**Data Security Center** 

# **Best Practices**

 Issue
 06

 Date
 2024-10-31





HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

### Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. 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 Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**

NUAWEI 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 How Do I Prevent Personal Sensitive Data From Being Disclosed During	
Development and Testing?	1
2 Best Practices of OBS Data Security Protection	10

# How Do I Prevent Personal Sensitive Data From Being Disclosed During Development and Testing?

Sensitive data refers to information that, if accessed, disclosed, or misused by unauthorized persons, may pose serious risks to individuals or organizations.

- For individuals, this includes personal information such as ID card numbers, home addresses, employers, and bank card numbers.
- For enterprises or organizations, sensitive data encompasses core information such as customer data, financial details, technical information, and major decisions.

Huawei Cloud Data Security Center (DSC) can perform static data masking on a large amount of data in one operation based on anonymization rules. Static anonymization is usually used when sensitive data in the production environment needs to be transferred to the development, test, or outside environment. It is applicable to scenarios such as development and test, data sharing, and data research.

# **Common Causes of Data Breaches**

- Insider leakage
  - Laptops or mobile devices are lost or stolen.
  - Sensitive data or storage is accessed by unauthorized personal
  - Sensitive data is sent, printed, and copied by employees.
  - Sensitive data is accidentally transmitted out.
- Leakage caused by external attacks
  - Data access is uncontrollable, or there are security vulnerabilities in the data storage system.
  - Improper configurations allow external attacks.
  - Sensitive data or storage is accessed by unauthorized personal

# Scenario

Assume that the **dsc\_bank** table in the **rsd-dsc-test** database stores the information of the following bank employees:

Figure 1-1 Bank employee information

Name	Birthday	Email	address
San Zhang	1999-06-03 10:10:00	13577 5@163.com	Chengdu, Sichuan
Si Li	1990-08-03 05:05:00	552 3gqq.com	Beijing

To identify and mask sensitive data in the table, you need to first identify the sensitive data and generate an identification result report, then mask the identified sensitive data using the **Hash masking** algorithm SHA256.

# Step 1: Purchasing a DSC Professional Edition Instance

- Step 1 Log in to the management console.
- **Step 2** Click **Sec** in the upper left corner and select a region or project.
- Step 3 In the navigation tree on the left, click =. Choose Security & Compliance > Data Security Center.
- Step 4 If you are a first-time user, click Buy DSC.
- Step 5 On the Buy DSC page, select a Region.

#### Figure 1-2 Selecting a region and edition

* Billing Mode	Yearly/Monthly	
* Region	• CN South-Guangzhou         •           Select a region where your data services reside. Separ	rate DSC instance purchase is required for your data services in different region
* Project	cn-south-1(default)	
* Edition	Standard         Satisfied basic compliance requirements         Database quantity       2         OBS storage       100 GB <ul> <li>Asset Map</li> <li>Sensitive Data Identification</li> <li>Risk Detection</li> <li>Data Masking</li> <li>Watermark injection/extraction</li> </ul> <ul> <li>Supported</li> <li>Not supported</li> <li>Not supported</li> </ul>	Professional         Satisfied basic compliance requirements         Database quantity       2         DBS storage       100 GB         ✓ Asset Map         ✓ Sensitive Data Identification         ✓ Risk Detection         ✓ Data Masking         ✓ Watermark injection/extraction

#### **NOTE**

To switch a region, select a region from the **Region** drop-down list. Only one DSC edition can be purchased in a region.

#### **Step 6** Set **Database Expansion Package** and **OBS Expansion Package**.

#### Figure 1-3 Selecting expansion packages

Database Expansion Package	?	0       +       One expansion package offers one database instance.         RDS and DWS databases, self-built databases on ECSs, DLI, Elasticsearch, and big data on ECSs are supported.
OBS Expansion Package	?	0 + One OBS expansion package offers 1 TB of OBS storage.

- One expansion package offers one database instance. RDS and DWS databases, self-built databases on ECSs, DLI, Elasticsearch, and big data on ECSs are supported.
- One OBS expansion package offers 1 TB (1024 GB) of OBS storage.
- **Step 7** Set **Required Duration**. Select the required duration from one month to three years.

Figure 1-4 Setting required duration

Required Duration	Cost Estimate (excluding pay-per-use) Starting from ¥100.00/day ¥83.00/day ¥70.00/day ¥50.00/day	
	1         2         3         4         5         6         7         8         9 months         1 year         2 years         3 years           ✓ Auto-renew              3 years         3 years	
Price		
This price is an estimate a	and may differ from the final price. Pricing details	Next

#### **NOTE**

Select **Auto-renew** to enable the system to renew your service by the purchased period when the service is about to expire.

Step 8 Click Next.

If you have any questions about the pricing, click Pricing details.

Step 9 Confirm the order information and agree to the DSC disclaimer by selecting I have read and agree to the Data Security Center Service Statement and click Pay Now.

Figure 1-5 Viewing details

Product Type	Specifications		Billing Mode	Required Duration	Discount	Price
	Standard					
Data Security Center	Database instance quantity	2	Yearly/Monthly	1 month	¥0.00	
	OBS storage	100GB				

**Step 10** Select a payment method to pay for your order on the displayed page.

----End

# Step 2: Identifying Sensitive Data

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

- Step 2 In the left navigation page, click =, and choose Security > Data Security Center.
- **Step 3** In the left navigation pane, choose **Sensitive Data Identification** > **Identification Task**.
- **Step 4** Click **Create Task**. In the displayed dialog box, configure the basic parameters.

Parameter	Description	Example Value
Task Name	<ul> <li>You can customize the task name.</li> <li>The task name must:</li> <li>Contain 4 to 255 characters.</li> <li>Consist of letters, digits, underscores (_), and hyphens (-).</li> <li>Start with a letter.</li> <li>Be unique.</li> </ul>	DSC_Test
Data Type	<ul> <li>Type of data to be identified. You can select multiple types.</li> <li>OBS: DSC is authorized to access your Huawei Cloud OBS assets and identify sensitive data in the assets. For details about how to add OBS assets, see Adding OBS Assets.</li> <li>Database: DSC identifies sensitive data of authorized database assets. For details about how to authorize database assets, see Authorizing Access to a Database Asset.</li> <li>Big Data: The DSC identifies sensitive data source assets, see Authorize big data source assets, see Authorizing Access to Big Data Assets.</li> <li>MRS: DSC identifies sensitive data of authorized MRS assets. For details about authorized MRS assets, see Authorizing Access to Big Data Assets.</li> <li>ITS: DSC will identify sensitive data of authorized LTS assets. For details about how to add a log stream, see Adding a Log Stream.</li> </ul>	Database > rsd-dsc- test

<b>Idule 1-1</b> Parameters for creating a sensitive data identification tas	Table 1-1	Parameters	for creating	a sensitive data	identification t	task
--	-----------	------------	--------------	------------------	------------------	------

Parameter	Description	Example Value
Identificatio n Template	You can select a built-in or custom template. DSC displays data by level and category based on the template you select. For details about how to add a template, see Adding an Identification Template.	Huawei Cloud Data Security Classifying and Grading Template
Identificatio n Period	Set the execution policy of the data identification task.	Once
	• <b>Once</b> : The task will be executed once at a specified time.	
	• <b>Daily</b> : The task is executed at a fixed time every day.	
	<ul> <li>Weekly: The task is executed at a specified time every week.</li> </ul>	
	<ul> <li>Monthly: The task is executed at a specified time every month.</li> </ul>	
When to Execute	This parameter is displayed when Identification Period is set to Once.	Now
	• Now: Select the option and click OK, the system executes the data identification task immediately.	
	<ul> <li>As scheduled: The task will be executed at a specified time.</li> </ul>	

**Step 5** Click **OK**. The sensitive data identification task list is displayed.

Figure 1-6 Sensitive data identification task list

	Task Name	Identification Template	Execution Per	Status	Last Identified	Last Identified R	Notification Topic	Operation	
^	DSC_Test	Huawei Cloud data security cat	Once	Identification completed	2024/10/15 11:04:19 GMT+08:00			Start Identification Identif	ication Result More ~
Asset		Data Type	Status			Risk Level	Last Identified	Operat	ion
rsd-dsc-t	est	Database	Identification co	mpleted			2024/10/15 11:04:19 GMT+08	:00 Start Io	entification Identification Res

**Step 6** When the status of the identification task changes to **Identification completed**. Click **View Result** in the **Operation** column to go to the result details page.

DSC_Test	✓ All types ✓	All Assets 🗸				
All Sensitive Data Tabl	es			Top 10 Matched Rules		
				Taiwan compatriot permit num	ber	1
				Birthday		1
				Email		1
				Time		1
	$\bigcirc$	<ul> <li>L3 1 (25.00%)</li> <li>L2 1 (25.00%)</li> <li>N/A 2 (50.00%)</li> </ul>				
0.000						Generate Result File Download
Q Select a property o	r enter a keyword.					Q
Object	Asset Type	Asset	Database	Table Name	Object Path/Collection Time Level 😣	Operation
address	Database	rsd-dsc-test	rsd-dsc-test	"dsc_bank"	rsd-dsc-test/'dsc_bank'/address N/A	View Leveling and Details
Name	Database	rsd-dsc-test	rsd-dsc-test	"dsc_bank"	rsd-dsc-test/'dsc_bank'/Name N/A	View Leveling and Details
Email	Database	rsd-dsc-test	rsd-dsc-test	"dsc_bank"	rsd-dsc-test/'dsc_bank'/Email L3	View Leveling and Details
Birthday	Database	rsd-dsc-test	rsd-dsc-test	"dsc bank"	rsd-dsc-test/'dsc bank'/Birthday L2	View Leveling and Details

### Figure 1-7 Identification result details

The birthday dates and email addresses are identified as sensitive data, as shown in **Figure 1-7**.

Step 7 Click View Leveling and Details to view the result details.

Figure 1-8 Categorizing and leveling results

Identification Object Details									
Object	Email		Object Pat	h/Collection Time	rsd-ds	sc-test/"dsc_bank"/Email			
Asset	rsd-dsc-test		Asset Type	3	Datab	ase			
Level	L3								
Result [	Details	Sample	Data						
Rule		Level		Category		Categorizing and Le			
Taiwan	compatriot	L3		Authoritative socia	al i	Huawei Cloud data se			
Email		L3		General personal	inf	Huawei Cloud data se			

Categorizing and Leveling Results

Perform operations described in **Step 3: Performing Static Data Masking** to mask the sensitive data in the **Birthday** and **Email** columns of the **dsc\_bank** table in the **rsd-dsc-test** database.

----End

# Step 3: Performing Static Data Masking

DSC allows you to create masking tasks for various data sources such as databases, Elasticsearch, MRS, and Hive. This section describes how to create a static masking task for a database. For details about other masking methods, see the following:

- Creating and Running an Elasticsearch Data Masking Task
- Creating and Running an MRS Data Masking Task.
- Creating and Running a Hive Masking Task.
- Creating and Running an HBase Masking Task.
- Creating a DLI Masking Task.
- Creating an OBS Masking Task.
- Step 1 In the left navigation pane, choose Data Asset Protection > Static Data Masking. The Data Masking page is displayed.

Step 2 Set Mask Sensitive RDS Data to



**Step 3** Click **Create Task** to configure the data source.

Select all data types if you want a complete table that contains all types of data after the data masking is completed.

#### Figure 1-9 Data source configuration

1 Configure Data Sou	rce 2 Set Masking Algorithm	Onfigure Data Masking     Period     Set Tan	get Data		
* Task Name	DSC_Test				
* Select Data Source	MySQL ~				
* Data Source	Database Instance rds-1b96	Database	Table Name ③	~	Add Databa
	Column Name	Risk Level	Data Type		
	address	0	varchar		
	Iiithday Birthday	3	datetime		
	🗹 Email	6	varchar		
	Name	0	varchar		
Masking Ratio	100 %				
Next Canc	el				



#### Figure 1-10 Configuring the data masking algorithm

Configure Dat	a Source — 2 Set Masking Algorithm –	3 Cor Per	nfigure Data Masking riod	4 Set Target Data
Data Source rds-1b96 /rsd-dsc-	test /"dsc_bank"			
	Column Name	Data Type	Masking Algorithm	
$\checkmark$	Birthday	datetime	Value Change ~	Masking Using the Null Va 🗸 Edit
$\checkmark$	Email	varchar	Hash ~	SHA256 V Edit
Total: 2				
Previous	Next Cancel			

**Step 5** Click **Next** to switch to the **Configure Data Masking Period** page and configure the data masking period.

○ Configure Data Source	🕑 Set M	asking Algorithm 3 Configure Data Masking (4) Set Target	t Data
Masking Period	<ul> <li>On demand</li> </ul>	Click Execute in the rule list to trigger a one-time masking task.	
		00 🗸 : 00 🗸	
	O Daily	00 🗸 : 00 🗸 : 00 🗸	
	O Weekly	Sunday 🗸 : 00:00:00 🗸	
	O Monthly	1st day 🗸 at 00:00:00 ∨	
Incremental Masking 🧿			
Previous Next	Cancel		

#### Figure 1-11 Configuring the data masking period

**Step 6** Click **Next** to the **Set Target Data** page and configure the storage location of the table generated after data masking.

**Figure 1-12** Configuring the storage location of the table generated after data masking

📀 Configure Data Source — 🕓 Set Masking Algorithm —	Configure Data Masking Period	(d) Set Target Data
Database Instance rds-1b96	Database V rsd-dsc-test	Table Name
Data Source Column Birthday	Risk Level	Target Column Birthday
Email	6	Email
Previous Finish Cancel		

**Step 7** Click **Finish** to return to the database data masking task list. Click to enable the masking task and then **Execute** in the **Operation** column to execute the task.

If the status changes to **Completed**, the data masking task has been successfully executed.

Figure 1-	13	Identification	and	masking	completed
-----------	----	----------------	-----	---------	-----------

	Enable/Disable	Task Name	Data Source/Target		Maskin	ig Period	Operation
^		DSC_Test	$rsd-dsc-test \longrightarrow rsd-dsc-test$		On den	nand	Execute Edit Delete
Start Time 🝦		End	Time	Execution Method	Executed Lines	Status	
2024/10/15 11:22:20 G	MT+08:00	2024	/10/15 11:24:04 GMT+08:00	On demand	2	Completed	

----End

# Verifying the Result

Birthday	÷	Email
(Null)		fb1d058a45cf4f67ac92c0142e60e3737a262f7aa860db40241c52f26e4773e2
(Null)		97dcf0644f0d5665e699d7a17e32dee325d67249f66afea58f09ab3f1a4c8f36

# **2** Best Practices of OBS Data Security Protection

This document describes how to use the Data Security Center (DSC) to identify, classify, and protect sensitive data stored in OBS.

## Overview

Sensitive data includes personal privacy information, passwords, keys, sensitive images, and other high-value data. Such data is usually stored in your OBS bucket in different formats. Once the data is leaked, enterprises will suffer significant economic and reputation losses.

After you authorize DSC to perform identification on the data source, DSC quickly identifies sensitive data from your massive data stored in OBS, classify the sensitive data and display it. DSC also traces the usage of sensitive data, and protects and audits data based on predefined security policies. In this way, DSC allows you to learn about the security status of your OBS data assets at any time.

# **Application Scenario**

• Sensitive data identification

OBS stores a large amount of data and files. However, it is difficult to have a clear knowledge of the sensitive information contained in OBS.

You can use the built-in algorithm rules of DSC or customize industry rules to scan, classify, and grade data stored in OBS, and take further security protection measures based on the scanning results. For example, you can use the access control and encryption functions of OBS.

• Anomaly detection and audit

The DSC can detect access, operation, and management anomalies related to sensitive data and send alarms to you for you to confirm and handle the anomalies. The following behaviors are regarded as anomalies:

- Unauthorized users access and download sensitive data.
- Authorized users access, download, and modify sensitive data, as well as change and delete permissions.
- Authorized users change or delete permissions granted for buckets that contain sensitive data.

- Users who accessed sensitive files fail to log in to the device.

# Procedure

- Step 1 Buy DSC.
- **Step 2** Log in to the management console.
- **Step 3** Click and choose **Security** > **Data Security Center**.
- Step 4 In the upper left corner of the Asset Map page, click Modify. The Allow Access to Cloud Assets page is displayed.
- **Step 5** Locate the row that contains the OBS asset, click in the **Operation** column to enable authorization.
- Step 6 For details about how to add OBS assets, see Adding OBS Assets.

(\_), and hyphens (-).

• Start with a letter.

• Be unique.

**Step 7** In the navigation tree on the left, choose **Sensitive Data Identification** > **Identification Task**. Click **Create Task** to configure a sensitive data scanning task.

Select **OBS** for **Data Type** and select the OBS asset added in section **Step 6**. For details about other configurations, see section **Creating a Task**.

Parameter	Example Value					
Task Name	You can customize the task name.	test				
	The task name must:					
	Contain 4 to 255 characters.					
	Consist of letters, digits, underscores					

Table 2-1 Parameters for creating a sensitive data identification task

Parameter	Description	Example Value
Data Type	Type of data to be identified. You can select multiple types.	OBS
	• <b>OBS</b> : DSC is authorized to access your Huawei Cloud OBS assets and identify sensitive data in the assets. For details about how to add OBS assets, see Adding OBS Assets.	
	• <b>Database</b> : DSC identifies sensitive data of authorized database assets. For details about how to authorize database assets, see Authorizing Access to a Database Asset.	
	• <b>Big Data</b> : The DSC identifies sensitive data of authorized big data assets. For details about how to authorize big data source assets, see <b>Authorizing Access</b> to <b>Big Data Assets</b> .	
	<ul> <li>MRS: DSC identifies sensitive data of authorized MRS assets. For details about authorized MRS assets, see Authorizing Access to Big Data Assets.</li> </ul>	
	<ul> <li>LTS: DSC will identify sensitive data of authorized LTS assets. For details about how to add a log stream, see Adding a Log Stream.</li> </ul>	
Identificatio n Template	You can select a built-in or custom template. DSC displays data by level and category based on the template you select. For details about how to add a template, see Adding an Identification Template.	Huawei Cloud Data Security Classifying and Grading Template
Identificatio n Period	Set the execution policy of the data identification task.	Once
	• <b>Once</b> : The task will be executed once at a specified time.	
	• <b>Daily</b> : The task is executed at a fixed time every day.	
	<ul> <li>Weekly: The task is executed at a specified time every week.</li> </ul>	
	<ul> <li>Monthly: The task is executed at a specified time every month.</li> </ul>	

Parameter	Description	Example Value
When to Execute	This parameter is displayed when Identification Period is set to Once.	Now
	<ul> <li>Now: Select the option and click OK, the system executes the data identification task immediately.</li> </ul>	
	<ul> <li>As scheduled: The task will be executed at a specified time.</li> </ul>	

- Step 8In the navigation pane, choose Sensitive Data Identification > IdentificationTask.
- **Step 9** Click **Identification Result** in the **Operation** column to view the Identification result.

Figure 2-1 Identification result details

In the upper left corner of the page, set **Task Name** to **dsc-test**, **Data Type** to **OBS**, and **Asset types** to **All Assets** to filter the OBS sensitive data identification result, as shown in Figure 2-1.

 All types
 All Assets DSC\_Test All Sensitive Data Tables Top 10 Matched Rules L3 1 (25.00%)
 L2 1 (25.00%)
 N/A 2 (50.00%) Generate Result File Download 00 Object Asset Type Asset Database Table Name Object Path/Collection Time Level O Operation Database rsd-dsc-tes rsd-dsc-tes 'dsc\_bank' rsd-dsc-test/"dsc\_bank"/address N/A Database rad-dac-tes rsd-dsc-test "dsc bank N/A

Step 10In the row containing the desired scan object, click View Categorizing and<br/>Leveling Result Details in the Operation column. The Categorizing and<br/>Leveling Result Details dialog box is displayed, as shown in Figure 2-2.

## Figure 2-2 Categorizing and leveling results

#### Categorizing and Leveling Results

#### Identification Object Details

Object	Email		Object Path/Collection Time	rsd-dsc-test/"dsc_bank"/Email
Asset	rsd-dsc-test		Asset Type	Database
Level	L3			
Result I	Details	Sample D	ata	
Rule		Level	Category	Categorizing and Le
Taiwan	compatriot	L3	Authoritative socia	al i Huawei Cloud data se
Email		L3	General personal	inf Huawei Cloud data se

- 1. In the alarm list, view anomalies based on the risk level and check whether there are high-risk events. For operation details, see **OBS Usage Auditing**.
- 2. On OBS Console, modify the read and write permissions of the risky buckets or files. For details, see **Bucket Policy**.

----End