Database Security Service

FAQs

Issue 41

Date 2021-08-20

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Contents

1 Product Consulting

1.1 What Is Database Audit?

Database Security Service (DBSS) is an intelligent database security service. Based on the machine learning mechanism and big data analytics technologies, it can audit your databases, detect SQL injection attacks, and identify high-risk operations.

1.2 What Editions Does DBSS Provide?

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

Table 1-1 describes the database audit editions.

Table 1-1 Database audit editions

Version	Maximum Databases	System Resource	Performance
Basic	3	• CPU: 4 vCPUs • Memory: 16 GB • Disk: 560 GB • Disk: 500 GB	• Peak QPS: 3,000 queries/second • Database load rate: 3.6 million statements/hour • Stores 400 million online SQL statements. • Stores 5 billion archived SQL statements.

Version	Maximum Databases	System Resource	Performance
Professional	6	• CPU: 8 vCPUs • Memory: 32 GB • Disk: 1084 GB	• Peak QPS: 6,000 queries/second • Database load rate: 7.2 million statements/hour • Stores 600 million online SQL statements. • Stores 10 billion archived SQL statements.
Advanced	30	• CPU: 16 vCPUs • Memory: 64 GB • Disk: 2108 GB	• Peak QPS: 30,000 queries/second • Database load rate: 10.80 million statements/hour • Stores 1.5 billion online SQL statements. • Stores 60 billion archived SQL statements.

1.3 What Databases on HUAWEI CLOUD Does DBSS Protect?

DBSS protects self-built databases 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 self-built databases and RDS instances on ECSs and BMSs if they are not in the same VPC and its subnets.

1.4 What Databases Does DBSS Support?

DBSS supports the following HUAWEI CLOUD databases:

- RDS instances
- Self-built databases on ECS
- Self-built databases on BMS

1.5 Which Regions Is DBSS Available In?

DBSS is available in the following regions:

- CN East-Shanghai1
- CN East-Shanghai2
- CN South-Guangzhou
- CN North-Beijing1
- CN North-Beijing4

- CN Southwest-Guiyang1

1.6 Why Can't I See the Instance that Is Being Created After I Purchased It?

When you purchase a set of database protection or database audit 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.

After purchasing a DBSS instance, you are advised to refresh the page before checking the instance that is being created.

1.7 Does DBSS Upload Logs Through the Internet or Intranet?

DBSS uploads logs through the intranet.

1.8 Will My Services Be Affected If I Do Not Renew DBSS After It Expires?

If you do not renew DBSS after it expires, DBSS will be unavailable. Your other services will not be affected. For database and asset security purposes, you are advised to renew DBSS.

1.9 How Do I Comply with PCI, HIPAA, SOX, and GDPR Requirements?

The database protection service of DBSS has built-in compliance knowledge bases, which include PCI, HIPAA, SOX, and GDPR rules and can be used for sensitive data discovery. You can generate masking and audit rules based on the predefined rules in one click.

1.10 How Do I Obtain the DBSS Sales License?

HUAWEI CLOUD provides the DBSS sales license. Click **here** and log in. The **salelicense.pdf** file will be automatically downloaded.

Allowing Pop-ups in Browsers

If the pop-up on the license website is blocked, perform the following steps to unblock it. This section takes Google Chrome as an example.

Step 1 In the address bar, click the icon that indicates a pop-up has been blocked.

Step 2 Modify the browser settings to allow pop-ups in https://console.huaweicloud.com, and download the sales license.

----End

1.11 Does Database Audit Support Offline or Non-HUAWEI CLOUD Databases?

No. Currently, database audit can only audit the following HUAWEI CLOUD databases in bypass mode:

- RDS instances
- Self-built databases on ECS
- Self-built databases on BMS

For more information, see **What Databases Does Database Audit Support?**

1.12 What Are Regions and AZs?

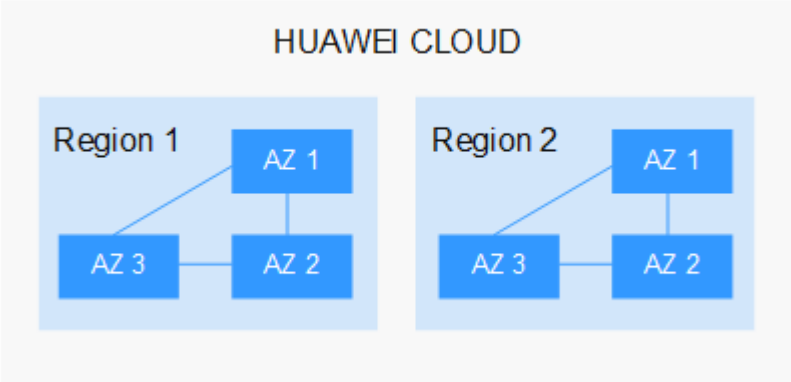
Concepts

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided from the dimensions of geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

Figure 1-1 shows the relationship between the regions and AZs.

Figure 1-1 Region and AZ



HUAWEI CLOUD provides services in many regions around the world. You can select a region and AZ as needed.

Selecting a Region

When selecting a region, consider the following factors:

- Location

  You are advised to select a region close to you or your target users. This reduces network latency and improves access rate. However, Chinese mainland regions provide basically the same infrastructure, BGP network quality, as well as operations and configurations on resources. Therefore, if you or your target users are in the Chinese mainland, you do not need to consider the network latency differences when selecting a region.

  - If you or your target users are in the Asia Pacific region, except the Chinese mainland, select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If you or your target users are in Africa, select the **AF-Johannesburg** region.
  - If you or your target users are in Europe, select the **EU-Paris** region.
- Resource price

  Resource prices may vary in different regions. For details, see **Product Pricing Details**.

Selecting an AZ

When determining whether to deploy resources in the same AZ, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs in the same region.
- For low network latency, deploy resources in the same AZ.

Regions and Endpoints

Before using an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

1.13 Does DBSS Support Real-Time Data Masking?

Sensitive data cannot be masked in real time. 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. For details, see **Configuring Privacy Data Protection Rules**.

1.14 Can DBSS Audit Databases Across Subnets?

Yes, as long as the databases are in the same VPC.

2 Purchase

2.1 Which Subnet Should I Choose When Purchasing an Instance?

Select a subnet that is in the same VPC as the database.

2.2 What Do I Do If a Message Is Displayed Indicating that Resources Are Sold Out During Instance Purchase?

While you purchase database audit, if a message is displayed indicating that resources are sold out in the region, you can click  in the upper left corner of the management console and switch to another region to buy services. Alternatively, you can submit a service ticket.

For details about the regions where DBSS is available, see **Which Regions Is DBSS Available In?**.

For details about how to submit a service ticket, see "Submitting a Service Ticket".

2.3 What Do I Do If a Message Indicating Insufficient Quota Is Displayed During Instance Purchase?

While you purchase database audit, if a message is displayed indicating that your quota is insufficient, submit a service ticket to apply for more quota.

For details about how to submit a service ticket, see "Submitting a Service Ticket".

2.4 Does My DBSS Purchase on DeC Consume DeC Resources?

Purchasing DBSS on Dedicated Cloud (DeC) consumes DeC resources, as described in **Table 2-1**.

If you do not want to consume DeC resources, purchase DBSS on the public cloud.

Table 2-1 Resources consumed by database audit

Edition	Consumed Resource
Basic	• vCPUs: 4 • Memory: 16 GB • Hard disk: 560 GB
Professional	• vCPUs: 8 • Memory: 32 GB • Hard disk: 1084 GB
Advanced	• vCPUs: 16 • Memory: 64 GB • Hard disk: 2108 GB

2.5 How Do I Renew Database Audit?

You can renew database audit instances before they expire.

Prerequisites

- The account for logging in to the management console has been granted the DBSS System Administrator, ECS Administrator, VPC Administrator, and BSS Administrator policies; or the Tenant Administrator permission policy.
- You have purchased a database audit instance.

Renewing Database Audit

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 & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

Step 5 On the **Renew** page, select a duration by which you want to renew the instance.

For details about renewal, see **Manually Renewing a Resource**.

----End

2.6 How Do I Unsubscribe from DBSS?

DBSS currently supports yearly and monthly subscription. Purchased DBSS instances cannot be deleted. If a purchased DBSS instance is no longer needed, you can unsubscribe it.

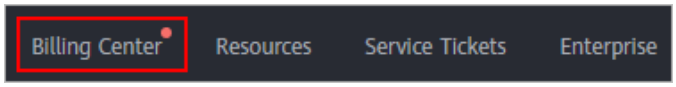
Prerequisites

- The account for logging in to the management console has been granted the DBSS System Administrator, ECS Administrator, VPC Administrator, and BSS Administrator roles; or the Tenant Administrator permission role.
- You have purchased a database audit instance.

Procedure

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

Step 2 In the upper right part of the page, click **Billing**. The **Billing Center** page is displayed.



Step 3 In the navigation pane, choose **Unsubscriptions and Changes** > **Unsubscriptions**.

For details about unsubscription, see **Unsubscriptions**.

----End

3 Database Audit Functions

3.1 Can Database Audit Be Used Across Regions?

No. Database audit is available only if the target database and your database audit instance are in the same region.

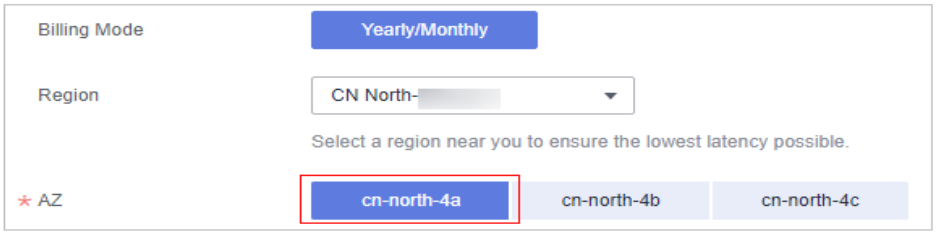
For example, if the database audit instance you purchased is deployed in **CN North-Beijing4** and the database to be audited is in **CN East-Shanghai1**, database audit is available.

3.2 Can Database Audit Be Used Across AZs?

Database audit is available only if the target database and your database audit instance are in the same region. If the database to be audited and the database audit instance you purchased are in different AZs in the same region, you can use database audit.

For example, if you have purchased database audit in **AZ1** in a region, as shown in Figure 3-1, and the database to be audited is deployed in AZ2 or AZ3 in the region, you can use the database audit you purchased.

Figure 3-1 Purchasing database audit in AZ1



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

No. Your databases are audited in bypass mode and this does not affect your services.

3.4 Can Database Audit Be Shared by Multiple Accounts?

No. For example, if you have two accounts (**domain1** and **domain2**) in a region, and purchase database audit under the **domain1** account, you cannot use the function under **domain2**.

In the same region, all the IAM users of an account can use database audit purchased under the account. Assume you have created a HUAWEI CLOUD account (**domain1**) in a region, and created two IAM users (**sub-user01** and **sub-user02**) under **domain1**. If you have granted the DBSS permission policy to **sub-user01** and **sub-user02**, both of them can use database audit purchased by **domain1**.

3.5 What Are the Functions of Database Audit?

Database audit is deployed in bypass pattern and can perform flexible audit on RDS databases and self-built ECS/BMS databases on HUAWEI CLOUD without affecting services. It 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.

3.6 What Databases Does Database Audit Support?

Database audit supports the following database types and versions.

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

Database Type	Version
MySQL	• 5.0, 5.1, 5.5, 5.6, 5.7 • 8.0
Oracle	• 11g 11.1.0.6.0, 11.2.0.1.0, 11.2.0.2.0, 11.2.0.3.0, and 11.2.0.4.0 • 12c 12.1.0.2.0, 12.2.0.1.0 • 19c

Database Type	Version
PostgreSQL	• 7.4 • 8.0, 8.1, 8.2, 8.3, 8.4 • 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 • 10.0, 10.1, 10.2, 10.3, 10.4, 10.5 • 11
SQL Server	• 2008, 2008R2 • 2012 • 2014 • 2016 • 2017
DWS	1.5
GaussDB(for Mysql)	Mysql 8.0
GaussDB for openGauss GaussDB(for openGauss)	2020 Enterprise Edition
DAMENG	DM8
KINGBASE	V8

3.7 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 3-2**.

Table 3-2 Supported Linux OS versions

System Name	System version
CentOS	• CentOS 6.3 (64bit) • CentOS 6.5 (64bit) • CentOS 6.8 (64bit) • CentOS 6.9 (64bit) • CentOS 7.0 (64bit) • CentOS 7.1 (64bit) • CentOS 7.2 (64bit) • CentOS 7.3 (64bit) • CentOS 7.4 (64bit) • CentOS 7.5 (64bit) • CentOS 7.6 (64bit) • CentOS 7.8 (64bit) • CentOS 7.9 (64bit) • CentOS 8.0 (64bit) • CentOS 8.1 (64bit) • CentOS 8.2 (64bit)
Debian	• Debian 7.5.0 (64bit) • Debian 8.2.0 (64bit) • Debian 8.8.0 (64bit) • Debian 9.0.0 (64bit) • Debian 10.0.0 (64bit)
Fedora	• Fedora 24 (64bit) • Fedora 25 (64bit)
SUSE	• SUSE 11 SP4 (64bit) • SUSE 12 SP1 (64bit) • SUSE 12 SP2 (64bit)
Ubuntu	• Ubuntu 14.04 (64bit) • Ubuntu 16.04 (64bit) • Ubuntu 18.04 (64bit)
Euler	• Euler 2.2 (64bit) • Euler 2.3 (64bit)
Oracle Linux	• Oracle Linux 6.9 (64bit) • Oracle Linux 7.4 (64bit)

- The following Windows OSs are supported:
  - Windows Server 2008 R2

  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
  - Windows 7
  - Windows 10

3.8 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.

3.9 Can Applications Using TLS Connections Be Audited?

No. Applications using TLS are encrypted.

3.10 How Long Is the Audit Data of Database Audit Stored by Default?

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

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

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

    For more information, see **Table 3-3**.
- Back up audit logs.

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

Table 3-3 Database audit editions

Version	Maximum Databases	System Resource	Performance
Basic	3	• CPU: 4 vCPUs • Memory: 16 GB • Disk: 560 GB • Disk: 500 GB	• Peak QPS: 3,000 queries/second • Database load rate: 3.6 million statements/hour • Stores 400 million online SQL statements. • Stores 5 billion archived SQL statements.
Professional	6	• CPU: 8 vCPUs • Memory: 32 GB • Disk: 1084 GB	• Peak QPS: 6,000 queries/second • Database load rate: 7.2 million statements/hour • Stores 600 million online SQL statements. • Stores 10 billion archived SQL statements.
Advanced	30	• CPU: 16 vCPUs • Memory: 64 GB • Disk: 2108 GB	• Peak QPS: 30,000 queries/second • Database load rate: 10.80 million statements/hour • Stores 1.5 billion online SQL statements. • Stores 60 billion archived SQL statements.

NOTE

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

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

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

3.11 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.

3.12 Is the Total Number Of Alarms Every Day the Same as that of Emails?

Yes. One alarm message corresponds to one email notification.

3.13 Why I Cannot Preview the Database Security Audit Report Online?

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

3.14 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 bypass 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:

- **Database Audit Is Unavailable**
- **Database Audit Is Running Properly But Generates No Audit Records**

3.15 Can DBSS Capture SQL Statements Executed by Third-Party Tools?

Yes. DBSS can audit all the logs and traffic accessible by the agent.

3.16 Can DBSS Be Deployed Off the Cloud?

No. You need to migrate services to the cloud before you can audit them using DBSS.

3.17 Can I Change the VPC of a DBSS Instance?

No. You can unsubscribe from DBSS and purchase it in the desired VPC, or contact technical support to connect the DBSS instance to the desired VPC.

A VPC consists of a private network segment, a route table, and at least one subnet. A VPC uses independent security groups and network ACLs to enhance cloud resource security. For details, see **What Is Virtual Private Cloud?**

- To unsubscribe from and purchase DBSS again, follow the instructions in **How Do I Unsubscribe from DBSS?** and **Purchasing Database Audit**.
- To connect the DBSS instance to the desired VPC, **submit a service ticket**.

3.18 How Do I Interconnect with DBSS Audit Data Storage?

Enable automatic backup in DBSS. Audit data will be backed up to an Object Storage Service (OBS) bucket. For details, see **Backing Up and Restoring Database Audit Logs**.

Then you can interconnect with the audit data storage via OBS APIs. For details, see **API Overview**.

4 Database Audit Agent

4.1 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

4.2 On What Windows OSs 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 OSs:

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows 7
- Windows 10

4.3 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 4-1** provides more details.

Table 4-1 Supported Linux OS versions

System Name	System version
CentOS	• CentOS 6.3 (64bit) • CentOS 6.5 (64bit) • CentOS 6.8 (64bit) • CentOS 6.9 (64bit) • CentOS 7.0 (64bit) • CentOS 7.1 (64bit) • CentOS 7.2 (64bit) • CentOS 7.3 (64bit) • CentOS 7.4 (64bit) • CentOS 7.5 (64bit) • CentOS 7.6 (64bit) • CentOS 7.8 (64bit) • CentOS 7.9 (64bit) • CentOS 8.0 (64bit) • CentOS 8.1 (64bit) • CentOS 8.2 (64bit)
Debian	• Debian 7.5.0 (64bit) • Debian 8.2.0 (64bit) • Debian 8.8.0 (64bit) • Debian 9.0.0 (64bit) • Debian 10.0.0 (64bit)
Fedora	• Fedora 24 (64bit) • Fedora 25 (64bit)
SUSE	• SUSE 11 SP4 (64bit) • SUSE 12 SP1 (64bit) • SUSE 12 SP2 (64bit)
Ubuntu	• Ubuntu 14.04 (64bit) • Ubuntu 16.04 (64bit) • Ubuntu 18.04 (64bit)
Euler	• Euler 2.2 (64bit) • Euler 2.3 (64bit)
Oracle Linux	• Oracle Linux 6.9 (64bit) • Oracle Linux 7.4 (64bit)

4.4 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.

4.5 (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

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

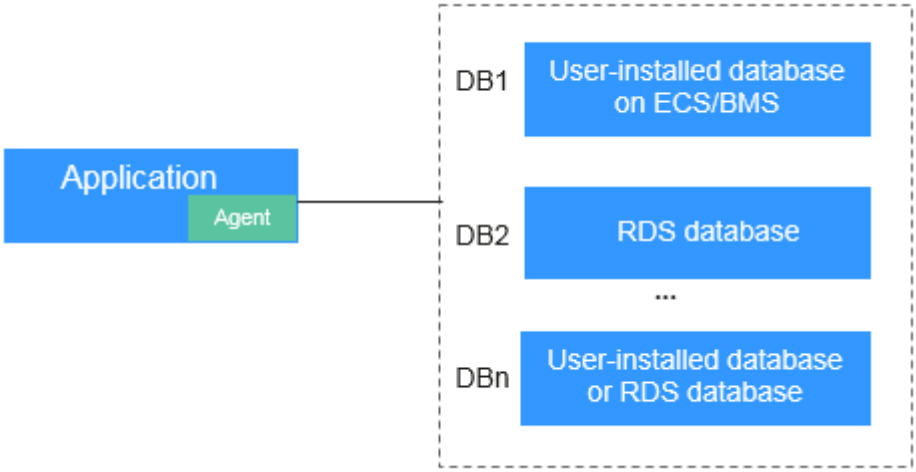
The path for saving agent logs is **/opt/dbss_audit_agent/log/audit_agent.log**.

4.7 When Should I Select an Existing Agent?

Do this if an application is connected to multiple databases, as shown in **Figure 4-1**, 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 4-2**.

After the agent is added, the database can be audited. For details about agent installation, see **How Do I Determine Where to Install an Agent?**

Figure 4-1 An application connected to multiple databases

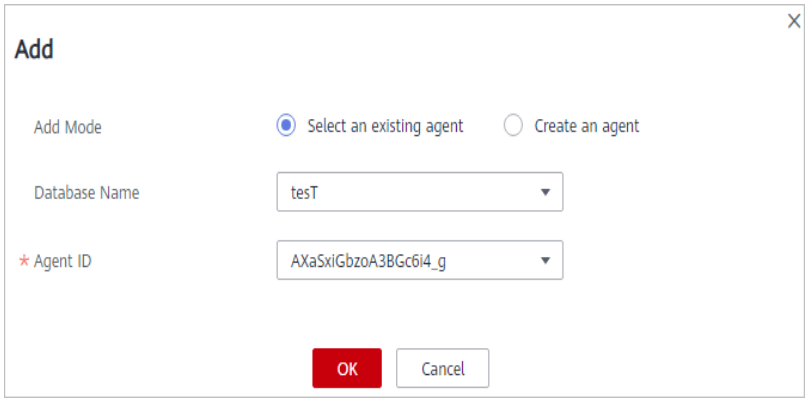


NOTE

Possible combinations of connected databases are:

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

Figure 4-2 Selecting an existing agent



4.8 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 4-3**.

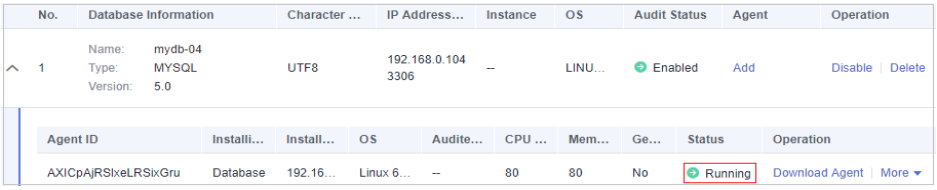
Figure 4-3 Successfully adding an agent

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

Check the agent status after you installed it. For details about how to install the agent, see **Installing an Agent**.

- If the agent status changes to **Running** after the installation, as shown in **Figure 4-4**, it indicates that the agent is running properly.

  Figure 4-4 Agent running properly

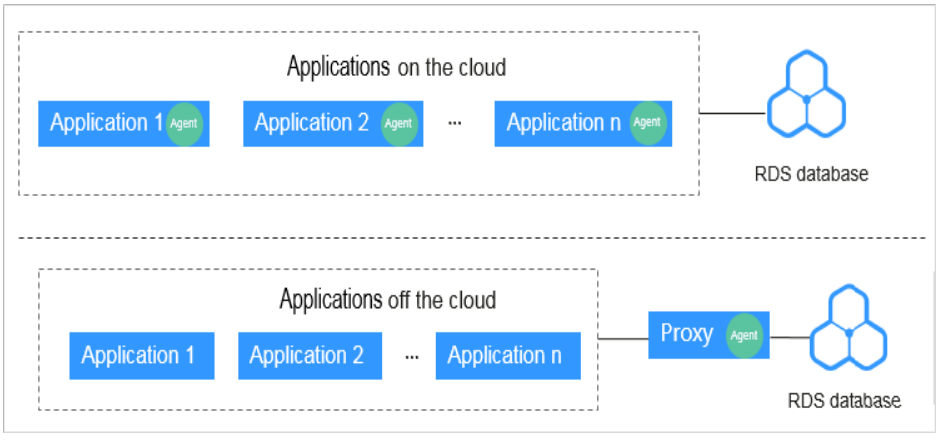
  

- If the agent status is still **Hibernating** after the installation, troubleshoot the problem by following the instructions provided in **What Do I Do If the Communication Between the Agent and Database Audit Instance Is Abnormal?**

4.9 How Do I Deploy the Agent If I Have an RDS Database That Connects to Multiple ECSs?

If multiple applications (ECSs) are connected to the RDS you want to audit, you need to deploy the agent on all the ECSs. See **Figure 4-5**.

Figure 4-5 Multiple applications connecting to one RDS database



After adding a database, perform the following steps to deploy the agent:

1. Add the agent.
   You need to add the agent for each ECS connected to RDS.
   For details, see **Step 2: Add an Agent**.
2. Install the agent.
   After downloading the agent, install it on all the ECSs connected to RDS.
   For details, see **Installing an Agent**.

4.10 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 4-2**. For details about how to install the agent, see **Installing an Agent**.

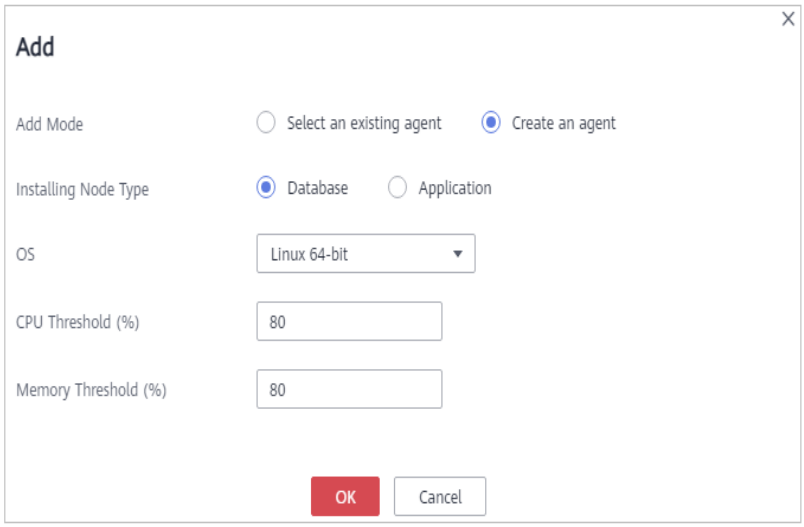
Table 4-2 Nodes to install agents

Node	Scenario	Audit Scope	Configuration
Database	Self-built database on ECS/BMS	All access records of applications that have accessed the database	Set **Installing Node Type** to **Database**, as shown in **Figure 4-6**.
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	• Set **Installing Node Type** to **Application**, as shown in **Figure 4-7**. • If an agent has been installed on a database connected to the same application as the desired database, select **Select an existing agent**.
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 **Installing Node Type** to **Application**, and set **Installing Node IP Address** to the IP address of the proxy.

Adding an Agent

- Database

Figure 4-6 Adding an agent to a database



- Application

Figure 4-7 Adding an agent to an application

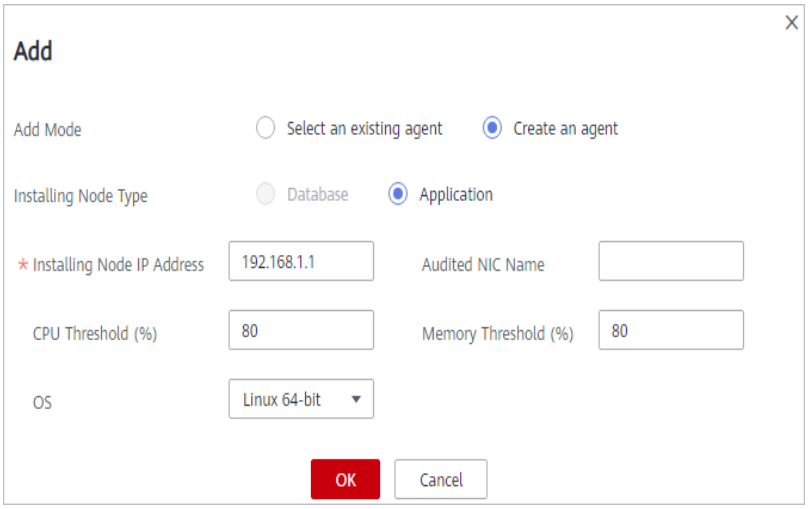
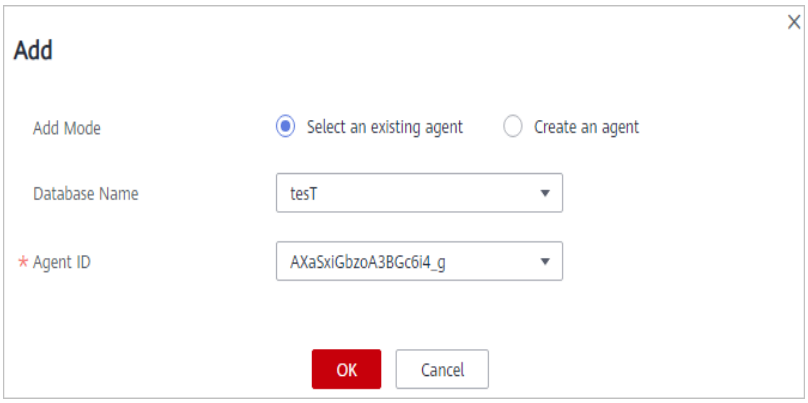


Figure 4-8 Selecting an existing agent

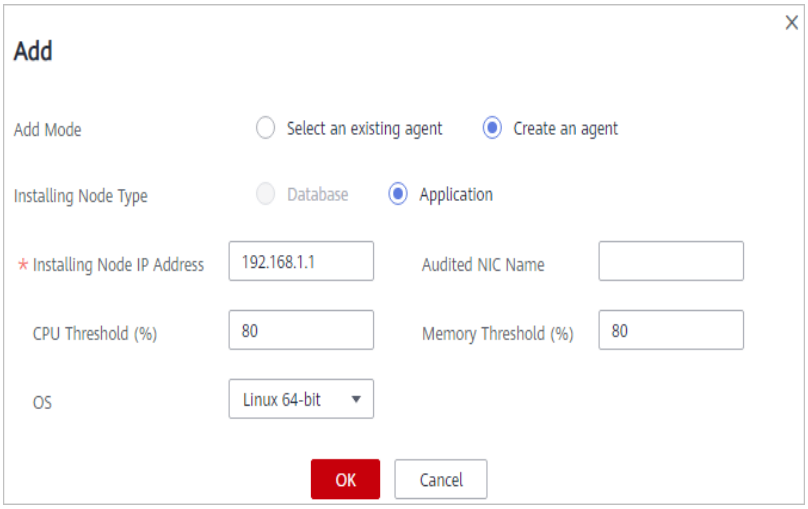


NOTICE

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 4-9 Adding an agent to an application



NOTICE

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

4.11 How Do I Run a Database Audit Agent?

After a database is successfully added and the audit function is enabled, perform the following steps to run the agent program:

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

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

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

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

Step 5 Click ⌄ next to the database to view details of its agent. In the **Operation** column of the agent, click **Download Agent** to download it to your local computer.

Step 6 Install the agent.

For details, see **Installing an Agent**.

----End

4.12 How Do I Check the Status of the Database Audit Agent?

After installing an agent on the node, perform the following steps to view the running status of the agent:

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 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

Windows OS

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

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

----End

4.13 How Do I Download a Database Audit Agent?

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

NOTE

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

Prerequisites

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

Procedure

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

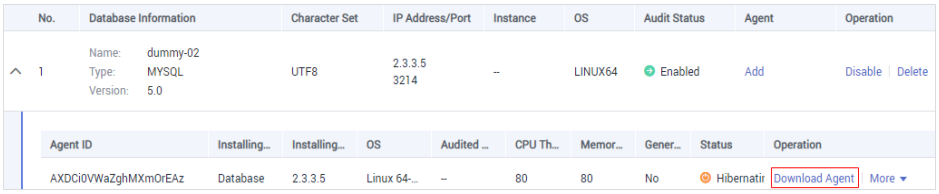
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 Click ⌄ next to the database to view details of its agent. In the **Operation** column of the agent, click **Download Agent**, as shown in **Figure 4-10**, to download an agent installation package.

Figure 4-10 Downloading an agent



Download the agent installation package suitable for your OS.

- Linux OS

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

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

----End

4.14 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

4.15 Can I Modify the CPU and Memory Thresholds of the Agent?

It depends on where the agent is installed.

If the agent is installed on the database side, contact technical support to modify the thresholds.

If the agent is installed on the application side, you can modify the thresholds when installing or reinstalling the agent.

Step 1 Log in to the node where the agent is installed and **uninstall the agent**.

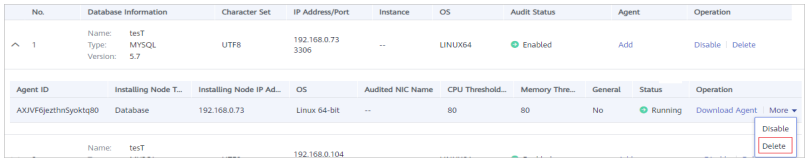
Step 2 Log in to the DBSS console.

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

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

Step 5 Click ⌄ on the left of the database to expand the agent details. In the **Operation** column of the agent, click **Delete**.

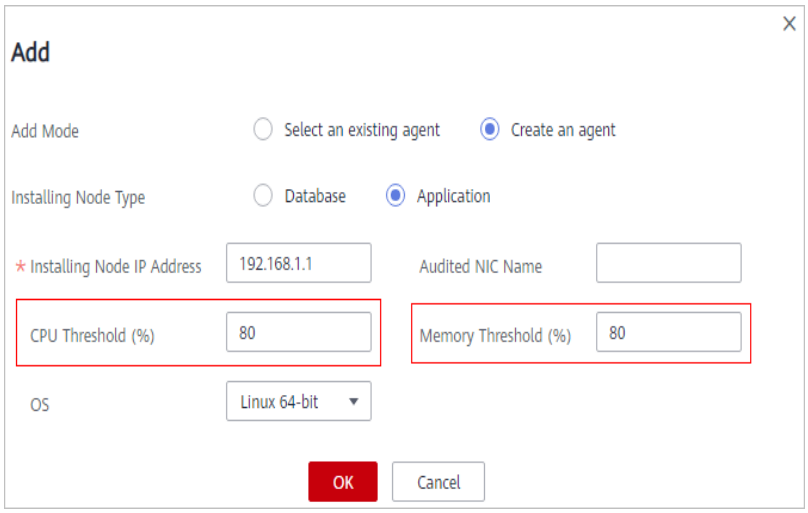
Figure 4-11 Deleting an agent



Step 6 **Add the agent** again and set the CPU and memory thresholds.

The default CPU and memory thresholds are both 80%. If the agent detects that the memory or CPU usage of the server exceeds the preset thresholds, the agent stops running immediately.

Figure 4-12 CPU and memory thresholds



Step 7 **Download the agent**.

Each agent has a unique ID, which is used as the key for connecting to a database audit instance. After you add the agent again and download it, and install the agent again.

Step 8 Install the agent **on Linux OS** or **Windows OS**.

----End

4.16 How Do I Install the Agent (in Linux OS)?

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

Prerequisites

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

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

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

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

After you add 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.

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

Prerequisites

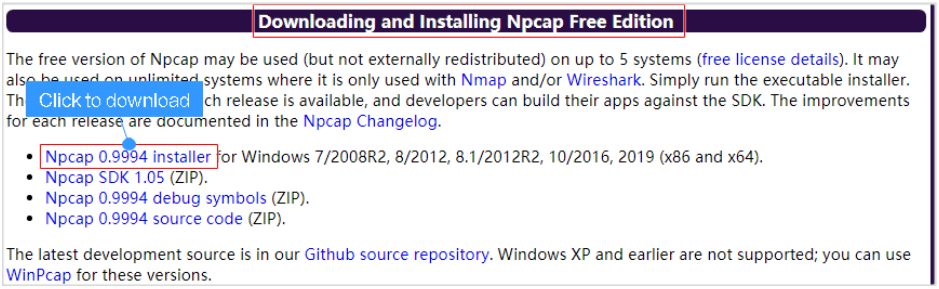
- You have purchased a database audit instance and the **Status** is **Running**.
- You have added an agent to your database.
- You have obtained the agent installation package for the Windows OS.
- The Windows OS version of the target node is supported by the agent. For details about the supported Windows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

Installing an Agent

Step 1 Install Npcap on the Windows server.

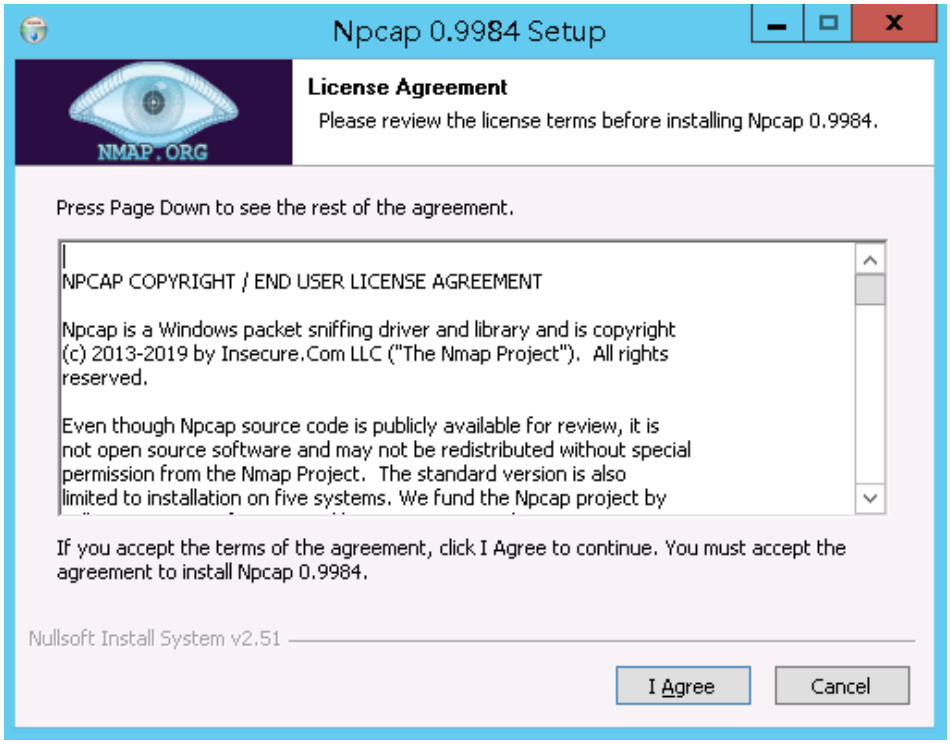
- If Npcap has been installed on the Windows OS, go to **Step 2**.
- If the Npcap has not been installed on the Windows server, perform the following steps:
  a. Download the latest Npcap software installation package from **https://nmap.org/npcap/**.

  Figure 4-13 Downloading npcap

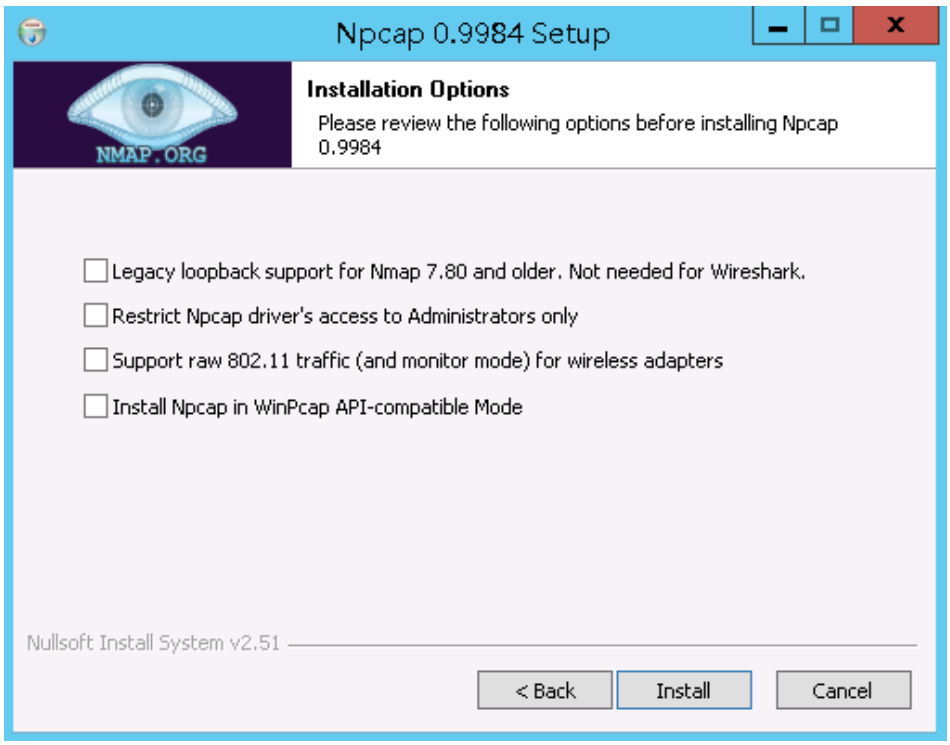
  b. Upload the **npcap-*xxxx*.exe** software installation package to the VM where the agent is to be installed.
  c. Double-click the npcap installation package.
  d. In the displayed dialog box, click **I Agree**, as shown in **Figure 4-14**.

Figure 4-14 Agreeing to install Npcap

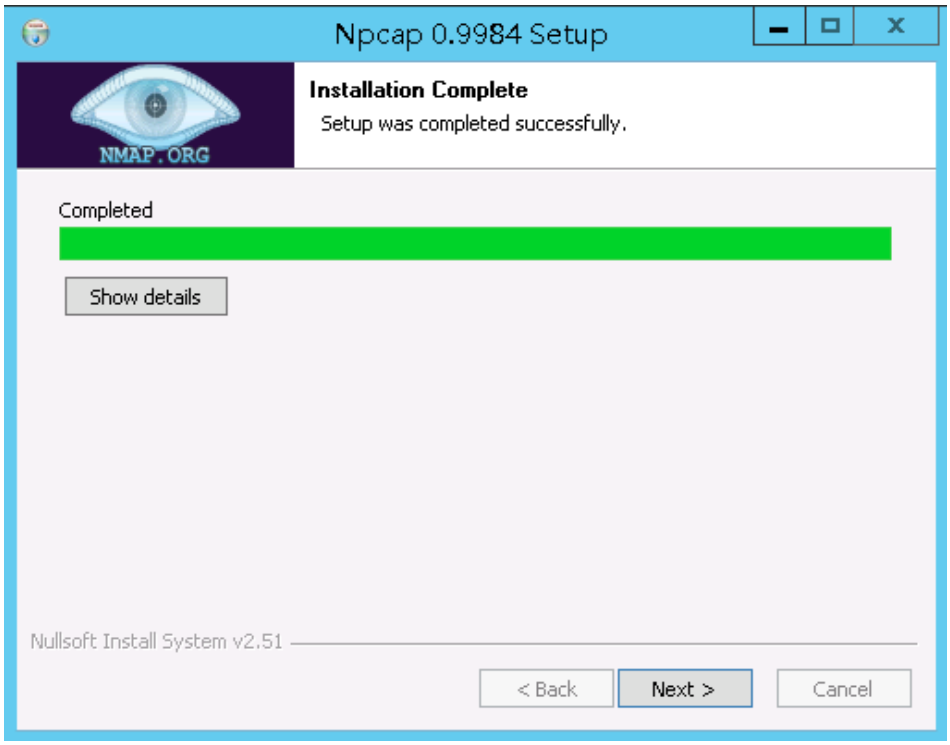


e. In the displayed dialog box, leave all the check boxes unselected and click **Install**, as shown in **Figure 4-15**.

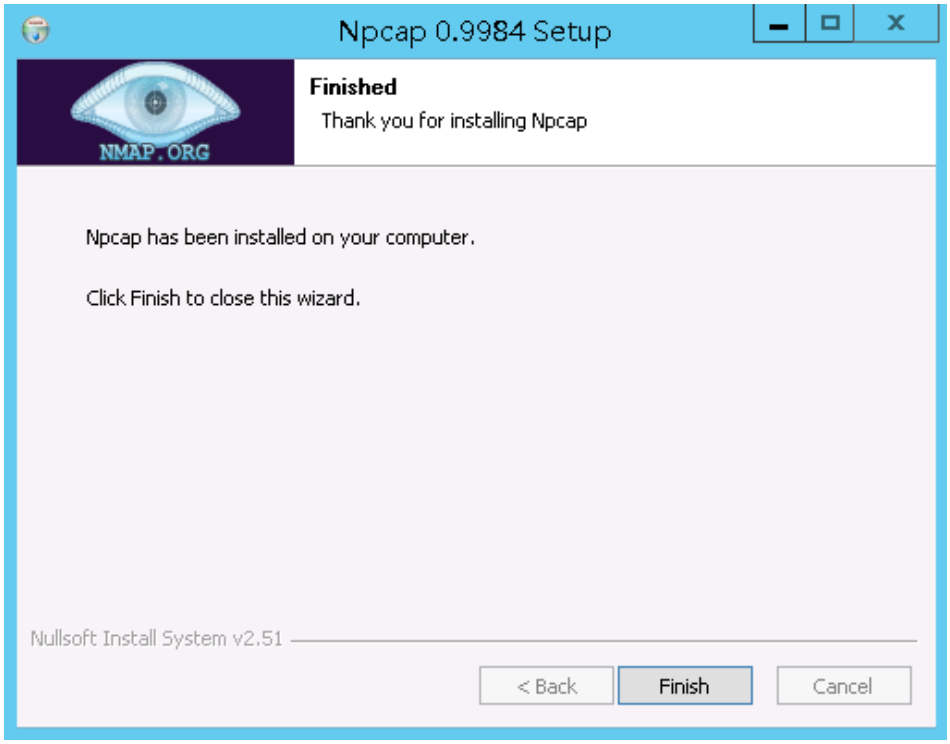
Figure 4-15 Installing Npcap



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



g. Click **Finish**.



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

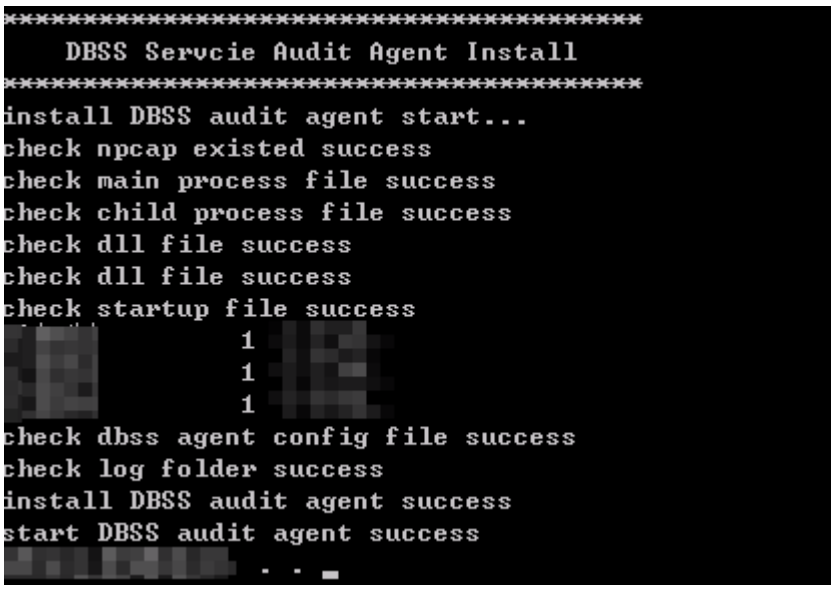
Step 3 Copy the downloaded .zip agent installation package to any directory on the server.

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 4-16** is displayed.

Figure 4-16 Installation completed



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

4.18 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

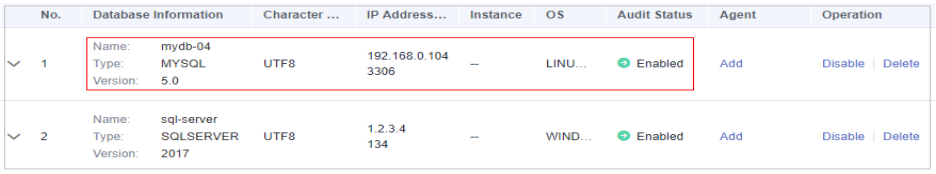
Step 1 **Log in to the management console.**

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

Step 3 In the **Instance** drop-down list, select the instance whose database is to be checked.

Step 4 Check the information about the database to be audited, as shown in **Figure 4-17**.

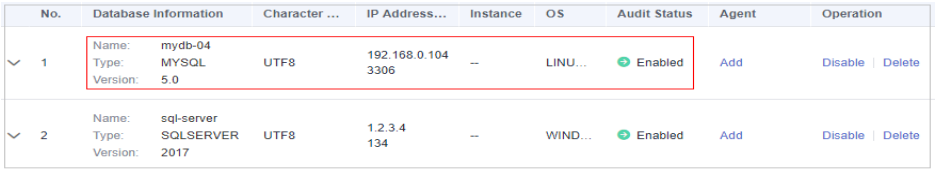
Figure 4-17 Viewing the information about the database to be audited



- If the database information is correct, go to **Step 5**.
- 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 5**.

Step 5 Check the audit status of the database to be audited, as shown in **Figure 4-18**.

Figure 4-18 Checking the database audit status



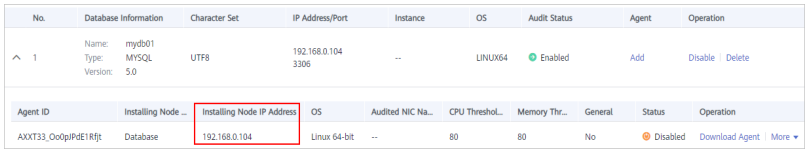
- If **Audit Status** is **Enabled**, go to **Checking the Security Group Rules of the Database Audit Instance**.
- If **Audit Status** is **Disabled**, click **Enable** to enable the database audit function.
  - If the fault is rectified, no further operation is required.
  - If the problem persists, 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 4-19**.

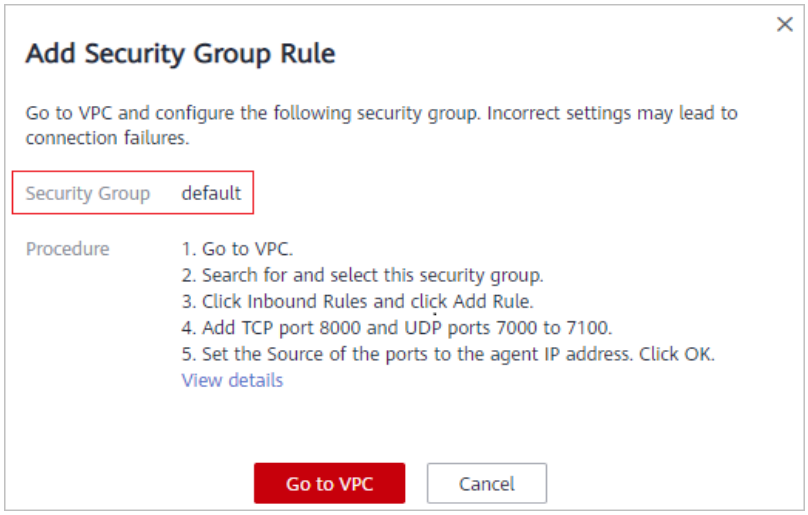
Figure 4-19 Recording the IP address of the installing node



Step 2 Click **Add Security Group**.

Step 3 In the displayed dialog box, record the security group name (for example, **default**) of the database audit instance.

Figure 4-20 Adding a security group rule



Step 4 Click **Go to VPC**.

Step 5 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 6 Click the name of the security group **default**. Click the **Inbound Rules** tab.

Step 7 Check inbound rules of the security group **default**.

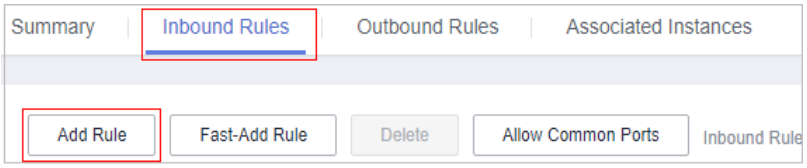
Check whether TCP (port number **8000**) and UDP protocols (port number from **7000** to **7100**) are configured in the inbound rules of the security group for the IP address of the installing node in **Step 1**.

- 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 8**.

Step 8 Add inbound rules for the security group of the database audit instance.

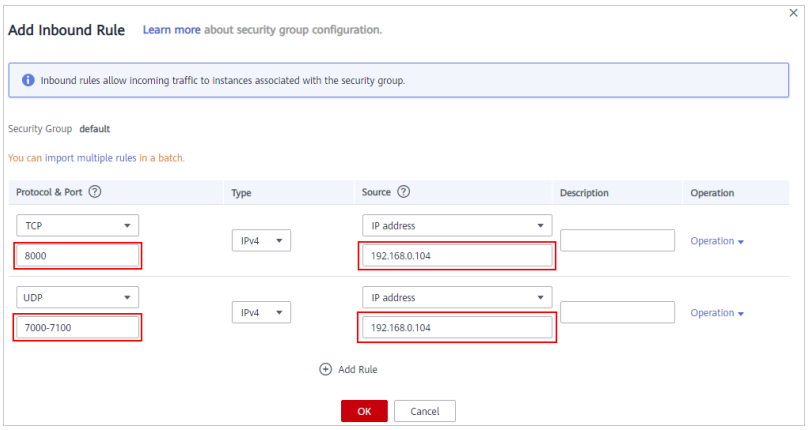
1. Click **Add Rule**, as shown in **Figure 4-21**.

Figure 4-21 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 4-22**.

Figure 4-22 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 (for example, 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, 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.

4.19 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

4.20 What Do I Do If Agent Installation Fails?

Uninstall the agent and reinstall it. Perform the following steps:

1. **Uninstall the agent** from the target database.
2. **Add the agent again**.
3. **Download the agent**.
4. Install the agent **on Linux OS** or **Windows OS**.

4.21 What Do I Do If the Error Message "unsupport this Linux version, please check your Linux version with install document!" Is Displayed During Agent Installation?

This error is reported if you set the installing node IP address to a public IP address when **you added the agent**. In this case, uninstall the agent and reinstall it. Perform the following steps:

1. **Uninstall the agent** from the target database.
2. **Add the agent again**. Set the installing node IP address to a valid intranet IP address.
3. **Download the agent**.
4. Install the agent **on Linux OS** or **Windows OS**.

5 Database Audit Operations

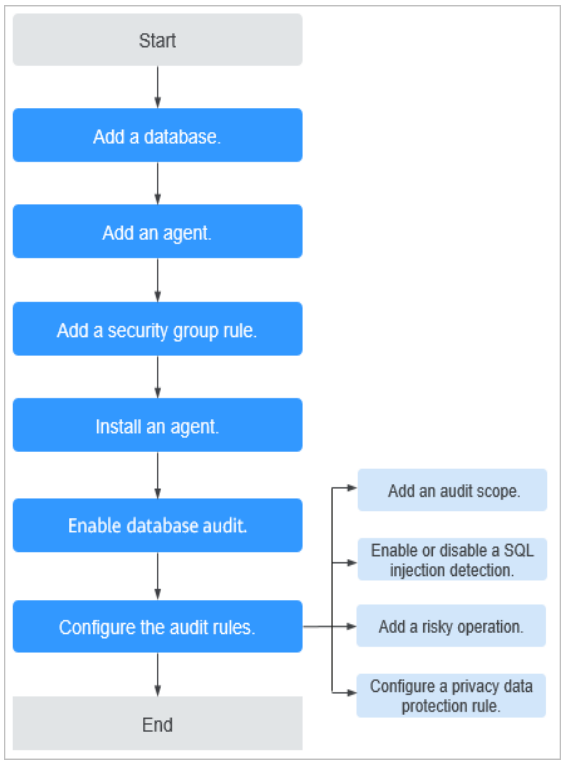
5.1 How Do I Configure Database Audit?

After purchasing a database audit instance, you need to add the database to be audited to the instance and install an agent on the database, application, or proxy side. A database can be audited only after it is connected to a database audit instance.

For easier O&M, you can deploy the database audit agent in a large number of containerized applications or databases in batches. This makes configuration quicker and easier. For details, see **Deploying the Database Audit Agent in a Container**.

Figure 5-1 illustrates the procedure for configuring database audit.

Figure 5-1 Database audit configuration process



For details about how to configure database audit, see:

1. **Add a Database**
2. **Add an Agent**
3. **Add a Security Group Rule**
4. **Install an Agent**
5. **Enable Database Audit**
6. Sections about configuring audit rules:
   - **Adding Audit Scope**
   - **Enabling or Disabling SQL Injection Detection**
   - **Adding Risky Operations**
   - **Configuring Privacy Data Protection Rules**

5.2 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

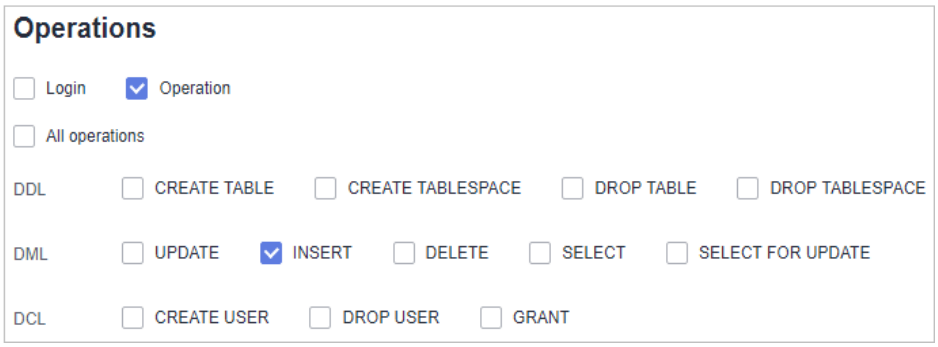
   If information similar to the following is displayed, SSL has been disabled for the MySQL database.
   ```
   SSL:            Not in use
   ```

----End

5.3 How Do I Set the INSERT Audit Policy for Database Audit?

You can add an INSERT audit policy while setting a risky operation, as shown in **Figure 5-2**.

Figure 5-2 Adding an INSERT audit policy



For details, see **Adding Risky Operations**.

5.4 How Do I Verify My Database Audit Configuration?

To verify your database audit configurations after you enabled audit, perform the following steps:

Step 1 Enter an SQL statement (for example, **show databases**) in the node where the agent is installed.

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

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

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

Step 5 Click the **Statements** tab.

Step 6 Click on the right of **Time**, select the start time and end time, and click **Submit**. The SQL statement entered in **Step 1** will be displayed in the list. See **Figure 5-3**.

Figure 5-3 Viewing SQL statements

- If the entered SQL statement is displayed in the SQL statement list, database audit has been correctly configured.
- If the entered SQL statement is not displayed in the SQL statement list, database audit is unavailable. Perform the following operations:
  - Disable database SSL. If SSL is enabled for a database, the database cannot be audited. For details, see **How Do I Disable SSL for a Database?**.
  - Rectify the fault by following the instructions provided in **What Do I Do If the Communication Between the Agent and Database Audit Instance Is Abnormal?**

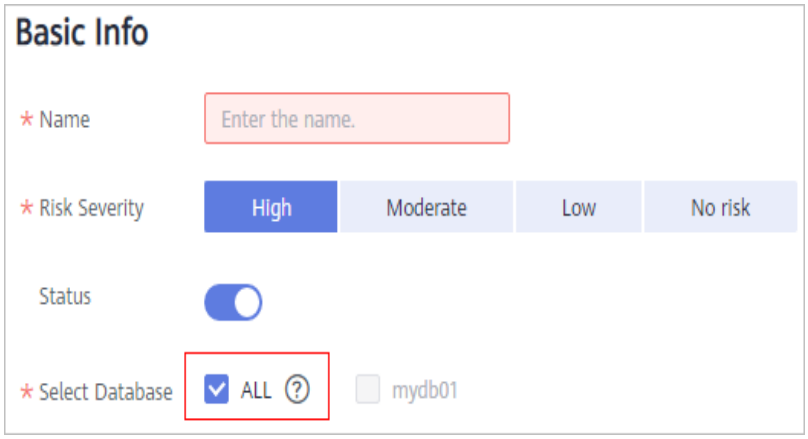
----End

5.5 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 5-4**.

Figure 5-4 Applying risk operation settings to all connected databases



For details, see **Adding Risky Operations**.

5.6 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.**

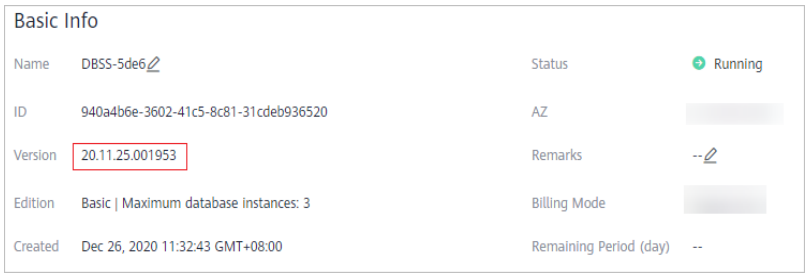
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 View the instance version, as shown in **Figure 5-5**.

Figure 5-5 Viewing the instance version



----End

5.7 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.**

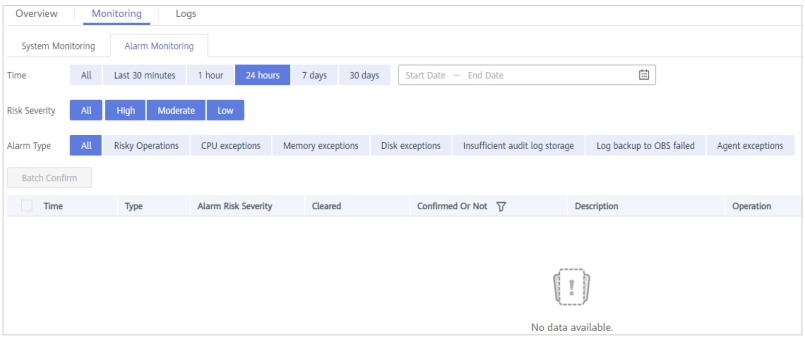
Step 2 Select a region, click , and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 View the alarm information, as shown in **Figure 5-6**.

Figure 5-6 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**, or click to set start time and end time, and click **OK** to view alarms of the specified time range.
- Select **All**, **High**, **Moderate**, or **Low** for **Risk Severity**. Alarms of specified severity are displayed in the list.
- Select an alarm type, and alarms of specified alarm type is displayed in the list.

----End

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

To audit an RDS database accessed by off-cloud PCs through the intranet, you can install the agent on a proxy (for example, a cloud bastion host). Access from the proxy to the database can be audited. Access from applications to the proxy cannot be audited.

For details about agent installation, see **How Do I Determine Where to Install an Agent?**

6 Database Audit Troubleshooting

6.1 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.

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.

For details about how to search for SQL statements, see **Viewing SQL Statement Details**.

- 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.

For details about how to search for SQL statements, see **Viewing SQL Statement Details**.

- 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

6.2 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.**

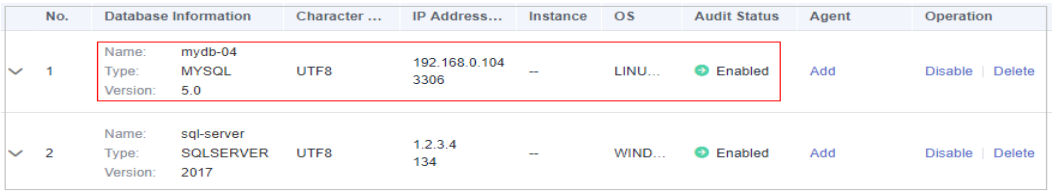
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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 6-1**.

Figure 6-1 Viewing the information about the database to be audited



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**.

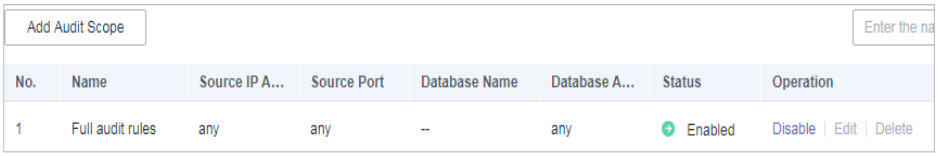
- If **Audit Status** is **Disabled**, click **Enable** to enable the database audit function.
  - If the fault is rectified, no further operation is required.
  - If the problem persists, go to **Checking Audited Database Settings**.

----End

Checking Audited Database Settings

In the navigation tree on the left, choose **Database Audit** > **Rules**. The **Audit Scope** page is displayed. See **Figure 6-2**.

Figure 6-2 Audit scope



- 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 6-3 Normal communication

```
-]# tailf  /opt/dbss_audit_agent/log/audit_agent.log
':37 INFO  [websocket_message_handle.cpp:357] send config data capture result begin...
':37 INFO  [websocket_message_handle.cpp:359] send config data capture result success
':37 INFO  [websocket_message_handle.cpp:136] audit ethernet is: eth0
':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)
':37 INFO  [catch_data_package.cpp:119] init libpcap tool begin...
':37 INFO  [catch_data_package.cpp:155] init libpcap tool success
':37 INFO  [udp_communication.cpp:28] init udp connection begin...
':37 INFO  [udp_communication.cpp:51] init udp connection success!
':37 INFO  [catch_data_package.cpp:167] catch data packet begin...
':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 6-4 Communication error

```
AWdimb74cL5BfUHrp8-t]# 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":"AWdimb74cL5BfUH
':"EulerOS","ostype":"Linux","osver":"3.10.0-327.36.58.4.x86_64","verify":"IHGabvph0aqK6Q+saLeIaIMLRBIA/S37uGRgQqJ
cJUMWkSsz1VSlHZwidlMraDnczItXe4NMiwn//fzcZdj9qeendGh0BIv3CXpdDDzY3SMoUlkfbauolqdMIpwrNw5utJD55id5Qn0vfgunuZJWTc2A
'OQTb2Cli0iEKGHLteQ=="},"code":1,"id":"98c43f29-e302-402a-9e75-321b2f6e86c2","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.

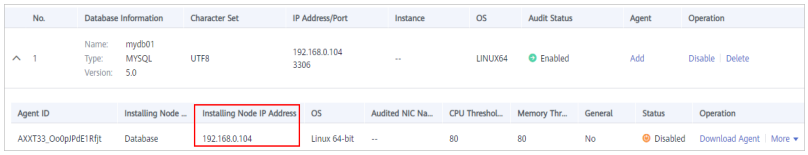
Step 2 In the navigation tree on the left, choose **Database Audit** > **Databases**. The **Databases** page is displayed.

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 6-5**.

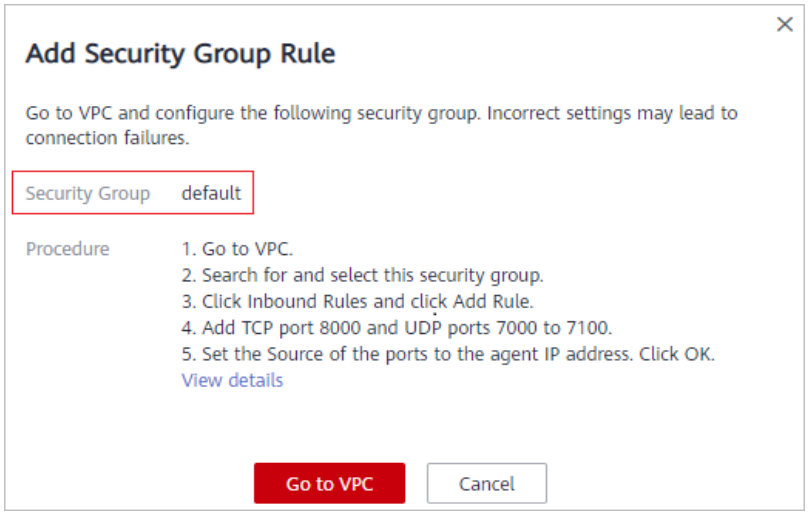
Figure 6-5 Installing node IP address



Step 5 Click **Add Security Group**.

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

Figure 6-6 Adding a security group rule



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 name of the security group **default**. Click the **Inbound Rules** tab.

Step 10 Check the inbound access rules of the security group.

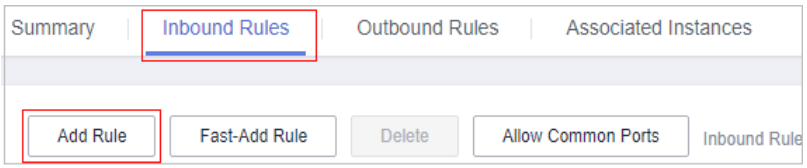
Check whether TCP (port number **8000**) and UDP protocols (port number from **7000** to **7100**) are configured in the inbound rules of the security group for the IP address of the installing node in **Step 4**.

- If the inbound rules of the security group have been configured for the installing node, go to **Verifying the Result**.
- 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.

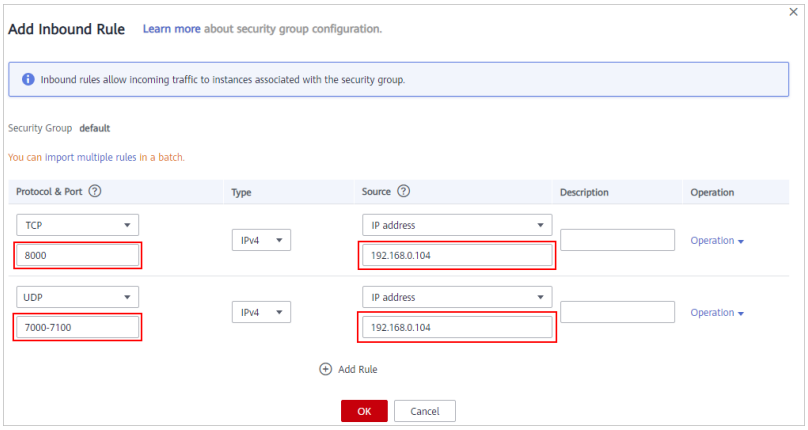
1. On the **Inbound Rules** tab, click **Add Rule**. See **Figure 6-7**.

   Figure 6-7 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 6-5**. See **Figure 6-8**.

Figure 6-8 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.

7 Logs

7.1 Can I Download the Backed Up Database Audit Logs?

Yes.

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.

You can use OBS Browser to download the logs to your local PC.

7.2 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?**

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

The operation logs of database audit are permanently saved.

7.4 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 & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

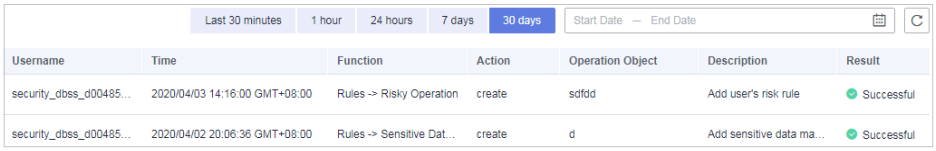
Step 3 In the navigation tree on the left, choose **Instances**.

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

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

Step 6 View the operation logs, as shown in **Figure 7-1**. For more information, see **Table 7-1**.

Figure 7-1 Viewing operation logs



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 7-1 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

7.5 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.

7.6 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 or manually back up audit logs.

NOTICE

A manual backup will back up all your database audit logs. If the number of logs is too large, you are advised to use automatic backup. Daily automatic backup is recommended.

Automatically Backing Up Database Audit Logs

Step 1 Log in to the management console.

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

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

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

Step 5 Click **Configure**. In the displayed dialog box, set the parameters, as shown in Figure 7-2. Table 7-2 describes the parameters.

Figure 7-2 Configure Automatic Backup dialog box

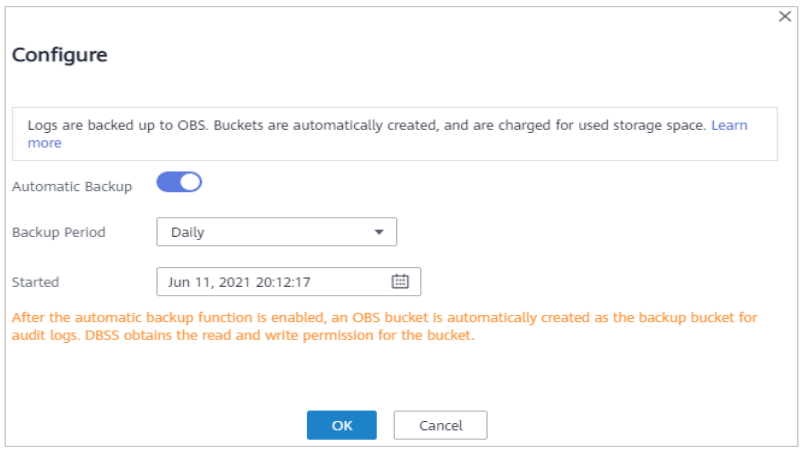


Table 7-2 Parameters

Parameter	Description	Example Value
Automatic Backup	Status of automatic backup • : enabled • : disabled	
Backup Period	Automatic backup period. The options are as follows: • **Daily** • **Weekly** • **Monthly**	Daily
Started	Start time of the backup. Click to configure.	2020/01/14 20:27:08
Estimated Next Time for Backup	Time when the next automatic backup starts	2020/01/15 20:21:29
Access Key ID(AK)	Access key (AK)	-
Secret Access Key(SK)	Secret access key (SK)	-

Step 6 Click **OK**.

----End

Manually Backing Up Database Audit Logs

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

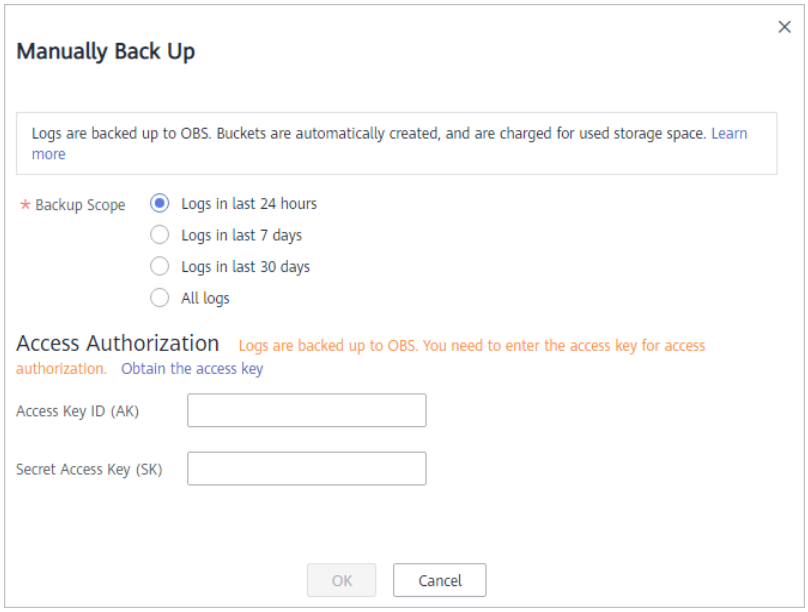
Step 2 Select a region, click , and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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

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

Step 5 Click **Manually Back Up**. In the displayed dialog box, set **Backup Scope**, AK, and SK, as shown in **Figure 7-3**.

Figure 7-3 Manually Back Up dialog box



Step 6 Click **OK**.

----End

7.7 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). For details, see **Backing Up Database Audit Logs**.

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 and billed per use. For details about OBS pricing, see **OBS Pricing Details**.

A Change History

Released On	Description
2021-08-20	This issue is the forty-first official release. Modified FAQs. Added the following sections: **Can DBSS Capture SQL Statements Executed by Third-Party Tools?** **Can DBSS Be Deployed Off the Cloud?** **Can I Change the VPC of a DBSS Instance?** **How Do I Interconnect with DBSS Audit Data Storage?**
2021-07-15	This is the fortieth official release. Changed the menu item **Security** to **Security & Compliance** on the console.
2021-06-29	This is the thirty-ninth official release. Added the following sections: **Does DBSS Support Real-Time Data Masking?** **Can DBSS Audit Databases Across Subnets?** **What Do I Do If Agent Installation Fails?** **What Do I Do If the Error Message "unsupport this Linux version, please check your Linux version with install document!" Is Displayed During Agent Installation?**
2021-04-19	This is the thirty-eighth official release. Added agent support for CentOS 7.9, CentOS 8.1, CentOS 8.2, and Debian 10.0.0 in **On What Linux OSs Can I Install the Agent?**
2021-04-01	This is the thirty-seventh official release. Deleted content related to database protection.

Released On	Description
2021-03-22	This is the thirty-sixth official release. • Added **How Many Resources Are Consumed by an Agent When It Runs on a Node?** • Optimized descriptions in **How Do I Configure Database Audit?** • Added **Disabling ForceEncryption for the SQL Server Protocol** in **Database Audit Is Running Properly But Generates No Audit Records**.
2021-02-25	This issue is the thirty-fifth official release. Added description about allowing pop-ups browsers in **How Do I Obtain the DBSS Sales License?**
2021-01-19	This is the thirty-fourth official release. Added **Can Database Audit Logs Be Directly Saved to OBS?**.
2020-12-18	This issue is the thirty-third official release. • Optimized the description about adding inbound security group rules in **What Do I Do If the Communication Between the Agent and Database Audit Instance Is Abnormal?**. • Optimized the description about adding inbound security group rules in **Database Audit Is Unavailable**.
2020-08-31	This issue is the thirty-second official release. Added the link for downloading the sales license in **How Do I Obtain the DBSS Sales License?**.
2020-07-20	This is the thirty-first official release. Added the description of backup logs in **How Do I Back Up the Database Audit Logs?**.
2020-06-29	This is the thirtieth official release. • Optimized descriptions in **How Do I Renew Database Audit?** • Optimized descriptions in **How Do I Unsubscribe from DBSS?**
2020-06-08	This is the twenty-ninth official release. Optimized descriptions in **If I Use Middleware at the Service Side, Will It Affect Database Audit?**.
2020-05-20	This is the twenty-eighth official release. Added **If I Use Middleware at the Service Side, Will It Affect Database Audit?**

Released On	Description
2020-04-22	This is the twenty-seventh official release. Added the support for CentOS 7.6 (64-bit) in **On What Linux OSs Can I Install the Agent?**.
2020-04-21	This is the twenty-sixth official release. Added "How Do I Obtain the DBSS Sales License?"
2020-03-16	This is the twenty-fifth official release. Adjusted the document structure, and added the following sections: • **Can I Modify the CPU and Memory Thresholds of the Agent?** • **How Do I Install the Agent (in Linux OS)?** • **How Do I Install the Agent (in Windows OS)?** • **What Do I Do If the Communication Between the Agent and Database Audit Instance Is Abnormal?**
2020-03-03	This is the twenty-fourth official release. Modified the description about audit resource consumption in "Does My DBSS Purchase on DeC Consume DeC Resources?"
2020-02-21	This is the twenty-third official release. • Added **On What Windows OSs Can I Install the Agent?** Modified the description about database audit for Windows OS. • What OSs Can Use the Audit Function of DBSS in Direct or Bypass Mode? • **What Is the Process Name of the Database Audit Agent?** • **How Do I Download a Database Audit Agent?** • **How Do I Check the Status of the Database Audit Agent?** • **How Do I Uninstall a Database Audit Agent?**

Released On	Description
2020-01-06	This is the twenty-second official release. Added the following FAQs: • Can I Audit Additions and Modifications If I Selected the Modify Check Box in the Monitored actions Area? • What Do I Do If a Message Is Displayed, Indicating that the Remote Log Database Is Disconnected and Data Is Unavailable? • **Can Database Audit Be Used Across AZs?** • How Do I Deploy the Agent If I Have an RDS Database That Connects to Multiple ECSs?
2019-12-23	This is the twenty-first official release. Updated console screenshots.
2019-11-30	This is the twentieth official release. Added the following FAQs: • **Which Functions Do the Database Audit Agent Provide?** • **On What Windows OSs Can I Install the Agent?** • **On What Linux OSs Can I Install the Agent?**

Released On	Description
2019-11-12	This is the nineteenth official release. Added the following FAQs: • What Functions Does Database Protection Provide? • **How Does Database Audit Process Logs?** • **Is the Database Audit Function Available to Users Other Than the Buyer?** • **How Do I Configure Database Audit?** • **How Do I Download a Database Audit Agent?** • **Can Applications Using TLS Connections Be Audited?** • **What Do I Do If the Database Audit Agent Is Hibernating?** • **How Do I Verify My Database Audit Configuration?** • **How Do I Check the Operation Logs of Database Audit?** • Is Port 5000 Automatically Added to Security Groups for Database Protection? • **How Do I Audit an RDS Database Accessed through Intranet (by Applications Off the Cloud)?** • What Do I Do If "Invalid IP address, port number or instance name" Is Displayed? • How Do I Purchase DBSS for RDS?

Released On	Description
2019-11-05	This is the eighteenth official release. Added the following FAQs: • What OSs Can Use the Audit Function of DBSS in Direct or Bypass Mode? • **Does DBSS Upload Logs Through the Internet or Intranet?** • **Does Database Audit (in Bypass Mode) Affect My Services?** • **Why I Cannot Preview the Database Security Audit Report Online?** • Can I Query All DDL or DML Statements at a Time on the Database Protection Page? • Can I Change the Network Segment of a Database Protection Instance? • Do I Need to Configure Multiple Log Storage Locations for Database Protection? • Can Database Protection Be Used Across Regions? • What IP Address of a Database Is Accessed by HexaTier? • **How Do I Set Database Audit Rules for All Databases?** • **How Do I Set the INSERT Audit Policy for Database Audit?** • **Which Subnet Should I Choose When Purchasing an Instance?**
2019-10-24	This is the seventeenth official release. • Added **How Do I Determine Where to Install an Agent?**. • Added section **How Do I Disable SSL for a Database?** • Added **When Should I Select an Existing Agent?**
2019-10-16	This is the sixteenth official release. Added **Can Database Audit Be Used Across Regions?**
2019-09-06	This is the fifteenth official release. • Added **Does My DBSS Purchase on DeC Consume DeC Resources?** • Added "What Are the Differences Between Database Audit and the Audit Function of Database Protection?"

Released On	Description
2019-08-29	This is the fourteenth official release. • Added "How Do I Modify the Security Group of a Database Protection Instance?" • Added "How Do I Log In to HexaTier?"
2019-08-26	This is the thirteenth official release. Added **What Are Regions and AZs?**
2019-08-21	This is the twelfth official release. Modified portal description in chapter "FAQs".
2019-08-01	This is the eleventh official release. Updated screenshots and descriptions in FAQ **How Do I Renew DBSS?**
2019-07-30	This is the tenth official release. Added FAQ **What Editions of DBSS Are There?**
2019-07-22	This is the ninth official release. • Added "How Do I Purchase Tailored DBSS Instances on the RDS DB Instance Purchase Page?" • Added **How Do I Renew DBSS?** • Added **How Do I Unsubscribe from DBSS?**
2019-06-14	This is the eighth official release. Modified descriptions in the FAQ "What Do I Do If I Forget the Initial Login Password for HexaTier?"
2019-05-16	This is the seventh official release. Modified FAQ **Which Regions Is DBSS Available In?**
2019-01-15	This is the sixth official release. Revised the document outline and optimized the content description.

Released On	Description
2018-12-25	This is the fifth official release. Added the following FAQs: • **What Is Database Audit?** • **Which Scenarios Does Database Audit Apply To?** • **What Databases Does Database Audit Support?** • **Which OSs Does Database Audit Support?** • **Does Database Audit Support Bidirectional Audit?** • **What Is the Process Name of the Database Audit Agent?** • **Where Are the Logs of the Database Audit Agent Saved?** • **How Long Are the Operation Logs of Database Audit Saved by Default?** • **How Long Is the Audit Data of Database Audit Stored by Default?** • **Can the Audit Logs of Database Audit Be Backed Up?** • **Can the Operation Logs of Database Audit Be Migrated?** • **How Long Do I Receive an Alarm When an Exception Occurs in Database Audit?** • **Is the Total Number Of Alarms Every Day the Same as that of Emails?** • **How Do I Check the Status of the Database Audit Agent?** • **How Do I Check the Version of Database Audit?** • **How Do I View All Alarms in Database Audit?**
2018-10-15	This is the fourth official release. Optimized some descriptions.
2018-07-19	This is the third official release. Added **Which Regions Is DBSS Available In?**

Released On	Description
2017-11-02	This is the second official release. ● Added "What Fine-Grained Functions Does DBSS Provide?" ● Added "What Is the Configuration Process on HexaTier?" ● Added "Does DBSS Require Rights of User root from a MySQL Database?" ● Added "Can I Import Logs Generated by DBSS to My Own Log Analysis Platform?" ● Added "What Should I Configure on My Databases for Database Protection?" ● Added "What Is the Difference Between DBSS and WAF in SQL Injection Prevention?" ● Added "Will My Raw Data in the Database Changed by the Dynamic Data Masking Function?" ● Added "How Will DBSS Affect My Service Latency?"
2017-09-15	This is the first official release.