Database Security Service

FAQs

Issue	21
Date	2024-04-10

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Product Consulting

1.1 What Is Database Audit?

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

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.

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 1-1 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.

1.3 What Editions Does DBSS Provide?

Database audit provides professional and advanced editions.

Table 1-2 describes the database audit editions.

Table 1-2 Database audit editions

Edition	Maximum Databases	System Resource	Performance
Professional	6	- CPU: 8 vCPUs - Memory: 32 GB - Hard disk: 1,084 GB	- Peak QPS: 6,000 queries/second - Database load rate: 7.2 million statements/hour - Stores 600 million online SQL statements. - Stores 10 billion archived SQL statements.
Advanced	30	- CPU: 16 vCPUs - Memory: 64 GB - Hard disk: 2,108 GB	- Peak QPS: 30,000 queries/second - Database load rate: 10.8 million records/hour - Stores 1.5 billion online SQL statements. - Stores 60 billion archived SQL statements.

1.4 What Databases on Huawei Cloud 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.

1.5 What Databases Does DBSS Support?

DBSS supports the following HUAWEI CLOUD databases:

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

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

When you purchase a database audit instance, 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.

1.7 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.

1.8 Does Database Audit Support On-premises or Non-Huawei Cloud Databases?

Currently, database audit cannot audit on-premises databases and non-Huawei cloud databases. It supports database audit in bypass mode for the following databases on the cloud:

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

For more information, see **Supported Database Types**

1.9 What Are Regions and AZs?

Concepts

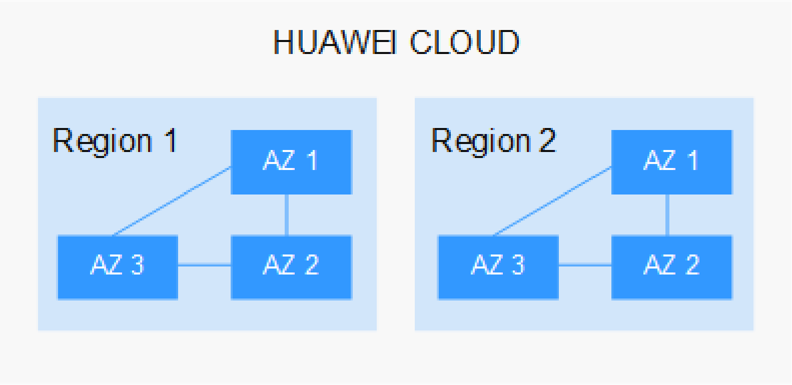
A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- 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.

  - If you or your users are in the Asia Pacific region and outside the Chinese mainland, select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If you or your users are in Africa, select the **AF-Johannesburg** region.
  - If you or your users are in Latin America, select the **LA-Santiago** 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**.

1.10 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 **Managing Privacy Data Protection Rules**.

1.11 Can DBSS Audit Databases Across Subnets?

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

1.12 Is There Any Restriction on the Gateway IP Address of DBSS Audit Instances?

User servers cannot occupy the gateway IP address of DBSS audit instances.

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 Why Do I Need to Select a VPC When Buying an Instance?

For a DBSS instance to edit an off-cloud database, the DBSS agent needs to be deployed on the database and in the same VPC as the instance. If the DBSS instance and the agent are in different VPCs, DBSS cannot audit the database.

2.3 How Many Database Audit Instances Can I Purchase in the Same Region?

- **Basic**: supports up to three database instances.
- **Professional**: supports up to six database instances.
- **Advanced**: supports up to 30 database instances.

2.4 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**.

2.5 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 DBSS 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 Click **Renew** in the row containing the target instance.

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

----End

2.6 How Do I Unsubscribe from DBSS?

You can unsubscribe from a DBSS instance on the console. DBSS currently supports yearly and monthly subscription. Purchased DBSS instances cannot be deleted, and their specifications cannot be changed.

Impact on the System

After you unsubscribed from a DBSS instance, its audit records and logs will be deleted. Audit logs that have been backed up to the OBS bucket are not deleted.

Prerequisites

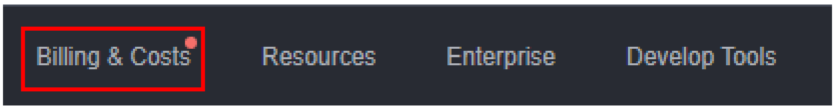
- The account for logging in to the management console has been granted the DBSS System Administrator, ECS Administrator, VPC Administrator, and BSS Administrator roles.
- You have purchased a database audit instance.

Procedure

Step 1 Log in to the management console.

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

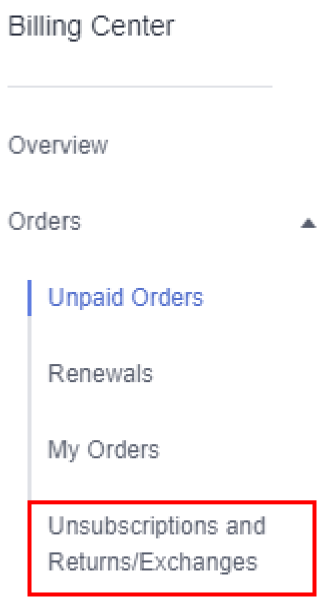
Figure 2-1 Billing & Costs



Step 3 In the navigation pane on the left, choose **Orders** > **Unsubscriptions and Returns/Exchanges**.

For details about unsubscription, see **Unsubscription Rules**. To purchase the service again after unsubscription, follow the instructions provided in **Purchasing Database Audit**.

Figure 2-2 Unsubscriptions and Returns/Exchanges



----End

3 Functions

3.1 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, and the database to be audited is deployed in AZ2 or AZ3 in the region, you can use the database audit you purchased.

3.2 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.

3.3 Is the Database Audit Function Available to Users Other Than the Buyer?

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**.

3.4 What Are the Functions of Database Audit?

Database audit is deployed in out-of-path pattern and can perform flexible audit on databases built on ECS, BMS, and RDS 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.

3.5 Supported Database Types

Database audit supports the following database types and versions.

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

Database Type	Edition
MySQL	• 5.0, 5.1, 5.5, 5.6, 5.7 • 8.0 (8.0.11 and earlier) • 8.0.20 • 8.0.23 • 8.0.25
Oracle (The Oracle database uses closed-source protocol and has complex adaptation versions. If you need to audit the Oracle database, contact customer service.)	• 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	Edition
PostgreSQL	● 7.4 ● 8.0 8.0, 8.1, 8.2, 8.3, 8.4 ● 9.0 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6 ● 10.0 10.0, 10.1, 10.2, 10.3, 10.4, 10.5 ● 11.0 ● 12.0 ● 13.0 ● 14.0
SQL Server	● 2008, 2008R2 ● 2012 ● 2014 ● 2016 ● 2017
DWS	● 1.5 ● 8.1
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8
Gbase XDM Cluster	V8.0
Greenplum	V6.0
HighGo	V6.0
GaussDB(for MYSQL)	MySQL 8.0
GaussDB	1.4 Enterprise Edition
DAMENG	DM8
KINGBASE	V8
MongoDB	V5.0
DDS	4.0
Hbase (Supported by CTS instance 23.02.27.182148 and later versions)	1.3.1 2.2.3

Database Type	Edition
Hive	1.2.2 2.3.9 3.1.2 3.1.3

3.6 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 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)

System Name	System version
Fedora	● Fedora 24 (64bit) ● Fedora 25 (64bit) ● Fedora 29 (64bit) ● Fedora 30 (64bit)
OpenSUSE	● SUSE 13 (64bit) ● SUSE 15 (64bit) ● SUSE 42 (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) ● Ubuntu 20.04 (64-bit)
EulerOS	● Euler 2.2 (64bit) ● Euler 2.3 (64bit) ● Euler 2.5 (64bit)
OpenEuler	● OpenEuler 20.03 (64bit)
Oracle Linux	● Oracle Linux 6.9 (64bit) ● Oracle Linux 7.4 (64bit)
Red Hat	● Red Hat Enterprise Linux 7.4 (64bit) ● Red Hat Enterprise Linux 7.6 (64bit)
NeoKylin	● NeoKylin 7.0 (64bit)
Kylin	● Kylin Linux Advanced Server release V10 (64bit)
Uniontech OS	● Uniontech OS Server 20 Enterprise (64bit)
Huawei Cloud Euler	● Huawei Cloud Euler 2.0 (64bit)
KylinSec	● KylinSec 3.4 (64bit)

- The following Windows OSs are supported:
  - Windows Server 2008 R2 (64bit)
  - Windows Server 2012 R2 (64bit)
  - Windows Server 2016 (64bit)
  - Windows Server 2019 (64bit)
  - Windows 7 (64bit)

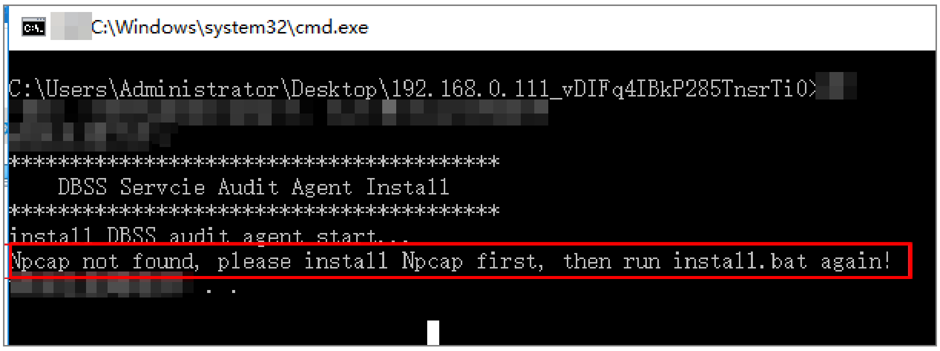
– Windows 10 (64bit)

NOTE

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

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

Figure 3-1 Npcap not found



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

3.7 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.

3.8 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 **Creating a VPC Peering Connection with Another VPC in Your Account**.

3.9 Can Applications Using TLS Connections Be Audited?

No. Applications using TLS are encrypted.

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

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

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

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

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

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

Table 3-3 Database audit editions

Edition	Maximum Databases	System Resource	Performance
Professional	6	● CPU: 8 vCPUs ● Memory: 32 GB ● Hard disk: 1,084 GB	● Peak QPS: 6,000 queries/second ● Database load rate: 7.2 million statements/hour ● Stores 600 million online SQL statements. ● Stores 10 billion archived SQL statements.
Advanced	30	● CPU: 16 vCPUs ● Memory: 64 GB ● Hard disk: 2,108 GB	● Peak QPS: 30,000 queries/second ● Database load rate: 10.8 million records/hour ● Stores 1.5 billion online SQL statements. ● Stores 60 billion archived SQL statements.

NOTE

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

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

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

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 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:

- **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 **submit a service ticket**submit a service ticket 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?**

- (Recommended) Unsubscribe from the DBSS instance by referring to **How Do I Unsubscribe from DBSS?** and then **purchase the database audit instance** in the desired VPC.
- To connect the DBSS instance to the desired VPC, **submit a service ticket**submit a service ticket.

3.18 How Do I Interconnect with DBSS Audit Data Storage?

You can enable automatic backup in DBSS to back up audit data to OBS buckets.

> NOTE
>
> Automatic backup requires fine-grained OBS authorization. For details, see **Backing Up and Restoring Database Audit Logs**.

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

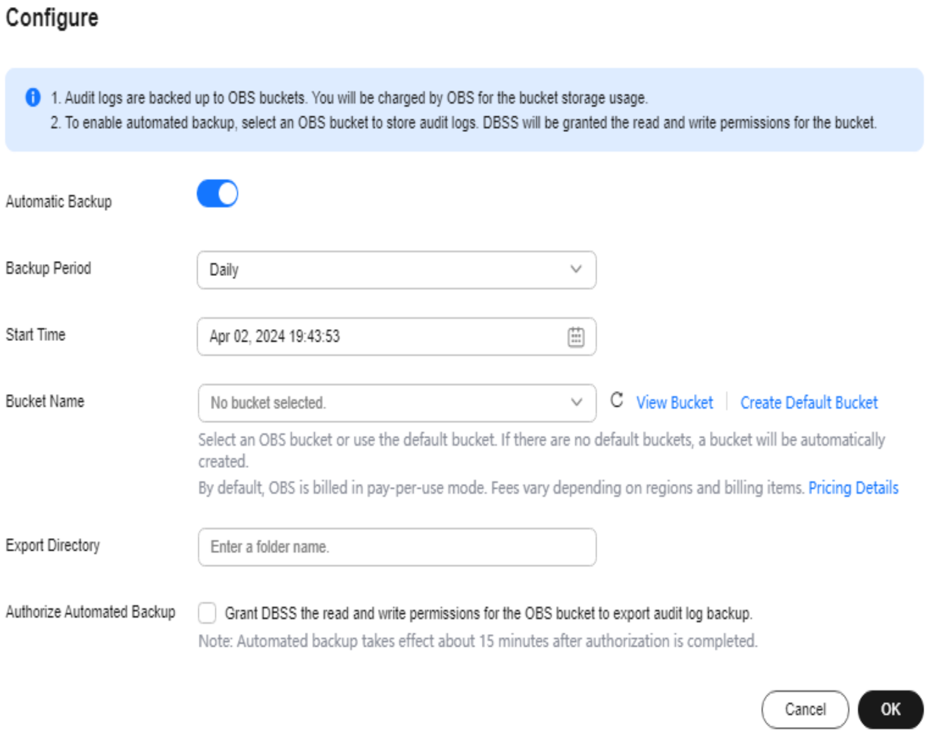
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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 **Modify Automated Backup Settings**. In the displayed dialog box, set the auto backup parameters. **Table 3-4** describes the parameters.

Figure 3-2 Configure Automatic Backup dialog box



Configure

1. Audit logs are backed up to OBS buckets. You will be charged by OBS for the bucket storage usage.
2. To enable automated backup, select an OBS bucket to store audit logs. DBSS will be granted the read and write permissions for the bucket.

Automatic Backup: ◉

Backup Period: Daily

Start Time: Apr 02, 2024 19:43:53

Bucket Name: No bucket selected.

Select an OBS bucket or use the default bucket. If there are no default buckets, a bucket will be automatically created.

By default, OBS is billed in pay-per-use mode. Fees vary depending on regions and billing items. Pricing Details

Export Directory: Enter a folder name.

Authorize Automated Backup: □ Grant DBSS the read and write permissions for the OBS bucket to export audit log backup.

Note: Automated backup takes effect about 15 minutes after authorization is completed.

Table 3-4 Parameters

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

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

Step 6 Click **OK**.

NOTE

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

----End

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

3.19 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.

4 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 Versions Can I Install the Agent?

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

The agent can be installed on the following Windows versions:

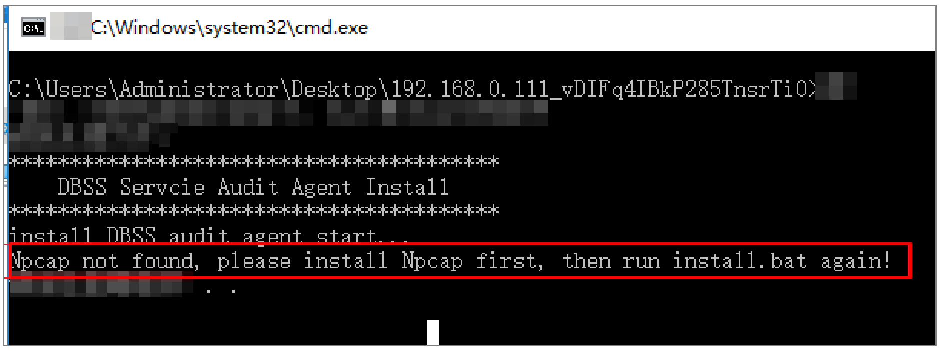
- Windows Server 2008 R2 (64bit)
- Windows Server 2012 R2 (64bit)
- Windows Server 2016 (64bit)
- Windows Server 2019 (64bit)
- Windows 7 (64bit)
- Windows 10 (64bit)

NOTE

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

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

Figure 4-1 Npcap not found



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

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

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 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)

System Name	System version
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) ● Fedora 29 (64bit) ● Fedora 30 (64bit)
OpenSUSE	● SUSE 13 (64bit) ● SUSE 15 (64bit) ● SUSE 42 (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) ● Ubuntu 20.04 (64-bit)
EulerOS	● Euler 2.2 (64bit) ● Euler 2.3 (64bit) ● Euler 2.5 (64bit)
OpenEuler	● OpenEuler 20.03 (64bit)
Oracle Linux	● Oracle Linux 6.9 (64bit) ● Oracle Linux 7.4 (64bit)
Red Hat	● Red Hat Enterprise Linux 7.4 (64bit) ● Red Hat Enterprise Linux 7.6 (64bit)
NeoKylin	● NeoKylin 7.0 (64bit)
Kylin	● Kylin Linux Advanced Server release V10 (64bit)
Uniontech OS	● Uniontech OS Server 20 Enterprise (64bit)
Huawei Cloud Euler	● Huawei Cloud Euler 2.0 (64bit)
KylinSec	● KylinSec 3.4 (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?

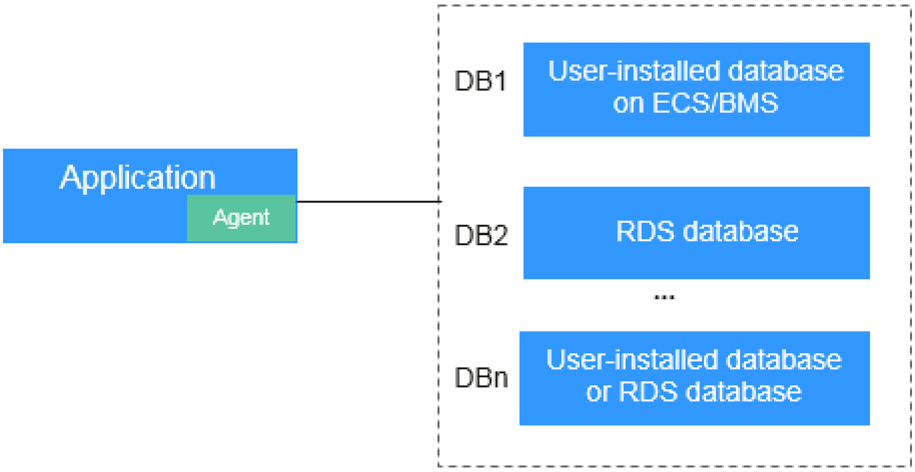
The path for saving agent logs is **/opt/dbss_audit_agent/log/audit_agent.log**.

4.7 When Should I Select an Existing Agent?

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

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 4-2 An application connected to multiple databases


Application
Agent
DB1
User-installed database on ECS/BMS
DB2
RDS database
...
DBn
User-installed database or RDS database

NOTE

Possible combinations of connected databases are:

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

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**.

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

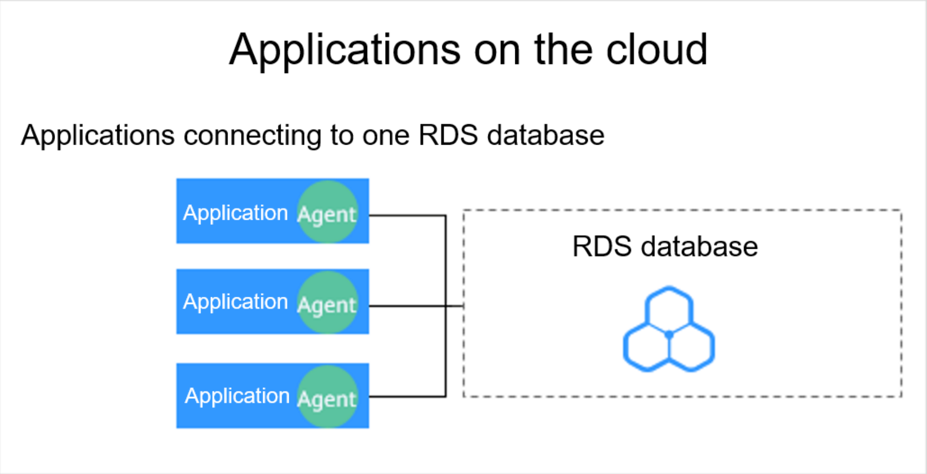
Check the agent status after you installed it. For details about how to install the Agent, see **Installing the Agent**.

- If the agent status changes to **Running** after the installation, it indicates that the agent is 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 4-3**.

Figure 4-3 Multiple applications connecting to one RDS database


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

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 the 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**.

Node	Scenario	Audit Scope	Configuration
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**. ● 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
- Application

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

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 an instance from the **Instance** drop-down list.

Step 3 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 4 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: **Table 4-3** describes possible agent statuses.

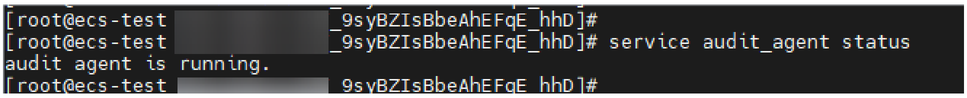
Linux OS

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:



```
[root@ecs-test [redacted] _9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test [redacted] _9syBZIsBbeAhEFqE_hhD]# service audit_agent status
audit agent is running.
[root@ecs-test [redacted] 9syBZIsBbeAhEFqE hhD]#
```

```
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

Table 4-3 Agent statuses

Status	Description
Enabled	The agent is running.

Status	Description
Disabled	The agent is disabled. To enable it, click **Enable** in the **Operation** column. **NOTE** If the CPU usage of an agent is too high, the agent will hibernate and its status will change to **Disabled**. In this case, check whether the CPU usage exceeds the threshold. Modify the threshold or expand the memory. If the CPU usage of a disabled agent falls below the threshold, the agent will automatically restart.
Hibernating	After an agent is added, its initial running status is **Hibernating**. For details about how to change the status, see **What Do I Do If the Database Audit Agent Is Hibernating?**

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**.

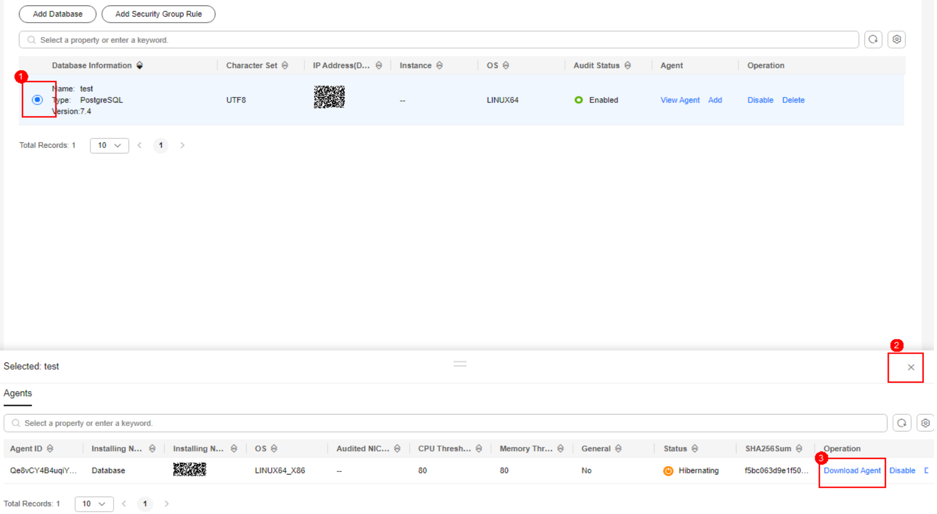
Step 2 Select a region, click ≡, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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 ^ 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 4-4 Downloading an agent



	Database Information	Character Set	IP Address(D...	Instance	OS	Audit Status	Agent	Operation
●	Name: test Type: PostgreSQL Version:7.4	UTF8	[redacted]	--	LINUX64	Enabled	View Agent Add	Disable Delete

Agent ID	Installing N...	Installing N...	OS	Audited NIC...	CPU Thresh...	Memory Thr...	General	Status	SHA256Sum	Operation
Qe8vCY4B4uqiY...	Database	[redacted]	LINUX64_X86	--	80	80	No	Hibernating	f5bc063d9e1f50...	Download Agent Disable D

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**.

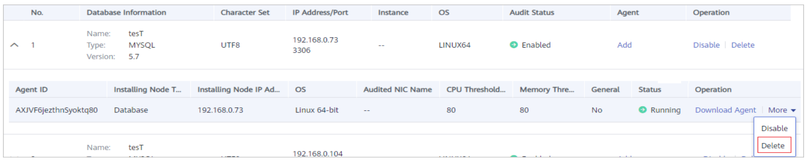
Step 2 Log in to the DBSS console.

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 4-5 Deleting an agent



No.	Database Information	Character Set	IP Address/Port	Instance	OS	Audit Status	Agent	Operation
1	Name: tesT Type: MYSQL Version: 5.7	UTF8	192.168.0.73 3306	--	LINUX64	Enabled	Add	Disable | Delete
	Name: tesT		192.168.0.104					

Agent ID	Installing Node T...	Installing Node IP Ad...	OS	Audited NIC Name	CPU Threshold...	Memory Thre...	General	Status	Operation
AXJVF6jezthnSyoktq80	Database	192.168.0.73	Linux 64-bit	--	80	80	No	Running	Download Agent | More

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.

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** or **Windows**.

----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 supported Linux versions, see **On What Linux OSs Can I Install the Agent?**

Installing an Agent

NOTE

When installing a new agent, you need to customize a password for it.

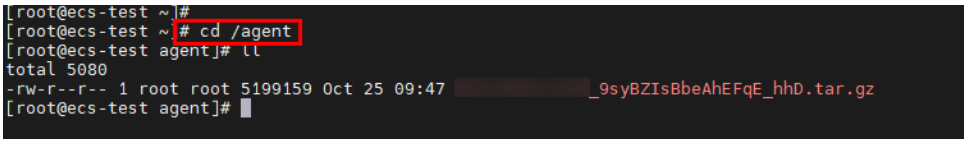
Install the agent on the node suitable for your service scenario.

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:

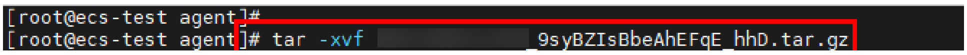
cd *Directory_containing_agent_installation_package*



```
[root@ecs-test ~]#
[root@ecs-test ~]# cd /agent
[root@ecs-test agent]# ll
total 5080
-rw-r--r-- 1 root root 5199159 Oct 25 09:47 [redacted]_9syBZIsBbeAhEFqE_hhD.tar.gz
[root@ecs-test agent]#
```

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

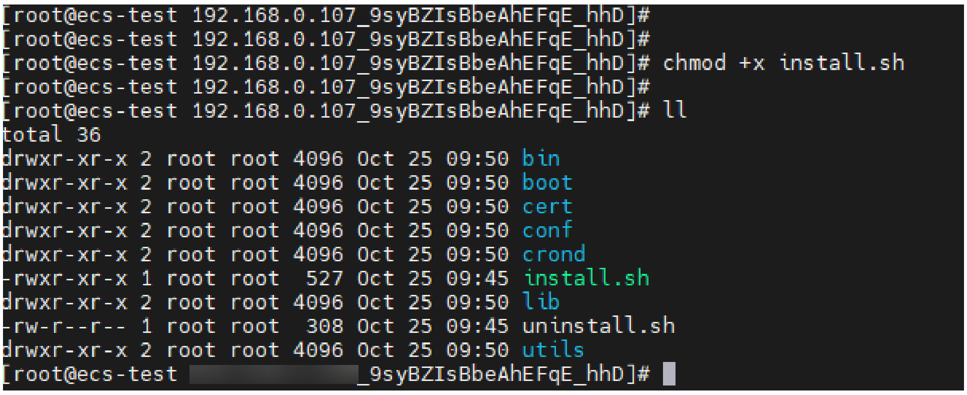
tar -xvf *xxx.tar.gz*



```
[root@ecs-test agent]#
[root@ecs-test agent]# tar -xvf [redacted]_9syBZIsBbeAhEFqE_hhD.tar.gz
```

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

cd *Decompressed_package_directory*



```
[root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]# chmod +x install.sh
[root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test 192.168.0.107_9syBZIsBbeAhEFqE_hhD]# ll
total 36
drwxr-xr-x 2 root root 4096 Oct 25 09:50 bin
drwxr-xr-x 2 root root 4096 Oct 25 09:50 boot
drwxr-xr-x 2 root root 4096 Oct 25 09:50 cert
drwxr-xr-x 2 root root 4096 Oct 25 09:50 conf
drwxr-xr-x 2 root root 4096 Oct 25 09:50 crond
-rwxr-xr-x 1 root root  527 Oct 25 09:45 install.sh
drwxr-xr-x 2 root root 4096 Oct 25 09:50 lib
-rw-r--r-- 1 root root  308 Oct 25 09:45 uninstall.sh
drwxr-xr-x 2 root root 4096 Oct 25 09:50 utils
[root@ecs-test [redacted]_9syBZIsBbeAhEFqE_hhD]#
```

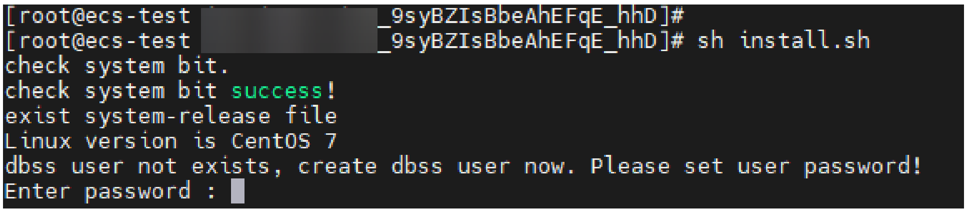
Step 6 Run the following command to check whether you have the permission for executing the **install.sh** script:

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



```
[root@ecs-test [redacted]_9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test [redacted]_9syBZIsBbeAhEFqE_hhD]# sh install.sh
check system bit.
check system bit success!
exist system-release file
Linux version is CentOS 7
dbss user not exists, create dbss user now. Please set user password!
Enter password :
```

NOTE

- In Ubantu, run the **bash install.sh** command to install the agent.
- The agent program is run by common DBSS users. When installing the agent for the first time, you need to create an agent user. After running the **sh install.sh** command, you need to set a password for the DBSS user.

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!
```

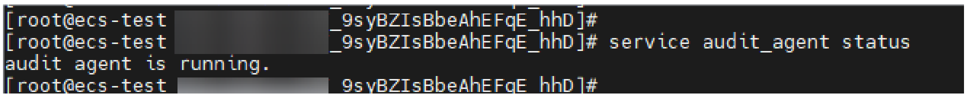
NOTICE

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:



```
[root@ecs-test [redacted] _9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test [redacted] _9syBZIsBbeAhEFqE_hhD]# service audit_agent status
audit agent is running.
[root@ecs-test [redacted] 9syBZIsBbeAhEFqE hhD]#
```

```
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 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.

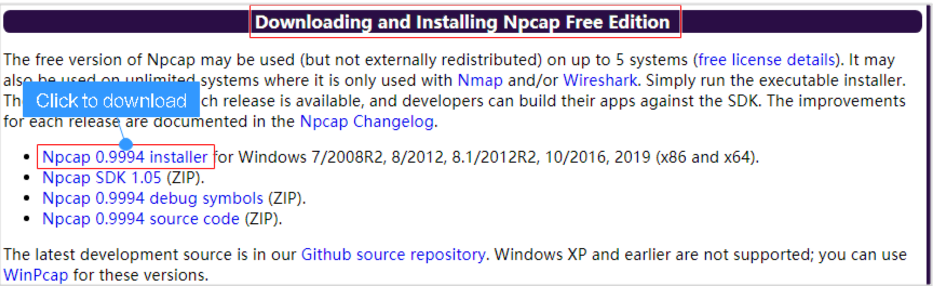
Installing an Agent

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 4-6 Downloading Npcap



Downloading and Installing Npcap Free Edition

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

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

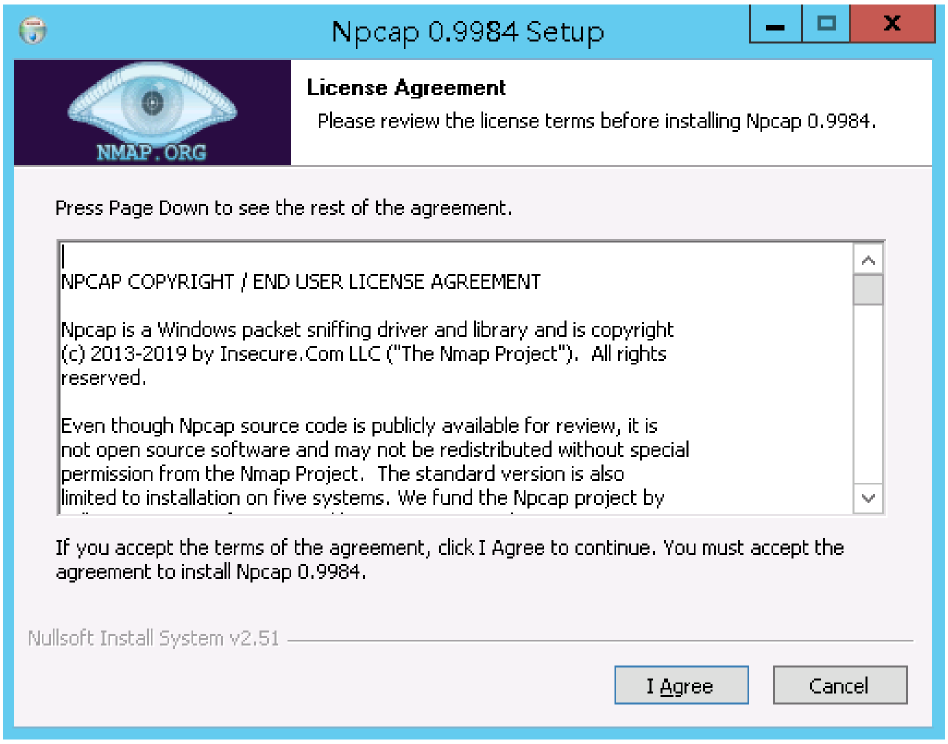
The latest development source is in our Github source repository. Windows XP and earlier are not supported; you can use WinPcap for these versions.

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

c. Double-click the Npcap installation package.

d. In the displayed dialog box, click **I Agree**, as shown in **Figure 4-7**.

Figure 4-7 Agreeing to install Npcap



Npcap 0.9984 Setup

License Agreement

Please review the license terms before installing Npcap 0.9984.

Press Page Down to see the rest of the agreement.

NPCAP COPYRIGHT / END USER LICENSE AGREEMENT

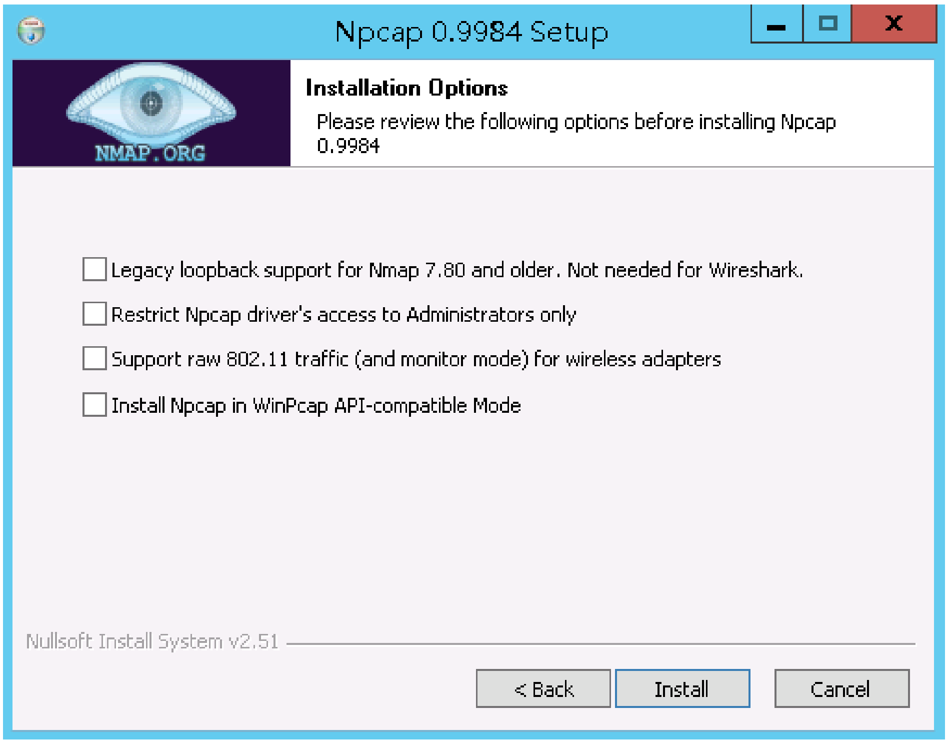
Npcap is a Windows packet sniffing driver and library and is copyright (c) 2013-2019 by Insecure.Com LLC ("The Nmap Project"). All rights reserved.

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

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

e. In the displayed dialog box, leave all the check boxes unselected and click **Install**, as shown in **Figure 4-8**.

Figure 4-8 Installing Npcap



Installation Options

Please review the following options before installing Npcap 0.9984

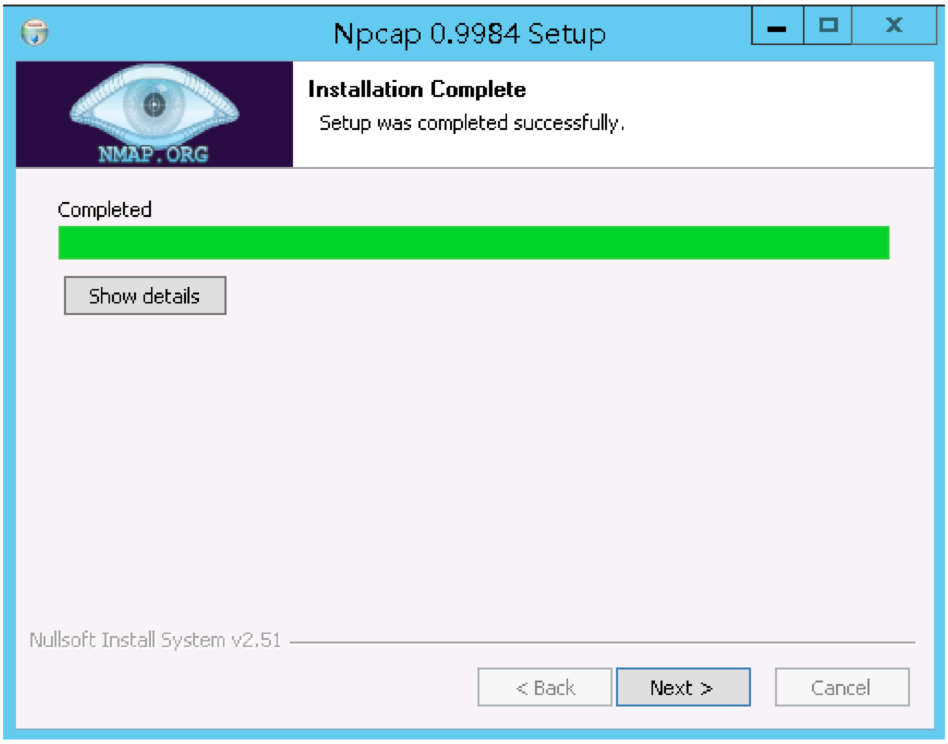
□ Legacy loopback support for Nmap 7.80 and older. Not needed for Wireshark.

□ Restrict Npcap driver's access to Administrators only

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

□ Install Npcap in WinPcap API-compatible Mode

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

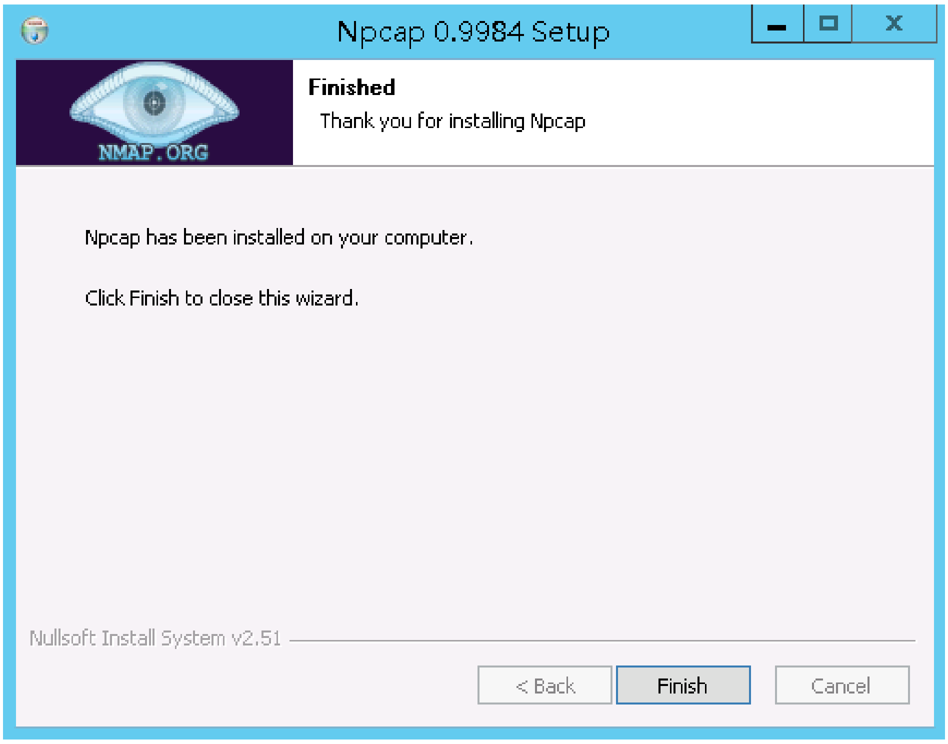


Installation Complete

Setup was completed successfully.

Completed

g. Click **Finish**.



Npcap 0.9984 Setup

Finished

Thank you for installing Npcap

Npcap has been installed on your computer.

Click Finish to close this wizard.

Nullsoft Install System v2.51

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

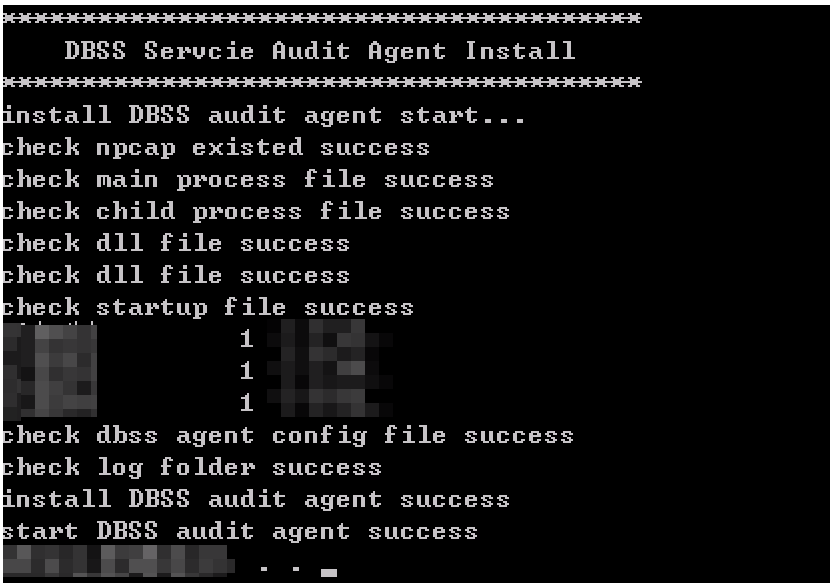
Step 3 Copy the downloaded .zip agent installation package to any directory on the server.

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 4-9** is displayed.

Figure 4-9 Installation completed



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

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

If it is not found, install the agent again.

----End

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 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.

- 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.

- 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

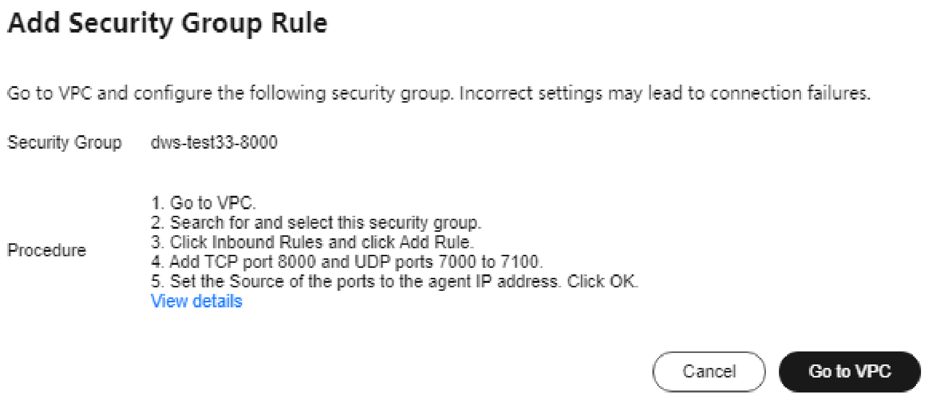
Checking the Security Group Rules of the Database Audit Instance

Step 1 Click ⌄ next to the database to expand the details about the agent and record the value of **Installing Node IP Address**.

Step 2 Click **Add Security Group Rule**.

Step 3 In the displayed dialog box, record the security group name (for example, **default**) of the database audit instance, as shown in **Figure 4-10**.

Figure 4-10 Adding a security group rule



Add Security Group Rule

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

Security Group dws-test33-8000

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

Step 4 Click **Go to VPC**.

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**.
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**.
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
  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).
  2. 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
  1. Open the Task Manager.
  2. 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.

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?

Check whether your agent ID is correct. If it is, perform the following operations to uninstall and then reinstall the agent:

Step 1 **Uninstall the agent** from the target database.

Step 2 **Add the agent again**.

Step 3 **Download the agent**.

Step 4 **Install an Agent (Linux)** or **Install an Agent (Windows)**.

----End

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 **add the agent**. In this case, uninstall the agent and reinstall it. Perform the following steps:

Step 1 **Uninstall the agent** from the target database.

Step 2 **Add the agent again**. Set the installing node IP address to a valid intranet IP address.

Step 3 **Download the agent**.

----End

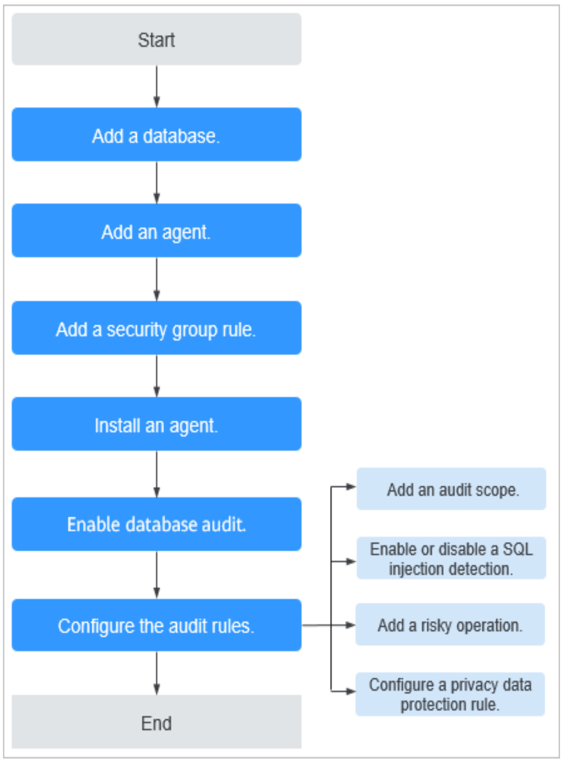
5 Operations

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.

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

Figure 5-1 Database audit configuration process


Start
Add a database.
Add an agent.
Add a security group rule.
Install an agent.
Enable database audit.
Configure the audit rules.
End
Add an audit scope.
Enable or disable a SQL injection detection.
Add a risky operation.
Configure a privacy data protection rule.

5.2 How Do I Disable SSL for a Database?

Scenario

- If you audit your database without installing the agent, you do not need to disable SSL for the database. Skip this section.
- If you audit your database by installing an agent, you need to disable SSL for the database. Otherwise, you cannot obtain audit data.

Procedure

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.

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**.

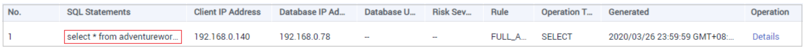
Step 3 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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 5-2**.

Figure 5-2 Viewing SQL statements



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

- If the entered SQL statement is 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.

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.

----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.

To query specified alarms, perform the following steps:

- Select **Last 30 minutes**, **1 hour**, **24 hours**, **7 days**, or **30 days** from the drop-down list, 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

5.8 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.

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

5.9 How Do I Add an HBase Database and Perform Audit?

An HBase database consists of an active master node, a standby master node, and multiple RegionServer nodes.

When auditing an HBase database, add its master node and RegionServer node as independent databases.

Constraints

- Only the HBase (protobuf) format protocol is supported. The HBase (thrift) protocol is not supported.
- Only the simple and kerberos authentication modes are supported.

  NOTE

  Kerberos authentication applies to the following scenarios: **authentication** (authentication only), **integrity** (Authentication+Integrity check), and **privacy** (Authentication+Integrity check+Encryption).

  Currently, Huawei Cloud supports only the **authentication** scenario.

  The **integrity** and **privacy** scenarios are not supported.

Operation

An HBase database consists of an active master node, a standby master node, and two RegionServer nodes.

- Active master node: IP address is **192.168.0.1** and service port number is **16000**.
- Standby master node: IP address is **192.168.0.2** and service port number is **16000**.
- RegionServer1 node: IP address is **192.168.0.3** and service port number is **16020**.
- RegionServer2 node: IP address is **192.168.0.4** and service port number is **16020**.

When auditing this HBase database, you need to add four databases. The IP addresses and ports of the four databases are as follows:

- **192.168.0.1:16000** (corresponding to the active master node)
- **192.168.0.2:16000** (corresponding to the standby master node)
- **192.168.0.3:16020** (corresponding to the RegionServer1 node)
- **192.168.0.4:16020** (corresponding to the RegionServer2 node)

NOTE

If there is no standby master node, you do not need to add the standby master database.

How Do I Use Audit the HBase Database in an MRS Cluster?

If an MRS cluster is created in the default mode, the cluster uses the "authentication + encryption" mode in Kerberos authentication. In this case, DBSS cannot audit the database. You need to change the authentication mode.

Change the authentication mode of an MRS cluster in the Kerberos authentication scenario:

Go to the cluster management page. On the **FusionInsight Manager** page, choose **Cluster** and click the name of the target cluster. Choose **HBase** > **Configuration** > **Basic Configuration**, locate the **hbase.rpc.protection** configuration item, and change its value.

Authentication methods corresponding to the value of **hbase.rpc.protection**:

- **authentication**: Authentication only
- **integrity**: Authentication + Integrity check
- **privacy**: Authentication + Integrity check + Encryption

6 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.
- 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.

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.

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.

- 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

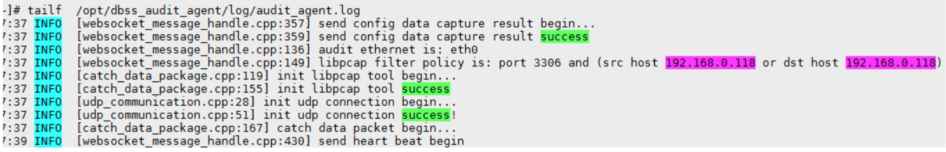
- If the fault is rectified, no further operation is required.
- If the problem persists, go to **Step 4**.

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**.

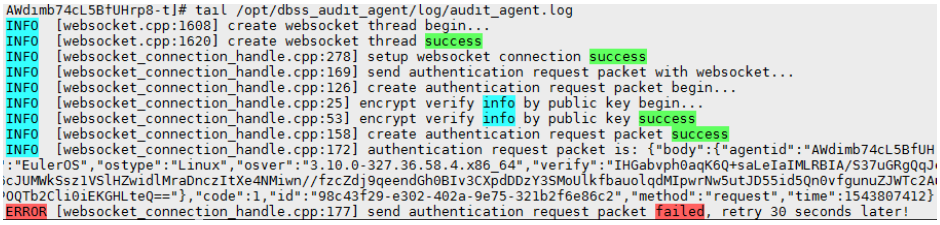
Figure 6-1 Normal communication



```
-]# 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 6-2 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
5cJUMWkSsz1VSlHZwidlMraDnczItXe4NMiwn//fzcZdj9qeendGh0BIv3CXpdDDzY3SMoUlkfbauolqdMIpwrNw5utJD55id5Qn0vfgunuZJWTc2A
'0QTb2Cli0iEKGHLteQ=="},"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**.

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 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**.
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.
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.

6.3 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%.

6.4 Why I Failed to Access the DBSS Purchase Page?

Symptom

An error is reported when an account with the FullAccess permission is used to access the DBSS purchase page.

Possible Causes

Fine-grained authentication is enabled. Accounts with insufficient permissions cannot access the purchase page.

Suggestion

Add the following permissions to your IAM accounts:

tms:predefineTags:list

bss:order:pay

bss:order:view

bss:order:update

bss:balance:view

vpc:vpcs:list

smn:topic:list

ces:metricData:create

gaussdb:instance:list

gaussdb:instance:modifyTraceSQLPolicy

eps:resources:list

rds:instance:list

dws:openAPICluster:list

rds:auditlog:operate

dws:cluster:setSecuritySettings

dws:ltsAccess:get

dws:ltsAccess:operate

dws:createAgency:create

6.5 What Do I Do If I Audit RDS Psostgres Database but No Audit Result Is Displayed?

Symptom

No audit result is displayed after an RDS Psostgres database is audited.

Possible Causes

- The configuration of the DBSS audit instance is incorrect. Check the configuration again.
- If the configuration is correct but no audit result is displayed, connect to the database instance in non-SSL mode.

Solutions

Run the following command to connect to the database:

psql -h xxx.xxx.xxx -p 5432 "dbname=postgres user=root sslmode=disable"

6.6 DBSS Automatic Backup Failed and The Failure Code is "Export backup file failed"

DBSS automatic backup failed. Failure code: Export backup file failed.

Cause

If the DBSS disk space is used up, automatic backup fails. In this case, you need to modify the automatic backup rule and set the log retention period.

You need to delete unnecessary backups in a timely manner to release space.

7 Logs

7.1 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?**

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

The operation logs of database audit are permanently saved.

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

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

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

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

Step 6 View operation logs. For details about related parameters, see **Table 7-1**.

NOTE

You can select last 30 minutes, last 1 hour, 24 hours, last 7 days, last 30 days, or a custom 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

7.4 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.

7.5 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**.

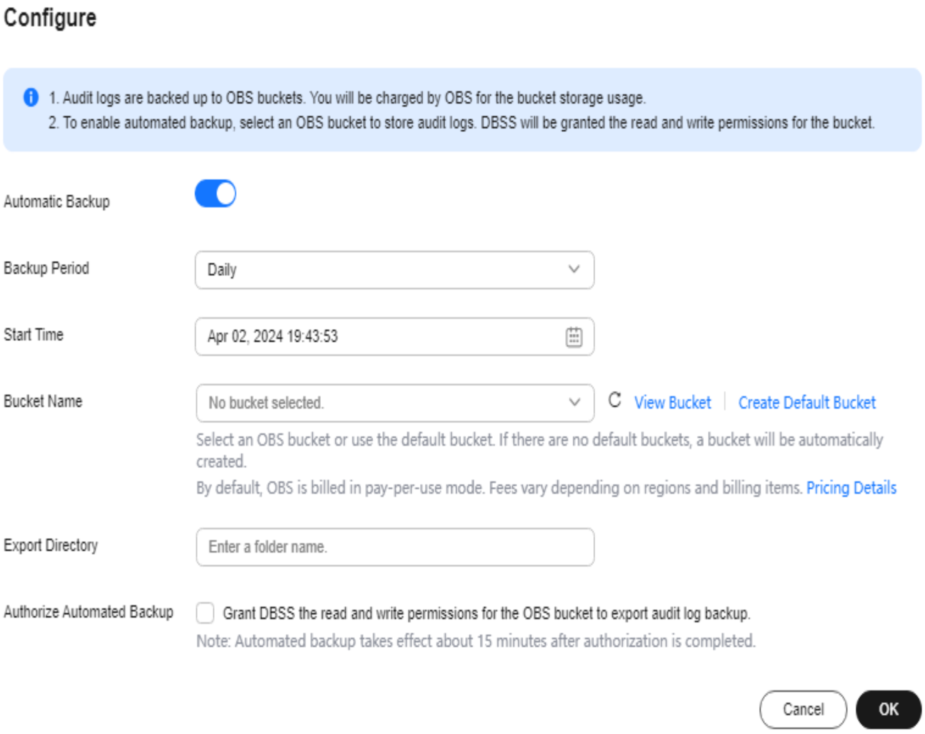
Step 2 Select a region, click ☰, and choose **Security & Compliance** > **Database Security Service**. The **Dashboard** page is displayed.

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 **Modify Automated Backup Settings**. In the displayed dialog box, set the auto backup parameters. **Table 7-2** describes the parameters.

Figure 7-1 Configure Automatic Backup dialog box



Configure

1. Audit logs are backed up to OBS buckets. You will be charged by OBS for the bucket storage usage.
2. To enable automated backup, select an OBS bucket to store audit logs. DBSS will be granted the read and write permissions for the bucket.

Automatic Backup

Backup Period: Daily

Start Time: Apr 02, 2024 19:43:53

Bucket Name: No bucket selected.

Select an OBS bucket or use the default bucket. If there are no default buckets, a bucket will be automatically created.
By default, OBS is billed in pay-per-use mode. Fees vary depending on regions and billing items. Pricing Details

Export Directory: Enter a folder name.

Authorize Automated Backup: □ Grant DBSS the read and write permissions for the OBS bucket to export audit log backup.
Note: Automated backup takes effect about 15 minutes after authorization is completed.

Table 7-2 Parameters

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

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

Step 6 Click **OK**.

NOTE

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

----End

7.6 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). 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 are billed per use. For details about OBS pricing, see **Pricing Details**.

7.7 Backup Gets Stuck at the Backup File Uploading Phase

This problem occurs probably because the amount of data to be backed up is too large. You are advised to perform hourly backup.

A Change History

Released On	Description
2024-04-10	This is the twenty-first official release. Upgraded the console style.
2023-04-07	This is the twentieth official release. Added **Why I Failed to Access the DBSS Purchase Page?**.
2022-11-01	This is the nineteenth official release. Modified: **How Do I Unsubscribe from DBSS?**
2022-06-21	This is the eighteenth official release. ● Added **Alarm Notifications Are Abnormal**. ● Added **Backup Gets Stuck at the Backup File Uploading Phase**. Optimized descriptions of some FAQ.
2022-05-12	This is the seventeenth official release. ● Added **What Are the Differences Between DBSS Database Audit and RDS SQL Audit?** ● Added **How Many Database Audit Instances Can I Purchase in the Same Region?** Optimized descriptions of some FAQ.
2022-03-18	This is the sixteenth official release. ● Added **Why Do I Need to Select a VPC When Buying an Instance?** ● Added **What Should I Do If an Alarm of Insufficient DBSS Capacity Is Displayed?**

Released On	Description
2021-11-03	This is the fifteenth official release. Modified FAQs. Updated the supported hard disk specifications in **What Editions Does DBSS Provide?**.
2021-10-20	This is the fourteenth official release. Modified FAQs. ● Added **Can I Audit Databases Across Different VPCs?** ● Added the following OSs supported by the agent in **On What Linux OSs Can I Install the Agent?** – Fedora 29 (64bit) – Fedora 30 (64bit) – SUSE 13 (64bit) – SUSE 15 (64bit) – SUSE 42 (64bit) – Euler 2.5 (64bit) – OpenEuler 20.03 (64bit) – Red Hat Enterprise Linux 7.4 (64bit) – Red Hat Enterprise Linux 7.6 (64bit) – NeoKylin 7.0 (64bit) – Kylin Linux Advanced Server release V10 (64bit) – Uniontech OS Server 20 Enterprise (64bit)
2021-04-19	This is the thirteenth 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?**.
2021-03-22	This is the twelfth 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 the section **Disabling ForceEncryption for the SQL Server Protocol** in **Database Audit Is Running Properly But Generates No Audit Records**.
2021-01-19	This is the eleventh official release. Added **Can Database Audit Logs Be Directly Saved to OBS?**.

Released On	Description
2020-12-18	This is the tenth 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**.
2020-05-20	This is the ninth official release. Optimized descriptions in **How Long Is the Database Audit Data Stored by Default?**.
2020-04-22	This is the eighth official release. Added the support for CentOS 7.6 (64-bit) in **On What Linux OSs Can I Install the Agent?**.
2020-03-16	This is the seventh official release. Adjusted the document structure. ● **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?**
2020-02-24	This is the sixth official release. Added the description about database audit for Windows OS.
2019-12-23	This is the fifth official release. Added descriptions about IPv6.
2019-12-03	This is the fourth official release. ● Added the description about database audit. ● Deleted the content about database protection.
2019-08-26	This is the third official release. Added **What Are Regions and AZs?**
2019-01-15	This is the second official release. Revised the document outline and optimized the content description.
2018-05-31	This is the first official release.