



**Copyright © Huawei Technologies Co., Ltd. 2021. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

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

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

---

# Contents

---

<b>1 DBSS.....</b>	<b>1</b>
<b>2 Database Audit.....</b>	<b>4</b>
2.1 Functions.....	4
2.2 Advantages.....	5
2.3 Deployment Architecture.....	5
2.4 Editions.....	6
2.5 Constraints.....	7
<b>3 Database Protection.....</b>	<b>11</b>
3.1 Functions.....	11
3.2 Advantages.....	12
3.3 Deployment Architecture.....	13
3.4 Editions.....	16
3.5 Constraints.....	17
<b>4 Billing.....</b>	<b>19</b>
<b>5 Personal Data Protection Mechanism.....</b>	<b>21</b>
<b>6 Permissions Management.....</b>	<b>23</b>
<b>7 Related Services.....</b>	<b>30</b>
<b>8 Monitoring Metrics.....</b>	<b>34</b>
<b>A Change History.....</b>	<b>37</b>

# 1 DBSS

Database Security Service (DBSS) is developed based on Huawei's 30 years of experience in database security practices. It has two subservices, database audit and database protection, which deliver functions such as data breach prevention, database firewall, and database audit to protect your databases and assets on the cloud.

## Database Audit

Database audit is deployed in bypass pattern. 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.

Database audit provides the database audit function in bypass disposition pattern for the following databases on HUAWEI CLOUD:

- RDS instances
- Databases on ECSs
- Databases on BMSs

Database audit supports the following database types and versions.

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

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

Database Type	Version
PostgreSQL	<ul style="list-style-type: none"> <li>• 7.4</li> <li>• 8.0, 8.1, 8.2, 8.3, 8.4</li> <li>• 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6</li> <li>• 10.0, 10.1, 10.2, 10.3, 10.4, 10.5</li> <li>• 11</li> </ul>
SQL Server	<ul style="list-style-type: none"> <li>• 2008, 2008R2</li> <li>• 2012</li> <li>• 2014</li> <li>• 2016</li> <li>• 2017</li> </ul>
DWS	1.5
GaussDB for Mysql	Mysql 8.0
DAMENG	DM8
KINGBASE	V8

Database audit can:

- Help you meet security compliance requirements.
  - Comply with DJCP (graded protection) standards for database audit.
  - Comply with security laws and regulations, and provide compliance reports that meet data security standards (such as Sarbanes-Oxley).
- Back up and restore database audit logs and meet the audit data retention requirements.
- Monitor risks, sessions, session distribution, and SQL distribution in real time.
- Report alarms for risky behaviors and attacks and responds to database attacks in real time.
- Locate internal violations and improper operations and keep data assets secure.

Deployed in bypass pattern, database audit can perform flexible audit on the database without affecting user services.

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

## Database Protection

Based on the reverse proxy and machine learning mechanism, database protection provides functions such as data masking, database audit, sensitive data discovery, data reduction, and anti-injection to ensure database security on the cloud.

- Attack prevention  
Multiple policies prevent database attacks and ensure database security on the cloud.
- Sensitive data masking  
Sensitive data discovery complies with industry standards. Once sensitive data is detected in user's database and it will be dynamically masked.
- Database audit  
Performance, data, and behavior exceptions are monitored, and audit logs are remotely stored to ensure compliance.

Database protection provides protection and audit functions for the following databases on HUAWEI CLOUD:

- Relational Database Service (RDS) instances
- Databases on Elastic Cloud Servers (ECSs)
- Databases on Bare Metal Servers (BMSs)

### NOTE

Database protection supports Distributed Database Middleware (DDM). However, only some functions of DDM are supported currently due to the defect of the DDM mechanism. For details about the restrictions on using the DDM, see [Constraints](#).

Database protection supports the following database types:

- Microsoft SQL Server 2008 to Microsoft SQL Server 2014
- MySQL 5.5 to MySQL 5.7
- PostgreSQL 9.4 to PostgreSQL 9.5
- DWS 1.2.3

# 2 Database Audit

---

## 2.1 Functions

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

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

- Fine-grained Reports for Various Abnormal Behaviors
  - Session behavior  
Provides session analysis report of the client and database users.
  - Risky operation  
Provides the risk distribution and analysis report.
  - Compliance report  
Provides compliance reports that meet data security standards (for example, Sarbanes-Oxley).

## 2.2 Advantages

Database audit provides you with the database audit function in bypass pattern, enabling the system to generate real-time alarms for risky operations. In addition, database audit generates compliance reports that meet data security standards. In this way, it locates internal violations and improper operations, protecting your data assets.

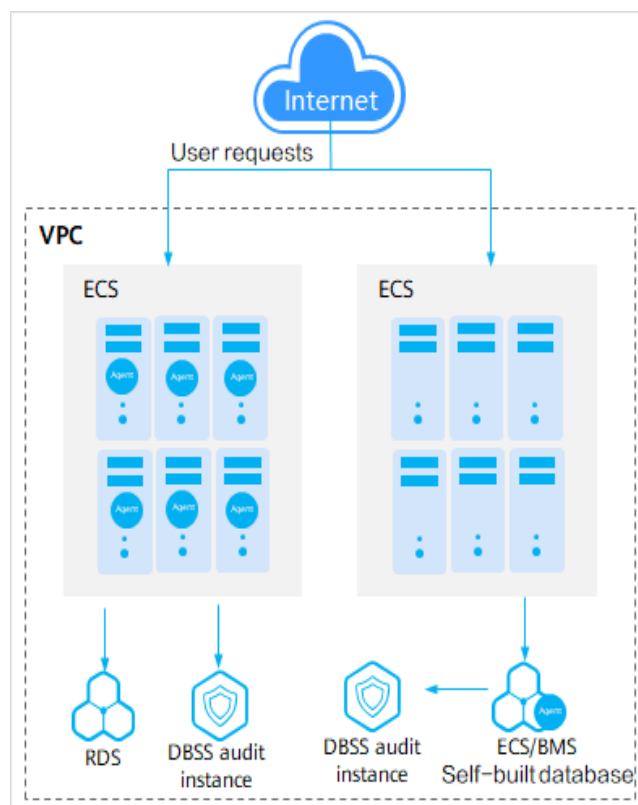
- Simple to set up  
Database audit is deployed in bypass pattern. It is simple to set up and operate.
- Comprehensive audit  
Supports audit of RDS databases and self-built databases on ECS/BMS on HUAWEI CLOUD.
- Quick identification  
Implements 99%+ application association audit, complete SQL parsing, and accurate protocol analysis.
- Efficient analysis  
Responds quickly for data query with 10,000 requests per second from massive volumes of data saved.
- Compliance with various regulations
  - Meets the requirements of database audit for Grade III security compliance.
  - Complies with laws and regulations, such as the cybersecurity law and SOX.
- Clear permission division  
Clearly divides permissions among the system administrator, security administrator, and audit administrator, meeting audit security requirements.

## 2.3 Deployment Architecture

Database audit is deployed in bypass pattern. It supports audit of RDS databases and self-built databases on ECS/BMS on HUAWEI CLOUD.

**Figure 2-1** shows the database audit deployment architecture.

**Figure 2-1** Database audit deployment architecture



The agent deployment for database audit is as follows:

- Self-built database on ECS/BMS  
Deploy the agent on the database side.
- RDS database  
Deploy the agent on the application or proxy side.

## 2.4 Editions

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

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

**Table 2-1** Database audit editions

Version	Maximum Databases	System Resource	Performance
Basic	3	<ul style="list-style-type: none"><li>• CPU: 4 vCPUs</li><li>• Memory: 8 GB</li><li>• Disk: 560 GB</li></ul>	<ul style="list-style-type: none"><li>• Peak QPS: 3,000 queries/second</li><li>• Database load rate: 3.6 million statements/hour</li><li>• Stores 400 million online SQL statements.</li><li>• Stores 5 billion archived SQL statements.</li></ul>
Professional	6	<ul style="list-style-type: none"><li>• CPU: 8 vCPUs</li><li>• Memory: 16 GB</li><li>• Disk: 1084 GB</li></ul>	<ul style="list-style-type: none"><li>• Peak QPS: 6,000 queries/second</li><li>• Database load rate: 7.2 million statements/hour</li><li>• Stores 600 million online SQL statements.</li><li>• Stores 10 billion archived SQL statements.</li></ul>
Advanced	30	<ul style="list-style-type: none"><li>• CPU: 16 vCPUs</li><li>• Memory: 32 GB</li><li>• Disk: 2108 GB</li></ul>	<ul style="list-style-type: none"><li>• Peak QPS: 30,000 queries/second</li><li>• Database load rate: 10.80 million statements/hour</li><li>• Stores 1.5 billion online SQL statements.</li><li>• Stores 60 billion archived SQL statements.</li></ul>

 **NOTE**

Online SQL statements are counted based on the assumption that the capacity of an SQL statement is 1 KB.

## 2.5 Constraints

Database audit is subject to certain constraints.

### Supported Database Types

The following types of databases on HUAWEI CLOUD can be audited in bypass mode:

- RDS instances
- Databases on ECSs
- Databases on BMSs

## Supported Database Versions

The following database versions can be audited.

**Table 2-2** Database types and versions supported by database audit

Database Type	Version
MySQL	<ul style="list-style-type: none"><li>• 5.0, 5.1, 5.5, 5.6, 5.7</li><li>• 8.0</li></ul>
Oracle	<ul style="list-style-type: none"><li>• 11g 11.1.0.6.0, 11.2.0.1.0, 11.2.0.2.0, 11.2.0.3.0, and 11.2.0.4.0</li><li>• 12c 12.1.0.2.0, 12.2.0.1.0</li><li>• 19c</li></ul>
PostgreSQL	<ul style="list-style-type: none"><li>• 7.4</li><li>• 8.0, 8.1, 8.2, 8.3, 8.4</li><li>• 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6</li><li>• 10.0, 10.1, 10.2, 10.3, 10.4, 10.5</li><li>• 11</li></ul>
SQL Server	<ul style="list-style-type: none"><li>• 2008, 2008R2</li><li>• 2012</li><li>• 2014</li><li>• 2016</li><li>• 2017</li></ul>
DWS	1.5
GaussDB for Mysql	Mysql 8.0
DAMENG	DM8
KINGBASE	V8

## Supported OSs

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

- For more information, see [Table 2-3](#).

**Table 2-3** Supported Linux OS versions

System Name	System version
CentOS	<ul style="list-style-type: none"> <li>• CentOS 6.3 (64bit)</li> <li>• CentOS 6.5 (64bit)</li> <li>• CentOS 6.8 (64bit)</li> <li>• CentOS 6.9 (64bit)</li> <li>• CentOS 7.0 (64bit)</li> <li>• CentOS 7.1 (64bit)</li> <li>• CentOS 7.2 (64bit)</li> <li>• CentOS 7.3 (64bit)</li> <li>• CentOS 7.4 (64bit)</li> <li>• CentOS 7.5 (64bit)</li> <li>• CentOS 7.6 (64bit)</li> <li>• CentOS 7.8 (64bit)</li> <li>• CentOS 8.0 (64bit)</li> </ul>
Debian	<ul style="list-style-type: none"> <li>• Debian 7.5.0 (64bit)</li> <li>• Debian 8.2.0 (64bit)</li> <li>• Debian 8.8.0 (64bit)</li> <li>• Debian 9.0.0 (64bit)</li> </ul>
Fedora	<ul style="list-style-type: none"> <li>• Fedora 24 (64bit)</li> <li>• Fedora 25 (64bit)</li> </ul>
SUSE	<ul style="list-style-type: none"> <li>• SUSE 11 SP4 (64bit)</li> <li>• SUSE 12 SP1 (64bit)</li> <li>• SUSE 12 SP2 (64bit)</li> </ul>
Ubuntu	<ul style="list-style-type: none"> <li>• Ubuntu 14.04 (64bit)</li> <li>• Ubuntu 16.04 (64bit)</li> <li>• Ubuntu 18.04 (64bit)</li> </ul>
Euler	<ul style="list-style-type: none"> <li>• Euler 2.2 (64bit)</li> <li>• Euler 2.3 (64bit)</li> </ul>
Oracle Linux	<ul style="list-style-type: none"> <li>• Oracle Linux 6.9 (64bit)</li> <li>• Oracle Linux 7.4 (64bit)</li> </ul>

- The following Windows OSs are supported:
  - Windows Server 2008 R2
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows 7
  - Windows 10

## Other Constraints

- Database audit cannot be used across regions. The database to be audited and the database audit instance you purchased must be in the same region.
- If SSL is enabled for a database, the database cannot be audited. To use database audit, disable SSL first. For details, see [How Do I Disable SSL for a Database?](#)
- Ensure the VPC of the database audit instance is the same as that of the node (application side or database side) where you plan to install the database audit agent. Otherwise, the instance will be unable to connect to the agent or perform audit. For more information, see [How Do I Determine Where to Install an Agent?](#)

# 3 Database Protection

---

## 3.1 Functions

This section describes the major functions of database protection.

### Database Security

- **Database firewall**  
Configure firewall policies, auto-learning policies, and Intrusion Detection System/Intrusion Prevention System (IDS/IPS) policies based on exception detection. If a request violating a security policy reaches the database firewall, database protection reports an alarm in real time or blocks the alarm as required. Database protection can establish user access behavior baselines through machine learning, generate query pattern groups, and apply the query pattern groups to database firewall policies.
- **Separation of duties**  
Manage accounts and permissions in a fine granularity, for example, based on role types, tables, views, or columns.
- **SQL injection detection and protection**  
Make use of the SQL injection feature library, with context-based learning models and a rating mechanism, built in to database protection to comprehensively identify and block SQL injections for your databases in real time.

### Sensitive Data Discovery

- Use the built-in compliance knowledge base for Payment Card Industry (PCI), Healthcare Information Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and General Data Protection Regulation (GDPR); or customize the rule knowledge base and discovery policies for sensitive data.
- Once sensitive data is identified, you can generate sensitive data masking and audit rules in one click.

## Database Data Reduction

Set data reduction rules to detect data operations on specific database tables from unauthorized users, IP addresses, and applications. When the amount of operated data exceeds the specified threshold, database protection will alert administrators and record this event in a data reduction log to prevent data leakage.

## Database Activity Monitoring

- Monitor databases, tables, and columns whose conditions are visualized in tables and charts. Database protection monitors and analyzes database activities and provides alarms about unauthorized activities.
- Database activity monitoring is also called database audit. It allows you to trace attackers based on various types of information, including source IP address, user identity, application, access time, databases requested for access, original SQL statement, operation, operation result, time taken, and content returned. Audit records are remotely stored to ensure compliance.

## Dynamic Data Masking

- Set masking rules for specified database tables or columns, and for queries from specific source IP addresses, users, and applications.
- A precise masking engine is used to mask sensitive data in real time without affecting application performance or changing data stored in the database.

## 3.2 Advantages

Deployed as a reverse proxy between an application server and a database, database protection provides you with database protection functions such as database firewall, database auditing, and dynamic data masking.

- Various functions  
Take advantage of the database audit, database firewall, and data leakage protection functions to effectively audit and protect your databases, and ensure compliance with laws and regulations.
- Few false alarms  
Use SQL injection feature libraries widely recognized in the industry, machine learning models, and a rating mechanism, to keep a low misreporting rate much lower than the industry average.
- Real-time protection  
Use the reverse proxy architecture to block malicious requests in real time.
- Fine-grained permission control  
Manage permissions in fine granularities without modifying the permissions of individual users.
- Powerful dynamic data masking  
Your sensitive data is automatically masked, without affecting the performance of databases and applications.
- Compliance with various regulations
  - Take advantages of accurate check reports. Use SQL injection feature libraries widely recognized in the industry, machine learning models, and

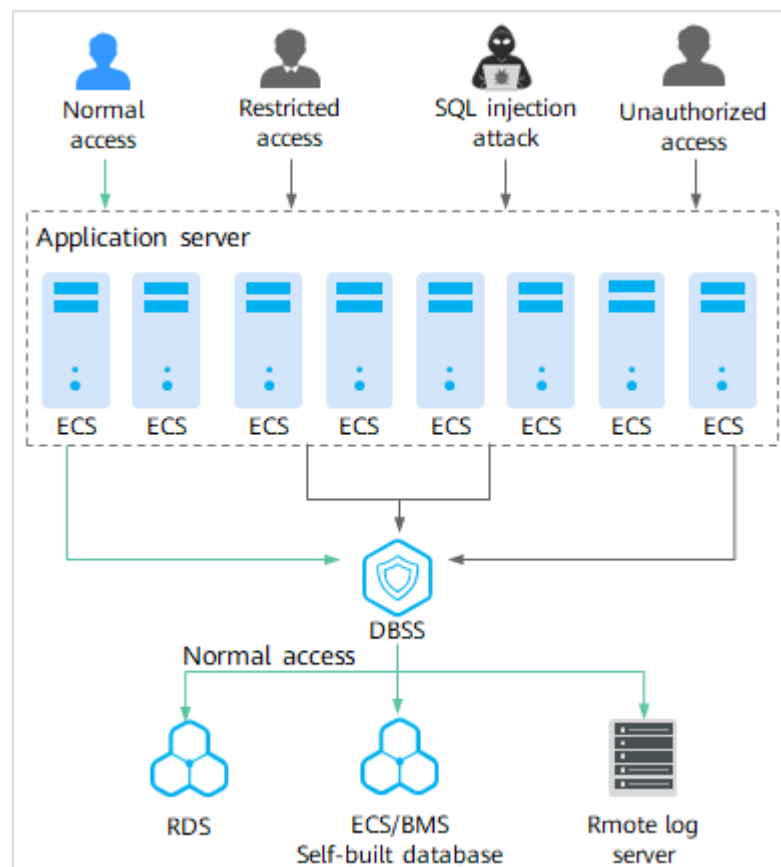
a rating mechanism, to keep a low misreporting rate much lower than the industry average.

- Use the built-in compliance knowledge base to comply with laws and regulations.

### 3.3 Deployment Architecture

Figure 3-1 shows the deployment architecture of database protection.

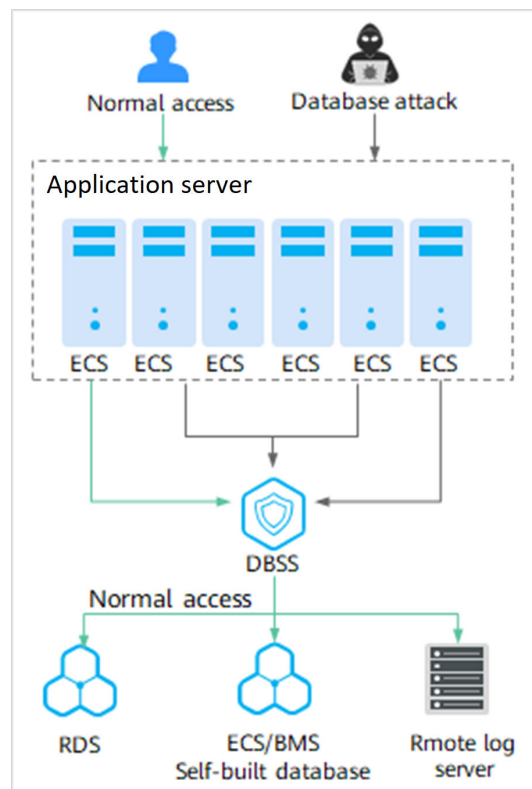
Figure 3-1 Database protection deployment architecture



- Attack prevention  
Database protection provides multiple policies to prevent database attacks and continuously protect databases on the cloud.

Figure 3-2 shows the attack prevention architecture.

**Figure 3-2** Attack prevention architecture

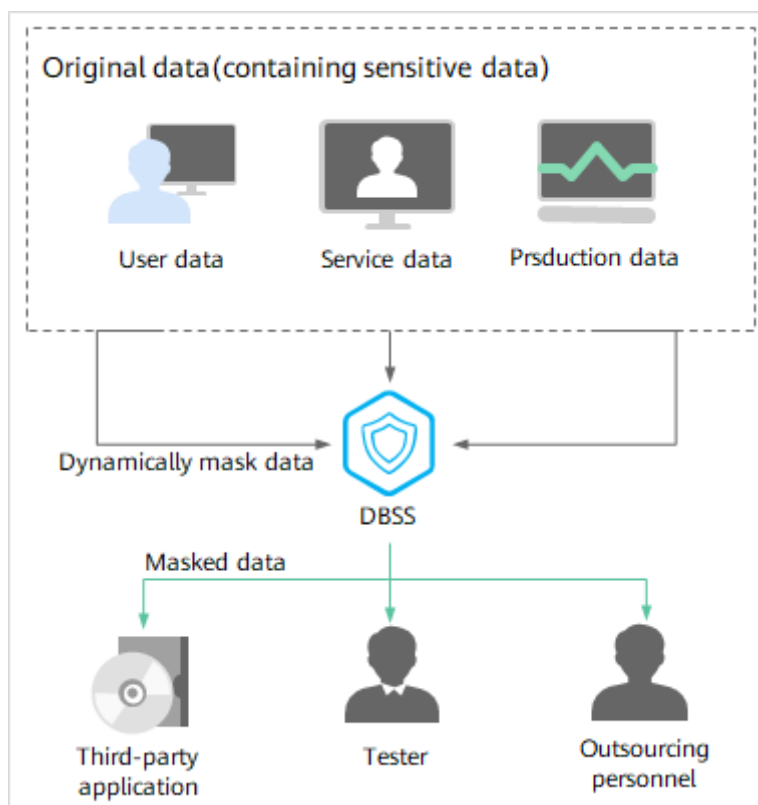


- Data masking

Database protection identifies and dynamically masks sensitive data in users' databases.

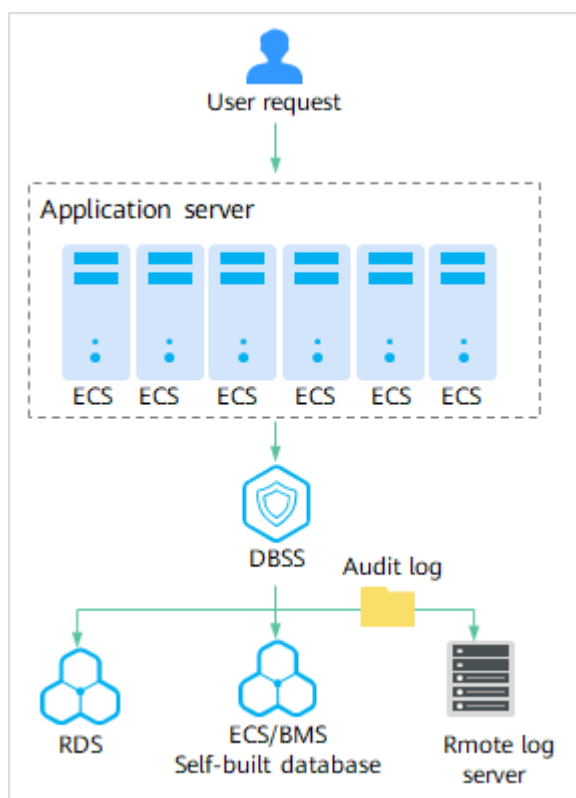
**Figure 3-3** shows the sensitive data masking architecture.

**Figure 3-3** Sensitive data masking architecture



- Database audit  
Database protection supports audits of cloud-based databases. This function meets users' requirements on database audit and log retention. **Figure 3-4** shows the database auditing architecture.

**Figure 3-4** Database audit architecture



## 3.4 Editions

Database protection provides advanced, professional, and premium editions for you to choose from.

[Table 3-1](#) provides more details.

### NOTICE

Based on the reverse proxy and machine learning mechanism, database protection provides functions such as data masking, database audit, sensitive data discovery, data reduction, and anti-injection to ensure database security on the cloud. If you only need to use the database audit function, you are advised to purchase database audit.

**Table 3-1** Database protection editions

Edition	Description
Advanced	Supports a maximum of eight databases and 5,000 concurrent connections.
Enterprise	Supports a maximum of eight databases and 10,000 concurrent connections.

Edition	Description
Premium	Supports a maximum of eight databases and 20,000 concurrent connections.

#### NOTICE

Select an edition that supports your maximum concurrency, or it will probably restrict your service performance. The highest concurrency of your databases depends on how much memory they have been allocated. Select an edition based on your total database memory.

- If the database memory is less than or equal to 32 GB, you are advised to select **Advanced**.
- If the database memory is greater than 32 GB and smaller than 128 GB, you are advised to select **Enterprise**.
- If the database memory is greater than or equal to 128 GB, you are advised to select **Flagship**.

## 3.5 Constraints

Database protection is subject to certain constraints.

### Supported Database Types

The following types of databases on HUAWEI CLOUD can be protected:

- RDS instances
- Databases on ECSs
- Databases on BMSs

### Supported Database Versions

- Microsoft SQL Server 2008 to Microsoft SQL Server 2014
- MySQL 5.5 to MySQL 5.7
- PostgreSQL 9.4 to PostgreSQL 9.5
- DWS 1.2.3

### Restrictions on DDM Usage

When using DDM as a protected database, pay attention to the following restrictions:

- The database protection instances you purchase should be in the same Virtual Private Cloud (VPC) as DDM.
- When configuring protected databases in database protection, you need to configure the connection addresses of the DDM instances. Therefore, confirm the number of the connection addresses of the protected DDM instances and

the database protection type before purchasing database protection instances. A maximum of eight addresses of a DDM are supported.

- Currently, DDM supports only some MySQL syntax. For MySQL syntax that DDM does not support, the database protection proxy can forward the data normally, but DDM will return an error.
- DDM does not support views, functions, and stored procedures. Therefore, database protection does not support views, functions, and stored procedures for DDM.
- The current database protection version does not support DDM as the log storage location.
- DDM users are different from those of MySQL. Database protection cannot obtain DDM user list or generate reports about database users
- The connection between HexaTier and database protection is not encrypted because DDM does not support SSL connections.
- While a protected database is created, database protection needs to connect to the database by using a DDM account with read permission. You can create the account on the DDM management console.
- When creating a protected database, the test connection is required for default databases. You need to configure the existing logical database in DDM instances for the test connection.

## Other Constraints

- If you choose RDS as the remote log database, you must change the value of database configuration parameter **local\_infile** to **ON** (the default value is **OFF**).
- If you want to protect an RDS instance, you must change the value of database configuration parameter **lower\_case\_table\_names** to **1** (the default value is **0**).
- Advanced activity monitoring  
Chinese names of data tables are not supported.

# 4 Billing

This section describes the DBSS billing items, billing modes, and renewal.

## Billing Items

DBSS provides database audit and database protection services, both billed based on the edition and duration you purchase.

The system automatically calculates the price after you select the edition and duration.

**Table 4-1** DBSS billing

Billing Item	Description
Database audit	Billed based on the edition and duration. <ul style="list-style-type: none"><li>• Edition: basic, professional, or advanced</li><li>• Duration: yearly or monthly</li></ul>
Database protection	Billed based on the edition and duration. <ul style="list-style-type: none"><li>• Edition: advanced, enterprise, or flagship</li><li>• Duration: yearly or monthly</li></ul>

## Billing Modes

For now, DBSS only supports yearly/monthly billing and cannot be billed per use. For pricing details, see [Product Pricing Details](#).

## Changing Billing Mode

- To change the edition of your DBSS instance, unsubscribe from it and purchase a new one.

- Unsubscription: To stop using DBSS, go to the Billing Center to [unsubscribe](#) from it.

## Renewal

If you do not renew a DBSS instance that is billed in yearly/monthly mode upon its expiration, a retention period will be granted.

The retention period depends on your level. For details, see [Retention Period](#).

A DBSS instance stops providing services when it expires. To avoid loss caused by security issues, you are advised to renew it in a timely manner. DBSS expiration does not affect your other services.

You can renew your resources on the [Renewals](#) page of the management console. For details, see [Renewal Management](#).

## Expiration and Overdue Payment

- Service expiration

If you do not renew an instance upon its expiration, a retention period will be granted. For details, see [Retention Period](#).

- Overdue payment

For database and asset security purposes, you are advised to top up your account and repay arrears in a timely manner. For details, see [Repaying Arrears](#).

## FAQ

For more charging FAQs, see [DBSS FAQs](#).

# 5 Personal Data Protection Mechanism

To ensure that website visitors' personal data, such as the username, password, and mobile phone number, will not be obtained by unauthorized or unauthenticated entities or people and to prevent data leakage, DBSS controls access to the data and records logs for operations performed on the data.

## Personal Data

[Table 5-1](#) lists the personal data generated or collected by DBSS.

**Table 5-1** Personal data

Type	Collection Method	Can Be Modified	Mandatory
Username	Entered by users on the console login page.	No	Yes Usernames are used to identify users.
Email	Entered by users when configuring email notifications for database audit.	Yes	No

## Storage Mode

- Usernames are not sensitive data and stored in plaintext.
- Emails are encrypted before storage.

## Access Control

Only users having the **DBSS System Administrator** permission can configure email notifications. Users can view only their own emails.

## Logging

All non-query operations on users' personal data, including creating and deleting instances, are recorded in audit logs by DBSS and uploaded to CTS. Users can only view their own audit logs.

# 6 Permissions Management

---

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

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

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

IAM can be used free of charge. You pay only for the resources in your account. For more information about IAM, see [IAM Service Overview](#).

## DBSS Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. After authorization, the user can perform specified operations on BMS based on the permissions.

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

**Table 6-1** describes all the system-defined DBSS roles. DBSS roles are dependent on the roles of other services. When assigning DBSS permissions to users, you need to also assign dependent roles for the DBSS permissions to take effect.

**Table 6-1** System roles supported by DBSS

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

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

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

**Table 6-2** lists the common operations supported by each system-defined permission of DBSS. Select the permissions as needed.

**Table 6-2** Common operations supported by each system-defined permission

Service	Operation	DBSS System Administrator	DBSS Audit Administrator	DBSS Security Administrator
Database Protection	Purchase an instance.	√	×	×
	Obtaining the instance list	√	√	√
	Starting, disabling, and restarting an instance	√	×	×
	Upgrading an instance	√	×	×
	Associating or disassociating an EIP	√	×	×
	Purchasing an instance	√	×	×
Database Audit	Starting, disabling, and restarting an instance	√	×	×
	Obtaining the instance list	√	√	√
	Obtaining the basic information of an instance	√	√	√
	Obtaining the audit statistics	√	√	√

Service	Operation	DBSS System Administrator	DBSS Audit Administrator	DBSS Security Administrator
	Obtaining the monitoring information	√	√	√
	Obtaining the operation logs	√	√	√
	Managing databases	√	×	×
	Managing agents	√	×	×
	Configuring email notifications	√	×	×
	Backup and restoration	√	×	×
	Obtaining the report results	×	√	√
	Obtaining the rule information	×	√	√
	Obtaining the statement information	×	√	√
	Obtaining the session information	×	√	√
	Obtaining the database list	√	√	√
	Managing reports	×	√	√
	Configuring audit rules	×	×	√

Service	Operation	DBSS System Administrator	DBSS Audit Administrator	DBSS Security Administrator
	Configuring alarm notifications	×	×	√

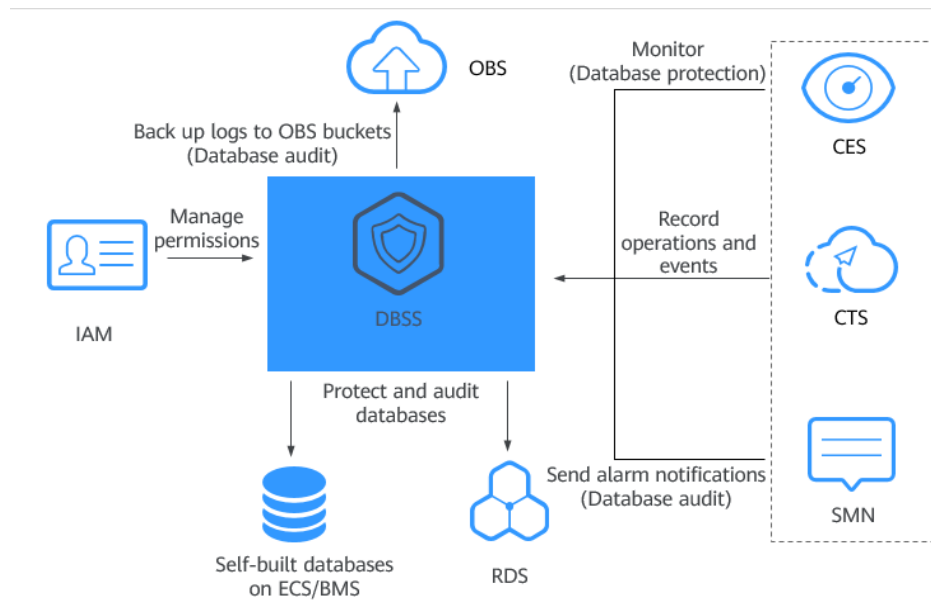
## Helpful Links

- [IAM Service Overview](#)
- [Creating a User Group, a User, and Granting DBSS Permissions](#)

# 7 Related Services

Figure 7-1 illustrates services related to DBSS.

Figure 7-1 Services related to DBSS



## ECS

DBSS instances are created on ECSs. You can use the DBSS instances to protect and audit databases already running on the ECSs.

## RDS

DBSS can protect and audit Relational Database Service (RDS) instances.

## BMS

DBSS can protect and audit databases already running on bare metal servers.

## CTS

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

**Table 7-1** DBSS operations that can be recorded by CTS

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

## Cloud Eye

Cloud Eye monitors metrics of database protection. You can learn about the protection status of database protection by viewing these metrics. For details, see the *Cloud Eye User Guide*.

**Table 7-2** Database protection metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
cpu_util	CPU Usage	CPU usage of the node Unit: %	0 to 100%	server_id	1 minute
mem_util	Memory Usage	Memory usage of the node Unit: %	0 to 100%	server_id	1 minute
hx_process_status	Protected Process Status	Status of the protected process of the node. When the value is <b>1</b> , the status is normal. When the value is <b>0</b> , the status is abnormal.	0, 1	server_id	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
hx_port_status	Port Status	Status of the port used by the protected process of the node. When the value is <b>1</b> , the status is normal. When the value is <b>0</b> , the status is abnormal.	0, 1	server_id	1 minute
hx_proxy_num	Proxy Quantity	Number of proxies configured for the instance, which is only displayed on the active node	0 to 8	server_id	1 minute
hx_proxy_status	Proxy Status	Status of the proxy configured for the instance, which is only displayed on the active node. When the value is <b>1</b> , the status is normal. When the value is <b>0</b> , the status is abnormal.	0, 1	server_id	1 minute
hx_qps	QPS	Number of SQL statement queries per second on the database protected by the instance (including stored procedures), which is only displayed on the active node Unit: queries/s	≥ 0 queries/s	server_id	1 minute
hx_rps	RPS	Number of requests per second to the database protected by the instance, which is only displayed on the active node Unit: requests/s	≥ 0 queries/s	server_id	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
hx_active_connections	Active Connections	Number of active connections of the instance. This parameter is displayed only on the primary node.	0~25000	server_id	1 minute

## OBS

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

## SMN

SMN is an extensible, high-performance message processing service.

- To enable notifications, you must configure SMN first.
- After enabling notifications, you can receive an email when an alarm is triggered or an audit report is generated.
- You can enable or disable alarm notifications on the **Alarm Notifications** tab of the **Settings** page.
- You can enable or disable report notifications on the **Reports** page.

For details about SMN, see *Simple Message Notification User Guide*.

## IAM

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

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

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

# 8 Monitoring Metrics

## Description

This section describes metrics reported by data protection to CES as well as their namespaces and dimensions. You can query the metrics on the CES management console.

## Metrics

**Table 8-1** Database protection metrics

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
cpu_util	CPU Usage	CPU usage of the node Unit: %	0 to 100%	server_id	1 minute
mem_util	Memory Usage	Memory usage of the node Unit: %	0 to 100%	server_id	1 minute
hx_process_status	Protected Process Status	Status of the protected process of the node. When the value is <b>1</b> , the status is normal. When the value is <b>0</b> , the status is abnormal.	0, 1	server_id	1 minute

Metric ID	Metric	Description	Value Range	Monitored Object	Monitoring Period (Original Metric)
hx_port_status	Port Status	Status of the port used by the protected process of the node. When the value is <b>1</b> , the status is normal. When the value is <b>0</b> , the status is abnormal.	0, 1	server_id	1 minute
hx_proxy_num	Proxy Quantity	Number of proxies configured for the instance, which is only displayed on the active node	0 to 8	server_id	1 minute
hx_proxy_status	Proxy Status	Status of the proxy configured for the instance, which is only displayed on the active node. When the value is <b>1</b> , the status is normal. When the value is <b>0</b> , the status is abnormal.	0, 1	server_id	1 minute
hx_qps	QPS	Number of SQL statement queries per second on the database protected by the instance (including stored procedures), which is only displayed on the active node Unit: queries/s	≥ 0 queries/s	server_id	1 minute
hx_rps	RPS	Number of requests per second to the database protected by the instance, which is only displayed on the active node Unit: requests/s	≥ 0 queries/s	server_id	1 minute

<b>Metric ID</b>	<b>Metric</b>	<b>Description</b>	<b>Value Range</b>	<b>Monitored Object</b>	<b>Monitoring Period (Original Metric)</b>
hx_active_connections	Active Connections	Number of active connections of the instance. This parameter is displayed only on the primary node.	0~25000	server_id	1 minute

# A Change History

Released On	Description
2021-02-01	This is the thirty-first official release. Changed the name of the <b>Taurus</b> database to <b>GaussDB for MySQL</b> .
2020-12-25	This is the thirtieth official release. Database types <b>DAMENG</b> and <b>KINGBASE</b> are newly supported by database audit.
2020-12-15	This is the twenty-ninth official release. Added support for CentOS 7.8 and CentOS 8.0 in <b>Constraints</b> .
2020-08-18	This is the twenty-eighth official release. Optimized descriptions in <b>Billing</b> .
2020-07-31	This is the twenty-seventh official release. Added description about dependency on Simple Message Notification (SMN) in <b>Related Services</b> .
2020-07-15	This is the twenty-sixth official release. Optimized descriptions in <b>DBSS</b> .
2020-06-29	This is the twenty-fifth official release. Added the ECS Administrator role required for instance purchase in <b>Permissions Management</b> .
2020-05-25	This is the twenty-fourth official release. Optimized descriptions in <b>Advantages</b> .
2020-05-21	This is the twenty-third official release. Deleted description about the grace period in <b>Billing</b> .

Released On	Description
2020-05-20	This is the twenty-second official release. Added <b>Billing</b> .
2020-04-22	This is the twenty-first official release. Added the support for CentOS 7.6 (64-bit) in <b>Constraints</b> .
2020-04-08	This is the twentieth official release. Updated the email storage mode in <b>Personal Data Protection Mechanism</b> .
2020-03-16	This is the nineteenth official release. Added monitoring metric <b>hx_active_connections_num</b> in <b>Related Services</b> .
2020-03-03	This is the eighteenth official release. <ul style="list-style-type: none"> <li>Modified the specifications in <b>Editions</b>.</li> <li>Added the database types and versions supported by CTS in <b>Constraints</b>.</li> </ul>
2020-02-21	This is the seventeenth official release. Added the Windows OS versions supported by the database audit agent in <b>Constraints</b> .
2020-01-20	This is the sixteenth official release. Optimized descriptions in <b>Permissions Management</b> .
2019-12-05	This is the fifteenth official release. Optimized the structure of "Product Introduction".
2019-11-30	This is the fourteenth official release. Added section "Constraints".
2019-11-05	This is the thirteenth official release. Added <b>Personal Data Protection Mechanism</b> .
2019-10-16	This is the twelfth official release. Optimized descriptions in <b>Functions</b> .
2019-07-02	This is the eleventh official release. Optimized descriptions in <b>DBSS</b> .
2019-06-10	This is the tenth official release. Optimized descriptions in <b>DBSS</b> .
2019-05-30	This is the ninth official release. Modified descriptions in <b>DBSS</b> .

Released On	Description
2019-05-22	This is the eighth official release. <ul style="list-style-type: none"><li>• Added <b>Permissions Management</b>.</li><li>• Optimized descriptions in <b>Related Services</b>.</li></ul>
2019-05-10	This is the seventh official release. Optimized descriptions in <b>DBSS</b> .
2019-03-19	This is the sixth official release. <ul style="list-style-type: none"><li>• Modified descriptions in <b>DBSS</b>.</li><li>• Added <b>Functions</b>.</li><li>• Added <b>Advantages</b>.</li></ul>
2019-01-15	This is the fifth official release. Revised the document outline and optimized the content description.
2018-12-06	This is the fourth official release. Updated the supported database types in section "Database Security Service".
2018-11-07	This is the third official release. Optimized descriptions in <b>Related Services</b> .
2018-07-19	This is the second official release. Added <b>Advantages</b> .
2017-09-15	This is the first official release.