Database Security Service

User Guide

Issue	1.0
Date	2022-09-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 Purchasing Database Audit

Before using the database audit function, you need to purchase database audit. Database audit charges yearly or monthly.

Constraints

- DBSS cannot be used across regions. The database to be audited and the database audit instance you purchased must be in the same region.
- Ensure the VPC of the database audit instance is the same as that of the node (application side or database side) where you plan to install the database audit agent. Otherwise, the instance will be unable to connect to the agent or perform audit.

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

Impact on the System

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

Prerequisites

You have obtained a username and its password for logging in to the management console.

NOTICE

Ensure that the **DBSS System Administrator**, **VPC Administrator**, **ECS Administrator**, and **BSS Administrator** policies have been configured for the account used for purchasing instances.

- **VPC Administrator**: Users with this set of permissions can perform all execution permission for VPC. It is a project-level role, which must be assigned in the same project.
- **BSS Administrator**: Users with this set of permissions can perform any operation on menu items on pages **My Account**, **Billing Center**, and **Resource Center**. It is a project-level role, which must be assigned in the same project.
- **ECS Administrator**: Users with this set of permissions can perform any operations on an ECS. It is a project-level role, which must be assigned in the same project.

Procedure

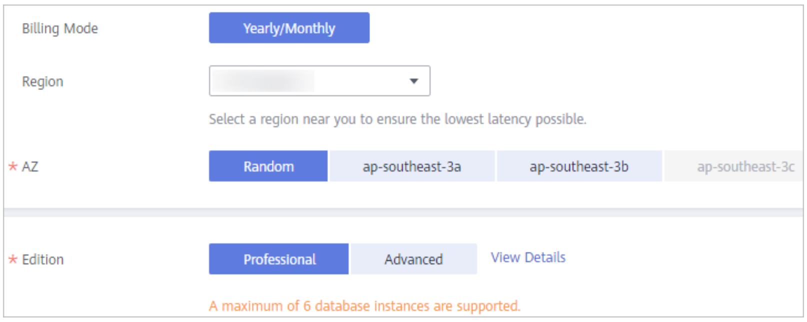
Step 1 Log in to the management console.

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

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

Step 4 Select a region, a project, an AZ, and an edition. See **Figure 1-1**.

Figure 1-1 Selecting an AZ and an edition



Billing Mode: Yearly/Monthly

Region: [redacted]

Select a region near you to ensure the lowest latency possible.

* AZ: Random | ap-southeast-3a | ap-southeast-3b | ap-southeast-3c

* Edition: Professional | Advanced | View Details

A maximum of 6 database instances are supported.

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

Table 1-1 describes the database audit editions.

Table 1-1 Database audit editions

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.

NOTE

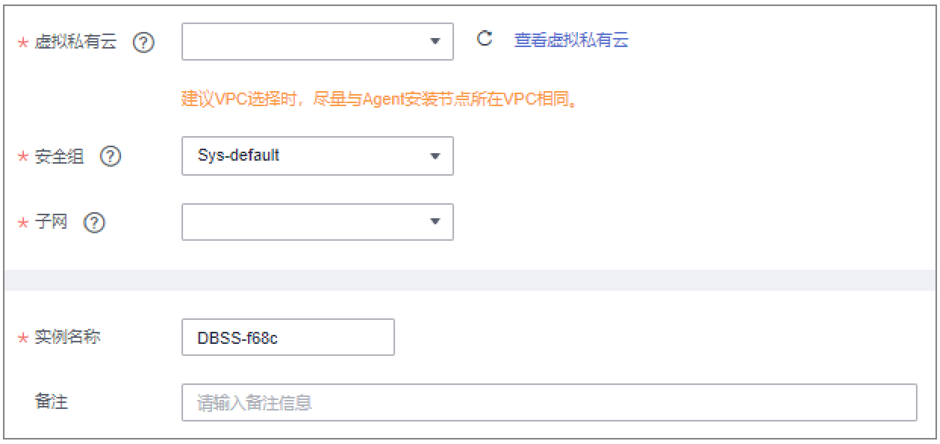
- A database instance is uniquely defined by its database IP address and port.

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

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

Step 5 Set database audit parameters, as shown in **Figure 1-2**. For details about related parameters, see **Table 1-2**.

Figure 1-2 Setting database audit parameters



* 虚拟私有云 ⑦ ▾ ↻ 查看虚拟私有云

建议VPC选择时，尽量与Agent安装节点所在VPC相同。

* 安全组 ⑦ Sys-default ▾

* 子网 ⑦ ▾

* 实例名称 DBSS-f68c

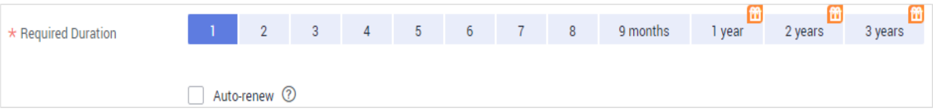
备注 请输入备注信息

Table 1-2 Database audit parameters

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

Step 6 Set **Required Duration**. See **Figure 1-3**.

Figure 1-3 Setting the required duration



* Required Duration [✓ 1] 2 3 4 5 6 7 8 9 months 1 year 2 years 3 years

□ Auto-renew ⑦

After you select **Auto-renew**, the system automatically renews the instance upon expiry if your account balance is sufficient. You can continue to use the instance. **Table 1-3** describes the auto-renewal period.

Table 1-3 Auto-renewal period description

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

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

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

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

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

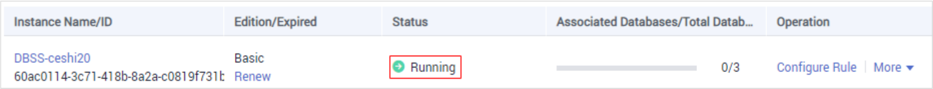
Step 10 After you pay for your order, you can view the creation status of your instances.

----End

Follow-Up Procedure

- If the **Status** of the instance is **Running**, as shown in **Figure 1-4**, you have successfully purchased the database audit instance.

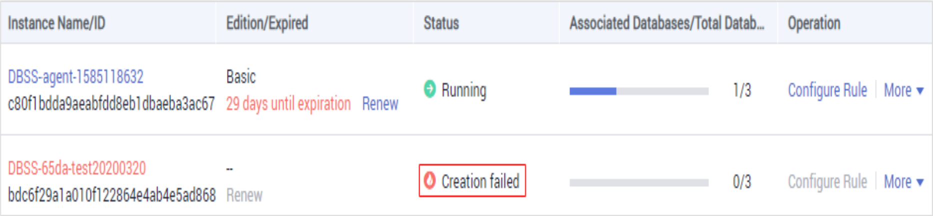
Figure 1-4 Successfully purchasing database audit



Instance Name/ID	Edition/Expired	Status	Associated Databases/Total Datab...	Operation
DBSS-ceshi20 60ac0114-3c71-418b-8a2a-c0819f731b	Basic Renew	Running	0/3	Configure Rule | More ▾

- If the instance status is **Creation failed**, as shown in **Figure 1-5**, you will be automatically refunded. You can click **More** in the **Operation** column and view details in the **Failure Details** dialog box.

Figure 1-5 Database audit instance creation failed



Instance Name/ID	Edition/Expired	Status	Associated Databases/Total Datab...	Operation
DBSS-agent-1585118632 c80f1bdda9aeabfdd8eb1dbaeba3ac67	Basic 29 days until expiration Renew	Running	1/3	Configure Rule | More ▾
DBSS-65da-test20200320 bdc6f29a1a010f122864e4ab4e5ad868	-- Renew	Creation failed	0/3	Configure Rule | More ▾

2 Quick Start

After purchasing a database audit instance, add the database to be audited to the instance and install an agent on the database or application side. Database audit works only when the database to be audited is connected to the database audit instance.

Background

Database audit supports auditing databases built on ECS, BMS, and RDS on Huawei Cloud.

NOTICE

- Database audit cannot be used across regions. The database to be audited and the database audit instance you purchased must be in the same region.
- If SSL is enabled for a database, the database cannot be audited. To use database audit, disable SSL first. For details, see **How Do I Disable SSL for a Database?**.
- For details about audit data storage, see **How Long Is the Audit Data of Database Audit Stored by Default?**

Quick Configuration Procedure

After purchasing database audit, you can quickly get started by following the configuration procedure shown in **Figure 2-1**. For details, see **Table 2-1**.

Figure 2-1 Procedure for quickly configuring database audit

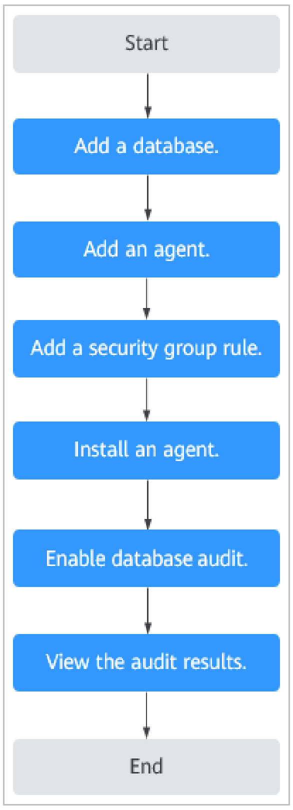


Table 2-1 Procedure for quickly configuring database audit

Step	Configuration	Description
1	**Adding a Database**	Purchase database audit. Add a database to the database audit instance and enable audit for the database.
2	**Adding an Agent**	Select an agent add mode. Database audit supports auditing databases built on ECS, BMS, and RDS on Huawei Cloud. Select an agent add mode based on your database deployed on Huawei Cloud.
3	**Adding Security Group Rules**	Configure TCP (port 8000) and UDP (ports 7000 to 7100) in the security group inbound rule of the database audit instance to allow the agent to communicate with the audit instance.
4	**Installing an Agent (Linux OS)**	Download and then install the agent on the database or application based on the add mode you chose.
5	**Enabling Database Audit**	Enable database audit and connect the added database to the database audit instance.

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

Helpful Links

- Choose the way to add an agent and the node to install it. For details, see **How Do I Install a Database Audit Agent?**
- If the audit function is unavailable, rectify the fault by following the instructions provided in **Database Audit Is Unavailable**.

Verifying the Result

When you connect the added database to the database audit instance, database audit records all operations performed on the database. You can view the audit result on the database audit page.

3 Step 1: Add a Database

Database audit supports databases built on ECS, BMS, and RDS on Huawei Cloud. After purchasing a database audit instance, you need to add the database to be audited to the instance.

For details about the types and versions of databases that can be audited by database audit, see **Supported Database Types and Versions**.

Prerequisites

You have purchased a database audit instance and the **Status** is **Running**.

Adding a Database

Step 1 Log in to the management console.

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

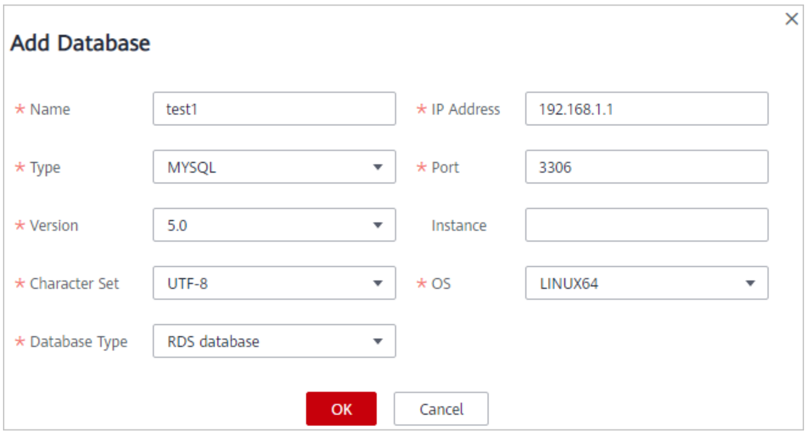
Step 3 In the navigation tree on the left, choose **Databases**.

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

Step 5 Click **Add Database**.

Step 6 In the dialog box displayed, set the database information, as shown in **Figure 3-1**.

Figure 3-1 Add Database dialog box



Add Database

* Name	test1	* IP Address	192.168.1.1
* Type	MYSQL	* Port	3306
* Version	5.0	Instance	
* Character Set	UTF-8	* OS	LINUX64
* Database Type	RDS database		

Table 3-1 Parameters

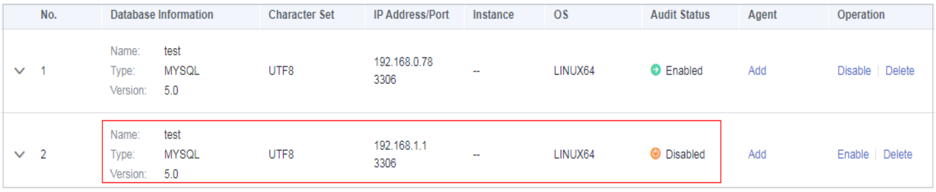
Parameter	Description	Example Value
Name	Custom name of the database to be added	test1
IP Address	IP address of the database to be added. It must be an intranet IPv4 (for example, 192.168.1.1) or intranet IPv6 (for example, fe80:0000:0000:0000:0000:0000:0000:0000) address.	192.168.1.1
Type	Supported database type. The options are as follows: ● MYSQL ● ORACLE ● POSTGRESQL ● SQLSERVER ● DWS ● GaussDB(for MYSQL) ● GaussDB(for openGauss) ● DAMENG ● KINGBASE ● MongoDB **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.	MYSQL
Port	Port number of the database to be added	3306

Parameter	Description	Example Value
Version	Supported database versions ● When **Type** is set to **MYSQL**, the following versions are available: – 5.0, 5.1, 5.5, 5.6, 5.7 – 8.0 (8.0.11 and earlier) – 8.0.23 – 8.0.25 – If **RDS database** is selected, a list of database instances will be displayed for you to choose from. You do not need to install the agent. ● When **Type** is set to **ORACLE**, the following versions are available: – 11g – 12c – 19c ● When **Type** is set to **POSTGRESQL**, the following versions are available: 7.4 or later ● When **Type** is set to **SQLSERVER**, the following versions are available: – 2008 – 2012 – 2014 – 2016 – 2017 ● When **Type** is set to **DWS**, the following versions are available: – 1.5 ● When **Type** is set to **GaussDB(for MySQL)**, the following versions are available: – When **Database Type** is set to **Self-built database**, you can select the **MySQL 8.0** version. – If **RDS database** is selected, a list of database instances will be displayed for you to choose from. You do not need to install the agent. ● When **Type** is set to **GaussDB(for openGauss)**, the following version is available: – 1.4 Enterprise Edition	5.0

Parameter	Description	Example Value
	- When **Type** is set to **DAMENG**, the following version is available: – DM8 - When **Type** is set to **KINGBASE**, the following version is available: – V8	
Instance	Instance name of the database to be audited **NOTE** - If you do not configure the **Instance** field, database audit will audit all instances in the database. - If you enter an instance name, database audit will audit the entered instance. Enter a maximum of five instance names and use semicolons (;) to separate instance names.	-
Character Set	Encoding format of the database character set. The options are as follows: - UTF-8 - GBK	UTF-8
OS	OS of the added database. The options are as follows: - LINUX64 - WINDOWS64	LINUX64
Database Type	Type of the database to be added. Its value can be **RDS database** or **Self-built database**.	RDS database

Step 7 Click **OK**. Then a database in the **Disabled** state has been added to the database list. See **Figure 3-2**.

Figure 3-2 Successfully adding a database



No.	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
1	Name: test Type: MYSQL Version: 5.0	UTF8	192.168.0.78 3306	--	LINUX64	Enabled	Add	Disable | Delete
2	Name: test Type: MYSQL Version: 5.0	UTF8	192.168.1.1 3306	--	LINUX64	Disabled	Add	Enable | Delete

NOTE

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

----End

4 Step 2: Add an Agent

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

After adding an agent, configure TCP (port 8000) and UDP (ports 7000 to 7100) in the security group inbound rule of the agent node to allow the agent to communicate with the audit instance.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- A database has been added.

Scenarios

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

- Deploy DBSS for databases built on ECS/BMS. For details, see **Figure 4-1** and **Figure 4-2**.

Figure 4-1 One application connecting to multiple databases built on ECS/BMS

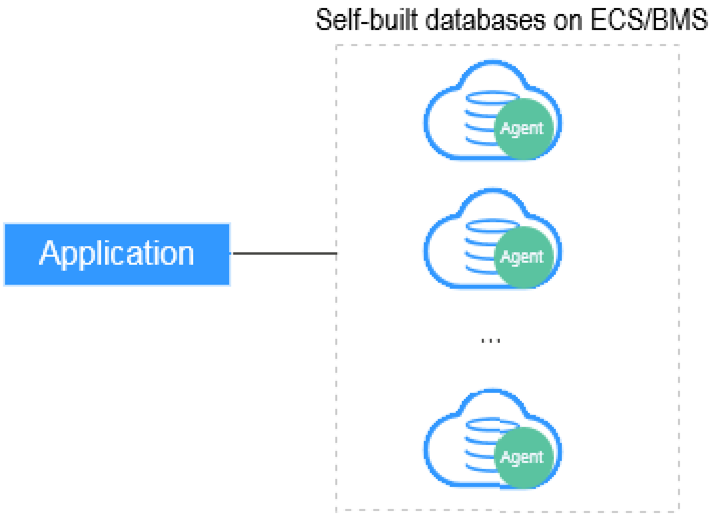
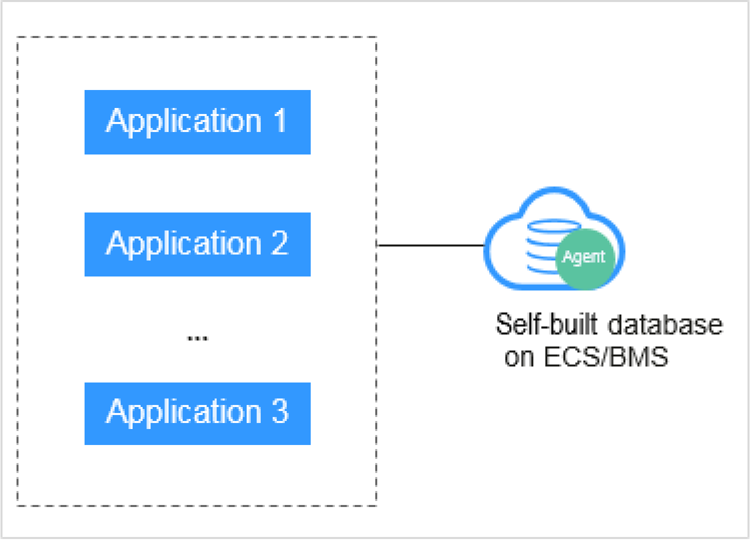


Figure 4-2 Multiple applications connecting to one database built on ECS/BMS



- Deploy DBSS for RDS databases. For details, see **Figure 4-3** and **Figure 4-4**.

Figure 4-3 One application connecting to multiple RDS databases

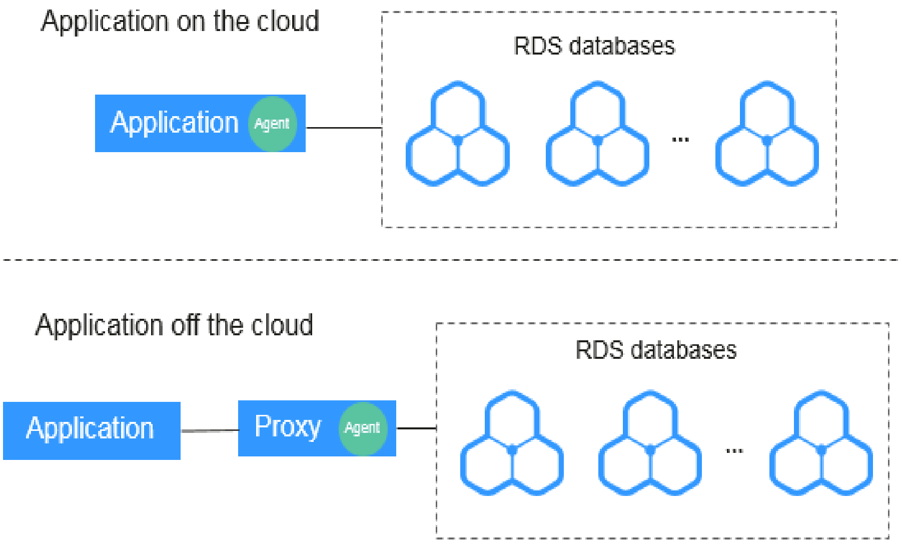


Figure 4-4 Multiple applications connecting to one RDS database

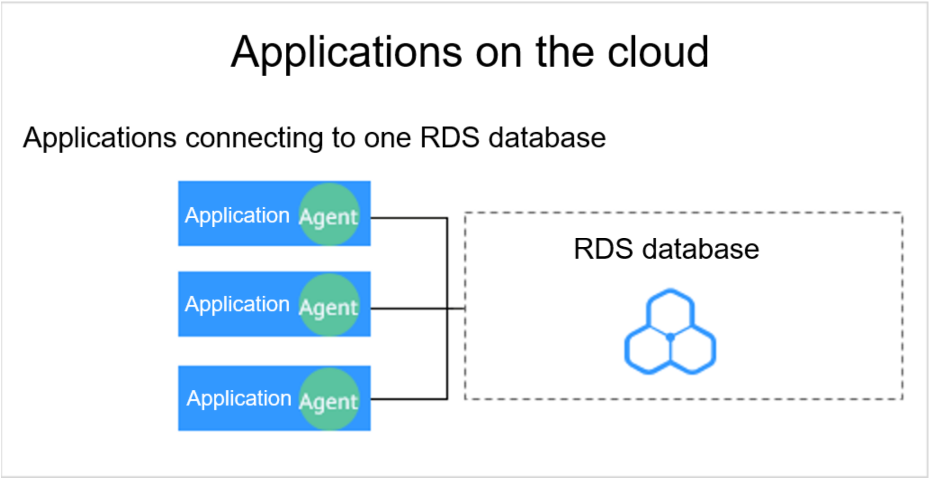

Applications on the cloud
Applications connecting to one RDS database
Application
Agent
Application
Agent
Application
Agent
RDS database

Table 4-1 provides more details.

NOTICE

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

Table 4-1 Agent locations

Scenario	Where to Add the Agent	Audit Scope	Description
Databases built on ECS/BMS	Database	All access records of applications that have accessed the database	• Add the agent on the database side. • If an application connects to multiple databases built on ECS/BMS, the agent must be added on all these databases.
RDS database	Application (if applications are deployed on the cloud)	Access records of all the databases connected to the application	• Add the agent on the application side. • If an application connects to multiple RDS databases, add an agent on each of the databases. Set **Installation Node Type** for one of them and select **Select an existing agent** for the rest of them. For details, see **Selecting an existing agent**. • If multiple applications connect to the same RDS database, add the agent must on all these applications.
	Proxy side (if applications are deployed off the cloud)	Only the access records between the proxy and database. Those between the applications and database cannot be audited.	• Add the agent on the application side. • **Installing Node IP Address** must be set to the IP address of the proxy.

Adding an Agent (Self-built Databases on ECS/BMS)

Step 1 Log in to the management console.

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

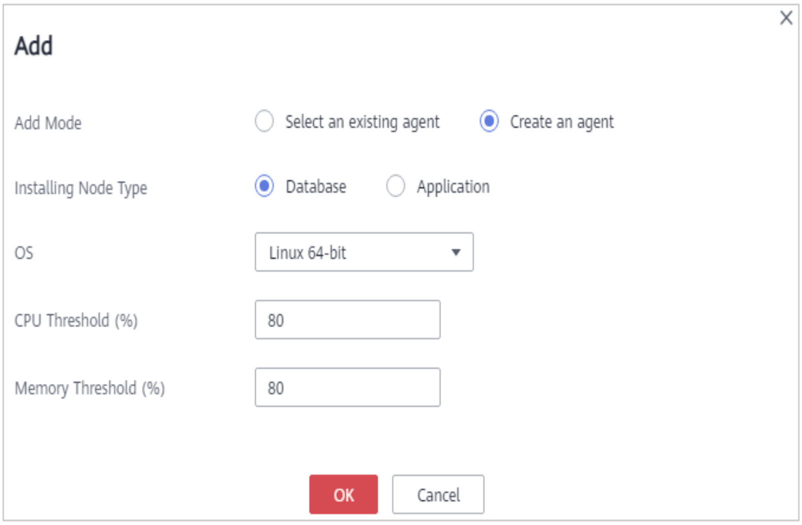
Step 3 In the navigation tree on the left, choose **Databases**.

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

Step 5 In the **Agent** column of the desired database, click **Add**.

Step 6 In the dialog box displayed, select an add mode, as shown in **Figure 4-5**. For details about related parameters, see **Table 4-2**.

Figure 4-5 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

Table 4-2 Parameters for adding an agent (databases built on ECS/BMS)

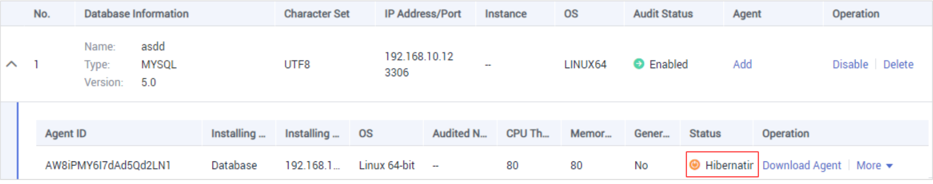
Parameter	Description	Example Value
Add Mode	Mode for adding an agent - **Select an existing agent** If an agent has been installed on a database connected to the same application as the desired database, select **Select an existing agent**. - **Create an agent** If no agent is available, select **Create an agent** to create one.	Create an agent
Installing Node Type	This parameter is mandatory when **Add Mode** is set to **Create an agent**. When auditing user-installed databases on ECS/ BMS, select **Database** for **Installing Node Type**.	Database
OS	OS of the database to be audited. Its value can be . Its value can be **LINUX64** or **WINDOWS64**.	LINUX64
CPU Threshold (%)	Optional. This parameter is configurable if **Installing Node Type** is set to **Application**. CPU threshold of the application node to be audited. The default value is **80**.	80

Parameter	Description	Example Value
Memory Threshold (%)	Optional. This parameter is configurable if **Installing Node Type** is set to **Application**. Memory threshold of the application node to be audited. The default value is **80**.	80

Step 7 Click **OK**.

Step 8 Click ∨ on the left of the database to view its details and information about the added agent. See **Figure 4-6**.

Figure 4-6 Successfully adding an agent



	No.	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
^	1	Name: asdd Type: MYSQL Version: 5.0	UTF8	192.168.10.12 3306	--	LINUX64	Enabled	Add	Disable | Delete

Agent ID	Installing ...	Installing ...	OS	Audited N...	CPU Th...	Memor...	Gener...	Status	Operation
AW8iPMY6I7dAd5Qd2LN1	Database	192.168.1...	Linux 64-bit	--	80	80	No	Hibernatir	Download Agent | More ▾

📖 NOTE

After adding the agent, confirm that the agent information is correct. If the agent is incorrectly added, locate the target agent, click **More** > **Delete** in the **Operation** column, and add an agent again.

----End

Adding an Agent (RDS Databases)

📖 NOTE

After you add a MySQL or GaussDB(for MySQL) database, you can start configuring security group rules. You do not need to install an agent on the database.

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

- Add an agent to each of the RDS databases.
- Select **Select an existing agent** if one of the databases already has an agent. Add that agent for the rest of the databases.

Step 1 Log in to the management console.

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

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

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

Step 5 In the **Agent** column of the desired database, click **Add**.

Step 6 In the displayed dialog box, select an add mode, as shown in **Figure 4-7** and **Figure 4-8**. For details about related parameters, see **Table 4-3**.

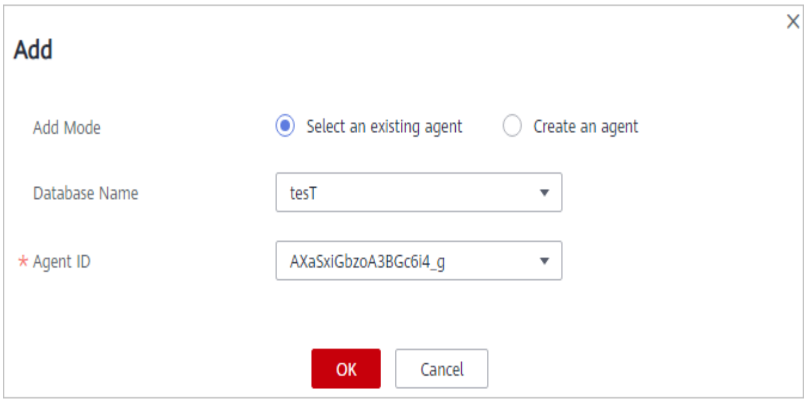
- Select **Select an existing agent** for **Add Mode**.

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

  NOTE

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

  Figure 4-7 Selecting an existing agent

  Add

  Add Mode ● Select an existing agent ○ Create an agent

  Database Name tesT

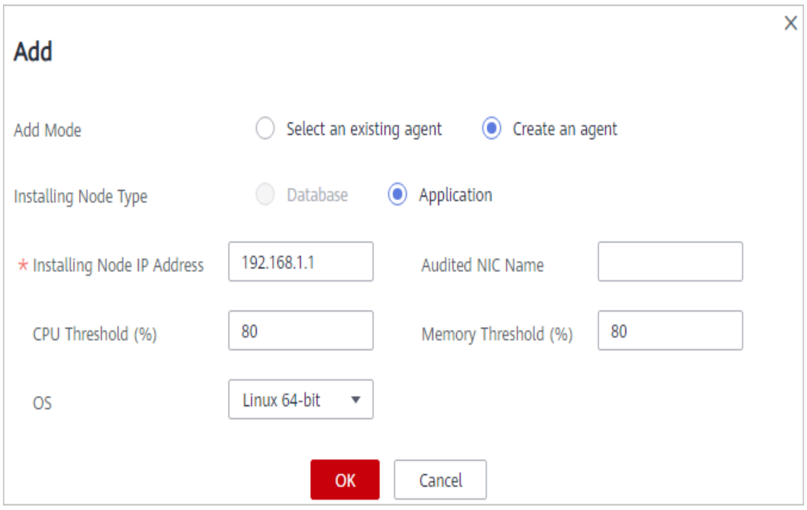
  * Agent ID AXaSxiGbzoA3BGc6i4_g

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

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

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

  Figure 4-8 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 192.168.1.1

  Audited NIC Name

  CPU Threshold (%) 80

  Memory Threshold (%) 80

  OS Linux 64-bit

Table 4-3 Parameters for adding an agent (RDS databases)

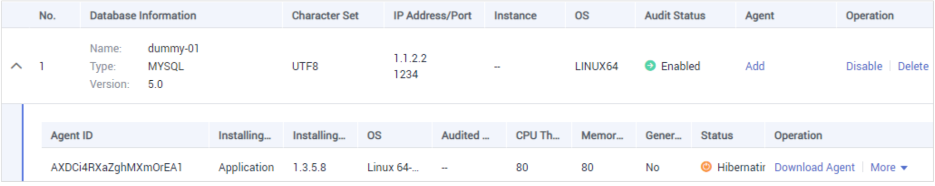
Parameter	Description	Example Value
Add Mode	Mode for adding an agent ● **Selecting an existing agent** If an agent has been installed on a database connected to the same application as the desired database, select **Select an existing agent**. ● **Create an agent** If no agent is available, select **Create an agent** to create one.	Create an agent
Installing Node Type	This parameter is mandatory when **Add Mode** is set to **Create an agent**. To audit the RDS databases, select **Application**.	Application
Installing Node IP Address	This parameter is mandatory if **Installing Node Type** is set to **Application**. You can enter only one installation node IP address. The IP address of an agent must be unique. The IP address is the intranet IP address of the application. It must be an intranet IPv4 (for example, 192.168.1.1) or intranet IPv6 (for example, fe80:0000:0000:0000:0000:0000:0000:0000) address. **NOTICE** To audit an RDS database connected to an off-cloud application, set this parameter to the IP address of the proxy.	192.168.1.1
Audited NIC Name	Optional. This parameter is configurable if **Installing Node Type** is set to **Application**. Name of the network interface card (NIC) of the application node to be audited	-
CPU Threshold (%)	Optional. This parameter is configurable if **Installing Node Type** is set to **Application**. CPU threshold of the application node to be audited. The default value is **80**. **NOTICE** If the CPU usage of a server exceeds the threshold, the agent on the server will stop running.	80

Parameter	Description	Example Value
Memory Threshold (%)	Optional. This parameter is configurable if **Installing Node Type** is set to **Application**. Memory threshold of the application node to be audited. The default value is **80**. **NOTICE** If the memory usage of your server exceeds the threshold, the agent will stop running.	80
OS	Optional. This parameter is configurable if **Installing Node Type** is set to **Application**. OS of the application node to be audited. The value can be **LINUX64** or **WINDOWS64**.	LINUX64

Step 7 Click **OK**.

Step 8 Click ⌄ next to the database to view its details and information about the added agent. See **Figure 4-9**.

Figure 4-9 Successfully adding an agent



No.	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
1	Name: dummy-01 Type: MYSQL Version: 5.0	UTF8	1.1.2.2 1234	--	LINUX64	● Enabled	Add	Disable | Delete

Agent ID	Installing...	Installing...	OS	Audited ...	CPU Th...	Memor...	Gener...	Status	Operation
AXDCi4RXaZghMXmOrEA1	Application	1.3.5.8	Linux 64-...	--	80	80	No	● Hibernatir	Download Agent | More ▾

NOTE

After adding the agent, confirm that the agent information is correct. If the agent is incorrectly added, locate the target agent, click **More** > **Delete** in the **Operation** column, and add an agent again.

----End

Follow-Up Procedure

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

5 Step 3: Add a Security Group Rule

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

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

NOTE

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

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- You have added an agent to your database.

Adding a Security Group Rule

Step 1 Log in to the management console.

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

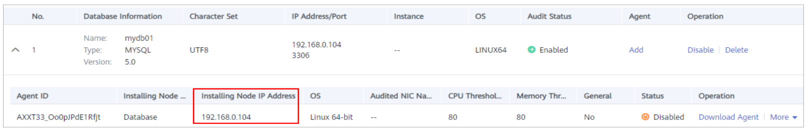
Step 3 In the navigation tree on the left, choose **Database Audit** > **Databases**.

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

Step 5 Record the IP address of the agent node.

Click ⌄ next to the database to view the information of its agent, and record **Installing Node IP Address**, as shown in **Figure 5-1**.

Figure 5-1 Installing Node IP Address



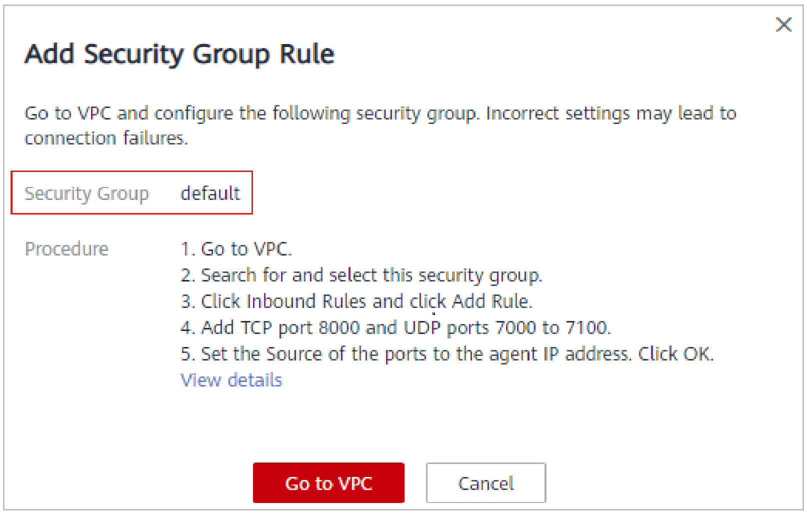
No.	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
1	Name: mydb01 Type: MYSQL Version: 5.0	UTF8	192.168.0.104 3306	--	LINUX64	Enabled	Add	Disable | Delete

Agent ID	Installing Node ...	Installing Node IP Address	OS	Audited NIC Na...	CPU Threshol...	Memory Thr...	General	Status	Operation
AXXT33_Oo0pJPdE1Rfjt	Database	192.168.0.104	Linux 64-bit	--	80	80	No	Disabled	Download Agent | More ▾

Step 6 Click **Add Security Group Rule**.

Step 7 In the displayed dialog box, record the security group name (for example, **default**) of the database audit instance, as shown in **Figure 5-2**.

Figure 5-2 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 8 Click **Go to VPC**.

Step 9 In the security group list, enter the 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 10 Click the group name **default**.

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

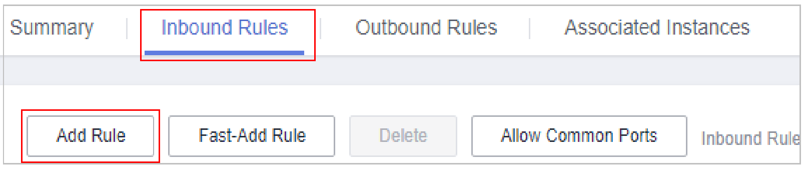
Check whether TCP (port number **8000**) and UDP protocols (port number from **7000** to **7100**) are configured in the inbound rules of the security group for the IP address of the installing node in **Step 5**.

- If the inbound rules of the security group have been configured for the installing node, go to **Downloading an Agent**.
- If no inbound rules of the security group have been configured for the installing node, go to **Step 12**.

Step 12 Add an inbound rule for the installing node.

1. On the **Inbound Rules** tab, click **Add Rule**. See **Figure 5-3**.

Figure 5-3 Adding rules



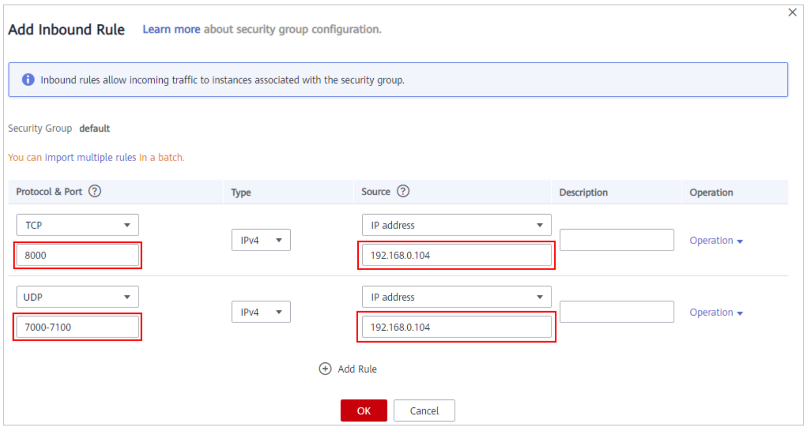
2. In the **Add Inbound Rule** dialog box, add **TCP** (port number **8000**) and **UDP** protocols (port number from **7000** to **7100**) for the installing node IP address in **Figure 5-1**. See **Figure 5-4**.

NOTE

The source can be an IP address, an IP address segment, or a security group. Examples:

- IP address: **192.168.10.10/32**
- IP address segment: **192.168.52.0/24**
- All IP addresses: **0.0.0.0/0**
- Security group: **sg-abc**

Figure 5-4 Add Inbound Rule dialog box



Add Inbound Rule Learn more about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

Security Group default

You can import multiple rules in a batch.

Protocol & Port	Type	Source	Description	Operation
TCP 8000	IPv4	IP address 192.168.0.104		Operation
UDP 7000-7100	IPv4	IP address 192.168.0.104		Operation

3. Click **OK**.

   After adding a security group rule, download and install the agent on a database or application, depending on the add mode you chose. Database audit can be enabled only if the audited object is connected to the database audit instance.

----End

6 Step 4: Download and Install the Agent

6.1 Downloading an Agent

Download and then install the agent on the database or application based on the add mode you chose.

NOTE

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

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- You have added an agent to the database.

Procedure

Step 1 Log in to the management console.

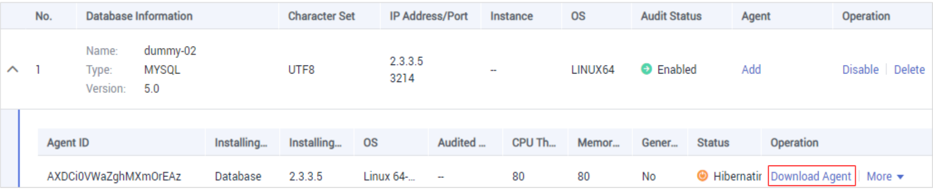
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 Click ⌄ next to the database to view details of its agent. In the **Operation** column of the agent, click **Download Agent**, as shown in **Figure 6-1**, to download an agent installation package.

Figure 6-1 Downloading an agent



	No.	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
^	1	Name: dummy-02 Type: MYSQL Version: 5.0	UTF8	2.3.3.5 3214	--	LINUX64	Enabled	Add	Disable | Delete

Agent ID	Installing...	Installing...	OS	Audited ...	CPU Th...	Memor...	Gener...	Status	Operation
AXDCi0VWaZghMXmOrEAz	Database	2.3.3.5	Linux 64-...	--	80	80	No	Hibernatir	Download Agent More ▾

Download the agent installation package suitable for your OS.

- Linux OS

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

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

----End

6.2 Installing an Agent (Linux OS)

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

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- You have added an agent to your database.
- You have obtained the agent installation package for the Linux OS.
- The Linux OS version of the target node is supported by the agent. For details about the supported Linux versions, see **On What Linux OSs Can I Install the Agent?**

Scenarios

You can install the agent on the database or application side, depending on your database type and deployment scenario. Common database scenarios are as follows:

- Deploy DBSS for databases built on ECS/BMS. For details, see **Figure 6-2** and **Figure 6-3**.

  Figure 6-2 One application connecting to multiple databases built on ECS/BMS

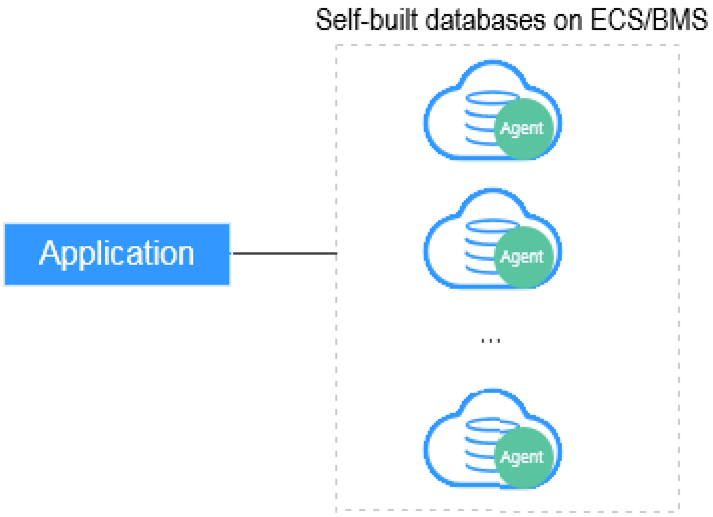
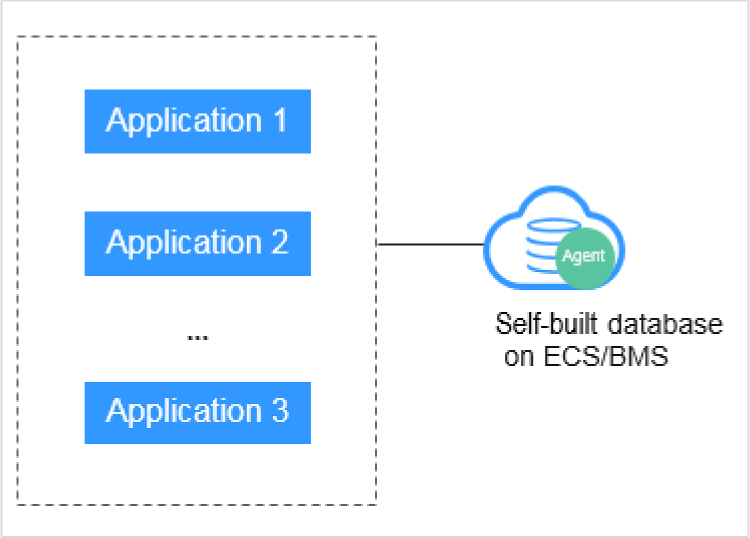


Figure 6-3 Multiple applications connecting to one database built on ECS/BMS



- Deploy DBSS for RDS databases. For details, see **Figure 6-4** and **Figure 6-5**.

Figure 6-4 One application connecting to multiple RDS databases

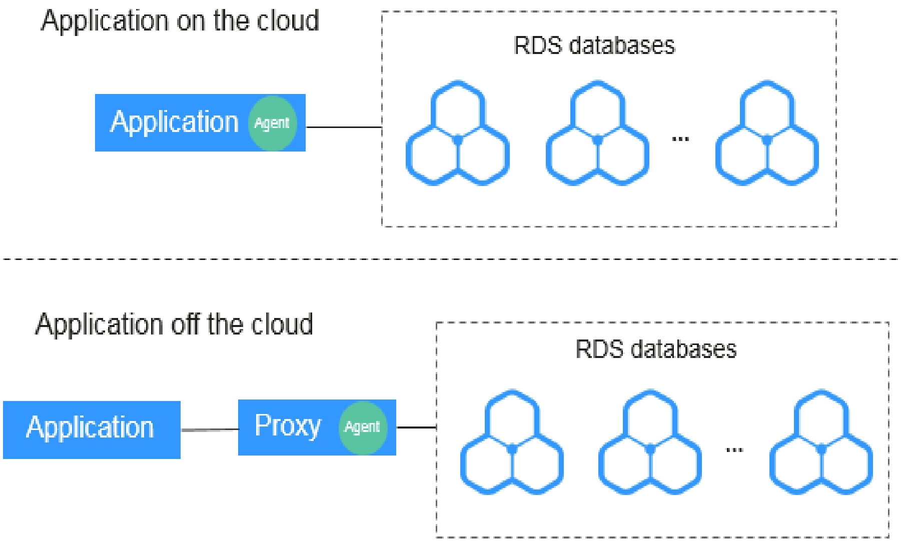


Figure 6-5 Multiple applications connecting to one RDS database

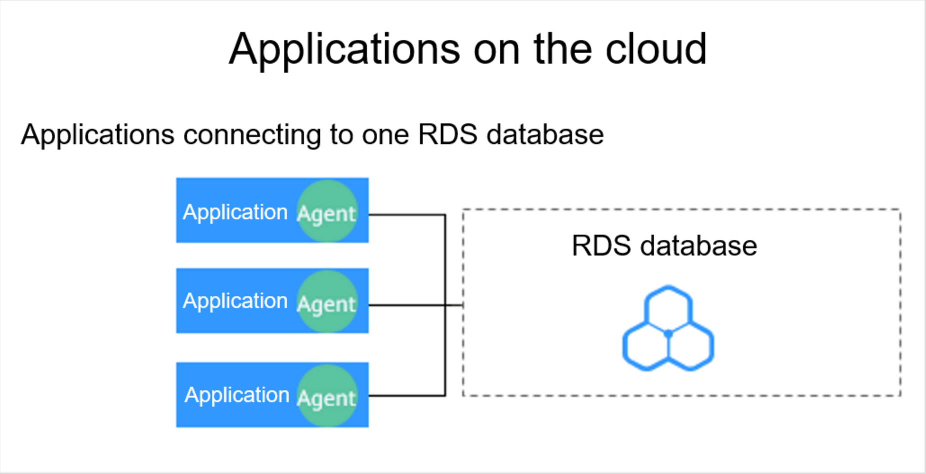

Applications on the cloud
Applications connecting to one RDS database
Application Agent
Application Agent
Application Agent
RDS database

Table 6-1 describes where to install the agent in the preceding scenarios.

NOTICE

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

Table 6-1 Agent installation scenarios

Scenario	Where to Install Agent	Audit Scope	Description
Self-built database on ECS/BMS	Database	All access records of applications that have accessed the database	- Install the agent on the database side. - If an application connects to multiple databases built on ECS/BMS, the agent must be installed on all these databases.
RDS database	Application side (if applications are deployed on the cloud)	Access records of all the databases connected to the application	- Install the agent on the application side. - If multiple applications are connected to the same RDS database, the agent must be installed on all these applications.

Scenario	Where to Install Agent	Audit Scope	Description
RDS database	Proxy side (if applications are deployed off the cloud)	Only the access records between the proxy and database. Those between the applications and database cannot be audited.	Install the agent on the proxy side.

Installing an Agent

Install the agent on the node suitable for your service scenario.

Step 1 Upload the downloaded agent installation package **xxx.tar.gz** to the node (for example, using WinSCP).

Step 2 Log in to the node as user **root** using SSH through a cross-platform remote access tool (for example, PuTTY).

Step 3 Run the following command to access the directory where the agent installation package **xxx.tar.gz** is stored:

cd *Directory_containing_agent_installation_package*

Step 4 Run the following command to decompress the installation package **xxx.tar.gz**:

tar -xvf *xxx.tar.gz*

Step 5 Run the following command to switch to the directory containing the decompressed files:

cd *Decompressed_package_directory*

Step 6 Run the following command to check whether you have the permission for executing the **install.sh** script:

ll

- If you do, go to **Step 7**.
- If you do not, perform the following operations:
  a. Run the following command to get the script execution permission:
     chmod +x install.sh
  b. Verify you have the required permissions.

Step 7 Run the following command to install the agent:

sh install.sh

NOTE

In Ubantu, run the following command to install the agent:

bash install.sh

If the following information is displayed, the agent has been installed. Otherwise, the installation fails.

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

NOTICE

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

Step 8 Run the following command to view the running status of the agent program:

service audit_agent status

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

```
audit agent is running.
```

----End

Helpful Links

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

6.3 Installing an Agent (Windows OS)

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

Prerequisites

- You have added an agent to your database.
- You have obtained the agent installation package for the Windows OS.
- The Windows OS version of the target node is supported by the agent. For details about the supported Windows versions, see **On What Windows OSs Can I Install the Agent?**

Scenarios

You can install the agent on the database or application side, depending on your database type and deployment scenario. Common database scenarios are as follows:

- Deploy DBSS for databases built on ECS/BMS. For details, see **Figure 6-6** and **Figure 6-7**.

Figure 6-6 One application connecting to multiple databases built on ECS/BMS

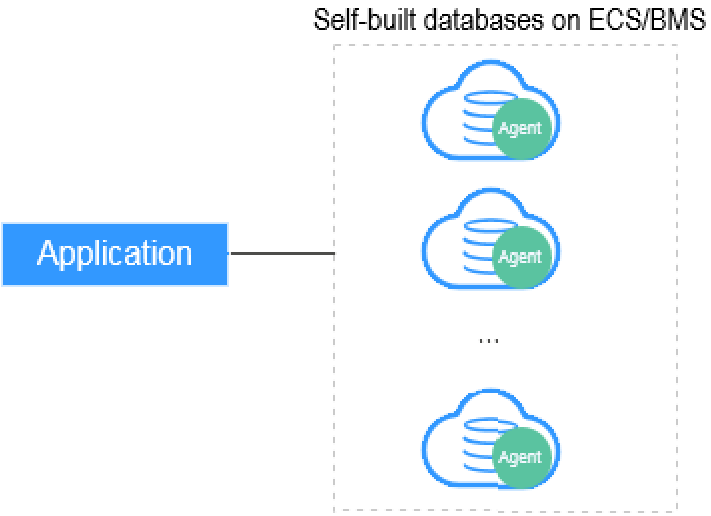
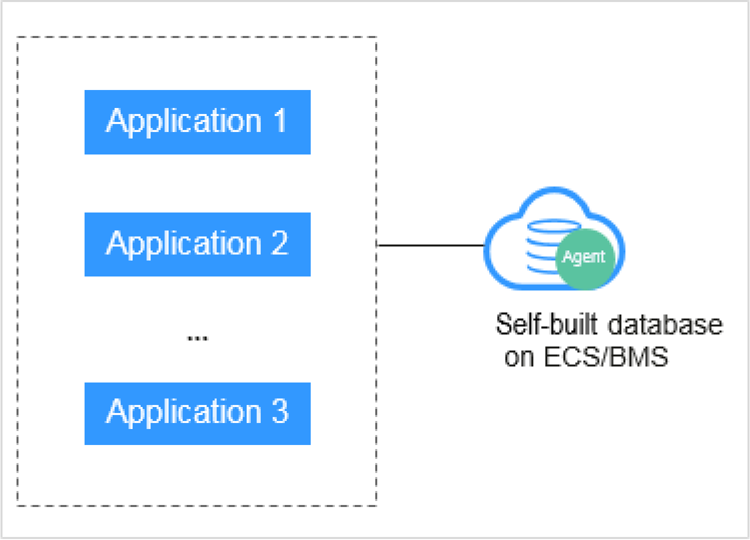


Figure 6-7 Multiple applications connecting to one database built on ECS/BMS



- Deploy DBSS for RDS databases. For details, see **Figure 6-8** and **Figure 6-9**.

Figure 6-8 One application connecting to multiple RDS databases

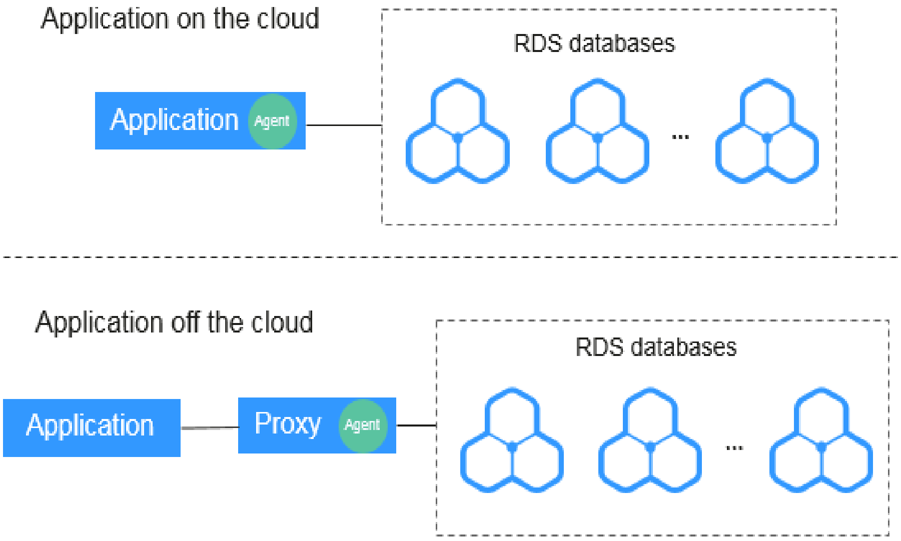


Figure 6-9 Multiple applications connecting to one RDS database

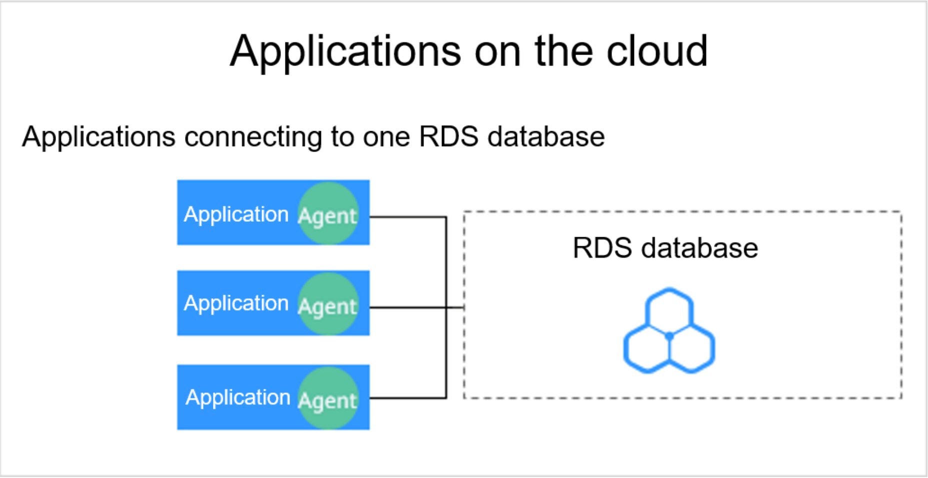

Applications on the cloud
Applications connecting to one RDS database
Application
Agent
Application
Agent
Application
Agent
RDS database

Table 6-2 describes where to install the agent in the preceding scenarios.

NOTICE

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

Table 6-2 Agent installation scenarios

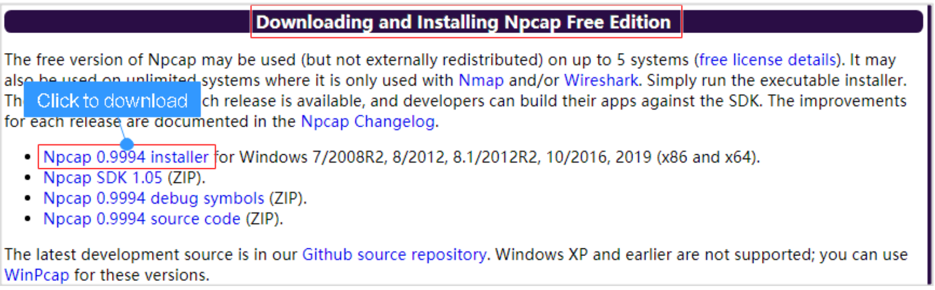
Scenario	Where to Install Agent	Audit Scope	Description
Self-built database on ECS/BMS	Database	All access records of applications that have accessed the database	● Install the agent on the database side. ● If an application connects to multiple databases built on ECS/BMS, the agent must be installed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

Installing an Agent

Step 1 Install Npcap on the Windows server.

- If Npcap has been installed on the Windows OS, go to **Step 2**.
- If the Npcap has not been installed on the Windows server, perform the following steps:
  a. Download the latest Npcap software installation package from **https://nmap.org/npcap/**.

Figure 6-10 Downloading Npcap



Downloading and Installing Npcap Free Edition

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

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

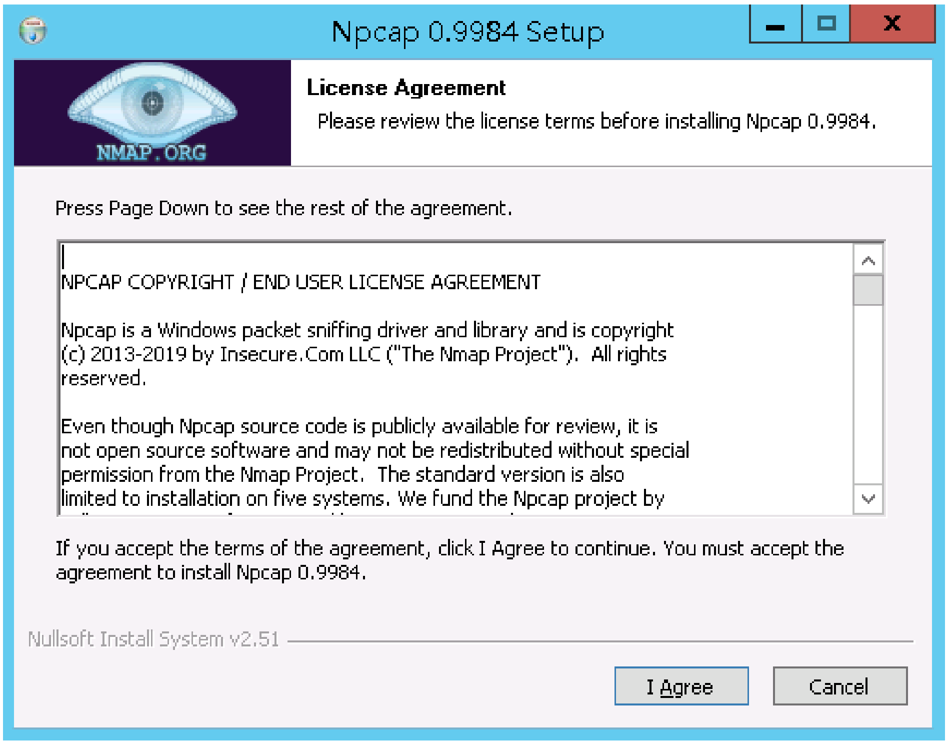
The latest development source is in our Github source repository. Windows XP and earlier are not supported; you can use WinPcap for these versions.

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

c. Double-click the Npcap installation package.

d. In the displayed dialog box, click **I Agree**, as shown in **Figure 6-11**.

Figure 6-11 Agreeing to install Npcap



Npcap 0.9984 Setup

License Agreement

Please review the license terms before installing Npcap 0.9984.

Press Page Down to see the rest of the agreement.

NPCAP COPYRIGHT / END USER LICENSE AGREEMENT

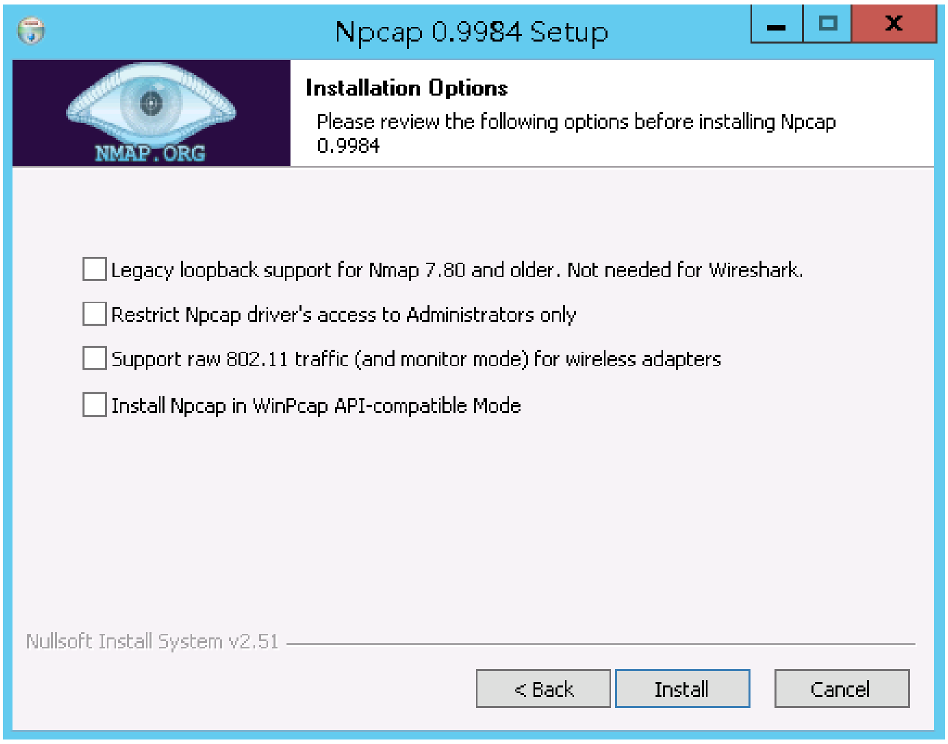
Npcap is a Windows packet sniffing driver and library and is copyright (c) 2013-2019 by Insecure.Com LLC ("The Nmap Project"). All rights reserved.

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

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

e. In the displayed dialog box, leave all the check boxes unselected and click **Install**, as shown in **Figure 6-12**.

Figure 6-12 Installing Npcap



Npcap 0.9984 Setup

Installation Options

Please review the following options before installing Npcap 0.9984

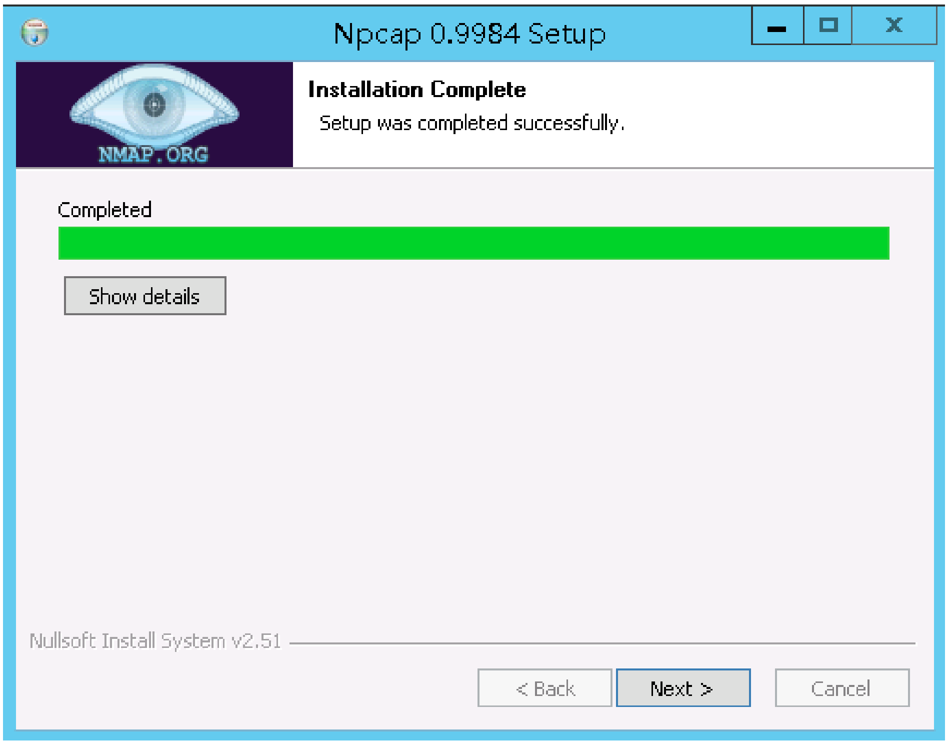
□ Legacy loopback support for Nmap 7.80 and older. Not needed for Wireshark.

□ Restrict Npcap driver's access to Administrators only

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

□ Install Npcap in WinPcap API-compatible Mode

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



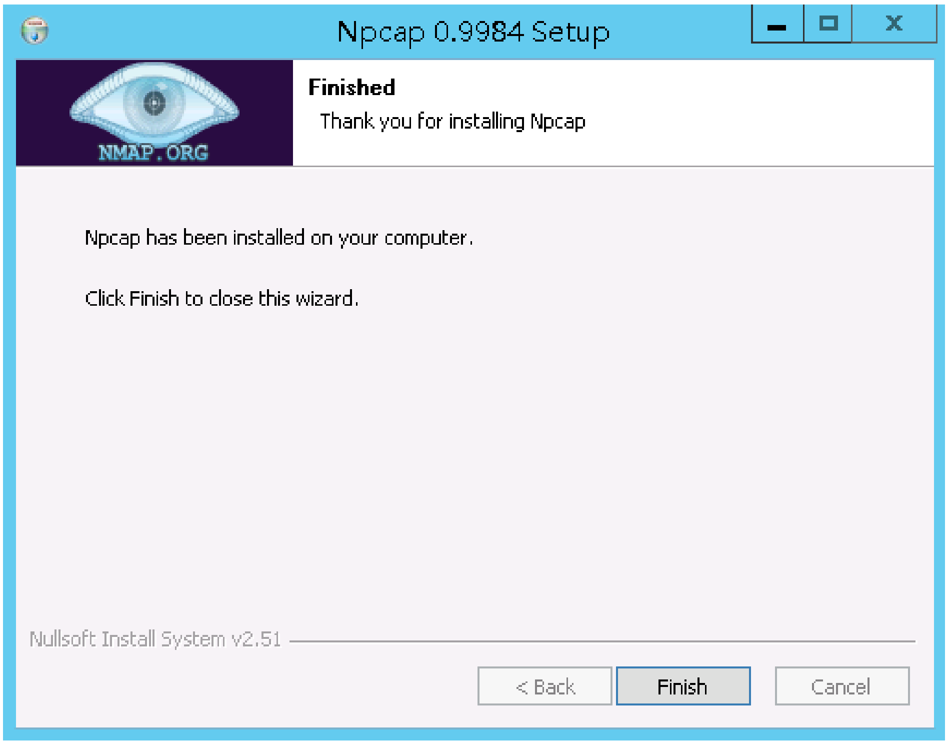
Npcap 0.9984 Setup

Installation Complete

Setup was completed successfully.

Completed

g. Click **Finish**.



Npcap 0.9984 Setup

Finished

Thank you for installing Npcap

Npcap has been installed on your computer.

Click Finish to close this wizard.

Step 2 Log in to the target Windows server as the **Administrator** user.

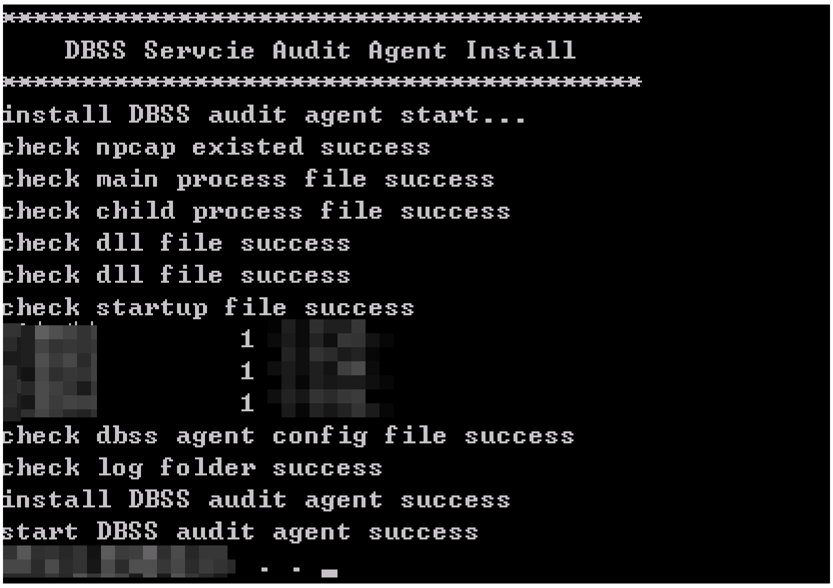
Step 3 Copy the downloaded .zip agent installation package to any directory on the server.

Step 4 Decompress the package.

Step 5 Double-click the **install.bat** file in the package directory.

Step 6 Press any key to complete installation after the output shown in **Figure 6-13** is displayed.

Figure 6-13 Installation completed



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

Step 7 Check the installation result. If the dbss_audit_agent process can be found in the Windows Task Manager, the installation succeeded.

If it is not found, install the agent again.

----End

7 Step 5: Enable Database Audit

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

Prerequisites

- You have added and installed an agent, and the agent status is **Running**.
- A security group rule has been configured for the database audit instance.

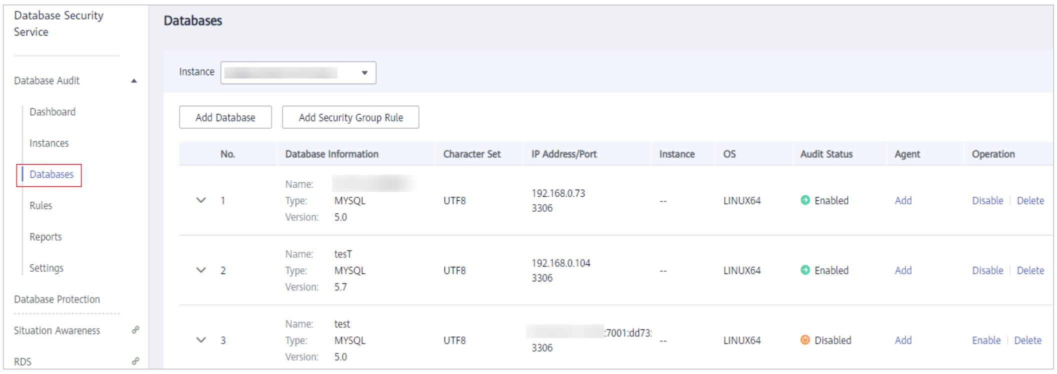
Enabling Database Audit

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 tree on the left, choose **Databases**.

Figure 7-1 Going to the Databases page



Instance [redacted]

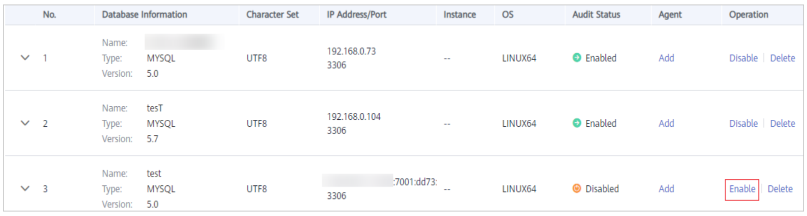
	No.	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
∨	1	Name: [redacted] Type: MYSQL Version: 5.0	UTF8	192.168.0.73 3306	--	LINUX64	Enabled	Add	Disable | Delete
∨	2	Name: tesT Type: MYSQL Version: 5.7	UTF8	192.168.0.104 3306	--	LINUX64	Enabled	Add	Disable | Delete
∨	3	Name: test Type: MYSQL Version: 5.0	UTF8	[redacted]:7001:dd73: 3306	--	LINUX64	Disabled	Add	Enable | Delete

Step 4 Select a database audit instance from the **Instance** drop-down list.

Step 5 In the database list, click **Enable** in the **Operation** column of the database to be audited.

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

Figure 7-2 Enabling database audit



	No.	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
⌄	1	Name: [redacted] Type: MYSQL Version: 5.0	UTF8	192.168.0.73 3306	--	LINUX64	● Enabled	Add	Disable | Delete
⌄	2	Name: tesT Type: MYSQL Version: 5.7	UTF8	192.168.0.104 3306	--	LINUX64	● Enabled	Add	Disable | Delete
⌄	3	Name: test Type: MYSQL Version: 5.0	UTF8	[redacted]:7001:dd73: 3306	--	LINUX64	● Disabled	Add	Enable | Delete

----End

Verifying Audit Results

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

Step 2 Log in to the management console.

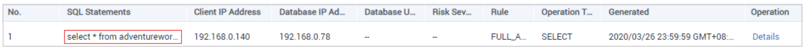
Step 3 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

Step 4 In the **Instance** drop-down list, select the instance that audits the target database.

Step 5 Click the **Statements** tab.

Step 6 Click 📅 next to **Time** to set the start and end time, and click **Submit**. The SQL statements entered in **Step 1** will be displayed, as shown in **Figure 7-3**.

Figure 7-3 Viewing SQL statements



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

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

----End

8 Step 6: View Audit Results

8.1 Viewing the Audit Dashboard

After connecting the database to the database audit instance, view the audit statistics, including the overall audit statistics, risk distribution, session statistics, and SQL distribution.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.
- A security group rule has been configured for the database audit instance.

Procedure

Step 1 Log in to the management console.

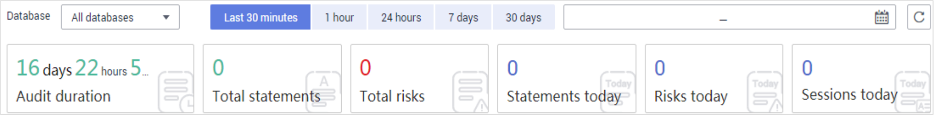
Step 2 Select a region, click ≡, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

Step 4 View the overall audit statistics, risk distribution, session statistics, and SQL distribution. See **Figure 8-1**, **Figure 8-2**, **Figure 8-3**, and **Figure 8-4**.

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

Figure 8-1 Viewing the audit statistics



16 days 22 hours 5...
Audit duration

0
Total statements

0
Total risks

0
Statements today

0
Risks today

0
Sessions today

Figure 8-2 Risk distribution

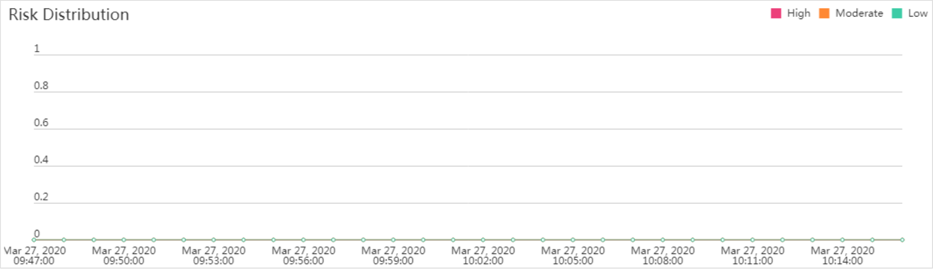


Figure 8-3 Session statistics

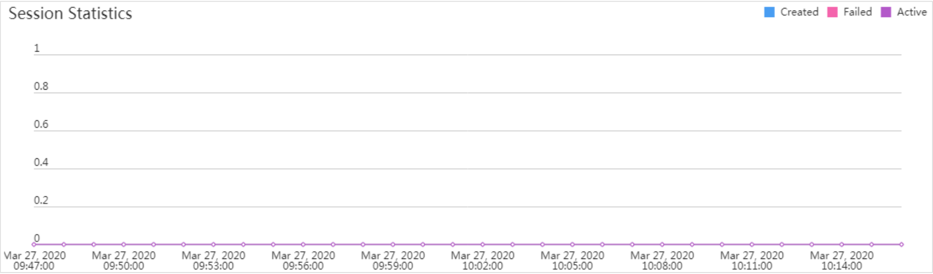
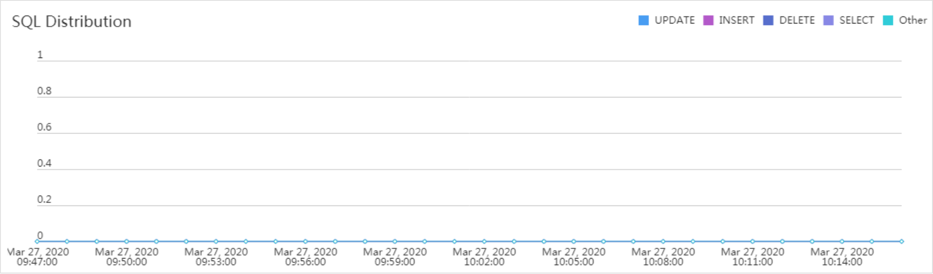


Figure 8-4 SQL distribution



----End

Helpful Links

- If SSL is enabled for a database, the database cannot be audited. To use database audit, disable SSL first. For details, see **How Do I Disable SSL for a Database?**.
- You can configure database audit rules. For details, see **Adding Audit Scope**.

8.2 Viewing SQL Statement Details

After connecting the database to the database audit instance, view SQL statements of the database.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.
- A security group rule has been configured for the database audit instance.

Procedure

Step 1 Log in to the management console.

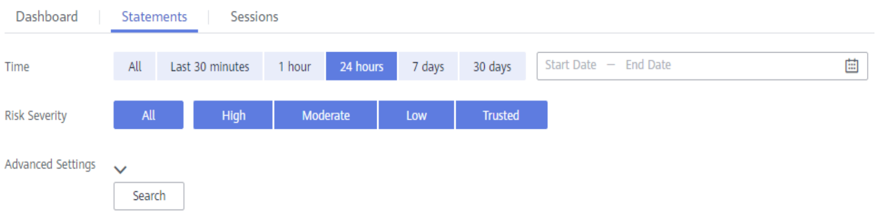
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

Step 4 Click the **Statements** tab.

Step 5 Query SQL statement information, as shown in **Figure 8-5**.

Figure 8-5 Querying SQL statements



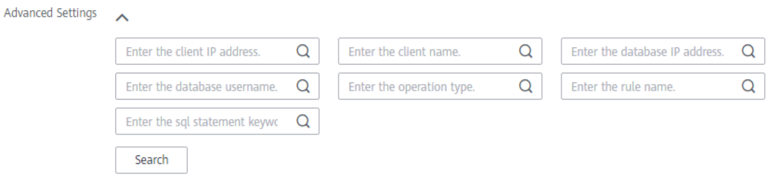
To query a specified SQL statement, perform the following steps:

- Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days**, or click 📅 to set start time and end time, and click **Search** to view SQL statements of the specified time range.
- Select **All**, **High**, **Moderate**, **Low**, or **Trusted** for **Risk Severity** and click **Search**. SQL statements of specified severity are displayed in the list.
- Click ⌄ next to **Advanced Settings**, enter the information, and click **Search**, as shown in **Figure 8-6**. The specified SQL statements are displayed in the list.

  NOTE

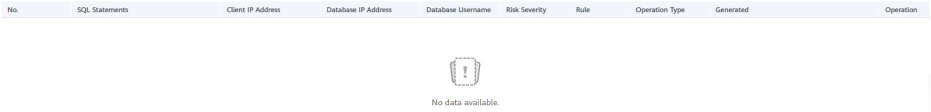
  A maximum of 10,000 records can be retrieved in a query.

  Figure 8-6 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 keywc
Search

Step 6 In the row containing the desired SQL statement, click **Details** in the **Operation** column. See **Figure 8-7**.

Figure 8-7 Viewing details of SQL statements



No.	SQL Statements	Client IP Address	Database IP Address	Database Username	Risk Severity	Rule	Operation Type	Generated	Operation

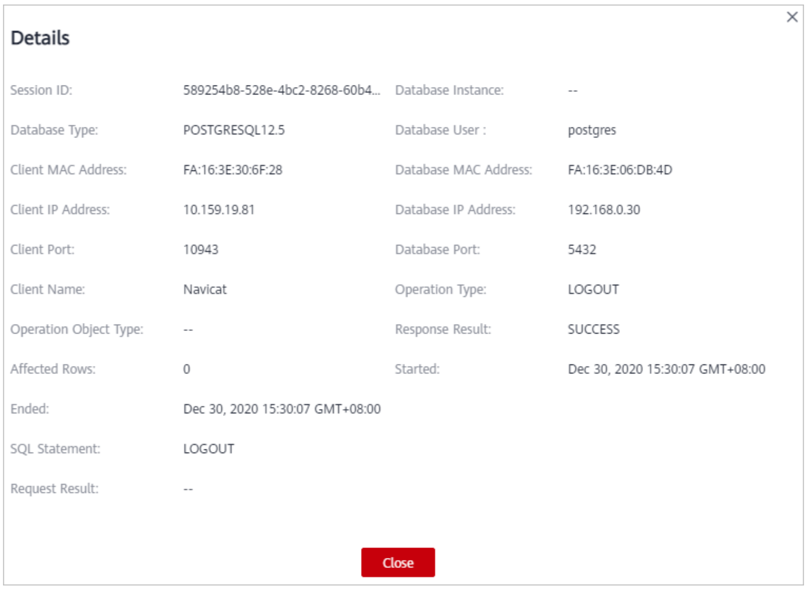
No data available.

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

NOTICE

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

Figure 8-8 Details dialog box



Details

Session ID:	589254b8-528e-4bc2-8268-60b4...	Database Instance:	--
Database Type:	POSTGRESQL12.5	Database User :	postgres
Client MAC Address:	FA:16:3E:30:6F:28	Database MAC Address:	FA:16:3E:06:DB:4D
Client IP Address:	10.159.19.81	Database IP Address:	192.168.0.30
Client Port:	10943	Database Port:	5432
Client Name:	Navicat	Operation Type:	LOGOUT
Operation Object Type:	--	Response Result:	SUCCESS
Affected Rows:	0	Started:	Dec 30, 2020 15:30:07 GMT+08:00
Ended:	Dec 30, 2020 15:30:07 GMT+08:00		
SQL Statement:	LOGOUT		
Request Result:	--		

Table 8-1 Parameters for details of SQL statements

Parameter	Description
Session ID	ID of an SQL statement, which is automatically generated
Database Instance	Database where an SQL statement is executed
Database Type	Type of the database where an SQL statement is executed
Database User	Database user for executing an SQL statement
Client MAC Address	MAC address of the client where an SQL statement is executed
Database MAC Address	MAC address of the database where an SQL statement is executed

Parameter	Description
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 by executing an SQL statement
Affected Rows	Number of rows affected by executing an SQL statement
Started	Time when an SQL statement starts to be executed
Ended	Time when the SQL statement execution ends
SQL Statement	Name of an SQL statement
Request Result	Result of requesting for executing an SQL statement

----End

Helpful Links

- If the entered SQL statement is not displayed, the connection between the agent and the database audit instance is abnormal. Rectify the fault by following the instructions in **What Do I Do If the Communication Between the Agent and Database Audit Instance Is Abnormal?**
- If SSL is enabled for a database, the database cannot be audited. To use database audit, disable SSL first. For details, see **How Do I Disable SSL for a Database?**.

8.3 Viewing Session Distribution

After connecting the database to the database audit instance, view session distribution of the database.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.
- A security group rule has been configured for the database audit instance.

Procedure

Step 1 Log in to the management console.

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

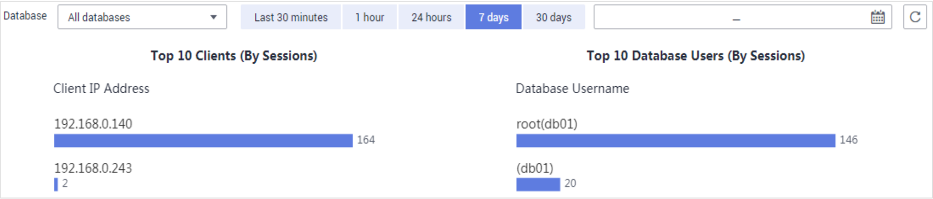
Step 3 In the **Instance** drop-down list, select the instance whose session information you want to view.

Step 4 Click the **Sessions** tab.

Step 5 View the session distribution chart, as shown in **Figure 8-9**.

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

Figure 8-9 Viewing session distribution



----End

8.4 Viewing Audit Reports

By default, database audit complies with a full audit rule, which is used to audit all databases that are successfully connected to the database audit instance. After connecting the database to the database audit instance, generate an audit report and preview online or download it.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.
- A security group rule has been configured for the database audit instance.

Report Types

Database audit provides eight types of report templates. **Table 8-2** lists the report names. You can generate reports and set report tasks as needed.

Table 8-2 Description

Template Name	Report Types	Description
Database Security General Report	Overview report	Provides the overall audit status of the database, including risks, sessions, and login status to better manage databases.
Database Security Compliance Report	Compliance report	This report helps database administrators and auditors detect abnormal behaviors, locate problems, and manage information.
SOX Report	Compliance report	Complies with the Sarbanes-Oxley Act (SOX) to provide statics on and evaluate database operations. This report helps database administrators and auditors detect abnormal behaviors, locate problems, and manage information.
Database Server Analysis Report	Database report	Provides statistics and analysis on active users, user IP addresses, database logins and requests, database usage duration, and database performance.
Client IP Address Analysis Report	Client report	Provides statistics on client applications, database users, and SQL statements collected from user IP addresses.
DML Command Report	Database operation report	Analyzes user and privileged operations based on DML commands.
DDL Command Report	Database operation report	Analyzes user and privileged operations based on DDL commands.
DCL Command Report	Database operation report	Analyzes user and privileged operations based on DCL commands.

Generating an Audit Report Immediately

Step 1 Log in to the management console.

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

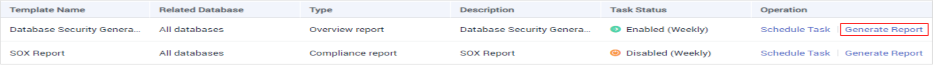
Step 3 In the navigation tree on the left, choose **Reports**.

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

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

Step 6 Locate the target template, and click **Generate Report** in the **Operation** column. See **Figure 8-10**.

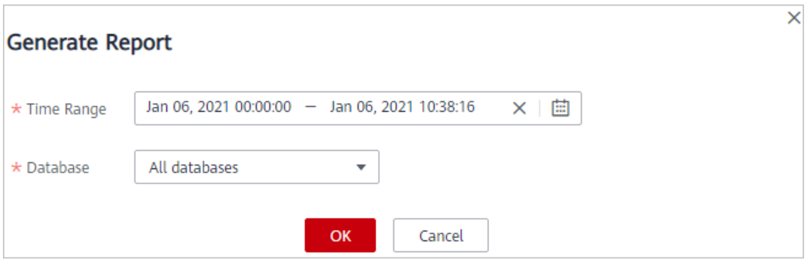
Figure 8-10 Report template list



Template Name	Related Database	Type	Description	Task Status	Operation
Database Security Genera...	All databases	Overview report	Database Security Genera...	Enabled (Weekly)	Schedule Task | Generate Report
SOX Report	All databases	Compliance report	SOX Report	Disabled (Weekly)	Schedule Task | Generate Report

Step 7 In the displayed dialog box, click 📅 to set the start time and end time of the report, and select the database for which you want to generate a report, as shown in **Figure 8-11**.

Figure 8-11 Generate Report



Generate Report

* Time Range: Jan 06, 2021 00:00:00 – Jan 06, 2021 10:38:16

* Database: All databases

Step 8 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.

----End

Previewing or Downloading an Audit Report

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

NOTICE

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

Step 1 Log in to the management console.

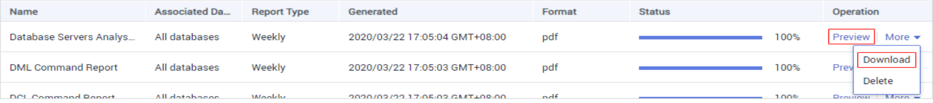
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 Locate the target template, and click **Preview** or **Download** in the **Operation** column to preview or download the report. See **Figure 8-12**..

Figure 8-12 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

Setting a Report Task

Step 1 Log in to the management console.

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

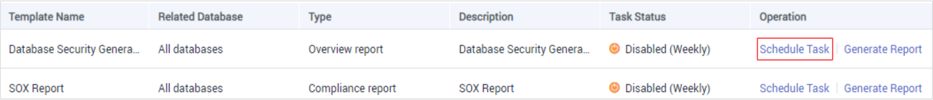
Step 3 In the navigation tree on the left, choose **Reports**.

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

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

Step 6 Locate the target template and click **Schedule Task** in the **Operation** column, as shown in **Figure 8-13**.

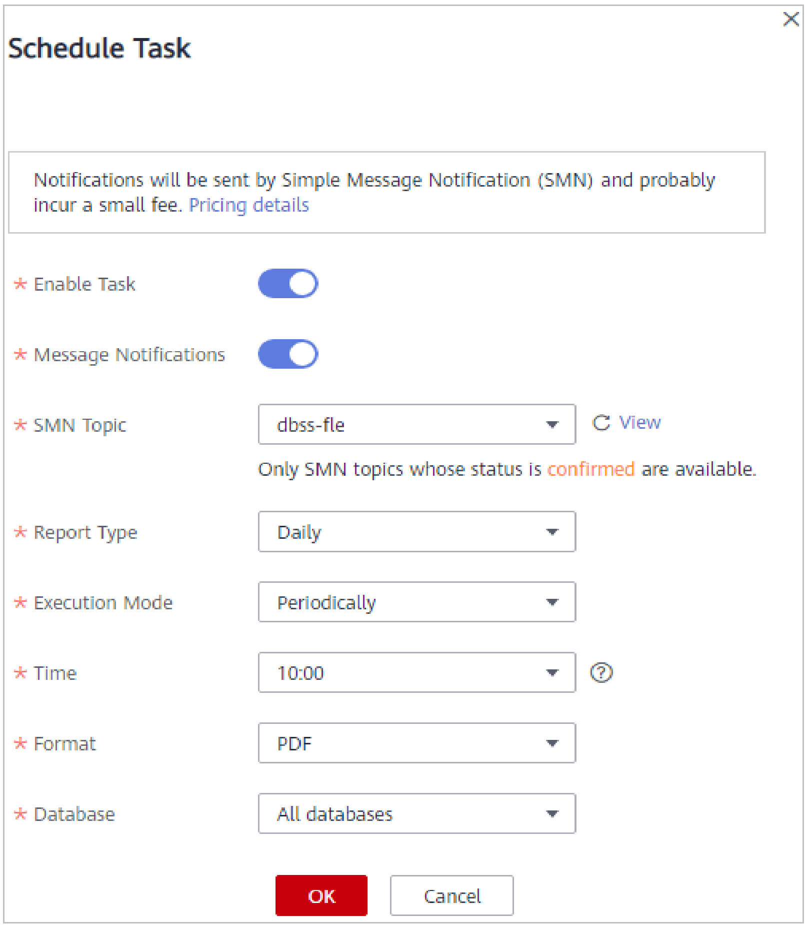
Figure 8-13 Setting a task



Template Name	Related Database	Type	Description	Task Status	Operation
Database Security Genera...	All databases	Overview report	Database Security Genera...	● Disabled (Weekly)	Schedule Task Generate Report
SOX Report	All databases	Compliance report	SOX Report	● Disabled (Weekly)	Schedule Task Generate Report

Step 7 In the displayed dialog box, set the parameters of the scheduled task, as shown in **Figure 8-14**. For details about related parameters, see **Table 8-3**.

Figure 8-14 Setting a scheduled task



Schedule Task

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

* Enable Task: ●

* Message Notifications: ●

* SMN Topic: dbss-fle

Only SMN topics whose status is confirmed are available.

* Report Type: Daily

* Execution Mode: Periodically

* Time: 10:00

* Format: PDF

* Database: All databases

Table 8-3 Parameters for setting a task

Parameter	Description	Example Value
Enable Task	Status of a scheduled task - ◉: enabled - ○: disabled	◉
Message Notifications	Enables or disables notifications. Notifications are sent by Simple SMN and will probably incur a small fee. See **SMN Pricing Details**. - ◉: enabled - ○: disabled	◉
SMN Topic	- Select an existing topic from the drop-down list or click **View** to create a topic. For details, see **Creating a Topic**. - You can add multiple subscriptions to a topic and select multiple subscription endpoints (such as SMS messages and emails). For details, see **Adding a Subscription**. For details about topics and subscriptions, see *Simple Message Notification User Guide*.	-
Report Type	Type of a report. The options are as follows: - **Daily** - **Weekly** - **Monthly**	Weekly
Execution Mode	Execution mode of the report. The options are as follows: - **Once** - **Periodically**	Periodically
Time	Time when the report is executed	10:00
Format	Only the PDF format is supported.	PDF
Database	Database for which you want to execute the report task	-

Step 8 Click **OK**.

----End

Helpful Links

Why I Cannot Preview the Database Security Audit Report Online?

9 Configuring Audit Rules

9.1 Adding Audit Scope

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 also add audit scope and specify the databases to be audited.

NOTICE

By default, the full audit rule takes effect even if other rules exist. To make another audit rule take effect, disable the full audit rule first.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.

Procedure

Step 1 Log in to the management console.

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

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

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

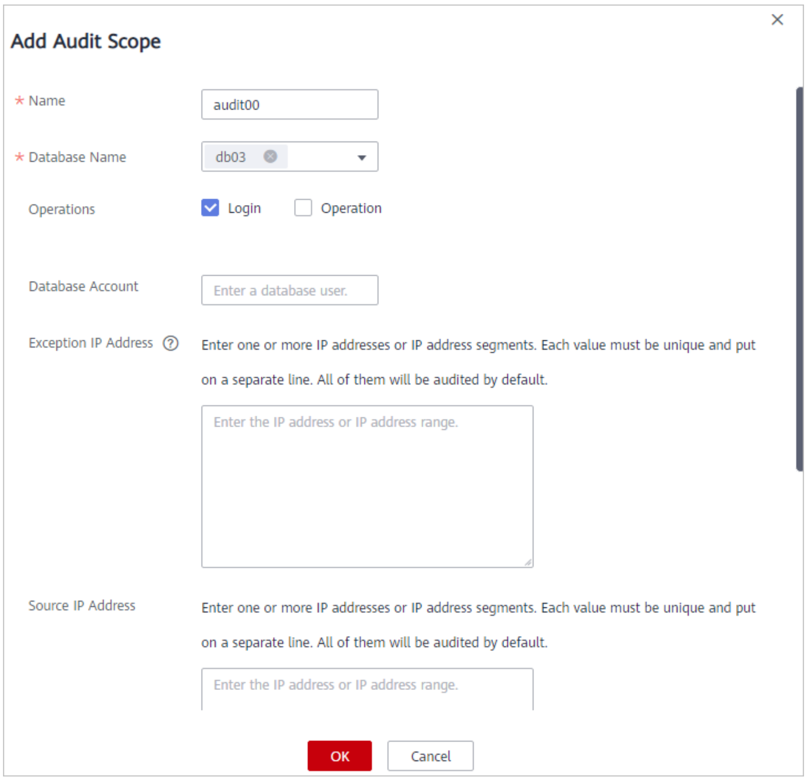
Step 5 **Add Audit Scope** above the audit scope list.

NOTE

- By default, database audit complies with a **full audit rule**, which is used to audit all databases that are connected to the database audit instance. This audit rule is enabled by default. You can disable it but cannot delete it.
- To make a custom rule take effect, disable the full audit rule first.

Step 6 In the displayed dialog box, set the audit scope, as shown in **Figure 9-1**. For details about related parameters, see **Table 9-1**.

Figure 9-1 Add Audit Scope dialog box



Add Audit Scope

* Name: audit00

* Database Name: db03

Operations: ☑ Login □ Operation

Database Account: Enter a database user.

Exception IP Address: Enter one or more IP addresses or IP address segments. Each value must be unique and put on a separate line. All of them will be audited by default.

Enter the IP address or IP address range.

Source IP Address: Enter one or more IP addresses or IP address segments. Each value must be unique and put on a separate line. All of them will be audited by default.

Enter the IP address or IP address range.

Table 9-1 Parameters

Parameter	Description	Example Value
Name	Name of the custom audit scope	audit00
Database Name	Select a database or **ALL**.	db03
Operations	Audited operation type. It can be **Login** or **Operation**. When you select the **Operation** check box, you can select **All operations** or the operations in **DDL**, **DML**, and **DCL**.	Login
Database Account	(Optional) Database username. You can specify multiple accounts, separated by commas (,).	-

Parameter	Description	Example Value
Exception IP Address	(Optional) IP addresses that do not need to be audited. **NOTE** If an IP address is set as both a source and an exception IP address, the IP address will not be audited.	-
Source IP Address	(Optional) IP address or IP address range used for accessing the database to be audited It must be an intranet IPv4 (for example, 192.168.1.1) or intranet IPv6 (for example, fe80:0000:0000:0000:0000:0000:0000:0000) address.	-
Source Port	(Optional) Port number used for accessing the database to be audited	-

Step 7 Click **OK**.

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

----End

Related Operations

In addition to adding the audit scope, you can enable or disable SQL injection detection and add risky operations to set audit rules for database audit.

9.2 Adding an SQL Injection Rule

You can add SQL injection rules to audit your databases.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- You have added a database and enabled database audit.
- A database has been added.

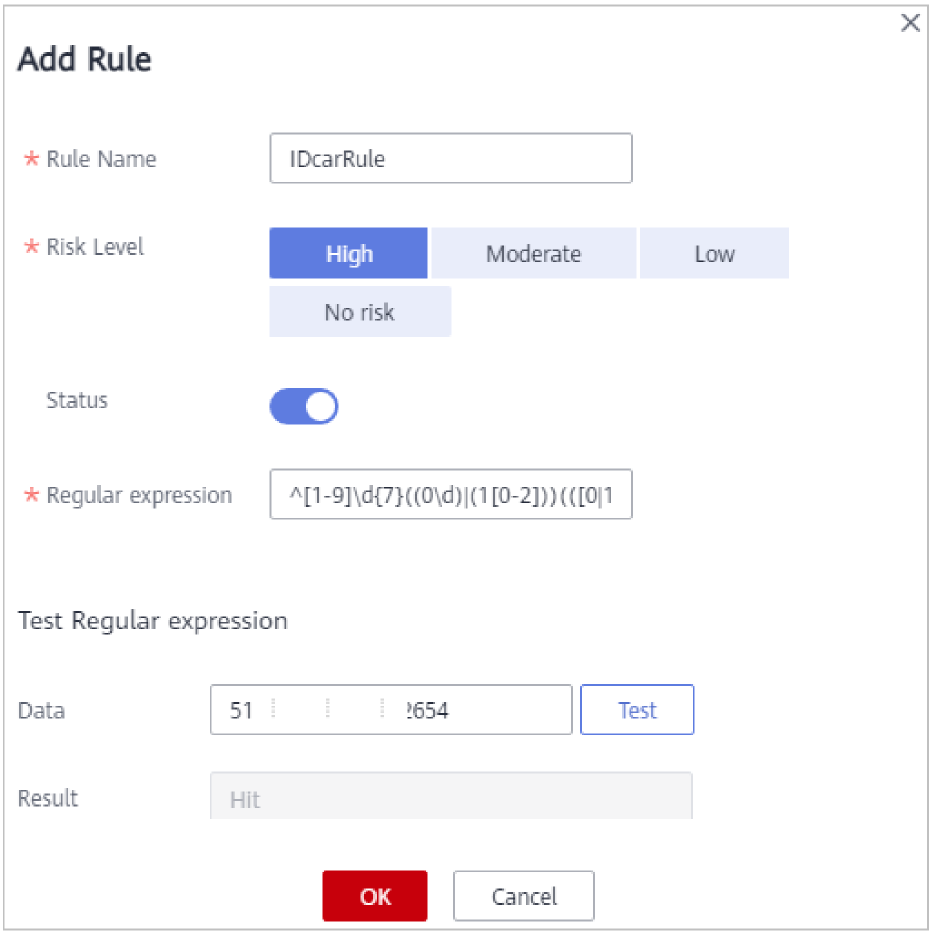
Procedure

Step 1 Log in to the management console.

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

Step 3 Click **Add Rule** and configure parameters. For more information, see **Table 9-2**.

Figure 9-2 Adding an SQL Injection Rule



Add Rule

* Rule Name: IDcarRule

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

Status: ●

* Regular expression: ^[1-9]\d{7}((0\d)|(1[0-2]))(([0|1

Test Regular expression

Data: 51[redacted]?654 | Test

Result: Hit

OK | Cancel

Table 9-2 SQL injection rule parameters

Parameter	Description	Example Value
Name	Name of an SQL rule.	Postal Code SQL injection Rule
Risk Level	Level of risks matching a SQL rule. Its value can be: • **High** • **Moderate** • **Low** • **No risk**	**Moderate**
Status	Enables or disables an SQL injection rule. • ●: enabled • ○: disabled	●

Parameter	Description	Example Value
Test Regular Expression	Regular expression that checks for content in certain pattern.	^\d{6}$
Data	Content that matches the regular expression. Enter content and click **Test** to verify that the regular expression works properly.	628307
Result	Test result. It can be: ● Hit ● Miss **NOTE** If the test result is **Hit**, the regular expression is correct. If the test result is **Miss**, the regular expression is incorrect.	Hit

Step 4 Confirm the information and click **OK**.

----End

9.3 Enabling or Disabling SQL Injection Detection

SQL injection detection is enabled by default. You can disable or enable the detection rules.

NOTICE

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

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- You can enable SQL injection detection when the status is **Disabled**.
- You can disable SQL injection detection when the status is **Enabled**.

Enabling SQL Injection Detection

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

Step 1 Log in to the management console.

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

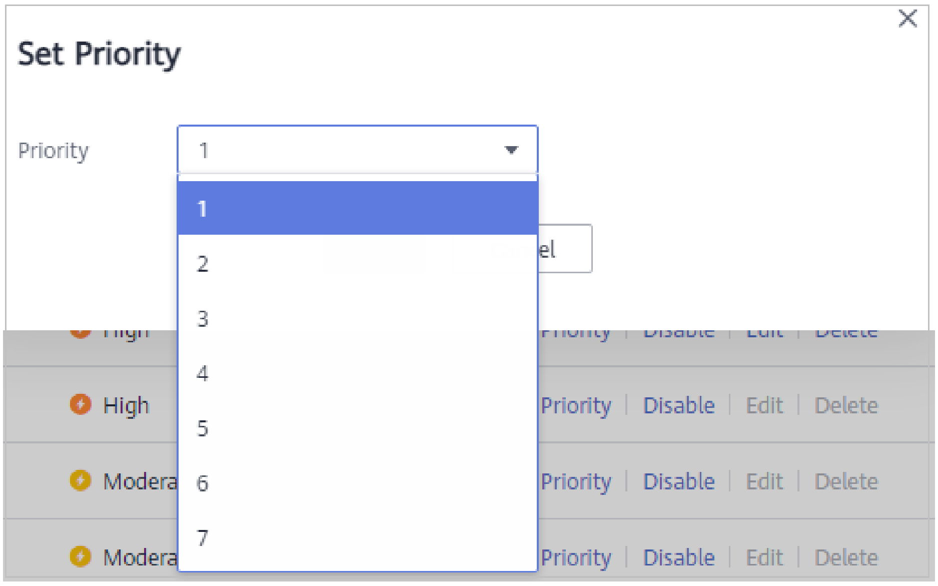
Step 3 In the navigation tree, choose **Rules**.

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

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

Step 6 Locate the target rule, and click **Set Priority** in the **Operation** column. In the displayed dialog box, select a priority. The smallest number indicates the highest priority. Click **OK**.

Figure 9-3 Configuring the priority



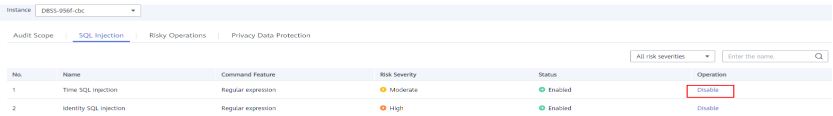
Set Priority

Priority 1

1
2
3
4
5
6
7
el
High
High
Modera
Modera
Priority | Disable | Edit | Delete
Priority | Disable | Edit | Delete
Priority | Disable | Edit | Delete

Step 7 Locate the target rule, and click **Disable** in the **Operation** column. See **Figure 9-4**.

Figure 9-4 Disabling an SQL injection detection rule



Instance DBSS-956f-cbc

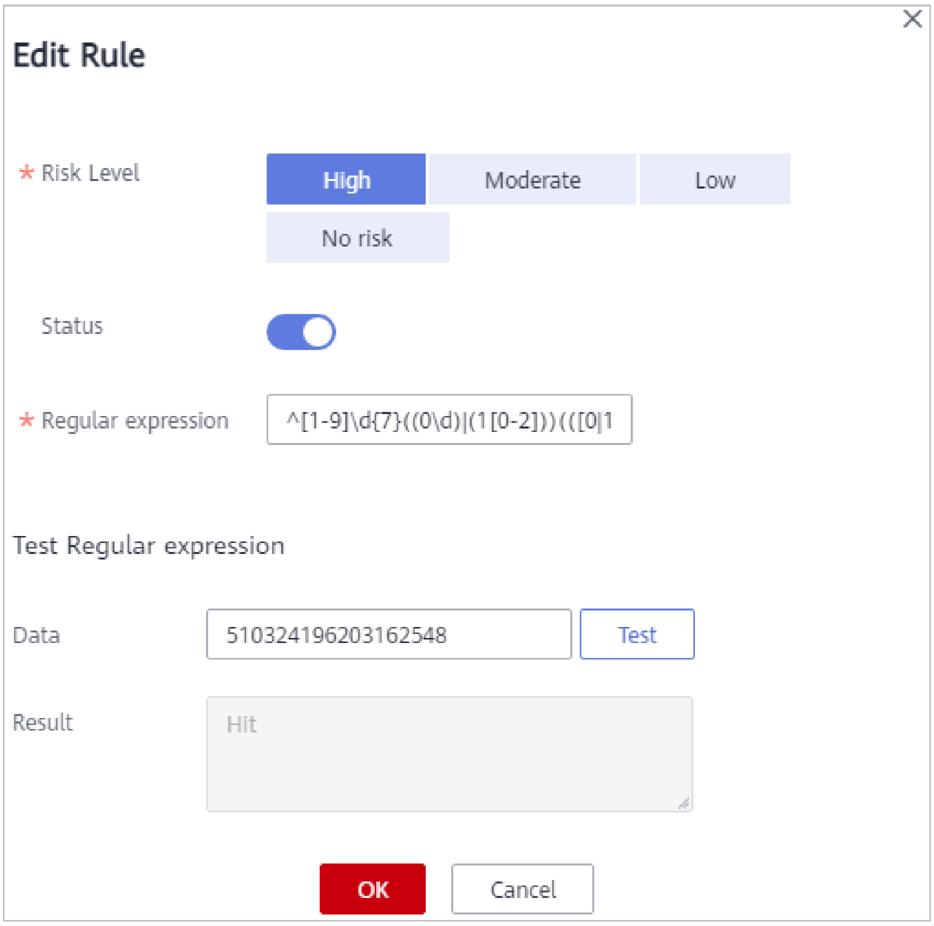
Audit Scope | SQL Injection | Risky Operations | Privacy Data Protection
All risk severities
Enter the name.

No.	Name	Command Feature	Risk Severity	Status	Operation
1	Time SQL injection	Regular expression	Moderate	Enabled	Disable
2	Identity SQL injection	Regular expression	High	Enabled	Disable

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

Step 8 Locate the target rule, and click **Edit** in the **Operation** column. Configure parameters and click **OK**. For more information, see **Table 9-3**.

Figure 9-5 Editing an SQL injection rule



Edit Rule

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

Status: ●

* Regular expression: ^[1-9]\d{7}((0\d)|(1[0-2]))(([0|1

Test Regular expression

Data: 510324196203162548

Result: Hit

Table 9-3 SQL injection rule parameters

Parameter	Description	Example Value
Name	Name of an SQL rule.	Postal Code SQL injection Rule
Risk Level	Level of risks matching a SQL rule. Its value can be: - **High** - **Moderate** - **Low** - **No risk**	**Moderate**
Status	Enables or disables an SQL injection rule. - ●: enabled - ○: disabled	●

Parameter	Description	Example Value
Test Regular Expression	Regular expression that checks for content in certain pattern.	^\d{6}$
Data	Content that matches the regular expression. Enter content and click **Test** to verify that the regular expression works properly.	628307
Result	Test result. It can be: ● Hit ● Miss **NOTE** If the test result is **Hit**, the regular expression is correct. If the test result is **Miss**, the regular expression is incorrect.	Hit

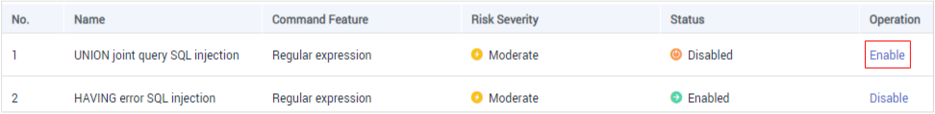
Step 9 In the **Operation** column, click **Delete**.

----End

Follow-Up Procedure

To restart an SQL injection detection rule, click **Enable** in the **Operation** column of the target rule, as shown in **Figure 9-6**.

Figure 9-6 Enabling an SQL injection detection rule



No.	Name	Command Feature	Risk Severity	Status	Operation
1	UNION joint query SQL injection	Regular expression	Moderate	Disabled	Enable
2	HAVING error SQL injection	Regular expression	Moderate	Enabled	Disable

When the status of an SQL injection detection rule is **Enabled**, SQL injection detection is enabled successfully.

9.4 Adding Risky Operations

Database audit has built-in rules for detecting data reduction and slow SQL statements. You can also add risky operations and customize detection rules.

NOTICE

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

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 In the **Instance** drop-down list, select an instance to add risky operations. Click the **Risky Operations** tab. Click **Add** above the risky operation list.

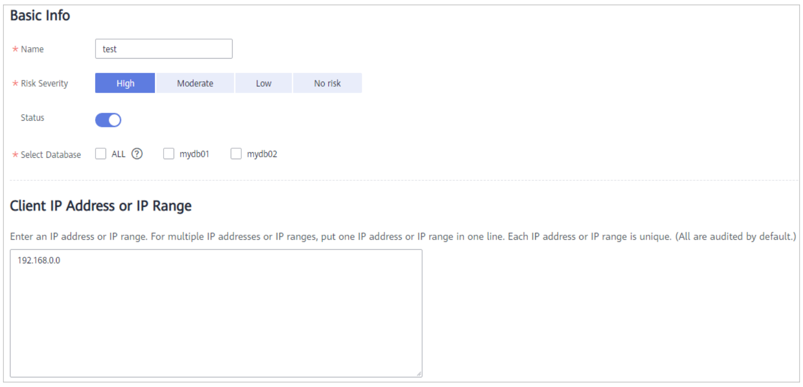
Step 5 In the **Instance** drop-down list, select an instance to add risky operations.

Step 6 Click the **Risky Operation** tab.

Step 7 Click **Add** above the risky operation list.

Step 8 On the **Add Risky Operation** page, set the basic information and client IP address, as shown in **Figure 9-7**. .

Figure 9-7 Setting the basic information and client IP address



Basic Info

* Name: test

* Risk Severity: High

Status: on

* Select Database: □ ALL □ mydb01 □ mydb02

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.)

192.168.0.0

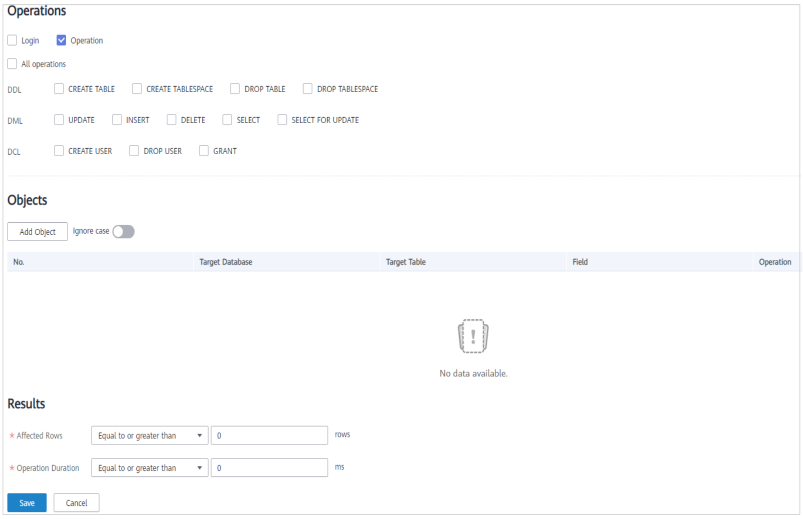
Table 9-4 Parameters

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

Parameter	Description	Example Value
Status	Status of a risky operation - ●: enabled - ○: disabled	●
Select Database	Database that the risky operation will be applied to You can select **ALL** or a specific database.	-
Client IP Address or IP Range	IP address or IP address range of the client The IP address can be an IPv4 address (for example, 192.168.1.1) or an IPv6 address (for example, fe80:0000:0000:0000:0000:0000:0000:0000).	192.168.0.0

Step 9 Set the operation type, operation object, and execution result, as shown in **Figure 9-8**. For details about related parameters, see **Table 9-5**.

Figure 9-8 Setting the operation type, operation object, and execution result



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

Objects

Add Object Ignore case ○

No.	Target Database	Target Table	Field	Operation

No data available.

Results

* Affected Rows: Equal to or greater than ▾ 0 rows

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

Table 9-5 Parameters

Parameter	Description	Example Value
Operations	Type of a risky operation, including **Login** and **Operation** When you select the **Operation** check box, you can select **All operations** or the operations in **DDL**, **DML**, and **DCL**.	Operation

Parameter	Description	Example Value
Objects	Enter the target database, target table, and field information after clicking **Add Operation Object**. Click **OK** to add an operation object.	-
Results	Set **Affected Rows** and **Operation Duration**. The operation conditions are as follows: ● **Greater than** ● **Less than** ● **Equal To** ● **Equal to or greater than** ● **Less than or equal to**	-

Step 10 Click **Save**.

----End

9.5 Configuring Privacy Data Protection Rules

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

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.

Procedure

Step 1 Log in to the management console.

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

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

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

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

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

- **Store Result Set**

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

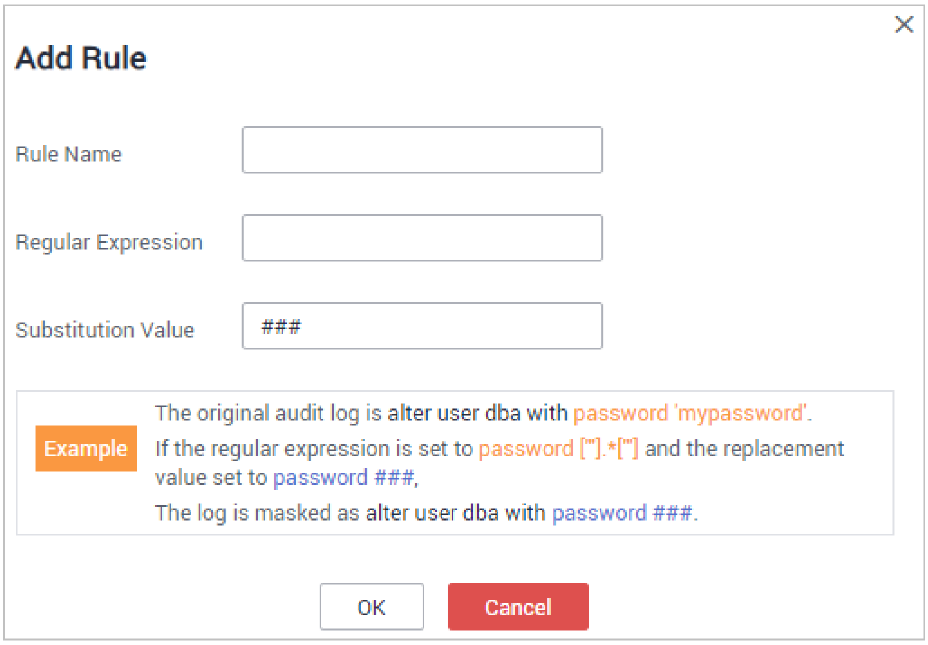
  Do not enable this function if you want to prepare for PCI DSS/PCI 3DS CSS certification.

- **Mask Privacy Data**

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

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

Figure 9-9 Add Rule dialog box



Add Rule

Rule Name

Regular Expression

Substitution Value: ###

Example

The original audit log is alter user dba with password 'mypassword'.

If the regular expression is set to password ['"].*['"] and the replacement value set to password ###,

The log is masked as alter user dba with password ###.

Table 9-6 Rule parameters

Parameter	Description	Example Value
Rule Name	Name of a rule	test
Regular Expression	Regular expression that specifies the sensitive data pattern	-
Substitution Value	Value used to replace sensitive data specified by the regular expression	###

Step 8 Click **OK**.

A masking rule in the **Enabled** status is added to the rule list.

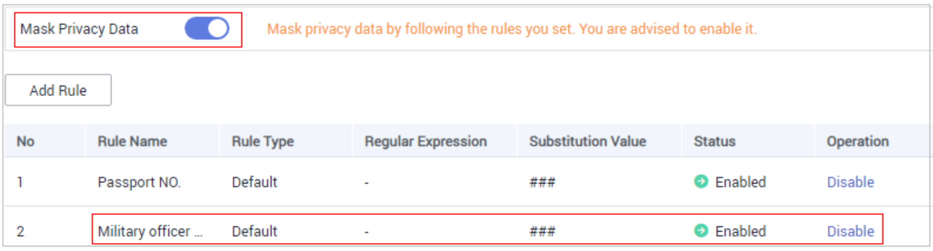
----End

Verifying a Rule

Perform the following steps to check whether a rule takes effect. The audit information about military officer card No. in a MySQL database is used as an example.

Step 1 Enable **Mask Privacy Data**, and ensure the "Military officer card NO." masking rule is enabled, as shown in **Figure 9-10**.

Figure 9-10 Enabling privacy data protection



Mask Privacy Data — 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
2	Military officer ...	Default	-	###	Enabled	Disable

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

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

select * from db where HOST="*Military officer card No.*";

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

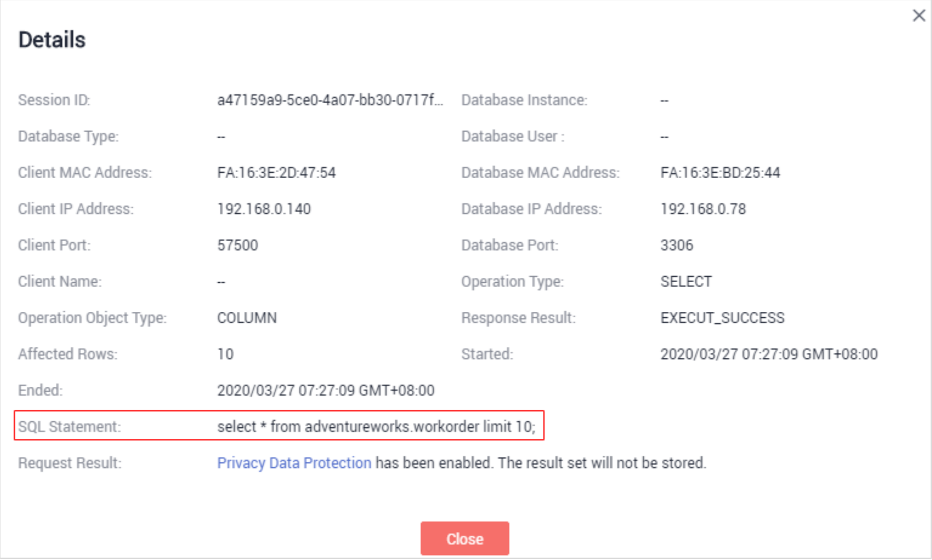
Step 5 In the **Instance** drop-down list, select the instance whose SQL statement information you want to view. Click the **Statements** tab.

Step 6 Set filtering conditions to find the entered SQL statement.

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

Step 8 Check the SQL statement information. The content of **SQL Statement** is shown in **Figure 9-11**, indicating that the masking function is normal.

Figure 9-11 SQL statement with sensitive data masked



Details

Session ID:	a47159a9-5ce0-4a07-bb30-0717f...	Database Instance:	--
Database Type:	--	Database User :	--
Client MAC Address:	FA:16:3E:2D:47:54	Database MAC Address:	FA:16:3E:BD:25:44
Client IP Address:	192.168.0.140	Database IP Address:	192.168.0.78
Client Port:	57500	Database Port:	3306
Client Name:	--	Operation Type:	SELECT
Operation Object Type:	COLUMN	Response Result:	EXECUT_SUCCESS
Affected Rows:	10	Started:	2020/03/27 07:27:09 GMT+08:00
Ended:	2020/03/27 07:27:09 GMT+08:00		
SQL Statement:	select * from adventureworks.workorder limit 10;		
Request Result:	Privacy Data Protection has been enabled. The result set will not be stored.		

----End

Common Operations

After adding a user-defined masking rule, you can perform the following operations on it:

- Disable

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

- Edit

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

- Delete

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

10 Configuring Email and Alarm Notifications

10.1 Configuring Email Notifications

After enabling email notifications, you can receive an email when an alarm is triggered or an audit report is generated.

Prerequisites

You have purchased a database audit instance and the **Status** is **Running**.

Procedure

Step 1 Log in to the management console.

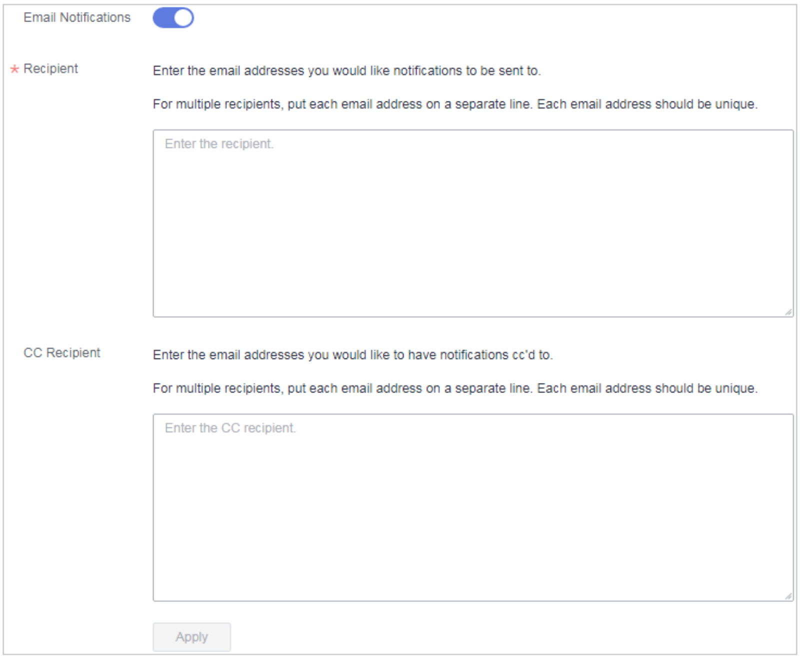
Step 2 Select a region, click ≡, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

Step 4 In the **Instance** drop-down list, select an instance to configure email settings

Step 5 Configure the email notification, as shown in **Figure 10-1**. **Table 10-1** describes the parameters.

Figure 10-1 Configuring email notifications



Email Notifications ●

* Recipient

Enter the email addresses you would like notifications to be sent to.

For multiple recipients, put each email address on a separate line. Each email address should be unique.

Enter the recipient.

CC Recipient

Enter the email addresses you would like to have notifications cc'd to.

For multiple recipients, put each email address on a separate line. Each email address should be unique.

Enter the CC recipient.

Apply

Table 10-1 Parameters

Parameter	Description	Example Value
Email Notifications	Status of the email notification function. By default, **Email Notifications** is enabled for database audit. You will receive an email when a configured alarm is triggered or an audit report is generated. - ●: enabled - ○: disabled	●
Recipient	Email address of the recipient	-
CC Recipient	Optional. Email address of the CC recipient	-

Step 6 Click **Apply**.

----End

10.2 Configuring Alarm Notifications

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

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

Prerequisites

You have purchased a database audit instance and the **Status** is **Running**.

Procedure

Step 1 Log in to the management console.

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

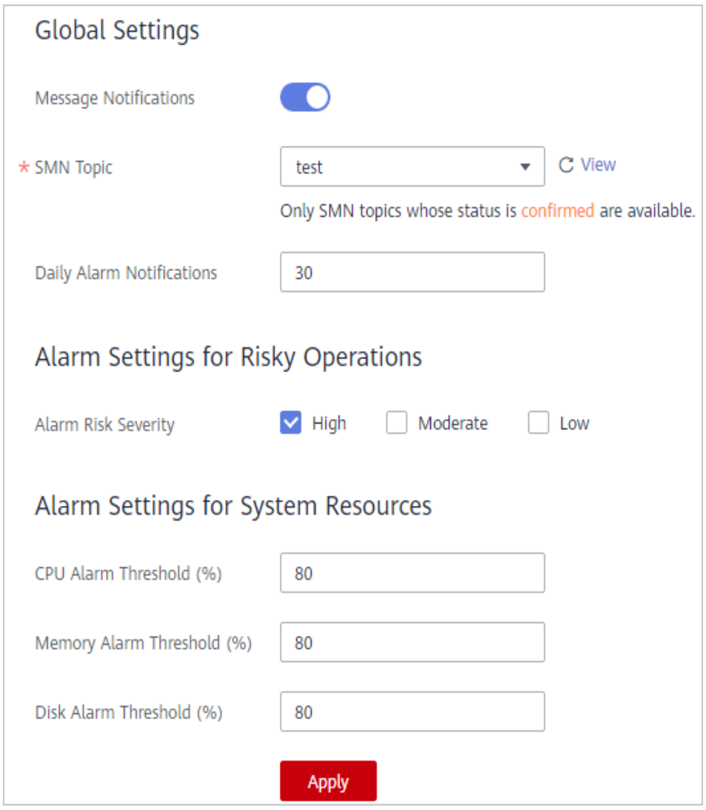
Step 3 In the navigation tree on the left, choose **Settings**.

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

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

Step 6 Set alarm notifications, as shown in **Figure 10-2**. For details about related parameters, see **Table 10-2**.

Figure 10-2 Configuring alarm notifications



Global Settings

Message Notifications: ●

* SMN Topic: test ▾ View

Only SMN topics whose status is confirmed are available.

Daily Alarm Notifications: 30

Alarm Settings for Risky Operations

Alarm Risk Severity: ☑ High ☐ Moderate ☐ Low

Alarm Settings for System Resources

CPU Alarm Threshold (%): 80

Memory Alarm Threshold (%): 80

Disk Alarm Threshold (%): 80

Table 10-2 Alarm notification parameters

Parameter	Description	Example Value
Message Notifications	Enables or disables notifications. Database audit alarm notifications are sent by SMN and will probably incur a small fee. See **SMN Pricing Details**. - ◉: enabled - ○: disabled	◉
SMN Topic	- Select an existing topic from the drop-down list or click **View** to create a topic. For details, see **Creating a Topic**. - You can add multiple subscriptions to a topic and select multiple subscription endpoints (such as SMS messages and emails). For details, see **Adding a Subscription**. **NOTE** Before selecting a topic, ensure that the subscription status of the topic is **Confirmed**. Otherwise, alarm notifications may not be received. For details about topics and subscriptions, see *Simple Message Notification User Guide*.	-
Daily Alarm Notifications	Total number of alarms allowed to be sent every day **NOTICE** - If the number of alarms exceeds this value on a day, no more notification will be sent on that day. - There is no fixed time point for sending alarm notifications. The system collects statistics every 5 minutes and sends alarm notifications (if any).	30
Alarm Risk Severity	Risk severity of the risk log. The options are as follows: - **High** - **Moderate** - **Low**	High
CPU Alarm Threshold (%)	CPU alarm threshold of an audit instance. When the threshold is exceeded, an alarm notification is generated.	80
Memory Alarm Threshold (%)	Memory alarm threshold of an audit instance. When the threshold is exceeded, an alarm notification is generated.	80

Parameter	Description	Example Value
Disk Alarm Threshold (%)	Disk alarm threshold of an audit instance. When the threshold is exceeded, an alarm notification is generated.	80

Step 7 Click **Apply**.

----End

11 Viewing Monitoring Information

11.1 Viewing the System Monitoring

This section describes how to view the system monitoring of database audit and learn about system resources and traffic usage.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.

Procedure

Step 1 Log in to the management console.

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

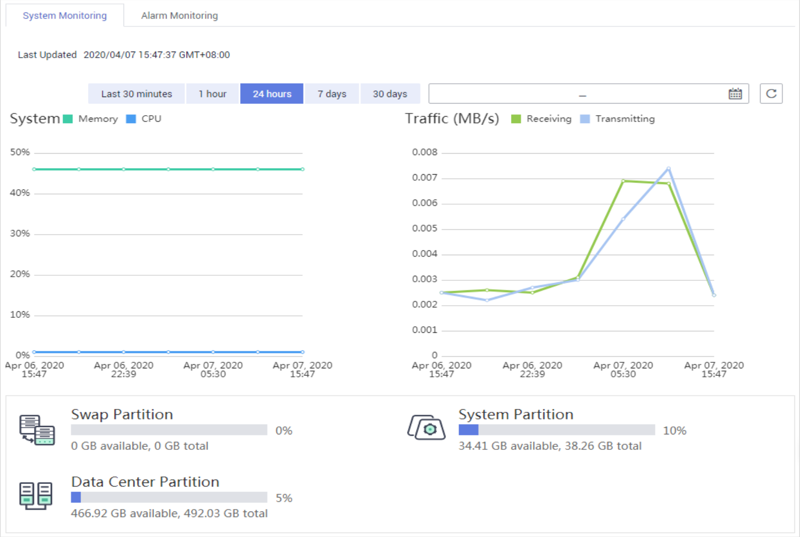
Step 3 In the navigation tree on the left, choose **Instances**.

Step 4 Click an instance name and then click the **Monitoring** tab. The **System Monitoring** page is displayed.

Step 5 View the system monitoring information, as shown in**Figure 11-1**.

Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days**, or click 📅 to customize start time and end time to view the system monitoring information of the specified time range.

Figure 11-1 Viewing the system monitoring



Last Updated 2020/04/07 15:47:37 GMT+08:00

Swap Partition 0%
0 GB available, 0 GB total

System Partition 10%
34.41 GB available, 38.26 GB total

Data Center Partition 5%
466.92 GB available, 492.03 GB total

----End

11.2 Viewing the Alarms

This section describes how to view and confirm alarms of database audit.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.
- You have configured alarm notifications.

Procedure

Step 1 Log in to the management console.

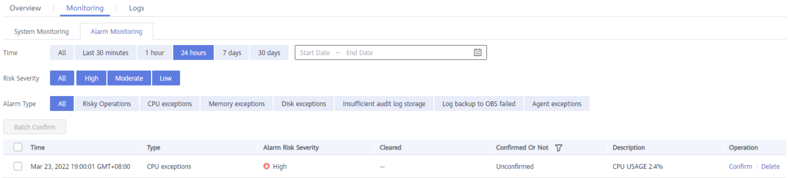
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 View the alarm information, as shown in **Figure 11-2**. For details about related parameters, see **Table 11-1**.

Figure 11-2 Viewing the alarms



Time: 24 hours

Risk Severity: All High Moderate Low

Alarm Type: All

□	Time	Type	Alarm Risk Severity	Cleared	Confirmed Or Not	Description	Operation
□	Mar 23, 2022 19:00:01 GMT+08:00	CPU exceptions	● High	--	Unconfirmed	CPU USAGE 2.4%	Confirm | Delete

Table 11-1 Parameters of alarms

Parameter	Description
Time	Time when an alarm occurred.
Type	Alarm type. The options are as follows: ● Risky operations ● CPU exceptions ● Memory exceptions ● Disk exceptions ● Insufficient audit log storage ● Log backup to OBS failed ● Agent exceptions
Alarm Risk Severity	Risk severity of an alarm. The options are as follows: ● **High** ● **Moderate** ● **Low**
Cleared	Time when an alarm is cleared
Confirmed Or Not	Confirmation status of an alarm. Click ▽ to filter alarms in **Unconfirmed** or **Confirmed** state.
Description	Description of an alarm

To query specified alarms, perform the following steps:

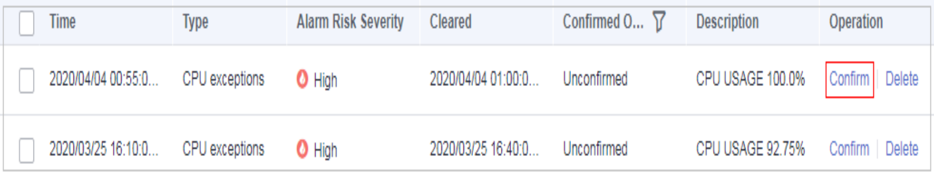
- Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days** for **Time**, or click 📅 to set start time and end time, and click **OK** to view alarms of the specified time range.
- Select **All**, **High**, **Moderate**, or **Low** for **Risk Severity**. Alarms of specified severity are displayed in the list.
- Select an alarm type, and alarms of specified alarm type is displayed in the list.

----End

Follow-Up Procedure

To confirm an alarm, click **Confirm** in the **Operation** column of the alarm, as shown in **Figure 11-3**.

Figure 11-3 Confirming an alarm



□	Time	Type	Alarm Risk Severity	Cleared	Confirmed O... ▽	Description	Operation
□	2020/04/04 00:55:0...	CPU exceptions	● High	2020/04/04 01:00:0...	Unconfirmed	CPU USAGE 100.0%	Confirm | Delete
□	2020/03/25 16:10:0...	CPU exceptions	● High	2020/03/25 16:40:0...	Unconfirmed	CPU USAGE 92.75%	Confirm | Delete

NOTE

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

12 Backing Up and Restoring Database Audit Logs

Database audit logs can be backed up to OBS buckets to achieve high availability for disaster recovery. You can back up or restore database audit logs as required.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.

Precautions

- Audit logs are backed up to OBS. Buckets are automatically created for you and billed per use.

OBS Fine-grained Authorization

DBSS backup and restoration require OBS permissions. Users without IAM authorization permissions must be manually authorized by a user having the **Security Administrator** permission.

Step 1 Log in to the management console.

Step 2 Select a region, click ≡ in the upper left corner, and choose **Management & Governance** > **Identity and Access Management**.

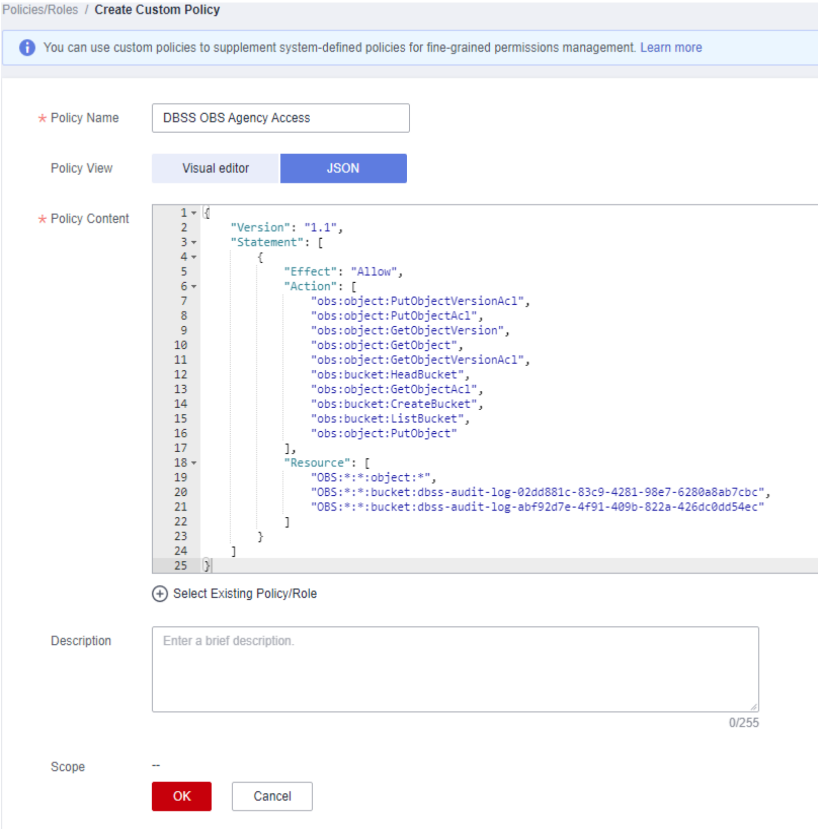
Step 3 In the navigation pane, choose **Permissions** > **Authorization**. Click **Create Custom Policy**.

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

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:object:PutObjectVersionAcl",
                "obs:object:PutObjectAcl",
                "obs:object:GetObjectVersion",
                "obs:object:GetObject",
                "obs:object:GetObjectVersionAcl",
                "obs:bucket:HeadBucket",
                "obs:object:GetObjectAcl",
                "obs:bucket:CreateBucket",
                "obs:bucket:ListBucket",
                "obs:object:PutObject"
            ],
            "Resource": [
                "OBS:*:*:object:*",
                "OBS:*:*:bucket:OBS_Bucket_Name_1",
                "OBS:*:*:bucket:OBS_bucket_2" //You can add multiple buckets.
            ]
        }
    ]
}
```

See **Figure 12-1**. Click **OK**.

Figure 12-1 Creating a custom policy



Policies/Roles / Create Custom Policy

You can use custom policies to supplement system-defined policies for fine-grained permissions management. Learn more

* Policy Name: DBSS OBS Agency Access

Policy View: Visual editor | JSON

* Policy Content:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:object:PutObjectVersionAcl",
                "obs:object:PutObjectAcl",
                "obs:object:GetObjectVersion",
                "obs:object:GetObject",
                "obs:object:GetObjectVersionAcl",
                "obs:bucket:HeadBucket",
                "obs:object:GetObjectAcl",
                "obs:bucket:CreateBucket",
                "obs:bucket:ListBucket",
                "obs:object:PutObject"
            ],
            "Resource": [
                "OBS:*:*:object:*",
                "OBS:*:*:bucket:dbss-audit-log-02dd881c-83c9-4281-98e7-6280a8ab7cbc",
                "OBS:*:*:bucket:dbss-audit-log-abf92d7e-4f91-409b-822a-426dc0dd54ec"
            ]
        }
    ]
}
```

⊕ Select Existing Policy/Role

Description: Enter a brief description.

0/255

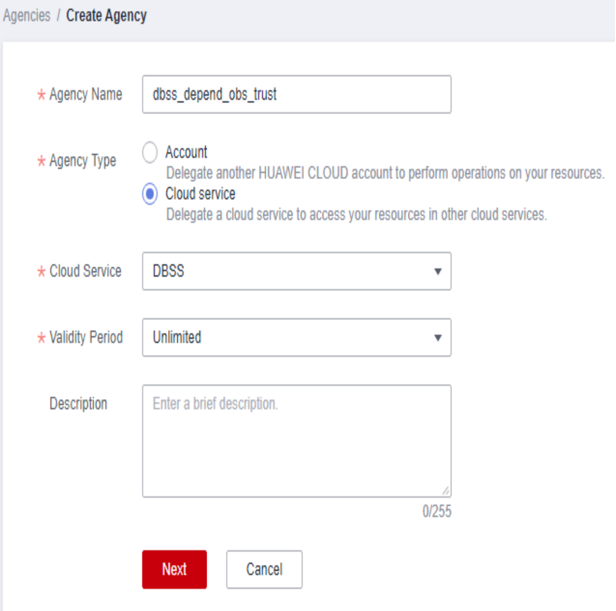
Scope: --

OK | Cancel

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

Step 6 Configure agency parameters. Set **Agency Name** to **dbss_depend_obs_trust**. Set **Agency Type** to **Cloud service**. Set **Cloud Service** to **DBSS**. See **Figure 12-2**.

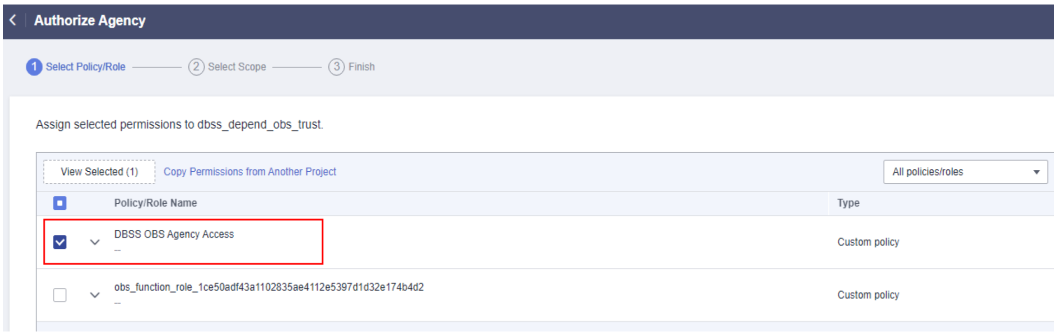
Figure 12-2 Creating an agency



* Agency Name	dbss_depend_obs_trust
* Agency Type	○ Account Delegate another HUAWEI CLOUD account to perform operations on your resources. ● Cloud service Delegate a cloud service to access your resources in other cloud services.
* Cloud Service	DBSS
* Validity Period	Unlimited
Description	Enter a brief description. 0/255

Step 7 Click **Next**. Select the custom policy created in **Step 4**, and add the permission **DBSS OBS Agency Access** to the agency **dbss_depend_obs_trust**, as shown in **Figure 12-3**. Click **Next** in the lower right corner.

Figure 12-3 Selecting a policy

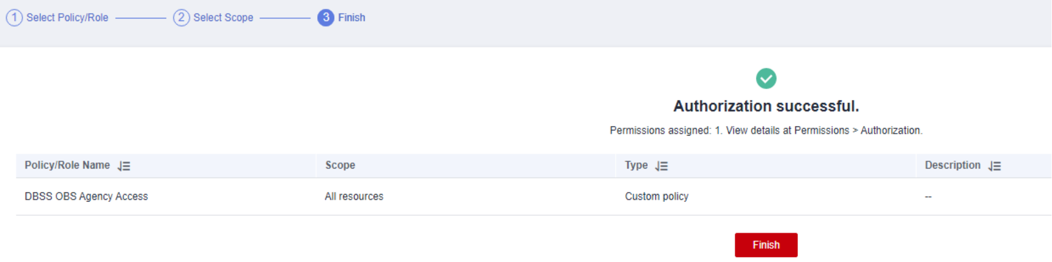


Assign selected permissions to dbss_depend_obs_trust.

	Policy/Role Name	Type
☑	DBSS OBS Agency Access --	Custom policy
□	obs_function_role_1ce50adf43a1102835ae4112e5397d1d32e174b4d2 --	Custom policy

Step 8 Set **Scope** to **All resources** and click **OK**. If the message in **Figure 12-4** is displayed, the authorization is successful. Click **Finish**. The authorization will take effect in about 15 minutes.

Figure 12-4 Authorization completed



Authorization successful.

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

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

----End

Automatically Backing Up Database Audit Logs

Step 1 Log in to the management console.

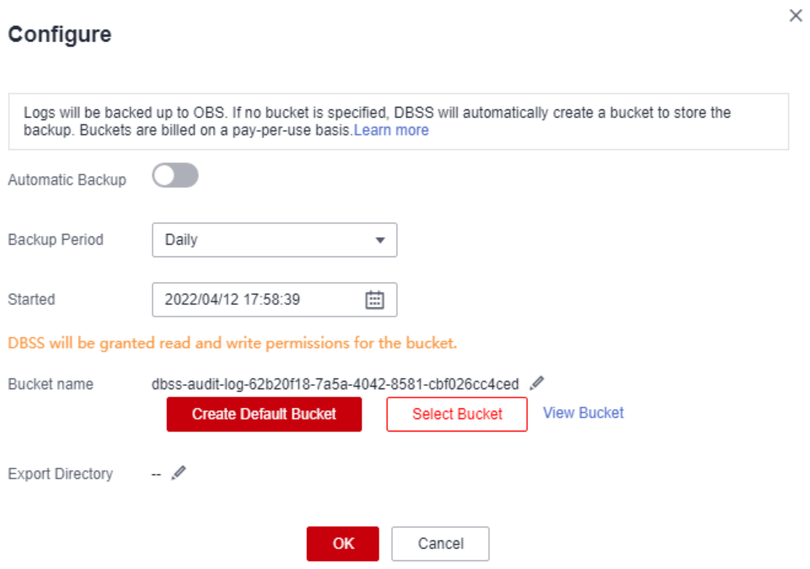
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 Click **Configure**. In the displayed dialog box, set the parameters, as shown in **Figure 12-5**. For details about related parameters, see **Table 12-1**.

Figure 12-5 Configure Automatic Backup dialog box



Configure

Logs will be backed up to OBS. If no bucket is specified, DBSS will automatically create a bucket to store the backup. Buckets are billed on a pay-per-use basis.Learn more

Automatic Backup

Backup Period: Daily

Started: 2022/04/12 17:58:39

DBSS will be granted read and write permissions for the bucket.

Bucket name: dbss-audit-log-62b20f18-7a5a-4042-8581-cbf026cc4ced

Export Directory: --

Table 12-1 Parameters

Parameter	Description	Example Value
Automatic Backup	Status of automatic backup ● : enabled ○ : disabled	●
Backup Period	Automatic backup period. Its options are as follows: - **Daily** - **Hourly**	Daily
Started	Start time of the backup. Click 📅 to configure.	2020/01/14 20:27:08

Parameter	Description	Example Value
Bucket Name	Name of the OBS bucket used for backup. Its options are as follows: ● Create Default Bucket ● Select Bucket **NOTE** ● If you click **Create Default Bucket**, you will be prompted to authorize OBS for exporting audit log backups. ● Audit logs can be exported only to the bucket created by DBSS.	20f18-7a5a-4042
Export Directory	Directory for storing backup files in the OBS bucket.	test

Step 6 Click **OK**.

NOTE

After the automatic backup function is configured, new data in the database will be backed up one hour later. Then you can view the backup information.

----End

Restoring Database Audit Logs

After backing up database audit logs, you can restore the audit logs as required.

NOTICE

Restoring logs is risky. Therefore before restoring logs, ensure that the backup log data is correct or complete.

Step 1 Log in to the management console.

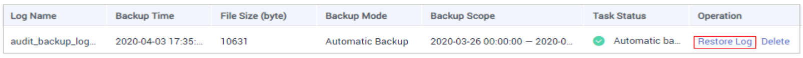
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 In the **Operation** column of the backup log to be restored, click **Restore Log**, as shown in **Figure 12-6**.

Figure 12-6 Restoring logs



Log Name	Backup Time	File Size (byte)	Backup Mode	Backup Scope	Task Status	Operation
audit_backup_log...	2020-04-03 17:35:...	10631	Automatic Backup	2020-03-26 00:00:00 – 2020-0...	✓ Automatic ba...	Restore Log Delete

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

----End

Exporting Risk Data

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

NOTE

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

Step 1 Log in to the management console.

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

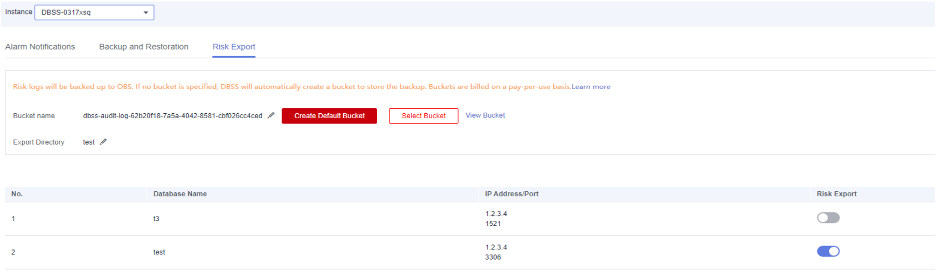
Step 3 In the navigation tree on the left, choose **Settings**.

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

Step 5 Click ○ in the row of a database to export risk data. An OBS bucket will be automatically created to store risk logs. See **Figure 12-7**.

- **Bucket Name**:Click **Create Default Bucket** or **Select Bucket**.
- **Export Directory**: Create a directory for storing risk files in the OBS bucket.

Figure 12-7 Automatically creating an OBS bucket



Instance DBSS-0317xsq

Risk logs will be backed up to OBS. If no bucket is specified, DBSS will automatically create a bucket to store the backup. Buckets are billed on a pay-per-use basis.Learn more

Bucket name dbss-audit-log-62b20f18-7a5a-4042-8581-cbf026cc4ced

Export Directory test

No.	Database Name	IP Address/Port	Risk Export
1	t3	1.2.3.4 1521	○
2	test	1.2.3.4 3306	●

----End

13 Other Operations

13.1 Managing Database Audit Instances

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

Prerequisites

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

Viewing the Instance

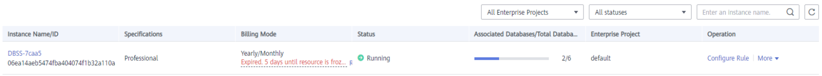
Step 1 Log in to the management console.

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

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

Step 4 View the database audit instances information, as shown in **Figure 13-1**. For details about related parameters, see **Table 13-1**.

Figure 13-1 Viewing database audit instances



Instance Name/ID	Specifications	Billing Mode	Status	Associated Databases/Total Databa...	Enterprise Project	Operation
DBSS-7caa5 06ea14aeb5474fba404074f1b32a110a	Professional	Yearly/Monthly Expired. 5 days until resource is froz...	Running	2/6	default	Configure Rule | More

NOTE

- You can click the name of an instance to view its overview.
- Select an instance status from the **All statuses** drop-down list in the upper right corner of the list, or enter a key word of an instance to search for it.

Table 13-1 Parameters

Parameter	Description
Instance Name/ID	Name and ID of an instance. Instance ID is automatically generated.
Specifications	Edition of an instance
Billing Mode	Billing mode (yearly/monthly) and expiration time of the instance
Status	Running status of an instance. The options are as follows: ● **Running** ● **Creating** ● **Faulty** ● **Disabled** ● **Frozen** ● **Frozen for legal management** ● **Frozen due to abuse** ● **Frozen due to lack of identity verification** ● **Frozen for partnership** ● **Creation failed**
Associated Databases/ Total Databases	Number of databases an instance has associated with and Number of databases an instance supports
Enterprise Project	Enterprise project name of the instance
Operation	Configure audit rules for an instance, or restart or enable the instance.

NOTE

You can perform the following operations on instances as required:

- Restart

  Locate the row that contains the desired instance, choose **More** > **Restart** in the **Operation** column, and click **OK** in the displayed dialog box.

- Enable

  Locate the row that contains the desired instance, choose **More** > **Enable** in the **Operation** column, and click **OK** in the displayed dialog box.

- Disable

  Locate the row that contains the desired instance, choose **More** > **Disable** in the **Operation** column, and click **OK** in the displayed dialog box. When an instance is disabled, the audit function is disabled for the databases on the instance.

- Delete

  Locate the row that contains the instance that failed to be created, choose **More** > **Delete** in the **Operation** column, and click **Delete** in the displayed dialog box. Deleted instances will not be displayed in the instance list.

----End

13.2 Viewing the Instance Overview

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

Prerequisites

You have purchased a database audit instance and the **Status** is **Running**.

Procedure

Step 1 Log in to the management console.

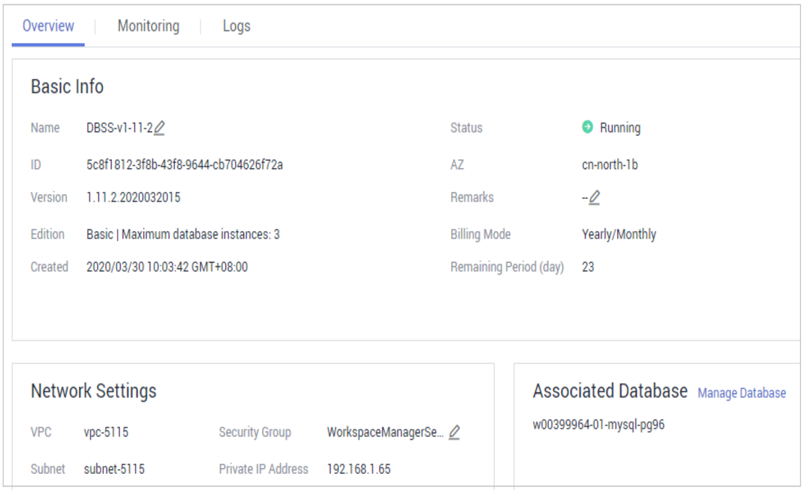
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 View the basic information, network settings, and associated databases about the instance. See **Figure 13-2**. For details about related parameters, see **Table 13-2**.

Figure 13-2 Viewing the instance overview



Basic Info

Name DBSS-v1-11-2 ✎

ID 5c8f1812-3f8b-43f8-9644-cb704626f72a

Version 1.11.2.2020032015

Edition Basic | Maximum database instances: 3

Created 2020/03/30 10:03:42 GMT+08:00

Status ● Running

AZ cn-north-1b

Remarks -- ✎

Billing Mode Yearly/Monthly

Remaining Period (day) 23

Network Settings

VPC vpc-5115

Subnet subnet-5115

Security Group WorkspaceManagerSe... ✎

Private IP Address 192.168.1.65

Associated Database Manage Database

w00399964-01-mysql-pg96

Table 13-2 Parameters of the instance overview

Category	Parameter	Description
Basic Info	Name	Name of an instance. You can click ✎ next to **Name** to change it.
	Status	Running status of an instance. The options are as follows: - **Running** - **Creating** - **Faulty** - **Disabled** - **Frozen** - **Frozen for legal management** - **Frozen due to abuse** - **Frozen due to lack of identity verification** - **Frozen for partnership** - **Creation failed**
	ID	Instance ID, which is automatically generated
	AZ	Availability Zone (AZ) where an instance resides
	Version	Version of an instance
	Remarks	Remarks about an instance Click ✎ next to remarks to modify it.
	Edition	Edition of an instance
	Billing Mode	Billing mode of an instance
	Created	Time when an instance is created

Category	Parameter	Description
	Remaining Period (day)	Remaining days for which an instance can be used
Network Settings	VPC	VPC where an instance resides
	Security Group	Security group where an instance resides
	Subnet	Subnet where an instance resides
	Private IP Address	IP address of an instance
Associated Database	-	Database information associated with an instance Click **Manage Database**, and the **Databases** page is displayed. For details about how to add a database, see **Step 1: Add a Database**.

----End

13.3 Managing Databases and Agents

After adding a database successfully, you can view, disable or delete the database. After adding an agent to the database, you can view, disable or delete the agent.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- You have added a database successfully.
- Before disabling a database, ensure that **Audit Status** of the database is **Enabled**.

Viewing the Database Information

Step 1 Log in to the management console.

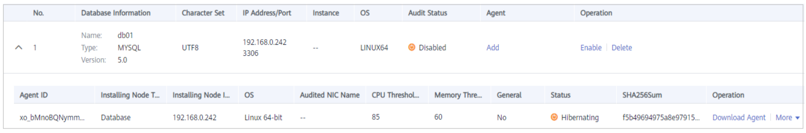
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 View the database information, as shown in **Figure 13-3**. For details about related parameters, see **Table 13-3**.

Figure 13-3 Viewing the database and agent information



No.	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
1	Name: db01 Type: MYSQL Version: 5.0	UTF8	192.168.0.242 3306	--	LINUX64	● Disabled	Add	Enable | Delete

Agent ID	Installing Node T...	Installing Node I...	OS	Audited NIC Name	CPU Threshol...	Memory Thre...	General	Status	SHA256Sum	Operation
xo_bMnoBQNymm...	Database	192.168.0.242	Linux 64-bit	--	85	60	No	● Hibernating	f5b49694975a8e97915...	Download Agent | More ▾

NOTE

Select an audit status from the **All audit statuses** drop-down list in the upper right corner of the list, or enter a key word of a database to search for it.

Table 13-3 Parameters

Parameter	Description	Example Value
Database Information	Name, type, and version of a database	-
Character Set	Encoding character set of the database	UTF8
IP Address/ Port	IP address of the database	192.168.0.104 3306
Instance	Database instance name	-
OS	Operating system of the database	LINUX64
Audit Status	Audit status of the database. The options are as follows: ● **Enabled** ● **Disabled**	Enabled
Agent	Click **Add** to add an agent for the database.	-

NOTE

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

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

----End

Viewing an Agent

Step 1 Log in to the management console.

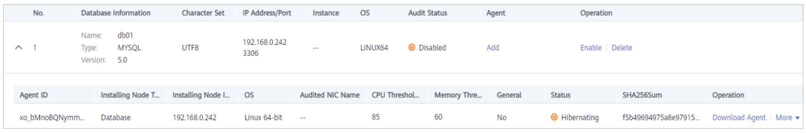
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 Click ⌄ on the left of the database to expand the agent details, as shown in **Figure 13-4**. For details about related parameters, see **Table 13-4**.

Figure 13-4 Viewing the database and agent information



No.	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
^ 1	Name: db01 Type: MYSQL Version: 5.0	UTF8	192.168.0.242 3306	--	LINUX64	● Disabled	Add	Enable | Delete

Agent ID	Installing Node T...	Installing Node I...	OS	Audited NIC Name	CPU Threshol...	Memory Thre...	General	Status	SHA256Sum	Operation
xo_bMnoBQNymm...	Database	192.168.0.242	Linux 64-bit	--	85	60	No	● Hibernating	f5b49694975a8e97915...	Download Agent | More ▾

Table 13-4 Parameters of an agent

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

NOTE

You can perform the following operations on an agent you added:

- Disable
  - Locate the row that contains the agent to be disabled, click **Disable** in the **Operation** column, and click **OK** in the displayed dialog box. The status of the agent will change to **Disabled**.
  - When an agent is disabled, database audit is disabled for the associated database.
- Delete
  - Locate the row that contains the agent to be deleted, click **Delete** in the **Operation** column, and click **OK** in the displayed dialog box.
  - After an agent is deleted, add another agent again if you want to audit the database.

----End

13.4 Uninstalling an Agent

You can uninstall an agent from the database or application if you do not need to audit the database.

Prerequisites

You have installed an agent on the desired node.

Uninstalling the Agent from a Linux OS

Step 1 Log in to the node where the agent is installed as user **root** using SSH through a cross-platform remote access tool (such as PuTTY).

Step 2 Run the following command to access the directory where the decompressed **xxx.tar.gz** agent installation package is stored:

cd *directory containing the decompressed agent installation package*

Step 3 Run the following command to check whether you have the permission for executing the **uninstall.sh** script:

ll

- If you do, go to **Step 4**.
- If you do not, perform the following operations:
  a. Run the following command to get the script execution permission:

     chmod +x uninstall.sh

  b. Verify you have the required permissions.

Step 4 Run the following command to uninstall the agent:

sh uninstall.sh

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

```
uninstall audit agent...
exist os-release file
```

```
stopping audit agent
audit agent stopped
stop audit_agent success
service audit_agent does not support chkconfig
uninstall audit agent completed!
```

----End

Uninstalling the Agent from a Windows OS

Step 1 Enter the directory where the agent installation file is stored.

Step 2 Double-click the **uninstall.bat** file to uninstall the agent.

Step 3 Verify the agent has been uninstalled.

1. Open the Task Manager and verify the dbss_audit_agent process is stopped.
2. Verify the entire agent installation directory has been deleted.

----End

13.5 Management an Audit Scope

After adding an audit scope, you can view, enable, edit, disable, or delete the audit scope.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- The audit scope has been added.
- Before enabling, editing, or deleting the audit scope, ensure that the status of audit scope is **Disabled**.
- Before disabling the audit scope, ensure that the status of audit scope is **Enabled**.

Precautions

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

Viewing the Audit Scope

Step 1 Log in to the management console.

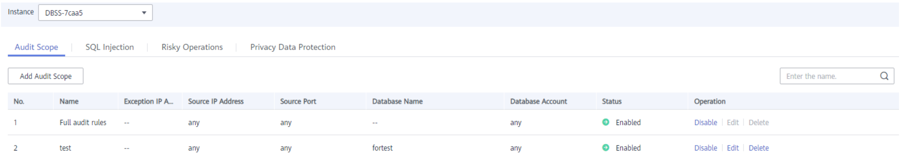
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 View the audit scope information, as shown in **Figure 13-5**. For details about related parameters, see **Table 13-5**.

Figure 13-5 Viewing the audit scope



Instance: DBSS-7caa5

Audit Scope | SQL Injection | Risky Operations | Privacy Data Protection

Add Audit Scope

Enter the name.

No.	Name	Exception IP A...	Source IP Address	Source Port	Database Name	Database Account	Status	Operation
1	Full audit rules	--	any	any	--	any	Enabled	Disable | Edit | Delete
2	test	--	any	any	fortest	any	Enabled	Disable | Edit | Delete

NOTE

Enter the key word of an audit scope to search.

Table 13-5 Parameters

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

NOTE

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

- Enable

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

- Edit

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

- Disable

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

- Delete

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

----End

13.6 Viewing Information About SQL Injection Detection

This section describes how to view SQL injection detection information of a database audit instance.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.

Procedure

Step 1 Log in to the management console.

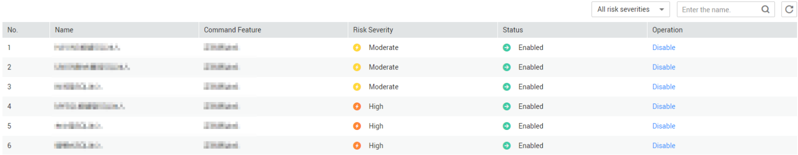
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 View information about SQL injection detection, as shown in **Figure 13-6**. For details about related parameters, see **Table 13-6**.

Figure 13-6 Viewing information about the SQL injection detection



No.	Name	Command Feature	Risk Severity	Status	Operation
1	[redacted]	[redacted]	Moderate	Enabled	Disable
2	[redacted]	[redacted]	Moderate	Enabled	Disable
3	[redacted]	[redacted]	Moderate	Enabled	Disable
4	[redacted]	[redacted]	High	Enabled	Disable
5	[redacted]	[redacted]	High	Enabled	Disable
6	[redacted]	[redacted]	High	Enabled	Disable

NOTE

Select a risk severity from the **All risk severities** drop-down list in the upper right corner of the list, or enter a key word of an SQL injection rule name to search.

Table 13-6 Parameters

Parameter	Description
Name	Name of the SQL injection detection
Command Feature	Command features of the SQL injection detection

Parameter	Description
Risk Severity	Risk level of the SQL injection detection. The options are as follows: ● **High** ● **Moderate** ● **Low** ● **No risks**
Status	Status of the SQL injection detection. The options are as follows: ● **Enabled** ● **Disabled**

----End

13.7 Managing Risky Operations

After adding a risky operation, you can view the risk, enable, edit, disable, or delete the risky operation, or set its priority.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- The risky operation has been added.
- Before enabling the risky operation, ensure that its status is **Disabled**.
- Before disabling the risky operation, ensure that its status is **Enabled**.

Sets the Priority of the Risky Operation

Step 1 Log in to the management console.

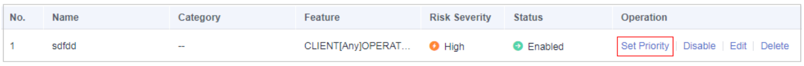
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 Locate the target risky operation, and click **Set Priority** in the **Operation** column, as shown in **Figure 13-7**.

Figure 13-7 Setting the priority



No.	Name	Category	Feature	Risk Severity	Status	Operation
1	sdfdd	--	CLIENT[Any]OPERAT...	● High	● Enabled	Set Priority | Disable | Edit | Delete

Step 6 In the displayed dialog box, select a priority and click **OK**.

----End

Viewing the Risky Operation

Step 1 Log in to the management console.

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

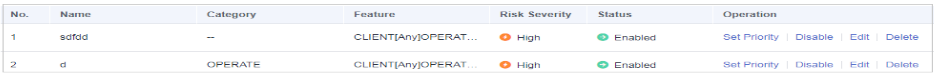
Step 3 In the navigation tree, choose **Rules**.

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

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

Step 6 View risky operations information, as shown in **Figure 13-8**. For details about related parameters, see **Table 13-7**.

Figure 13-8 Viewing risky operations



No.	Name	Category	Feature	Risk Severity	Status	Operation
1	sdfdd	--	CLIENT[Any]OPERAT...	High	Enabled	Set Priority | Disable | Edit | Delete
2	d	OPERATE	CLIENT[Any]OPERAT...	High	Enabled	Set Priority | Disable | Edit | Delete

NOTE

Select a risk severity from the **All risk severities** drop-down list in the upper right corner of the list, or enter a key word of a risky operation name to search.

Table 13-7 Parameters

Parameter	Description
Name	Name of the risky operation
Category	Category of the risky operation
Feature	Feature of the risky operation
Risk Severity	Risk severity of the risky operation. The options are as follows: ● **High** ● **Moderate** ● **Low** ● **No risks**
Status	Status of the risky operation. The options are as follows: ● **Enabled** ● **Disabled**

NOTE

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

- Enable

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

- Edit

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

- Disable

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

- Delete

  Locate the row that contains the risky operation to be deleted, click **Delete** in the **Operation** column, and click **OK** in the displayed dialog box. You need to add the risky operation again if a risky operation is deleted and you need to audit its rule.

----End

13.8 Managing Privacy Data Protection Rules

You can view, enable, edit, disable, or delete data masking rules.

Prerequisites

You have purchased a database audit instance and the **Status** is **Running**.

Viewing Privacy Data Protection Rules

Step 1 Log in to the management console.

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

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

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

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

Step 6 View the rules, as shown in **Figure 13-9**. For details about related parameters, see **Table 13-8**.

NOTE

- **Store Result Set**

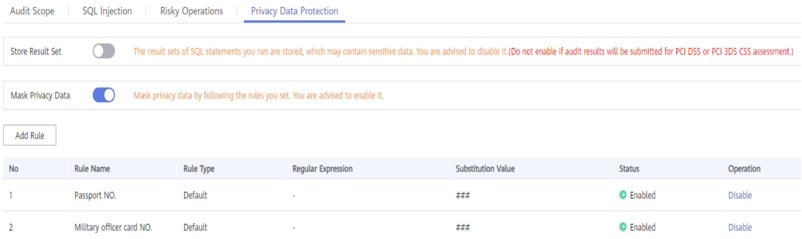
  You are advised to disable . After this function is disabled, database audit will not store the result sets of user SQL statements.

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

- **Mask Privacy Data**

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

Figure 13-9 Masking rule information



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

Mask Privacy Data ● 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
2	Military officer card NO.	Default	-	###	Enabled	Disable

Table 13-8 Masking rule parameters

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

NOTE

You can perform the following operations on a rule:

- Disable

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

- Edit

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

- Delete

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

----End

13.9 Managing Audit Reports

By default, database audit complies with a full audit rule, which is used to audit all databases that are successfully connected to the database audit instance. After connecting the database to the database audit instance, view report templates and report results.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.

Viewing a Report

Step 1 Log in to the management console.

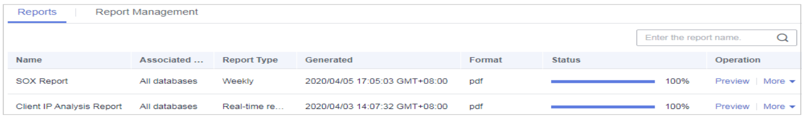
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 View the report information, as shown in **Figure 13-10**.

Figure 13-10 Viewing a report



Name	Associated ...	Report Type	Generated	Format	Status	Operation
SOX Report	All databases	Weekly	2020/04/05 17:05:03 GMT+08:00	pdf	100%	Preview | More ▾
Client IP Analysis Report	All databases	Real-time re...	2020/04/03 14:07:32 GMT+08:00	pdf	100%	Preview | More ▾

NOTE

- Enter a report name in the upper right corner to search.
- A real-time report is automatically generated in PDF format.
- Locate the row that contains the report to be deleted, click **Delete** in the **Operation** column, and click **OK** in the displayed dialog box. When a report is deleted, you need to manually generate a report if you want to view the report result.

----End

Viewing a Report Template

Step 1 Log in to the management console.

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

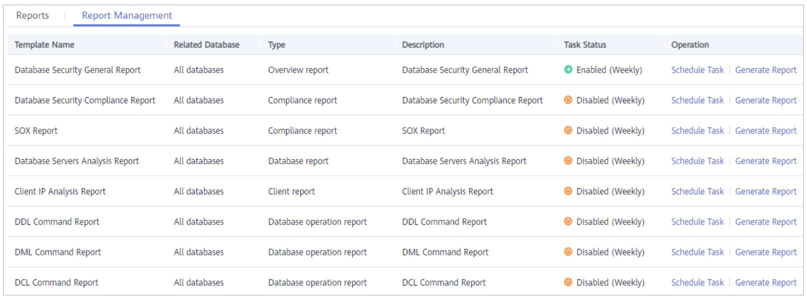
Step 3 In the navigation tree on the left, choose **Reports**.

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

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

Step 6 View the report template information, as shown in **Figure 13-11**.

Figure 13-11 Viewing the template list



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

NOTE

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

----End

13.10 Managing Backup Audit Logs

After backing up audit logs, you can view or delete backup audit logs.

Prerequisites

- You have purchased a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.
- You have backed up audit logs.

Viewing Backup Audit Logs

Step 1 Log in to the management console.

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

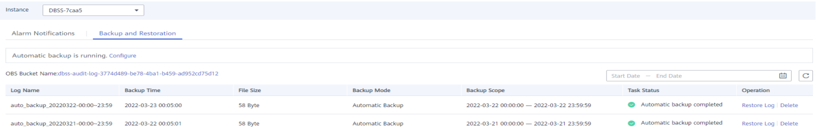
Step 3 In the navigation tree on the left, choose **Settings**.

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

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

Step 6 View the backup audit log information, as shown in **Figure 13-12**. For details about related parameters, see **Table 13-9**.

Figure 13-12 Viewing backup audit logs



Instance: DBSS-7caa5

Automatic backup is running. Configure

OBS Bucket Name:dbss-audit-log-3774d489-be78-4ba1-b459-ad952cd75d12

Log Name	Backup Time	File Size	Backup Mode	Backup Scope	Task Status	Operation
auto_backup_20220322-00:00~23:59	2022-03-23 00:05:00	58 Byte	Automatic Backup	2022-03-22 00:00:00 — 2022-03-22 23:59:59	Automatic backup completed	Restore Log | Delete
auto_backup_20220321-00:00~23:59	2022-03-22 00:05:01	58 Byte	Automatic Backup	2022-03-21 00:00:00 — 2022-03-21 23:59:59	Automatic backup completed	Restore Log | Delete

Click 📅 in the upper right corner of the list and select the start time and end time to view backup logs in a specified time range.

Table 13-9 Parameters of audit logs

Parameter	Description
Log Name	Name of a log, which is automatically generated
Backup Time	Time when a log is backed up
File Size	Log file size
Backup Mode	Log backup mode.
Backup Scope	Backup time window
Task Status	Backup status of a log

NOTE

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

----End

13.11 Viewing Operation Logs

This section describes how to view operation logs of a database audit instance.

Prerequisites

You have purchased a database audit instance and the **Status** is **Running**.

Procedure

Step 1 Log in to the management console.

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

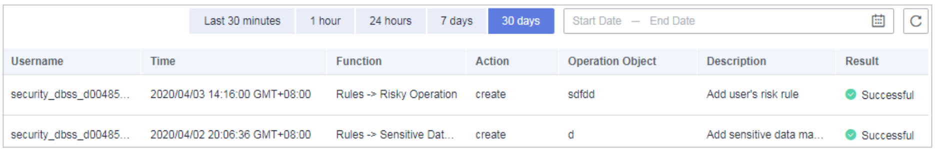
Step 3 In the navigation tree on the left, choose **Instances**.

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

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

Step 6 View operation logs, as shown in **Figure 13-13**. For details about related parameters, see **Table 13-10**.

Figure 13-13 Viewing operation logs



Username	Time	Function	Action	Operation Object	Description	Result
security_dbss_d00485...	2020/04/03 14:16:00 GMT+08:00	Rules -> Risky Operation	create	sdfdd	Add user's risk rule	✓ Successful
security_dbss_d00485...	2020/04/02 20:06:36 GMT+08:00	Rules -> Sensitive Dat...	create	d	Add sensitive data ma...	✓ Successful

NOTE

Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days**, or click 📅 to set start time and end time to view the operation logs of a specified time range.

Table 13-10 Parameters

Parameter	Description
Username	User who performs the operation
Time	Time when the operation was performed
Function	Function of the operation

Parameter	Description
Action	Action of the operation
Operation Object	Object of the operation
Description	Description of the operation
Result	Result of the operation

----End

14 Key Operations Recorded by CTS

14.1 Viewing Tracing Logs

After you enable CTS, the system starts recording operations on DBSS. Operation records for the last seven days can be viewed on the CTS console.

Viewing a DBSS Trace on the CTS Console

Step 1 Log in to the management console.

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

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

Step 4 Click **Region** at the top of the **Trace List** page to set the corresponding conditions.

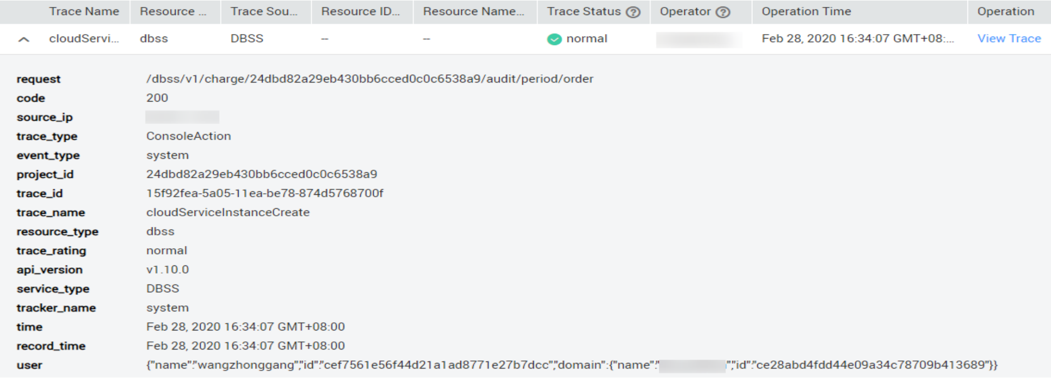
The following four filters are available:

- **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**
  - Select the filter from the drop-down list. Set **Trace Source** to **DBSS**.
  - When you select **Trace name** for **Search By**, you also need to select a specific trace name.
  - When you select **Resource ID** for **Search By**, you also need to select or enter a specific resource ID.
  - When you select **Resource name** for **Search By**, you also need to select or enter a specific resource name.
- **Operator**: Select a specific operator (a user other than tenant).
- **Trace Rating**: Available options include **All trace status**, **normal**, **warning**, and **incident**. You can only select one of them.
- In the upper right corner of the page, you can query traces in the last 1 hour, last 1 day, last 1 week, or within a customized period.

Step 5 Click **Query**.

Step 6 Click ⌄ on the left of a trace to expand its details.

Figure 14-1 Expanding trace details

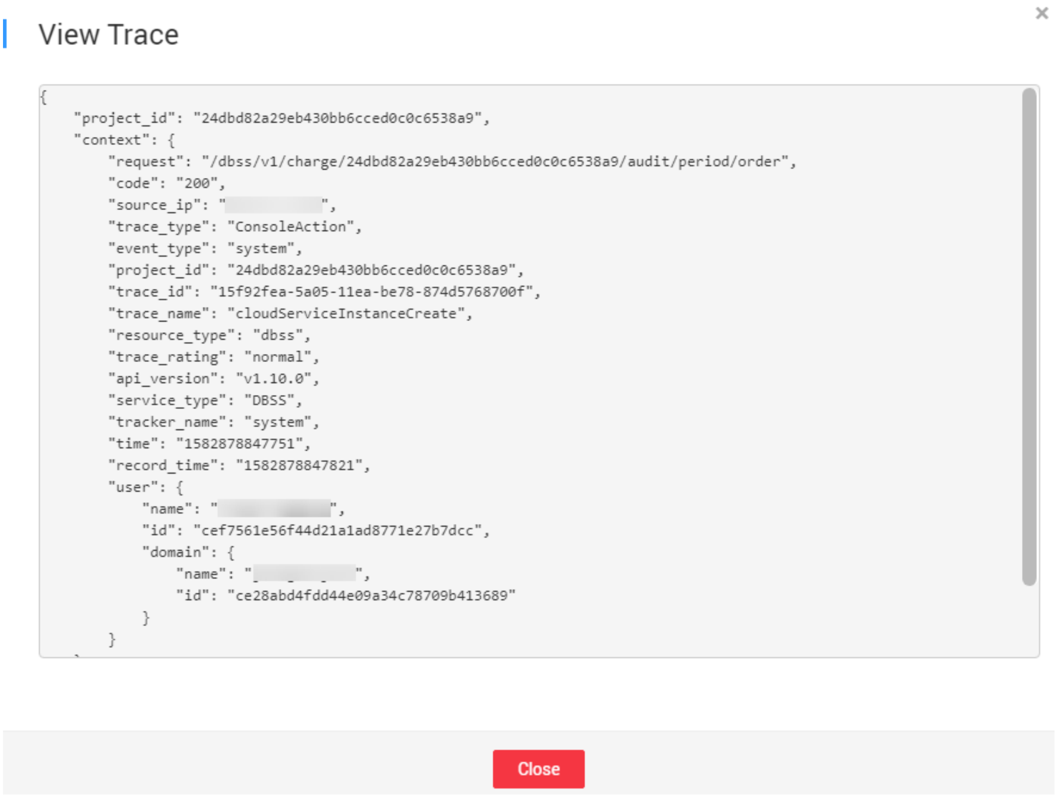


	Trace Name	Resource ...	Trace Sou...	Resource ID...	Resource Name...	Trace Status ⓘ	Operator ⓘ	Operation Time	Operation
^	cloudServi...	dbss	DBSS	--	--	✓ normal	[redacted]	Feb 28, 2020 16:34:07 GMT+08:...	View Trace

request	/dbss/v1/charge/24dbd82a29eb430bb6cced0c0c6538a9/audit/period/order
code	200
source_ip	[redacted]
trace_type	ConsoleAction
event_type	system
project_id	24dbd82a29eb430bb6cced0c0c6538a9
trace_id	15f92fea-5a05-11ea-be78-874d5768700f
trace_name	cloudServiceInstanceCreate
resource_type	dbss
trace_rating	normal
api_version	v1.10.0
service_type	DBSS
tracker_name	system
time	Feb 28, 2020 16:34:07 GMT+08:00
record_time	Feb 28, 2020 16:34:07 GMT+08:00
user	{"name":"wangzhonggang","id":"cef7561e56f44d21a1ad8771e27b7dcc","domain":{"name":"[redacted]","id":"ce28abd4fdd44e09a34c78709b413689"}}

Step 7 Click **View Trace** in the **Operation** column. On the displayed **View Trace** dialog box shown in **Figure 14-2**, the trace structure details are displayed.

Figure 14-2 Viewing a trace



View Trace

```
{
    "project_id": "24dbd82a29eb430bb6cced0c0c6538a9",
    "context": {
        "request": "/dbss/v1/charge/24dbd82a29eb430bb6cced0c0c6538a9/audit/period/order",
        "code": "200",
        "source_ip": "[redacted]",
        "trace_type": "ConsoleAction",
        "event_type": "system",
        "project_id": "24dbd82a29eb430bb6cced0c0c6538a9",
        "trace_id": "15f92fea-5a05-11ea-be78-874d5768700f",
        "trace_name": "cloudServiceInstanceCreate",
        "resource_type": "dbss",
        "trace_rating": "normal",
        "api_version": "v1.10.0",
        "service_type": "DBSS",
        "tracker_name": "system",
        "time": "1582878847751",
        "record_time": "1582878847821",
        "user": {
            "name": "[redacted]",
            "id": "cef7561e56f44d21a1ad8771e27b7dcc",
            "domain": {
                "name": "[redacted]",
                "id": "ce28abd4fdd44e09a34c78709b413689"
            }
        }
```

----End

14.2 Auditable Operations

Cloud Trace Service (CTS) records all cloud service operations on DBSS, including requests initiated from the management console or open APIs and responses to the requests, for tenants to query, audit, and trace.

Table 14-1 lists DBSS operations recorded by CTS.

Table 14-1 DBSS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating an instance	dbss	createInstance
Deleting an instance	dbss	deleteInstance
Starting an instance	dbss	startInstance
Stopping an instance	dbss	stopInstance
Restarting an instance	dbss	rebootInstance

15 Monitoring

15.1 DBSS Monitored Metrics

Description

This section describes monitored metrics reported by DBSS to Cloud Eye as well as their namespaces and dimensions. You can use console or APIs provided by Cloud Eye to query the metrics of the monitored objects and alarms generated for DBSS.

Namespace

SYS.DBSS

NOTE

A namespace is an abstract collection of resources and objects. Multiple namespaces can be created in a single cluster with the data isolated from each other. This enables namespaces to share the same cluster services without affecting each other.

Metrics

Table 15-1 DBSS metrics

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

15.2 Configuring Alarm Monitoring Rules

You can set DBSS alarm rules to customize the monitored objects and notification policies, and set parameters such as the alarm rule name, monitored object, metric, threshold, monitoring scope, and whether to send notifications. This helps you learn the database security status in a timely manner.

Prerequisites

You have purchased a DBSS instance.

Procedure

Step 1 Log in to the management console.

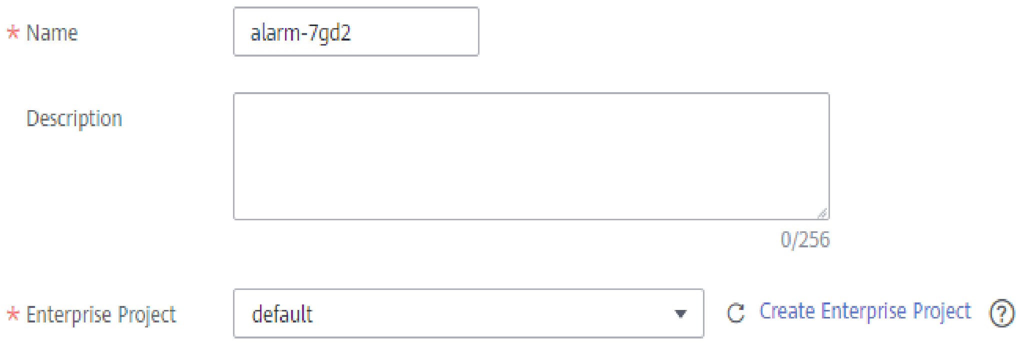
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Click ≡ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.

Step 5 In the upper right corner of the page, click **Create Alarm Rule**.

Step 6 Set the alarm rule name and select an enterprise project to which the alarm rule belongs.



* Name: alarm-7gd2

Description:

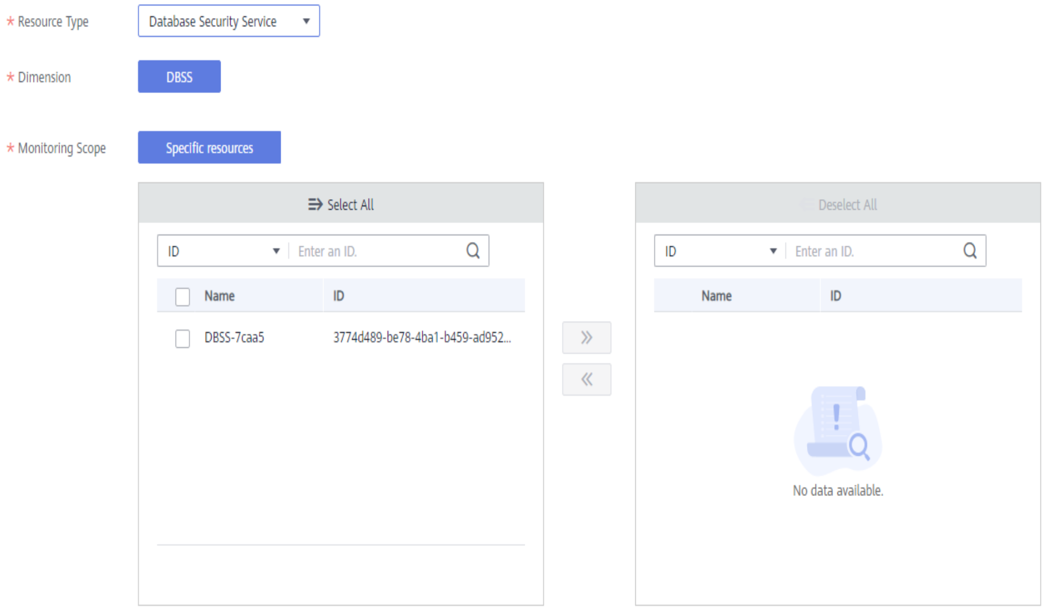
0/256

* Enterprise Project: default ▾

Create Enterprise Project ?

Step 7 Select **Database Security Service** from the **Resource Type** drop-down list, and select a dimension, monitoring scope, alarm template, and whether to send a notification. **Figure 15-1** shows an example.

Figure 15-1 Configuring a DBSS alarm monitoring rule



* Resource Type: Database Security Service ▾

* Dimension: DBSS

* Monitoring Scope: Specific resources

Select All

ID ▾ Enter an ID.

□ Name	ID
□ DBSS-7caa5	3774d489-be78-4ba1-b459-ad952...

»

«

Deselect All

ID ▾ Enter an ID.

Name	ID

No data available.

Step 8 Click **Create**. In the displayed dialog box, click **OK**.

----End

15.3 Viewing Monitoring Metrics

You can view DBSS metrics on the management console to learn about the database security status in a timely manner and configure protection policies based on the metrics.

Prerequisites

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

Procedures

Step 1 Log in to the management console.

Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Cloud Service Monitoring** > **Database Security Service**.

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

----End

16 Permission Control

16.1 DBSS Custom Policies

Custom policies can be created to supplement the system-defined policies of DBSS. For the actions supported for custom policies, see **DBSS Permissions and Supported Actions**.

Examples of Custom Policies

- Example 1: Allowing a user to query the database audit list

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "dbss:auditInstance:list"
            ]
        }
    ]
}
```

- Example 2: Denying database audit instance deletion

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

  The following method can be used if you need to assign permissions of the **DBSS FullAccess** policy to a user but also forbid the user from deleting database audit instances. Create a custom policy to disallow audit instance deletion and assign both policies to the group the user belongs to. Then the user can perform all operations on DBSS except deleting database audit instances. The following is an example of a deny policy:

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Action": [
                                "dbss:auditInstance:delete"
                        ],
                        "Effect": "Deny"
                }
        ]
}
```

- Example 3: Defining permissions for multiple services in a policy

  A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "dbss:defendInstance:eipOperate",
                "dbss:auditInstance:getSpecification"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "hss:accountCracks:unblock",
                "hss:commonIPs:set"
            ]
        }
    ]
}
```

16.2 DBSS Permissions and Supported Actions

This section describes fine-grained permissions management for your DBSS resources. If your Huawei Cloud account does not need individual IAM users, you can skip this section.

By default, new IAM users do not have any permissions. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added. Users inherit permissions from the groups and can perform operations on cloud services as allowed by the permissions.

Supported Actions

DBSS provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control. Operations supported by policies are specific to APIs. The following are common concepts related to policies:

- Permissions: Statements in a policy that allow or deny certain operations.
- Actions: Specific operations that are allowed or denied.
- Related actions: Actions on which a specific action depends to take effect. When assigning permissions for the action to a user, you also need to assign permissions for the related actions.

Table 16-1 lists the API actions supported by DBSS.

Table 16-1 Actions

Permission	Action
Query the list of database audit instances	dbss:auditInstance:list
Obtain available specifications of database audit instances	dbss:auditInstance:getSpecification
View database protection instance details	dbss:defendInstance:list
Delete a database audit instance	dbss:auditInstance:delete
Purchase database protection instances on demand	dbss:defendInstance:createOnDemand
Purchase database audit instances on demand	dbss:auditInstance:createOnDemand
Purchase database audit instances on demand	dbss:auditInstance:createOnOrder
Restart a database protection instance	dbss:defendInstance:reboot
Start a database audit instance	dbss:auditInstance:start
Stop a database audit instance	dbss:auditInstance:stop
Restart a database audit instance	dbss:auditInstance:reboot
Start a database protection instance	dbss:defendInstance:start
Stop a database protection instance	dbss:defendInstance:stop

17 How Long Is the Database Audit Data Stored by Default?

Database audit can store online and archived audit data for at least 180 days. If the backup function is disabled and disk space is sufficient, logs are stored on the audit instance for 180 days by default. If a large number of new audit logs need to be stored, the system automatically deletes the old logs on a rolling basis to ensure sufficient disk space. If the backup function is enabled, logs and backup logs will also be stored in OBS for same duration.

However, the storage duration also depends on the disk capacity of the log database. To store your audit data long enough, you are advised to:

- Choose a database audit edition suitable for your business.
  - To audit a small volume of data, purchase the basic edition.
  - To audit a large volume of data, purchase the professional or advanced edition.

    For more information, see **Table 17-1**.
- Back up audit logs.

  For details, see **Backing Up and Restoring Database Audit Logs**.

Table 17-1 Database audit editions

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.

Version	Maximum Databases	System Resource	Performance
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.

NOTE

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

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

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

18 On What Windows Versions Can I Install the Agent?

To use database audit, you need to install its agent on database nodes or application nodes.

The agent can be installed on the following Windows versions:

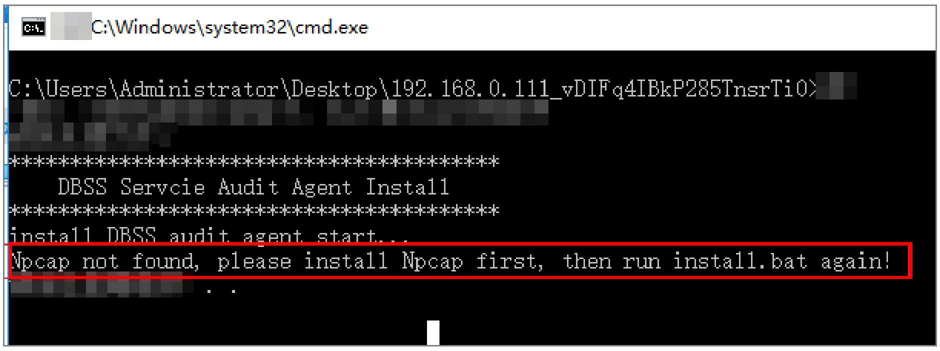
- Windows Server 2008 R2 (64bit)
- Windows Server 2012 R2 (64bit)
- Windows Server 2016 (64bit)
- Windows Server 2019 (64bit)
- Windows 7 (64bit)
- Windows 10 (64bit)

NOTE

The DBSS agent depends on Npcap. If the message "Npcap not found, please install Npcap first" is displayed when you install the DBSS agent, first install Npcap and then the DBSS agent.

Npcap download link: **https://npcap.com/#download**

Figure 18-1 Npcap not found



```
[redacted] C:\Windows\system32\cmd.exe

C:\Users\Administrator\Desktop\192.168.0.111_vDIFq4IBkP285TnsrTi0>[redacted]
[redacted]
*******************************************
    DBSS Servcie Audit Agent Install
*******************************************
install DBSS audit agent start...
Npcap not found, please install Npcap first, then run install.bat again!
[redacted] . .
```

A Change History

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