Database Security Service (DBSS)

Quick Start

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Purchasing and Enabling DBSS

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.

The section describes how to purchase the starter edition to manage one database and enable DBSS. You can use the default audit rules to detect abnormal behavior through multi-dimensional analysis, real-time alarms, and reports.

Operation Process

Procedure	Description
Preparation	You need to register a HUAWEI ID and top up your account.
Step 1: Buy Starter Edition DBSS	Set the configuration items, such as the subnet, security group, and required duration, and purchase DBSS of the starter edition.
Step 2: Add a Database	Add a database. You can select agent-free or agent-installed based on the database type.
Step 3: Enabling Database Audit	Enable database audit and verify the audit result.
Related Operations	Customize audit rules and view audit results and monitoring information.

Preparation

- Before purchasing WAF, create a Huawei account and subscribe to Huawei Cloud. For details, see **Registering a Huawei ID and Enabling Huawei Cloud Services** and **Real-Name Authentication**.

  If you have enabled Huawei Cloud and completed real-name authentication, skip this step.

- Make sure that your account has sufficient balance, or you may fail to pay to your WAF orders.

Step 1: Buy Starter Edition DBSS

Step 1 Log in to the management console.

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

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

Step 4 On the DBSS purchase page, complete the following configurations.

Table 1-1 Database audit instance parameters

Parameter	Example Value	Description
VPC	**default_vpc**	You can select an existing VPC, or click **View VPC** to create one on the VPC console. **NOTE** • Select the VPC of the node (application or database side) where you plan to install the agent. For more information, see **How Do I Determine Where to Install an Agent?** • To change the VPC of a DBSS instance, unsubscribe from it and purchase a new one. For more information about VPC, see *Virtual Private Cloud User Guide*.
Security Group	**default**	You can select an existing security group in the region or create a security group on the VPC console. Once a security group is selected for an instance, the instance is protected by the access rules of this security group. For more information about security groups, see *Virtual Private Cloud User Guide*.
Subnet	**default_subnet**	You can select a subnet configured in the VPC or create a subnet on the VPC console.
Name	**DBSS-test**	Instance name
Remarks	-	You can add instance remarks.
Enterprise Project	**default**	This parameter is provided for enterprise users. An enterprise project groups cloud resources, so you can manage resources and members by project. The default project is **default**. Select an enterprise project from the drop-down list. For more information about enterprise project, see **Enterprise Management User Guide**.

Parameter	Example Value	Description
Required Duration	**1**	Select the validity period of DBSS. After you select **Auto-renew**, the system automatically renews the instance upon expiry if your account balance is sufficient. You can continue to use the instance.

Step 5 Confirm the configuration and click **Next**.

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

Step 6 On the **Details** page, read the *Database Audit of Database Security Service Disclaimer*, select **I have read and agree to the Database Audit of Database Security Service Disclaimer**, and click **Submit**.

Step 7 On the displayed page, select a payment method.

Step 8 After you pay for your order, you can view the creation status of your instances.

----End

Step 2: Add a Database

Databases audited by DBSS support agent-free installation and agent installation. **Table 1-2** lists the types and versions of databases that support agent-free installation. **Table 1-3** lists the types and versions of databases that support agent installation. You can enable database audit without installing an agent or by installing an agent based on the database type and version.

Adding a Database Without Installing an Agent

Table 1-2 Agent-free database types and versions

Database Type	Supported Edition
GaussDB for MySQL	All editions are supported by default.
PostgreSQL **NOTICE** If the size of an SQL statement exceeds 4 KB, the SQL statement will be truncated during auditing. As a result, the SQL statement is incomplete.	• 14 (14.4 or later) • 13 (13.6 or later) • 12 (12.10 or later) • 11 (11.15 or later) • 9.6 (9.6.24 or later) • 9.5 (9.5.25 or later)
RDS for SQLServer	All editions are supported by default.

Database Type	Supported Edition
RDS for MySQL	- 5.6 (5.6.51.1 or later) - 5.7 (5.7.29.2 or later) - 8.0 (8.0.20.3 or later)
GaussDB(DWS)	- 8.2.0.100 or later
RDS for MariaDB	All editions are supported by default.

Step 1 In the navigation tree on the left, choose **Databases**.

Step 2 In the **Instance** drop-down list, select the instance whose database is to be added.

Step 3 Click **Add Database**.

Step 4 In the displayed dialog box, set the database parameters.

Step 5 Click **OK**. A database whose **Audit Status** is **Disabled** is added to the database list.

----End

Adding a Database By Installing an Agent

Table 1-3 Type and version of the database where the agent is to be installed

Database Type	Edition
MySQL	- 5.0, 5.1, 5.5, 5.6, and 5.7 - 8.0 (8.0.11 and earlier) - 8.0.30 - 8.0.35 - 8.1.0 - 8.2.0
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, 8.1, 8.2, 8.3, and 8.4 - 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, and 9.6 - 10.0, 10.1, 10.2, 10.3, 10.4, and 10.5 - 11 - 12 - 13 - 14
SQLServer	- 2008 - 2012 - 2014 - 2016 - 2017
GaussDB(for MySQL)	MySQL 8.0
DWS	- 1.5 - 8.1
DAMENG	DM8
KINGBASE	V8
SHENTONG	V7.0
GBase 8a	V8.5
GBase 8s	V8.8
Gbase XDM Cluster	V8.0
Greenplum	V6.0
HighGo	V6.0
GaussDB	- 1.3 Enterprise Edition - 1.4 Enterprise Edition - 2.8 Enterprise Edition - 3.223 Enterprise Edition
MongoDB	V5.0
DDS	4.0
Hbase (Supported by CTS 23.02.27.182148 and later versions)	- 1.3.1 - 2.2.3

Database Type	Edition
Hive (Supported by CTS 23.02.27.182148 and later versions)	• 1.2.2 • 2.3.9 • 3.1.2 • 3.1.3
MariaDB	10.6
TDSQL	10.3.17.3.0
Vastbase	G100 V2.2
TiDB	• V4 • V5 • V6 • V7 • V8

Step 1 Add a database.

1. In the navigation tree on the left, choose **Databases**.
2. In the **Instance** drop-down list, select the instance whose database is to be added.
3. Click **Add Database**.
4. In the displayed dialog box, set the database parameters.
5. Click **OK**. A database whose **Audit Status** is **Disabled** is added to the database list.

Step 2 Add an agent.

1. In the navigation tree on the left, choose **Databases**.
2. In the **Instance** drop-down list, select the instance whose agent is to be added.
3. In the **Agent** column of the desired database, click **Add**.
4. In the displayed dialog box, select an add mode.
5. Click **OK**.

Step 3 Download and install an agent.

1. In the navigation tree on the left, choose **Databases**.
2. In the **Instance** drop-down list, select the instance whose agent is to be downloaded.
3. 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 The agent installation package will be downloaded.
4. Install an agent.

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

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

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

cd *Directory_containing_agent_installation_package*

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

tar -xvf xxx.tar.gz

e. Run the following command to switch to the directory containing the decompressed files:

cd *Decompressed_package_directory*

f. Run the following command to install the agent:

sh install.sh

g. 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            _9syBZIsBbeAhEFqE_hhD]#
[root@ecs-test            _9syBZIsBbeAhEFqE_hhD]# service audit_agent status
audit agent is running.
[root@ecs-test            _9syBZIsBbeAhEFqE_hhD]#
```

audit agent is running.

----End

Step 3: Enabling Database Audit

Step 1 Enable database audit.

1. In the navigation tree on the left, choose **Databases**.

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

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

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

Step 2 Verify the audit result.

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

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

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

4. Click the **Statements** tab.

5. Click 🗓 on the right of **Time**, select the start time and end time, and click **Submit**. The SQL statement entered in **Figure 1-1** is displayed in the list.

Figure 1-1 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

----End

Related Operations

To effectively audit the database, you can customize audit rules and view audit results and monitoring information. This helps you locate internal violations and improper operations and ensure data asset security. For details, see **Configuring Audit Rules**, **Viewing Audit Results**, and **Viewing Monitoring Information**.

2 Getting Started with Common Practices

After configuring DBSS, you can view common practices to better use DBSS.

Table 2-1 Common practices

Practice		Description
Auditing a Database	**Auditing a User-built Database on ECS**	Database audit is deployed in out-of-path mode. The database audit agent is deployed on the database or application server to obtain access traffic, upload traffic data to the audit system, receive audit system configuration commands, and report database monitoring results, implementing security audit on databases built on ECS or BMS.
	Auditing an RDS Database (with Agents) **Auditing an RDS Database (Agent-free)**	DBSS can audit the security of relational database instances. (Applications connected to this DB instance are deployed on ECS.) DBSS can audit certain types of relational databases without installing agents.
	Deploying the Database Audit Agent in a Container	For easier O&M, you can deploy the database audit agent in a large number of containerized applications or databases in batches. This makes configuration quicker and easier.
Checking a Database	**Data Reduction Detection**	Database audit provides a preconfigured rule to check audit logs for data security risks, such as SQL statements used for data breach. You can learn the execution duration, number of affected rows, and database information of the SQL statements.

Practice		Description
	Checking for Slow SQL Statements	Database audit provides a preconfigured rule to check for slow SQL statements, whose response time recorded in audit logs is greater than 1 second.
		You can learn the execution duration, number of affected rows, and database information of the slow SQL statements, and optimize the statements accordingly.
	Checking for Dirty Tables	Configure a rule to detect operations on dirty tables. You can configure unnecessary databases, tables, and columns as dirty tables. Programs that access the dirty tables will be marked as suspicious programs.
		In this way, you can detect the SQL statements that access dirty tables and detect data security risks in a timely manner.
DJCP MLPS	**DBSS for DJCP Compliance Items**	DBSS provides you with one-stop solutions, helping you quickly and cost-effectively complete security modifications and meet security compliance requirements.
Configuring Database Audit	**Configuring Oracle RAC Cluster Audit**	When using DBSS for an Oracle RAC cluster, each node in the cluster is regarded as an independent database and requires an agent to forward network traffic.
	Configuring Database Audit Instance Rules	DBSS allows you to trace attackers based on various types of information, including the source IP address, user identity, application, access time, requested database, original SQL statement, and operations.