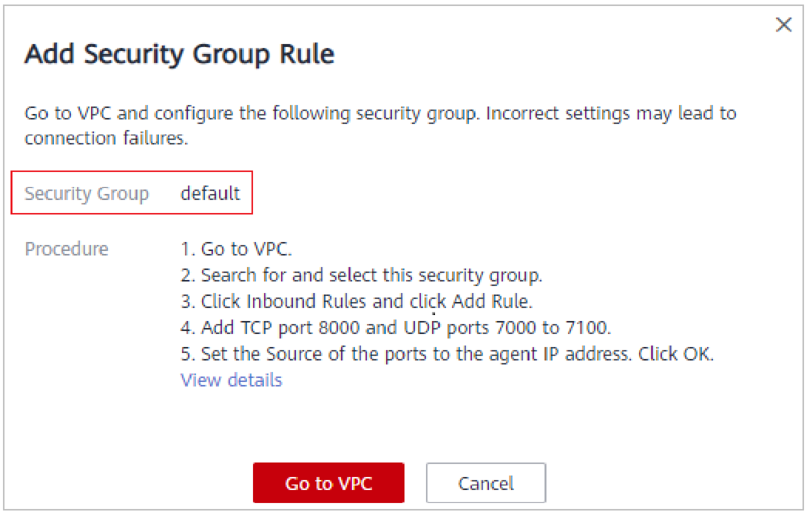
You can configure security group rules before or after installing an agent.

Step 1 Obtain the **IP address of the installation node**.

Step 2 On the **Databases** page, click **Add Security Group Rule**.

Step 3 In the dialog box that is displayed, check and make a note of the security group of the database audit instance, for example, **default**.

Figure 1-5 Adding a security group rule



Add Security Group Rule

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

Security Group default

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

Step 4 Click **Go to VPC**. The **Security Groups** page will be displayed.

Step 5 Enter the security group name **default** in the search box in the upper right corner of the list, and click 🔍 or press **Enter**. The group information is displayed in the list.

Step 6 Click **default**. The **Summary** tab will be displayed.

Step 7 On the **Inbound Rules** tab, click **Add Rule**.

Step 8 In the **Add Inbound Rule** dialog box, add **TCP** (port number **8000**) and **UDP** protocols (port number from **7000** to **7100**) for the installing node IP address.

Step 9 Click **OK**.

----End

Step 5: Install an Agent

Download the agent package and install it on the required node. A database can be audited only after it is connected to a database audit instance.

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 and install the agent again.

Step 1 Log in to the DBSS management console.

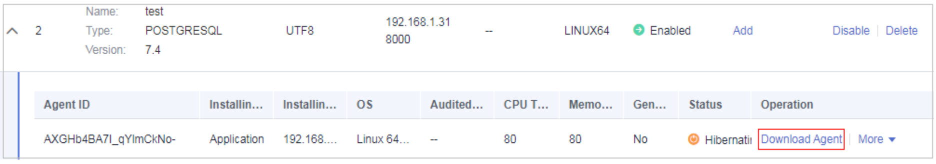
Step 2 In the navigation pane, choose **Databases**.

Step 3 In the **Instance** drop-down list, select an instance.

Step 4 Click ⌄ next to the instance to expand agent details. In the **Operation** column, click **Download Agent**. See **Figure 1-6**.

The agent installation package will be downloaded to your local PC.

Figure 1-6 Downloading an agent



2 Name: test Type: POSTGRESQL Version: 7.4 UTF8 192.168.1.31 8000 -- LINUX64 Enabled Add Disable | Delete

Agent ID	Installin...	Installin...	OS	Audited...	CPU T...	Memo...	Gen...	Status	Operation
AXGHb4BA7I_qYlmCkNo-	Application	192.168....	Linux 64...	--	80	80	No	Hibernati	Download Agent | More

Step 5 Use a cross-platform transmission tool (for example, WinSCP) to upload the downloaded agent installation package **xxx.tar** to the node specified by **Installing Node IP Address** in **Figure 1-6**.

Step 6 Log in to the node as user **root** by using a cross-platform remote access tool (for example, PuTTY) via SSH.

Step 7 Run the following command to access the directory where the agent installation package **xxx.tar** is stored:

Step 8 **cd** *Agent_installation_package_directory*

Step 9 Run the following command to decompress the installation package **xxx.tar**:

Step 10 **tar -xvf** *xxx.tar*

Step 11 Run the following command to go to the directory in which the **install.sh** script is stored:

Step 12 **cd** *install.sh_script_directory*

Step 13 Run the following command to install the agent:

Step 14 **sh install.sh**

Step 15 If the following information is displayed, the agent has been installed successfully:

```
start agent
starting audit agent
audit agent started
start success
install dbss audit agent done!
```

----End

Step 6: Verify the Communication Between the Agent and the Database Audit Instance

Check to ensure the communication between the agent and the database audit instance is normal.

Step 1 Run an SQL statement or perform an operation on the database (for example, **Select 1;**) on the node where the agent is installed.

Step 2 In the navigation pane, choose **Dashboard**.

Step 3 In the **Instance** drop-down list, select the instance whose slow SQL statement information you want to view.

Step 4 Click the **Statements** tab.

Step 5 The SQL statement list displays the record of database login.

If no SQL statement is displayed, check your network connection. For details, see **What Should I Do If the Communication Between the Agent and Database Audit Instance Is Abnormal?**

----End

Step 7: View Audit Results

You can check audit results on the **Dashboard** page, or generate, preview, or download reports.

Step 1 Check overview information.

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

The **Dashboard** page displays the audit duration, total number of SQL statements and risks, statements and risks today, and today's sessions of an instance.

You can click the **Statements** or **Sessions** tab to view session distribution.

Step 2 Generate, download, or preview reports.

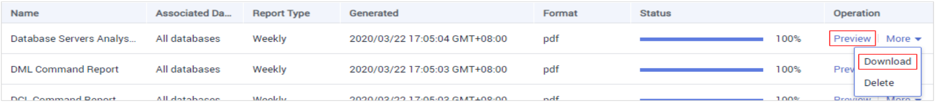
1. In the navigation pane, choose **Reports**.
2. Select an instance from the **Instance** drop-down list. Click the **Report Management** tab.
3. In the **Operation** column of a report template, click **Generate Report**.
4. In the displayed dialog box, click 📅 to set the start time and end time of the report, and select the database for which you want to generate a report.
5. Click **OK**.

   See **Figure 1-7**.

NOTICE

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

Figure 1-7 Previewing or downloading an audit report



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

----End

2 Auditing an RDS DB instance (with Agents)

Overview

This section describes how to audit the security of an RDS DB instance. (Applications connected to this DB instance are deployed on ECS.) DBSS can audit certain types of relational databases without installing agents.

- If the database you want to audit is included in **Table 2-1**, see **Auditing an RDS DB Instance (Without Agents)**.

Table 2-1 Agent-free relational databases

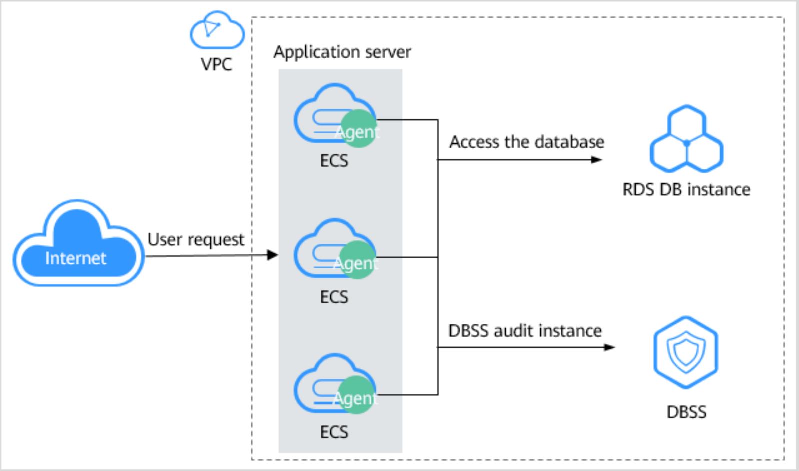
Database Type	Supported Edition
GaussDB(for MySQL)	All editions are supported by default.
RDS for SQLServer	All editions are supported by default.
RDS for MySQL	● 5.6 (5.6.51.1 or later) ● 5.7 (5.7.29.2 or later) ● 8.0 (8.0.20.3 or later)
GaussDB(DWS)	● 8.2.0.100 or later
PostGresql	● 14 (14.4 or later) ● 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)

- If the database that you want to audit is not included in **Table 2-1**, install agents and audit your database by referring to this section.

Solution Architecture

Database audit is deployed in out-of-path mode. The database audit agent is deployed on the database or application server to obtain access traffic, upload traffic data to the audit system, receive audit system configuration commands, and report database monitoring results, implementing security audit on your database instances.

Figure 2-1 Auditing an RDS DB instance (with agents)



Take the following relational database instance of the **PostgreSQL 7.4 version** as an example. Assume you need to locate and track internal violations and improper operations in the database to meet compliance requirements. This section describes how to enable the database audit function and check audit results.

Table 2-2 Database example

Database Type	PostgreSQL
Database Version	7.4
IP Address	192.168.1.31
Application IP address **(Agent node IP address)**	192.168.1.132
Port	8000
OS	Linux 64-bit

Limitations and Constraints

- Disable SSL for a database before auditing it.
- The database audit instance and the database to be audited must be in the same region.

- For connection purposes, ensure the VPC of the database audit instance is the same as that of the agent node.

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

Step 1: Purchase Database Audit

Configure and purchase the database audit service. For details, see **Purchasing Database Audit**.

NOTE

For connection purposes, ensure the VPC of the database audit instance is the same as that of the agent node.

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

Step 2: Add a Database and Enable Audit

After purchasing database audit, add a database to the database audit instance and enable audit for the database.

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

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

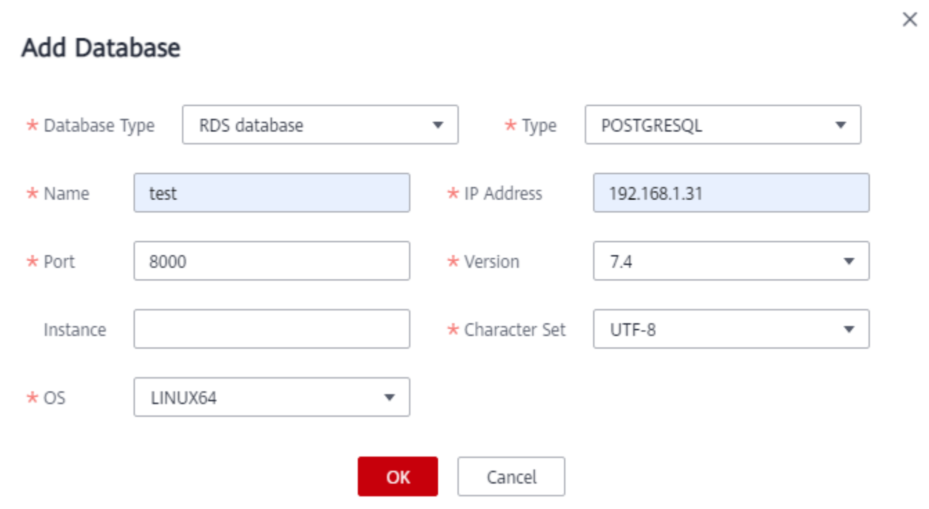
Step 3 In the navigation pane, choose **Databases**.

Step 4 Select an instance from the **Instance** drop-down list. Click **Add Database**.

Step 5 In the displayed dialog box, set database parameters described in **Figure 2-2**.

Database audit supports UTF-8 and GBK character sets encoding.

Figure 2-2 Add Database dialog box



Add Database

* Database Type	RDS database	* Type	POSTGRESQL
* Name	test	* IP Address	192.168.1.31
* Port	8000	* Version	7.4
Instance		* Character Set	UTF-8
* OS	LINUX64		

Step 6 Click **OK**. The database will be displayed in the database list and its **Audit Status** will be **Disabled**.

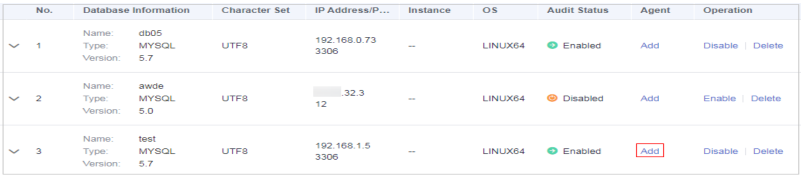
Step 7 In the **Operation** column of the database, click **Enable**.

----End

Step 3: Add an Agent

Step 1 Locate the target database, and click **Add** in the **Agent** column, as shown in **Figure 2-3**.

Figure 2-3 Adding an agent



	No.	Database Information	Character Set	IP Address/P...	Instance	OS	Audit Status	Agent	Operation
﹀	1	Name: db05 Type: MYSQL Version: 5.7	UTF8	192.168.0.73 3306	--	LINUX64	Enabled	Add	Disable | Delete
﹀	2	Name: awde Type: MYSQL Version: 5.0	UTF8	[redacted].32.3 12	--	LINUX64	Disabled	Add	Enable | Delete
﹀	3	Name: test Type: MYSQL Version: 5.7	UTF8	192.168.1.5 3306	--	LINUX64	Enabled	Add	Disable | Delete

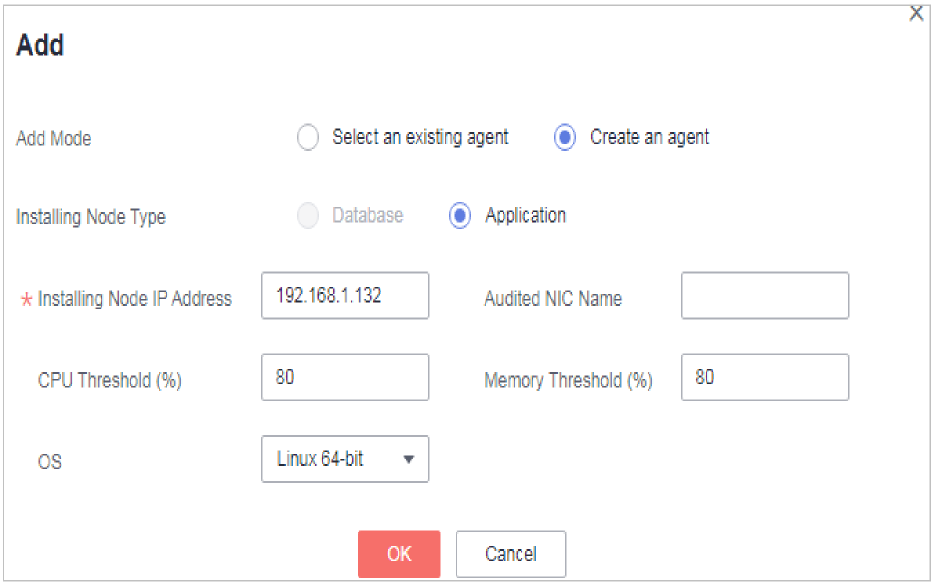
Step 2 In the displayed dialog box, select an addition mode.

- **Method 1: Create an agent**.

  If no agent has been added for the database audit instance, you need to create an agent.

  Set **Installing Node Type** to **Application**. Set **Installing Node IP Address** to the application IP address in **Table 2-2**. See **Figure 2-4**.

  Figure 2-4 Adding an agent to an application

  Add

  Add Mode ○ Select an existing agent ● Create an agent

  Installing Node Type ○ Database ● Application

  * Installing Node IP Address: 192.168.1.132

  Audited NIC Name:

  CPU Threshold (%): 80

  Memory Threshold (%): 80

  OS: Linux 64-bit

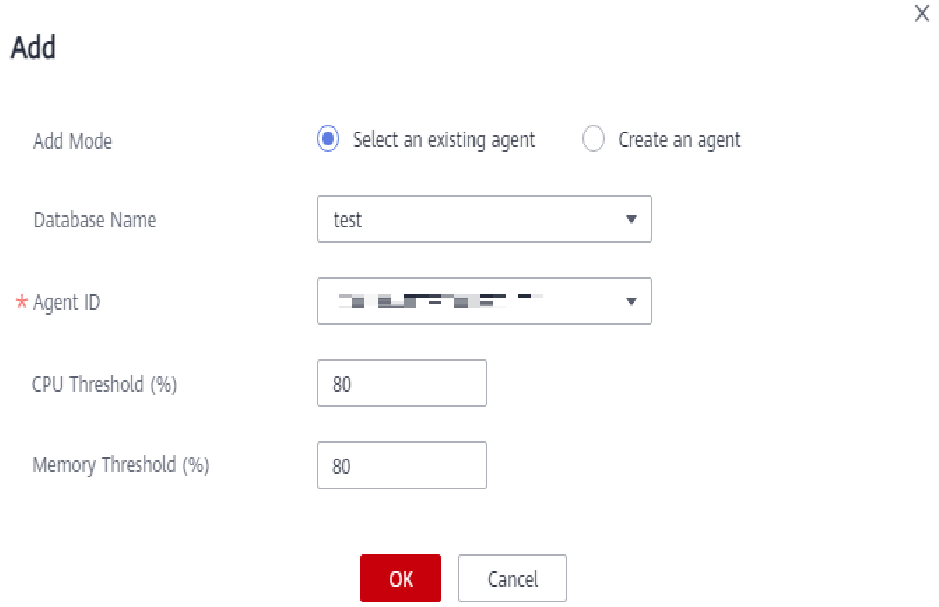
- **Method 2: Select an existing agent**, as shown in **Figure 2-5**.

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

  NOTE

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

Figure 2-5 Selecting an existing agent



Add

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

Database Name: test

* Agent ID: [redacted]

CPU Threshold (%): 80

Memory Threshold (%): 80

Step 3 Click **OK**.

----End

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.

- If the inbound rules of the security group have been configured for the installing node, go to **Step 5: Install an Agent**.
- If no inbound rule has been configured, perform the following operations.

NOTE

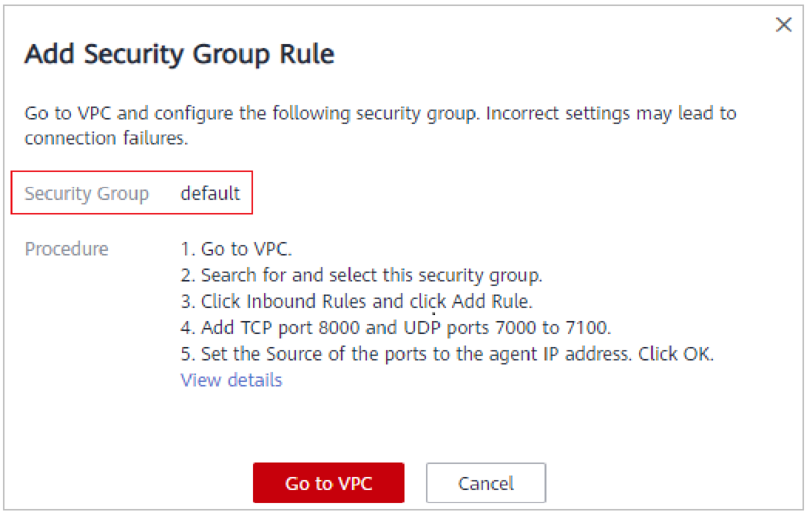
You can configure security group rules before or after installing an agent.

Step 1 **Obtain the IP address of the agent node**.

Step 2 On the **Databases** page, click **Add Security Group Rule**.

Step 3 In the dialog box that is displayed, check and make a note of the security group of the database audit instance, for example, **default**.

Figure 2-6 Adding a security group rule



Add Security Group Rule

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

Security Group default

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

View details

Step 4 Click **Go to VPC**. The **Security Groups** page will be displayed.

Step 5 Enter the security group name **default** in the search box in the upper right corner of the list, and click 🔍 or press **Enter**. The group information is displayed in the list.

Step 6 Click **default**. The **Summary** tab will be displayed.

Step 7 On the **Inbound Rules** tab, click **Add Rule**.

Step 8 In the **Add Inbound Rule** dialog box, add **TCP** (port number **8000**) and **UDP** protocols (port number from **7000** to **7100**) for the installing node IP address in **Table 2-2**.

Step 9 Click **OK**.

----End

Step 5: Install an Agent

Download the agent package and install it on the required node. A database can be audited only after it is connected to a database audit instance.

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 and install the agent again.

Step 1 Log in to the DBSS management console.

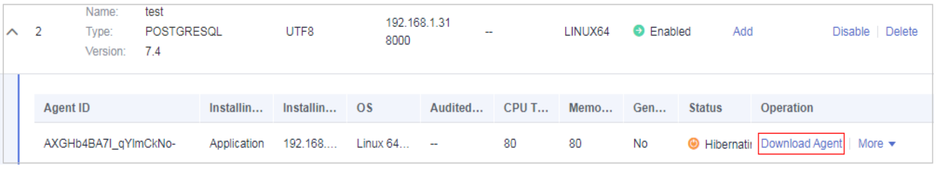
Step 2 In the navigation pane, choose **Databases**.

Step 3 In the **Instance** drop-down list, select an instance.

Step 4 Click ⌄ on the left of the database to view agent details. In the **Operation** column, click **Download Agent**. See **Figure 2-7**.

The agent installation package will be downloaded.

Figure 2-7 Downloading an agent



2 Name: test Type: POSTGRESQL Version: 7.4 UTF8 192.168.1.31 8000 -- LINUX64 Enabled Add Disable | Delete

Agent ID	Installin...	Installin...	OS	Audited...	CPU T...	Memo...	Gen...	Status	Operation
AXGHb4BA7I_qYlmCkNo-	Application	192.168....	Linux 64...	--	80	80	No	Hibernati	Download Agent | More ▾

Step 5 Use a cross-platform transmission tool (for example, WinSCP) to upload the downloaded agent installation package **xxx.tar** to the node specified by **Installing Node IP Address** in **Figure 2-7**.

Step 6 Log in to the node as user **root** by using a cross-platform remote access tool (for example, PuTTY) via SSH.

Step 7 Run the following command to access the directory where the agent installation package **xxx.tar** is stored:

cd *Directory_containing_agent_installation_package*

Step 8 Run the following command to decompress the installation package **xxx.tar**:

tar -xvf *xxx.tar*

Step 9 Run the following command to go to the directory in which the **install.sh** script is stored:

cd *install.sh_script_directory*

Step 10 Run the following command to install the agent:

sh install.sh

If the following information is displayed, the agent has been installed successfully:

```
start agent
starting audit agent
audit agent started
start success
install dbss audit agent done!
```

----End

Step 6: Verify the Communication Between the Agent and the Database Audit Instance

Check to ensure the communication between the agent and the database audit instance is normal.

Step 1 Run an SQL statement or perform an operation on the database (for example, **Select 1;**) on the node where the agent is installed.

Step 2 In the navigation pane, choose **Dashboard**.

Step 3 In the **Instance** drop-down list, select the instance whose slow SQL statement information you want to view.

Step 4 Click the **Statements** tab.

Step 5 The SQL statement list displays the record of database login.

If no SQL statement is displayed, check your network connection. For details, see **What Should I Do If the Communication Between the Agent and Database Audit Instance Is Abnormal?**

----End

Step 7: View Audit Results

You can check audit results on the **Dashboard** page, or generate, preview, or download reports.

Step 1 Check overview information.

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

The **Dashboard** page displays the audit duration, total number of SQL statements and risks, statements and risks today, and today's sessions of an instance.

You can click the **Statements** or **Sessions** tab to view session distribution.

Step 2 Generate, download, or preview reports.

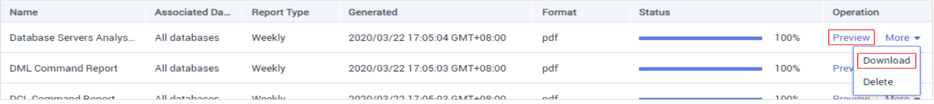
1. In the navigation pane, choose **Reports**.
2. Select an instance from the **Instance** drop-down list. Click the **Report Management** tab.
3. In the **Operation** column of a report template, click **Generate Report**.
4. In the displayed dialog box, click 📅 to set the start time and end time of the report, and select the database for which you want to generate a report.
5. Click **OK**.

   See **Figure 2-8**.

NOTICE

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

Figure 2-8 Previewing or downloading an audit report



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

----End

3 Auditing an RDS DB Instance (Without Agents)

Overview

This section describes how to audit the security of a relational database instance. (Applications connected to this DB instance are deployed on ECS.) DBSS can audit certain types of relational databases without installing agents.

- If the database you want to audit is included in **Table 3-1**, use DBSS to audit your database without installing agents by referring to this section.

Table 3-1 Agent-free relational databases

Database Type	Supported Edition
GaussDB(for MySQL)	All editions are supported by default.
RDS for SQLServer	All editions are supported by default.
RDS for MySQL	● 5.6 (5.6.51.1 or later) ● 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)

- If the database you want to audit is not included in **Table 3-1**, see **Auditing an RDS DB instance (with Agents)**.

NOTE

DBSS without agents is easy to configure and use, but the following functions are not supported:

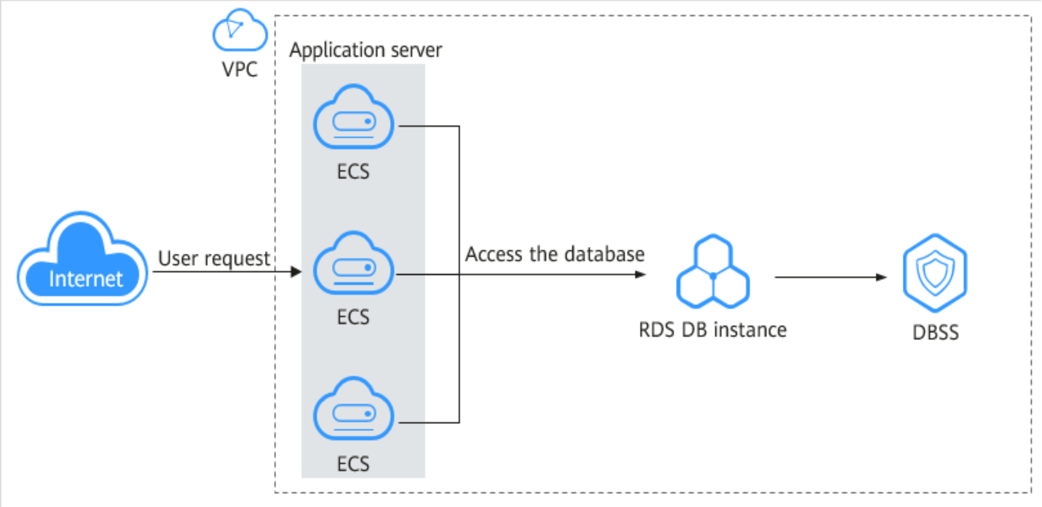
- Successful and failed login sessions cannot be counted.
- The port number of the client for accessing the database cannot be obtained.

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.

Solution Architecture

The DBSS instance receives the logs sent from databases, such as certain GaussDB(for MySQL) or RDS for MySQL versions, and saves the logs to its log library for security analysis, aggregation statistics, and compliance analysis.

Figure 3-1 Auditing an RDS DB instance (without agents)



Take the **GaussDB(for MySQL)** database as an example. Assume you need to locate and track internal violations and improper operations in the database to meet compliance requirements. This section describes how to enable the database audit function and check audit results.

Table 3-2 Database example

Database Type	RDS database
Database Type	GaussDB(for MySQL)
Version	MySQL 8.0
IP Address	192.168.0.237
Database Port	3306

Limitations and Constraints

The database audit instance and the database to be audited must be in the same region.

Step 1: Purchase Database Audit

Configure and purchase the database audit service. For details, see **Purchasing Database Audit**.

Step 2: Add a Database and Enable Audit

After purchasing database audit, add a database to the database audit instance and enable audit for the database.

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

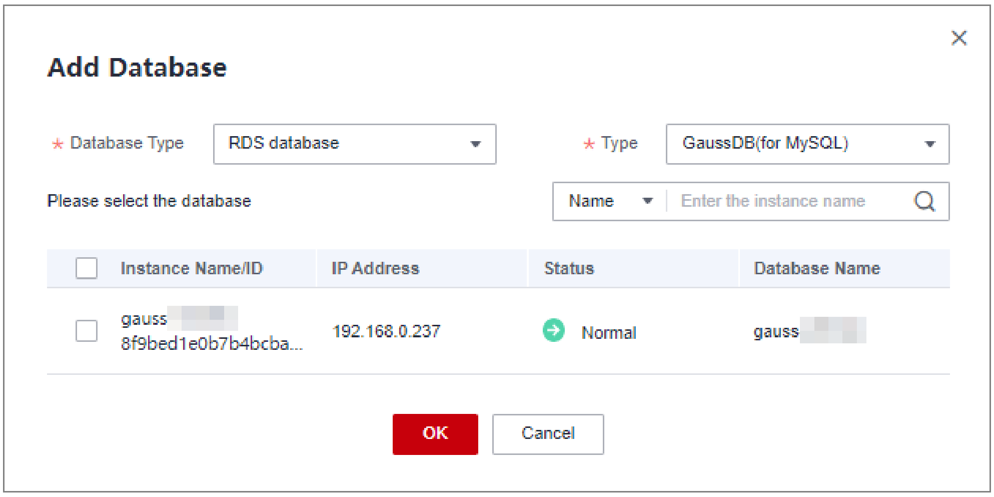
Step 2 Select a region and click ☰. Choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

Step 3 In the navigation pane, choose **Databases**.

Step 4 Select an instance from the **Instance** drop-down list. Click **Add Database**.

Step 5 In the displayed dialog box, set database parameters described in **Table 3-2**.

Figure 3-2 Adding a database



Add Database

* Database Type: RDS database

* Type: GaussDB(for MySQL)

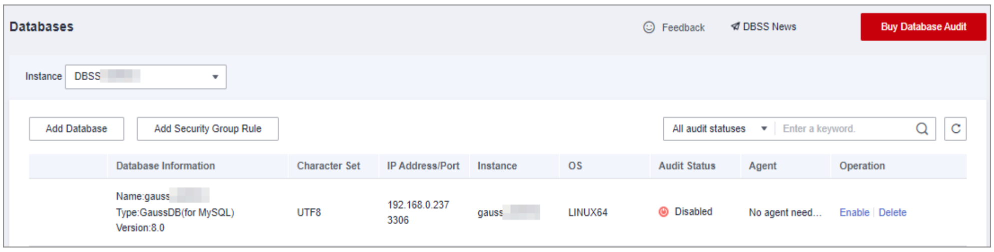
Please select the database

Name: Enter the instance name

□	Instance Name/ID	IP Address	Status	Database Name
□	gauss [redacted] 8f9bed1e0b7b4bcba...	192.168.0.237	Normal	gauss [redacted]

Step 6 Click **OK**. The database will be displayed in the database list and its **Audit Status** will be **Disabled**.

Figure 3-3 Database list



Databases

Instance: DBSS [redacted]

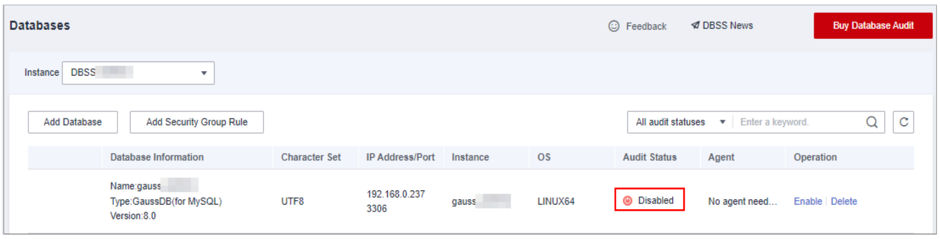
All audit statuses: Enter a keyword.

Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
Name:gauss [redacted] Type:GaussDB(for MySQL) Version:8.0	UTF8	192.168.0.237 3306	gauss [redacted]	LINUX64	Disabled	No agent need...	Enable | Delete

Step 7 In the database list, view the information in the **Agent** column.

- If the message **No agent needs to be added** is displayed, the database can be audited without installing agents. In this case, go to step **Step 8**.

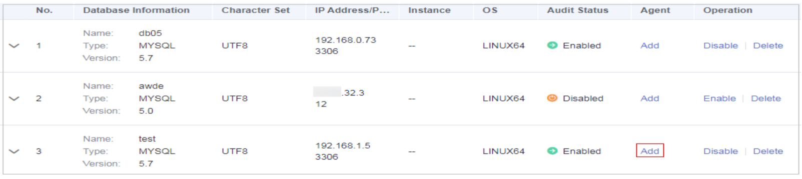
  Figure 3-4 No agent needs to be added

Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
Name:gauss[redacted] Type:GaussDB(for MySQL) Version:8.0	UTF8	192.168.0.237 3306	gauss[redacted]	LINUX64	Disabled	No agent need...	Enable | Delete

- If **Add** is displayed, the database can be audited only after an agent is added. In this case, click **Add** in the **Agent** column. For details, see **Auditing an RDS DB instance (with Agents)**.

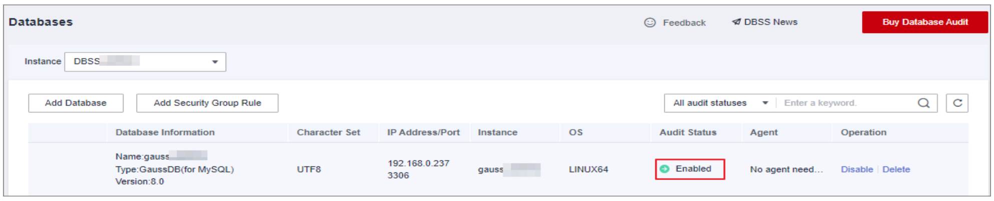
  Figure 3-5 Adding an agent

No.	Database Information	Character Set	IP Address/P...	Instance	OS	Audit Status	Agent	Operation
1	Name: db05 Type: MYSQL Version: 5.7	UTF8	192.168.0.73 3306	--	LINUX64	Enabled	Add	Disable | Delete
2	Name: awde Type: MYSQL Version: 5.0	UTF8	[redacted].32.3 12	--	LINUX64	Disabled	Add	Enable | Delete
3	Name: test Type: MYSQL Version: 5.7	UTF8	192.168.1.5 3306	--	LINUX64	Enabled	Add	Disable | Delete

Step 8 In the **Operation** column of the database, click **Enable**.

Figure 3-6 Enabling database audit



Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
Name:gauss[redacted] Type:GaussDB(for MySQL) Version:8.0	UTF8	192.168.0.237 3306	gauss[redacted]	LINUX64	Enabled	No agent need...	Disable | Delete

----End

Step 3: Viewing the Audit Result

You can check audit results on the dashboard page, or generate, preview, or download reports.

Step 1 Check overview information.

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

The **Dashboard** page displays the audit duration, total number of SQL statements and risks, statements and risks today, and today's sessions of an instance.

You can click the **Statements** or **Sessions** tab to view session distribution.

Step 2 Generate, download, or preview reports.

1. In the navigation pane, choose **Reports**.
2. Select an instance from the **Instance** drop-down list. Click the **Report Management** tab.

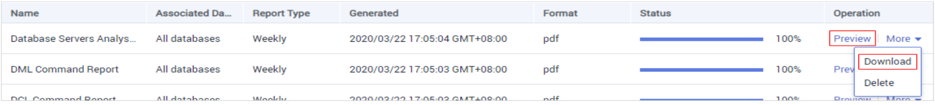
3. In the **Operation** column of a report template, click **Generate Report**.
4. In the displayed dialog box, click 📅 to set the start time and end time of the report, and select the database for which you want to generate a report.
5. Click **OK**.

   See **Figure 3-7**.

NOTICE

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

Figure 3-7 Previewing or downloading an audit report



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

----End

4 Deploying the Database Audit Agent in a Container

4.1 Scenario

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.

Assume the database and the cluster in **Table 4-1** are connected, and you need to audit the database, locate internal violations and improper operations, protect data, and meet compliance requirements. This section describes how to enable the database audit function and check audit results.

NOTICE

- To audit a database, export the database configurations and install the agent on the nodes of the Cloud Container Engine (CCE) clusters connected to the database. For details, see **Installing the Agent on CCE Cluster Nodes**.
- 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.

Table 4-1 Database and CCE cluster to be audited

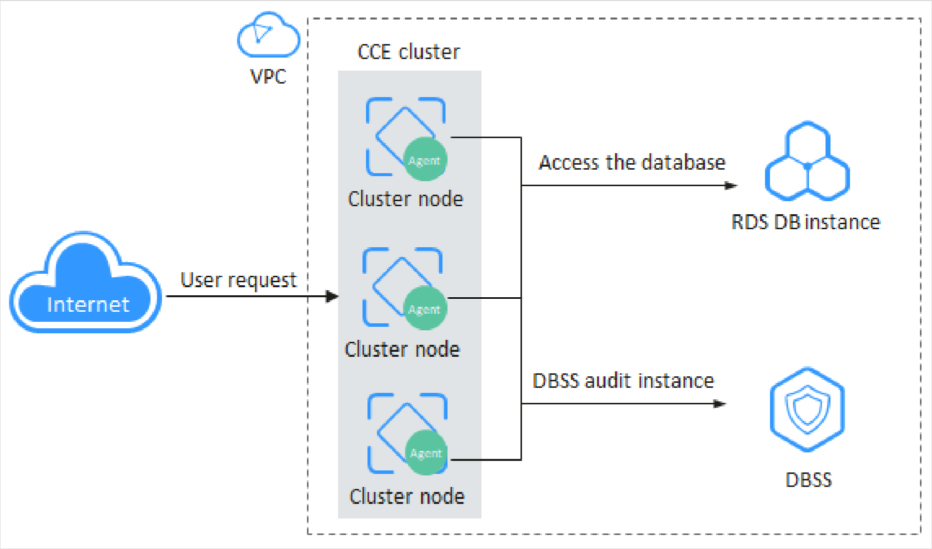
Cluster Name	scc-cmv-bj4
Namespace	default **NOTE** You can select an existing namespace or create one. A namespace is a collection of resources and objects. Multiple namespaces can be created in a single cluster, but they are isolated from each other. This enables namespaces to share the same cluster services without affecting each other.
Database Type	RDS

Database Type	MySQL
Database Version	5.0
IP Address	192.168.1.31, 192.168.0.159
Port	3306
OS	Linux 64-bit

How Databases Are Audited

Database audit is deployed in out-of-path mode. The database audit agent is deployed on the application server that accesses the database and obtains access logs for audit.

Figure 4-1 Application architecture



4.2 Adding a Database and Exporting Database Configurations

Add a database to be audited, enable the audit function, and import the database configurations to Object Storage Service (OBS).

Limitations and Constraints

- Before adding a database, you need to check the databases bound to cluster workloads and ensure:
  - A database is added to only one audit instance.
  - Databases accessed by the same workload must be added to the same audit instance.

  - If the databases accessed by multiple workloads overlap, all these databases must be added to the same audit instance.

- If any of the following changes occurred, you need to export your latest database configurations to an OBS bucket, import the bucket to the CCE cluster, and use the bucket for cluster storage:

  You just purchased a database audit instance, or a database is added or deleted.

- Disable SSL for a database before auditing it.

Adding a Database and Enabling Audit

After purchasing database audit, add the database to be audited to the database audit instance and enable the database audit function for the database.

For details about how to purchase database audit, see **Purchasing Database Audit**.

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

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

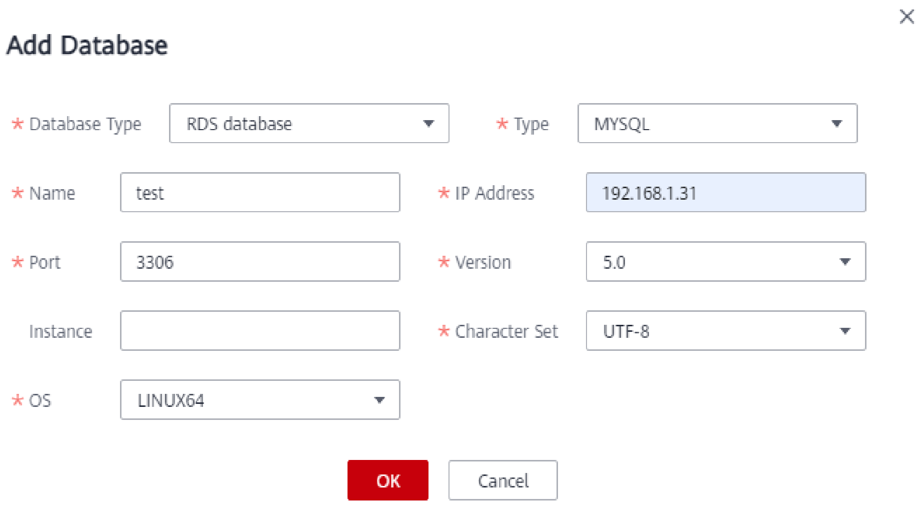
Step 3 In the navigation pane, choose **Databases**.

Step 4 Select an instance from the **Instance** drop-down list. Click **Add Database**.

Step 5 In the displayed dialog box, set database parameters described in **Table 4-1**.

Database audit supports UTF-8 and GBK character encoding.

Figure 4-2 Add Database dialog box



Add Database

* Database Type: RDS database
* Type: MYSQL
* Name: test
* IP Address: 192.168.1.31
* Port: 3306
* Version: 5.0
Instance:
* Character Set: UTF-8
* OS: LINUX64

Step 6 Click **OK**. The database will be displayed in the database list and its **Audit Status** will be **Disabled**.

Step 7 In the **Operation** column of the database, click **Enable**.

----End

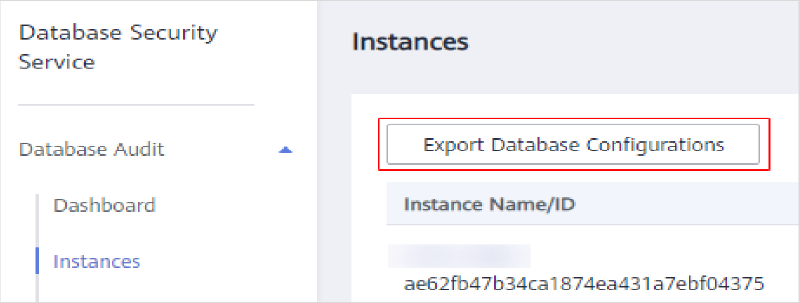
Export database configurations.

Import the database configurations to OBS.

Step 1 In the navigation pane, choose **Instances**.

Step 2 Click **Export Database Configurations**.

Figure 4-3 Exporting database configurations



Database Security Service
Database Audit
Dashboard
Instances
Instances
Export Database Configurations
Instance Name/ID
ae62fb47b34ca1874ea431a7ebf04375

NOTICE

- The **Export Database Configurations** button is hidden. To show this button, add **?exportCfg** at the end of the link of the instance list page, and press **Enter**.
- Database configuration includes the configurations of the database to be audited and the database audit agent.

Step 3 Click **OK**.

Step 4 After you agree to the authorization, a bucket named **dbss-audit-agent-***{projectid}* will be created in OBS.

NOTE

If any of the following changes occurred, your audit instance configurations will also change and you need to export them again:

You just purchased a database audit instance, or a database is added or deleted.

----End

4.3 Installing the Agent on CCE Cluster Nodes

4.3.1 Importing Configurations to OBS

In the cluster that connects to the database, import database configurations (**dbss-audit-agent-***{projectid}*) to OBS. The configurations will be used to deploy the database audit agent in batches in the cloud storage of the agent container workload.

Making Preparations

To ensure reliable and stable OBS buckets for storage, ensure that access keys have been configured before you create OBS buckets.

Procedure

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

Step 2 Select a region and click ☰. Choose **Compute** > **Cloud Container Engine**.

Step 3 In the navigation pane, choose **Resource Management** > **Storage**. Click the **OBS** tab and click **Import**.

Step 4 In the **Import OBS Bucket** dialog box, select an OBS bucket (for example, **dbss-audit-agent-***{projectid}*).

Step 5 Select the cluster and namespace described in **Table 4-1**.

Step 6 Click **OK**.

The imported OBS bucket will be displayed in the OBS list.

NOTE

If your database configurations changed, you need to export the latest configurations to an OBS bucket, import the bucket to the CCE cluster, and use the bucket for cluster storage.

----End

4.3.2 Creating a ConfigMap

Create a ConfigMap to store the database information required by the agent container workload. The ConfigMap is used as a file in the workload.

Procedure

Step 1 In the navigation pane, choose **Configuration Center** > **ConfigMaps**. Click **Create ConfigMap**.

Step 2 Configure parameters on the **Create ConfigMap** page, For more information, see **Table 4-2**.

Table 4-2 Parameters

Parameter	Description	Example Value
Name	Name of a ConfigMap, which must be unique in a namespace.	db-config-for-default
Cluster	Cluster to be audited	scc-cmv-bj4
Namespace	Namespace of the cluster	default
Description	Description of the ConfigMap	-

Parameter	Description	Example Value
Data	Database IP address required by the workload. Perform the following steps to configure it: 1. Click **Add Data**. 2. Set **Key** to **db_config**. 3. Set **Value** to the IP addresses of the databases to be audited. Use commas (,) to separate multiple IP addresses.	Set **Key** to **db_config**. Set **Value** to **192.168.1.31,192.168.0.159**

NOTE

To create a ConfigMap for VPC, click **Add Data** and set **Key** and **Value**.

- **Key**: **vpc_config**
- **Value**: VPC ID of the CCE cluster that the workload belongs to

Step 3 Click **Create**.

----End

4.3.3 Creating an Agent DaemonSet Workload

After you create a ConfigMap, deploy the database audit agent and configure database information in the agent DaemonSet. Your database can then be connected to the database audit instance.

Creating an Agent DaemonSet

Step 1 In the navigation pane, choose **Workloads** > **DaemonSets**. Click **Create DaemonSet**.

Step 2 Configure basic information about the workload For more information, see **Table 4-3**.

Table 4-3 Workload parameters

Parameter	Description	Example Value
Workload Name	Name of a workload, which must be unique	agent-docker
Cluster Name	Cluster connected to the database to be audited	scc-cmv-bj4
Namespace	Namespace of the cluster connected to the database to be audited	default

Step 3 Click **Next: Add Container**. Click **Add Container**. In the dialog box that is displayed, click the **Open source Images** tab. Search for **centos**, and click **OK**.

Step 4 Set CentOS image parameters.

1. Click the **Basic Information** tab. Select the image **centos7.6.1810** and retain the default values for other parameters.

   If the **centos7.5.1804** image is not supported in your region, perform the operations in **Changing an Image**.

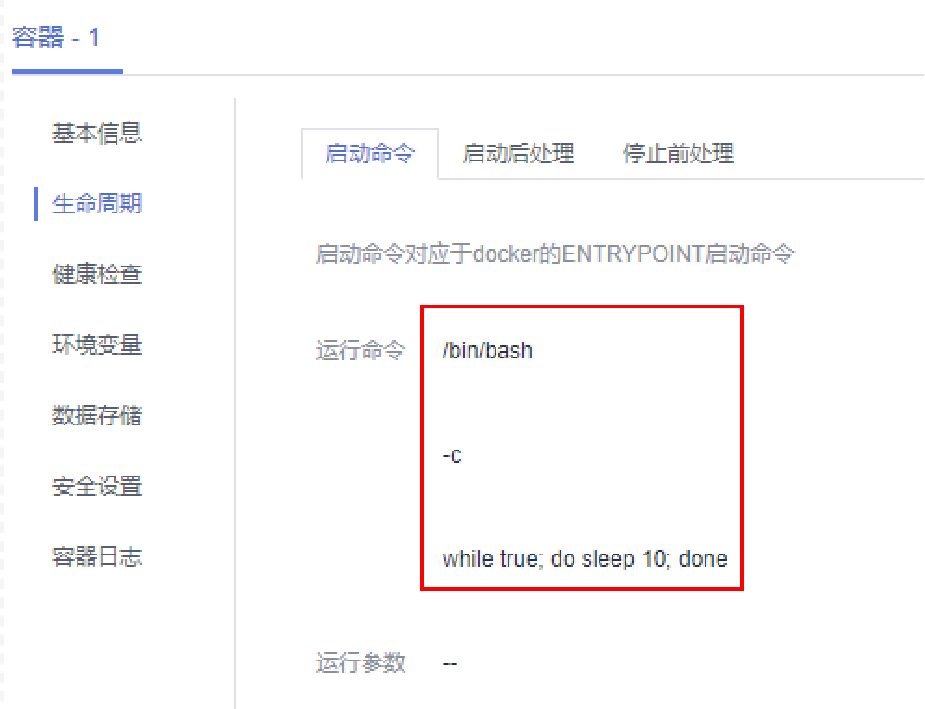
2. Click the **Lifecycle** tab and set the commands used when the container is started or running. Configure the following parameters and retain the default values for other parameters:

   – **Start Command**: command executed when a container is started

     /bin/bash

     -c

     while true; do sleep 10; done;



启动命令对应于docker的ENTRYPOINT启动命令

运行命令
```
/bin/bash

-c

while true; do sleep 10; done
```

运行参数 --

   – **Post-Start**: command executed while a container is up and running

     - **Method**: Select the installation package based on the CPU architecture and run the corresponding commands.

     - If the x86 CPU is used, run the following commands:

       /bin/bash

       -c

       tar xvf /tmp/dbss/agent/audit_agent-x86_64-linux-cce.tar.gz -C /opt;/opt/dbss_agent/install.sh;rm -rf /opt/dbss_agent

     - If the Arm CPU is used, run the following commands:

       /bin/bash

       -c

tar xvf /tmp/dbss/agent/audit_agent-aarch64-linux-cce.tar.gz -C /opt;/opt/dbss_agent/install.sh;rm -rf /opt/dbss_agent

3. Click the **Data Storage** tab and mount extra volumes to the container.
   a. Click the **Local Volume** tab and click **Add Local Volume**. In the dialog box that is displayed, set the following parameters and retain the default values for other parameters.
      - Set **Type** to **ConfigMap**.
      - Set **ConfigMap** to the one created in **Creating a ConfigMap**.
      - Set **Container Path** for the ConfigMap (for example, **/tmp/dbss/db**).

   b. Click **OK**.
   c. Click the **Cloud Volume** tab and click **Add Cloud Volume**. In the dialog box that is displayed, set the following parameters and retain the default values for other parameters.
      - Set **Type** to **OBS**.
      - Set **Allocation Mode** to **Manual**.
      - Set **Name** to the PVC of the OBS bucket created in **Importing Configurations to OBS**.
      - Set **Container Path** for the storage (for example, **/tmp/dbss/agent**).

   d. Click **OK**.

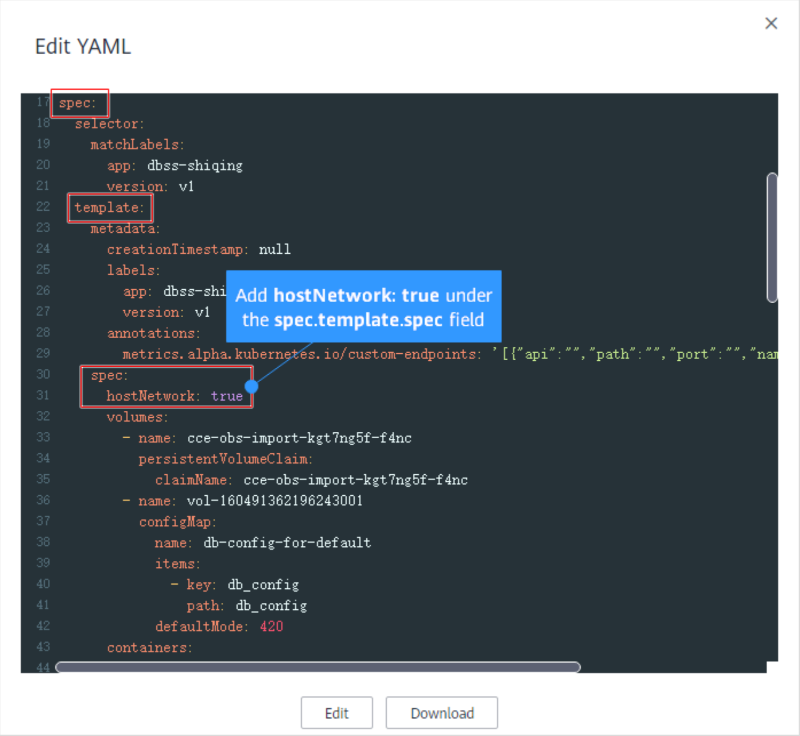
> NOTE
>
> If your database configurations changed, you need to add a new cloud volume and remove the old one.
>
> To add a cloud volume, click a workload and click the **Upgrade** tab. Click **Advanced Settings**, **Data Storage**, and **Cloud Volume**. Click **Add Cloud Volume**.

Step 5 Keep the access settings and advanced settings as they are. Click **Next: Set Application Access**, **Next: Configure Advanced Settings**, and **Create**.

Step 6 Choose **Workloads** > **DaemonSets**. In the **Operation** column of the new DaemonSet, choose **More** > **Edit YAML**.

Step 7 In the **Edit YAML** dialog box, add **hostNetwork: true** under the **spec.template.spec** field.

Figure 4-4 Editing a YAML file



Edit YAML
×
Add **hostNetwork: true** under the **spec.template.spec** field
Edit
Download

```
spec:
  selector:
    matchLabels:
      app: dbss-shiqing
      version: v1
  template:
    metadata:
      creationTimestamp: null
      labels:
        app: dbss-shi
        version: v1
      annotations:
        metrics.alpha.kubernetes.io/custom-endpoints: '[{"api":"","path":"","port":"","nam
    spec:
      hostNetwork: true
      volumes:
        - name: cce-obs-import-kgt7ng5f-f4nc
          persistentVolumeClaim:
            claimName: cce-obs-import-kgt7ng5f-f4nc
        - name: vol-160491362196243001
          configMap:
            name: db-config-for-default
            items:
              - key: db_config
                path: db_config
            defaultMode: 420
      containers:
```

Step 8 Click **Edit**.

Step 9 Check the DaemonSet workload status.

If the workload is in the **Running** state, it has been successfully created.

Step 10 Wait for 2 to 3 minutes. After the deployment succeeded, return to the DBSS console. Check the agent status.

In the agent list of a database, if the value of **General** is **Yes** and **Status** is **Running**, the agent has been connected to the database audit instance.

----End

Changing an Image

If the **centos7.5.1804** image is not supported in your region, perform the following steps to change to this image:

Step 1 Configure the image name.

1. You are advised to do this in a new browser window: On the management console, choose **Containers** > **SoftWare Repository for Container**.
2. In the navigation pane, choose **Image Resources** > **Image Center**.
3. Click **Image Accelerator**. In the displayed **Image Accelerator** dialog box, copy the accelerator address. Remove **https://** from the address, and add **/library/centos:centos7.5.1804** to the end of the address.

   Example: **7b01ab6xxxxfb06b2.mirror.swr.myhuaweicloud.com/library/centos:centos7.5.1804**

Step 2 Change the image.

1. Go back to the page for **setting CentOS image parameters**.
2. Click **Change Image**. In the **Select Container Image** dialog box, click the **Third-Party Images** tab.
3. Enter an image name.
4. Click **OK**.

----End

4.4 Enabling Database Audit

If your database has been connected to the database audit instance, you can enable database audit.

Procedure

Step 1 Go to the DBSS console.

Step 2 In the navigation pane, choose **Databases**.

Step 3 Locate the target database, and click **Enable** in the **Operation** column.

----End

4.5 Checking Audit Results

Check to ensure the communication between the agent and the database audit instance is normal. Then you can use the database audit function and check audit results.

Verifying the Connection Between the Agent and the Database Audit Instance

Run an SQL statement in the database. Wait for a few minutes, log in to the DBSS console, and view the SQL statement.

Step 1 Log in to the application server and run an SQL statement (for example, **select 1;**) in the database.

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

Step 3 In the navigation pane, choose **Dashboard**.

Step 4 Click the **Statements** tab.

Step 5 Check whether the SQL statement executed in **Step 1** is displayed in the SQL statement list.

If the 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

Checking Audit Results

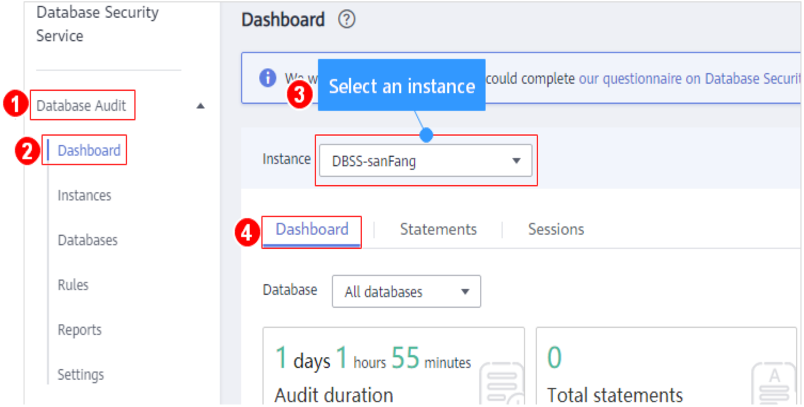
By default, database audit complies with a full audit rule, which is used to audit all databases that are successfully connected to database audit. You can check the audit statistics, including the overall audit statistics, risk distribution, session statistics, SQL distribution, and audit reports.

You can also customize audit rules. For details, see **Configuring Audit Rules**.

Step 1 View the audit dashboard.

1. Go to the **Dashboard** page, as shown in **Figure 4-5**.

Figure 4-5 Accessing the dashboard

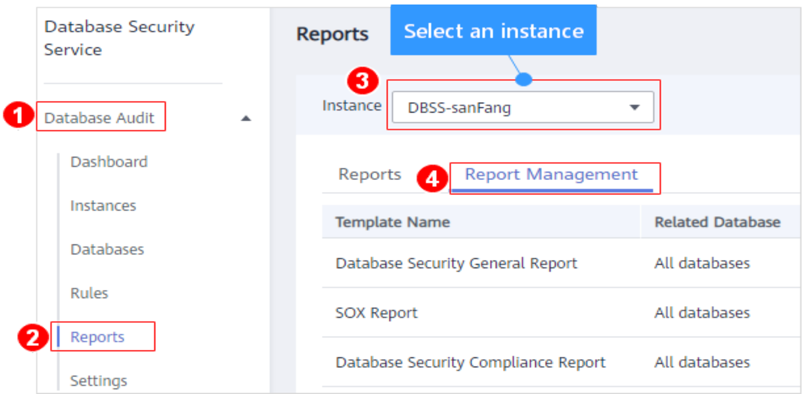


2. Click the **Statements** tab to view SQL statement information or the **Sessions** tab to view session distribution.

Step 2 View audit reports.

1. Go to the report management page, as shown in **Figure 4-6**.

Figure 4-6 Accessing the report management page



Template Name	Related Database
Database Security General Report	All databases
SOX Report	All databases
Database Security Compliance Report	All databases

2. In the row containing the desired report template, click **Generate Report** in the **Operation** column.

3. 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.

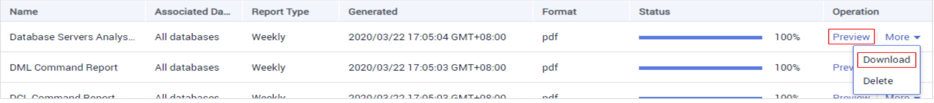
4. Click **OK**.

The **Reports** page is displayed. You can view the report status on this page. After a report is generated, preview or download the report, as shown in **Figure 4-7**.

NOTICE

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

Figure 4-7 Previewing or downloading an audit report



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

----End

5 Checking for Slow SQL Statements

Scenarios

Database audit provides a preconfigured rule to check for slow SQL statements, whose response time recorded in audit logs is greater than 1 second.

You can learn the execution duration, number of affected rows, and database information of the slow SQL statements, and optimize the statements accordingly.

The following types of statements can be audited:

- Data Definition Language (DDL):
  - CREATE TABLE
  - CREATE TABLESPACE
  - DROP TABLE
  - DROP TABLESPACE
- Data Manipulation Language (DML):
  - INSERT
  - UPDATE
  - DELETE
  - SELECT
  - SELECT FOR UPDATE
- Data Control Language (DCL):
  - CREATE USER
  - DROP USER
  - GRANT

Checking Slow SQL Statements

Perform the following steps:

Step 1 Log in to the management console.

Step 2 Select a region and click ☰ . Choose **Security & Compliance** > **Database Security Service**.

Step 3 In the navigation pane, choose **Dashboard**.

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

Step 5 Click the **Statements** tab.

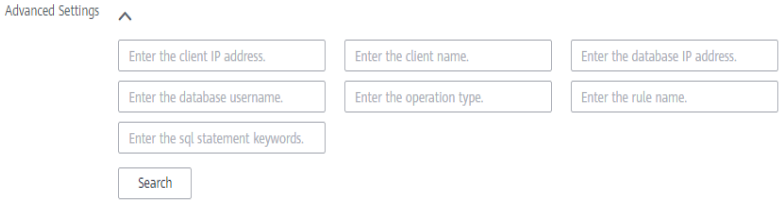
Step 6 Set filter criteria to query SQL statements.

- Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days**, or click 📅 to set start time and end time. Click **Submit** to view SQL statements of the specified time range.
- Set **Risk Severity** (the default value in the slow SQL rule is **Low**) and click **Submit**.
- Click ⌄ next to **Advanced Settings**, set parameters, and click **Search**.

NOTE

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

Figure 5-1 Advanced settings


Advanced Settings
Enter the client IP address.
Enter the client name.
Enter the database IP address.
Enter the database username.
Enter the operation type.
Enter the rule name.
Enter the sql statement keywords.
Search

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

Step 8 In the **Details** dialog box, view the detailed information about the SQL statement. Table 5-1 describes the parameters.

Table 5-1 SQL statement parameters

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	IP address of the database where an SQL statement is executed

Parameter	Description
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 to 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

Managing Slow SQL Detection Settings

Choose **Rules** and click the **Risky Operations** tab. Here you can manage slow SQL settings.

- Enable

  In the row containing the slow SQL detection rule, click **Enable** in the **Operation** column.

- Edit

  In the row containing the slow SQL detection rule, click **Edit** in the **Operation** column.

- Disable

  In the row containing the slow SQL detection rule, click **Disable** in the **Operation** column. Disabled rules will not be audited.

- Delete

  In the row containing the slow SQL detection rule, click **Delete** in the **Operation** column. To add the rule again, follow the instructions in **Adding Risky Operations**.

6 Checking for Data Reduction

Scenario

Database audit provides a preconfigured rule to check audit logs for data security risks, such as SQL statements used for data breach.

You can learn the execution duration, number of affected rows, and database information of the SQL statements.

The following types of statements can be audited:

- DDL:
  - CREATE TABLE
  - CREATE TABLESPACE
  - DROP TABLE
  - DROP TABLESPACE
- DML:
  - INSERT
  - UPDATE
  - DELETE
  - SELECT
  - SELECT FOR UPDATE
- DCL:
  - CREATE USER
  - DROP USER
  - GRANT

Configuring Data Reduction Detection

To check for data reduction, configure the database to be audited, client IP address or IP address segment, operation type, operation object, and execution result.

Step 1 Log in to the management console.

Step 2 Select a region and click ☰ . Choose **Security & Compliance** > **Database Security Service**.

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

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

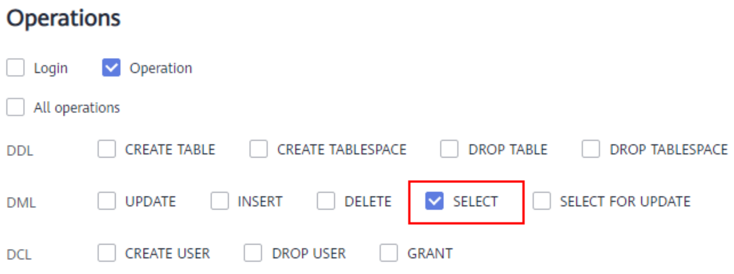
Step 5 Click the **Risky Operations** tab.

Step 6 In the **Operation** column of a data reduction event, click **Edit**. The **Edit Risky Operation** page will be displayed.

Step 7 (Optional) Configure an IP address or IP address segment, or all the IP addresses will be checked by default.

Step 8 In the **Operations** area, select **Operation** and **SELECT**.

Figure 6-1 Operations



Operations

☐ Login ☑ Operation

☐ All operations

DDL ☐ CREATE TABLE ☐ CREATE TABLESPACE ☐ DROP TABLE ☐ DROP TABLESPACE

DML ☐ UPDATE ☐ INSERT ☐ DELETE ☑ SELECT ☐ SELECT FOR UPDATE

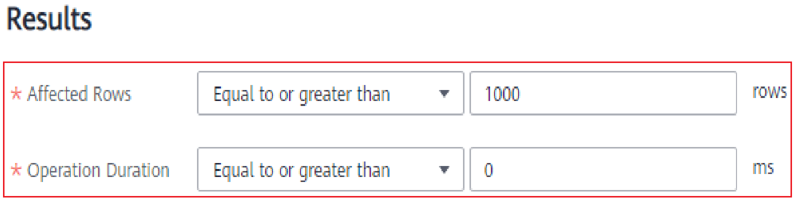
DCL ☐ CREATE USER ☐ DROP USER ☐ GRANT

Step 9 (Optional) Configure operation objects, or all the operation objects will be scanned by default.

1. Click an operation object. Enter the target database, target table, and field information.
2. Click **OK**.

Step 10 In the **Results** area, configure **Affected Rows** and **Operation Duration**.

Figure 6-2 Results



Results

* Affected Rows: Equal to or greater than ▾ 1000 rows

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

NOTICE

If your application changes (for example, because of service upgrade or code changes), you need to modify **Affected Rows** to ensure the results are fully audited.

Step 11 Click **Save**.

----End

Viewing Data Reduction Check Results

Perform the following steps:

Step 1 Log in to the management console.

Step 2 Select a region and click ☰ . Choose **Security & Compliance** > **Database Security Service**.

Step 3 In the navigation pane, choose **Dashboard**.

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

Step 5 Click the **Statements** tab.

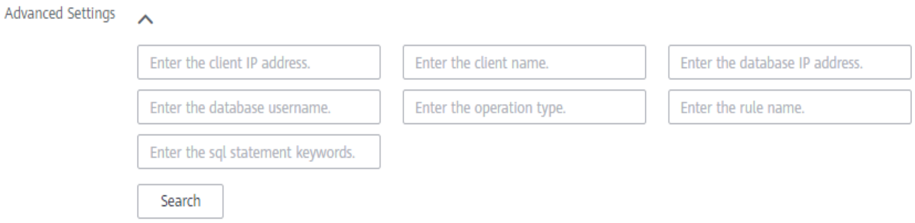
Step 6 Set filter criteria to query SQL statements.

- Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days**, or click 📅 to set start time and end time. Click **Submit** to view SQL statements of the specified time range.
- Set **Risk Severity** (the default value in the data reduction rule is **High**) and click **Submit**.
- Click ∨ next to **Advanced Settings**. Configure parameters, as shown in **Figure 6-3**, and click **Search**.

NOTE

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

Figure 6-3 Advanced settings


Advanced Settings
Enter the client IP address.
Enter the client name.
Enter the database IP address.
Enter the database username.
Enter the operation type.
Enter the rule name.
Enter the sql statement keywords.
Search

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

Step 8 In the **Details** dialog box, view the detailed information about the SQL statement. **Table 6-1** describes the parameters.

Table 6-1 SQL statement parameters

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

Parameter	Description
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	IP address 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 to 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

Viewing Data Reduction Check Rules

Choose **Rules** and click the **Risky Operations** tab. Here you can manage slow SQL settings.

- Enable

  In the row containing the data reduction detection rule, click **Enable** in the **Operation** column.
- Edit

  In the row containing the data reduction detection rule, click **Edit** in the **Operation** column.
- Disable

  In the row containing the data reduction detection rule, click **Disable** in the **Operation** column. Disabled rules will not be audited.
- Delete

In the row containing the data reduction detection rule, click **Delete** in the **Operation** column. To add the rule again, follow the instructions in **Adding Risky Operations**.

7 Checking for Dirty Tables

Scenario

Configure a rule to detect operations on dirty tables. You can configure unnecessary databases, tables, and columns as dirty tables. Programs that access the dirty tables will be marked as suspicious programs.

In this way, you can detect the SQL statements that access dirty tables and detect data security risks in a timely manner.

Prerequisites

You have configured unnecessary databases, tables, or columns.

Procedure

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

Step 2 Select a region and click ☰ . Choose **Security & Compliance** > **Database Security Service**.

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

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

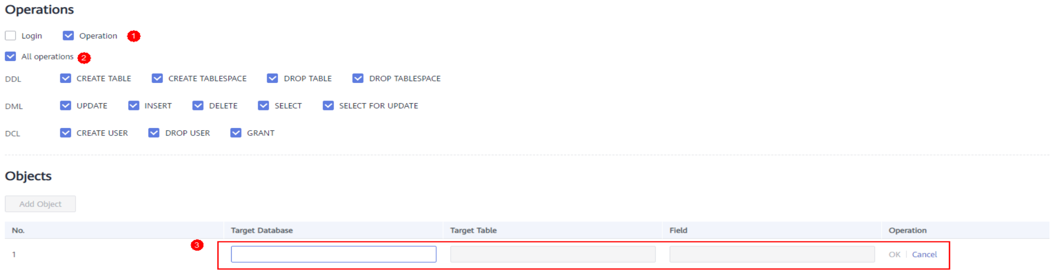
Step 5 Click the **Risky Operations** tab.

Step 6 In the **Basic Information** area, set **Risk Level** to **High**.

Step 7 (Optional) Configure an IP address or IP address segment, or all the IP addresses will be checked by default.

Step 8 Select **Operation** and **All operations**. Configure unnecessary databases, tables, or columns, as shown in **Figure 7-1**.

Figure 7-1 Adding a dirty table detection rule



Operations

□ Login ☑ Operation 1

☑ All operations 2

DDL ☑ CREATE TABLE ☑ CREATE TABLESPACE ☑ DROP TABLE ☑ DROP TABLESPACE

DML ☑ UPDATE ☑ INSERT ☑ DELETE ☑ SELECT ☑ SELECT FOR UPDATE

DCL ☑ CREATE USER ☑ DROP USER ☑ GRANT

Objects

Add Object

No.	Target Database	Target Table	Field	Operation
1				OK | Cancel

Step 9 Click **Save**.

----End

Viewing Dirty Table Detection Results

Perform the following steps:

Step 1 Log in to the management console.

Step 2 Select a region and click ☰ . Choose **Security & Compliance** > **Database Security Service**.

Step 3 In the navigation pane, choose **Dashboard**.

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

Step 5 Click the **Statements** tab.

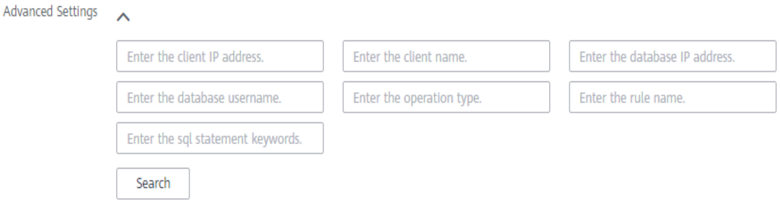
Step 6 Set filter criteria to query SQL statements.

- Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days**, or click 📅 to set start time and end time. Click **Submit** to view SQL statements of the specified time range.
- Set **Risk Severity** (the default value in the dirty table detection rule is **High**) and click **Submit**.
- Click ⌄ next to **Advanced Settings**. Configure parameters as shown in **Figure 7-2**. Click **Search**.

  NOTE

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

Figure 7-2 Advanced settings



Advanced Settings

Enter the client IP address. | Enter the client name. | Enter the database IP address.

Enter the database username. | Enter the operation type. | Enter the rule name.

Enter the sql statement keywords.

Search

Step 7 In the **Operation** column of an SQL statement, click **Details**. For more information, see **Table 7-1**.

Table 7-1 SQL statement parameters

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	IP address 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
Operations	Type of an SQL statement operation
Operation Object Type	Type of an SQL statement operation object
Response Result	Response to 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

View Dirty Table Detection Rules

Choose **Rules** and click the **Risky Operations** tab. Here you can perform the following operations.

- Enable

  In the row containing the dirty table detection rule, click **Enable** in the **Operation** column.

- Edit

  In the row containing the dirty table detection rule, click **Edit** in the **Operation** column.

- Disable

  In the row containing the dirty table detection rule, click **Disable** in the **Operation** column. Disabled rules will not be audited.

- Delete

  In the row containing the dirty table detection rule, click **Delete** in the **Operation** column. To add the rule again, follow the instructions in **Adding Risky Operations**.

8 Configuring Oracle RAC Cluster Audit

When using DBSS for an Oracle RAC cluster, each node in the cluster is regarded as an independent database and requires an agent to forward network traffic.

Configuration

The maximum number of audited databases depends on the DBSS edition you purchased. Before the configuration, check whether the maximum number of instances supported by the DBSS edition you purchased is greater than or equal to the number of RAC cluster nodes.

Example:

- If your RAC cluster has no more than three nodes, you are advised to purchase the DBSS basic edition.
- If your RAC cluster has no more than six nodes, you are advised to purchase the DBSS professional edition.
- If your RAC cluster has more than six nodes, you are advised to purchase the DBSS advanced edition.

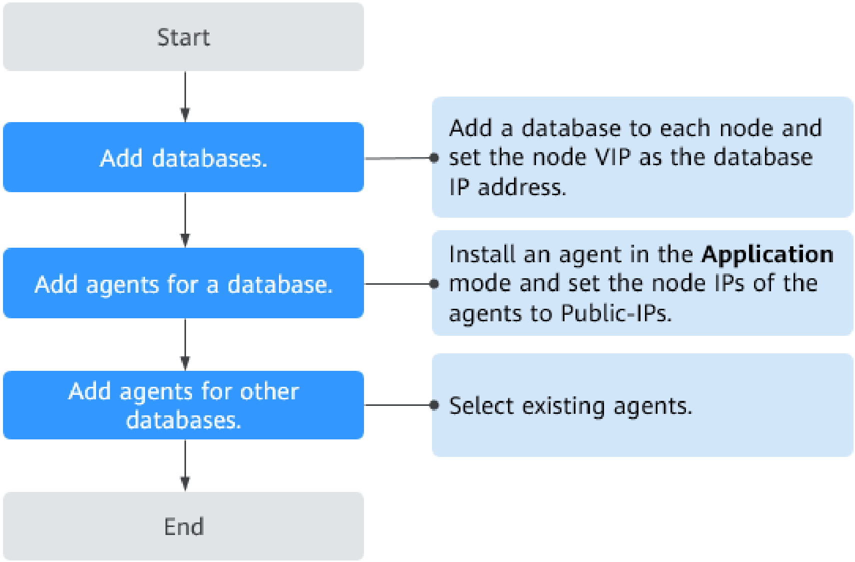
Table 8-1 DBSS performance and specifications

Version	Maximum Databases	System Resource	Performance
Basic	3	● CPU: 4 vCPUs ● Memory: 16 GB ● Disk: 500 GB	● Peak QPS: 3,000 queries/second ● Database load rate: 3.6 million statements/hour ● Stores 400 million online SQL statements. ● Stores 5 billion archived SQL statements.

Version	Maximum Databases	System Resource	Performance
Professional	6	- CPU: 8 vCPUs - Memory: 32 GB - Hard disk: 1000 GB	- Peak QPS: 6,000 queries/second - Database load rate: 7.2 million statements/hour - Stores 600 million online SQL statements. - Stores 10 billion archived SQL statements.
Advanced	30	- CPU: 16 vCPUs - Memory: 64 GB - Hard disk: 2000 GB	- Peak QPS: 30,000 queries/second - Database load rate: 10.80 million statements/hour - Stores 1.5 billion online SQL statements. - Stores 60 billion archived SQL statements.

Configuration Process

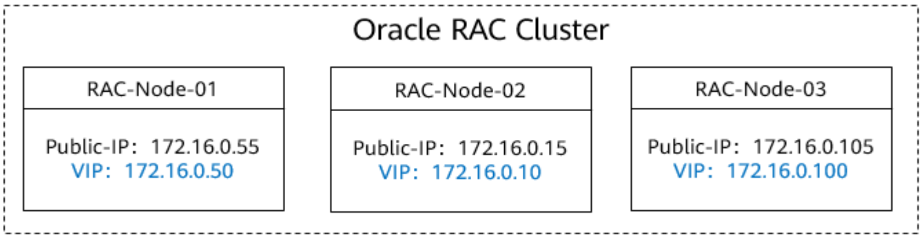
To configure the RAC cluster audit, you just need to add a database and an agent.


Start
Add databases.
Add a database to each node and set the node VIP as the database IP address.
Add agents for a database.
Install an agent in the **Application** mode and set the node IPs of the agents to Public-IPs.
Add agents for other databases.
Select existing agents.
End

Prerequisites

- You have purchased a DBSS instance.
- You have obtained the Public-IPs and VIPs of all nodes in the cluster.

  Example: The Oracle RAC cluster for which DBSS is to be enabled has three nodes.



Procedure

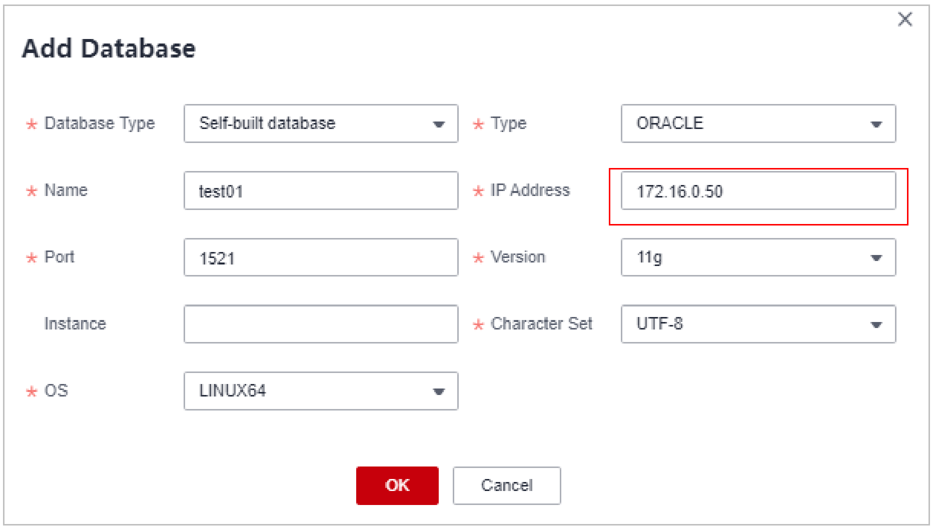
Step 1 Log in to the Huawei Cloud management console and choose **Database Security Service**. Choose **Database Audit** > **Databases**. The **Databases** page is displayed.

Step 2 In the instance drop-down list, select an instance. In the upper left corner of the database list, click **Add Database**.

Step 3 In the dialog box that is displayed, enter the information about the RAC cluster database.

Example: Add a database to the RAC cluster node **RAC-Node-01**.

Figure 8-1 Adding an Oracle database



Add Database

* Database Type	Self-built database	* Type	ORACLE
* Name	test01	* IP Address	172.16.0.50
* Port	1521	* Version	11g
Instance		* Character Set	UTF-8
* OS	LINUX64		

Table 8-2 Parameters

Parameter	Description	Example Value
Database Type	Type of the database to be added, which can be **RDS** or **Self-built database**.	Self-built database
Type	Supported database type. **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.	ORACLE
Name	Name of the database to be added	test01

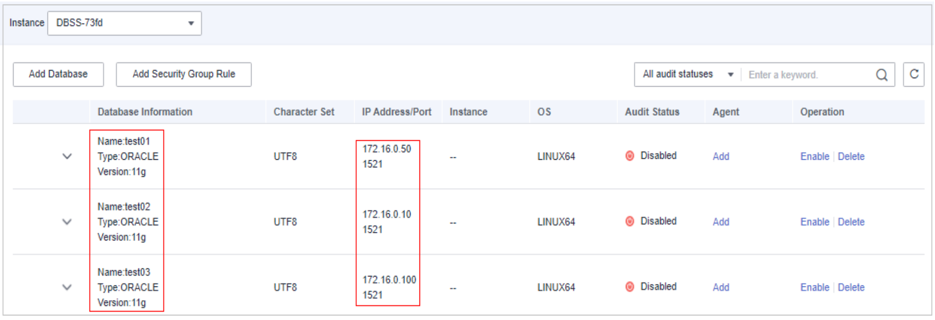
Parameter	Description	Example Value
IP Address	IP address of the database to be added. Set this parameter to the VIP field of the cluster node.	172.16.0.50
Port	Open port of the database to be added. The default port number of Oracle databases is **1521**.	1521
Version	Supported database version. ● If **Type** is set to **ORACLE**, the following database versions are supported: – 11g – 12c – 19c	11g
Instance	Database instance to be audited. **NOTE** ● If the instance name is not specified, all instances in the database will be audited. ● You can specify up to five instance names and use semicolons (;) to separate the names.	-
Character Set	Supported encoding format of the database character set. The options are as follows: ● UTF-8 ● GBK	UTF-8
OS	Operating system of the added database. The options are as follows: ● LINUX64 ● WINDOWS64	LINUX64

Step 4 Confirm the information and click **OK**. The database is added to the node **RAC-Node-01**.

Repeat **Step 3** to add databases to the node **RAC-Node-02** and **RAC-Node-03** in sequence. After all databases are added, view the database list, as shown in **Figure 8-2**.

Example: Databases (**test01**, **test02**, and **test03**) have been added to all nodes in the cluster.

Figure 8-2 Database list



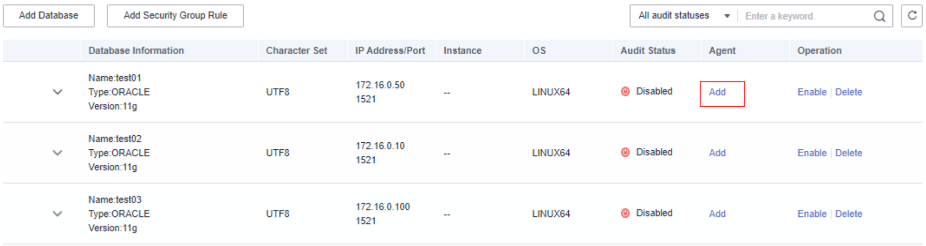
Instance DBSS-73fd

	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
⌄	Name:test01 Type:ORACLE Version:11g	UTF8	172.16.0.50 1521	--	LINUX64	● Disabled	Add	Enable | Delete
⌄	Name:test02 Type:ORACLE Version:11g	UTF8	172.16.0.10 1521	--	LINUX64	● Disabled	Add	Enable | Delete
⌄	Name:test03 Type:ORACLE Version:11g	UTF8	172.16.0.100 1521	--	LINUX64	● Disabled	Add	Enable | Delete

Step 5 Locate a database name, and click **Add** in the **Agent** column.

Example: Add an agent to the database **test01**.

Figure 8-3 Adding an agent

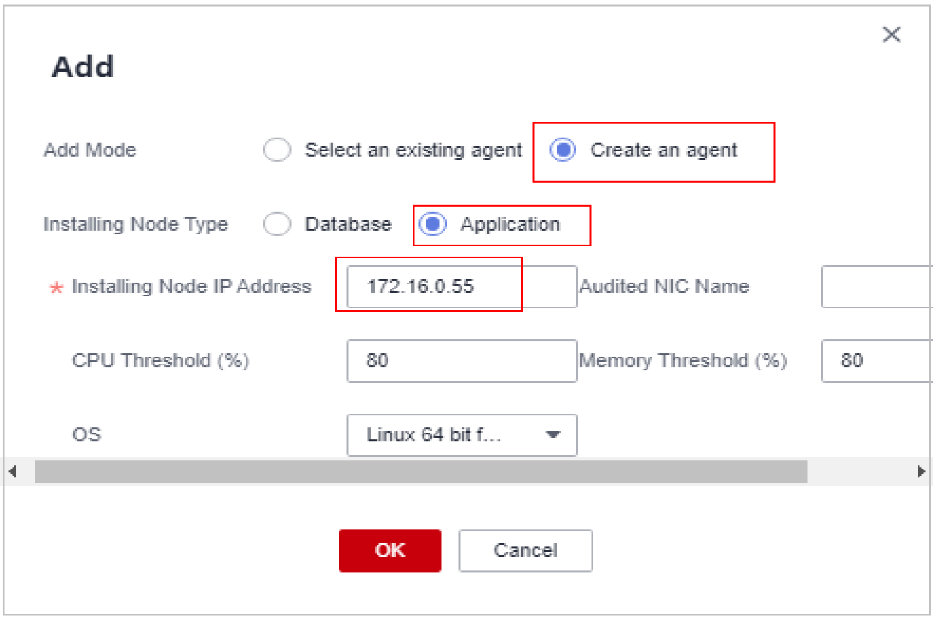


	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
⌄	Name:test01 Type:ORACLE Version:11g	UTF8	172.16.0.50 1521	--	LINUX64	● Disabled	Add	Enable | Delete
⌄	Name:test02 Type:ORACLE Version:11g	UTF8	172.16.0.10 1521	--	LINUX64	● Disabled	Add	Enable | Delete
⌄	Name:test03 Type:ORACLE Version:11g	UTF8	172.16.0.100 1521	--	LINUX64	● Disabled	Add	Enable | Delete

Step 6 In the dialog box that is displayed, enter the information about the agent to be added, as shown in **Table 8-3**.

Example: Add an agent to the node **RAC-Node-01**.

Figure 8-4 Adding an agent



Add

Add Mode ○ Select an existing agent ● Create an agent

Installing Node Type ○ Database ● Application

* Installing Node IP Address 172.16.0.55 Audited NIC Name

CPU Threshold (%) 80 Memory Threshold (%) 80

OS Linux 64 bit f...

Table 8-3 Parameters for adding an agent for the first time

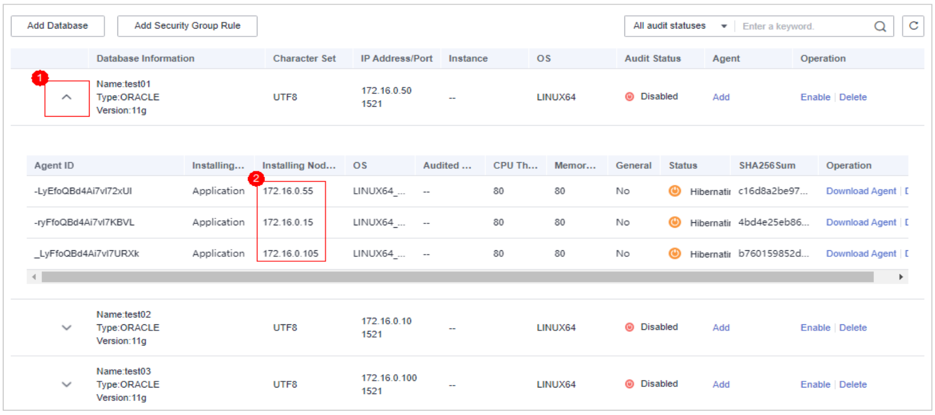
Parameter	Description	Example Value
Add Mode	Method of adding an agent. The options are as follows: ● **Select an existing agent** ● **Create an agent**	Create an agent
Installing Node Type	This parameter is mandatory when **Add Mode** is set to **Create an agent**. The options are as follows: ● **Database** ● **Application**	Application
Installing Node IP Address	This parameter is mandatory if **Installing Node Type** is set to **Application**. If the agent is added to an RAC cluster node, enter the Public-IP field of the node.	172.16.0.55
Audited NIC Name	Optional. This parameter is configurable when **Installing Node Type** is set to **Application**. Name of the network interface card (NIC) of the application node to be audited	test-rac-01
CPU Threshold (%)	Optional. This parameter is configurable when **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 when **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 when **Installing Node Type** is set to **Application**. OS of the application node to be audited. The value can be **LINUX64** or **WINDOWS64**.	LINUX64_X86

Step 7 Click **OK**. The agent is added to the node **RAC-Node-01**.

Repeat **Step 6** to add agents to the node **RAC-Node-02** and **RAC-Node-03** of the database **test01**. Expand the details of the database **test01** to view all added agents, as shown in **Figure 8-5**.

Example: The agent has been added to all the nodes in the database **test01** of the RAC cluster. The agent IDs are as follows: **p7U_dIQBUQf7E9XurmjX**, **rLVIdIQBUQf7E9Xug2iQ**, **rrVIdIQBUQf7E9Xu3Wja**

Figure 8-5 Viewing the added agents



	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
^	Name:test01 Type:ORACLE Version:11g	UTF8	172.16.0.50 1521	--	LINUX64	Disabled	Add	Enable | Delete

Agent ID	Installing...	Installing Nod...	OS	Audited ...	CPU Th...	Memor...	General	Status	SHA256Sum	Operation
-LyEfoQBd4Ai7vI72xUI	Application	172.16.0.55	LINUX64_...	--	80	80	No	Hibernatir	c16d8a2be97...	Download Agent | [
-ryFfoQBd4Ai7vI7KBVL	Application	172.16.0.15	LINUX64_...	--	80	80	No	Hibernatir	4bd4e25eb86...	Download Agent | [
_LyFfoQBd4Ai7vI7URXk	Application	172.16.0.105	LINUX64_...	--	80	80	No	Hibernatir	b760159852d...	Download Agent | [

	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
v	Name:test02 Type:ORACLE Version:11g	UTF8	172.16.0.10 1521	--	LINUX64	Disabled	Add	Enable | Delete
v	Name:test03 Type:ORACLE Version:11g	UTF8	172.16.0.100 1521	--	LINUX64	Disabled	Add	Enable | Delete

Step 8 Add agents to the databases **test02** and **test03**.

Locate the database **test02**, and click **Add** in the **Agent** column.

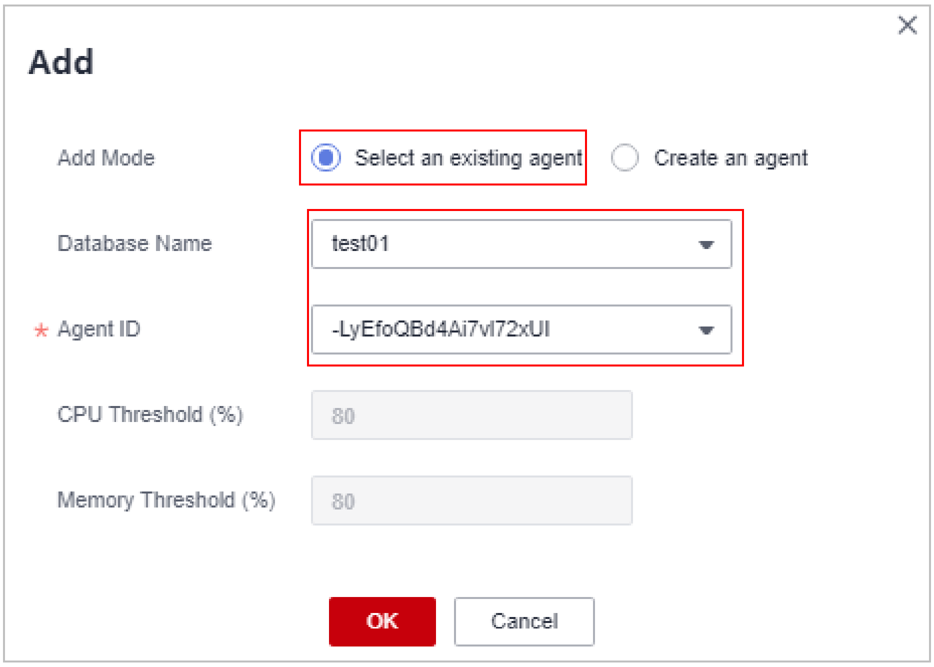
Step 9 In the dialog box that is displayed, enter the information about the agent to be added, as shown in **Table 8-4**.

Example: Add an agent to the database **test02**.

NOTE

Select the agent that has been added to the database **test01** and add it to the database **test02**.

Figure 8-6 Adding an existing agent



Add

Add Mode ● Select an existing agent ○ Create an agent

Database Name: test01

* Agent ID: -LyEfoQBd4Ai7vI72xUI

CPU Threshold (%): 80

Memory Threshold (%): 80

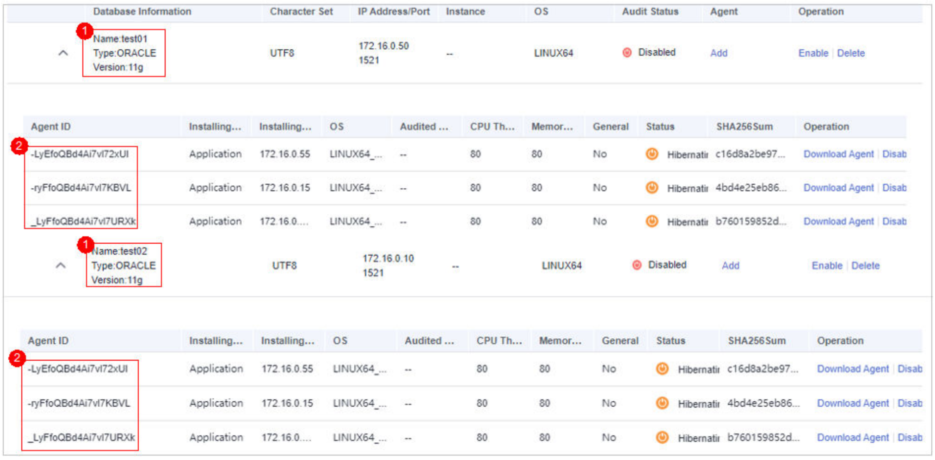
Table 8-4 Parameters for adding an existing agent

Parameter	Description	Example Value
Add Mode	Method of adding an agent. The options are as follows: ● **Select an existing agent** ● **Create an agent**	Selecting an existing agent
Database Name	Select a database that has added an agent. **Example**: **test01**	test01
AgentID	Select an agent ID of the selected database. **Example**: Three nodes of the database **test01** have added agents. You need to select one agent at a time and add the three agents in sequence.	p7U_dIQBUQf7E9XurmjX

Step 10 Click **OK**. An existing agent is added to the database **test02**.

Repeat **Step 8** and **Step 9** to add the other two agents. After the agents are added, check whether the database **test01** and **test02** contain the same agents.

Figure 8-7 Checking the agent information



Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
Name:test01 Type:ORACLE Version:11g	UTF8	172.16.0.50 1521	--	LINUX64	Disabled	Add	Enable | Delete

Agent ID	Installing...	Installing...	OS	Audited ...	CPU Th...	Memor...	General	Status	SHA256Sum	Operation
-LyEfoQBd4Ai7vI72xUI	Application	172.16.0.55	LINUX64_...	--	80	80	No	Hibernatir	c16d8a2be97...	Download Agent | Disab
-ryFfoQBd4Ai7vI7KBVL	Application	172.16.0.15	LINUX64_...	--	80	80	No	Hibernatir	4bd4e25eb86...	Download Agent | Disab
_LyFfoQBd4Ai7vI7URXk	Application	172.16.0....	LINUX64_...	--	80	80	No	Hibernatir	b760159852d...	Download Agent | Disab

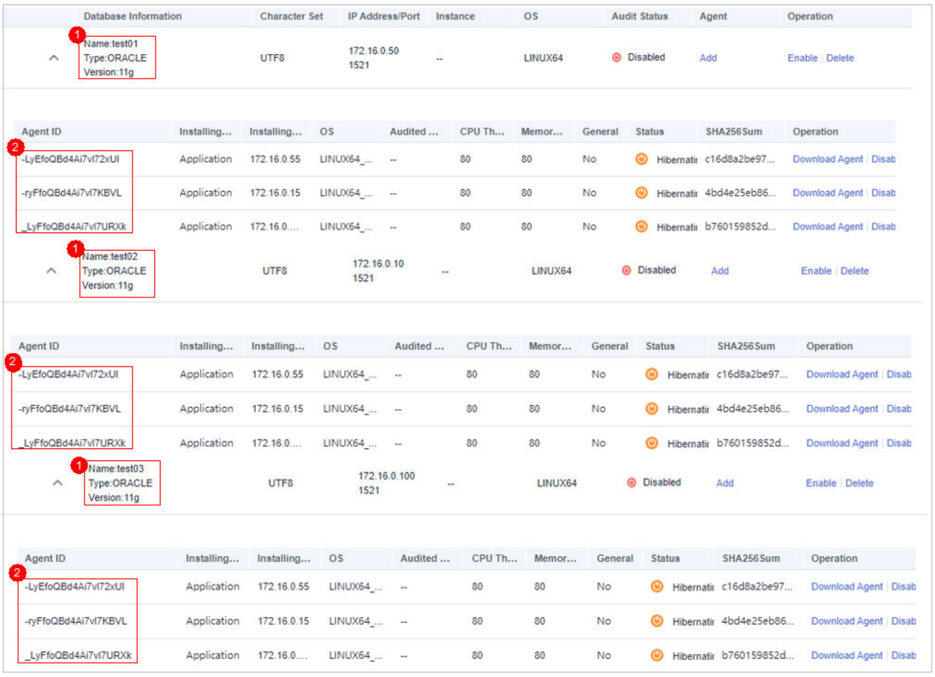
Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
Name:test02 Type:ORACLE Version:11g	UTF8	172.16.0.10 1521	--	LINUX64	Disabled	Add	Enable | Delete

Agent ID	Installing...	Installing...	OS	Audited ...	CPU Th...	Memor...	General	Status	SHA256Sum	Operation
-LyEfoQBd4Ai7vI72xUI	Application	172.16.0.55	LINUX64_...	--	80	80	No	Hibernatir	c16d8a2be97...	Download Agent | Disab
-ryFfoQBd4Ai7vI7KBVL	Application	172.16.0.15	LINUX64_...	--	80	80	No	Hibernatir	4bd4e25eb86...	Download Agent | Disab
_LyFfoQBd4Ai7vI7URXk	Application	172.16.0....	LINUX64_...	--	80	80	No	Hibernatir	b760159852d...	Download Agent | Disab

Step 11 Repeat **Step 8** to **Step 10** to add agents to the database **test03**. Ensure that the agents of all databases in the RAC cluster are the same.

Example: After the cluster is deployed, add the the same agents to the databases **test01**, **test02**, and **test03** and ensure that the number of agents in each database is the same as the number of nodes in the cluster.

Figure 8-8 Checking the agent information



	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
^	Name:test01 Type:ORACLE Version:11g	UTF8	172.16.0.50 1521	--	LINUX64	Disabled	Add	Enable | Delete

Agent ID	Installing...	Installing...	OS	Audited ...	CPU Th...	Memor...	General	Status	SHA256Sum	Operation
-LyEfoQBd4Ai7vl72xUI	Application	172.16.0.55	LINUX64_...	--	80	80	No	Hibernati	c16d8a2be97...	Download Agent | Disab
-ryFfoQBd4Ai7vl7KBVL	Application	172.16.0.15	LINUX64_...	--	80	80	No	Hibernati	4bd4e25eb86...	Download Agent | Disab
_LyFfoQBd4Ai7vl7URXk	Application	172.16.0....	LINUX64_...	--	80	80	No	Hibernati	b760159852d...	Download Agent | Disab

^	Name:test02 Type:ORACLE Version:11g	UTF8	172.16.0.10 1521	--	LINUX64	Disabled	Add	Enable | Delete

Agent ID	Installing...	Installing...	OS	Audited ...	CPU Th...	Memor...	General	Status	SHA256Sum	Operation
-LyEfoQBd4Ai7vl72xUI	Application	172.16.0.55	LINUX64_...	--	80	80	No	Hibernati	c16d8a2be97...	Download Agent | Disab
-ryFfoQBd4Ai7vl7KBVL	Application	172.16.0.15	LINUX64_...	--	80	80	No	Hibernati	4bd4e25eb86...	Download Agent | Disab
_LyFfoQBd4Ai7vl7URXk	Application	172.16.0....	LINUX64_...	--	80	80	No	Hibernati	b760159852d...	Download Agent | Disab

^	Name:test03 Type:ORACLE Version:11g	UTF8	172.16.0.100 1521	--	LINUX64	Disabled	Add	Enable | Delete

Agent ID	Installing...	Installing...	OS	Audited ...	CPU Th...	Memor...	General	Status	SHA256Sum	Operation
-LyEfoQBd4Ai7vl72xUI	Application	172.16.0.55	LINUX64_...	--	80	80	No	Hibernati	c16d8a2be97...	Download Agent | Disab
-ryFfoQBd4Ai7vl7KBVL	Application	172.16.0.15	LINUX64_...	--	80	80	No	Hibernati	4bd4e25eb86...	Download Agent | Disab
_LyFfoQBd4Ai7vl7URXk	Application	172.16.0....	LINUX64_...	--	80	80	No	Hibernati	b760159852d...	Download Agent | Disab

Step 12 After the cluster databases and agents are configured, you can add security group rules, download and install agents, and enable the audit function.

For details, see **Adding a Security Group Rule**, **Downloading and Installing an Agent**, and **Enabling Database Audit**.

----End

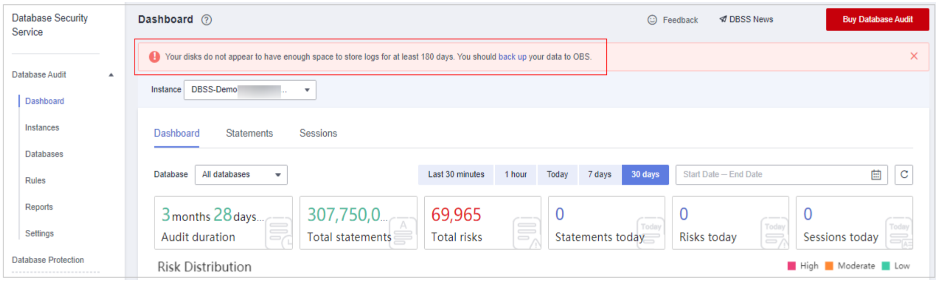
9 Meeting Database Audit Compliance Requirements

To meet compliance requirements, DBSS allows you to configure the retention period for audit logs, audit reports, and privacy audit logs

Configuring Audit Log Retention Duration

According to relevant audit laws and regulations, audit logs must be retained for at least half a year. DBSS automatically predicts whether the remaining storage space of the audit instance meets the compliance requirements. If the remaining storage space is insufficient, a message is displayed.

Figure 9-1 Insufficient disk space notice



Your disks do not appear to have enough space to store logs for at least 180 days. You should back up your data to OBS.

Instance: DBSS-Demo[redacted]..

Database: All databases

30 days

3 months 28 days... Audit duration

307,750,0... Total statements

69,965 Total risks

0 Statements today

0 Risks today

0 Sessions today

If the message shown in **Figure 9-1** is displayed, enable automatic backup. For details, see **Automatically Backing Up Database Audit Logs**.

NOTE

If automatic backup is enabled, set **Backup Period** to **Hourly**.

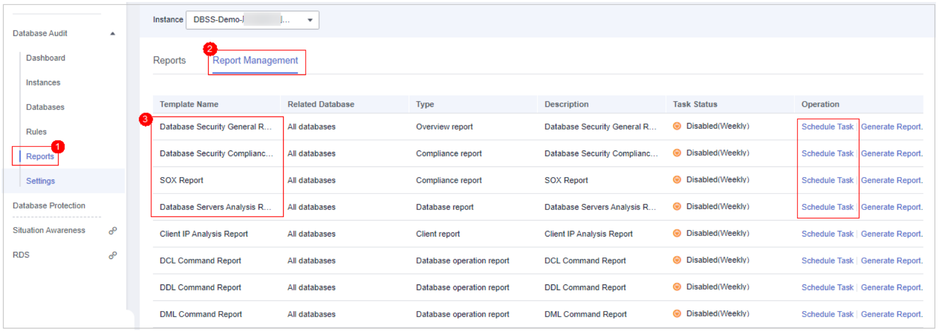
If the total size of backup files generated every day is less than 50 MB, you are advised to select **Daily**.

Configuring Audit Reports

To check whether compliance requirements are met in a timely and accurate manner, you are advised to enable audit report for schedule tasks.

You are advised to configure reports as shown in **Figure 9-2**.

Figure 9-2 Report Management tab page

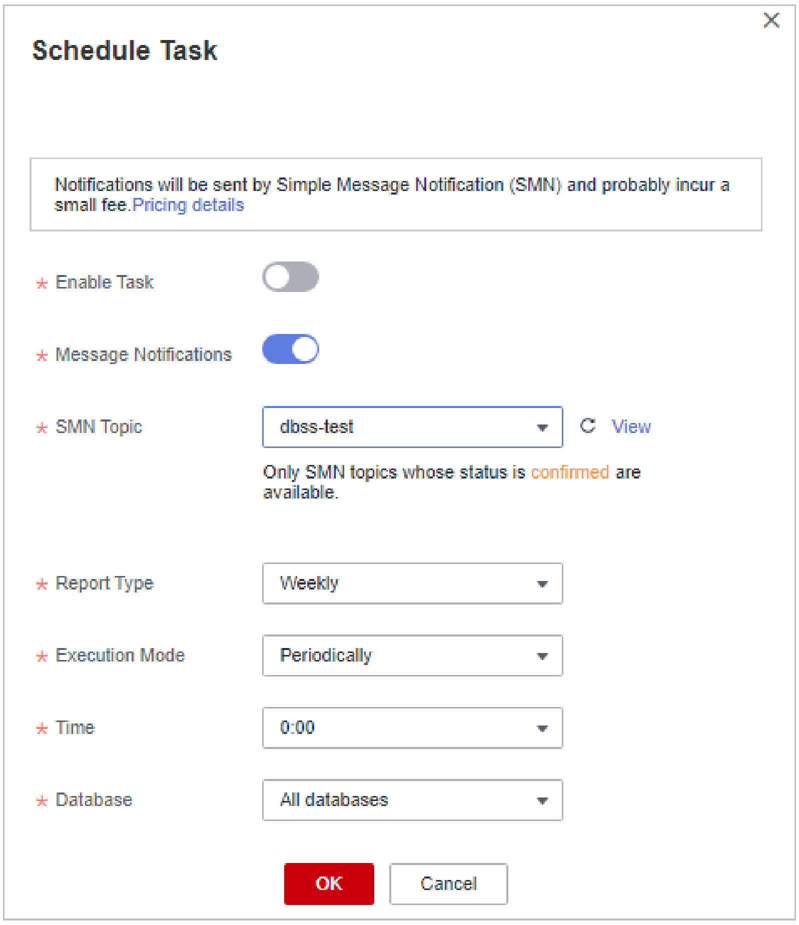


Instance DBSS-Demo-[redacted]...

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

Locate a report and click **Schedule Task** in the **Operation** column. For more information, see **Table 9-1**.

Figure 9-3 Configuring a schedule task



Schedule Task

Notifications will be sent by Simple Message Notification (SMN) and probably incur a small fee. Pricing details

* Enable Task: Off

* Message Notifications: On

* SMN Topic: dbss-test

Only SMN topics whose status is confirmed are available.

* Report Type: Weekly

* Execution Mode: Periodically

* Time: 0:00

* Database: All databases

Table 9-1 Parameters for schedule tasks

Parameter	Description	Example Value
Enable Task	Whether to start the current task. - Disabled: ○ - Enabled: ●	●
Message Notifications	Whether to send a notification after a report is generated. - Disabled: ○ - Enabled: ●	●
SMN Topic	If **Message Notifications** is enabled, select a message notification topic.	-
Report Type	Select the frequency for generating reports. - **Daily**: If more than 10 million audit logs are generated daily, you are advised to select **Daily**. - **Weekly**: If 10,000 to 10 million audit logs are generated daily, you are advised to select **Weekly**. - **Monthly**: If less than 10,000 audit logs are generated daily, you are advised to select **Monthly**.	Weekly
Execution Mode	Number of times a scheduled task is executed. - **Periodically**: The scheduled task is executed periodically based on the report type. - **Once**: The scheduled task is executed once only.	Periodically
Time	Select an execution time, which can only be the top of an hour. A task will be automatically executed after being created. You are advised to select off-peak hours, for example, in the early morning.	2:00
Database	Select the database where the task is to be executed. You can select all databases or a specified database.	All databases

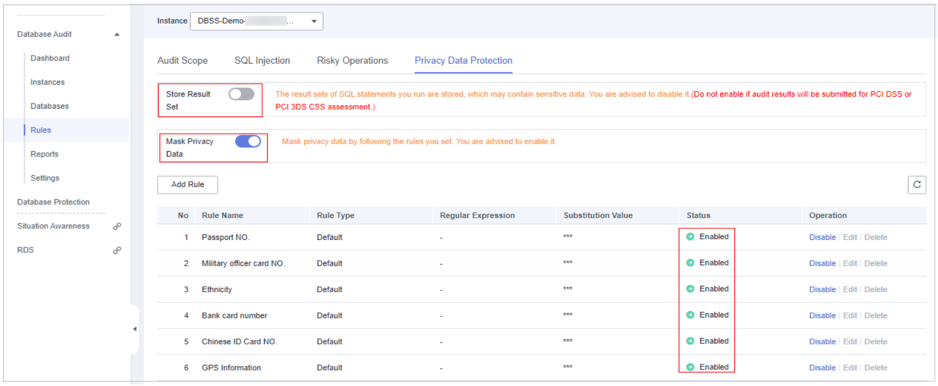
Configuring Privacy Data Protection

The SQL request statements and result sets in audit logs may contain users' privacy data. Therefore, you are advised to enable privacy data protection for audit logs.

Configure the following functions to meet privacy data compliance requirements:

- Toggle on **Mask Privacy Data**. Privacy data in audit logs is masked for storage.
- Toggle off **Store Result Set**. Result sets that contain privacy information will not be stored in audit logs.
- Enable all privacy protection rules.

Figure 9-4 Configuring privacy data protection



Instance: DBSS-Demo-[redacted]...

Store Result Set: off

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

Mask Privacy Data: on

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

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

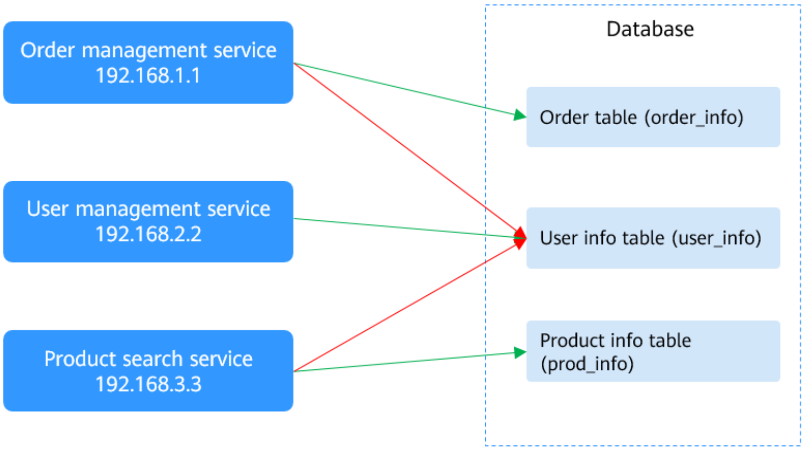
10 Configuring Database Audit Instance Rules

You can configure audit rules to detect database risks. To get notified of risks, you also need to **Configuring Alarm Notifications**.

Scenario 1: Detecting Abnormal Access to Important Tables

Example: An e-commerce website has multiple microservices in the backend, including order management, user management, and offering search. These services are deployed on different nodes and have different IP addresses, as shown in **Figure 10-1**.

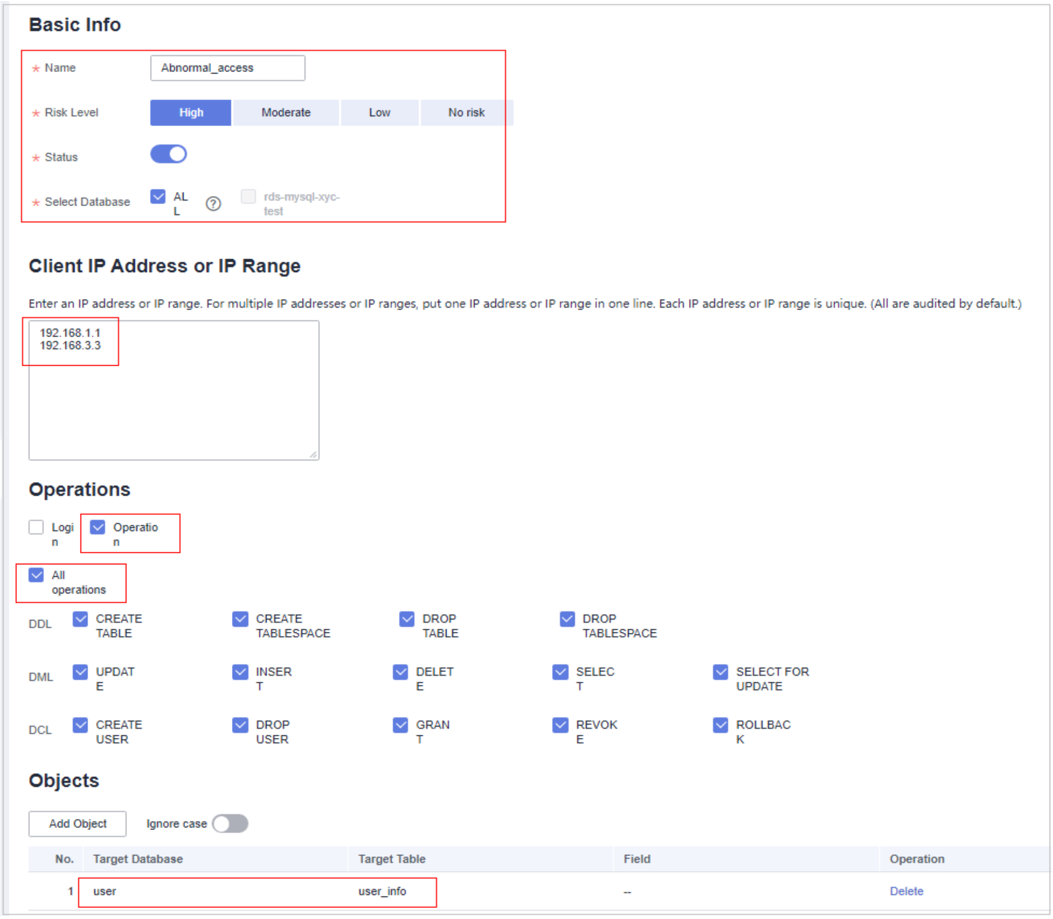
Figure 10-1 Service deployment



The green arrows indicate the access paths. If the order management service or product search service node is attacked, the attacker will access the user information tables from the intruded node. Such access is abnormal.

DBSS allows you to set the following rule to detect abnormal database access.

Figure 10-2 Adding abnormal database access



Basic Info

* Name: Abnormal_access

* Risk Level: High | Moderate | Low | No risk

* Status

* Select Database ☑ ALL ⓘ □ rds-mysql-xyc-test

Client IP Address or IP Range

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

```
192.168.1.1
192.168.3.3
```

Operations

□ Login ☑ Operation

☑ All operations

DDL	☑ CREATE TABLE	☑ CREATE TABLESPACE	☑ DROP TABLE	☑ DROP TABLESPACE	
DML	☑ UPDATE	☑ INSERT	☑ DELETE	☑ SELECT	☑ SELECT FOR UPDATE
DCL	☑ CREATE USER	☑ DROP USER	☑ GRANT	☑ REVOKE	☑ ROLLBACK

Objects

Add Object Ignore case

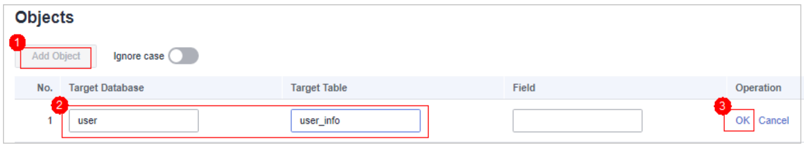
No.	Target Database	Target Table	Field	Operation
1	user	user_info	--	Delete

The rule shown in Figure 10-2 indicates that all requests sent from **192.168.1.1** or **192.168.3.3** to the **user_info** table are regarded highly risky.

After this rule is set, all abnormal access to the high-risk table will be audited, and risk alarms will be triggered.

Click **Add Object**, enter the target database and target table, and click **OK**.

Figure 10-3 Adding a target table



Objects

Add Object Ignore case

No.	Target Database	Target Table	Field	Operation
1	user	user_info		OK Cancel

Scenario 2: Optimizing SQL Statements

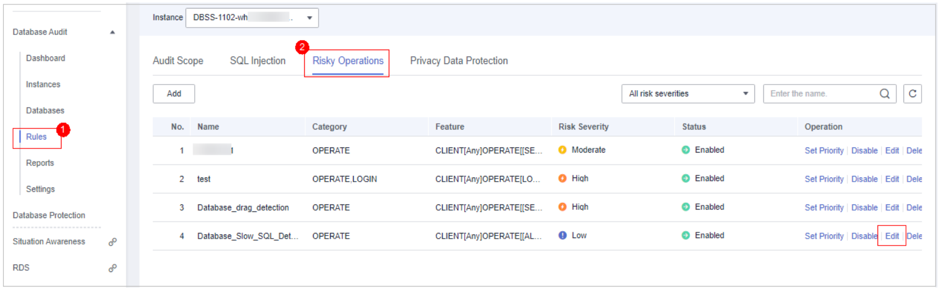
Example: An application responds slowly when users perform some operations. It is found that latency occurs when the application accesses the database. However, the statements that cause the latency cannot be identified.

In this case, you can use the database slow SQL detection function of DBSS to locate the fault and optimize the performance.

Perform the following steps:

Step 1 Log in to the DBSS console and choose the **Risky Operation** tab.

Figure 10-4 Accessing the Risky Operations tab page

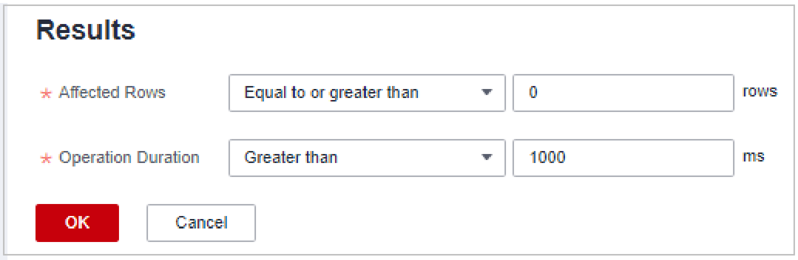


Instance DBSS-1102-wh[redacted].

No.	Name	Category	Feature	Risk Severity	Status	Operation
1	[redacted]1	OPERATE	CLIENT[Any]OPERATE[[SE...	Moderate	Enabled	Set Priority | Disable | Edit | Dele
2	test	OPERATE,LOGIN	CLIENT[Any]OPERATE[LO...	High	Enabled	Set Priority | Disable | Edit | Dele
3	Database_drag_detection	OPERATE	CLIENT[Any]OPERATE[[SE...	High	Enabled	Set Priority | Disable | Edit | Dele
4	Database_Slow_SQL_Det...	OPERATE	CLIENT[Any]OPERATE[[AL...	Low	Enabled	Set Priority | Disable | Edit | Dele

Step 2 Locate **Database_Slow_SQL_Detection** and click **Edit** in the **Operation** column. In the **Results** dialog box that is displayed, set **Operation Duration** to **Greater than 1000 ms**.

Figure 10-5 Setting the operation duration



Results

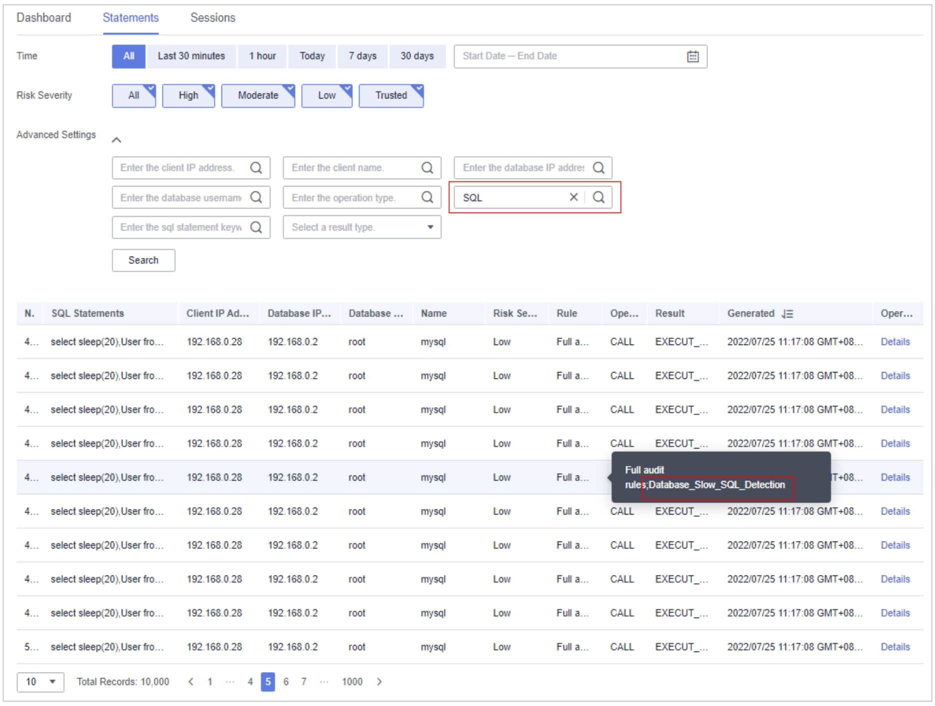
* Affected Rows: Equal to or greater than 0 rows

* Operation Duration: Greater than 1000 ms

Step 3 Click **OK**.

Step 4 After the configuration is complete, wait for a while and search for the slow SQL detection rule by its name. For example, enter **SQL** in the **Rule Name** search box on the **Statements** tab page.

Figure 10-6 Slow SQL detection results



Time: **All** | Last 30 minutes | 1 hour | Today | 7 days | 30 days | Start Date -- End Date

Risk Severity: All | High | Moderate | Low | Trusted

Advanced Settings

Enter the client IP address. | Enter the client name. | Enter the database IP addres

Enter the database usernam | Enter the operation type. | SQL

Enter the sql statement keyw | Select a result type.

Search

N.	SQL Statements	Client IP Ad...	Database IP...	Database ...	Name	Risk Se...	Rule	Ope...	Result	Generated	Oper...
4...	select sleep(20),User fro...	192.168.0.28	192.168.0.2	root	mysql	Low	Full a...	CALL	EXECUT_...	2022/07/25 11:17:08 GMT+08...	Details
4...	select sleep(20),User fro...	192.168.0.28	192.168.0.2	root	mysql	Low	Full a...	CALL	EXECUT_...	2022/07/25 11:17:08 GMT+08...	Details
4...	select sleep(20),User fro...	192.168.0.28	192.168.0.2	root	mysql	Low	Full a...	CALL	EXECUT_...	2022/07/25 11:17:08 GMT+08...	Details
4...	select sleep(20),User fro...	192.168.0.28	192.168.0.2	root	mysql	Low	Full a...	CALL	EXECUT_...	2022/07/25 11:17:08 GMT+08...	Details
4...	select sleep(20),User fro...	192.168.0.28	192.168.0.2	root	mysql	Low	Full a...			T+08...	Details
4...	select sleep(20),User fro...	192.168.0.28	192.168.0.2	root	mysql	Low	Full a...	CALL	EXECUT_...	2022/07/25 11:17:08 GMT+08...	Details
4...	select sleep(20),User fro...	192.168.0.28	192.168.0.2	root	mysql	Low	Full a...	CALL	EXECUT_...	2022/07/25 11:17:08 GMT+08...	Details
4...	select sleep(20),User fro...	192.168.0.28	192.168.0.2	root	mysql	Low	Full a...	CALL	EXECUT_...	2022/07/25 11:17:08 GMT+08...	Details
4...	select sleep(20),User fro...	192.168.0.28	192.168.0.2	root	mysql	Low	Full a...	CALL	EXECUT_...	2022/07/25 11:17:08 GMT+08...	Details
5...	select sleep(20),User fro...	192.168.0.28	192.168.0.2	root	mysql	Low	Full a...	CALL	EXECUT_...	2022/07/25 11:17:08 GMT+08...	Details

Full audit rules;Database_Slow_SQL_Detection

10 Total Records: 10,000 < 1 ··· 4 5 6 7 ··· 1000 >

NOTE

- You can analyze the search result and optimize the SQL statements.
- You can gradually decrease the value of **Operation Duration** and perform multiple rounds of optimization.

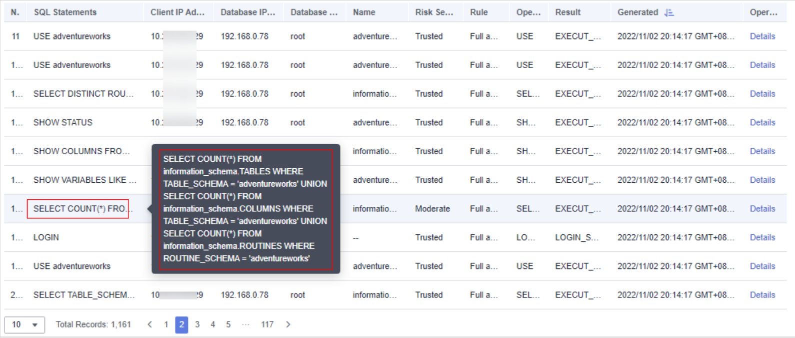
----End

Scenario 3: Adding a Whitelist to Reduce False Positive SQL Injection Alarms

DBSS provides the SQL injection detection function and built-in SQL injection detection rules. You can also add SQL injection detection rules.

Example: A normal statement generated by an internal program hits an SQL injection rule, as shown in **Figure 10-7**.

Figure 10-7 False positive SQL injection alarm



N.	SQL Statements	Client IP Ad...	Database IP...	Database ...	Name	Risk Se...	Rule	Ope...	Result	Generated	Oper...
11	USE adventureworks	10.[redacted]29	192.168.0.78	root	adventure...	Trusted	Full a...	USE	EXECUT_...	2022/11/02 20:14:17 GMT+08...	Details
1...	USE adventureworks	10.[redacted]29	192.168.0.78	root	adventure...	Trusted	Full a...	USE	EXECUT_...	2022/11/02 20:14:17 GMT+08...	Details
1...	SELECT DISTINCT ROU...	10.[redacted]29	192.168.0.78	root	informatio...	Trusted	Full a...	SEL...	EXECUT_...	2022/11/02 20:14:17 GMT+08...	Details
1...	SHOW STATUS	10.[redacted]29	192.168.0.78	root	adventure...	Trusted	Full a...	SH...	EXECUT_...	2022/11/02 20:14:17 GMT+08...	Details
1...	SHOW COLUMNS FRO...				informatio...	Trusted	Full a...	SH...	EXECUT_...	2022/11/02 20:14:17 GMT+08...	Details
1...	SHOW VARIABLES LIKE ...				adventure...	Trusted	Full a...	SH...	EXECUT_...	2022/11/02 20:14:17 GMT+08...	Details
1...	SELECT COUNT(*) FRO...				informatio...	Moderate	Full a...	SEL...	EXECUT_...	2022/11/02 20:14:17 GMT+08...	Details
1...	LOGIN				--	Trusted	Full a...	LO...	LOGIN_S...	2022/11/02 20:14:17 GMT+08...	Details
1...	USE adventureworks				adventure...	Trusted	Full a...	USE	EXECUT_...	2022/11/02 20:14:17 GMT+08...	Details
2...	SELECT TABLE_SCHEM...	10[redacted]29	192.168.0.78	root	informatio...	Trusted	Full a...	SEL...	EXECUT_...	2022/11/02 20:14:17 GMT+08...	Details

```
SELECT COUNT(*) FROM
information_schema.TABLES WHERE
TABLE_SCHEMA = 'adventureworks' UNION
SELECT COUNT(*) FROM
information_schema.COLUMNS WHERE
TABLE_SCHEMA = 'adventureworks' UNION
SELECT COUNT(*) FROM
information_schema.ROUTINES WHERE
ROUTINE_SCHEMA = 'adventureworks'
```

10 Total Records: 1,161 < 1 2 3 4 5 ··· 117 >

You can add this SQL statement to the whitelist, so that DBSS will no longer report alarms on it.

NOTE

The priority of risky operation rules is higher than that of SQL injection rules.

As shown in **Figure 10-7**, the executed SQL statement is as follows:

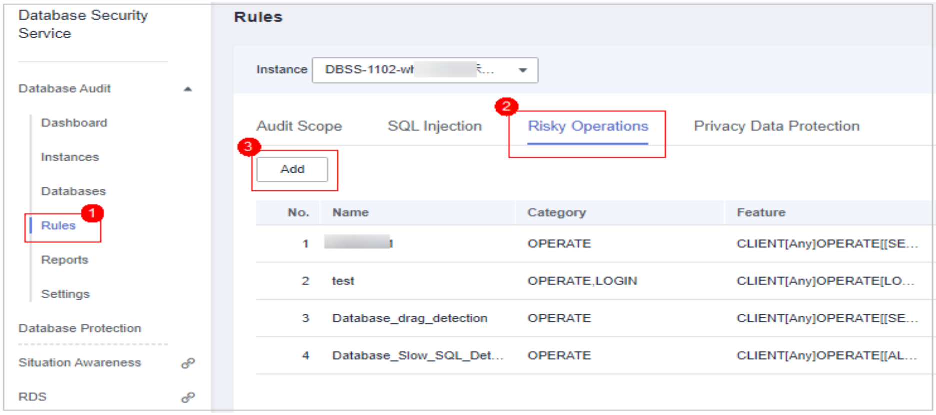
SELECT COUNT(*) FROM information_schema.TABLES WHERE TABLE_SCHEMA = 'adventureworks' UNION SELECT COUNT(*) FROM information_schema.COLUMNS WHERE TABLE_SCHEMA = 'adventureworks' UNION SELECT COUNT(*) FROM information_schema.ROUTINES WHERE ROUTINE_SCHEMA = 'adventureworks'

This statement uses the **SELECT** statement to access the **TABLES** table in the **information_schema** database.

Procedure

Step 1 Access the **Risky Operations** tab page.

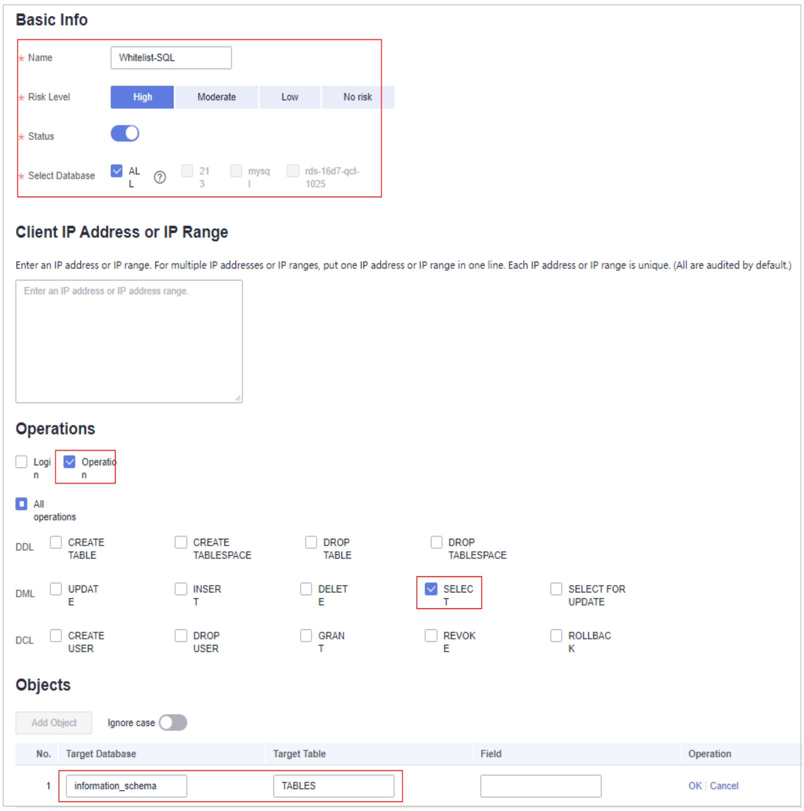
Figure 10-8 Accessing the Risky Operations tab page



No.	Name	Category	Feature
1	[redacted]	OPERATE	CLIENT[Any]OPERATE[[SE...
2	test	OPERATE,LOGIN	CLIENT[Any]OPERATE[LO...
3	Database_drag_detection	OPERATE	CLIENT[Any]OPERATE[[SE...
4	Database_Slow_SQL_Det...	OPERATE	CLIENT[Any]OPERATE[[AL...

Step 2 Click **Add** and enter rule information.

Figure 10-9 Setting a rule



Basic Info

- * Name: Whitelist-SQL
- * Risk Level: High | Moderate | Low | No risk (High selected)
- * Status: on
- * Select Database: ☑ ALL □ 213 □ mysql □ rds-16d7-qct-1025

Client IP Address or IP Range

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

Enter an IP address or IP address range.

Operations

□ Login ☑ Operation

■ All operations

DDL	□ CREATE TABLE	□ CREATE TABLESPACE	□ DROP TABLE	□ DROP TABLESPACE	
DML	□ UPDATE	□ INSERT	□ DELETE	☑ SELECT	□ SELECT FOR UPDATE
DCL	□ CREATE USER	□ DROP USER	□ GRANT	□ REVOKE	□ ROLLBACK

Objects

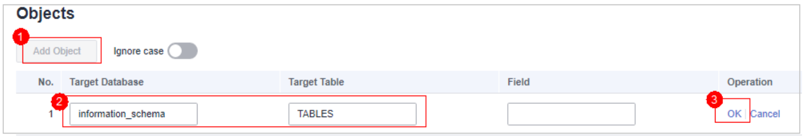
Add Object   Ignore case

No.	Target Database	Target Table	Field	Operation
1	information_schema	TABLES		OK | Cancel

As shown in **Figure 10-9**, the rule indicates that the **SELECT** statement executed in the **TABLES** table in the **information_schema** database is safe.

Click **Add Object**, enter the target database and target table, and click **OK**.

Figure 10-10 Adding an object to the SQL injection whitelist



Objects

Add Object   Ignore case

No.	Target Database	Target Table	Field	Operation
1	information_schema	TABLES		OK Cancel

Step 3 Click **OK**.

After the configuration is complete, the statement will no longer be regarded as risky or trigger an alarm.

----End

A Change History

Released On	Description
2022-11-18	This issue is the ninth official release. Added: ● **Auditing an RDS DB Instance (Without Agents)** ● **Configuring Oracle RAC Cluster Audit** ● **Meeting Database Audit Compliance Requirements** ● **Configuring Database Audit Instance Rules** Modified: ● **Auditing an RDS DB instance (with Agents)**
2021-12-31	This issue is the eighth official release. Added **Checking for Dirty Tables**.
2021-08-30	This issue is the seventh official release. Added **Deploying the Database Audit Agent in a Container**. Changed the entry of the service list on the console to **Security & Compliance**.
2021-03-23	This issue is the sixth official release. Added the section about configuring data reduction rule in **Checking for Data Reduction**.

Released On	Description
2020-12-25	This issue is the fifth official release. - Added **Checking for Slow SQL Statements**. - Added **Checking for Data Reduction**.
2020-12-21	This issue is the fourth official release. - Added the description about setting a security group rule in **Auditing a User-built Database on ECS**. - Added the description about setting a security group rule in **Auditing an RDS DB instance (with Agents)**.
2020-05-20	This issue is the third official release. Updated some screenshots.
2020-02-24	This is the second official release. Modified descriptions in this document.
2019-09-18	This is the first official release.