

Database Security Service

Best Practices

Issue 1.0
Date 2022-09-30



Copyright © Huawei Technologies Co., Ltd. 2023. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei 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

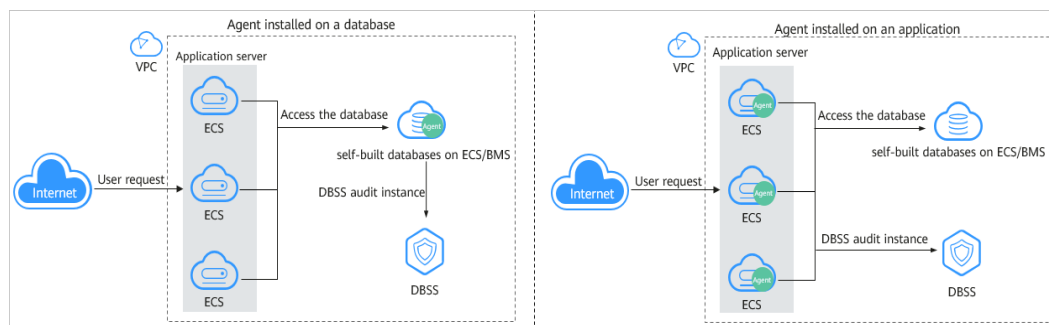
1 Auditing a User-built Database on ECS.....	1
2 Auditing an RDS DB instance (with Agents).....	8
3 Auditing an RDS DB Instance (Without Agents).....	16
4 Deploying the Database Audit Agent in a Container.....	21
4.1 Scenario.....	21
4.2 Adding a Database and Exporting Database Configurations.....	22
4.3 Installing the Agent on CCE Cluster Nodes.....	24
4.3.1 Importing Configurations to OBS.....	24
4.3.2 Creating a ConfigMap.....	25
4.3.3 Creating an Agent DaemonSet Workload.....	26
4.4 Enabling Database Audit.....	29
4.5 Checking Audit Results.....	29
5 Checking for Slow SQL Statements.....	32
6 Checking for Data Reduction.....	35
7 Checking for Dirty Tables.....	40
A Change History.....	44

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

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	192.168.0.32.3 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 X

Add Mode Select an existing agent Create an agent

Installing Node Type Database Application

OS Linux 64-bit ▼

CPU Threshold (%) 80

Memory Threshold (%) 80

OK Cancel

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

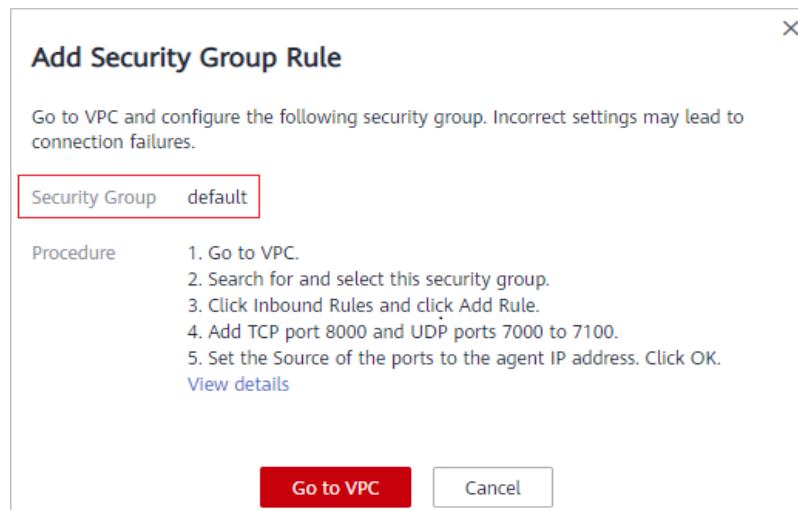
You can configure security group rules before or after installing an agent.

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



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	UTF8	192.168.1.31 8000	--	LINUX64	Enabled	Add	Disable	Delete
Version: 7.4										
Agent ID	Installin...	Installin...	OS	Audited...	CPU T...	Memo...	Gen...	Status	Operation	
AXGHb4BA7L_qYimCkNo-	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	<div style="width: 100%; height: 10px; background-color: #0070c0;"></div> 100%	Preview More ▾
DML Command Report	All databases	Weekly	2020/03/22 17:05:03 GMT+08:00	pdf	<div style="width: 100%; height: 10px; background-color: #0070c0;"></div> 100%	Preview Download Delete
DML Command Report	All databases	Weekly	2020/03/22 17:05:03 GMT+08:00	pdf	<div style="width: 100%; height: 10px; background-color: #0070c0;"></div> 100%	Preview Download Delete

----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

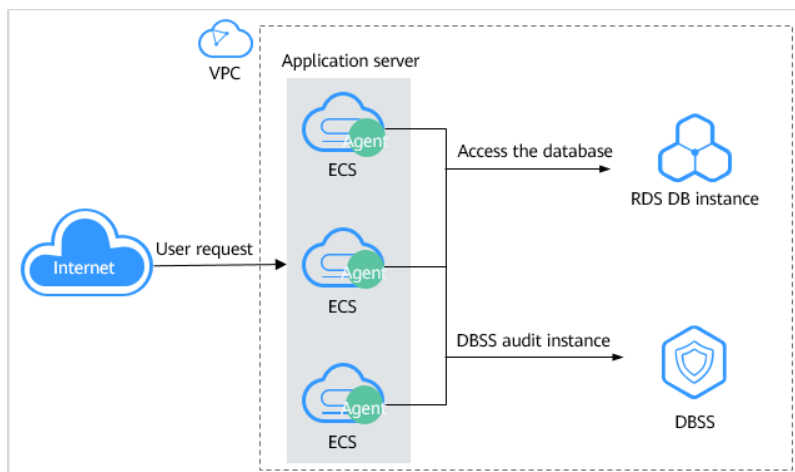
Database Type	Supported Edition
GaussDB(for MySQL)	All editions are supported by default.
RDS for MySQL	<ul style="list-style-type: none">• 5.6 (5.6.51.1 or later)• 5.7 (5.7.29.2 or later)• 8.0 (8.0.20.3 or later)

- 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.

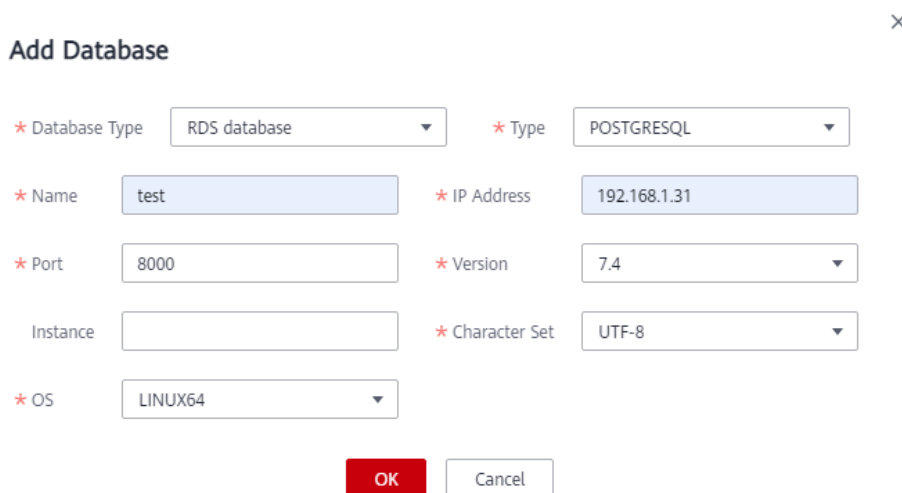
Step 3 In the navigation pane, choose **Databases**.

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



The screenshot shows the 'Add Database' dialog box with the following fields and values:

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

Buttons: OK, Cancel

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	192.168.0.32.3 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 Audited NIC Name

CPU Threshold (%) Memory Threshold (%)

OS

- **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 X

Add Mode Select an existing agent Create an agent

Database Name

* Agent ID

CPU Threshold (%)

Memory Threshold (%)

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

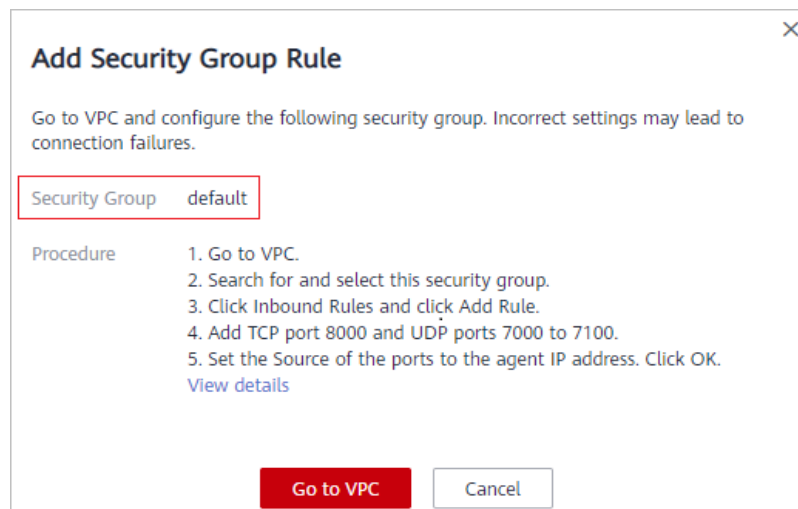
You can configure security group rules before or after installing an agent.

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



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.

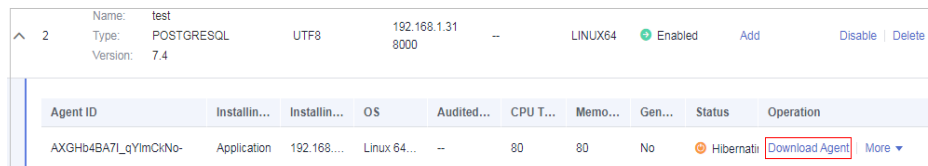
Step 1 Log in to the DBSS management console.

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

Name:	test								
Type:	POSTGRESQL	UTF8	192.168.1.31	--	LINUX64	Enabled	Add	Disable	Delete
Version:	7.4		8000						
Agent ID	Installin...	Installin...	OS	Audited...	CPU T...	Memo...	Gen...	Status	Operation
AXGHb4BA7I_qYImCkNo-	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%	Preview Download Delete
DML Command Report	All databases	Weekly	2020/03/22 17:05:03 GMT+08:00	pdf	100%	Preview Download Delete

----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 MySQL	<ul style="list-style-type: none">• 5.6 (5.6.51.1 or later)• 5.7 (5.7.29.2 or later)• 8.0 (8.0.20.3 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

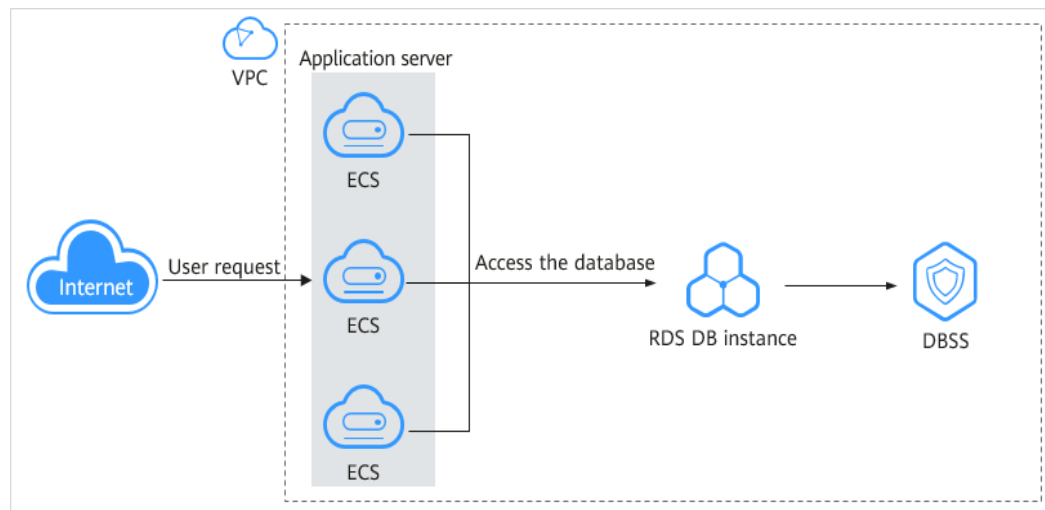
DBSS without agents is easy to configure and use, but the following functions are not supported:

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

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.


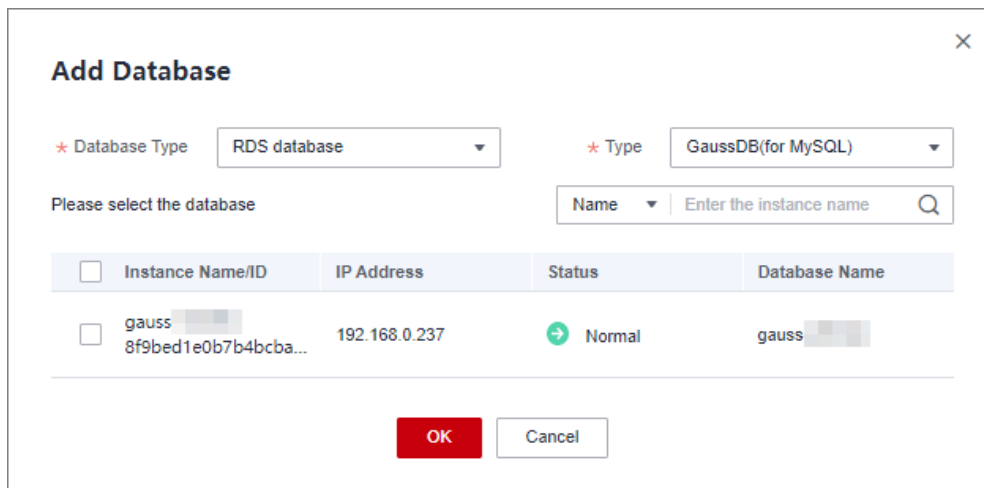
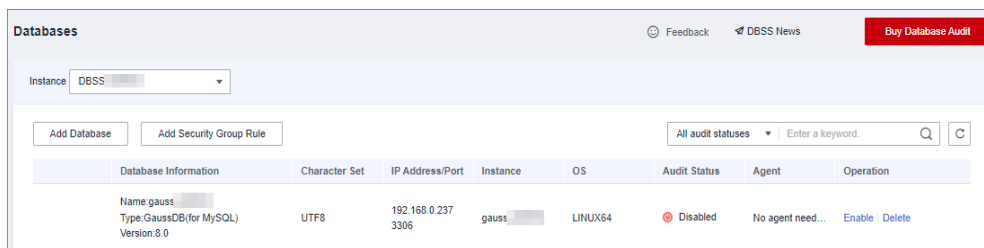
- Step 2** Select a region and click . Choose **Security & Compliance > Database Security Service**. The **Dashboard** page is displayed.
- Step 3** In the navigation pane, choose **Databases**.
- Step 4** Select an instance from the **Instance** drop-down list. Click **Add Database**.
- Step 5** In the displayed dialog box, set database parameters described in [Table 3-2](#).

Figure 3-2 Adding a database



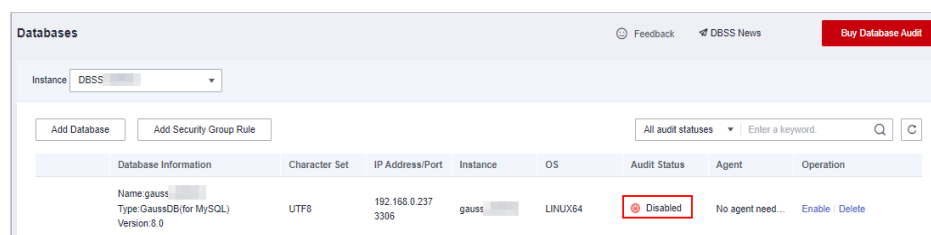
- Step 6** Click **OK**. The database will be displayed in the database list and its **Audit Status** will be **Disabled**.

Figure 3-3 Database list



- 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 8](#).

Figure 3-4 No agent needs to be added



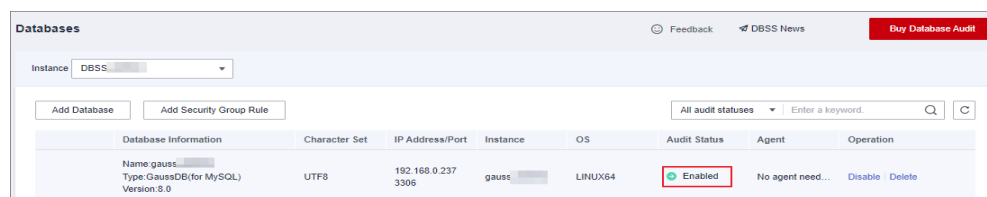
- If **Add** is displayed, the database can be audited only after an agent is added. In this case, click **Add** in the **Agent** column. For details, see [Auditing an RDS DB instance \(with Agents\)](#).

Figure 3-5 Adding an agent

No.	Database Information	Character Set	IP Address/P...	Instance	OS	Audit Status	Agent	Operation
1	Name: qb05 Type: MYSQL Version: 5.7	UTF8	192.168.0.73 3306	--	LINUX64	Enabled	Add	Disable Delete
2	Name: aw06 Type: MYSQL Version: 5.0	UTF8	192.168.0.32.3 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



----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.

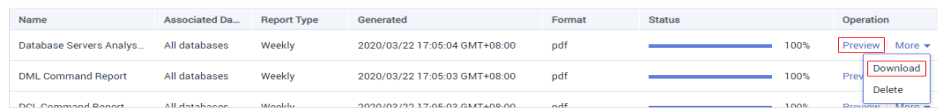
1. In the navigation pane, choose **Reports**.
2. Select an instance from the **Instance** drop-down list. Click the **Report Management** tab.
3. In the **Operation** column of a report template, click **Generate Report**.
4. In the displayed dialog box, click  to set the start time and end time of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



The screenshot shows a table with columns: Name, Associated Da..., Report Type, Generated, Format, Status, and Operation. The first row is 'Database Servers Analys...' with 'All databases' as the associated data, 'Weekly' as the report type, and a generated date of '2020/03/22 17:05:04 GMT+08:00'. The status is '100%'. The 'Operation' column for this row has a 'Preview' button highlighted with a red box. The second row is 'DML Command Report' with 'All databases' as the associated data, 'Weekly' as the report type, and a generated date of '2020/03/22 17:05:03 GMT+08:00'. The status is '100%'. The 'Operation' column for this row has a 'Download' button highlighted with a red box. A third row is partially visible below it.

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%	Preview Download Delete
DML Command Report	All databases	Weekly	2020/03/22 17:05:03 GMT+08:00	pdf	100%	Preview Download Delete

----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

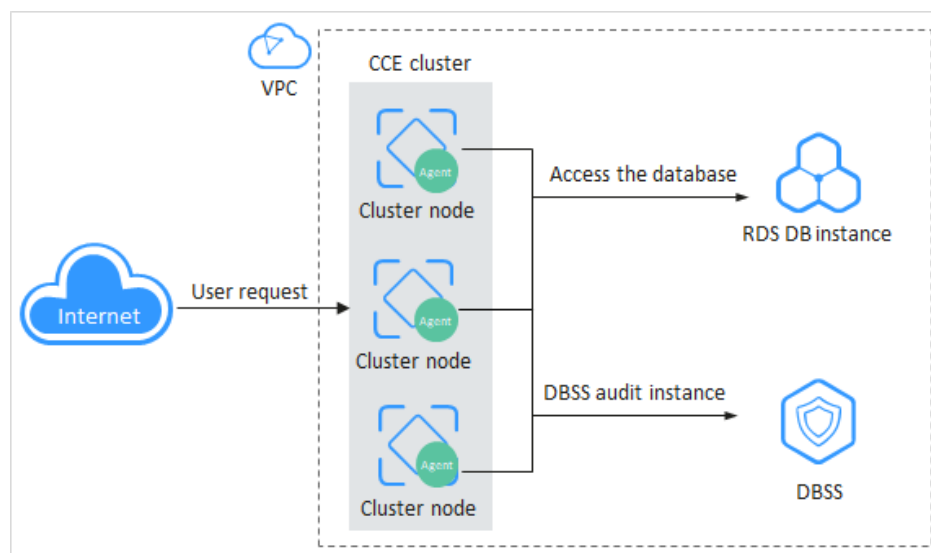
Cluster Name	scc-cmv-bj4
Namespace	default NOTE You can select an existing namespace or create one. A namespace is a collection of resources and objects. Multiple namespaces can be created in a single cluster, but they are isolated from each other. This enables namespaces to share the same cluster services 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.

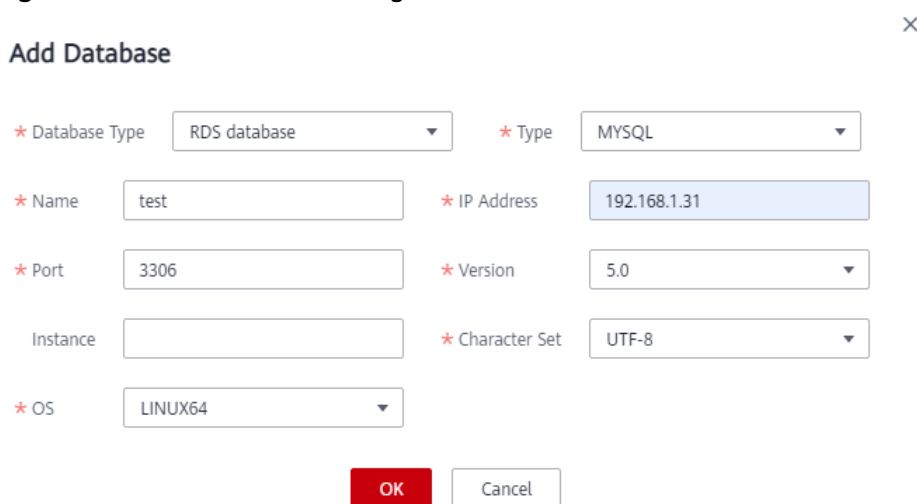
Step 3 In the navigation pane, choose **Databases**.

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 * Type

* Name * IP Address

* Port * Version

Instance

* OS * Character Set

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

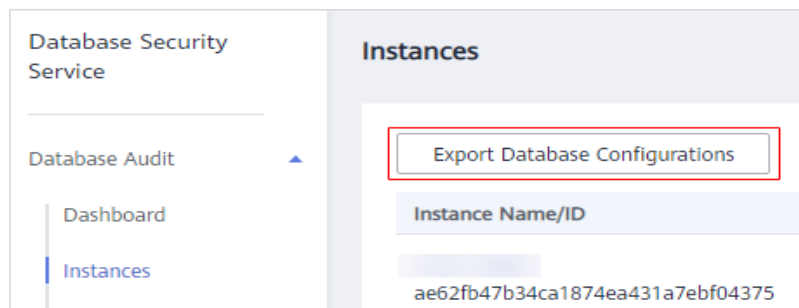
Export database configurations.

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



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.

For details, see [Configuring Keys](#).

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: <ol style="list-style-type: none"> 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

- **Command:** `top`

- **Args:** `-b`

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

- **Args:** `CLI`

- **Command:**

 - `/bin/bash`

 - `-c`

 - `tar xvf /tmp/dbss/agent/dbss_agent.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**.

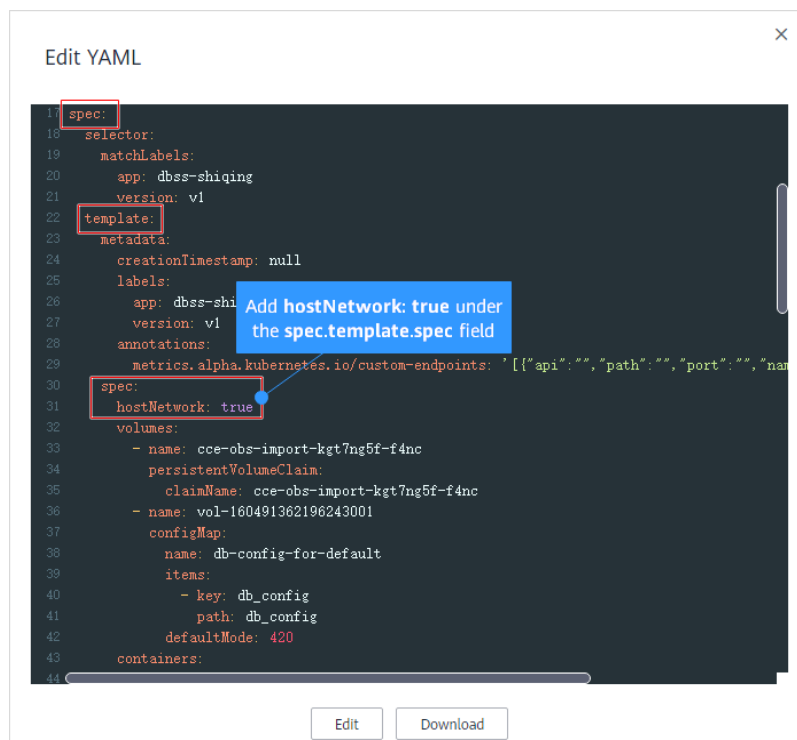
NOTE

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



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

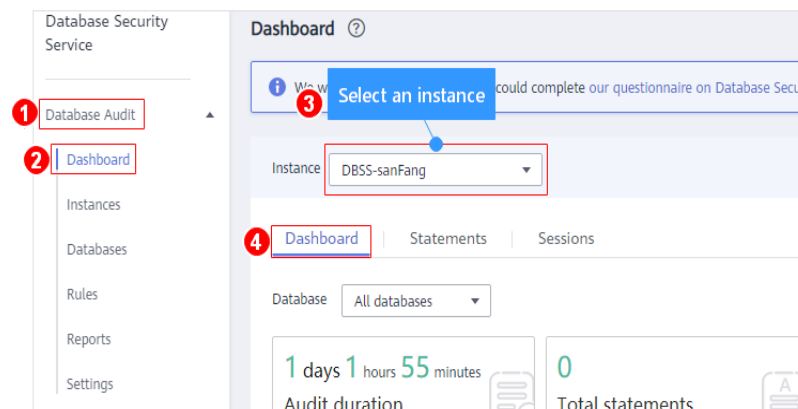
By default, database audit complies with a full audit rule, which is used to audit all databases that are successfully connected to database audit. You can check the audit statistics, including the overall audit statistics, risk distribution, session statistics, SQL distribution, and audit reports.

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

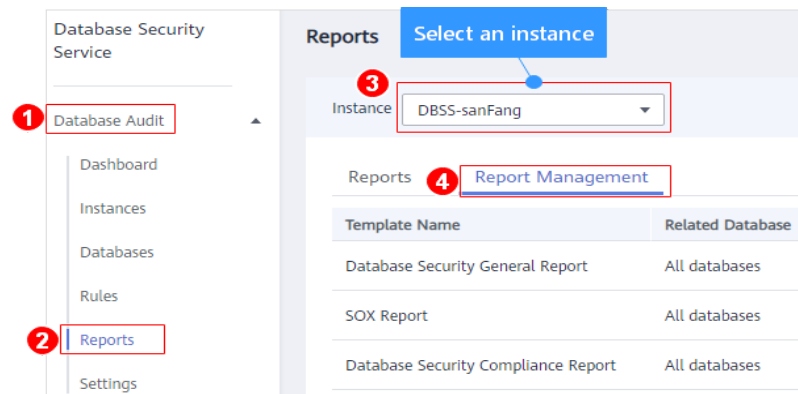



2. Click the **Statements** tab to view SQL statement information or the **Sessions** tab to view session distribution.

- 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



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%	Preview Download Delete
DCL Command Report	All databases	Weekly	2020/03/22 17:05:03 GMT+08:00	pdf	100%	Preview Download Delete

----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.

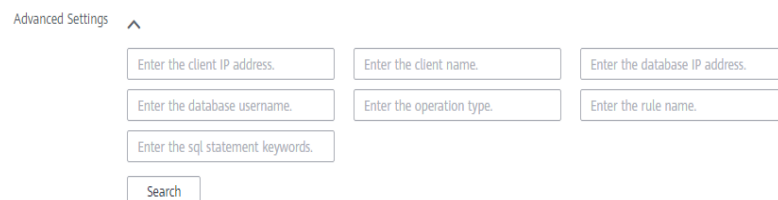
Step 6 Set filter criteria to query SQL statements.

- 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



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,
For details, see [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.


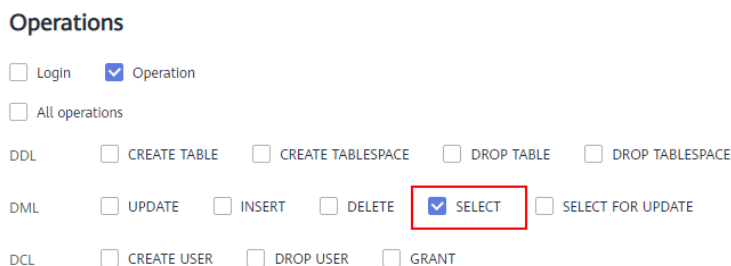
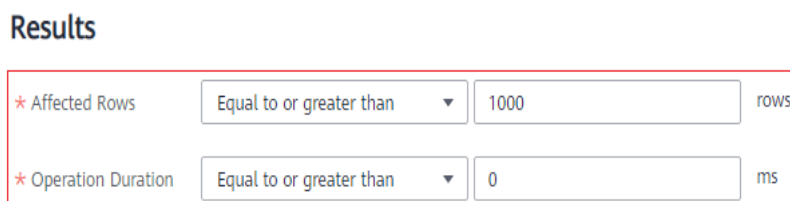
- Step 2** Select a region and click . Choose **Security & Compliance > Database Security Service**.
- Step 3** In the navigation pane, choose **Rules**.
- Step 4** In the **Instance** drop-down list, select an instance.
- Step 5** Click the **Risky Operations** tab.
- Step 6** In the **Operation** column 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



- 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






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

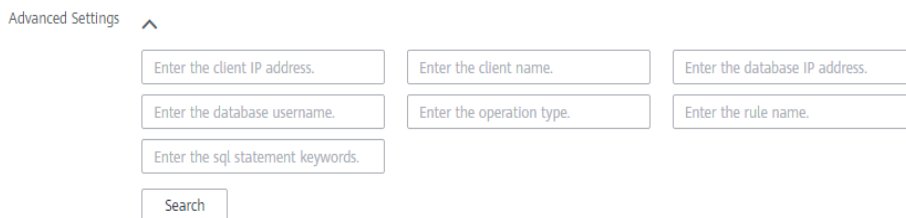
Perform the following steps:

- 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



- 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, For details, see [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


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

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,
For details, see [Adding Risky Operations](#).

A Change History

Released On	Description
2022-09-30	This is the first official release.