

**Database Security Service**

# **User Guide**

**Date**      **2021-06-15**

---

# Contents

---

<b>1 Overview</b>	<b>1</b>
1.1 DBSS	1
1.2 Functions	3
1.3 Advantages	3
1.4 Deployment Architecture	4
1.5 Editions	5
1.6 Constraints	6
1.7 Permissions Management	9
1.8 Related Services	15
<b>2 Process Overview</b>	<b>17</b>
<b>3 Applying for a Database Audit Instance</b>	<b>20</b>
<b>4 Step 1: Add a Database</b>	<b>22</b>
<b>5 Step 2: Add an Agent</b>	<b>26</b>
<b>6 Step 3: Download and Install the Agent</b>	<b>35</b>
6.1 Downloading an Agent	35
6.2 Installing an Agent (Linux OS)	36
6.3 Installing an Agent (Windows OS)	40
<b>7 Step 4: Add a Security Group Rule</b>	<b>47</b>
<b>8 Step 5: Enable Database Audit</b>	<b>49</b>
<b>9 Adding Audit Scope</b>	<b>51</b>
<b>10 Enabling or Disabling SQL Injection Detection</b>	<b>54</b>
<b>11 Adding Risky Operations</b>	<b>56</b>
<b>12 Configuring Privacy Data Protection Rules</b>	<b>59</b>
<b>13 Viewing SQL Statement Details</b>	<b>63</b>
<b>14 Viewing Session Distribution</b>	<b>66</b>
<b>15 Viewing the Audit Dashboard</b>	<b>68</b>
<b>16 Viewing Audit Reports</b>	<b>70</b>

<b>17 Configuring Alarm Notifications.....</b>	<b>75</b>
<b>18 Viewing the System Monitoring.....</b>	<b>78</b>
<b>19 Viewing the Alarms.....</b>	<b>80</b>
<b>20 Managing Database Audit Instances.....</b>	<b>83</b>
<b>21 Viewing the Instance Overview.....</b>	<b>86</b>
<b>22 Managing Databases and Agents.....</b>	<b>89</b>
<b>23 Uninstalling an Agent.....</b>	<b>93</b>
<b>24 Management an Audit Scope.....</b>	<b>95</b>
<b>25 Viewing Information About SQL Injection Detection .....</b>	<b>97</b>
<b>26 Managing Risky Operations.....</b>	<b>99</b>
<b>27 Managing Privacy Data Protection Rules.....</b>	<b>102</b>
<b>28 Managing Audit Reports.....</b>	<b>104</b>
<b>29 Managing Backup Audit Logs.....</b>	<b>106</b>
<b>30 Viewing Operation Logs.....</b>	<b>108</b>
<b>31 Viewing Tracing Logs.....</b>	<b>110</b>
<b>32 Auditable Operations.....</b>	<b>112</b>
<b>33 FAQs.....</b>	<b>113</b>
33.1 Product Consulting.....	113
33.1.1 What Is Database Audit?.....	113
33.1.2 What Are the Differences Between DBSS Database Audit and RDS SQL Audit?.....	113
33.1.3 What Editions Does DBSS Provide?.....	114
33.1.4 What Databases Does DBSS Protect?.....	114
33.1.5 What Databases Does DBSS Support?.....	114
33.1.6 Why Can't I See the Instance that Is Being Created After I Applied for It?.....	114
33.2 Functions.....	115
33.2.1 Does Database Audit (in Bypass Mode) Affect My Services?.....	115
33.2.2 What Are the Functions of Database Audit?.....	115
33.2.3 Supported Database Types.....	115
33.2.4 What OSs Can I Install the Database Audit Agent On?.....	116
33.2.5 Does Database Audit Support Bidirectional Audit?.....	118
33.2.6 Can I Audit Databases Across Different VPCs?.....	118
33.2.7 Can Applications Using TLS Connections Be Audited?.....	118
33.2.8 How Long Is the Database Audit Data Stored by Default?.....	118
33.2.9 How Soon Can I Receive an Alarm Notification If an Exception Occurs in Database Audit?.....	119
33.2.10 Is the Total Number Of Alarms Every Day the Same as that of Emails?.....	120
33.2.11 Why I Cannot Preview the Database Security Audit Report Online?.....	120

33.2.12 If I Use Middleware at the Service Side, Will It Affect Database Audit?.....	120
33.2.13 What Should I Do If an Alarm of Insufficient DBSS Capacity Is Displayed?.....	120
33.3 Agent.....	120
33.3.1 Which Functions Do the Database Audit Agent Provide?.....	120
33.3.2 On What Windows Versions Can I Install the Agent?.....	121
33.3.3 On What Linux OSs Can I Install the Agent?.....	121
33.3.4 What Is the Process Name of the Database Audit Agent?.....	122
33.3.5 (Linux OS) What Should I Do If I Lack the Permission to Run the Agent Installation Script?.....	123
33.3.6 (Linux OS) Where Are the Logs of the Database Audit Agent Saved?.....	123
33.3.7 When Should I Select an Existing Agent?.....	123
33.3.8 What Do I Do If the Database Audit Agent Is Hibernating?.....	124
33.3.9 How Do I Determine Where to Install an Agent?.....	125
33.3.10 How Do I Download a Database Audit Agent?.....	127
33.3.11 How Do I Uninstall a Database Audit Agent?.....	128
33.3.12 How Do I Install the Agent (in Windows OS)?.....	129
33.3.13 What Do I Do If the Communication Between the Agent and Database Audit Instance Is Abnormal?.....	133
33.3.14 How Many Resources Are Consumed by an Agent When It Runs on a Node?.....	136
33.4 Operations.....	137
33.4.1 How Do I Disable SSL for a Database?.....	137
33.4.2 How Do I Set Database Audit Rules for All Databases?.....	138
33.4.3 How Do I Check the Version of Database Audit?.....	138
33.4.4 How Do I View All Alarms in Database Audit?.....	139
33.4.5 How Do I Audit an RDS Database Accessed through Intranet (by Applications Off the Cloud)?....	139
33.5 Troubleshooting.....	139
33.5.1 Database Audit Is Running Properly But Generates No Audit Records.....	140
33.5.2 Database Audit Is Unavailable.....	141
33.5.3 Alarm Notifications Are Abnormal.....	146
33.6 Logs.....	146
33.6.1 Can the Operation Logs of Database Audit Be Migrated?.....	146
33.6.2 How Long Are the Operation Logs of Database Audit Saved by Default?.....	146
33.6.3 How Do I Check the Operation Logs of Database Audit?.....	146
33.6.4 How Does Database Audit Process Logs?.....	147
33.6.5 How Do I Back Up the Database Audit Logs?.....	148
33.6.6 Can Database Audit Logs Be Directly Saved to OBS?.....	149
<b>A Change History.....</b>	<b>150</b>

# 1 Overview

## 1.1 DBSS

Database Security Service (DBSS) provides the database audit service in out-of-path mode. It records user access to the database in real time, generates fine-grained audit reports, sends real-time alarms for high-risk operations and attacks. In addition, database audit generates compliance reports that meet data security standards (such as Sarbanes-Oxley) to locate internal violations and improper operations, thus ensuring data asset security.

### Supported Databases

Database audit provides the audit function in out-of-path mode for the following databases on the management console:

- Relational Database Service (RDS)
- Databases built on ECS
- Databases built on BMS

Database audit supports the following database types and versions.

**Table 1-1** Database types and versions supported by database audit

Database Type	Edition
MySQL	<ul style="list-style-type: none"><li>• 5.0, 5.1, 5.5, 5.6, 5.7</li><li>• 8.0 (8.0.11 and earlier)</li><li>• 8.0.23</li></ul>
Oracle	<ul style="list-style-type: none"><li>• 11g 11.1.0.6.0, 11.2.0.1.0, 11.2.0.2.0, 11.2.0.3.0, and 11.2.0.4.0</li><li>• 12c 12.1.0.2.0, 12.2.0.1.0</li><li>• 19c</li></ul>

Database Type	Edition
PostgreSQL	<ul style="list-style-type: none"> <li>• 7.4</li> <li>• 8.0 8.0, 8.1, 8.2, 8.3, 8.4</li> <li>• 9.0 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6</li> <li>• 10.0 10.0, 10.1, 10.2, 10.3, 10.4, 10.5</li> <li>• 11.0</li> <li>• 12.0</li> <li>• 13.0</li> </ul>
SQL Server	<ul style="list-style-type: none"> <li>• 2008, 2008R2</li> <li>• 2012</li> <li>• 2014</li> <li>• 2016</li> <li>• 2017</li> </ul>
DWS	<ul style="list-style-type: none"> <li>• 1.5</li> </ul>
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8
Gbase XDM Cluster	V8.0
TAURUS	MySQL 8.0

## Service Features

- Back up and restore database audit logs and meet the audit data retention requirements.
- Monitor risks, sessions, session distribution, and SQL distribution in real time.
- Report alarms for risky behaviors and attacks and responds to database attacks in real time.
- Locate internal violations and improper operations and keep data assets secure.

Deployed in out-of-path pattern, database audit can perform flexible audit on the database without affecting user services.

- Monitors database login, operation type (data definition, operation, and control), and operation object based on risky operations to effectively audit the database.
- Analyzes risks, sessions, and SQL injection to help you master the database situation in a timely manner.

- Provides a report template library to generate daily, weekly, or monthly audit reports according to your configurations. Sends real-time alarm notifications to help you obtain audit reports in a timely manner.

## 1.2 Functions

Database audit delivers functions such as user behavior detection and audit, multi-dimensional lead analysis, real-time alarms, and reports.

- User Behavior Detection and Audit
  - Associates access operations in the application layer with those in the database layer.
  - Uses built-in or user-defined privacy data protection rules to mask private data (such as accounts and passwords) in audit logs displayed on the console.
- Multi-dimensional Lead Analysis
  - Behavior analysis  
Supports analysis in multiple dimensions, such as audit duration, statement quantity, risk quantity, risk distribution, session statistics, and SQL distribution.
  - Session analysis  
Conducts analysis based on time, user, IP address, and client.
  - Statement analysis  
Provides multiple search criteria, such as time, risk severity, user, client IP address, database IP address, operation type, and rule.
- Real-time Alarms for Risky Operations and SQL Injection
  - Risky operation  
Defines a risky operation in fine-grained dimensions such as operation type, operation object, and risk severity.
  - SQL injection  
Provides an SQL injection library, which facilitates alarm reporting for database exceptions based on the SQL command feature or risk severity.
  - System resource  
Reports alarms when the usage of system resources (CPU, memory, and disk) reaches configured threshold.
- Fine-grained Reports for Various Abnormal Behaviors
  - Session behavior  
Provides session analysis report of the client and database users.
  - Risky operation  
Provides the risk distribution and analysis report.

## 1.3 Advantages

Database audit provides you with the database audit function in out-of-path pattern, enabling the system to generate real-time alarms for risky operations. In

In addition, database audit generates compliance reports that meet data security standards. In this way, it locates internal violations and improper operations, protecting your data assets.

- **Simple to set up**  
Database audit is deployed in out-of-path pattern. It is simple to set up and operate.
- **Comprehensive audit**  
Supports audit of databases built on RDS, ECS, and BMS on the management console.
- **Quick identification**  
Implements 99%+ application association audit, complete SQL parsing, and accurate protocol analysis.
- **Efficient analysis**  
Responds quickly for data query with 10,000 requests per second from massive volumes of data saved.
- **Clear permission division**  
Clearly divides permissions among the system administrator, security administrator, and audit administrator, meeting audit security requirements.

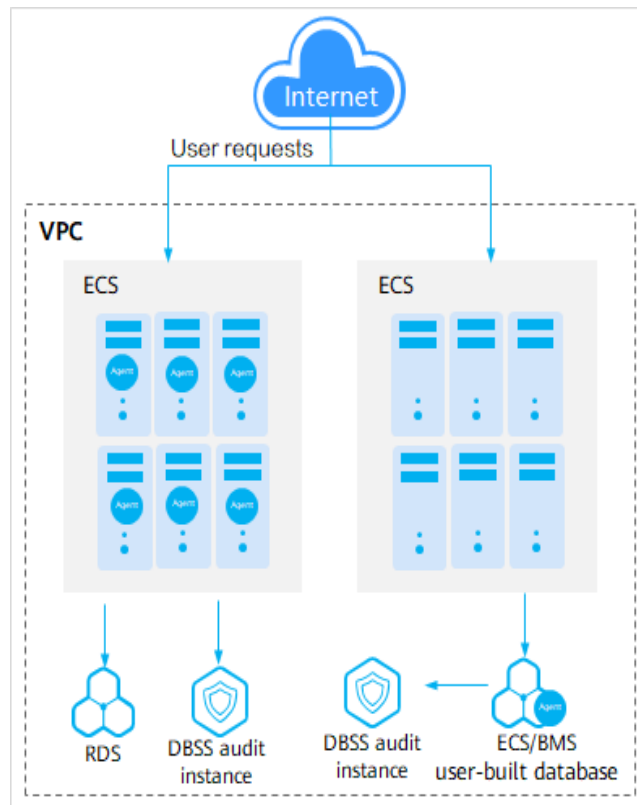
## 1.4 Deployment Architecture

Database audit is deployed in out-of-path pattern. It can audit databases built on ECS, BMS and RDS on the management console.

**Figure 1-1** shows the database audit deployment architecture.



**Figure 1-1** Database audit deployment architecture



The agent deployment for database audit is as follows:

- For databases built on ECS or BMS, agents must be deployed on the database side.
- For relational databases, agents must be deployed on the application or proxy side.

## 1.5 Editions

Database audit provides basic, professional, and advanced editions. You can select one of them as needed.

**Table 1-2** describes the database audit editions.

**Table 1-2** Database audit editions

Version	Maximum Databases	System Resource	Performance
Basic	3	<ul style="list-style-type: none"> <li>• CPU: 4 vCPUs</li> <li>• Memory: 16 GB</li> <li>• Disk: 500 GB</li> </ul>	<ul style="list-style-type: none"> <li>• Peak QPS: 3,000 queries/second</li> <li>• Database load rate: 3.6 million statements/hour</li> <li>• Stores 400 million online SQL statements.</li> <li>• Stores 5 billion archived SQL statements.</li> </ul>
Professional	6	<ul style="list-style-type: none"> <li>• CPU: 8 vCPUs</li> <li>• Memory: 32 GB</li> <li>• Disk: 1 TB</li> </ul>	<ul style="list-style-type: none"> <li>• Peak QPS: 6,000 queries/second</li> <li>• Database load rate: 7.2 million statements/hour</li> <li>• Stores 600 million online SQL statements.</li> <li>• Stores 10 billion archived SQL statements.</li> </ul>

 **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<sub>1</sub> and IP<sub>2</sub>. IP<sub>1</sub> has a database port. IP<sub>2</sub> has three database ports. IP<sub>1</sub> and IP<sub>2</sub> 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 apply for a new one.
- Online SQL statements are counted based on the assumption that the capacity of an SQL statement is 1 KB.

## 1.6 Constraints

Database audit is subject to certain constraints.

### Supported Database Types

The following types of databases on the management console can be audited in out-of-path mode:

- Relational Database Service (RDS)
- Databases built on ECS
- Databases built on BMS

## Databases That Need Agents

The following database versions can be audited.

**Table 1-3** Database types and versions supported by database audit

Database Type	Edition
MySQL	<ul style="list-style-type: none"> <li>• 5.0, 5.1, 5.5, 5.6, 5.7</li> <li>• 8.0 (8.0.11 and earlier)</li> <li>• 8.0.23</li> </ul>
Oracle	<ul style="list-style-type: none"> <li>• 11g 11.1.0.6.0, 11.2.0.1.0, 11.2.0.2.0, 11.2.0.3.0, and 11.2.0.4.0</li> <li>• 12c 12.1.0.2.0, 12.2.0.1.0</li> <li>• 19c</li> </ul>
PostgreSQL	<ul style="list-style-type: none"> <li>• 7.4</li> <li>• 8.0 8.0, 8.1, 8.2, 8.3, 8.4</li> <li>• 9.0 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6</li> <li>• 10.0 10.0, 10.1, 10.2, 10.3, 10.4, 10.5</li> <li>• 11.0</li> <li>• 12.0</li> <li>• 13.0</li> </ul>
SQL Server	<ul style="list-style-type: none"> <li>• 2008, 2008R2</li> <li>• 2012</li> <li>• 2014</li> <li>• 2016</li> <li>• 2017</li> </ul>
DWS	<ul style="list-style-type: none"> <li>• 1.5</li> </ul>
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8
Gbase XDM Cluster	V8.0
TAURUS	MySQL 8.0

## Supported OSs

To use database audit, you need to install its agent on database nodes or application nodes. The database audit agent can run on the 64-bit Linux or Windows.

- For more information, see [Table 1-4](#).

**Table 1-4** Supported Linux OS versions

System Name	System version
CentOS	<ul style="list-style-type: none"> <li>• CentOS 7.0 (64bit)</li> <li>• CentOS 7.1 (64bit)</li> <li>• CentOS 7.2 (64bit)</li> <li>• CentOS 7.3 (64bit)</li> <li>• CentOS 7.4 (64bit)</li> <li>• CentOS 7.5 (64bit)</li> <li>• CentOS 7.6 (64bit)</li> <li>• CentOS 7.8 (64bit)</li> <li>• CentOS 8.0 (64bit)</li> </ul>
Debian	<ul style="list-style-type: none"> <li>• Debian 7.5.0 (64bit)</li> <li>• Debian 8.2.0 (64bit)</li> <li>• Debian 8.8.0 (64bit)</li> <li>• Debian 9.0.0 (64bit)</li> </ul>
Fedora	<ul style="list-style-type: none"> <li>• Fedora 24 (64bit)</li> <li>• Fedora 25 (64bit)</li> </ul>
SUSE	<ul style="list-style-type: none"> <li>• SUSE 11 SP4 (64bit)</li> <li>• SUSE 12 SP1 (64bit)</li> <li>• SUSE 12 SP2 (64bit)</li> </ul>
Ubuntu	<ul style="list-style-type: none"> <li>• Ubuntu 14.04 (64bit)</li> <li>• Ubuntu 16.04 (64bit)</li> <li>• Ubuntu 18.04 (64bit)</li> <li>• Ubuntu 20.04 (64-bit)</li> </ul>
EulerOS	<ul style="list-style-type: none"> <li>• Euler 2.2 (64bit)</li> <li>• Euler 2.3 (64bit)</li> </ul>
Oracle Linux	<ul style="list-style-type: none"> <li>• Oracle Linux 6.9 (64bit)</li> <li>• Oracle Linux 7.4 (64bit)</li> </ul>

- The following Windows OSs are supported:
  - Windows Server 2008 R2 (64bit)
  - Windows Server 2012 R2 (64bit)

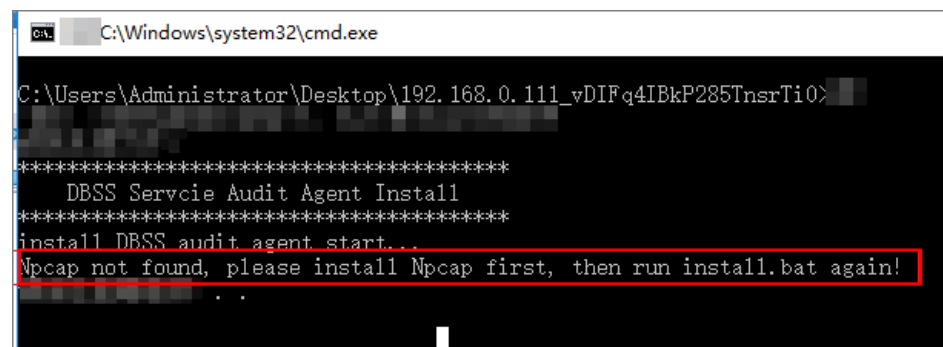
- Windows Server 2016 (64bit)
- Windows 7 (64bit)
- Windows 10 (64bit)

**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 1-2** Npcap not found



## Other Constraints

- If SSL is enabled for a database, the database cannot be audited. To use database audit, disable SSL first.
- 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.

## 1.7 Permissions Management

If you need to assign different permissions to employees in your enterprise to access your DBSS resources, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your cloud resources.

With IAM, you can use your account to create IAM users for your employees, and assign permissions to the users to control their access to specific resource types. For example, some software developers in your enterprise need to use DBSS but must not delete DBSS resources or perform any high-risk operations. To achieve this result, you can create IAM users for the software developers and grant them only the permissions required for using DBSS resources.

If your account does not need individual IAM users for permissions management, then you may skip over this chapter.

### DBSS Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these

groups. After authorization, the user can perform specified operations on BMS based on the permissions.

DBSS is a project-level service deployed and accessed in specific physical regions. To assign DBSS permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing DBSS, the users need to switch to a region where they have been authorized to use cloud services.

DBSS roles are dependent on the roles of other services. When assigning DBSS permissions to users, you need to also assign dependent roles for the DBSS permissions to take effect.

**Table 1-5** System roles supported by DBSS

Role Name	Description	Dependency
<p>DBSS System Administrator (DBSS system administrator, who has the permissions to perform operations on DBSS system resources)</p>	<ul style="list-style-type: none"> <li>• Users with this set of permissions can perform the following operations on database audit:                             <ul style="list-style-type: none"> <li>– Purchasing an instance</li> <li>– Starting, disabling, and restarting an instance</li> <li>– Obtaining the instance list</li> <li>– Obtaining the basic information of an instance</li> <li>– Obtaining the audit statistics</li> <li>– Obtaining the monitoring information</li> <li>– Obtaining the operation logs</li> <li>– Managing databases</li> <li>– Managing agents</li> <li>– Configuring email notifications</li> <li>– Backup and restoration</li> </ul> </li> </ul>	<p>To perform payment operations (for example, purchasing or renewing a DBSS instance), you must have the <b>BSS Administrator</b>, <b>VPC Administrator</b>, and <b>ECS Administrator</b> roles.</p> <ul style="list-style-type: none"> <li>• <b>VPC Administrator:</b> Users with this set of permissions can perform all execution permission for Virtual Private Cloud (VPC). It is a project-level role, which must be assigned in the same project.</li> <li>• <b>BSS Administrator:</b> Users with this set of permissions can perform any operation on menu items on pages <b>My Account</b>, <b>Billing Center</b>, and <b>Resource Center</b>. It is a project-level role, which must be assigned in the same project.</li> <li>• <b>ECS Administrator:</b> 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.</li> </ul>

Role Name	Description	Dependency
<p>DBSS Audit Administrator (DBSS audit administrator, who has the permissions to check DBSS security logs)</p>	<ul style="list-style-type: none"> <li>• Users with this set of permission can perform the following operations on database audit:               <ul style="list-style-type: none"> <li>- Obtaining the instance list</li> <li>- Obtaining the basic information of an instance</li> <li>- Obtaining the audit statistics</li> <li>- Obtaining the report results</li> <li>- Obtaining the rule information</li> <li>- Obtaining the statement information</li> <li>- Obtaining the session information</li> <li>- Obtaining the monitoring information</li> <li>- Obtaining the operation logs</li> <li>- Obtaining the database list</li> <li>- Managing reports</li> </ul> </li> </ul>	<p>None</p>



Role Name	Description	Dependency
DBSS Security Administrator (DBSS security administrator, who has the permissions to set DBSS security policies)	<ul style="list-style-type: none"> <li>• Users with this set of permission can perform the following operations on database audit:                             <ul style="list-style-type: none"> <li>- Obtaining the instance list</li> <li>- Obtaining the basic information of an instance</li> <li>- Obtaining the audit statistics</li> <li>- Obtaining the report results</li> <li>- Obtaining the rule information</li> <li>- Obtaining the statement information</li> <li>- Obtaining the session information</li> <li>- Obtaining the monitoring information</li> <li>- Obtaining the operation logs</li> <li>- Obtaining the database list</li> <li>- Configuring audit rules</li> <li>- Configuring alarm notifications</li> <li>- Managing reports</li> </ul> </li> </ul>	None

**Table 1-6** lists the common operations supported by each system-defined permission of DBSS. Select the permissions as needed.

**Table 1-6** Common operations supported by each system-defined permission

Operation	DBSS System Administrator	DBSS Audit Administrator	DBSS Security Administrator
Purchasing an instance	√	×	×
Starting, disabling, and restarting an instance	√	×	×
Obtaining the instance list	√	√	√
Obtaining the basic information of an instance	√	√	√
Obtaining the audit statistics	√	√	√
Obtaining the monitoring information	√	√	√
Obtaining the operation logs	√	√	√
Managing databases	√	×	×
Managing agents	√	×	×
Configuring email notifications	√	×	×
Backup and restoration	√	×	×
Obtaining the report results	×	√	√
Obtaining the rule information	×	√	√
Obtaining the statement information	×	√	√

Operation	DBSS System Administrator	DBSS Audit Administrator	DBSS Security Administrator
Obtaining the session information	×	√	√
Obtaining the database list	√	√	√
Managing reports	×	√	√
Configuring audit rules	×	×	√
Configuring alarm notifications	×	×	√

## 1.8 Related Services

### ECS

DBSS instances are created on ECSs. You can use the DBSS instances to audit databases built on ECSs.

### RDS

DBSS can audit RDS instances.

### BMS

DBSS can audit databases built on BMSs.

### CTS

Cloud Trace Service (CTS) provides you with a history of DBSS operations. After enabling CTS, you can view all generated traces to review and audit performed DBSS operations. For details, see the *Cloud Trace Service User Guide*.

**Table 1-7** 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

Operation	Resource Type	Trace Name
Restarting an Instance	dbss	rebootInstance

## OBS

Object Storage Service (OBS) is an object-based cloud storage service. It provides massive, secure, highly reliable, and low-cost data storage capabilities. Database audit logs can be backed up to OBS buckets to achieve high availability for disaster recovery.

## IAM

Identity and Access Management (IAM) provides you with permission management for DBSS.

Only users who have the DBSS System Administrator permissions can use DBSS.

To obtain the permissions, contact users who have the Security Administrator permissions. For details, see the *Identity and Access Management User Guide*.

# 2 Process Overview

---

This section describes how to quickly enable database audit.

## Background

Database audit supports auditing user-installed databases on ECS/BMS as well as RDS databases on the management console.

---

### NOTICE

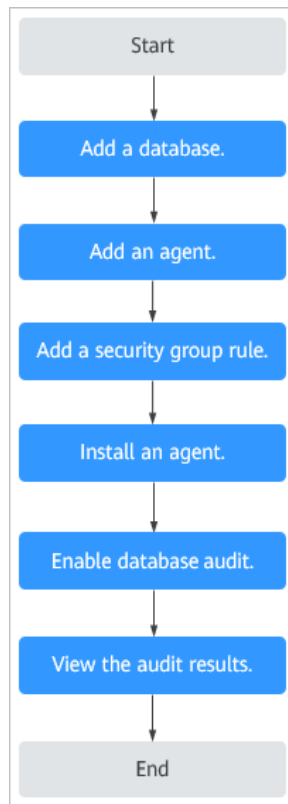
- Ensure the VPC, security group, and subnet of the database audit instance are the same as those of the node (application side or database side) where you plan to install the database audit agent. Otherwise, the instance will be unable to connect to the agent or perform audit.
- If SSL is enabled for a database, the database cannot be audited. To use database audit, disable SSL first.

---

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

## Auditing Databases Using Agents

**Figure 2-1** Procedure for quickly configuring database audit



**Table 2-1** Procedure for quickly configuring database audit

Step	Configuration	Description
1	<b>Adding a Database</b>	Apply for database audit. Add a database to the database audit instance and enable audit for the database.
2	<b>Adding an Agent</b>	Select an agent add mode. Database audit supports auditing databases built on ECS, BMS, and RDS on the cloud. Select an agent add mode based on your database deployed on the management console.
4	<b>Installing an Agent (Linux OS)</b>	Download and then install the agent on the database or application, as required by the add mode you chose.
5	<b>Enabling Database Audit</b>	Enable database audit and connect the added database to the database audit instance.

Step	Configuration	Description
6	<b>Viewing the Audit Results</b>	By default, database audit complies with a <b>full audit rule</b> , 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.

## 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 Applying for a Database Audit Instance

---


Before using the database audit function, you need to apply for a database audit instance.

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.

## Impact on the System

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

## Procedure

- Step 1** Log in to the management console.
- Step 2** Select a region, click , and choose **Security > Database Security Service**. The **Dashboard** page is displayed.
- Step 3** In the upper right corner, click **Apply for Database Audit**.
- Step 4** On the **Apply for Database Audit** page, select an **AZ** and a **Type**.
  - **AZ**: If resources are sold out in an AZ, **Sold out in this AZ** will be displayed for the AZ. In this case, select another AZ.
  - **Type**: For details about the supported editions, see [Editions](#).
- Step 5** Set database audit parameters. See [Table 3-1](#).



**Table 3-1** Parameters

Parameter	Description	Example Value
VPC	<p>You can select an existing VPC, or click <b>View VPC</b> to create one.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>Select the VPC of the node (application or database side) where you plan to install the agent.</li> <li>To change the VPC of a DBSS instance, unsubscribe from it and apply for a new one.</li> </ul> <p>For more information about VPC, see <i>Virtual Private Cloud User Guide</i>.</p>	vpc-sec
Security Group	<p>The security group configured for the instance is displayed on the page. Once a security group is selected for an instance, the instance is protected by the access rules of this security group.</p> <p>For more information about security groups, see <i>Virtual Private Cloud User Guide</i>.</p>	sg
Subnet	<p>The <b>Subnet</b> drop-down list displays all available subnets.</p> <p>For more information about subnets, see <i>Virtual Private Cloud User Guide</i>.</p>	public_subnet
Instance Name	Custom name of the instance	DBSS-test

**Step 6** Confirm the configuration and click **Try Now**.

**Step 7** On the details confirmation page, you can click **Submit**.

On the **Instances** page, you can view the created database audit instance.

If the **Status** is **Running**, you have successfully applied for the database audit instance.

----End


# 4 Step 1: Add a Database

Database audit supports databases built on ECS, BMS, and RDS on the console. After applying for a database audit instance, you need to add the database to be audited to the instance.

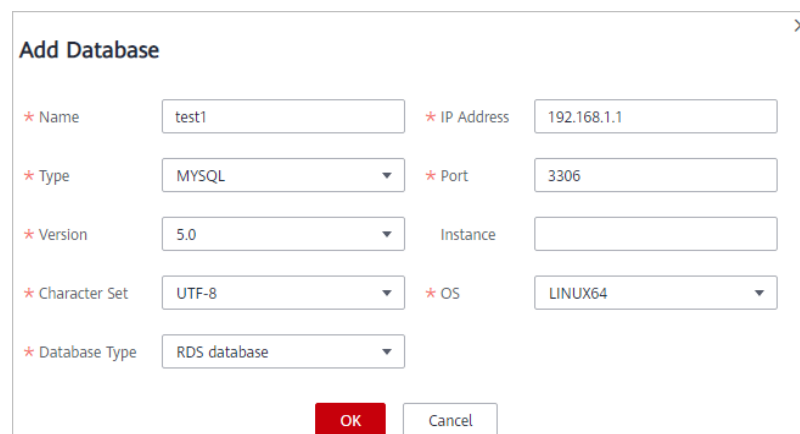
## Prerequisites

You have applied for 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 > 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 4-1](#).

**Figure 4-1** Add Database dialog box



* Name	<input type="text" value="test1"/>	* IP Address	<input type="text" value="192.168.1.1"/>
* Type	<input type="text" value="MYSQL"/>	* Port	<input type="text" value="3306"/>
* Version	<input type="text" value="5.0"/>	Instance	<input type="text"/>
* Character Set	<input type="text" value="UTF-8"/>	* OS	<input type="text" value="LINUX64"/>
* Database Type	<input type="text" value="RDS database"/>		

OK Cancel

**Table 4-1** 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. The IP address must be an internal IP address in IPv4 or IPv6 format.	IPv4: 192.168.1.1 IPv6: fe80:0000:0000:0000:0000:0000:0000:0000
Type	Supported database type. The options are as follows: <ul style="list-style-type: none"> <li>• MYSQL</li> <li>• ORACLE</li> <li>• POSTGRESQL</li> <li>• SQLSERVER</li> <li>• DWS</li> <li>• TAURUS</li> <li>• GaussDB</li> <li>• DAMENG</li> <li>• KINGBASE</li> <li>• SHENTONG</li> <li>• GBase 8a</li> <li>• GBase XDM Cluster</li> <li>• Greenplum</li> <li>• HighGo</li> <li>• Mariadb</li> </ul> <p><b>NOTE</b> If <b>ORACLE</b> is selected, to make the audit settings take effect, restart the applications to be audited and log in to the database again.</p>	MYSQL
Port	Port number of the database to be added	3306

Parameter	Description	Example Value
Version	<p>Supported database versions</p> <ul style="list-style-type: none"> <li>• When <b>Type</b> is set to <b>MYSQL</b>, the following versions are available:</li> <li>• When <b>Type</b> is set to <b>ORACLE</b>, the following versions are available: <ul style="list-style-type: none"> <li>- 11g</li> <li>- 12c</li> <li>- 19c</li> </ul> </li> <li>• When <b>Type</b> is set to <b>POSTGRESQL</b>, the following versions are available: <ul style="list-style-type: none"> <li>- 7.4</li> <li>- 8.0</li> <li>8.0, 8.1, 8.2, 8.3, 8.4</li> <li>- 9.0</li> <li>9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6</li> <li>- 10.0</li> <li>10.0, 10.1, 10.2, 10.3, 10.4, 10.5</li> <li>- 11.0</li> <li>- 12.0</li> <li>- 13.0</li> </ul> </li> <li>• When <b>Type</b> is set to <b>SQLSERVER</b>, the following versions are available: <ul style="list-style-type: none"> <li>- 2008</li> <li>- 2012</li> <li>- 2014</li> <li>- 2016</li> <li>- 2017</li> </ul> </li> <li>• When <b>Type</b> is set to <b>DWS</b>, the following versions are available: <ul style="list-style-type: none"> <li>- 1.5</li> </ul> </li> <li>• When <b>Type</b> is set to <b>TAURUS</b>, the following versions are available: <ul style="list-style-type: none"> <li>- MySQL 8.0</li> </ul> </li> <li>• When <b>Type</b> is set to <b>GaussDB</b>, the following version is available: <ul style="list-style-type: none"> <li>- 1.4 Enterprise Edition</li> </ul> </li> <li>• When <b>Type</b> is set to <b>DAMENG</b>, the following version is available: <ul style="list-style-type: none"> <li>- DM8</li> </ul> </li> <li>• When <b>Type</b> is set to <b>KINGBASE</b>, the following version is available:</li> </ul>	5.0

Parameter	Description	Example Value
	- V8	
Instance	Instance name of the database to be audited <b>NOTE</b> <ul style="list-style-type: none"> <li>If you do not configure the <b>Instance</b> field, database audit will audit all instances in the database.</li> <li>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.</li> </ul>	-
Character Set	Encoding format of the database character set. The options are as follows: <ul style="list-style-type: none"> <li>UTF-8</li> <li>GBK</li> </ul>	UTF-8
OS	OS of the added database. The options are as follows: <ul style="list-style-type: none"> <li>LINUX64</li> </ul>	LINUX64
Database Type	Type of the database to be added. Its value can be <b>RDS database</b> or <b>Self-built database</b> .	RDS database

**Step 7** Click **OK**. Then a database in the **Disabled** state has been added to the database list. See **Figure 4-2**.

**Figure 4-2** 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

# 5 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.

## NOTE

Currently, only the following types of databases support agent-free audit:

- GaussDB for MySQL
- RDS for SQLServer
- RDS for MySQL
  - 5.6 (5.6.51.1 or later)
  - 5.7 (5.7.29.2 or later)
  - 8.0 (8.0.20.3 or later)

## Prerequisites

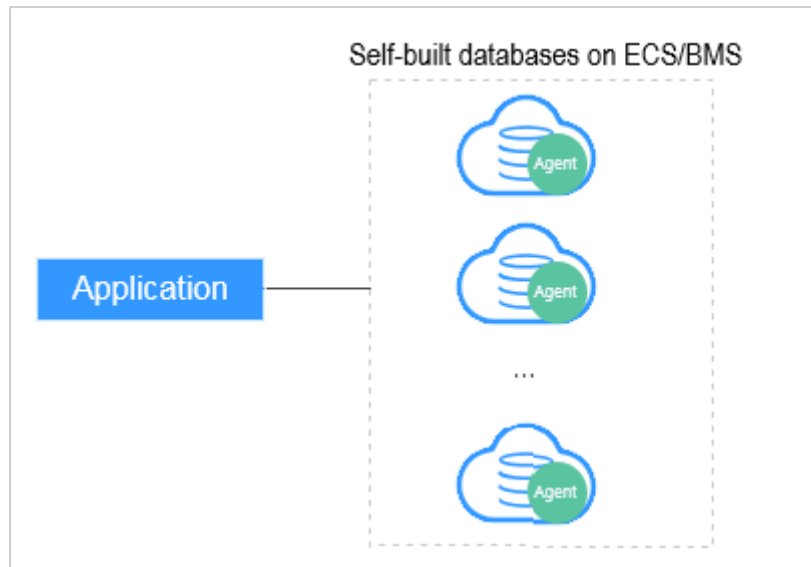
- You have applied for a database audit instance and the **Status** is **Running**.
- A database has been added.

## Scenarios

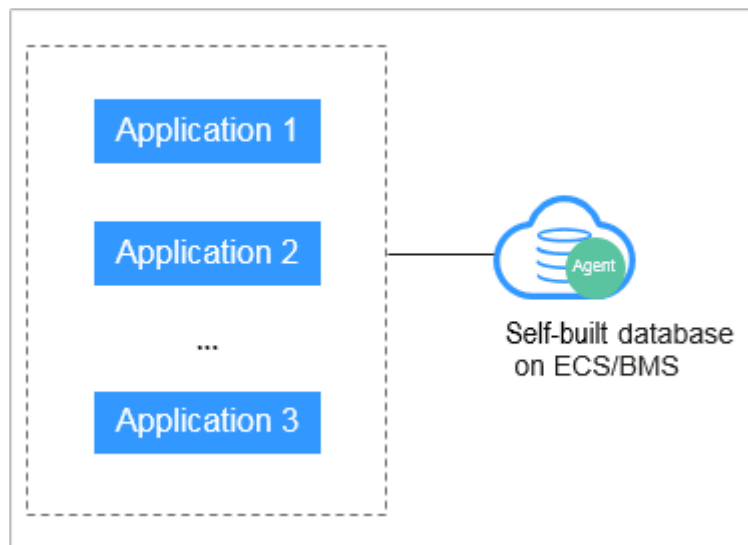
Determine where to add the agent based on how your database is deployed. Common database deployment modes are as follows:

- Deploy DBSS for databases built on ECS/BMS. For details, see [Figure 5-1](#) and [Figure 5-2](#).

**Figure 5-1** One application connecting to multiple databases built on ECS/BMS

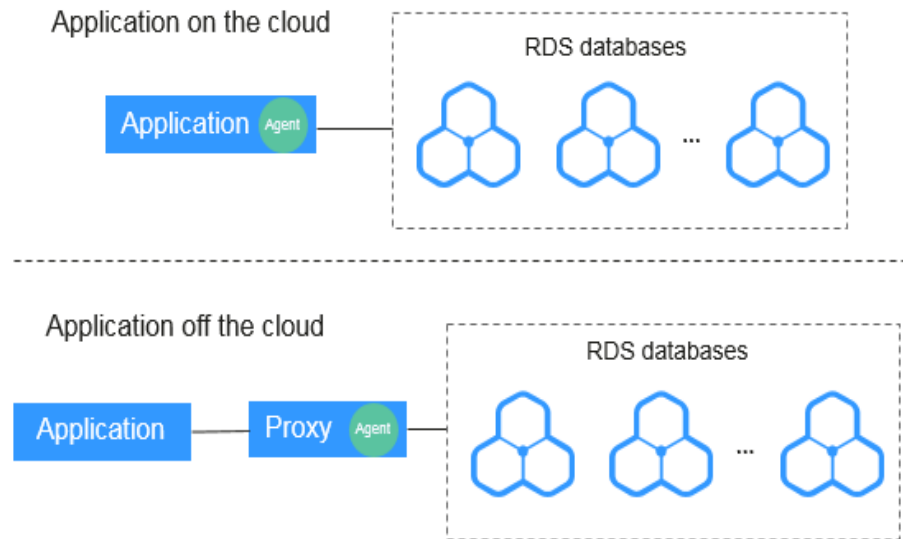


**Figure 5-2** Multiple applications connecting to one database built on ECS/BMS

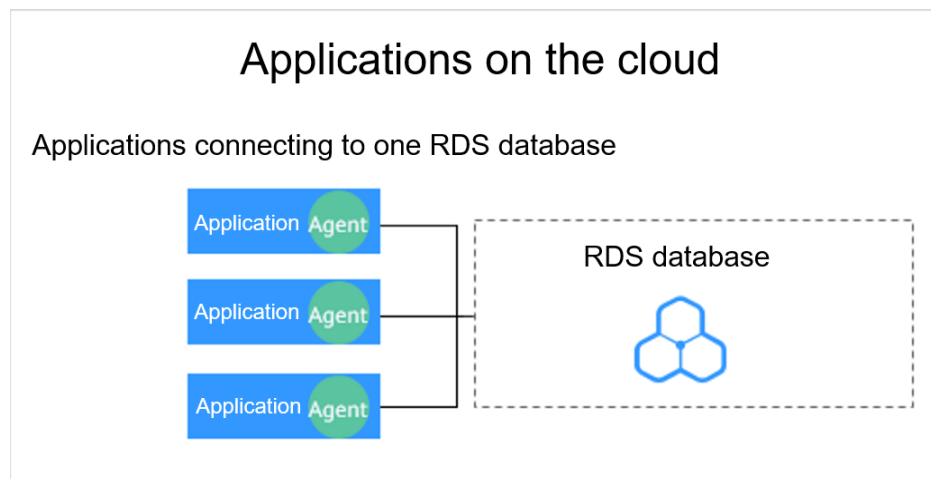


- Deploy DBSS for RDS databases. For details, see [Figure 5-3](#) and [Figure 5-4](#).

**Figure 5-3** One application connecting to multiple RDS databases



**Figure 5-4** Multiple applications connecting to one RDS database



**Table 5-1** 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 5-1** 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	<ul style="list-style-type: none"> <li>• Add the agent on the database side.</li> <li>• If an application connects to multiple databases built on ECS/BMS, the agent must be added on all these databases.</li> </ul>
RDS database	Application (if applications are deployed on the cloud)	Access records of all the databases connected to the application	<ul style="list-style-type: none"> <li>• Add the agent on the application side.</li> <li>• If an application connects to multiple RDS databases, add an agent on each of the databases. Set <b>Installation Node Type</b> for one of them and select <b>Select an existing agent</b> for the rest of them. For details, see <a href="#">Selecting an existing agent</a>.</li> <li>• If multiple applications connect to the same RDS database, add the agent must on all these applications.</li> </ul>
	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.	<ul style="list-style-type: none"> <li>• Add the agent on the application side.</li> <li>• <b>Installing Node IP Address</b> must be set to the IP address of the proxy.</li> </ul>

## 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 > Database Security Service**. The **Dashboard** page is displayed.

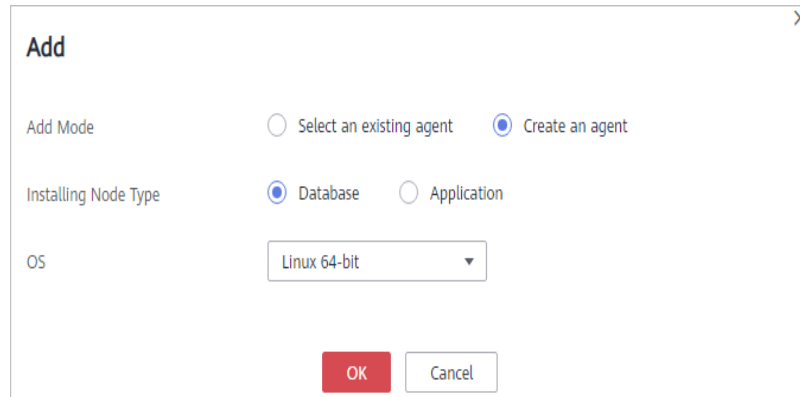
**Step 3** In the navigation tree on the left, choose **Databases**.

**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 5-5**. For details about related parameters, see **Table 5-2**.


**Figure 5-5** Adding an agent to a database



**Table 5-2** Parameters for adding an agent (databases built on ECS/BMS)

Parameter	Description	Example Value
Add Mode	<p>Mode for adding an agent</p> <ul style="list-style-type: none"> <li><b>Select an existing agent</b> If an agent has been installed on a database connected to the same application as the desired database, select <b>Select an existing agent</b>.</li> <li><b>Create an agent</b> If no agent is available, select <b>Create an agent</b> to create one.</li> </ul>	Create an agent
Installing Node Type	<p>This parameter is mandatory when <b>Add Mode</b> is set to <b>Create an agent</b>.</p> <p>When auditing user-installed databases on ECS/BMS, select <b>Database</b> for <b>Installing Node Type</b>.</p>	Database
OS	<p>OS of the database to be audited. Its value can be .</p> <p>You can select <b>LINUX64-X86</b>, <b>LINUX64-ARM</b>, or <b>WINDOWS64</b>.</p> <p><b>NOTE</b> Select <b>LINUX64_X86</b> or <b>LINUX64_ARM</b> based on the server architecture.</p>	LINUX64-X86

**Step 7** Click **OK**.

**Step 8** Click  in the lower part of the database list page to expand the database details and view the information about the added agent.

**Figure 5-6** Successfully adding 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 ▾

**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 > 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 5-7](#) and [Figure 5-8](#). For details about related parameters, see [Table 5-3](#).

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

**NOTE**

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

**Figure 5-7** Selecting an existing agent

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. It contains the following fields and options:

- Add Mode:** Two radio buttons are present. The first, "Select an existing agent", is selected (indicated by a blue dot). The second, "Create an agent", is unselected.
- Database Name:** A dropdown menu showing "tesT".
- Agent ID:** A dropdown menu showing "AXa5xiGbzoA3BGc6i4\_g".
- Buttons:** "OK" (red) and "Cancel" (white) buttons are at the bottom.

- 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 5-8** Adding an agent to an application

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. It contains the following fields and options:


- Add Mode:** Two radio buttons are present. The first, "Select an existing agent", is unselected. The second, "Create an agent", is selected (indicated by a blue dot).
- Installing Node Type:** Two radio buttons are present. The first, "Database", is unselected. The second, "Application", is selected (indicated by a blue dot).
- Installing Node IP Address:** A text input field containing "192.168.1.1".
- Audited NIC Name:** An empty text input field.
- CPU Threshold (%):** A text input field containing "80".
- Memory Threshold (%):** A text input field containing "80".
- OS:** A dropdown menu showing "Linux 64-bit".
- Buttons:** "OK" (red) and "Cancel" (white) buttons are at the bottom.

**Table 5-3** Parameters for adding an agent (RDS databases)

Parameter	Description	Example Value
Add Mode	<p>Mode for adding an agent</p> <ul style="list-style-type: none"> <li>• <b>Selecting an existing agent</b> If an agent has been installed on a database connected to the same application as the desired database, select <b>Select an existing agent</b>.</li> <li>• <b>Create an agent</b> If no agent is available, select <b>Create an agent</b> to create one.</li> </ul>	Create an agent

Parameter	Description	Example Value
Installing Node Type	This parameter is mandatory when <b>Add Mode</b> is set to <b>Create an agent</b> . To audit the RDS databases, select <b>Application</b> .	Application
Installing Node IP Address	This parameter is mandatory if <b>Installing Node Type</b> is set to <b>Application</b> . 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. The IP address must be an internal IP address in IPv4 or IPv6 format. <b>NOTICE</b> 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 <b>Installing Node Type</b> is set to <b>Application</b> . Name of the network interface card (NIC) of the application node to be audited	-
CPU Threshold (%)	Optional. This parameter is configurable if <b>Installing Node Type</b> is set to <b>Application</b> . CPU threshold of the application node to be audited. The default value is <b>80</b> . <b>NOTICE</b> If the CPU usage of a server exceeds the threshold, the agent on the server will stop running.	80
Memory Threshold (%)	Optional. This parameter is configurable if <b>Installing Node Type</b> is set to <b>Application</b> . Memory threshold of the application node to be audited. The default value is <b>80</b> . <b>NOTICE</b> If the memory usage of your server exceeds the threshold, the agent will stop running.	80
OS	Optional. This parameter is configurable if <b>Installing Node Type</b> is set to <b>Application</b> . OS of the application node to be audited. The value can be <b>LINUX64</b> or <b>WINDOWS64</b> .	LINUX64

**Step 7** Click **OK**.

**Step 8** Click  next to the database to view its details and information about the added agent.

**Figure 5-9** Successfully adding 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
AXDCIOVWaZghMXmOfEAz	Database	2.3.3.5	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**

After adding an agent, install the agent on the database or application based on the add mode you chose. Database audit works only when the database to be audited is connected to the database audit instance. For details about how to install an agent, see [Installing an Agent](#).

# 6 Step 3: Download and Install the Agent

---

## 6.1 Downloading an Agent

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

 **NOTE**

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

### Prerequisites

- You have applied for 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 > 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  in the lower part of the database list to expand the agent details. Locate the target agent and click **Download Agent** in the **Operation** column. 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
AXDCiOVWazghMXmOrEAz	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 applied for 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.

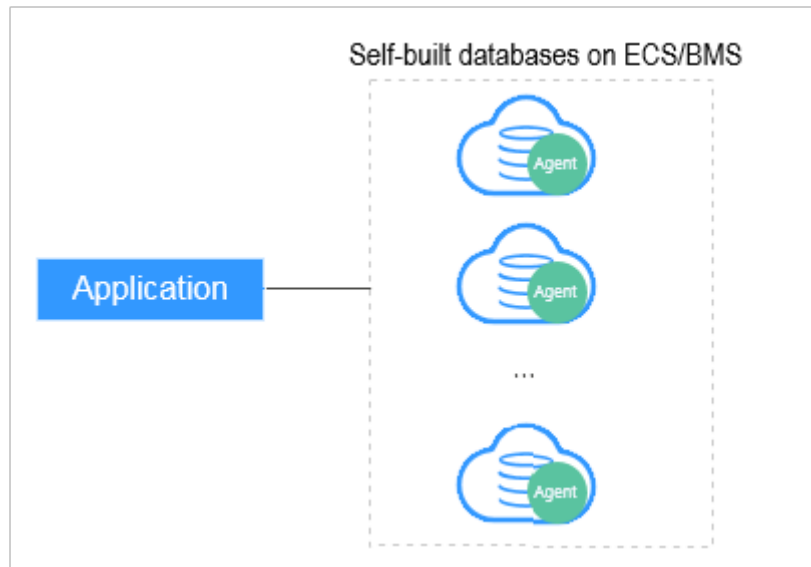
### Scenarios

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:

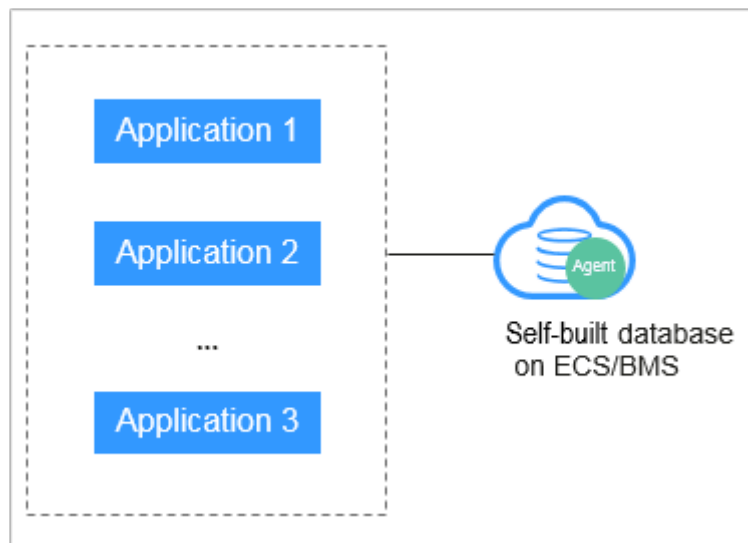
- Deploy DBSS for databases built on ECS/BMS. For details, see [Figure 6-2](#) and [Figure 6-3](#).



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

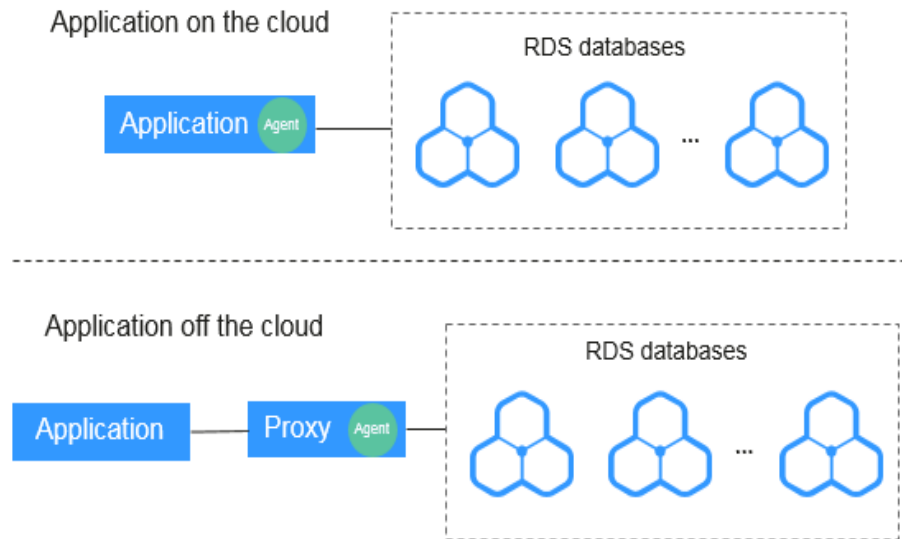


**Figure 6-3** Multiple applications connecting to one database built on ECS/BMS

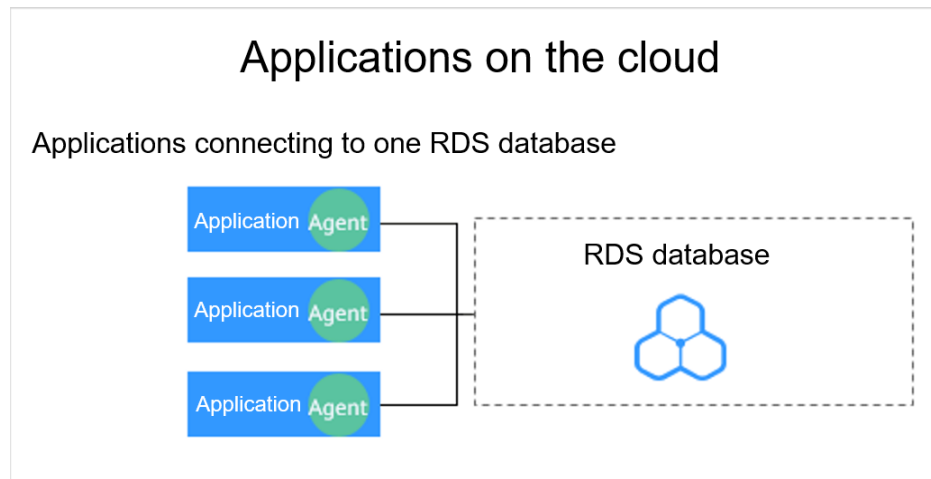


- Deploy DBSS for RDS databases. For details, see [Figure 6-4](#) and [Figure 6-5](#).

**Figure 6-4** One application connecting to multiple RDS databases



**Figure 6-5** Multiple applications connecting to one RDS database



**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	<ul style="list-style-type: none"> <li>Install the agent on the database side.</li> <li>If an application connects to multiple databases built on ECS/BMS, the agent must be installed on all these databases.</li> </ul>
RDS database	Application side (if applications are deployed on the cloud)	Access records of all the databases connected to the application	<ul style="list-style-type: none"> <li>Install the agent on the application side.</li> <li>If multiple applications are connected to the same RDS database, the agent must be installed on all these applications.</li> </ul>
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 Ubuntu, 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

## 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

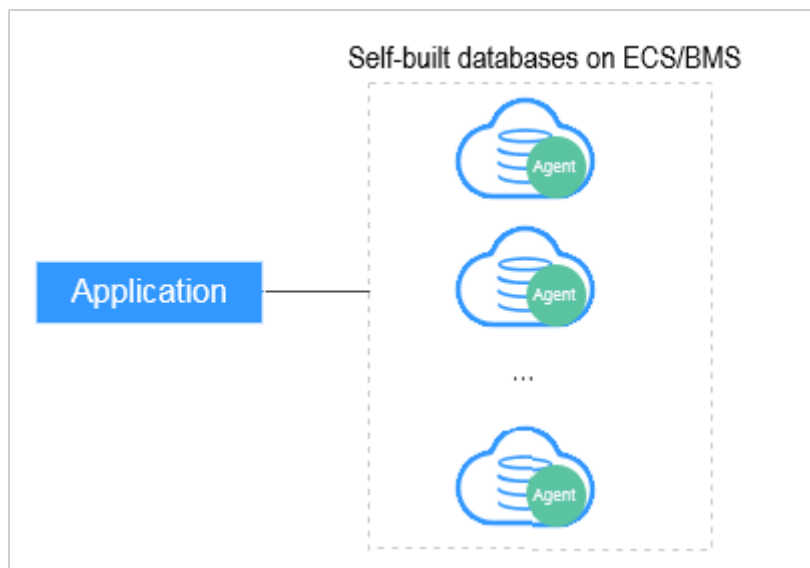
- You have applied for a database audit instance and the **Status** is **Running**.
- You have added an agent to your database.
- You have obtained the agent installation package for the Windows OS.
- The Windows OS version of the target node is supported by the agent.

## Scenarios

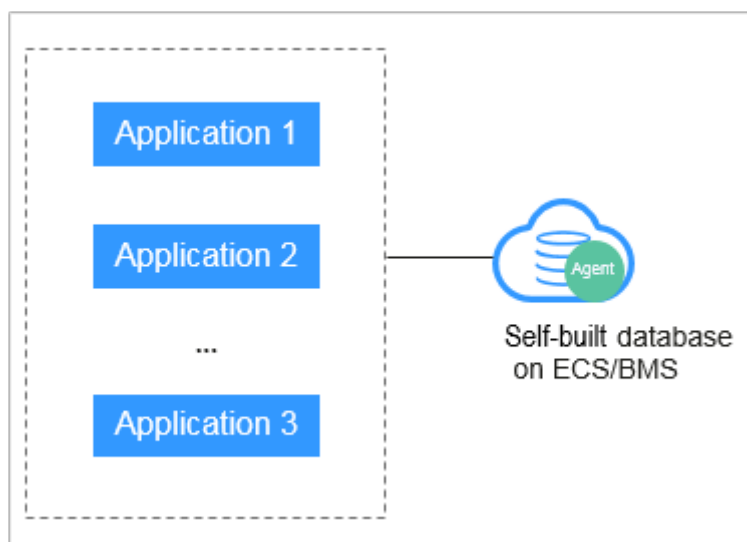
You can install the agent on the database or application side, depending on your database type and deployment scenario. Common database scenarios are as follows:

- 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

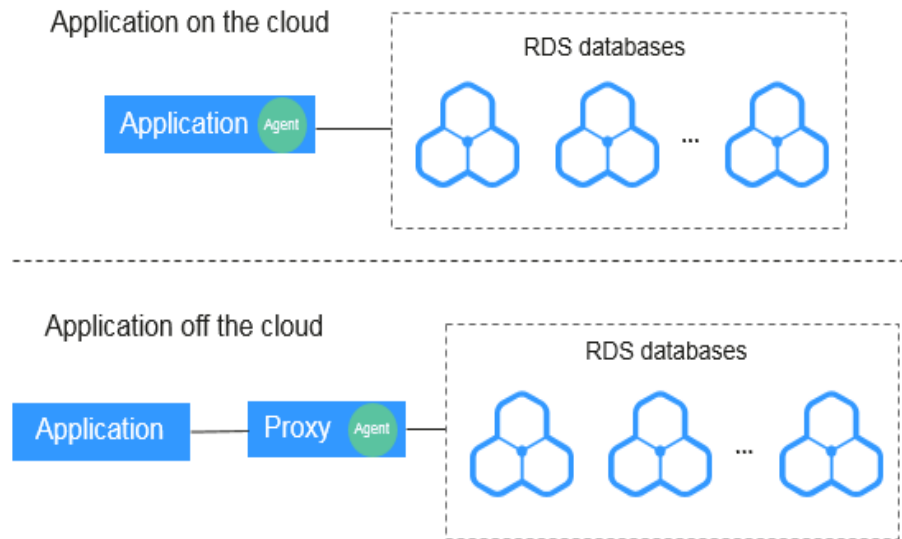


**Figure 6-7** Multiple applications connecting to one database built on ECS/BMS

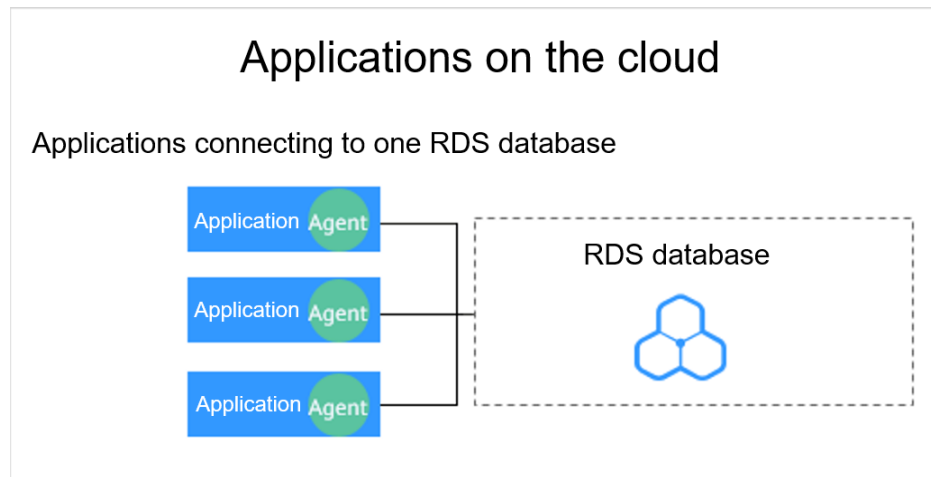


- Deploy DBSS for RDS databases. For details, see [Figure 6-8](#) and [Figure 6-9](#).

**Figure 6-8** One application connecting to multiple RDS databases



**Figure 6-9** Multiple applications connecting to one RDS database



**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                                                     | <ul style="list-style-type: none"> <li>Install the agent on the database side.</li> <li>If an application connects to multiple databases built on ECS/BMS, the agent must be installed on all these databases.</li> </ul>     |
| RDS database                   | Application side (if applications are deployed on the cloud) | Access records of all the databases connected to the application                                                       | <ul style="list-style-type: none"> <li>Install the agent on the application side.</li> <li>If multiple applications are connected to the same RDS database, the agent must be installed on all these applications.</li> </ul> |
| 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/>.

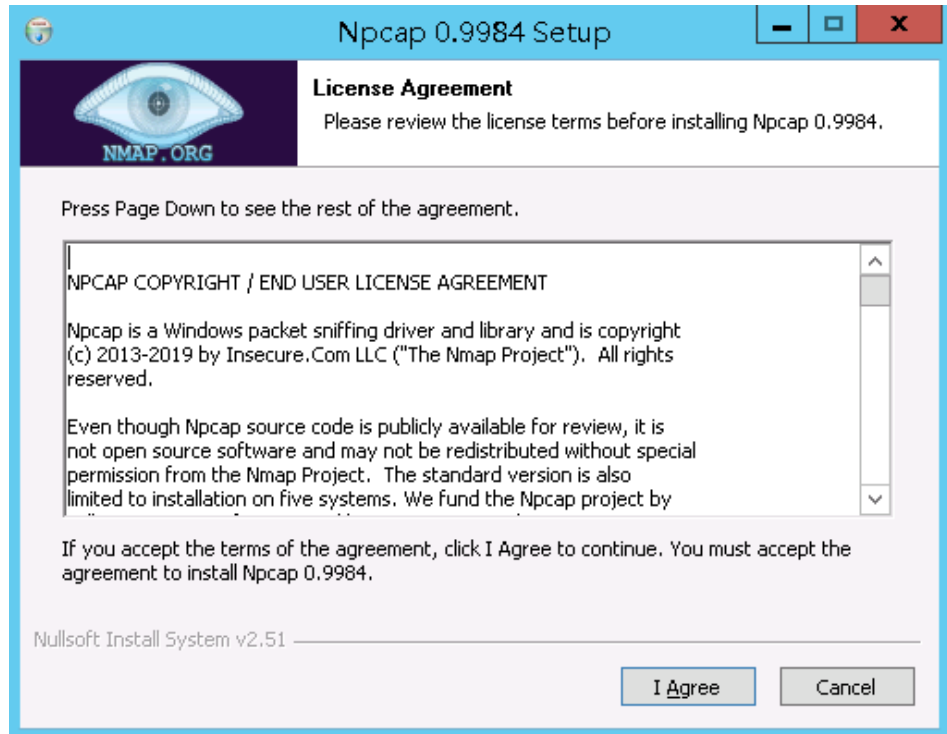
**Figure 6-10** Downloading Npcap



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

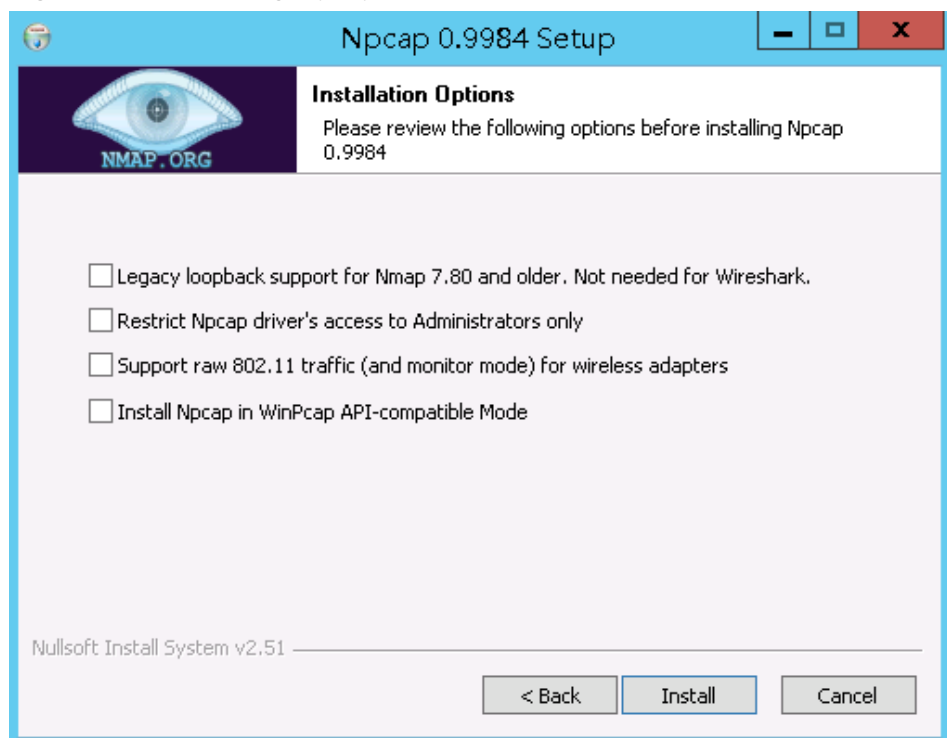
- c. Double-click the Npcap installation package.
- d. In the displayed dialog box, click **I Agree**, as shown in [Figure 6-11](#).

**Figure 6-11** Agreeing to install Npcap



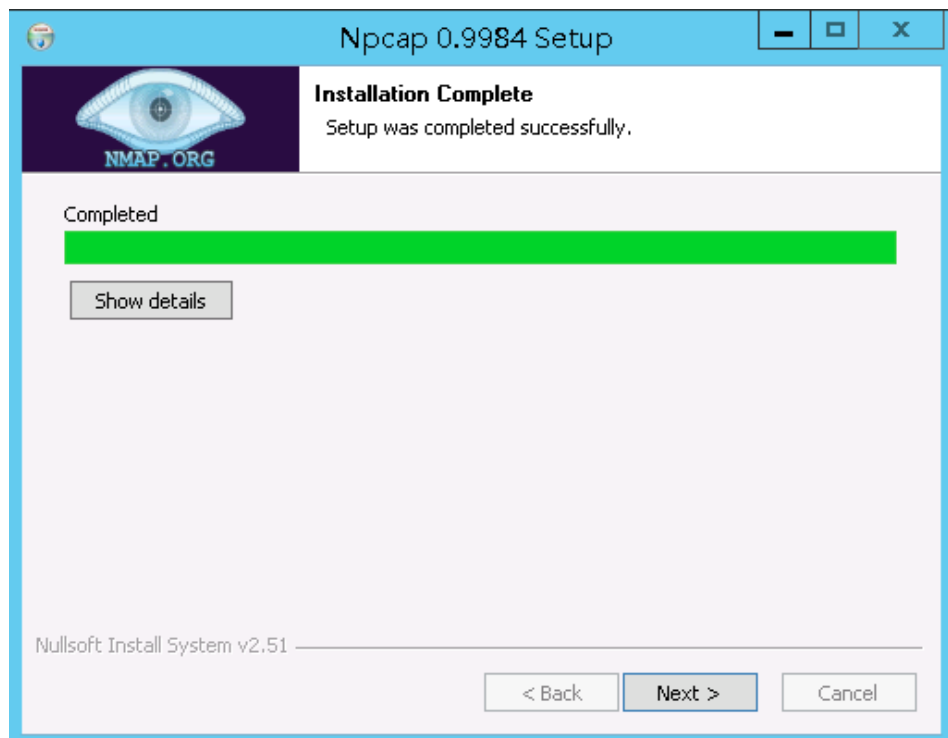
- e. In the displayed dialog box, leave all the check boxes unselected and click **Install**, as shown in [Figure 6-12](#).

**Figure 6-12** Installing Npcap

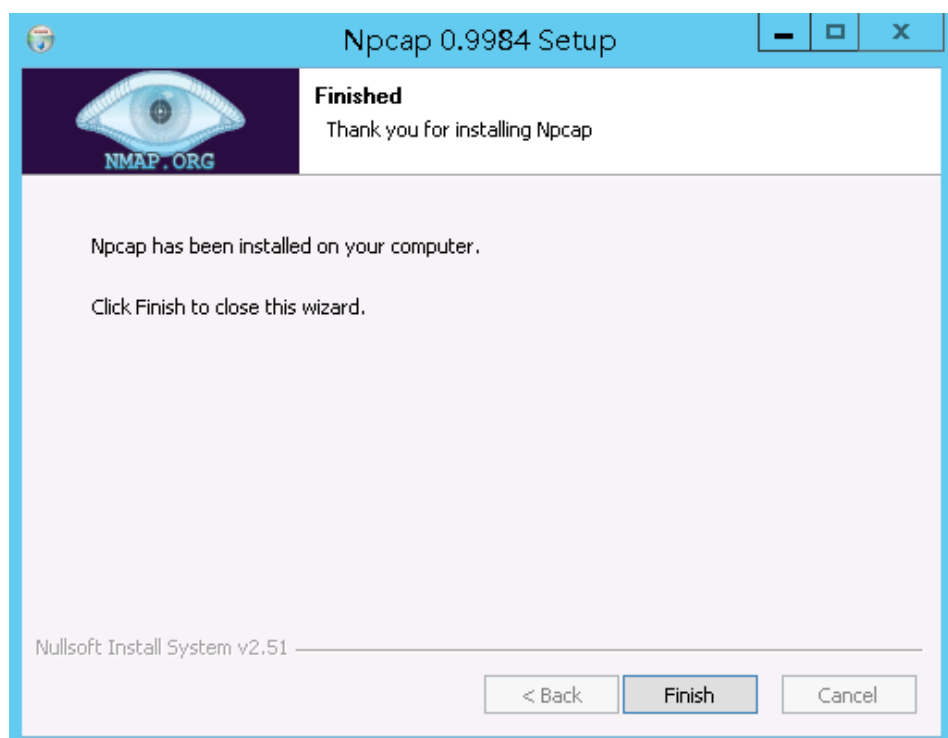




- f. In the displayed dialog box, click **Next**.



- g. Click **Finish**.

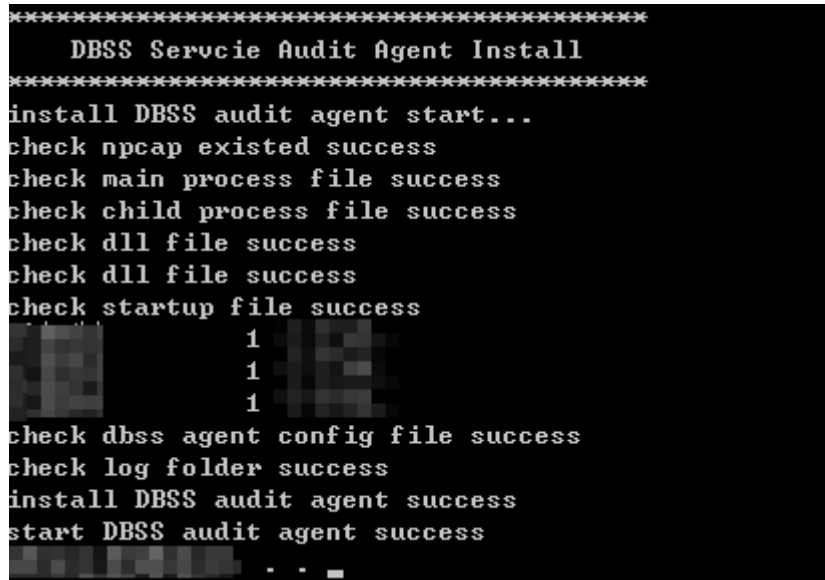


**Step 2** Log in to the target Windows server as the **Administrator** user.

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

- Step 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 4: Add a Security Group Rule

---

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

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

## NOTE

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

## Prerequisites

- You have applied for 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** In the navigation tree on the left, choose **Database Audit > Databases**.

**Step 3** In the **Instance** drop-down list, select the instance whose security group rule is to be added.


**Step 4** 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**.

**Step 5** Click **Add Security Group Rule**.

**Step 6** In the displayed dialog box, record the security group name (for example, **default**) of the database audit instance.

**Step 7** Click **Go to VPC**.

**Step 8** 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 9** Click the group name **default**.

**Step 10** 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 4](#).

- 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 11](#).

**Step 11** Add an inbound rule for the installing node.

1. 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

# 8 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**.

## Enabling Database Audit

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

**Step 2** In the navigation tree on the left, choose **Databases**.

**Step 3** Select a database audit instance from the **Instance** drop-down list.

**Step 4** In the database list, click **Enable** in the **Operation** column of the database you want to audit.

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

**Figure 8-1** Enabling database audit

| No. | Database Information                      | Character Set | IP Address/Port       | Instance | OS      | Audit Status | Agent | Operation        |
|-----|-------------------------------------------|---------------|-----------------------|----------|---------|--------------|-------|------------------|
| 1   | Name:<br>Type: MYSQL<br>Version: 5.0      | UTF8          | 192.168.0.73<br>3306  | ..       | LINUX64 | Enabled      | Add   | Disable   Delete |
| 2   | Name: test<br>Type: MYSQL<br>Version: 5.7 | UTF8          | 192.168.0.104<br>3306 | ..       | LINUX64 | Enabled      | Add   | Disable   Delete |
| 3   | Name: test<br>Type: MYSQL<br>Version: 5.0 | UTF8          | .7001.d473:<br>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** In the left navigation pane, choose **Dashboard**.

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

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

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

**Step 7** Click  next to **Time** to set the start and end time, and click **Submit**.

**Figure 8-2** Viewing SQL statements

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

----End

# 9 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 applied for 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 > 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

**Table 9-1** Parameters

| Parameter            | Description                                                                                                                                                                                                  | Example Value |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Name                 | Name of the custom audit scope                                                                                                                                                                               | audit00       |
| Database Name        | Database to be added to the audit scope                                                                                                                                                                      | db03          |
| Operations           | Audited operation type. It can be <b>Login</b> or <b>Operation</b> .<br>When you select the <b>Operation</b> check box, you can select <b>All operations</b> or the operations in <b>DDL, DML, and DCL</b> . | Login         |
| Database Account     | (Optional) Database username.<br>You can specify multiple accounts, separated by commas (,).                                                                                                                 | -             |
| Exception IP Address | (Optional) IP addresses that do not need to be audited.<br><b>NOTE</b><br>If an IP address is set as both a source and an exception IP address, the IP address will not be audited.                          | -             |



| Parameter         | Description                                                                                                                                                          | Example Value |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Source IP Address | (Optional) IP address or IP address range used for accessing the database to be audited<br><br>The IP address must be an internal IP address in IPv4 or IPv6 format. | -             |
| Source Port       | (Optional) Port number used for accessing the database to be audited                                                                                                 | -             |

**Step 7** Click **OK**.

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

----End

## Related Operations

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

# 10 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 applied for 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**.

### Disabling 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 > 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.

#### NOTE

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

**Step 6** Locate the SQL injection rule you want to disable, and click **Disable** in the **Operation** column.

**Figure 10-1** Disabling an SQL injection detection rule

| No. | Name | Command Feature    | Risk Severity | Status  | Operation                               |
|-----|------|--------------------|---------------|---------|-----------------------------------------|
| 1   | qwe  | Regular expression | High          | Enabled | Set Priority <b>Disable</b> Edit Delete |

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

----End

## Follow-Up Procedure

To restart an SQL injection detection rule, click **Enable** in the **Operation** column of the target rule.

**Figure 10-2** Enabling an SQL injection detection rule

| No. | Name                            | Command Feature    | Risk Severity | Status   | Operation     |
|-----|---------------------------------|--------------------|---------------|----------|---------------|
| 1   | UNION joint query SQL injection | Regular expression | Moderate      | Disabled | <b>Enable</b> |
| 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.

# 11 Adding Risky Operations

---

After enabling database audit, add and configure risky operations for audit.

---

## NOTICE

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

---

## Prerequisites

- You have applied for 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 > 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** On the **Add Risky Operation** page, set the basic information and client IP address, as shown in [Figure 11-1](#).

**Figure 11-1** Setting the basic information and client IP address

The screenshot shows a configuration interface with two main sections. The top section, titled 'Basic Info', contains several controls: a text input for 'Name' with the value 'test'; a radio button group for 'Risk Severity' with 'High' selected; a toggle switch for 'Status' which is turned on; and a 'Select Database' section with three radio buttons: 'ALL' (selected), 'mydb01', and 'mydb02'. The bottom section, titled 'Client IP Address or IP Range', has a text area containing the IP address '192.168.0.0'. A small note above the text area reads: 'Enter an IP address or IP range. For multiple IP addresses or IP ranges, put one IP address or IP range in one line. Each IP address or IP range is unique. (All are audited by default.)'

**Table 11-1** 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: <ul style="list-style-type: none"> <li>• High</li> <li>• Moderate</li> <li>• Low</li> <li>• No risks</li> </ul>                  | High                                                                                  |
| Status                        | Status of a risky operation                                                                                                                                                                 |  |
| Select Database               | Database that the risky operation will be applied to<br>You can select <b>ALL</b> or a specific database.                                                                                   | -                                                                                     |
| Client IP Address or IP Range | IP address or IP address range of the client<br>The IP address can be an IPv4 address (for example, 192.168.1.1) or an IPv6 address (for example, fe80:0000:0000:0000:0000:0000:0000:0000). | 192.168.0.0                                                                           |

**Step 6** Set the operation type, operation object, and execution result, as shown in [Figure 11-2](#). For details about related parameters, see [Table 11-2](#).

**Figure 11-2** Setting the operation type, operation object, and execution result

**Table 11-2** Parameters

| Parameter  | Description                                                                                                                                                                                                                                                                                                         | Example Value |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Operations | Type of a risky operation, including <b>Login</b> and <b>Operation</b><br>When you select the <b>Operation</b> check box, you can select <b>All operations</b> or the operations in <b>DDL, DML, and DCL</b> .                                                                                                      | Operation     |
| Objects    | Enter the schema, target table, and field information after clicking <b>Add Operation Object</b> . Click <b>OK</b> to add an operation object.                                                                                                                                                                      | -             |
| Results    | Set <b>Affected Rows</b> and <b>Operation Duration</b> . The operation conditions are as follows: <ul style="list-style-type: none"> <li>• <b>Greater than</b></li> <li>• <b>Less than</b></li> <li>• <b>Equal To</b></li> <li>• <b>Equal to or greater than</b></li> <li>• <b>Less than or equal to</b></li> </ul> | -             |

**Step 7** Click **Save**.

----End

# 12 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 applied for 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 > Database Security Service**. The **Dashboard** page is displayed.

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

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


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

### NOTE

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

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

- **Store Result Set**

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

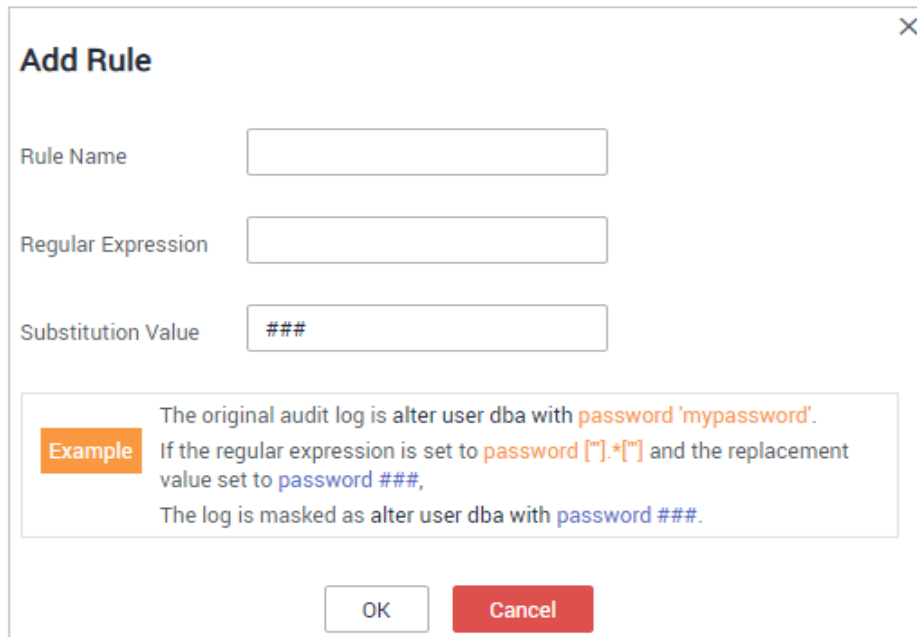
Do not enable this function if you want to prepare for PCI DSS/PCI 3DS CSS certification.

- **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 12-1](#). For details about related parameters, see [Table 12-1](#).

**Figure 12-1** Add Rule dialog box



**Table 12-1** Rule parameters

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

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

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

----End

## Verifying a Rule

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

**Step 1** Enable **Mask Privacy Data**, and ensure the "Passport NO." masking rule is enabled, as shown in [Figure 12-2](#).



**Figure 12-2** Enabling privacy data protection

| No | Rule Name       | Rule Type | Regular Expression | Substitution Value | Status  | Operation               |
|----|-----------------|-----------|--------------------|--------------------|---------|-------------------------|
| 1  | GPS Information | Default   | -                  | ***                | Enabled | Disable   Edit   Delete |

- Step 2** Log in to the database as user **root** through the MySQL database client.
- Step 3** On the database client, enter an SQL statement.  
`select * from db where HOST="Passport NO";`
- Step 4** In the navigation pane, choose **Dashboard**.
- Step 5** In the navigation tree on the left, choose **Data Reports**. The **Data Reports** page is displayed.
- Step 6** In the **Instance** drop-down list, select the instance whose SQL statement information you want to view. Click the **Statements** tab.
- Step 7** Set filtering conditions to find the entered SQL statement.
- Step 8** In the row containing the SQL statement, click **Details** in the **Operation** column.
- Step 9** Check the SQL statement information. The content of **SQL Statement** is shown in [Figure 12-3](#), indicating that the masking function is normal.

**Figure 12-3** 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.

# 13 Viewing SQL Statement Details


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

## Prerequisites

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

## Procedure

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

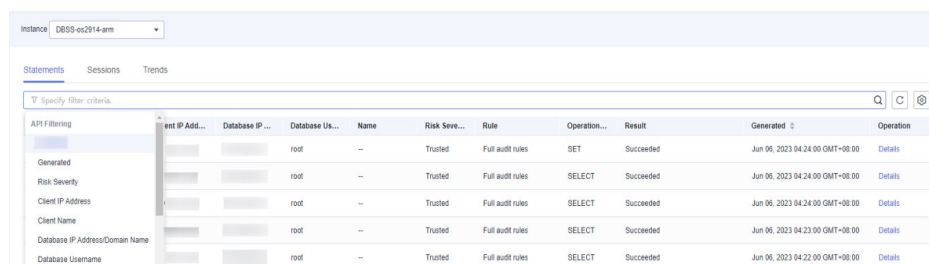
**Step 2** Select a region, click , and choose **Security > Database Security Service**. The **Dashboard** page is displayed.

**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** View SQL statement information.


**Figure 13-1** Querying SQL statements



| Instance       | Client IP Address | Database IP Address | Database Username | Name | Risk Severity | Rule             | Operation | Result    | Generated                       | Operation |
|----------------|-------------------|---------------------|-------------------|------|---------------|------------------|-----------|-----------|---------------------------------|-----------|
| DBSS-oc2914-am |                   |                     | root              | --   | Trusted       | Full audit rules | SET       | Succeeded | Jun 06, 2023 04:24:00 GMT+08:00 | Details   |
|                |                   |                     | root              | --   | Trusted       | Full audit rules | SELECT    | Succeeded | Jun 06, 2023 04:24:00 GMT+08:00 | Details   |
|                |                   |                     | root              | --   | Trusted       | Full audit rules | SELECT    | Succeeded | Jun 06, 2023 04:24:00 GMT+08:00 | Details   |
|                |                   |                     | root              | --   | Trusted       | Full audit rules | SELECT    | Succeeded | Jun 06, 2023 04:23:00 GMT+08:00 | Details   |
|                |                   |                     | root              | --   | Trusted       | Full audit rules | SELECT    | Succeeded | Jun 06, 2023 04:22:00 GMT+08:00 | Details   |

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

- Select **All**, **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days** for **Time** and click  to view SQL statements of the specified time range.

- Select **All**, **High**, **Moderate**, **Low**, or **Trusted** for **Risk Severity** and click . SQL statements of specified severity are displayed in the list.

 **NOTE**

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

**Step 6** In the row containing the desired SQL statement, click **Details** in the **Operation** column.

**Figure 13-2** Viewing details of SQL statements

| SQL Statements                   | Client IP Add... | Database IP... | Database Us... | Name | Risk Seve... | Rule             | Operation... | Result    | Generated                       | Operation               |
|----------------------------------|------------------|----------------|----------------|------|--------------|------------------|--------------|-----------|---------------------------------|-------------------------|
| set @@session.wait_timeout=36000 |                  |                | root           | --   | Trusted      | Full audit rules | SET          | Succeeded | Jun 06, 2023 04:24:00 GMT+08:00 | <a href="#">Details</a> |
| SELECT @@transaction_isolation   |                  |                | root           | --   | Trusted      | Full audit rules | SELECT       | Succeeded | Jun 06, 2023 04:24:00 GMT+08:00 | <a href="#">Details</a> |

**Step 7** View the SQL statement information in the **Details** dialog box, as shown in [Figure 13-3](#). For details about related parameters, see [Table 13-1](#).

**NOTICE**

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

**Figure 13-3** Details dialog box

×

**Details**

|                       |                                  |                                 |                                 |
|-----------------------|----------------------------------|---------------------------------|---------------------------------|
| Session ID            | 29057003                         | Database Instance               | --                              |
| Database Type         | MySQL8.0.22                      | Database User                   | root                            |
| Client MAC Address    | --                               | Database MAC Address            | --                              |
| Client IP Address     |                                  | Database IP Address/Domain Name |                                 |
| Client Port           | 0                                | Database Port                   | 3306                            |
| Client Name           | --                               | Operation Type                  | SET                             |
| Operation Object Type | VARIABLE                         | Response Result                 | EXECUT_SUCCESS                  |
| Affected Rows         | 0                                | Started                         | Jun 06, 2023 04:24:00 GMT+08... |
| Response Received     | Jun 06, 2023 04:24:00 GMT+08...  |                                 |                                 |
| SQL Statement         | set @@session.wait_timeout=36000 |                                 |                                 |
| Request Result        | --                               |                                 |                                 |

Close

**Table 13-1** Parameters for details of SQL statements

| Parameter  | Description                                              |
|------------|----------------------------------------------------------|
| Session ID | ID of an SQL statement, which is automatically generated |

| Parameter                       | Description                                                                      |
|---------------------------------|----------------------------------------------------------------------------------|
| Database Instance               | Database where an SQL statement is executed                                      |
| Database Type                   | Type of the database where an SQL statement is executed                          |
| Database User                   | Database user for executing an SQL statement                                     |
| Client MAC Address              | MAC address of the client where an SQL statement is executed                     |
| Database MAC Address            | MAC address of the database where an SQL statement is executed                   |
| Client IP Address               | IP address of the client where an SQL statement is executed                      |
| Database IP Address/Domain Name | IP address or the domain name of the database where an SQL statement is executed |
| Client Port                     | Port of the client where an SQL statement is executed                            |
| Database Port                   | Port of the database where the SQL statement is executed                         |
| Client Name                     | Name of the client where an SQL statement is executed                            |
| Operation Type                  | Type of an SQL statement operation                                               |
| Operation Object Type           | Type of an SQL statement operation object                                        |
| Response Result                 | Response by executing an SQL statement                                           |
| Affected Rows                   | Number of rows affected by executing an SQL statement                            |
| Started                         | Time when an SQL statement starts to be executed                                 |
| Ended                           | Time when the SQL statement execution ends                                       |
| SQL Statement                   | Name of an SQL statement                                                         |
| Request Result                  | Result of requesting for executing an SQL statement                              |

----End

# 14 Viewing Session Distribution

---

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

## Prerequisites

- You have applied for 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 > Database Security Service**. The **Dashboard** page is displayed.

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

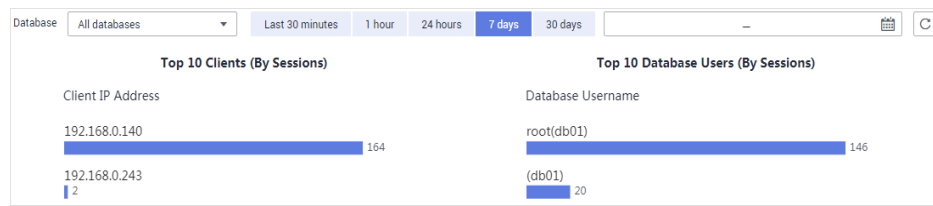
**Step 4** In the **Instance** drop-down list, select the instance whose session information you want to view.

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

**Step 6** View the session distribution chart, as shown in [Figure 14-1](#).

- 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 14-1** Viewing session distribution



----End



# 15 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.

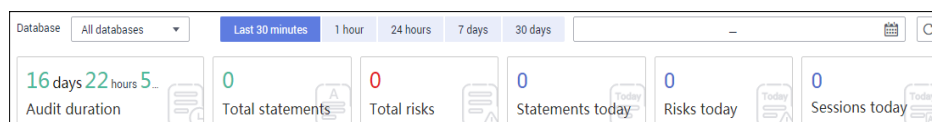
## Prerequisites

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

## Procedure

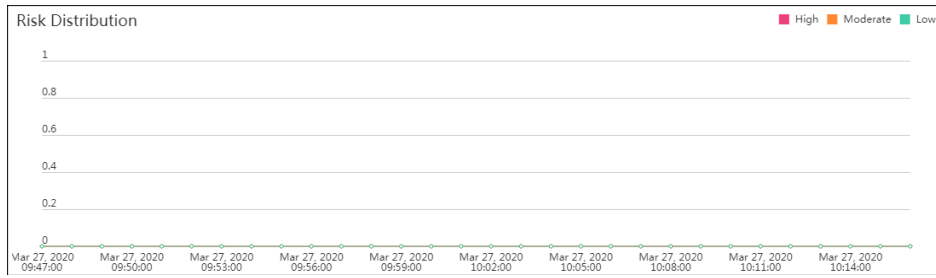
- Step 1** Log in to the management console.
- Step 2** Select a region, click , and choose **Security > Database Security Service**. The **Dashboard** page is displayed.
- Step 3** In the navigation tree on the left, choose **Data Reports**. The **Data Reports** page is displayed.
- Step 4** In the **Instance** drop-down list, select the instance whose audit information you want to view.
- Step 5** View the overall audit statistics, risk distribution, session statistics, and SQL distribution.
  - Select **All databases** or a specified database from the **Database** drop-down list to view the statistics about all databases in the instance or a specified database.
  - Select **Last 30 minutes**, **1 hour**, **Today**, **7 days**, or **30 days**, or click  to customize start time and end time to view the statistics of the specified time range.

**Figure 15-1** Viewing the audit statistics

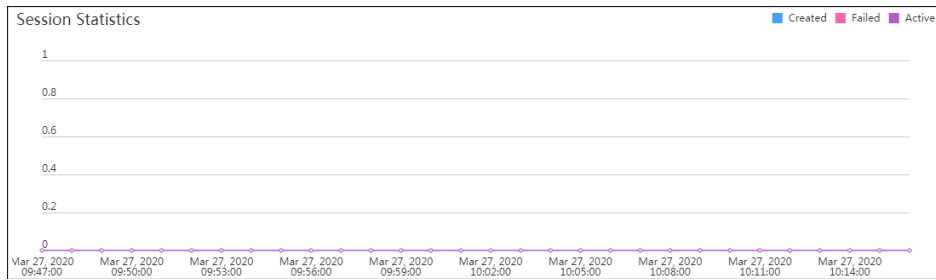




**Figure 15-2 Risk distribution**



**Figure 15-3 Session statistics**



----End

# 16 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 applied for a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.

## Report Types

Database audit provides eight types of report templates. [Table 16-1](#) lists the report names. You can generate reports and set report tasks as needed.

**Table 16-1** 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. |


| Template Name                     | Report Types              | Description                                                                                                                                           |
|-----------------------------------|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Database Server Analysis Report   | Database report           | Provides statistics and analysis on active users, user IP addresses, database logins and requests, database usage duration, and database performance. |
| Client IP Address Analysis Report | Client report             | Provides statistics on client applications, database users, and SQL statements collected from user IP addresses.                                      |
| DML Command Report                | Database operation report | Analyzes user and privileged operations based on DML commands.                                                                                        |
| DDL Command Report                | Database operation report | Analyzes user and privileged operations based on DDL commands.                                                                                        |
| DCL Command Report                | Database operation report | Analyzes user and privileged operations based on DCL commands.                                                                                        |

## Step 1: Generating a Report

You can generate reports immediately or periodically. You can also customize the generation time, frequency, and format of reports.

- **Method 1: Generating a Report Immediately**

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

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

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


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

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

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

**Figure 16-1** 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 <a href="#">Generate Report</a> |
| SOX Report                  | All databases    | Compliance report | SOX Report                  | Disabled (Weekly) | Schedule Task <a href="#">Generate Report</a> |

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

**Figure 16-2** Generate Report

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

----End

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

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

**Step 2** Select a region, click , and choose **Security > 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 16-3](#).

**Figure 16-3** Setting a task

| Template Name               | Related Database | Type              | Description                 | Task Status       | Operation                                                     |
|-----------------------------|------------------|-------------------|-----------------------------|-------------------|---------------------------------------------------------------|
| Database Security Genera... | All databases    | Overview report   | Database Security Genera... | Disabled (Weekly) | <a href="#">Schedule Task</a> <a href="#">Generate Report</a> |
| SOX Report                  | All databases    | Compliance report | SOX Report                  | Disabled (Weekly) | <a href="#">Schedule Task</a> <a href="#">Generate Report</a> |

**Step 7** In the displayed dialog box, set the parameters of the scheduled task, as shown in [Figure 16-4](#). For details about related parameters, see [Table 16-2](#).

**Figure 16-4** Setting a scheduled task

✕

### Schedule Task

Notifications are sent and billed by SMN. [Pricing Details](#)

★ Enable Task

★ Message Notifications

★ SMN Topic --Select-- [View](#)  
Only SMN topics whose status is **confirmed** are available.

★ Report Type Weekly

★ Execution Mode Periodically

★ Time 17:00

★ Database All databases

OK
Cancel

**Table 16-2** Parameters for setting a task

| Parameter             | Description                                                                                                                                                                                                                                                                                       | Example Value |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Enable Task           | Status of a scheduled task.<br><ul style="list-style-type: none"> <li>●  : enabled</li> <li>●  : disabled</li> </ul>                                                                                                                                                                              |               |
| Message Notifications | Enables or disables notifications.<br><ul style="list-style-type: none"> <li>●  : enabled</li> <li>●  : disabled</li> </ul>                                                                                                                                                                       |               |
| SMN Topic             | Select an existing topic from the drop-down list or click <b>View Topic</b> and create an SMN topic on the displayed page for configuring the terminals for receiving alarm notifications.<br><br>For details about topics and subscriptions, see <i>Simple Message Notification User Guide</i> . | -             |

| Parameter      | Description                                                                                                                                                       | Example Value |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Report Type    | Type of a report. The options are as follows: <ul style="list-style-type: none"> <li>• <b>Daily</b></li> <li>• <b>Weekly</b></li> <li>• <b>Monthly</b></li> </ul> | Weekly        |
| Execution Mode | Execution mode of the report. The options are as follows: <ul style="list-style-type: none"> <li>• <b>Once</b></li> <li>• <b>Periodically</b></li> </ul>          | Periodically  |
| Time           | Time when the report is executed                                                                                                                                  | 10:00         |
| Database       | Database for which you want to execute the report task                                                                                                            | -             |

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

----End

## Step 2: Previewing and Downloading Audit Reports

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

### NOTICE

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

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

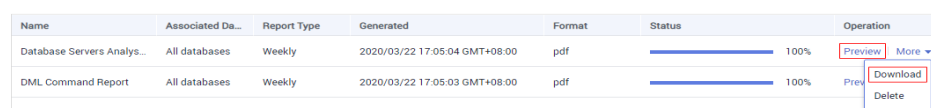
**Step 2** Select a region, click , and choose **Security > Database Security Service**. The **Dashboard** page is displayed.

**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 16-5](#).

**Figure 16-5** 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%   | Pre Download Delete |
| DCL Command Report         | All databases    | Weekly      | 2020/03/22 17:05:03 GMT+08:00 | pdf    | 100%   | Pre Download Delete |

----End

# 17 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).
- You can also enable report notifications to get notified when the reports you subscribed to are generated. For details, see [Viewing Audit Reports](#).

## Prerequisites

You have applied for 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 > Database Security Service**. The **Dashboard** page is displayed.

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

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

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

**Step 6** Set alarm notifications. For details about related parameters, see [Table 17-1](#).

**Figure 17-1** Configuring alarm notifications

The screenshot shows a configuration interface with the following elements:

- Global Settings:**
  - Message Notifications:
  - \* SMN Topic:  [View](#)
  - Only SMN topics whose status is **confirmed** are available.
  - Daily Alarm Notifications:
- Alarm Settings for Risky Operations:**
  - Alarm Risk Severity:  High  Moderate  Low
- Alarm Settings for System Resources:**
  - CPU Alarm Threshold (%):
  - Memory Alarm Threshold (%):
  - Disk Alarm Threshold (%):

An **Apply** button is located at the bottom of the form.

**Table 17-1** Alarm notification parameters

| Parameter                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Example Value |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Message Notifications     | Enables or disables notifications.                                                                                                                                                                                                                                                                                                                                                                                                                                   |               |
| SMN Topic                 | Select an existing topic from the drop-down list or click <b>View Topic</b> and create an SMN topic on the displayed page for configuring the terminals for receiving alarm notifications.<br><b>NOTE</b><br>Before selecting a topic, ensure that the subscription status of the topic is <b>Confirmed</b> . Otherwise, alarm notifications may not be received.<br>For details about topics and subscriptions, see <i>Simple Message Notification User Guide</i> . | -             |
| Daily Alarm Notifications | Total number of alarms allowed to be sent every day<br><b>NOTICE</b> <ul style="list-style-type: none"> <li>If the number of alarms exceeds this value on a day, no more notification will be sent on that day.</li> <li>There is no fixed time point for sending alarm notifications. The system collects statistics every 5 minutes and sends alarm notifications (if any).</li> </ul>                                                                             | 30            |



| Parameter                  | Description                                                                                                                                                                 | Example Value |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Alarm Risk Severity        | Risk severity of the risk log. The options are as follows: <ul style="list-style-type: none"> <li>• <b>High</b></li> <li>• <b>Moderate</b></li> <li>• <b>Low</b></li> </ul> | High          |
| CPU Alarm Threshold (%)    | CPU alarm threshold of an audit instance. When the threshold is exceeded, an alarm notification is generated.                                                               | 80            |
| Memory Alarm Threshold (%) | Memory alarm threshold of an audit instance. When the threshold is exceeded, an alarm notification is generated.                                                            | 80            |
| Disk Alarm Threshold (%)   | Disk alarm threshold of an audit instance. When the threshold is exceeded, an alarm notification is generated.                                                              | 80            |

**Step 7** Click **Apply**.

----End

# 18 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 applied for 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 > Database Security Service**. The **Dashboard** page is displayed.

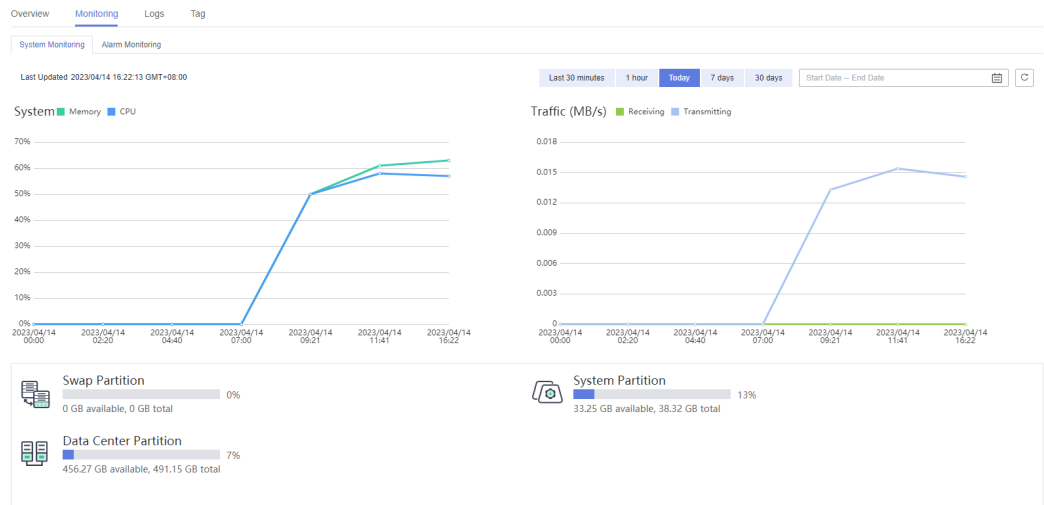
**Step 3** In the navigation tree on the left, choose **Instances**.

**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 18-1](#).

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 18-1** Viewing the system monitoring



----End

# 19 Viewing the Alarms

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

## Prerequisites

- You have applied for 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.

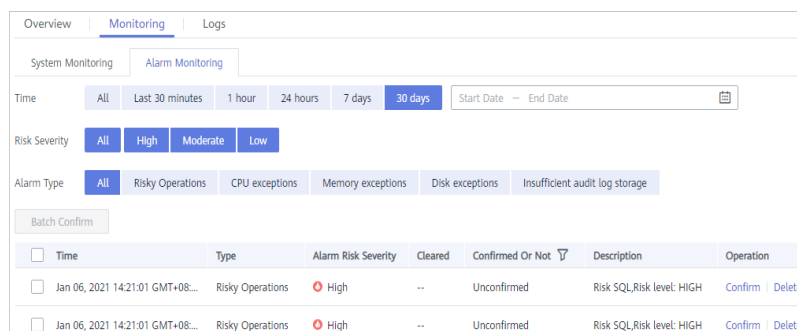
**Step 2** Select a region, click , and choose **Security > Database Security Service**. The **Dashboard** page is displayed.

**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 19-1](#). For details about related parameters, see [Table 19-1](#).

**Figure 19-1** Viewing the alarms




| Time                             | Type             | Alarm Risk Severity | Cleared | Confirmed Or Not | Description               | Operation        |
|----------------------------------|------------------|---------------------|---------|------------------|---------------------------|------------------|
| Jan 06, 2021 14:21:01 GMT+08:... | Risky Operations | High                | --      | Unconfirmed      | Risk SQL_Risk level: HIGH | Confirm   Delete |
| Jan 06, 2021 14:21:01 GMT+08:... | Risky Operations | High                | --      | Unconfirmed      | Risk SQL_Risk level: HIGH | Confirm   Delete |

**Table 19-1** Parameters of alarms

| Parameter           | Description                                                                                                                                                                                                                              |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time                | Time when an alarm occurred.                                                                                                                                                                                                             |
| Type                | Alarm type. The options are as follows: <ul style="list-style-type: none"> <li>• Risky operations</li> <li>• CPU exceptions</li> <li>• Memory exceptions</li> <li>• Disk exceptions</li> <li>• Insufficient audit log storage</li> </ul> |
| Alarm Risk Severity | Risk severity of an alarm. The options are as follows: <ul style="list-style-type: none"> <li>• <b>High</b></li> <li>• <b>Moderate</b></li> <li>• <b>Low</b></li> </ul>                                                                  |
| Cleared             | Time when an alarm is cleared                                                                                                                                                                                                            |
| Confirmed Or Not    | Confirmation status of an alarm. Click  to filter alarms in <b>Unconfirmed</b> or <b>Confirmed</b> 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**, and click  to view alarms of the specified time range.
- Select **All, High, Moderate, or Low** for **Risk Severity**. Alarms of specified severity are displayed in the list.
- Select an alarm type, and alarms of specified alarm type is displayed in the list.

----End

## Follow-Up Procedure

To confirm an alarm, click **Confirm** in the **Operation** column of the alarm.

**Figure 19-2** Confirming an alarm

| <input type="checkbox"/> | Time                  | Type           | Alarm Risk Severity                                                                      | Cleared               | Confirmed O...  | Description      | Operation                                                                  |
|--------------------------|-----------------------|----------------|------------------------------------------------------------------------------------------|-----------------------|------------------------------------------------------------------------------------------------------|------------------|----------------------------------------------------------------------------|
| <input type="checkbox"/> | 2020/04/04 00:55:0... | CPU exceptions |  High | 2020/04/04 01:00:0... | Unconfirmed                                                                                          | CPU USAGE 100.0% | <span style="border: 1px solid red; padding: 2px;">Confirm</span>   Delete |
| <input type="checkbox"/> | 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.

# 20 Managing Database Audit Instances

---

After applying for a database audit instance, you can view, enable, restart, disable, or delete the instance.


## Prerequisites

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

## Deleting an Instance

You can delete a database audit instance that is no longer needed. You can also delete the associated EIP at the same time.

**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  and choose **Security > Database Security Service**. The **Dashboard** page is displayed.

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


**Step 5** In the row containing the desired instance, choose **More > Delete** in the **Operation** column.

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

----End

## Viewing the Instance

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

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

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

**Step 4** View the database audit instances information. For details about related parameters, see [Table 20-1](#).

**Figure 20-1** Viewing database audit instances

 **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 20-1** Parameters

| Parameter                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Instance Name/ID                      | Name and ID of an instance. Instance ID is automatically generated.                                                                                                                                                                                                                                                                                                                                                                                                |
| Specifications                        | Edition of an instance                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Status                                | Running status of an instance. The options are as follows: <ul style="list-style-type: none"> <li>• <b>Running</b></li> <li>• <b>Creating</b></li> <li>• <b>Faulty</b></li> <li>• <b>Disabled</b></li> <li>• <b>Frozen</b></li> <li>• <b>Frozen for legal management</b></li> <li>• <b>Frozen due to abuse</b></li> <li>• <b>Frozen due to lack of identity verification</b></li> <li>• <b>Frozen for partnership</b></li> <li>• <b>Creation failed</b></li> </ul> |
| Associated Databases/ Total Databases | Number of databases an instance has associated with and Number of databases an instance supports                                                                                                                                                                                                                                                                                                                                                                   |
| Operation                             | Operations can be performed on the instance. The options are as follows: <ul style="list-style-type: none"> <li>• Configure Rules</li> <li>• Enable</li> <li>• Disable</li> <li>• Restart</li> <li>• View Details</li> <li>• Delete</li> </ul>                                                                                                                                                                                                                     |



 **NOTE**

You can perform the following operations on instances as required:

- Restart  
Locate the row that contains the desired instance, choose **More > Restart** in the **Operation** column, and click **OK** in the displayed dialog box.
- Enable  
Locate the row that contains the desired instance, choose **More > Enable** in the **Operation** column, and click **OK** in the displayed dialog box.
- Disable  
Locate the row that contains the desired instance, choose **More > Disable** in the **Operation** column, and click **OK** in the displayed dialog box. When an instance is disabled, the audit function is disabled for the databases on the instance.
- Delete  
Locate the row that contains the instance that failed to be created, choose **More > Delete** in the **Operation** column, and click **Delete** in the displayed dialog box. Deleted instances will not be displayed in the instance list.
- View Details  
Locate the row that contains the instance that failed to be created, choose **More > View Details** in the **Operation** column. In the dialog box that is displayed, view the instance creation failure details.

----End


# 21 Viewing the Instance Overview

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

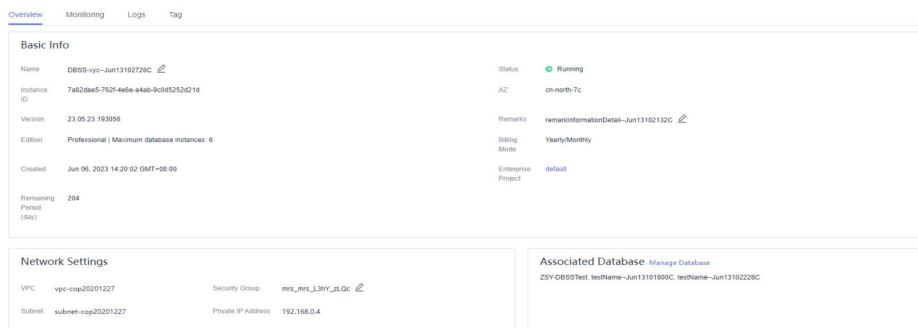
## Prerequisites

You have applied for 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 > 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 21-1](#). For details about related parameters, see [Table 21-1](#).

**Figure 21-1** Viewing the instance overview



**Table 21-1** Parameters of the instance overview

| Category           | Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic Info         | Name             | Instance name. You can click  next to <b>Name</b> to change it.                                                                                                                                                                                                                                                                                                                 |
|                    | Status           | Running status of an instance. The options are as follows: <ul style="list-style-type: none"> <li>• <b>Running</b></li> <li>• <b>Creating</b></li> <li>• <b>Faulty</b></li> <li>• <b>Disabled</b></li> <li>• <b>Frozen</b></li> <li>• <b>Frozen for legal management</b></li> <li>• <b>Frozen due to abuse</b></li> <li>• <b>Frozen due to lack of identity verification</b></li> <li>• <b>Frozen for partnership</b></li> <li>• <b>Creation failed</b></li> </ul> |
|                    | ID               | Instance ID, which is automatically generated                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                    | AZ               | Availability Zone (AZ) where an instance resides                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                    | Version          | Version of the DBSS instance when you create the DBSS instance. The version of the DBSS instance created at different time may be different.<br>Impact scope of DBSS instance versions: <ul style="list-style-type: none"> <li>• Supported database types</li> <li>• Supported database versions</li> </ul>                                                                                                                                                        |
|                    | Remarks          | Remarks about an instance. You can click  next to <b>Remarks</b> to modify it.                                                                                                                                                                                                                                                                                                |
|                    | Edition          | Edition of an instance                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                    | Created          | Time when an instance is created                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                    | Network Settings | VPC                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Security Group     |                  | Security group where an instance resides                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Subnet             |                  | Subnet where an instance resides                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Private IP Address |                  | IP address of an instance                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Category            | Parameter | Description                                                                                                                    |
|---------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------|
| Associated Database | -         | Database information associated with an instance<br>Click <b>Manage Database</b> , and the <b>Databases</b> page is displayed. |

----End

# 22 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 applied for 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 > Database Security Service**. The **Dashboard** page is displayed.

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

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

**Step 5** View the database information. For details about related parameters, see [Table 22-1](#).

**Figure 22-1** Viewing the database and agent information

| No. | Database Information                      | Character Set | IP Address/...       | Instance | OS      | Audit Status | Agent | Operation        |
|-----|-------------------------------------------|---------------|----------------------|----------|---------|--------------|-------|------------------|
| 1   | Name: db05<br>Type: MYSQL<br>Version: 5.7 | UTF8          | 192.168.0.73<br>3306 | --       | LINUX64 | Enabled      | Add   | Disable   Delete |

| Agent ID             | Install... | Install... | OS         | Audite... | CPU ... | Mem... | Gen... | Status  | Operation             |
|----------------------|------------|------------|------------|-----------|---------|--------|--------|---------|-----------------------|
| AXEQcF-WiHueH60XdgGx | Database   | 192.168... | Linux 6... | --        | 80      | 80     | No     | Running | 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 22-1** 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                                                                                                                              | 192.168.0.10<br>4<br>3306 |
| Instance             | Database instance name                                                                                                                                  | -                         |
| OS                   | Operating system of the database                                                                                                                        | LINUX64                   |
| Audit Status         | Audit status of the database. The options are as follows: <ul style="list-style-type: none"> <li>• <b>Enabled</b></li> <li>• <b>Disabled</b></li> </ul> | Enabled                   |
| Agent                | Click <b>Add</b> to add an agent for the database.                                                                                                      | Add an agent.             |

 **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.

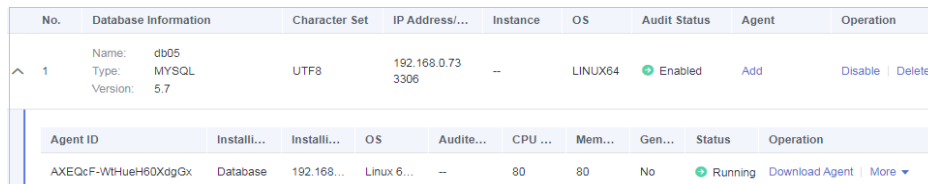
**Step 2** Select a region, click , and choose **Security > Database Security Service**. The **Dashboard** page is displayed.

**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 22-2](#). For details about related parameters, see [Table 22-2](#).

**Figure 22-2** Viewing the database and agent information



| No. | Database Information                      | Character Set | IP Address/...       | Instance | OS      | Audit Status | Agent | Operation        |
|-----|-------------------------------------------|---------------|----------------------|----------|---------|--------------|-------|------------------|
| 1   | Name: db05<br>Type: MYSQL<br>Version: 5.7 | UTF8          | 192.168.0.73<br>3306 | --       | LINUX64 | Enabled      | Add   | Disable   Delete |

| Agent ID            | Installi... | Installi... | OS         | Audite... | CPU ... | Mem... | Gen... | Status  | Operation             |
|---------------------|-------------|-------------|------------|-----------|---------|--------|--------|---------|-----------------------|
| AXEQcF-WHueH60XdgGx | Database    | 192.168...  | Linux 6... | --        | 80      | 80     | No     | Running | Download Agent   More |

**Table 22-2** 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 <b>Database</b> and <b>Application</b> .                                                                                                                                                              |
| 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 <b>80</b> .<br><b>NOTE</b><br>The agent on a node will stop working if the CPU usage of the node exceeds this threshold. You can scale up CPU resources to avoid this problem.          |
| Memory Threshold (%)       | Memory threshold of the installing node. The default value is <b>80</b> .<br><b>NOTE</b><br>The agent on a node will stop working if the memory usage of the node exceeds this threshold. You can scale up memory resources to avoid this problem. |
| General                    | Whether an agent is a general-purpose agent.                                                                                                                                                                                                       |
| 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



# 23 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

# 24 Management an Audit Scope

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

## Prerequisites

- You have applied for 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.

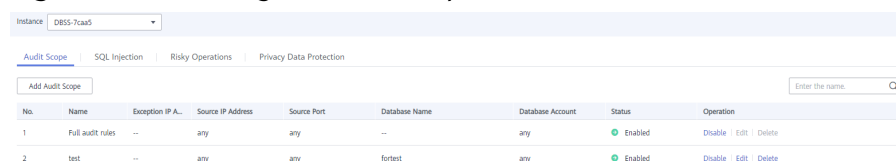
**Step 2** Select a region, click , and choose **Security > Database Security Service**. The **Dashboard** page is displayed.

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

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

**Step 5** View the audit scope information. For details about related parameters, see [Table 24-1](#).

**Figure 24-1** Viewing the audit scope



| 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         | testdb        | any              | Enabled | Disable   Edit   Delete |

 **NOTE**

Enter the key word of an audit scope to search.

**Table 24-1** 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: <ul style="list-style-type: none"> <li>• <b>Enabled</b></li> <li>• <b>Disabled</b></li> </ul> |

 **NOTE**

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

- **Enable**  
Locate the row that contains the audit scope to be enabled, and click **Enable** in the **Operation** column. Databases within the scope will be audited.
- **Edit (supported in customized audit scopes only)**  
Locate the row that contains the audit scope to be edited, click **Edit** in the **Operation** column, and modify the scope in the displayed dialog box.
- **Disable**  
Locate the row that contains the audit scope to be disabled, click **Disable** in the **Operation** column, and click **OK** in the displayed dialog box. When the audit scope is disabled, the audit scope rule will not be executed in the audit.
- **Delete (supported in customized audit scopes only)**  
Locate the row that contains the audit scope to be deleted, click **Delete** in the **Operation** column, and click **OK** in the displayed dialog box. You need to add the audit scope again if it is deleted and you want to audit it.

----End

# 25 Viewing Information About SQL Injection Detection

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

## Prerequisites

- You have applied for 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 > Database Security Service**. The **Dashboard** page is displayed.

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

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

**Step 5** View information about SQL injection detection, as shown in [Figure 25-1](#). For details about related parameters, see [Table 25-1](#).

**Figure 25-1** Viewing information about the SQL injection detection

| No. | Name                            | Command Feature    | Risk Severity | Status  | Operation                                                                                        |
|-----|---------------------------------|--------------------|---------------|---------|--------------------------------------------------------------------------------------------------|
| 1   | Identify SQL injection 2        | Regular expression | High          | Enabled | <a href="#">Set Priority</a> <a href="#">Disable</a> <a href="#">Edit</a> <a href="#">Delete</a> |
| 2   | MYSQL error type SQL injection  | Regular expression | High          | Enabled | <a href="#">Set Priority</a> <a href="#">Disable</a> <a href="#">Edit</a> <a href="#">Delete</a> |
| 3   | HAWND error type SQL injection  | Regular expression | Moderate      | Enabled | <a href="#">Set Priority</a> <a href="#">Disable</a> <a href="#">Edit</a> <a href="#">Delete</a> |
| 4   | UNION joint query SQL injection | Regular expression | Moderate      | Enabled | <a href="#">Set Priority</a> <a href="#">Disable</a> <a href="#">Edit</a> <a href="#">Delete</a> |
| 5   | Time SQL injection              | Regular expression | Moderate      | Enabled | <a href="#">Set Priority</a> <a href="#">Disable</a> <a href="#">Edit</a> <a href="#">Delete</a> |
| 6   | Identify SQL injection 1        | Regular expression | High          | Enabled | <a href="#">Set Priority</a> <a href="#">Disable</a> <a href="#">Edit</a> <a href="#">Delete</a> |
| 7   | Boolean SQL injection           | Regular expression | High          | Enabled | <a href="#">Set Priority</a> <a href="#">Disable</a> <a href="#">Edit</a> <a href="#">Delete</a> |

### 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.
- Click **Set Priority** in the **Operation** column of an SQL injection rule to change its priority.

**Table 25-1** Parameters

| Parameter       | Description                                                                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name            | Name of the SQL injection detection                                                                                                                                                                           |
| Command Feature | Command features of the SQL injection detection                                                                                                                                                               |
| Risk Severity   | Risk level of the SQL injection detection. The options are as follows: <ul style="list-style-type: none"><li>• <b>High</b></li><li>• <b>Moderate</b></li><li>• <b>Low</b></li><li>• <b>No risks</b></li></ul> |
| Status          | Status of the SQL injection detection. The options are as follows: <ul style="list-style-type: none"><li>• <b>Enabled</b></li><li>• <b>Disabled</b></li></ul>                                                 |
| Operation       | Operations on an SQL injection rule. The options are as follows: <ul style="list-style-type: none"><li>• <b>Set Priority</b></li><li>• <b>Disable</b></li><li>• <b>Edit</b></li><li>• <b>Delete</b></li></ul> |

----End

# 26 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 applied for 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 > 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 26-1](#).

**Figure 26-1** 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 > Database Security Service**. The **Dashboard** page is displayed.
- Step 3** In the navigation tree, choose **Rules**.
- Step 4** In the **Instance** drop-down list, select an instance to view risky operations.
- Step 5** Click the **Risky Operations** tab.
- Step 6** View the risky operation information. For details about related parameters, see [Table 26-1](#).

**Figure 26-2** Viewing risky operations

| No. | Name  | Category | Feature              | Risk Severity | Status  | Operation                              |
|-----|-------|----------|----------------------|---------------|---------|----------------------------------------|
| 1   | sdffd | --       | 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 26-1** 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: <ul style="list-style-type: none"> <li>• <b>High</b></li> <li>• <b>Moderate</b></li> <li>• <b>Low</b></li> <li>• <b>No risks</b></li> </ul> |
| Status        | Status of the risky operation. The options are as follows: <ul style="list-style-type: none"> <li>• <b>Enabled</b></li> <li>• <b>Disabled</b></li> </ul>                                                      |



 **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**

# 27 Managing Privacy Data Protection Rules

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

## Prerequisites

You have applied for 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 > Database Security Service**. The **Dashboard** page is displayed.

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

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

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


### NOTE

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

**Step 6** View the rules. For details about related parameters, see [Table 27-1](#).


### 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 27-1** Masking rule information

| 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 27-1** Masking rule parameters

| Parameter          | Description                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Rule Name          | Rule name                                                                                                                         |
| Rule Type          | Rule type. <ul style="list-style-type: none"> <li>• Default</li> <li>• User-defined</li> </ul>                                    |
| 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: <ul style="list-style-type: none"> <li>• <b>Enabled</b></li> <li>• <b>Disabled</b></li> </ul> |

**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

# 28 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 applied for a database audit instance and the **Status** is **Running**.
- Database audit has been enabled.
- Audit reports have been generated.

## Viewing a Report

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

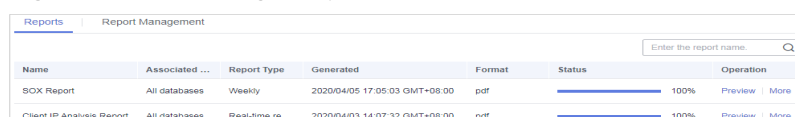
**Step 2** Select a region, click , and choose **Security > Database Security Service**. The **Dashboard** page is displayed.

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

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

**Step 5** Viewing reports

**Figure 28-1** 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    | <div style="width: 100%;"><div style="width: 100%;"></div></div> 100% | Preview   More ▾ |
| Client IP Analysis Report | All databases  | Real-time re... | 2020/04/03 14:07:32 GMT+08:00 | pdf    | <div style="width: 100%;"><div style="width: 100%;"></div></div> 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 > 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 28-2](#).

**Figure 28-2** 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

# 29 Managing Backup Audit Logs

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

## Prerequisites

- You have applied for 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 > Database Security Service**. The **Dashboard** page is displayed.

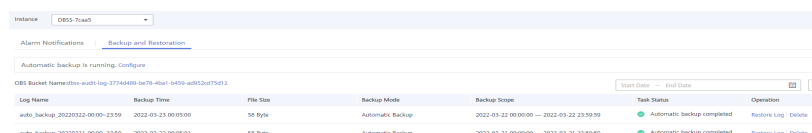
**Step 3** In the navigation tree on the left, choose **Settings**.

**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 29-1](#). For details about related parameters, see [Table 29-1](#).

**Figure 29-1** Viewing backup audit logs



| Log Name                         | Backup Time         | File Size | Backup Mode      | Backup Scope                              | Task Status                | Operation            |
|----------------------------------|---------------------|-----------|------------------|-------------------------------------------|----------------------------|----------------------|
| auto_backup_20220322-00:00-23:59 | 2022-03-22 00:00:00 | 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 00:00:00 | 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 29-1** 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**


# 30 Viewing Operation Logs

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



## Prerequisites

You have applied for 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 > 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 30-1](#). For details about related parameters, see [Table 30-1](#).

**Figure 30-1** Viewing operation logs

| <span>Last 30 minutes</span> <span>1 hour</span> <span>24 hours</span> <span>7 days</span> <span style="background-color: #007bff; color: white;">30 days</span> <span style="float: right;">Start Date — End Date  </span> |                               |                           |        |                  |                          |                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|---------------------------|--------|------------------|--------------------------|-------------------------------------------------|
| Username                                                                                                                                                                                                                                                                                                                                                                                              | Time                          | Function                  | Action | Operation Object | Description              | Result                                          |
| security_dbss_000485...                                                                                                                                                                                                                                                                                                                                                                               | 2020/04/03 14:16:00 GMT+08:00 | Rules -> Risky Operation  | create | sdfdd            | Add user's risk rule     | <span style="color: green;">✔</span> Successful |
| security_dbss_000485...                                                                                                                                                                                                                                                                                                                                                                               | 2020/04/02 20:06:36 GMT+08:00 | Rules -> Sensitive Dat... | create | d                | Add sensitive data ma... | <span style="color: green;">✔</span> 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 30-1** Parameters

| <b>Parameter</b> | <b>Description</b>                    |
|------------------|---------------------------------------|
| Username         | User who performs the operation       |
| Time             | Time when the operation was performed |
| Function         | Function of the operation             |
| Action           | Action of the operation               |
| Operation Object | Object of the operation               |
| Description      | Description of the operation          |
| Result           | Result of the operation               |

----End

# 31 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** Choose **Trace List** in the navigation pane.

**Step 3** 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 4** Click **Query**.

**Step 5** Click  on the left of a trace to expand its details.

**Figure 31-1** Expanding trace details

| Trace Name    | Resource ... | Trace Sou... | Resource ID... | Resource Name... | Trace Status | Operator | Operation Time                   | Operation                  |
|---------------|--------------|--------------|----------------|------------------|--------------|----------|----------------------------------|----------------------------|
| cloudServi... | dbss         | DBSS         | --             | --               | normal       |          | Feb 28, 2020 16:34:07 GMT+08:... | <a href="#">View Trace</a> |

|                      |                                                                                                                                |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <b>request</b>       | /dbss/v1/charge/24dbd82a29eb430bb6cccd0c0c6538a9/audit/period/order                                                            |
| <b>code</b>          | 200                                                                                                                            |
| <b>source_ip</b>     |                                                                                                                                |
| <b>trace_type</b>    | ConsoleAction                                                                                                                  |
| <b>event_type</b>    | system                                                                                                                         |
| <b>project_id</b>    | 24dbd82a29eb430bb6cccd0c0c6538a9                                                                                               |
| <b>trace_id</b>      | 15f92fea-5a05-11ea-be78-874d5768700f                                                                                           |
| <b>trace_name</b>    | cloudServiceInstanceCreate                                                                                                     |
| <b>resource_type</b> | dbss                                                                                                                           |
| <b>trace_rating</b>  | normal                                                                                                                         |
| <b>api_version</b>   | v1.10.0                                                                                                                        |
| <b>service_type</b>  | DBSS                                                                                                                           |
| <b>tracker_name</b>  | system                                                                                                                         |
| <b>time</b>          | Feb 28, 2020 16:34:07 GMT+08:00                                                                                                |
| <b>record_time</b>   | Feb 28, 2020 16:34:07 GMT+08:00                                                                                                |
| <b>user</b>          | {"name": "...", "id": "cef7561e56f44d21a1ad8771e27b7dcc", "domain": {"name": "...", "id": "ce28abd4fdd44e09a34c78709b413689"}} |

**Step 6** Click **View Trace** in the **Operation** column. On the displayed **View Trace** dialog box shown in **Figure 31-2**, the trace structure details are displayed.

**Figure 31-2** Viewing a trace

View Trace
✕

```

{
  "project_id": "24dbd82a29eb430bb6cccd0c0c6538a9",
  "context": {
    "request": "/dbss/v1/charge/24dbd82a29eb430bb6cccd0c0c6538a9/audit/period/order",
    "code": "200",
    "source_ip": "...",
    "trace_type": "ConsoleAction",
    "event_type": "system",
    "project_id": "24dbd82a29eb430bb6cccd0c0c6538a9",
    "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": "...",
      "id": "cef7561e56f44d21a1ad8771e27b7dcc",
      "domain": {
        "name": "...",
        "id": "ce28abd4fdd44e09a34c78709b413689"
      }
    }
  }
}

```

Close

----End

# 32 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 32-1** lists DBSS operations recorded by CTS.

**Table 32-1** 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 |

# 33 FAQs

## 33.1 Product Consulting

### 33.1.1 What Is Database Audit?

Database audit is deployed in out-of-path mode. It records user access to the database in real time, generates fine-grained audit reports, sends real-time alarms for risky operations and attack behaviors. In addition, database audit generates compliance reports that meet data security standards (such as Sarbanes-Oxley) to locate internal violations and improper operations, thus ensuring data asset security.

### 33.1.2 What Are the Differences Between DBSS Database Audit and RDS SQL Audit?

The following table describes the differences between DBSS database audit and RDS SQL audit regarding their functions and applicable scope.

**Table 33-1** Audit service differences

| Audit         | Function                                                                                                                                                                                                                              | Scenario                                                         |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| RDS SQL audit | Only SQL access operations are recorded.                                                                                                                                                                                              | Edit only RDS databases.                                         |
| DBSS audit    | All the unsafe operations on the database are audited. DBSS records SQL access, performs security scans and statistical analysis, identifies risks, and generates reports to help you enhance the security of databases on the cloud. | Edit all the database scenarios, including user-built databases. |

### 33.1.3 What Editions Does DBSS Provide?

Database audit provides basic, professional, and advanced editions for you to choose from.

**Table 33-2** describes the database audit editions.

**Table 33-2** Database audit editions

| Version      | Maximum Databases | System Resource                                                                                                   | Performance                                                                                                                                                                                                                                              |
|--------------|-------------------|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic        | 3                 | <ul style="list-style-type: none"> <li>• CPU: 4 vCPUs</li> <li>• Memory: 16 GB</li> <li>• Disk: 500 GB</li> </ul> | <ul style="list-style-type: none"> <li>• Peak QPS: 3,000 queries/second</li> <li>• Database load rate: 3.6 million statements/hour</li> <li>• Stores 400 million online SQL statements.</li> <li>• Stores 5 billion archived SQL statements.</li> </ul>  |
| Professional | 6                 | <ul style="list-style-type: none"> <li>• CPU: 8 vCPUs</li> <li>• Memory: 32 GB</li> <li>• Disk: 1 TB</li> </ul>   | <ul style="list-style-type: none"> <li>• Peak QPS: 6,000 queries/second</li> <li>• Database load rate: 7.2 million statements/hour</li> <li>• Stores 600 million online SQL statements.</li> <li>• Stores 10 billion archived SQL statements.</li> </ul> |

### 33.1.4 What Databases Does DBSS Protect?

DBSS protects databases built on Elastic Cloud Server (ECS) and Bare Metal Server (BMS), and RDS instances within the same VPC and its subnets. Due to network restrictions, DBSS cannot protect databases built and RDS instances on ECSs and BMSs if they are not in the same VPC and its subnets.

### 33.1.5 What Databases Does DBSS Support?

DBSS supports the following databases on the management console:

- Relational Database Service (RDS)
- Databases built on ECS
- Databases built on BMS

### 33.1.6 Why Can't I See the Instance that Is Being Created After I Applied for It?

When you apply for a set of DBSS instances, a system disk will be created on the virtual machine (VM) where the instances reside. In addition, the network will be configured. The creation and configuration may take some time. Therefore, the instances are not immediately displayed.

## 33.2 Functions

### 33.2.1 Does Database Audit (in Bypass Mode) Affect My Services?

No. Your databases are audited in out-of-path mode. Database audit neither affects your services nor conflicts with local audit tools.

### 33.2.2 What Are the Functions of Database Audit?

Database audit is deployed in out-of-path pattern. You can perform flexible audit on databases built on ECS, BMS, and RDS without affecting services. Database audit provides the following functions:

- Monitors database login, operation type (data definition, operation, and control), and operation object based on risky operations to effectively audit the database.
- Analyzes risks, sessions, and SQL injection to help you learn the database situation in a timely manner.
- Provides a report template library to generate daily, weekly, or monthly audit reports according to your configurations. Sends real-time alarm notifications to help you obtain audit reports in a timely manner.

### 33.2.3 Supported Database Types

Database audit supports the following database types and versions.

**Table 33-3** Database types and versions supported by database audit

| Database Type | Edition                                                                                                                                                                             |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MySQL         | <ul style="list-style-type: none"><li>• 5.0, 5.1, 5.5, 5.6, 5.7</li><li>• 8.0 (8.0.11 and earlier)</li><li>• 8.0.23</li></ul>                                                       |
| Oracle        | <ul style="list-style-type: none"><li>• 11g<br/>11.1.0.6.0, 11.2.0.1.0, 11.2.0.2.0,<br/>11.2.0.3.0, and 11.2.0.4.0</li><li>• 12c<br/>12.1.0.2.0, 12.2.0.1.0</li><li>• 19c</li></ul> |

| Database Type     | Edition                                                                                                                                                                                                                                                        |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PostgreSQL        | <ul style="list-style-type: none"> <li>• 7.4</li> <li>• 8.0<br/>8.0, 8.1, 8.2, 8.3, 8.4</li> <li>• 9.0<br/>9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6</li> <li>• 10.0<br/>10.0, 10.1, 10.2, 10.3, 10.4, 10.5</li> <li>• 11.0</li> <li>• 12.0</li> <li>• 13.0</li> </ul> |
| SQL Server        | <ul style="list-style-type: none"> <li>• 2008, 2008R2</li> <li>• 2012</li> <li>• 2014</li> <li>• 2016</li> <li>• 2017</li> </ul>                                                                                                                               |
| DWS               | <ul style="list-style-type: none"> <li>• 1.5</li> </ul>                                                                                                                                                                                                        |
| SHENTONG          | V7.0                                                                                                                                                                                                                                                           |
| GBase 8a          | V8.5                                                                                                                                                                                                                                                           |
| GBase 8s          | V8.8                                                                                                                                                                                                                                                           |
| Gbase XDM Cluster | V8.0                                                                                                                                                                                                                                                           |
| TAURUS            | MySQL 8.0                                                                                                                                                                                                                                                      |

### 33.2.4 What OSs Can I Install the Database Audit Agent On?

To use database audit, you need to install its agent on the required database, application, or proxy side, and then connect to the database audit instance.

The database audit agent can run on 64-bit Linux or 64-bit Windows. The following table describes the supported OSs.

- For more information, see [Table 33-4](#).



**Table 33-4** Supported Linux OS versions

| System Name  | System version                                                                                                                                                                                                                                                                                                         |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CentOS       | <ul style="list-style-type: none"> <li>• CentOS 7.0 (64bit)</li> <li>• CentOS 7.1 (64bit)</li> <li>• CentOS 7.2 (64bit)</li> <li>• CentOS 7.3 (64bit)</li> <li>• CentOS 7.4 (64bit)</li> <li>• CentOS 7.5 (64bit)</li> <li>• CentOS 7.6 (64bit)</li> <li>• CentOS 7.8 (64bit)</li> <li>• CentOS 8.0 (64bit)</li> </ul> |
| Debian       | <ul style="list-style-type: none"> <li>• Debian 7.5.0 (64bit)</li> <li>• Debian 8.2.0 (64bit)</li> <li>• Debian 8.8.0 (64bit)</li> <li>• Debian 9.0.0 (64bit)</li> </ul>                                                                                                                                               |
| Fedora       | <ul style="list-style-type: none"> <li>• Fedora 24 (64bit)</li> <li>• Fedora 25 (64bit)</li> </ul>                                                                                                                                                                                                                     |
| SUSE         | <ul style="list-style-type: none"> <li>• SUSE 11 SP4 (64bit)</li> <li>• SUSE 12 SP1 (64bit)</li> <li>• SUSE 12 SP2 (64bit)</li> </ul>                                                                                                                                                                                  |
| Ubuntu       | <ul style="list-style-type: none"> <li>• Ubuntu 14.04 (64bit)</li> <li>• Ubuntu 16.04 (64bit)</li> <li>• Ubuntu 18.04 (64bit)</li> <li>• Ubuntu 20.04 (64-bit)</li> </ul>                                                                                                                                              |
| EulerOS      | <ul style="list-style-type: none"> <li>• Euler 2.2 (64bit)</li> <li>• Euler 2.3 (64bit)</li> </ul>                                                                                                                                                                                                                     |
| Oracle Linux | <ul style="list-style-type: none"> <li>• Oracle Linux 6.9 (64bit)</li> <li>• Oracle Linux 7.4 (64bit)</li> </ul>                                                                                                                                                                                                       |

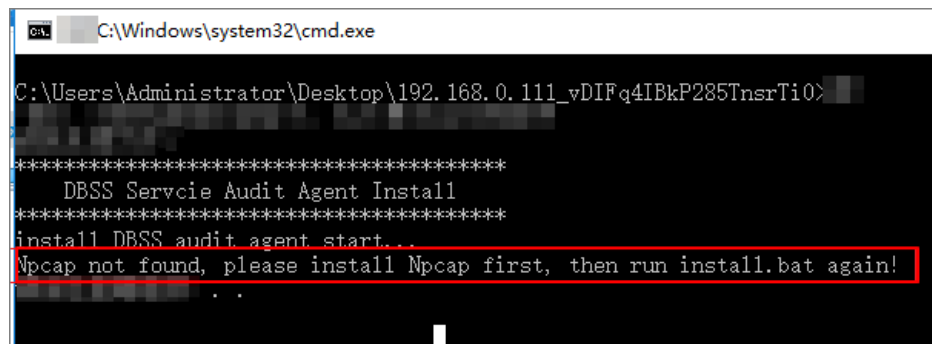
- The following Windows OSs are supported:
  - Windows Server 2008 R2 (64bit)
  - Windows Server 2012 R2 (64bit)
  - Windows Server 2016 (64bit)
  - Windows 7 (64bit)
  - Windows 10 (64bit)

**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 33-1** Npcap not found



### 33.2.5 Does Database Audit Support Bidirectional Audit?

Yes. In bidirectional audit, both requests and responses to the database are audited.

Bidirectional audit is used for database audit by default.

### 33.2.6 Can I Audit Databases Across Different VPCs?

Yes. To audit databases in different VPCs, ensure the VPCs can communicate with each other. You can create peering connections between the VPCs. For details, see .

### 33.2.7 Can Applications Using TLS Connections Be Audited?

No. Applications using TLS are encrypted.

### 33.2.8 How Long Is the Database Audit Data Stored by Default?

Database audit can store online and archived audit data for at least 180 days.

On the **Dashboard** of database audit, you can select the database and audit period to view audit data.

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, apply for the basic edition.
  - To audit a large volume of data, apply for the professional or advanced edition.

For more information, see [Table 33-5](#).

- Back up audit logs.

**Table 33-5** Database audit editions

| Version      | Maximum Databases | System Resource                                                                                                   | Performance                                                                                                                                                                                                                                              |
|--------------|-------------------|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic        | 3                 | <ul style="list-style-type: none"> <li>• CPU: 4 vCPUs</li> <li>• Memory: 16 GB</li> <li>• Disk: 500 GB</li> </ul> | <ul style="list-style-type: none"> <li>• Peak QPS: 3,000 queries/second</li> <li>• Database load rate: 3.6 million statements/hour</li> <li>• Stores 400 million online SQL statements.</li> <li>• Stores 5 billion archived SQL statements.</li> </ul>  |
| Professional | 6                 | <ul style="list-style-type: none"> <li>• CPU: 8 vCPUs</li> <li>• Memory: 32 GB</li> <li>• Disk: 1 TB</li> </ul>   | <ul style="list-style-type: none"> <li>• Peak QPS: 6,000 queries/second</li> <li>• Database load rate: 7.2 million statements/hour</li> <li>• Stores 600 million online SQL statements.</li> <li>• Stores 10 billion archived SQL statements.</li> </ul> |

 **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<sub>1</sub> and IP<sub>2</sub>. IP<sub>1</sub> has a database port. IP<sub>2</sub> has three database ports. IP<sub>1</sub> and IP<sub>2</sub> 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 apply for a new one.
- Online SQL statements are counted based on the assumption that the capacity of an SQL statement is 1 KB.

### 33.2.9 How Soon Can I Receive an Alarm Notification If an Exception Occurs in Database Audit?

When database audit is running properly, if an exception occurs, you will receive an alarm notification within 5 minutes.

If you set alarm notifications, when database audit is running properly, the system generates an alarm notification when a metric of a database audit instance resource (CPU, memory, or disk) exceeds the alarm threshold. You can receive the notification within about 5 minutes.

### **33.2.10 Is the Total Number Of Alarms Every Day the Same as that of Emails?**

Yes. One alarm message corresponds to one email notification.

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

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

### **33.2.12 If I Use Middleware at the Service Side, Will It Affect Database Audit?**

No.

Middleware is a type of software deployed between applications and software including OSs, networks, and databases. Middleware provides an environment for application operation and development, helping users flexibly and efficiently develop and integrate complex application software.

Database audit is deployed in out-of-path mode. The database audit agent (installed on database or application nodes) obtains database access traffic, uploads the traffic to the audit system, receives commands issued by the audit system, and reports database status.

Using middleware on the service side does not affect the agent during SQL listening or auditing.

If database audit cannot obtain any data, troubleshoot the problem by referring to:

### **33.2.13 What Should I Do If an Alarm of Insufficient DBSS Capacity Is Displayed?**

The disk capacity of an existing DBSS instance cannot be expanded. If you find your disk space insufficient to store logs for at least 180 days, as required by compliance standards, you need to back up the logs.

This alarm indicates that the disk usage of your instances is high. You are advised to back up data every hour. If you have enabled backup, ignore this alarm.

## **33.3 Agent**

### **33.3.1 Which Functions Do the Database Audit Agent Provide?**

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

The database audit agent delivers the following functions:

- Obtain database access traffic

- Upload traffic data to the audit system
- Receive configuration commands from the audit system
- Report database status monitoring data

### 33.3.2 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:

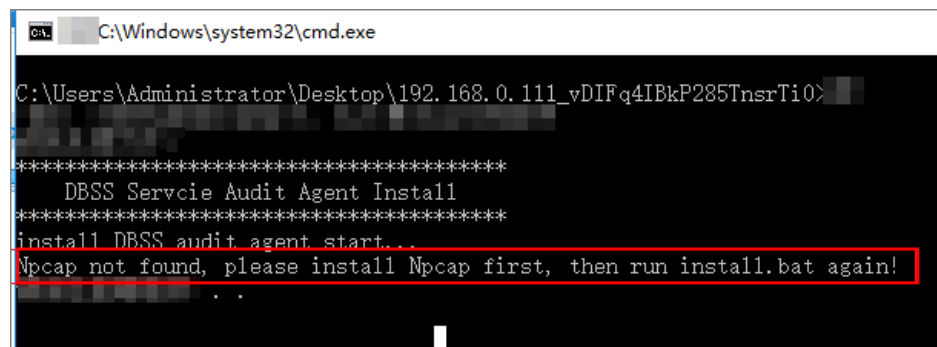
- Windows Server 2008 R2 (64bit)
- Windows Server 2012 R2 (64bit)
- Windows Server 2016 (64bit)
- Windows 7 (64bit)
- Windows 10 (64bit)

 **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 33-2** Npcap not found



### 33.3.3 On What Linux OSs Can I Install the Agent?

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

The database audit agent can be installed on a 64-bit Linux OS. [Table 33-6](#) provides more details.

**Table 33-6** Supported Linux OS versions

| System Name  | System version                                                                                                                                                                                                                                                                                                         |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CentOS       | <ul style="list-style-type: none"> <li>● CentOS 7.0 (64bit)</li> <li>● CentOS 7.1 (64bit)</li> <li>● CentOS 7.2 (64bit)</li> <li>● CentOS 7.3 (64bit)</li> <li>● CentOS 7.4 (64bit)</li> <li>● CentOS 7.5 (64bit)</li> <li>● CentOS 7.6 (64bit)</li> <li>● CentOS 7.8 (64bit)</li> <li>● CentOS 8.0 (64bit)</li> </ul> |
| Debian       | <ul style="list-style-type: none"> <li>● Debian 7.5.0 (64bit)</li> <li>● Debian 8.2.0 (64bit)</li> <li>● Debian 8.8.0 (64bit)</li> <li>● Debian 9.0.0 (64bit)</li> </ul>                                                                                                                                               |
| Fedora       | <ul style="list-style-type: none"> <li>● Fedora 24 (64bit)</li> <li>● Fedora 25 (64bit)</li> </ul>                                                                                                                                                                                                                     |
| SUSE         | <ul style="list-style-type: none"> <li>● SUSE 11 SP4 (64bit)</li> <li>● SUSE 12 SP1 (64bit)</li> <li>● SUSE 12 SP2 (64bit)</li> </ul>                                                                                                                                                                                  |
| Ubuntu       | <ul style="list-style-type: none"> <li>● Ubuntu 14.04 (64bit)</li> <li>● Ubuntu 16.04 (64bit)</li> <li>● Ubuntu 18.04 (64bit)</li> <li>● Ubuntu 20.04 (64-bit)</li> </ul>                                                                                                                                              |
| EulerOS      | <ul style="list-style-type: none"> <li>● Euler 2.2 (64bit)</li> <li>● Euler 2.3 (64bit)</li> </ul>                                                                                                                                                                                                                     |
| Oracle Linux | <ul style="list-style-type: none"> <li>● Oracle Linux 6.9 (64bit)</li> <li>● Oracle Linux 7.4 (64bit)</li> </ul>                                                                                                                                                                                                       |

### 33.3.4 What Is the Process Name of the Database Audit Agent?

#### Linux OS

The process name of the agent is `/opt/dbss_audit_agent/bin/audit_agent`

After installing the agent, you can perform the following steps to view its operating status:

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

**Step 2** Run the following command to view the operating status of the agent:

```
ps -ef|grep audit_agent
```

- If the following information is displayed, the agent is running properly:  
`/opt/dbss_audit_agent/bin/audit_agent`
- If no information is displayed, the agent does not run properly.

----End

## Windows OS

After the agent is installed, you can find the agent process `dbss_audit_agent` process in the Windows Task Manager.

### 33.3.5 (Linux OS) What Should I Do If I Lack the Permission to Run the Agent Installation Script?

Run the following command on the node where the agent will be installed to add the execute permission on the installation script:

```
chmod +x install.sh
```

### 33.3.6 (Linux OS) Where Are the Logs of the Database Audit Agent Saved?

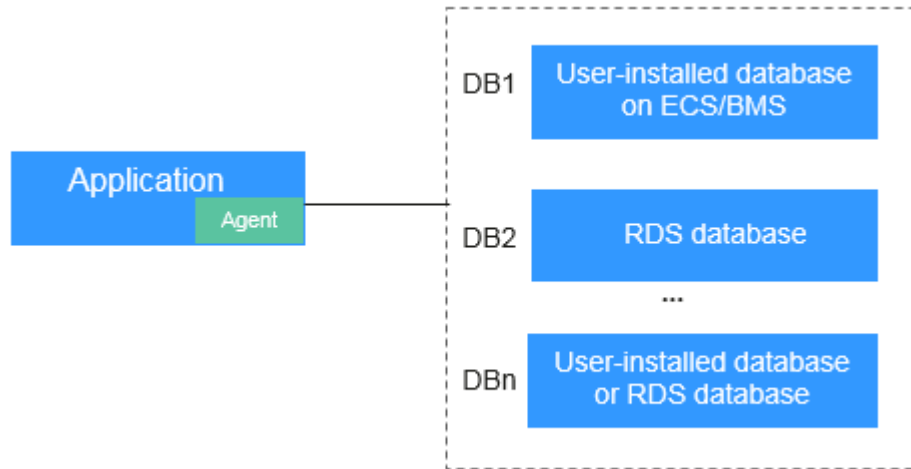
The path for saving agent logs is `/opt/dbss_audit_agent/log/audit_agent.log`.

### 33.3.7 When Should I Select an Existing Agent?

Do this if an application is connected to multiple databases, as shown in [Figure 33-3](#), and an agent has been installed on the application (by setting **Installing Node Type** to **Application**) for one of the databases (for example, **DB1**). To add an agent for another of them, select **Selecting an existing agent** for **Add Mode**, and select the agent added for **DB1**, as shown in [Figure 33-4](#).

After the agent is added, the database can be audited.

**Figure 33-3** An application connected to multiple databases



**NOTE**

Possible combinations of connected databases are:

- User-installed databases on ECS/BMS
- RDS databases
- User-installed databases on ECS/BMS and RDS databases

**Figure 33-4** Selecting an existing agent

The screenshot shows a dialog box titled 'Add'. It has two radio buttons for 'Add Mode': 'Select an existing agent' (selected) and 'Create an agent'. Below are two dropdown menus: 'Database Name' with 'tesT' and 'Agent ID' with 'AXaSxiGbzoA3BGc6i4\_g'. At the bottom are 'OK' and 'Cancel' buttons.

### 33.3.8 What Do I Do If the Database Audit Agent Is Hibernating?

After an agent is added for a database to be audited, the initial status of the agent will be **Hibernating**, as shown in [Figure 33-5](#).

**Figure 33-5** Successfully adding an agent

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

| Agent ID            | Installing... | Installing... | OS          | Audited ... | CPU Th... | Memor... | Gener... | Status      | Operation             |
|---------------------|---------------|---------------|-------------|-------------|-----------|----------|----------|-------------|-----------------------|
| AXDCiRXaZghMXmOrEA1 | Application   | 1.3.5.8       | Linux 64... | --          | 80        | 80       | No       | Hibernating | Download Agent   More |



To use database audit, you need to install the agent.

Check the agent status after you installed it.

- If the agent status changes to **Running** after the installation, as shown in [Figure 33-6](#), it indicates that the agent is running properly.

**Figure 33-6** Agent running properly

| No. | Database Information                         | Character ... | IP Address...         | Instance | OS      | Audit Status | Agent | Operation        |
|-----|----------------------------------------------|---------------|-----------------------|----------|---------|--------------|-------|------------------|
| 1   | Name: mydb-04<br>Type: MYSQL<br>Version: 5.0 | UTF8          | 192.168.0.104<br>3306 | --       | LINU... | Enabled      | Add   | Disable   Delete |

| Agent ID             | Install... | OS        | Audite...  | CPU ... | Mem... | Ge... | Status | Operation                       |
|----------------------|------------|-----------|------------|---------|--------|-------|--------|---------------------------------|
| AXICpAJRSIxeLRSixGru | Database   | 192.16... | Linux 6... | --      | 80     | 80    | No     | Running   Download Agent   More |

- If the agent status is still **Hibernating** after the installation, troubleshoot the problem by following the instructions provided in [What Do I Do If the Communication Between the Agent and Database Audit Instance Is Abnormal?](#)

### 33.3.9 How Do I Determine Where to Install an Agent?

The database audit agent can be installed on the database, application, or proxy node (ranked in descending order of preference).

For details about the nodes, see [Table 33-7](#).

**Table 33-7** Nodes to install agents

| Node        | Scenario                                                                                                                                                                            | Audit Scope                                                                                                           | Configuration                                                                                                                                                                                                                                                                                                  |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Database    | Self-built database on ECS/BMS                                                                                                                                                      | All access records of applications that have accessed the database                                                    | Set <b>Installing Node Type</b> to <b>Database</b> .                                                                                                                                                                                                                                                           |
| Application | You cannot log in to the node where your database (for example, RDS database) is deployed.                                                                                          | Access records of all the databases connected to the application                                                      | <ul style="list-style-type: none"> <li>• Set <b>Installing Node Type</b> to <b>Application</b>, as shown in <a href="#">Figure 33-8</a>.</li> <li>• If an agent has been installed on a database connected to the same application as the desired database, select <b>Select an existing agent</b>.</li> </ul> |
| Proxy       | You cannot log in to the node where your database (for example, RDS database) is deployed, and cannot install an agent on your application (for example, an off-cloud application). | Only the access records between the proxy and database. Those between the application and database cannot be audited. | Set <b>Installing Node Type</b> to <b>Application</b> , and set <b>Installing Node IP Address</b> to the IP address of the proxy.                                                                                                                                                                              |

## Adding an Agent

- Database

**Figure 33-7** Adding an agent to a database

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. It contains the following fields and options:

- Add Mode:** Two radio buttons: "Select an existing agent" (unselected) and "Create an agent" (selected).
- Installing Node Type:** Two radio buttons: "Database" (selected) and "Application" (unselected).
- OS:** A dropdown menu with "Linux 64-bit" selected.
- Buttons:** "OK" (red) and "Cancel" (white) buttons at the bottom.

- Application

**Figure 33-8** Adding an agent to an application

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. It contains the following fields and options:

- Add Mode:** Two radio buttons: "Select an existing agent" (unselected) and "Create an agent" (selected).
- Installing Node Type:** Two radio buttons: "Database" (unselected) and "Application" (selected).
- \* Installing Node IP Address:** Text input field containing "192.168.1.1".
- Audited NIC Name:** Empty text input field.
- CPU Threshold (%):** Text input field containing "80".
- Memory Threshold (%):** Text input field containing "80".
- OS:** A dropdown menu with "Linux 64-bit" selected.
- Buttons:** "OK" (red) and "Cancel" (white) buttons at the bottom.

**Figure 33-9** Selecting an existing agent

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. It contains the following fields and options:

- Add Mode:** Two radio buttons: "Select an existing agent" (selected) and "Create an agent" (unselected).
- Database Name:** A dropdown menu with "tesT" selected.
- \* Agent ID:** A dropdown menu with "AXaSxiGbzoA3BGc6i4\_g" selected.
- Buttons:** "OK" (red) and "Cancel" (white) buttons at the bottom.

**NOTICE**

If an agent has been installed on a database connected to the same application as the desired database, select **Select an existing agent**. For details, see [When Should I Select an Existing Agent?](#)

- Proxy

**Figure 33-10** Adding an agent to an application

**NOTICE**

**Installing Node IP Address** must be set to the IP address of the proxy.

### 33.3.10 How Do I Download a Database Audit Agent?

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

**NOTE**

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


#### Prerequisites

- You have applied for 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 > 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  in the lower part of the database list to expand the agent details. Locate the target agent and click **Download Agent** in the **Operation** column. to download an agent installation package.

**Figure 33-11** Downloading an agent

| No.                   | Database Information | Character Set | IP Address/Port | Instance    | OS        | Audit Status | Agent    | Operation        |                         |
|-----------------------|----------------------|---------------|-----------------|-------------|-----------|--------------|----------|------------------|-------------------------|
| ^ 1                   | Name: dummy-02       | UTF8          | 2.3.3.5<br>3214 | -           | LINUX64   | Enabled      | Add      | Disable   Delete |                         |
|                       | Type: MYSQL          |               |                 |             |           |              |          |                  |                         |
|                       | Version: 5.0         |               |                 |             |           |              |          |                  |                         |
| Agent ID              | Installing...        | Installing... | OS              | Audited ... | CPU Th... | Memor...     | Gener... | Status           | Operation               |
| AXDCIOVWwZqhlMXmOfEAz | 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

### 33.3.11 How Do I Uninstall a Database Audit 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

## 33.3.12 How Do I Install the Agent (in Windows OS)?

To install the agent on a Windows OS, perform the following operations.

### Prerequisites

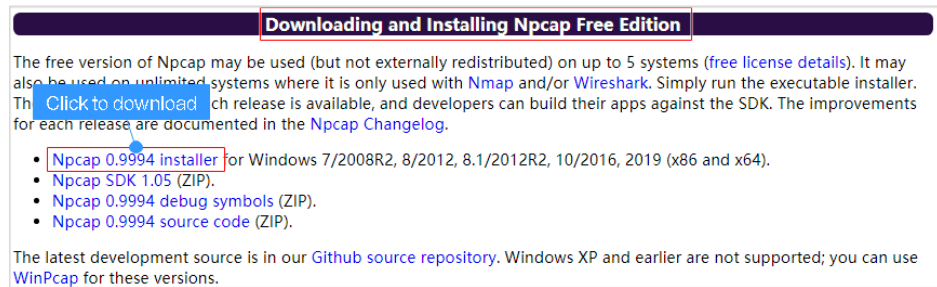
- You have added an agent to your database.
- You have obtained the agent installation package for the Windows OS.
- The Windows OS version of the target node is supported by the agent.

### Installing an Agent

**Step 1** Install Npcap on the Windows server.

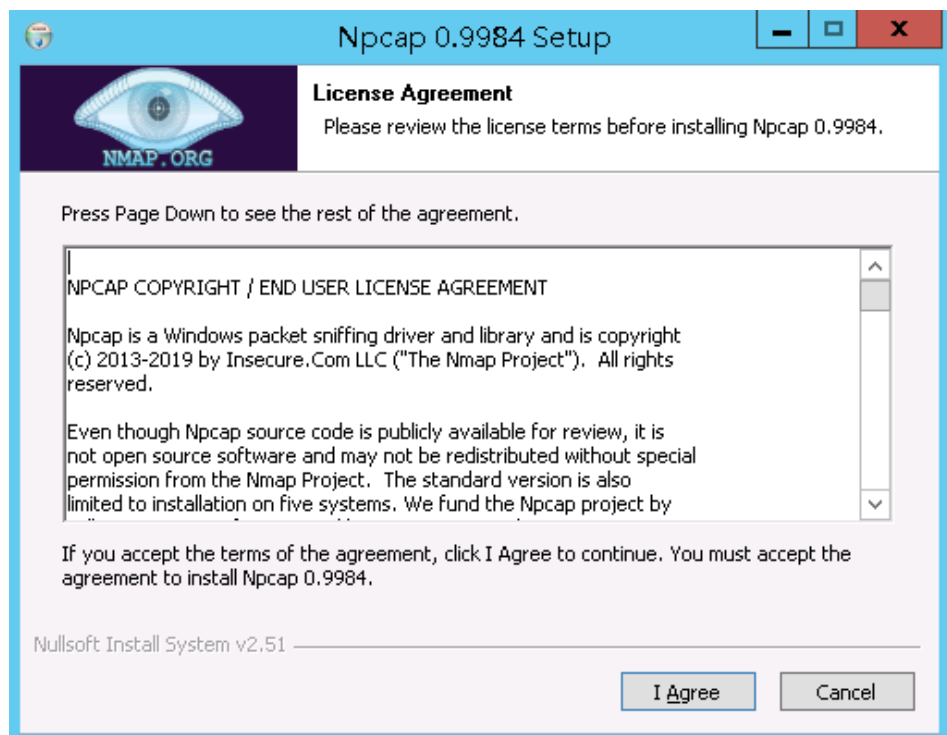
- If Npcap has been installed on the Windows OS, go to [Step 2](#).
- If the Npcap has not been installed on the Windows server, perform the following steps:
  - a. Download the latest Npcap software installation package from <https://nmap.org/npcap/>.

**Figure 33-12** Downloading Npcap



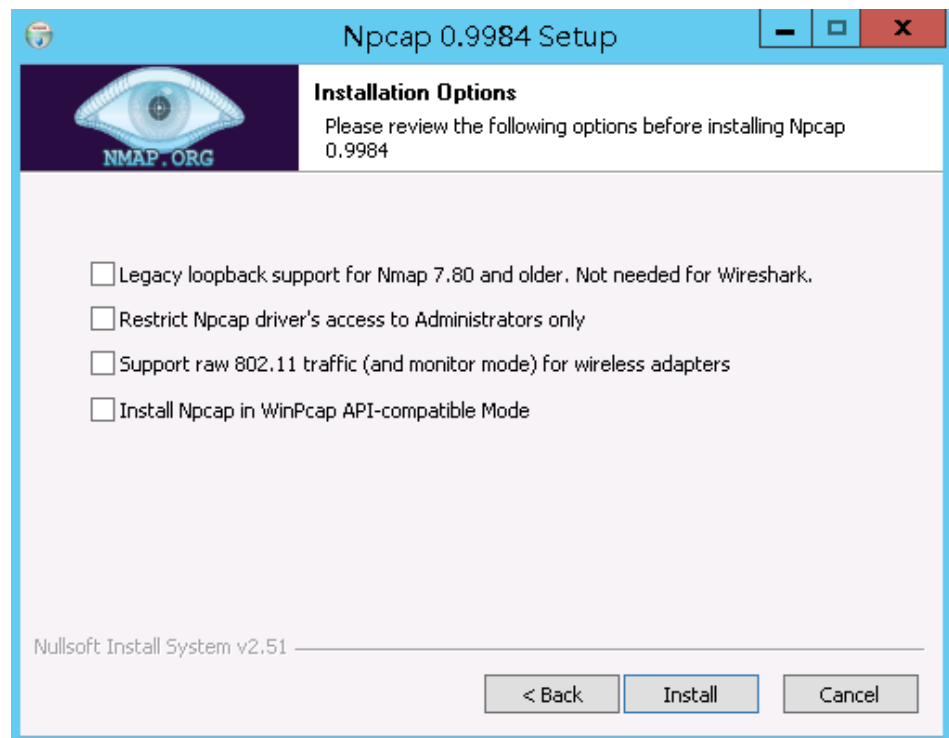
- b. Upload the **npcap-xxxx.exe** software installation package to the VM where the agent is to be installed.
- c. Double-click the Npcap installation package.
- d. In the displayed dialog box, click **I Agree**, as shown in [Figure 33-13](#).

**Figure 33-13** Agreeing to install Npcap

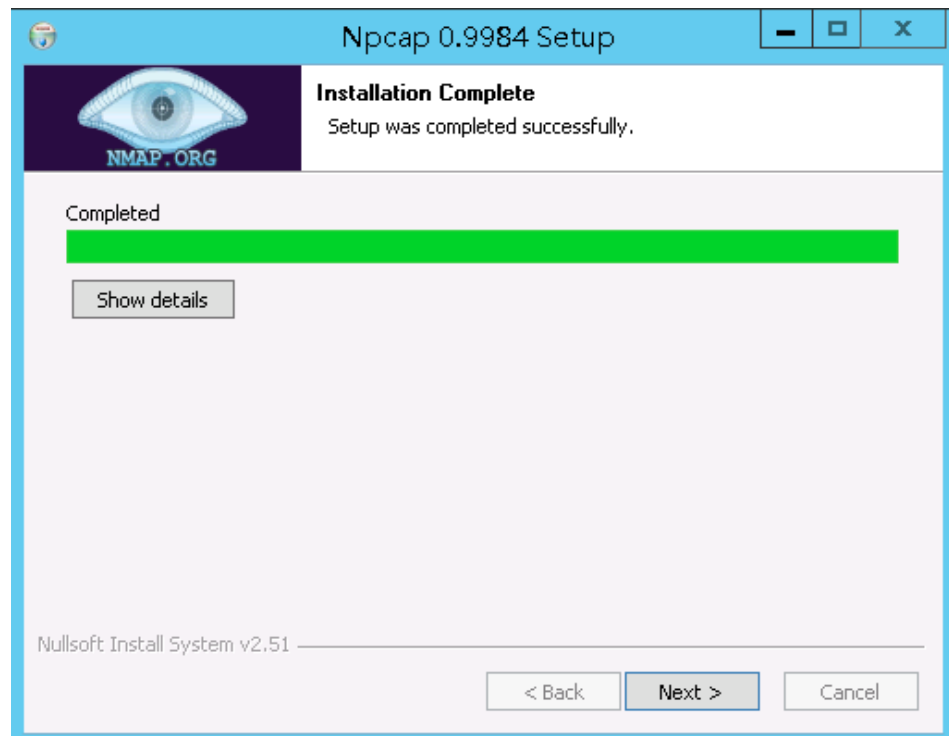


- e. In the displayed dialog box, leave all the check boxes unselected and click **Install**, as shown in [Figure 33-14](#).

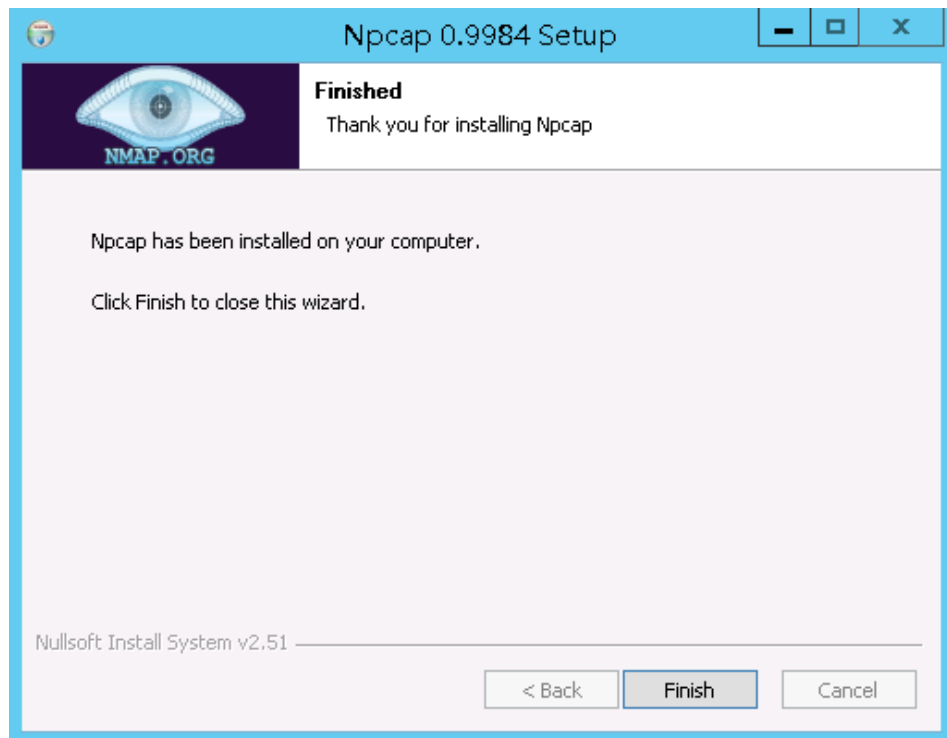
**Figure 33-14** Installing Npcap



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



- g. Click **Finish**.



- 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 33-15** is displayed.

**Figure 33-15** Installation completed

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



**Step 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

### 33.3.13 What Do I Do If the Communication Between the Agent and Database Audit Instance Is Abnormal?

#### Symptom

An agent has been installed on the database or application, but the SQL statement is not displayed in the SQL statement list after you enter an SQL statement in the database.

Perform the following operations to troubleshoot the problem:

- [Checking the Audited Database](#)
- [Checking the Security Group Rules of the Database Audit Instance](#)
- [Check the running status of the agent on the installing node.](#)

#### Checking the Audited Database

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

**Step 2** Select a region, click , and choose **Security > 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 checked.

**Step 5** Check the information about the database to be audited, as shown in [Figure 33-16](#).

**Figure 33-16** Viewing the information about the database to be audited

| No. | Database Information                                 | Character ... | IP Address...         | Instance | OS      | Audit Status | Agent | Operation        |
|-----|------------------------------------------------------|---------------|-----------------------|----------|---------|--------------|-------|------------------|
| 1   | Name: mydb-04<br>Type: MYSQL<br>Version: 5.0         | UTF8          | 192.168.0.104<br>3306 | --       | LINU... | Enabled      | Add   | Disable   Delete |
| 2   | Name: sql-server<br>Type: SQLSERVER<br>Version: 2017 | UTF8          | 1.2.3.4<br>134        | --       | WIND... | Enabled      | Add   | Disable   Delete |

- If the database information is correct, go to [Step 6](#).
- If the database information is incorrect, click **Delete** to delete the database, and then click **Add Database** to add the database again.
  - If the fault is rectified, no further operation is required.
  - If the problem persists, go to [Step 6](#).

**Step 6** Check the audit status of the database to be audited, as shown in [Figure 33-17](#).

**Figure 33-17** Checking the database audit status

| No. | Database Information                                   | Character ... | IP Address...         | Instance | OS      | Audit Status | Agent | Operation        |
|-----|--------------------------------------------------------|---------------|-----------------------|----------|---------|--------------|-------|------------------|
| 1   | Name: mydb-04<br>Type: MYSQL<br>Version: 5.0           | UTF8          | 192.168.0.104<br>3306 | --       | LINU... | Enabled      | Add   | Disable   Delete |
| 2   | Name: sql-server<br>Type: MSSQLSERVER<br>Version: 2017 | UTF8          | 1.2.3.4<br>134        | --       | WIND... | Enabled      | Add   | Disable   Delete |

- If **Audit Status** is **Enabled**, go to [Checking the Security Group Rules of the Database Audit Instance](#).
- If **Audit Status** is **Disabled**, click **Enable** to enable the database audit function.
  - If the fault is rectified, no further operation is required.
  - If the problem persists, go to [Checking the Security Group Rules of the Database Audit Instance](#).

----End

## Checking the Security Group Rules of the Database Audit Instance

**Step 1** Click  next to the database to expand the details about the agent and record the value of **Installing Node IP Address**, as shown in [Figure 33-18](#).

**Figure 33-18** Recording the IP address of the installing node

| No. | Database Information                        | Character Set | IP Address/Port       | Instance | OS      | Audit Status | Agent | Operation        |
|-----|---------------------------------------------|---------------|-----------------------|----------|---------|--------------|-------|------------------|
| 1   | Name: mydb01<br>Type: MYSQL<br>Version: 5.0 | UTF8          | 192.168.0.104<br>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_OoOpIDeIRft | Database            | 192.168.0.104              | Linux 64-bit | --                | 80              | 80            | No      | Disabled | Download Agent   More |

**Step 2** In the navigation tree on the left, choose **Database Audit > Instances**.


**Step 3** Click the required instance. The **Overview** page is displayed.

**Step 4** In the **Network Settings** area, record the value of **Security Group** (for example, **default**) of the database audit instance, as shown in [Figure 33-19](#).

**Figure 33-19** Checking the security group of the database audit instance



| Basic Info             |                                                                                               |
|------------------------|-----------------------------------------------------------------------------------------------|
| Name                   | DBSS-5de6  |
| ID                     | 940a4b6e-3602-41c5-8c81-31cdeb936520                                                          |
| Version                | 20.11.25.001953                                                                               |
| Edition                | Basic   Maximum database instances: 3                                                         |
| Created                | Dec 26, 2020 11:32:43 GMT+08:00                                                               |
| Status                 | Running  |
| AZ                     |          |
| Remarks                | --       |
| Billing Mode           |          |
| Remaining Period (day) | --                                                                                            |

| Network Settings   |                                                                                             |
|--------------------|---------------------------------------------------------------------------------------------|
| VPC                | vpc-default                                                                                 |
| Security Group     | default  |
| Subnet             | subnet-dbss                                                                                 |
| Private IP Address | 192.168.1.83                                                                                |

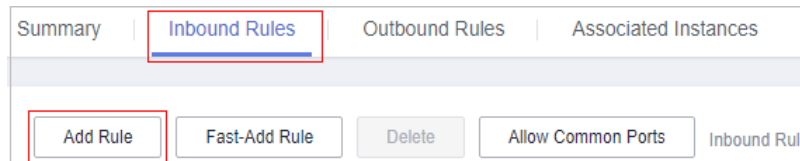
  

| Associated Database |                                 |
|---------------------|---------------------------------|
| mydb01              | <a href="#">Manage Database</a> |

- Step 5** Click  in the upper left corner of the management console and choose **Network > Virtual Private Cloud**.
- Step 6** In the navigation tree on the left, choose **Access Control > Security Groups**. The security group list page is displayed.
- Step 7** Enter the security group **default** recorded in **Step 4** in the search box in the upper right corner of the list, and click  or press **Enter**. Its information is displayed in the list.
- Step 8** Click the name of the security group **default**. Click the **Inbound Rules** tab.
- Step 9** Check inbound rules of the security group **default**.
- 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 1**.
- If inbound rules have been configured for the security group, go to **Check the running status of the agent on the installing node..**
  - If no inbound rule is configured for the security group, go to **Step 10**.
- Step 10** Add inbound rules for the security group of the database audit instance.

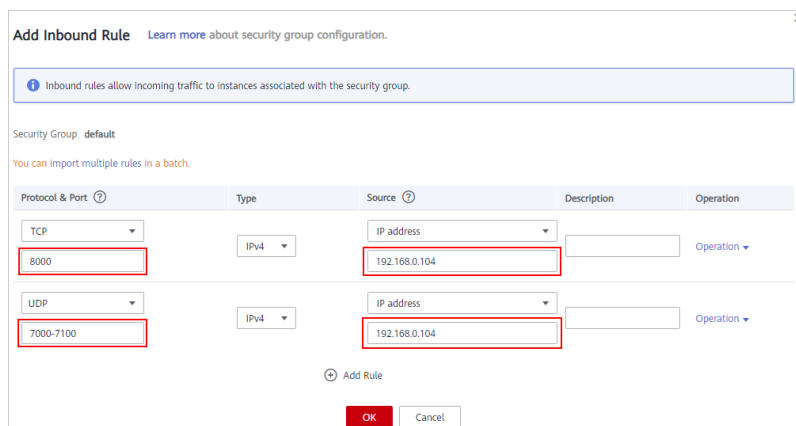
1. Click **Add Rule**, as shown in **Figure 33-20**.

**Figure 33-20** 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 **Step 1**. See **Figure 33-21**.

**Figure 33-21** Add Inbound Rule dialog box



3. Click **OK**.
  - If the fault is rectified, no further operation is required.

- If the problem persists, go to [Check the running status of the agent on the installing node.](#)

----End

## Check the running status of the agent on the installing node.

- Linux OS
  - a. 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).
  - b. Run the following command to view the running status of the agent:  
**service audit\_agent status**
    - If the following information is displayed, the agent is running properly. Go to [Verifying the Result](#).  
audit agent is running.
    - If no information is displayed, the agent is running abnormally. Run the following command to restart the agent:  
**service audit\_agent restart**
- Windows OS
  - a. Open the Task Manager.
  - b. Query the status of the dbss\_audit\_agent process.
    - If the process is running, go to [Verifying the Result](#).
    - If the process is stopped, go to the directory where the agent installation file is stored, and double-click the **start.bat** file to start the audit process.

## Verifying the Result

In your database, run an SQL statement on the node where the agent is installed. Choose **Overview > Statements** and then search for the executed statement.

- If the SQL statement is found, the problem has been solved.
- If the SQL statement is not found, the problem persists. Contact customer service.

## 33.3.14 How Many Resources Are Consumed by an Agent When It Runs on a Node?

When an agent is running, it consumes no more than 5% CPU and no more than 300 MB memory. The following resource metrics are monitored to prevent the agent from consuming too many resources:

- Overall CPU and memory usage of the system. If the CPU or memory usage exceeds the specified threshold (80% by default), the agent will stop running.
- CPU and memory of the agent process

## 33.4 Operations

### 33.4.1 How Do I Disable SSL for a Database?

If SSL is enabled for a database, the database cannot be audited. To use database audit, disable SSL first.

The MySQL database client is used as an example. Perform the following steps:

**Step 1** Log in to the MySQL database client as user **root**.

**Step 2** Run the following command to check the connection mode of the MySQL database:

```
\s
```

- If information similar to the following is displayed, SSL has been disabled for the MySQL database.  
SSL: Not in use
- If information similar to the following is displayed, SSL has been enabled for the MySQL database. Go to [Step 3](#).  
SSL: Cipher in use is XXX-XXX-XXXXXX-XXX

**Step 3** Log in to the MySQL database in SSL mode.

1. Run the following command to exit from the MySQL database:

```
exit
```

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

Add the following parameters at the end of the login command:

```
--ssl-mode=DISABLED
```

Or

```
--ssl=0
```

---

#### NOTICE

If you logged in to the MySQL database in SSL mode, you can disable SSL only for this login. To use the database audit function, log in to the MySQL database as instructed in this step.

3. Run the following command to check the connection mode of the MySQL database:

```
\s
```

If information similar to the following is displayed, SSL has been disabled for the MySQL database.

```
SSL: Not in use
```

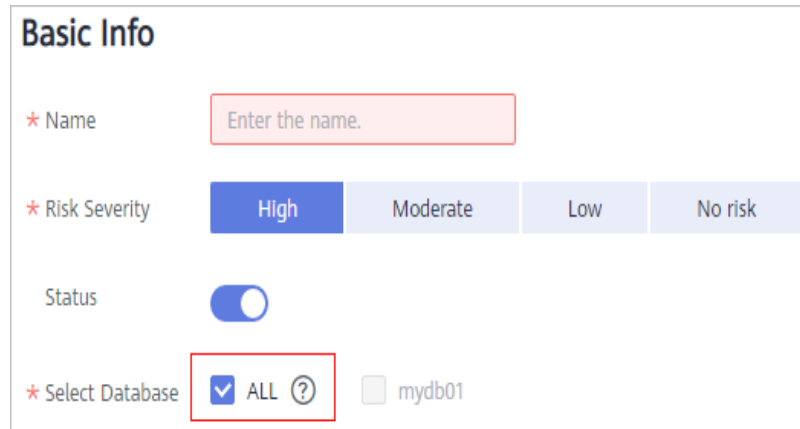
----End

### 33.4.2 How Do I Set Database Audit Rules for All Databases?

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.


You can also apply risky operation settings to all databases connected to a database audit instance, as shown in [Figure 33-22](#).

**Figure 33-22** Applying risk operation settings to all connected databases

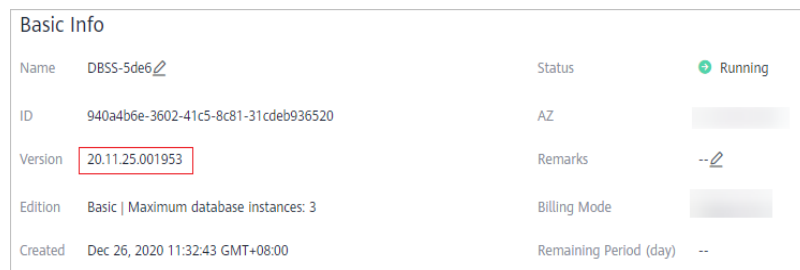


### 33.4.3 How Do I Check the Version of Database Audit?

To check the version of database audit, perform the following steps:

- Step 1** Log in to the management console.
- Step 2** Select a region, click , and choose **Security > 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 instance version, as shown in [Figure 33-23](#).


**Figure 33-23** Viewing the instance version



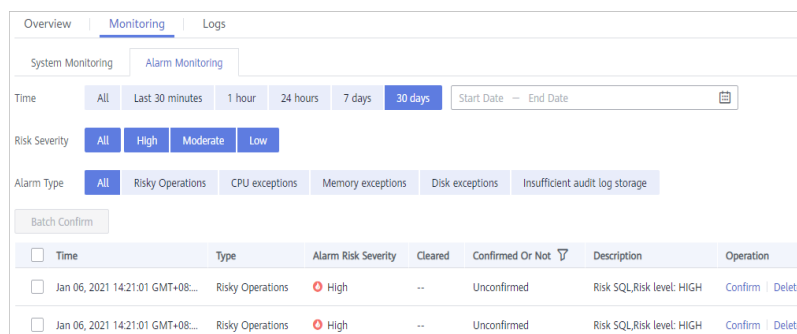
----End

### 33.4.4 How Do I View All Alarms in Database Audit?


To check the alarms of database audit, perform the following steps:

- Step 1** Log in to the management console.
- Step 2** Select a region, click , and choose **Security > 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 33-24](#).

**Figure 33-24** Viewing the alarms



To query specified alarms, perform the following steps:

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

----End

### 33.4.5 How Do I Audit an RDS Database Accessed through Intranet (by Applications Off the Cloud)?

If your PC accesses RDS through a private line, you can install the agent on a proxy your set up. Access from the proxy to the database can be audited. Access from applications to the proxy cannot be audited.

## 33.5 Troubleshooting

## 33.5.1 Database Audit Is Running Properly But Generates No Audit Records

### Symptom

The functions of the database audit instance are normal. When there is database traffic, audit information about the executed SQL statement cannot be found in the SQL statement list.

### Possible Causes

- SSL is enabled for the database.
- ForceEncryption is enabled for the SQL Server database protocol.
- The data volume is too large. As a result, the Agent process is suspended. You are advised to restart the container or optimize audit rules to reduce the data volume.

#### NOTE

- If SSL is enabled for a database, the database cannot be audited.
- If ForceEncryption is enabled for a database, database audit cannot obtain file content from the database for analysis.

### Disabling Database SSL

The MySQL database client is used as an example. Perform the following steps:

**Step 1** Log in to the MySQL database client as user **root**.

**Step 2** Run the following command to check the connection mode of the MySQL database:

```
\s
```

- If information similar to the following is displayed, SSL has been disabled for the MySQL database. Go to [Step 4](#).  
SSL: Not in use
- If information similar to the following is displayed, SSL has been enabled for the MySQL database. Go to [Step 3](#).  
SSL: Cipher in use is XXX-XXX-XXXXXX-XXX

**Step 3** Log in to the MySQL database in SSL mode.

1. Run the following command to exit from the MySQL database:

```
exit
```

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

Add the following parameters at the end of the login command:

```
--ssl-mode=DISABLED
```

or

```
--ssl=0
```



#### NOTICE

If you log in to the MySQL database in SSL mode, you can only disable SSL for this login. To use the database audit function, log in to the MySQL database in the mode described in [Step 3.2](#).

3. Run the following command to check the connection mode of the MySQL database:

```
\s
```

If information similar to the following is displayed, SSL has been disabled for the MySQL database. Go to [Step 4](#).

```
SSL: Not in use
```

**Step 4** Run an SQL statement and search for it in the SQL statement list.

- If the SQL statement is found, the problem has been solved.
- If the SQL statement is not found, the problem persists. In this case, [Disable ForceEncryption for the SQL Server protocol](#).

----End

## Disabling ForceEncryption for the SQL Server Protocol

**Step 1** Open the **SQL Server Configuration Manager** dialog box.

**Step 2** Select **SQL Server Network Configuration**.

**Step 3** Right-click **Protocols for MSSQLSERVER** and choose **Properties**.

**Step 4** Click the **Flags** tab. Set **ForceEncryption** to **No**.

**Step 5** Restart the SQL Server service for the modification to take effect.

**Step 6** Run an SQL statement and search for it in the SQL statement list.

- If the SQL statement is found, the problem has been solved.
- If the SQL statement is not found, the problem persists. Contact customer service.

----End

## 33.5.2 Database Audit Is Unavailable

### Symptom

After the database traffic is triggered, you cannot find the audit information about an executed statement in the SQL statement list.

In this case, perform the following operations to troubleshoot the problem:

- [Checking Database Information and Audit Function Settings](#)
- [Checking Audited Database Settings](#)

- [Checking Database Agent Status](#)
- [Checking the Security Group Rules of the Database Audit Instance](#)

## Checking Database Information and Audit Function Settings

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

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

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

**Step 4** Select an instance where the database is located from the **Instance** drop-down list.

**Step 5** View the database information, as shown in [Figure 33-25](#).

**Figure 33-25** Viewing the information about the database to be audited

| No. | Database Information                                 | Character ... | IP Address...         | Instance | OS      | Audit Status | Agent | Operation        |
|-----|------------------------------------------------------|---------------|-----------------------|----------|---------|--------------|-------|------------------|
| 1   | Name: mydb-04<br>Type: MYSQL<br>Version: 5.0         | UTF8          | 192.168.0.104<br>3306 | --       | LINU... | Enabled      | Add   | Disable   Delete |
| 2   | Name: sql-server<br>Type: SQLSERVER<br>Version: 2017 | UTF8          | 1.2.3.4<br>134        | --       | WIND... | Enabled      | Add   | Disable   Delete |

**Step 6** Check whether the database information is correct.

- If the database information is correct, go to [Step 7](#).
- If the database information is incorrect, click **Delete** to delete the database, and then click **Add Database** to add the database again.
  - If the fault is rectified, no further operation is required.
  - If the problem persists, go to [Step 7](#).

**Step 7** Check whether the database audit function is enabled.

- If **Audit Status** is **Enabled**, go to [Checking Audited Database Settings](#).
- If **Audit Status** is **Disabled**, click **Enable** to enable the database audit function.
  - If the fault is rectified, no further operation is required.
  - If the problem persists, go to [Checking Audited Database Settings](#).

----End

## Checking Audited Database Settings

In the navigation tree on the left, choose **Database Audit > Rules**. The **Audit Scope** page is displayed. See [Figure 33-26](#).

**Figure 33-26** Audit scope

| No. | Name             | Source IP A... | Source Port | Database Name | Database A... | Status  | Operation               |
|-----|------------------|----------------|-------------|---------------|---------------|---------|-------------------------|
| 1   | Full audit rules | any            | any         | --            | any           | Enabled | Disable   Edit   Delete |

- If **Status** is **Enabled**, go to [Checking Database Agent Status](#).
- If **Status** is **Disabled**, click **Enable** to enable the desired audit scope rule of the database.
  - If the fault is rectified, no further operation is required.
  - If the problem persists, go to [Checking Database Agent Status](#).

## Checking Database Agent Status

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

**Step 2** Run the following command to view the running status of the agent program:

**ps -ef|grep audit\_agent**

- If the following information is displayed, the agent is running properly. Go to [Step 4](#).  

```
/opt/dbss_audit_agent/bin/audit_agent
```
- If no information is displayed, the agent does not run properly. Go to [Step 3](#).

**Step 3** Run the following command to restart the agent:

**service audit\_agent restart**

- If the fault is rectified, no further operation is required.
- If the problem persists, go to [Step 4](#).

**Step 4** Run the following command to check the communication status between the agent and database audit instance:

**tailf /opt/dbss\_audit\_agent/log/audit\_agent.log**

- If information similar to the following is displayed, the communication between the agent and database audit instance is normal. Go to [Verifying the Result](#).

**Figure 33-27** Normal communication

```
~]# tailf /opt/dbss_audit_agent/log/audit_agent.log
7:37 INFO [websocket_message_handle.cpp:357] send config data capture result begin...
7:37 INFO [websocket_message_handle.cpp:359] send config data capture result success
7:37 INFO [websocket_message_handle.cpp:136] audit ethernet is: eth0
7:37 INFO [websocket_message_handle.cpp:149] libpcap filter policy is: port 3306 and (src host 192.168.0.118 or dst host 192.168.0.118)
7:37 INFO [catch_data_package.cpp:119] init libpcap tool begin...
7:37 INFO [catch_data_package.cpp:155] init libpcap tool success
7:37 INFO [udp_communication.cpp:28] init udp connection begin...
7:37 INFO [udp_communication.cpp:51] init udp connection success
7:37 INFO [catch_data_package.cpp:167] catch data packet begin...
7:39 INFO [websocket_message_handle.cpp:430] send heart beat begin
```

- If information similar to the following is displayed, the communication between the agent and database audit instance is abnormal. Go to [Checking the Security Group Rules of the Database Audit Instance](#).


**Figure 33-28** Communication error

```
Awdimb74cLSBfUhrp8-tj# tail /opt/dbss_audit_agent/log/audit_agent.log
INFO [websocket.cpp:1608] create websocket thread begin...
INFO [websocket.cpp:1620] create websocket thread success
INFO [websocket_connection_handle.cpp:278] setup websocket connection success
INFO [websocket_connection_handle.cpp:169] send authentication request packet with websocket...
INFO [websocket_connection_handle.cpp:126] create authentication request packet begin...
INFO [websocket_connection_handle.cpp:25] encrypt verify info by public key begin...
INFO [websocket_connection_handle.cpp:53] encrypt verify info by public key success
INFO [websocket_connection_handle.cpp:158] create authentication request packet success
INFO [websocket_connection_handle.cpp:172] authentication request packet is: {"body":{"agentid":"Awdimb74cLSBfU
":"EulerOS","ostype":"Linux","osver":"3.10.0-327.36.58.4.x86_64","verify":"IHGbvph0aqK6Q+saleIaIMLRBIA/537UGRgQqJ
icJUWmKs2:1VSLH2widWraDnczITXe4NM1wn/fzcZd;9eeendGh08Iv3CXpDDzY3SMoulkfbauLqdmIPwrNw5utJD55i05Qn0vfgunuzJWTC2A
i0QTb2cLi0iEKGHLeQ=="}, "code":1, "id":"98c43f29-e302-402a-9e75-321b2f6e06c2", "method":"request", "time":1543807412}
ERROR [websocket_connection_handle.cpp:177] send authentication request packet failed, retry 30 seconds later!
```

----End

## Checking the Security Group Rules of the Database Audit Instance

- Step 1** Go to the **Database Security Service** page.
- Step 2** In the navigation tree on the left, choose **Database Audit > Databases**. The **Databases** page is displayed.
- Step 3** Select an instance where the database is located from the **Instance** drop-down list.
- Step 4** 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**. See [Figure 33-29](#).

**Figure 33-29** Installing node IP address






| No. | Database Information                        | Character Set | IP Address/Port       | Instance | OS      | Audit Status | Agent | Operation      |
|-----|---------------------------------------------|---------------|-----------------------|----------|---------|--------------|-------|----------------|
| 1   | Name: mydb01<br>Type: MySQL<br>Version: 5.0 | UTF8          | 192.168.0.104<br>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_OoQpIPIeIRft | Database            | 192.168.0.104              | Linux 64-bit | --                | 80              | 80            | No      | Disabled | Download Agent More |

- Step 5** Record the security group information about the database to be audited.
  1. In the navigation tree on the left, choose **Database Audit > Instances**.
  2. Click the required instance. The **Overview** page is displayed.
  3. In the **Network Settings** area, record the value of **Security Group** (for example, **default**) of the database audit instance, as shown in [Figure 33-30](#).



**Figure 33-30** Security group information about the database to be audited

| Basic Info             |                                                                                               |
|------------------------|-----------------------------------------------------------------------------------------------|
| Name                   | DBSS-5de6  |
| ID                     | 940a4b6e-3602-41c5-8c81-31cdeb936520                                                          |
| Version                | 20.11.25.001953                                                                               |
| Edition                | Basic   Maximum database instances: 3                                                         |
| Created                | Dec 26, 2020 11:32:43 GMT+08:00                                                               |
| Status                 | Running  |
| AZ                     |          |
| Remarks                | --       |
| Billing Mode           |          |
| Remaining Period (day) | --                                                                                            |

| Network Settings   |                                                                                             | Associated Database |
|--------------------|---------------------------------------------------------------------------------------------|---------------------|
| VPC                | vpc-default                                                                                 | mydb01              |
| Subnet             | subnet-dbss                                                                                 |                     |
| Security Group     | default  | Manage Database     |
| Private IP Address | 192.168.1.83                                                                                |                     |

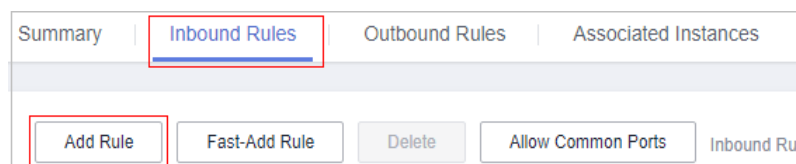
**Step 6** Go to the **Security Groups** page to check the rules of the recorded group.

1. Click  in the upper left corner of the management console and choose **Network > Virtual Private Cloud**.
2. In the navigation tree on the left, choose **Access Control > Security Groups**. The security group list page is displayed.
3. Enter the security group **default** recorded in [5.c](#) in the search box in the upper right corner of the list, and click  or press **Enter**. Its information is displayed in the list.
4. Click the name of the security group **default**. Click the **Inbound Rules** tab.
5. Check inbound rules of the security group **default**.  
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 4](#).
  - If inbound rules have been configured for the security group, go to [Verifying the Result](#).
  - If no inbound rule is configured for the security group, go to [Step 7](#).

**Step 7** Add an inbound rule for the installing node.

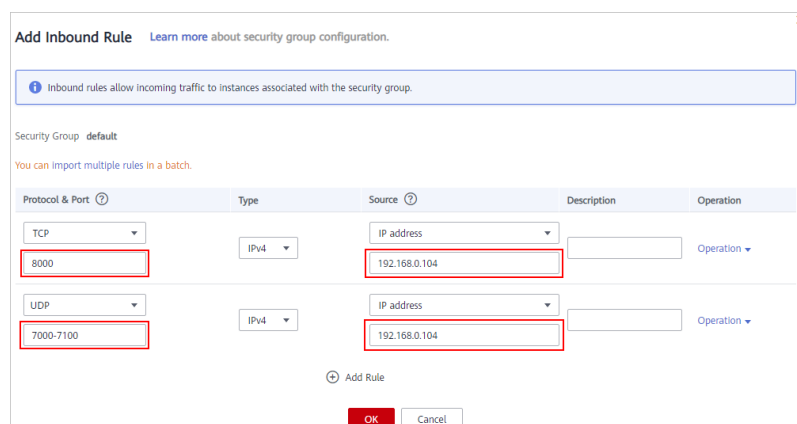
1. On the **Inbound Rules** tab, click **Add Rule**. See [Figure 33-31](#).

**Figure 33-31** 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 33-29](#). See [Figure 33-32](#).

**Figure 33-32** Adding an inbound rule



3. Click **OK**.

----End

## Verifying the Result

In your database, run an SQL statement on the node where the agent is installed, and then search for the statement in the SQL statement list.

- If the SQL statement is found, the problem has been solved.
- If the SQL statement is not found, the problem persists. Contact customer service.

## 33.5.3 Alarm Notifications Are Abnormal

### Symptom

- The database audit instance is running properly. An alarm about a high-risk statement alarm is sent via email, but no high-risk SQL statements are displayed on the console.
- Alarm email sending is delayed.

### Possible Causes

There are too many audit logs and data audit is delayed.

### Suggestion

- Add DBSS instances and balance the loads processed by each instance. Alternatively, modify audit rules to narrow down the audit scope.
- Create an automated hourly backup task to prevent log deletion, which will be triggered if the disk usage reaches 85%.

## 33.6 Logs

### 33.6.1 Can the Operation Logs of Database Audit Be Migrated?

No. Database audit does not support migrating database operation logs.

You can view the operation logs of database audit. For details, see [How Long Are the Operation Logs of Database Audit Saved by Default?](#)


### 33.6.2 How Long Are the Operation Logs of Database Audit Saved by Default?

The operation logs of database audit are permanently saved.

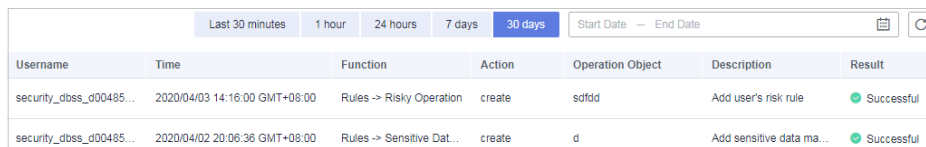
### 33.6.3 How Do I Check the Operation Logs of Database Audit?

To check the operation logs of database audit, perform the following steps:

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


- Step 2** Select a region, click , and choose **Security > 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 33-33](#). For details about related parameters, see [Table 33-8](#).

**Figure 33-33** Viewing operation logs



| Username                | Time                          | Function                  | Action | Operation Object | Description              | Result     |
|-------------------------|-------------------------------|---------------------------|--------|------------------|--------------------------|------------|
| security_dbss_000485... | 2020/04/03 14:16:00 GMT+08:00 | Rules -> Risky Operation  | create | sdfdd            | Add user's risk rule     | Successful |
| security_dbss_000485... | 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 33-8** Parameters

| Parameter        | Description                           |
|------------------|---------------------------------------|
| Username         | User who performs the operation       |
| Time             | Time when the operation was performed |
| Function         | Function of the operation             |
| Action           | Action of the operation               |
| Operation Object | Object of the operation               |
| Description      | Description of the operation          |
| Result           | Result of the operation               |

----End

### 33.6.4 How Does Database Audit Process Logs?

Database audit logs are stored in a log database and processed based on disk usage.


- If the disk usage of the log database is 85% or higher, the system automatically deletes the audit logs generated on the earliest date until the disk usage drops below 85%.
- If the disk usage is 90% or higher, database audit stops and the system no longer saves new audit logs.

### 33.6.5 How Do I Back Up the Database Audit Logs?

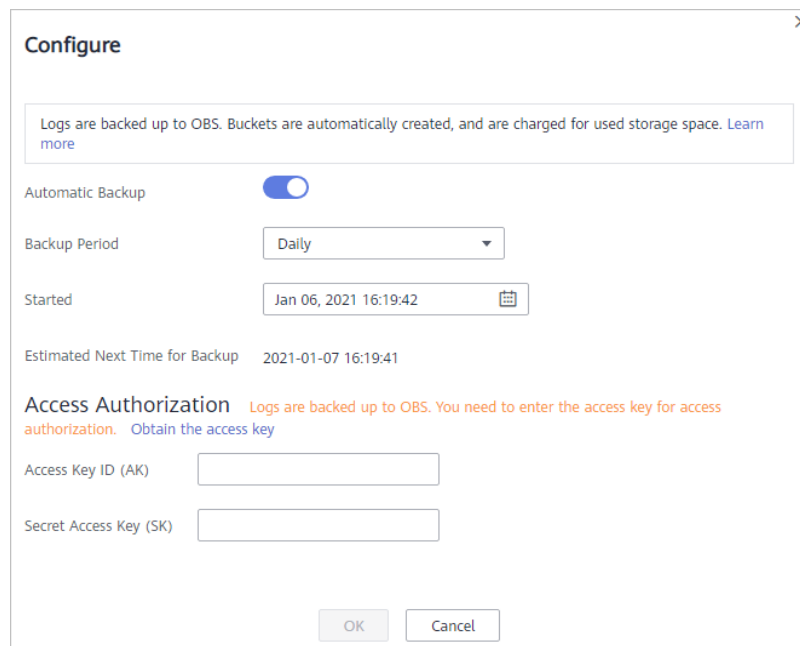
Database audit supports manual backup and automatic backup. Audit logs are backed up to OBS. Buckets will be automatically created and will incur a separate bill.

Perform the following operations to automatically back up audit logs.

#### Automatically Backing Up Database Audit Logs

- Step 1** Log in to the management console.
- Step 2** Select a region, click , and choose **Security > 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 33-34**. For details about related parameters, see **Table 33-9**.


**Figure 33-34** Configure Automatic Backup dialog box



**Table 33-9** Parameters

| Parameter        | Description                | Example Value |
|------------------|----------------------------|---------------|
| Automatic Backup | Status of automatic backup |               |



| Parameter                      | Description                                                                                                                                    | Example Value          |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Backup Period                  | Automatic backup period. Its options are as follows: <ul style="list-style-type: none"> <li>• <b>Daily</b></li> <li>• <b>Hourly</b></li> </ul> | Daily                  |
| Started                        | Start time of the backup. Click  to configure.              | 2020/01/14<br>20:27:08 |
| Estimated Next Time for Backup | Time when the next automatic backup starts                                                                                                     | 2020/01/15<br>20:21:29 |
| Access Key ID(AK)              | Access key (AK)                                                                                                                                | -                      |
| Secret Access Key(SK)          | Secret access key (SK)                                                                                                                         | -                      |

**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

### 33.6.6 Can Database Audit Logs Be Directly Saved to OBS?

No. Database audit logs are directly saved to the log database. You can back up the logs to Object Storage Service (OBS).

Database audit logs can be manually or automatically backed up.

Automatic backup: Logs can be automatically backed up on a daily, weekly, or monthly basis.

Manual backup: You can back up logs generated in the last 24 hours, last 7 days, last 30 days, and or all logs.

If there are a large number of logs generated, you are advised to automatically back up logs every day.

If you back up logs to OBS, an OBS bucket will be automatically created to store the logs Buckets are billed per use.

---

# A Change History

---

| Released On | Description                          |
|-------------|--------------------------------------|
| 2021-06-15  | This is the second official release. |
| 2021-01-28  | This is the first official release.  |