Data Security Center

Service Overview

Issue	01
Date	2024-09-25

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

and other Huawei trademarks are the property 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 Cloud 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.

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 What Is DSC?

The Data Security Center (DSC) is a next-generation, cloud-native data security management platform. It offers fundamental data security features, including data classification and grading, data masking, and data watermarking. The DSC visualizes the overall data security posture in the cloud via an asset map and facilitates comprehensive, one-stop data security operations.

Extensive Range of Data Sources

DSC aggregates various data sources on the cloud and provides one-stop protection for structured and unstructured data on both cloud-native environments and self-built ECSs.

Flexible Data Masking

DSC leverages preset and user-defined masking algorithms to limit exposure of sensitive data, preventing unauthorized access to sensitive data.

NOTICE

DSC only detects sensitive data and does not save data files.

2 Specifications of Different DSC Editions

DSC provides the **standard** and **professional** editions. **Table 2-1** describes the specifications of each edition.

NOTE

- If the number of databases and OBS capacity of the current version cannot meet your service requirements, you can **upgrade edition and specifications**.
- The OBS capacity is the **used capacity** of the OBS bucket. On the OBS console, choose **Buckets** to view the **used capacity** of the bucket. Select an OBS volume that is greater than or equal to the **used capacity** of the OBS bucket.

Table 2-1 Specifications of different DSC editions

Edition	Database Quantity	OBS Capacity	API Calling Quota	Function
Standard	2	100	Not supported	• Asset Map • Sensitive Data Identification • Data Risk Detection
Professional	2	100	1,000,000 times	• Asset Map • Sensitive data identification • Risk detection • Data masking • Data watermark injection/extraction • API calling

3 Functions

Table 3-1 lists the DSC functions.

Table 3-1 DSC functions

Function	Description	Reference Document
Asset Map	You can view multiple aspects of your asset security, such as asset overview, categories and levels, permission configuration, data storage, and sensitive data. This helps you quickly detect risky assets and handle them. ● Asset Visualization – Service data assets: All data assets on the cloud, including OBS, RDS, CSS, Hive, and HBase assets are visualized. – Data risk: The categorization and leveling results display the risk levels of data. – Region display: The region where each asset is located is displayed based on the cloud resource VPC and associated with the service region. ● Egress Visualization – Data egresses: All data egresses on the cloud are identified, including EIP, NAT, API Gateway, and ROMA. – Asset and egress association: Cloud egresses are associated with data assets and data asset categorization and leveling results. – Cascading association: Egresses and the cascading egresses are displayed. ● Policy Visualization – Data security policies: All security policies of data assets are detected based on cloud native capabilities and policy risks are displayed. – Policy recommendation: Different security policy configurations are recommended based on the data asset level.	**Asset Map**

Function	Description	Reference Document
Asset Management	● **Asset center**: You can manage data assets from OBS, databases, big data, Log Tank Service (LTS), and MRS. ● **Asset catalog**: You can view statistics about your data from different domains or of different types. ● **Data exploration**: You can view details about all the added data assets and add descriptions, tags, security levels, and classifications to databases, tables, and data views to manage data assets by level and classification. ● **Metadata tasks**: You can create metadata tasks to collect data assets as metadata. In this way, you can manage data assets by level and classification. ● **Asset group management**: Data can be managed by group.	**Allowing or Disallowing Access to Cloud Assets**

Function	Description	Reference Document
Sensitive Data Identification	● **Automatic data classification and grading**: DSC automatically discovers and analyzes sensitive data. Utilizing DSC's data identification engines, both structured data (RDS and DWS) and unstructured data (OBS) are scanned, classified, and graded. This process ensures continuous identification and analysis of sensitive data to enhance security. – File types: DSC can identify sensitive data from over 200 types of unstructured files. – Data types: DSC is able to identify dozens of personal privacy data types (Chinese or English). – Image types: DSC is able to identify sensitive words (Chinese and English) in eight types of images such as PNG, JPEG, x-portable-pixmap, TIFF, BMP, GIF, JPX, and JP2. ● **Automatic identification of sensitive data** – Automatic identification of sensitive data and personal privacy data – Customized identification rules to meet various requirements of different industries – Visualized identification results which can be downloaded to the local PC The identification duration depends on the data volume, number of identification rules, and scan mode. For details, see **How Long Does It Take for DSC to Identify and Mask Sensitive Data?**	**Creating a Sensitive Data Identification TaskCreating a Sensitive Data Identification Task**

Function	Description	Reference Document
Data Masking	Supports static data masking and dynamic data masking. Data masking has the following features: ● **Zero impact**: DSC reads data from original databases, statically masks sensitive data using precise masking engines, and saves the masked data separately without affecting your data assets. ● **Various data sources**: Data of various sources on the cloud, such as RDS, self-built databases on ECSs, or big data, can be masked to meet security requirements. ● **Custom data masking policies**: DSC provides you with over 20 preset data masking rules. You can use the default masking rules or customize the masking rules to mask sensitive data in the specified database table. For details about the data masking algorithms supported by DSC, see **Data Masking Algorithms**. ● **Easy and quick masking rule configuration for security compliance**: Easy and quick data masking rule configuration can be achieved based on data scanning results. In addition, DSC provides APIs for dynamic data masking. For details, see **Dynamic Data Masking**. DSC uses preset and customized masking algorithms to mask sensitive data stored in RDS, Elasticsearch, MRS, Hive, HBase, DLI, and OBS. For details about the masking duration, see **How Long Does It Take for DSC to Identify and Mask Sensitive Data?**	**Configuring a Data Masking Rule**

Function	Description	Reference Document
Data Watermarking	Provides the functions of adding and extracting watermarks for databases and documents. ● **Copyright proof**: The owner information is added to the assets to specify the ownership, achieving copyright protection. ● **Automated monitoring**: The user information is added to the assets for tracing data leak. DSC provides APIs for dynamically adding data watermarks and extracting watermarks from data. For details, see **DSC API Reference**.	**Watermark Injection**
Dashboard	By default, DSC provides an integrated situational awareness dashboard that presents a thorough analysis of risky assets, identification, masking, and watermarking tasks, as well as events and alarms in the cloud. This dashboard facilitates swift recognition and response to the overall status of assets, including addressing risky assets and urgent alarms.	**Large Screen**
Alarms	When a system or service risk alarm is generated for DBSS, the alarm event is sent to DSC. You can view the alarm event on the DSC console.	**Alarm Management**
Events	DSC integrates with key security components, including Database Audit, and Cloud Bastion Host, enabling centralized event management and real-time event delivery to DSC. This allows users to promptly verify and handle events. You can also convert alarms on the **Alarm Management** page to events.	**Event Management**
OBS Usage Audit	DSC detects OBS buckets based on sensitive data identification rules and monitors identified sensitive data. After abnormal operations of the sensitive data are detected, DSC allows you to view the monitoring result and handle the abnormal events as required.	**OBS Usage Audit**

Function	Description	Reference Document
Alarm Notifications	Sends notifications through the notification method configured by users when sensitive data identification is completed or abnormal events are detected.	**Alarm Notifications**

4 Advantages

Actionable Insights into Data Security

DSC displays security status in data collection, transmission, storage, exchange, usage and deletion. You can efficiently locate the risks and take immediate actions to ensure data security.

Extensive Range of Data Sources

DSC provides one-stop protection for both structured and unstructured data from a wide range of sources, such as Object Storage Service, databases (self-built databases on ECSs), and big data sources.

Efficient Identification

DSC efficiently identifies sensitive data sources based on expert knowledge bases and Natural Language Processing (NLP).

Flexible Data Masking

DSC leverages preset and user-defined masking algorithms to limit exposure of sensitive data, preventing unauthorized access to sensitive data.

5 Applicable Scenarios

Automatic Identification and Classification of Sensitive Data

DSC automatically identifies sensitive data and analyzes the usage of such data. With data identification engines, DSC scans and classifies structured data and unstructured data in RDS and OBS. It then automatically identifies sensitive data and analyzes the usage of such data for further ensuring security.

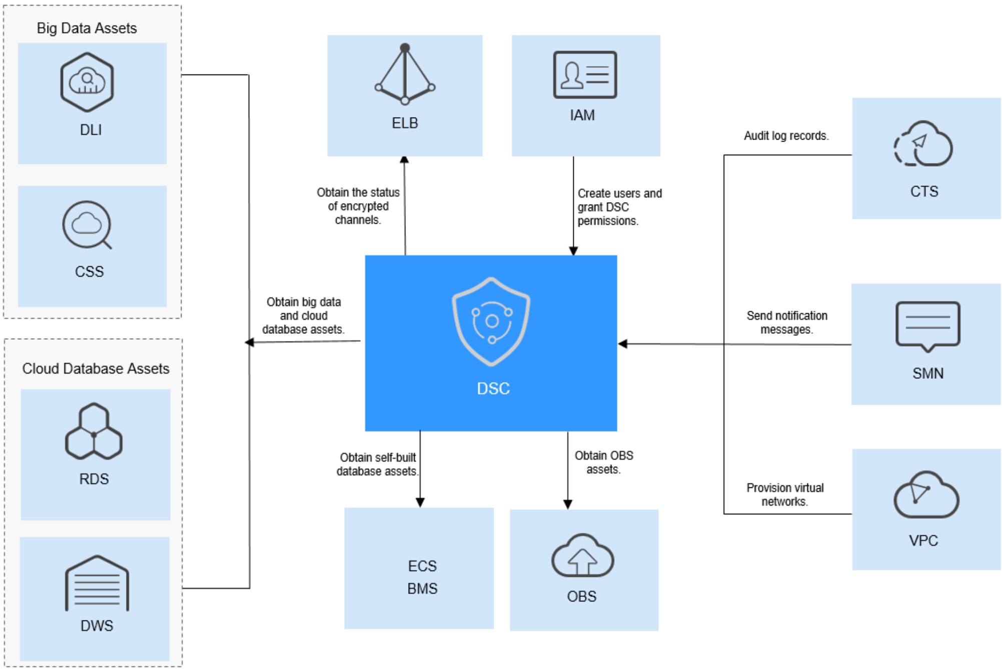
Data Masking

DSC builds a data masking engine by leveraging multiple preset and customized masking algorithms. It then masks structured and unstructured data for storage.

6 DSC and Related Services

Figure 6-1 shows the relationships between DSC and related services.

Figure 6-1 DSC and related services


Big Data Assets
DLI
CSS
Cloud Database Assets
RDS
DWS
ELB
IAM
Obtain the status of encrypted channels.
Create users and grant DSC permissions.
Obtain big data and cloud database assets.
DSC
Audit log records.
CTS
Send notification messages.
SMN
Provision virtual networks.
VPC
Obtain self-built database assets.
Obtain OBS assets.
ECS
BMS
OBS

OBS

Object Storage Service (OBS) is a stable, secure, efficient, and easy-to-use cloud storage service that can store any amount and form of unstructured data. After OBS access permissions are granted, DSC is allowed to automatically identify and classify sensitive data, analyze abnormal user behaviors, and protect data stored in OBS.

RDS

Relational Database Service (RDS) is a cloud-based web service that is reliable, scalable, easy to manage, and immediately ready for use. After RDS access permissions are granted, DSC is allowed to automatically identify and classify sensitive data and protect data stored in RDS instances.

DWS

Data Warehouse Service (DWS) is an online data processing database that uses the cloud infrastructure to provide scalable, fully-managed, and immediately read for use database services. After DWS access permissions are granted, DSC is allowed to automatically identify and classify sensitive data and protect data stored in DWS.

ECS

Elastic Cloud Server (ECS) is a cloud server that provides scalable, on-demand computing resources. After ECS access permissions are granted, DSC is allowed to automatically identify and classify sensitive data and protect data stored in self-built databases on ECSs.

Bare Metal Server (BMS)

Bare Metal Server (BMS) features both the scalability of VMs and high performance of physical servers. After BMS access permissions are granted, DSC is allowed to automatically identify and classify sensitive data and protect data stored in self-built databases on BMSs.

CSS

Cloud Search Service (CSS) is a fully managed, distributed search service. It is fully compatible with open-source Elasticsearch and provides functions including structured and unstructured data search, statistics, and reporting. The process of using CSS is similar to that of using a database. After CSS access permissions are granted, DSC is allowed to automatically identify and classify sensitive data and protect data stored in big data assets on CSS.

DLI

Data Lake Insight (DLI) is a Serverless big data compute and analysis service that is fully compatible with Apache Spark, Apache Flink, and openLooKeng (Apache Presto) ecosystems. With multi-model engines, enterprises can use SQL statements or programs to easily complete batch processing, stream processing, in-memory computing, and machine learning of heterogeneous data sources. After DLI access permissions are granted, DSC is allowed to automatically identify and classify sensitive data and protect data stored in big data assets on DLI.

MRS

MapReduce Service (MRS) provides enterprise-level big data clusters on the cloud. Tenants can fully control the clusters and run big data components such as Hadoop, Spark, HBase, Kafka, and Storm in the clusters. After MRS access permissions are granted, DSC is allowed to automatically identify and classify sensitive data and protect data stored in Hive on CSS.

ELB

DSC is bound to to query the encryption communications status.

SMN

Simple Message Notification (SMN) provides the message notification function. Once this function is enabled, DSC sends messages to you by email when sensitive data identification is complete or an abnormal event is detected.

Relationship with CTS

Cloud Trace Service (CTS) is used to record the operations you have performed using DSC for later querying, auditing, or backtracking.

VPC

Virtual Private Cloud (VPC) enables you to provision logically isolated, configurable, and manageable virtual networks for cloud servers, cloud containers, and cloud databases, improving cloud service security and simplifying network deployment.

IAM

Identity and Access Management (IAM) provides you with permission management for DSC. Only users who have Tenant Administrator permissions can perform operations such as authorizing, managing, and detect cloud assets using DSC. To obtain the permissions, contact the users who have the Security Administrator permissions.

7 Constraints

DSC can only manage data assets on HUAWEI CLOUD at present.

Supported Huawei Cloud Data Sources

- Relational Database Service (RDS)
- Object Storage Service (OBS)

  NOTE

  OBS supports only bucket lists and does not support parallel file systems.
- Data Warehouse Service (DWS)
- Cloud Search Service (CSS)
- Data Lake Insight (DLI)
- GaussDB
- Databases on Elastic Cloud Servers (ECSs)
- Databases on Bare Metal Servers (BMSs)
- Log Tank Service (LTS)

Supported Datasource Versions

Table 7-1 lists the asset types and versions supported by DSC.

Table 7-1 Asset sources and versions supported by DSC

Data Source	Version
MySQL	5.6, 5.7, 5.8, and 8.0
SQL Server	● 2017_SE, 2017_EE, and 2017_WEB ● 2016_SE, 2016_EE, and 2016_WEB ● 2014_SE and 2014_EE ● 2012_SE, 2012_EE, and 2012_WEB ● 2008_R2_EE and 2008_R2_WEB
Kingbase	V8

Data Source	Version
DMDBMS (Dameng)	7 and 8
PostgreSQL	11, 10, 9.6, 9.5, 9.4, and 9.1
TDSQL	10.3.X
Oracle	11, 12
DDS	4.2, 4.0, and 3.4
DWS	4.2, 4.0, and 3.4
Elasticsearch	5.x, 6.x, and 7.x
DLI	1.0
Hive	1.0
HBase	1.0
OBS	V3

Data Sources Supported by Sensitive Data Identification

Table 7-2 Data sources supported by sensitive data identification

Asset Type	Data Source Type
OBS	OBS bucket
Databases	RDS, DWS, DDS, GaussDB, and self-built databases (MySQL, TDSQL, KingBase, DMDBMS, PostgreSQL, SQLServer, and Oracle)
Big data	Elasticsearch, DLI, Hive, HBase
Logs	LTS

Data Sources Supported by Data Masking

Table 7-3 Data sources supported by data masking

Masking Type	Asset Type	Data Source
Data masking	Database	SQLServer, MySQL, TDSQL, PostgreSQL, KingBase, DMDBMS, OpenGauss, Oracle, and DWS
Elasticsearch masking	Big data	Elasticsearch

Masking Type	Asset Type	Data Source
Hive masking		Hive
HBase masking		HBase
DLI masking	Big data	DLI
MRS masking	MRS	MRS_HIVE

Data Sources Supported by Data Watermarking

Table 7-4 Data source types supported by data watermarking

Watermarking Target	Watermark Type	Data Source
Databases	Lossy - column watermark	DWS and MRS_HIVE databases
	Lossless - pseudocolumn/pseudorow watermarking	DWS, PostgreSQL, and MySQL databases
Documents	-	OBS buckets and local files
Images	-	OBS buckets and local files

8 Personal Data Protection Mechanism

To ensure that your personal data, such as the username, password, and mobile phone number, will not be leaked or obtained by unauthorized or unauthenticated entities or people, DSC controls access to the data and records logs for operations performed on the data.

Personal Data

Table 8-1 lists the personal data generated or collected by DSC.

Table 8-1 Personal data

Type	Source	Modifiable	Mandatory
Tenant ID	● Tenant ID in the token used for authentication when an operation is performed on the console ● Tenant ID in the token used for authentication when an API is called	No	Yes
Password	Entered by the tenant on the console	Yes	Yes. When scanning, desensitizing, and injecting watermarks to database data, DSC needs to use the database password to connect to the database and obtain data.

Storage Mode

- Tenant ID is not sensitive data and can be stored in plaintext.
- Database password: encrypted for storage.

Access Permission Control

Users can view only logs related to their own services.

Log Records

DSC records logs for all operations, such as modifying, querying, and deleting, performed on personal data. The logs are uploaded to Cloud Trace Service (CTS). You can view only the logs generated for operations you performed.

9 Permissions Management

If you want to assign different access permissions to employees in an enterprise for the DSC resources purchased on HUAWEI CLOUD, you can use Identity and Access Management (IAM) to perform refined permission management. IAM provides identity authentication, permissions management, and access control, helping you efficiently manage access to your DSC resources.

With IAM, you can create IAM users under your account for your employees, and assign permissions to these IAM users to control their access to DSC resources. For example, if you have software developers and you want to assign them the permission to access DSC but not to delete DSC or its resources, you can create an IAM policy to assign the developers the permission to access DSC but prevent them from deleting DSC data.

If your HUAWEI CLOUD account does not require individual IAM users for permissions management, skip this section.

IAM is free. You pay only for the resources in your account. For more information about IAM, see **IAM Service Overview**.

DSC Permissions

By default, new IAM users do not have any permissions. You need to add a user to one or more groups, and attach permission policies or roles to these groups. Users inherit permissions from their groups and can perform specified operations on cloud services based on the permissions.

DSC is a project-level service deployed and accessed in specific physical regions. To assign 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. To access DSC, the users need to switch to a region where they have been authorized to use cloud services.

You can grant users permissions by using roles and policies.

- Roles: A coarse-grained authorization mechanism provided by IAM to define permissions based on users' job responsibilities. This mechanism provides a limited number of service-level roles for authorization. You need to also assign other dependent roles for the permission control to take effect. Roles are not an ideal choice for fine-grained authorization and secure access control.

- Policies: A fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, meeting requirements for secure access control. For example, you can grant DSC users the permissions to manage only a certain type of resources.

Table 9-1 describes the system-defined policies of DSC.

Table 9-1 DSC system permissions

Policy	Description	Type	Dependency
DSC DashboardReadOnlyAccess	Read-only permissions for the overview page of DSC	System-defined policy	None
DSC FullAccess	All permissions for DSC	System-defined policy	To purchase a yearly/monthly RDS DB instance, you need to configure the following actions: bss:order:update bss:order:pay
DSC ReadOnlyAccess	Read-only permissions for Data Security Center	System-defined policy	None

NOTICE

Only users with the **Security Administrator** permission can perform **Allowing or Disallowing Access to Cloud Assets**.

Helpful Links

- **IAM Service Overview**
- **Creating a User and Assigning DSC Permissions**