

Data Security Center

User Guide

Issue 25
Date 2025-01-17



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. 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



HUAWEI 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 Service Provisioning.....	1
1.1 Buying DSC.....	1
1.2 Upgrading Edition and Specifications.....	3
2 Allowing or Disallowing Access to Cloud Assets.....	5
3 Asset Map.....	10
4 Asset Management.....	21
4.1 Asset Center.....	21
4.1.1 Introduction to the Asset Center.....	21
4.1.2 Adding OBS Assets.....	22
4.1.3 Adding Self-Built Database Instances.....	24
4.1.4 Authorizing Access to a Database Asset.....	29
4.1.5 Authorizing Access to a Big Data Asset.....	32
4.1.6 Authorizing Access to a Big Data Asset.....	35
4.1.7 Adding a Log Stream.....	36
4.2 Managing Asset by Group.....	38
4.3 Metadata Tasks.....	39
4.3.1 Creating a Metadata Collection Task.....	39
4.3.2 Running a Metadata Collection Task.....	41
4.4 Data Exploration.....	43
4.5 Asset Catalog.....	45
5 Sensitive Data Identification.....	49
5.1 Overview of Sensitive Data Identification.....	49
5.2 Sensitive Data Identification Configuration.....	51
5.2.1 Creating an Identification Template.....	51
5.2.2 Managing Identification Templates.....	52
5.2.3 Customizing a Rule.....	54
5.2.4 Editing a Rule.....	57
5.2.5 Viewing Built-in Rules.....	57
5.2.6 Adding a Sensitive Level.....	61
5.2.7 Managing Levels.....	62
5.3 Sensitive Data Identification Tasks.....	63
5.3.1 Creating an Identification Task.....	63

5.3.2 Starting a Task.....	69
5.3.3 Identification Tasks.....	70
5.3.4 Identification Results.....	73
6 Policy Center.....	78
6.1 Policy Baseline.....	78
6.1.1 Policy Baseline Overview.....	78
6.1.2 Data Collection.....	82
6.1.3 Data Transmission.....	84
6.1.4 Data Storage.....	85
6.1.5 Data Use.....	87
6.1.6 Data Sharing.....	88
6.1.7 Data Destruction.....	90
6.2 Policy Management.....	92
6.3 Transfer Log Collection.....	94
7 Data Asset Protection.....	98
7.1 Data Masking.....	98
7.1.1 Data Masking Overview.....	98
7.1.2 Configuring and Viewing Masking Rules.....	100
7.1.3 Static Data Masking.....	113
7.1.3.1 Creating a Static Data Masking Task.....	113
7.1.3.2 Checking the Running Status of a Static Data Masking Task.....	132
7.1.3.3 Editing and Deleting a Static Data Masking Task	133
7.2 Data Watermarking.....	133
7.2.1 Data Watermarking Overview.....	133
7.2.2 Injecting Watermarks.....	135
7.2.2.1 Injecting Watermarks to Databases.....	135
7.2.2.2 Injecting Watermarks to Documents.....	144
7.2.2.3 Injecting Watermarks to Images.....	148
7.2.3 Extracting Watermarks.....	155
7.2.3.1 Extracting Watermarks from Databases.....	155
7.2.3.2 Extracting Watermarks from Documents.....	157
7.2.3.3 Extracting Watermarks from Images.....	159
7.3 (Optional) Configuring GaussDB(DWS) and MRS Hive.....	161
8 Data Security Operations.....	164
8.1 Situational Awareness Dashboard.....	164
8.2 Data Transfer Details.....	174
8.3 Event Management.....	175
8.4 Alarm Management.....	179
8.5 OBS Usage Audit.....	181
8.6 Watermarks.....	183
8.6.1 Extracting Watermarks from Databases.....	183

8.6.2 Extracting Watermarks from an OBS Bucket File.....	185
8.6.3 Extracting Watermarks from a Local File.....	186
9 Alarm Notifications.....	187
10 Multi-Account Management.....	189
10.1 Multi-Account Management Overview.....	189
10.2 Enable Multi-account Management.....	190
10.3 Viewing Multi-Account Management.....	190
11 Permissions Management.....	192
11.1 Creating a User and Assigning DSC Permissions.....	192
11.2 DSC Custom Policies.....	194
11.3 DSC Permissions and Supported Actions.....	195
12 Key DSC Operations.....	197
12.1 Operations Recorded by CTS.....	197
12.2 Viewing CTS Traces in the Trace List.....	201

1 Service Provisioning

1.1 Buying DSC

If you use DSC through the console, you will be billed on a yearly/monthly basis, which is prepaid. If you use DSC by APIs, including data masking and watermark APIs, you pay for what you used. DSC provides the standard and professional editions, and the database and OBS expansion packages. Buy a required DSC edition and additional expansion packages based on your site requirements.

Prerequisites

You have added the obtained account to the user group that has been assigned with the **DSC FullAccess** permission. For details, see [Creating a User and Assigning DSC Permissions](#).

Constraints

- The specifications of DSC cannot be downgraded once you complete the purchase. If you want to downgrade the DSC specifications, unsubscribe from the current edition and purchase DSC of the edition with lower specifications.
- The database and OBS expansion packages included in the purchased DSC of an edition cannot be renewed or unsubscribed separately.


Specification Limitations

- 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.

Procedure

Step 1 [Log in to the management console](#).

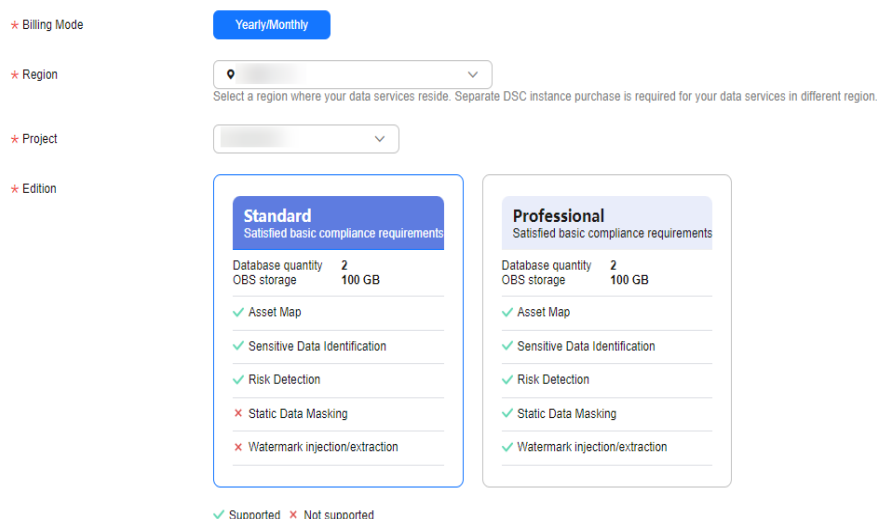
Step 2 Click  in the upper left corner and select a region or project.

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 1-1 Selecting a region and edition



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 1-2 Selecting expansion packages



- 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.

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**.

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

----End

1.2 Upgrading Edition and Specifications

After purchasing DSC, you can upgrade it from the standard edition to the professional edition, and purchase additional database and OBS expansion packages based on your site requirements.

Prerequisites

- You have added the obtained account to the user group that has been assigned with the **DSC FullAccess** permission. For details, see [Creating a User and Assigning DSC Permissions](#).
- You have purchased the standard DSC or professional DSC.

Constraints

The expired DSC cannot be directly upgraded. Renew DSC before upgrading it.


Specification Limitations

- 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.

Procedure

Step 1 [Log in to the management console](#).

Step 2 Click  in the upper left corner and select a region or project.

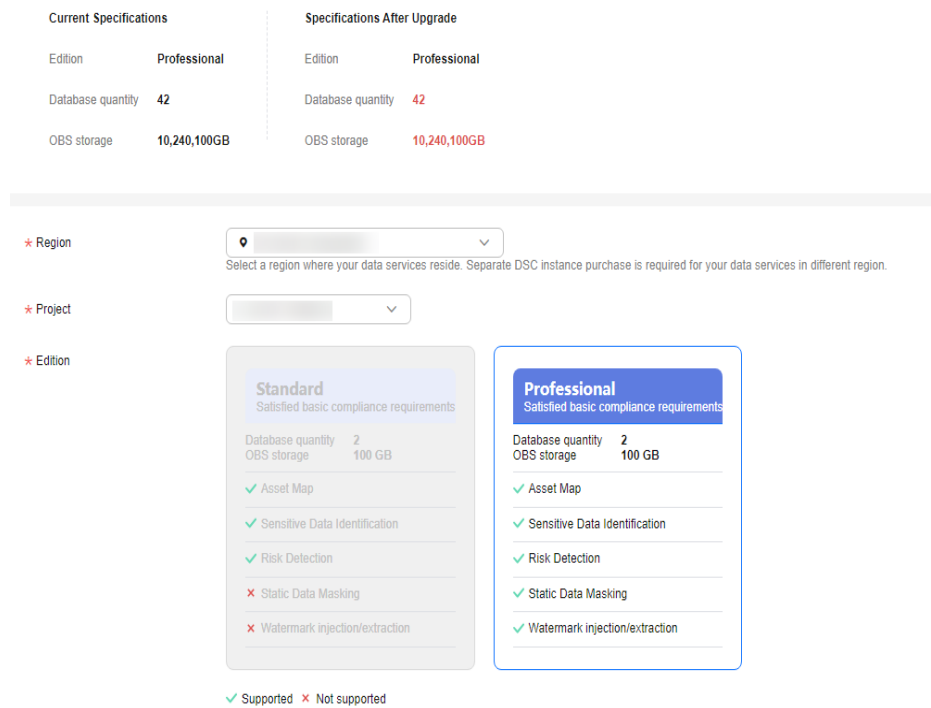
Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the upper right corner of the page, click **Upgrade Specifications**.

Step 5 The current edition is selected by default for **Edition** on the displayed page, and you can select an edition with higher specifications.

The edition listed on the right side of the current one is a more feature-rich edition.

Figure 1-3 Upgrading edition specifications



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

Figure 1-4 Selecting expansion packages



- 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 Click **Next**.

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

Step 8 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**.

Step 9 Select a payment method to pay for your order on the displayed page.

----End

2 Allowing or Disallowing Access to Cloud Assets

This section describes how to grant or revoke permissions for accessing OBS buckets, databases, big data, LTS, and MRS, as well as the asset map feature. The system will create an agency for you to use DSC.

Prerequisites

The user has been bound to a user group with the **Tenant Administrator** permission using IAM. For details, see [Creating a User Group and Assigning Permissions](#).

Constraints

- After permissions are granted, DSC will be able to access your OBS buckets, databases, big data instances, and other cloud assets as needed.

NOTE

- After DSC is granted permissions for accessing the OBS bucket to obtain the logs, fees are incurred. For details, see [Requests](#).
- After the permissions are revoked, ensure that your assets have no ongoing tasks. DSC will delete your agencies and assets and all related data. Exercise caution when performing this operation.

Agency Policies Obtained After Access to Assets Is Allowed

Table 2-1 Agency policies

Asset	Policy	Scope	Remarks
OBS	OBS Administrator	Global	Used to configure OBS logs, obtain the OBS object list, download OBS objects, and obtain OBS delivery logs.

Asset	Policy	Scope	Remarks
	EVS ReadOnlyAccess	Regional	Used to obtain the EVS disk list.
Database	ECS ReadOnlyAccess	Regional	Used to obtain the list of ECSs where databases are built.
	RDS ReadOnlyAccess	Regional	Used to obtain the RDS database list and related information.
	DWS ReadOnlyAccess	Regional	Used to obtain the DWS instance list.
	VPC FullAccess	Regional	Used to establish network connection and create VPC ports and security group rules
	KMS CMKFullAccess	Regional	Used to perform encryption using KMS in data masking.
	GaussDB ReadOnlyAccess	Regional	Used to obtain the GaussDB list.
Big Data	ECS ReadOnlyAccess	Regional	Used to obtain the list of ECSs where big data sources reside.
	CSS ReadOnlyAccess	Regional	Used to obtain the CSS data cluster list and data indexes.
	DLI Service User	Regional	Used to obtain the DLI queue and database.
	VPC FullAccess	Regional	Used to establish network connection and create VPC ports and security group rules
	KMS CMKFullAccess	Regional	Used to perform encryption using KMS in data masking.
MRS	MRS CommonOperations	Regional	Used for cluster query and task creation.
Asset Map	Tenant Guest	Regional	Used to obtain the list of cloud services used for data storage and processing.

Asset	Policy	Scope	Remarks
	OBS Administrator	Global	Used to configure OBS logs, obtain the OBS bucket list, and download items from OBS.
	EVS ReadOnlyAccess	Regional	Used to obtain the EVS disk list.
	OBS Administrator	Global	Used for OBS to deliver logs.
LTS	LTS ReadOnlyAccess	Regional	Used to read LTS log groups or log streams.

Procedure



- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**, then go to the **Asset Map** page.
- 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** On the displayed page, allow or disallow DSC to access your cloud assets. For details, see [Table 2-2](#).

Figure 2-1 Allowing access to cloud assets

×

Allow Access to Cloud Assets

1 After you allow access to assets, DSC will be able to access your OBS buckets, databases, big data sources, and other assets as needed. When you need to revoke asset access permissions, stop ongoing scans. After the permissions are revoked, your asset information and related data will be deleted. Exercise caution when performing this operation.

1 If you authorize Data Security Overview to access your resources, DSC automatically enables logging for all your OBS buckets. The bucket access logs are stored in the buckets. You may be billed for log storage. If you authorize DSC to access OBS, logging for OBS buckets that you add to your assets will be enabled based on your usage. You will be billed based on data requests to scan the sensitive data in the buckets. The billing formulas are as follows:



OBS log storage fee = Storage usage x Unit price ?

OBS data request fee = Number of scans x 2 x Number of files x Unit price ?

For details, see [OBS Price Calculator](#) -> [Product Pricing Details](#)

Asset	Authorization Status	Operation
OBS	● Authorized	<input checked="" type="checkbox"/>
Database	● Authorized	<input checked="" type="checkbox"/>
Big Data	● Authorized	<input checked="" type="checkbox"/>
MRS	● Authorized	<input checked="" type="checkbox"/>
Asset Map	● Authorized	<input checked="" type="checkbox"/>
LTS	● Authorized	<input checked="" type="checkbox"/>

Table 2-2 Parameter description

Parameter	Description
Asset	<ul style="list-style-type: none"> ● OBS: OBS assets. ● Database: database assets. For details about the database types and versions supported by DSC, see Constraints. ● Big Data: assets in Cloud Search Service (CSS), Data Lake Insight (DLI), Hive, and HBase ● MRS: assets in MapReduce Service (MRS). ● Asset Map: assets on the cloud. ● LTS: assets in Log Tank Service (LTS). <p>Agency Policies Obtained After Access to Assets Is Allowed describes the agency policies obtained after the access to assets is allowed.</p>
Authorization Status	<p>Authorization Status</p> <ul style="list-style-type: none"> ● Authorized ● Unauthorized
Operation	<p>Click the following toggle buttons to allow or disallow access to your assets:</p> <ul style="list-style-type: none"> ●  : Unauthorized ●  : Authorized

----End

3 Asset Map

The data asset map allows you to view the security status of your assets from multiple dimensions, such as asset overview, categories and risk levels, permissions, storage, sensitivity, and data egress analysis. This helps you quickly detect risky assets and handle them.

Constraints

- A maximum of 1000 assets can be displayed.
- The following table lists the data sources supported by DSC.

Table 3-1 Asset sources and versions supported by DSC

Data Type	Data Source	Version
Database	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
	PostgreSQL	10, 9.6, 9.5, 9.4, 9.1, and 1.0
	TDSQL	10.3.X
	Oracle	11 and 12
	DDS	4.2, 4.0, and 3.4
GaussDB	1.3, 1.4, 2.7	

Data Type	Data Source	Version
	KingBase	V8
	DMDBMS	7 and 8
	DWS	8.1.X
Big Data	ElasticSearch	5.x, 6.x, and 7.x
	DLI	1.0
	Hive	1.0
	Hbase	1.0
OBS	OBS	V3
MRS	MRS-Hive	3.x

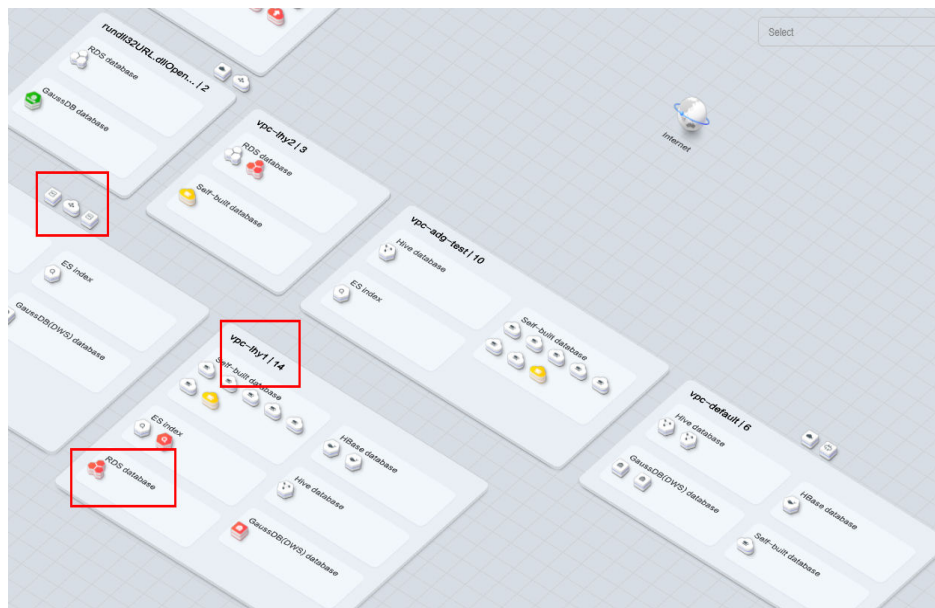
Prerequisites

Cloud asset access permissions are granted. For details, see [Allowing or Disallowing Access to Cloud Assets](#).

Asset Map Functions

- Sorts out data assets on the cloud and displays them by region:** DSC automatically scans and sorts out data assets on the cloud and displays asset distribution on a map. The asset map displays regions of assets based on VPCs and associates asset regions with service regions.

Figure 3-1 Asset Map

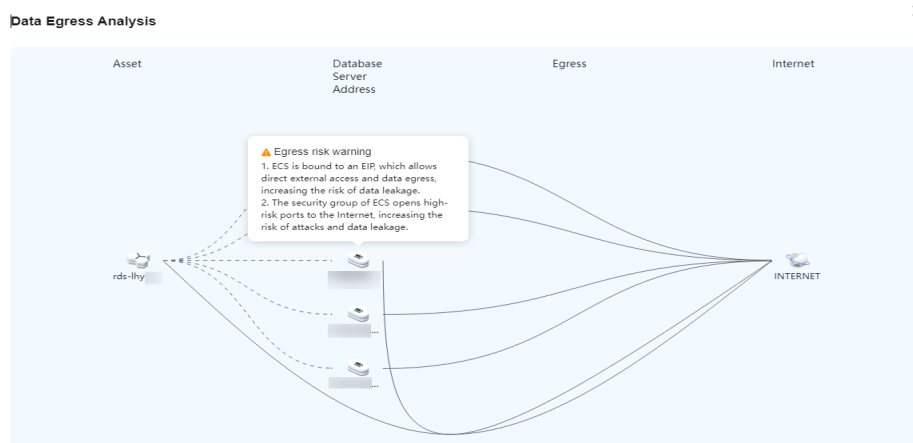


- Sensitive data display:** DSC displays sensitive data by categories. It identifies and classifies sensitive data using a three-layer identification engine, including

default compliance rules, natural language semantic identification, and advanced file similarity detection.

- **Data egress analysis:** DSC provides a unified data egress view based on the asset map to help you identify all data egresses of on the cloud and potential security risks of these egresses, so you can take corresponding data security protection measures.

Figure 3-2 Data egress analysis




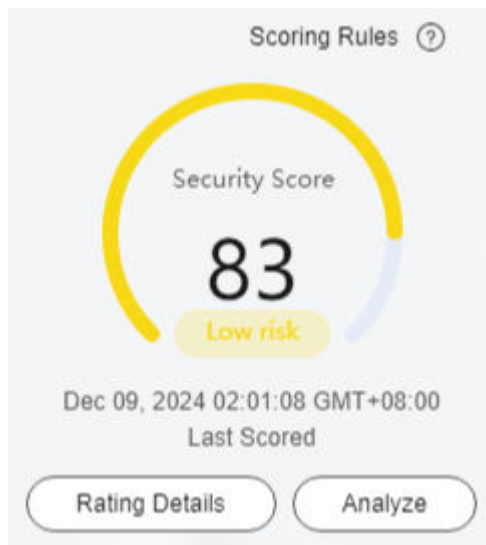
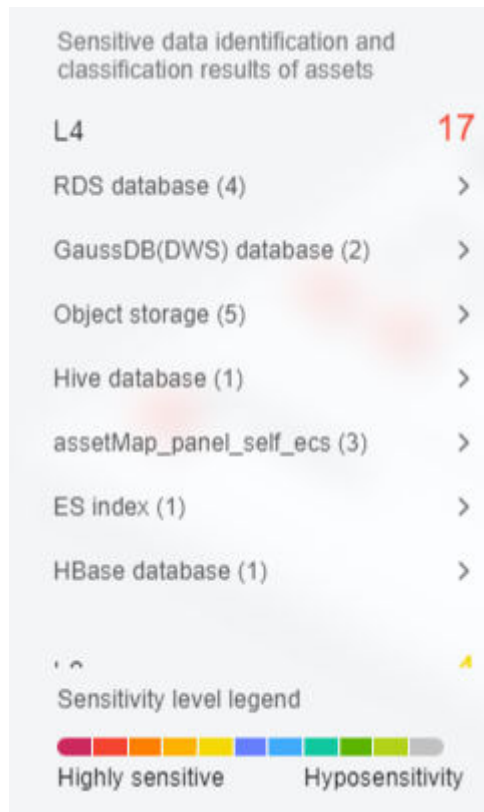
- **Risk monitoring and alarming:** DSC monitors data asset risks using the risk identification engine, displays the risk distribution for each asset type, and reports alarms for you to take quick response.
 - Security Score: The asset map displays the overall **security score** of all your assets. You can click  next to **Scoring Rules** to view the asset security score calculation rule, as shown in [Figure 3-3](#).

Figure 3-3 Scoring Rule





- **Security Level:** Assets are classified into different security levels to facilitate viewing and management. You can click an asset with risks to view the risk details.

Figure 3-4 Security levels

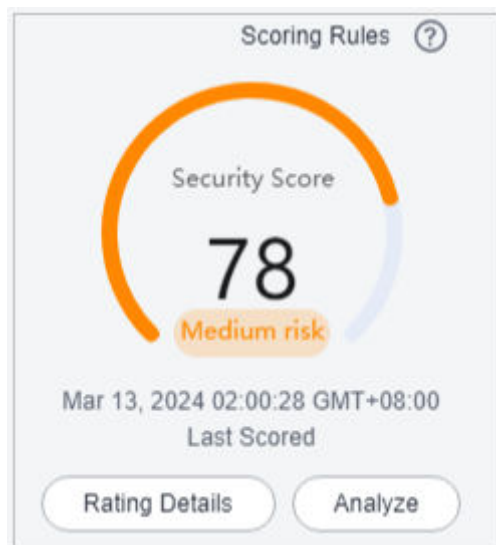



Procedure

- Step 1** Log in to the management console.
 - Step 2** Click  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** In the navigation pane, choose **Asset Map**.
 - Step 5** After assets are **added** or **authorized**, refresh the **Asset Map** page. The following describes the functions and usage of each module on the page.
- End

Risk Statistics

- The **security score**, **last scored time**, and **rating details** of the asset are displayed, as shown in [Figure 3-5](#). You can manually re-analyze the score. The details are as follows:

Figure 3-5 Security score

- The security score of the asset is displayed. Click  next to the scoring rule to view the asset security score calculation rule.
- Click **Analyze** to perform security analysis and scanning on cloud assets again.
- Click **Rating Details** to view the **Protection Policy Analysis**. Click **Modify** in the **Operation** column to configure policies based on the **Configuration Policy Recommendation**.

As shown in [Figure 3-6](#), **Protection Policy Analysis** displays only assets whose **Risk Level** is **Medium** or **High**. As shown in [Table 3-2](#), the **risk level** is calculated based on the **Configuration Risk Level** and **Categorization and Leveling Result**.

Figure 3-6 Security policy analysis

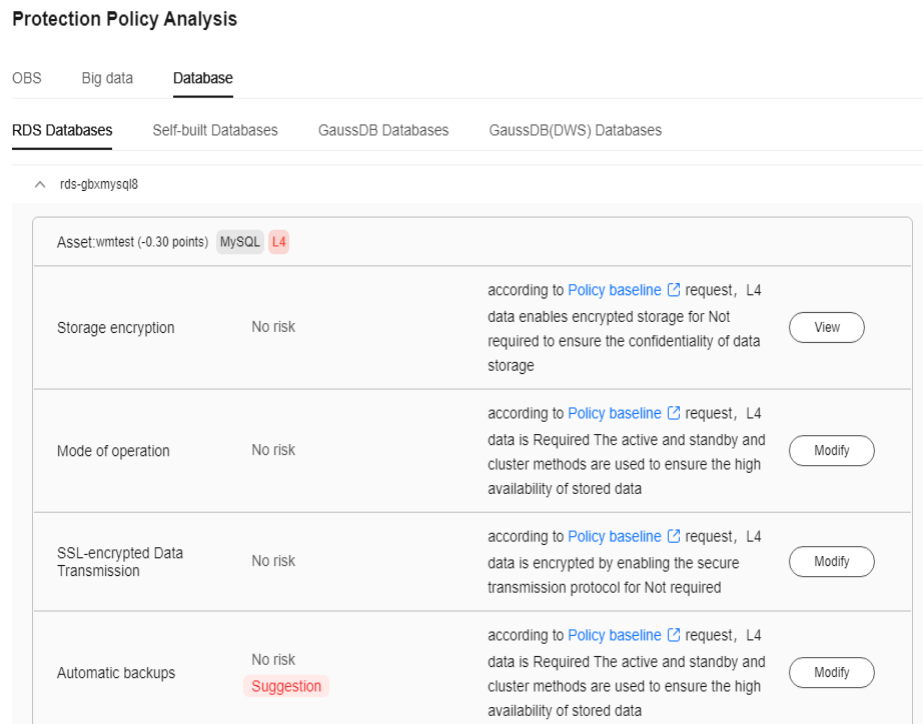


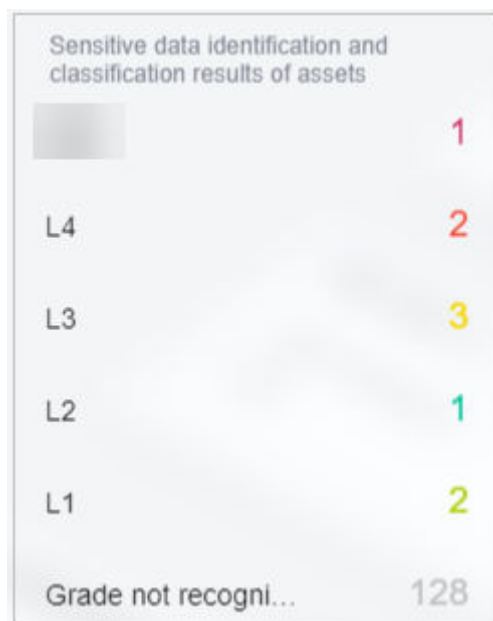
Table 3-2 Protection policy analysis parameters

Config urion Risk Level	Categoriza tion and Leveling Result	Risk Level	Display
Low	L0-L3 (low-risk)	Low	No
	L4-L7 (medium risk)	Low	No
	L8-L10 (high-risk)	Medium	Yes
Medium	L0-L3 (low-risk)	Low	No
	L4-L7 (medium risk)	Medium	Yes
	L8-L10 (high-risk)	High	Yes
High	L0-L3 (low-risk)	Medium	Yes

Config uration Risk Level	Categoriza tion and Leveling Result	Risk Level	Display
	L4-L7 (medium risk)	High	Yes
	L8-L10 (high-risk)	High	Yes

- The sensitive data identification and leveling results of assets are displayed. Assets are displayed by category based on the grading results, as shown in [Figure 3-7](#). The details are as follows:

Figure 3-7 Sensitive data identification and leveling result




- You can hover the cursor over a sensitivity level to show information about all assets at the sensitivity level.
- You can hover the cursor over an asset category to display the names and scan times of all its scanned assets in the adjacent dialog box.
- You can select an asset to view its details in the right-hand dialog box, which includes basic asset information, sensitive data detection, protection policy analysis, and data egress analysis. For details, see [Viewing Database Instance Details](#).

Viewing Database Instance Details

- Basic Info:** displays the type, port number, version, private IP address, and engine type of the instance.

- **Sensitive data identification:** displays authorized and unauthorized databases in the instance.
 - For an **authorized database** that has **not been scanned**. Click **Create identification task** to go to the sensitive data identification page and create an identification task to identify sensitive information in the database. For details, see [Creating an Identification Task](#).
 - For an **authorized database** that **has been scanned**. Click **Expand** to view database scan details.
 - For an unauthorized database, click **Go to Authorize** to obtain the access permission to the database. For details, see [Asset Center](#).

Figure 3-8 Sensitive data identification



rds [redacted] ○ Scanned Protected L4

Instance ID: 743e14026ff14aa18fa530e02cc22fa5in01

Created: Dec 06, 2024 03:52:05 GMT+08:00

✕


Basic Info

Type	Private IP Address
RDS	192.168.0.93
Port	Engine Type
3306	MySQL
Version	
8.0	

Sensitive data identification

Analysis of security protection polici ...

Authorized databases(1)



gbx-jiami ○ Scanned

Scanned.

Hide ^

Security Level		L4	
Total number of tables scanned	0		Details
Sensitive Tables	0		Details
Last Scanned	Dec 06, 2024 17:09:37		
Categorizing and Leveling Template	[redacted]		Details

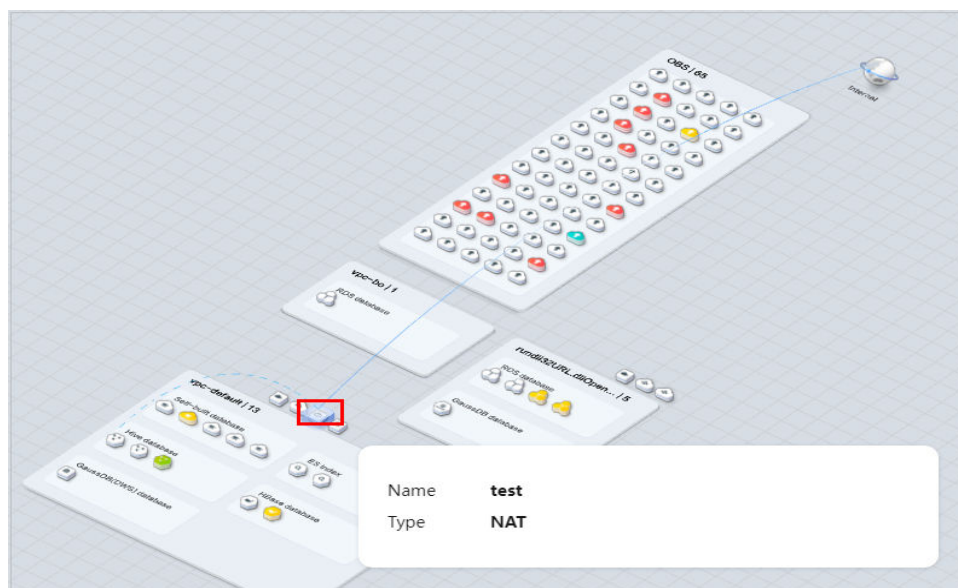
Unauthorized databases(0)

NOTE

For OBS data, click **View Details** to view the **Result Details** of the sensitive data identification task. If there is no identification result, create an identification task by referring to section [Creating an Identification Task](#) and view the identification result again.





- **Security policy analysis:**
 - Checks whether high-risk permissions, such as server-side encryption, database encryption, transmission encryption, security group, and public network access, are enabled and displays handling notifications. You can click **View** or **Modify** to handle the permissions.
 - Allows you to view the current status of security configurations, including encryption, backup, and audit, for all assets, along with the specific requirements of the policy baseline. Additionally, you can switch to the policy/task configuration page to configure policies and tasks.
- **Data Egress Analysis:** identifies all data egresses on the cloud, including EIP, NAT, API Gateway, and ROMA. You can also move the cursor to the data type icon or VPC icon on the asset map to view the data egress gateway lines.

Figure 3-9 Data exit analysis



Related Operations

- If you want to change authorization status of your assets, click **Modify** in the upper right corner. If you want to stop authorization of your assets, ensure that the assets have no ongoing tasks. DSC will delete your agencies and assets and all related data. Exercise caution when performing this operation. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- Asset security level legend: Each color represents an asset security level from L0 to L10.
- You can drag the slider on the progress bar to adjust the scale of the asset map.

- Click  in the lower right corner.
- Click  in the lower right corner to display the asset map operation guide.
- Click  in the lower right corner to display the data exception events, so that you can handle the exceptions in time.
- Click  in the lower right corner to display the asset legend.

4 Asset Management

4.1 Asset Center

4.1.1 Introduction to the Asset Center

DSC can automatically discover data assets on the cloud and allows you to manually add self-built database assets on the cloud. Through [cloud asset authorization](#), the system creates an agency for DSC. You can view and add your data assets in the asset center. For details about the supported asset types and data source types, see [Table 4-1](#).

- After an OBS bucket is added, you can directly perform [sensitive data scan](#), [OBS masking](#), and [data watermarking](#) operations on the bucket.
- [Sensitive data identification](#), [data masking](#), and [database watermarking](#) can be only be performed on authorized databases and big data assets.

Table 4-1 Asset types and data source types supported by the asset center

Asset Type	Data Source Type	Post-Addition Operations
OBS	OBS	Adding OBS Assets
Database	RDS	Authorizing Access to a Database Asset
	DWS	
	DDS	
	GaussDB	
	Self-built databases	<ul style="list-style-type: none">• Adding Self-Built Database Instances• Authorizing Access to a Database Asset

Asset Type	Data Source Type	Post-Addition Operations
Big Data	Elasticsearch	<ul style="list-style-type: none">• Authorizing Access to a Database Asset• Authorizing Access to a Big Data Asset
	Hive	
	HBase	
	DLI	Adding a DLI Database
Logs	LTS	Adding a DLI Database
NOTE Database assets with IPv6 VPC enabled cannot be managed.		

4.1.2 Adding OBS Assets

Once you have authorized OBS assets, you can add them to DSC for data asset management. This includes identifying sensitive data, applying data masking, and injecting and extracting data watermarks.

Prerequisites

- DSC has been authorized to access OBS assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- To add a self-built OBS bucket or other buckets, ensure that you have enabled OBS and created assets on it. For details about how to enable OBS, see [Enabling and Using OBS Buckets](#).
- If you want to add other buckets, set the bucket policy to **public** or use private buckets on which the current account has permissions.

Constraints


DSC does not support the parallel file system of OBS.

Adding Self-built OBS Buckets

Self-built buckets are created by the current user, including public buckets and private buckets.

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation tree on the left, choose **Asset Management > Asset Center**. The **Asset Center** page is displayed.

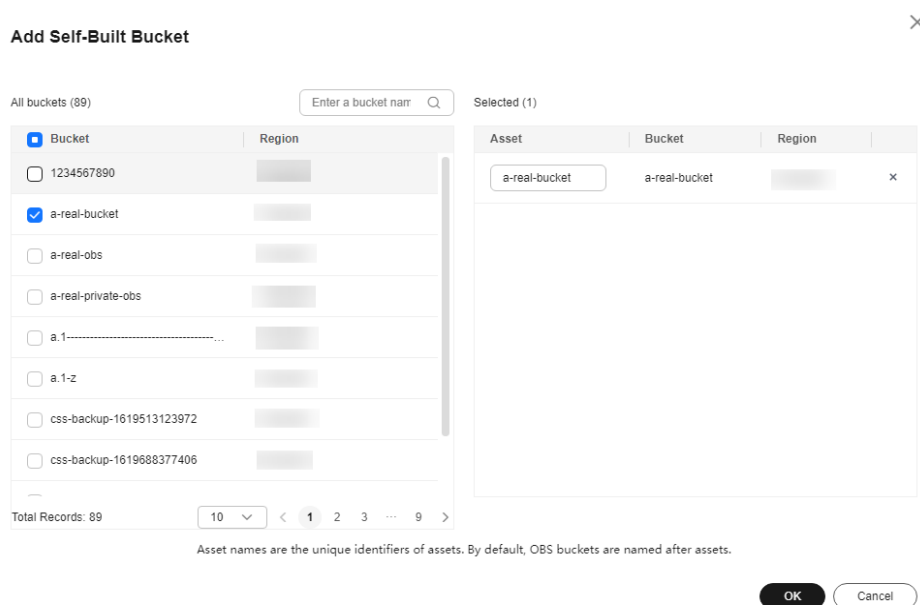
Step 5 Click **OBS**. The OBS asset list page is displayed.

Step 6 In the upper left corner of the **OBS** tab page, click **Add Self-Built Bucket**. In the displayed dialog box, select the OBS buckets to be added.

 **NOTE**

The asset name is used as the unique identifier of the asset. By default, the bucket name is set to the asset name.

Figure 4-1 Adding Self-built OBS Buckets



Step 7 Click **OK**.


----End

Adding Other Buckets

Other buckets refer to the buckets created by other users with the **public** permission or the private buckets on which the current account has permissions.

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation tree on the left, choose **Asset Management > Asset Center**. The **Asset Center** page is displayed.

Step 5 Click **OBS**. The OBS asset list page is displayed.

Step 6 In the upper left corner of the **OBS** tab page, click **Add Other Bucket**. In the displayed dialog box, enter the name of a bucket to be added.

To add more buckets, click  **Add**.

Figure 4-2 Adding Other Buckets

Add Other Bucket ✕

Region

* Bucket Add

Asset	Bucket	Operation
<input type="text" value="dsc-obs"/>	<input type="text" value="dsc-obs"/>	Delete
<input type="text" value="Enter an asset name."/>	<input type="text" value="Enter a bucket name."/>	Delete

Step 7 Click **OK**.

----End

Related Operations

- Deleting OBS assets
Select multiple OBS assets and click **Batch Delete** in the upper left corner of the asset list to delete the assets. You can also click **Delete** in the **Operation** column of the asset list to delete a single asset.
- Creating an identification task
Click **Create Identification Task** in the **Operation** column of the asset list to create a sensitive data identification task. For details, see [Creating an Identification Task](#).
- Enabling database audit
Click **Enable Audit** in the **Operation** column of the asset list to enable audit for OBS assets. After this function is enabled, you can view audit records in [OBS Usage Audit](#). Enabling this function will incur additional [request fees](#).

4.1.3 Adding Self-Built Database Instances

If your asset is a self-built database, add the database instance to DSC by referring to this section.

Prerequisites

- DSC has been allowed to access the database assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- You have applied for an ECS instance and installed the database on it. For details, see [Purchasing and Using a Windows ECS](#).

Constraints

Only data sources and versions supported by DSC can be added. For details, see [Table 4-2](#).

Table 4-2 Data sources and versions supported by DSC

Data Source	Version
MySQL	5.6, 5.7, 5.8, and 8.0
SQL Server	<ul style="list-style-type: none">• 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
DMDBMS	7 and 8
PostgreSQL	15, 14, 13, 12, 11, 10, 9.6, 9.5, 9.4, and 9.1
TDSQL	10.3.X
Oracle	11, 12

Adding a Self-Built Database Instance

You can add and delete self-built database instances. For details about the database types and versions supported by DSC, see [Table 4-2](#). This section describes how to add a self-built database on the cloud.



- Step 1** [Log in to the management console](#).
- Step 2** Click  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** In the navigation tree on the left, choose **Asset Management > Asset Center**. The **Asset Center** page is displayed.
- Step 5** Choose **Databases > Self-built Databases**. The **Database Instances** tab page is displayed.
- Step 6** Click the **Database Instances** tab. The **Database Instance** tab page is displayed.
- Step 7** Click **Add Instance** in the upper left corner of the database instance list. The **Add Database Instance** dialog box is displayed.

Figure 4-3 Adding a database instance

Add Database Instance ✕

* Region: CN North-Ulanqab203 * ECS: e1d802e6-54ce-48e1-a5...

* Security Group: mrs_mrs_... * Database Engine: MySQL

* Version: 5.6 * Database Server Address: 192.86

* Port: 22 * Database: test

* Username: root * Password: Enter a password.

* Asset: Enter an asset name.

* Creating a metadata drawing task

OK Cancel

Step 8 Set related parameters based on [Table 4-3](#) and click **OK** to add the self-built database instance.

Table 4-3 Configuring database instance information

Parameter	Description
ECS	Select the ECS of the self-built database instance from the drop-down list.
Security group	Select a security group from the drop-down list.
Database Engine	Select a DB engine from the drop-down list. Currently, the following DB engines are supported: <ul style="list-style-type: none">• MySQL• TDSQL• KingBase• DMDBMS• PostgreSQL• SQLServer• Oracle
Version	Select a DB engine version from the drop-down list box.
Connection Method	This parameter is displayed when Database Engine is set to Oracle . Select a connection mode from the drop-down list. <ul style="list-style-type: none">• Service Name: Enter the service name.• SID: Enter the service name.

Parameter	Description
Database Server Address	Select a server address from the drop-down list box. If the database is deployed in the cluster mode and data masking is required, set this parameter to the IP address of the primary node.
Database Port	Enter an integer ranging from 0 to 65535.
Database Name	Enter a database name.
Username/ Password	Enter the username and password of the database.
Asset	Enter 4 to 255 characters. Only letters, digits, hyphens (-), and "_" are allowed. The value must start with a letter.
Creating a metadata drawing task	After this function is enabled, metadata tasks are automatically delivered based on the default database of the instance to obtain the database, table, and column information of the instance.

Step 9 After an instance is added, if you need to identify and mask sensitive data in the databases of the instance, authorize access to the databases first. For details, see [Authorizing Access to a Database Asset](#).


----End

Adding Instances and Databases in Batches

You can use [Direct Connect](#) to connect your on-premises assets to the proxy VPCs in the cloud, and subsequently add your on-premises databases to DSC in batches.

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation tree on the left, choose **Asset Management** > **Asset Center**. The **Asset Center** page is displayed.

Step 5 Choose **Database** > **Self-built databases**. The **Databases** tab page is displayed.

Step 6 Click the **Database Instances** tab. The **Database Instance** tab page is displayed.

Step 7 Click **Adding DB Instances and Databases in Batches** in the upper left corner. The **Adding DB Instances and Databases in Batches** dialog box is displayed.

Step 8 Click **Download Template** to download the Excel template and set parameters based on [Table 4-4](#).

Table 4-4 Database Instance Information

Parameter	Description
Asset	User-defined asset name displayed in the database instance list.
ECS Instance ID	You do not need to enter the ID for an external self-built database. However, if you purchase an ECS self-built database, you must enter the ID of the corresponding ESC instance.
Oracle Connection Mode (Default Service Name)	This parameter is required only for Oracle databases.
Oracle Service Name/SID	Enter a service name.
Proxy VPC	This parameter is optional for cloud databases and is mandatory for external self-built databases. It corresponds to the proxy VPC of the ECS.
Subnet	This parameter is optional for cloud databases and is mandatory for external ESCs. It corresponds to the ECS subnet ID.
Security group	This parameter is optional for cloud databases and mandatory for external ESCs. It corresponds to the security group of the ECS.
Database Engine	If an ECS instance has been added, the engine of the added ECS will be used.
Version	If an ECS instance has been added, the version of the added ECS will be used.
Host IP Address	If an ECS has been added, the IP address of the added ECS will be used.
Database Port	If an ECS has been added, the port of the added ECS will be used.
Database Name	Database name
User Name	Database account
Password	Database password
Draw Metadata	TRUE or FALSE.

Step 9 Click **Select File**, select the prepared template, and click **OK**.

Step 10 After this function is enabled, metadata tasks are automatically delivered based on the default database of the instance to obtain the database, table, and column information of the instance.

Step 11 After an instance is added, if you need to identify and mask sensitive data in the databases of the instance, authorize access to the databases first. For details, see [Authorizing Access to a Database Asset](#).

----End

Related Operations

- Deleting a DB instance
Only self-built DB instances can be deleted. You can delete an instance only when there are no authorized databases and metadata under it.
Select multiple self-built database instances and click **Batch Delete** in the upper left corner of the instance list to delete the instances. You can also click **Delete** in the **Operation** column of the instance list to delete a single DB instance.
- Drawing metadata of an instance
 - If the number of authorized databases of a cloud database instance is greater than 0, click **Refresh** in the **Operation** column of the instance list to obtain the database, table, and column information of the instance.
Cloud databases that do not support metadata collection, such as DDS, are excluded. For details, see section [Creating a Metadata Collection Task](#).
 - If you enable the function of **automatically creating a metadata task** when adding a self-built database instance, the system automatically creates a metadata task to obtain all metadata of the instance after the instance is created.
Self-built databases that do not support metadata collection, such as SQL Server, are excluded. For details, see section [Creating a Metadata Collection Task](#).
 - Manually create a metadata task by referring to section [Creating a Metadata Collection Task](#).
- Creating an identification task
On the **Databases** tab page, click **Create Identification Task** in the **Operation** column of the asset list to create an identification task for an asset. For details, see section [Creating an Identification Task](#).
- Testing connectivity in batches
You can select multiple database instances and data instances to perform connectivity tests in batches.

4.1.4 Authorizing Access to a Database Asset

To identify sensitive data, mask data, or add or extract watermarks for a database instance, you must authorize access to the instance's databases. This section explains how to authorize database access.

Prerequisites


- RDS, GaussDB(DWS), DDS, or GaussDB service has been enabled, you have assets on them, and there are available IP addresses in the corresponding subnets.


- The **Status** of the database instance is **Normal**, and the number of security groups is 1.

Authorizing Access to a Database Asset

The following uses the **RDS** database type as an example to describe how to authorize access to database assets in an RDS database instance. To authorize access to other types of database instance, click the corresponding database type (for example, **DWS** or **Self-built databases**) and perform the following steps:

Step 1 [Log in to the management console](#).


Step 2 Click  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 In the navigation tree on the left, choose **Asset Management > Asset Center**. The **Asset Center** page is displayed.

Step 5 Click **RDS**. The **RDS Databases** tab page.

Figure 4-4 RDS database instances

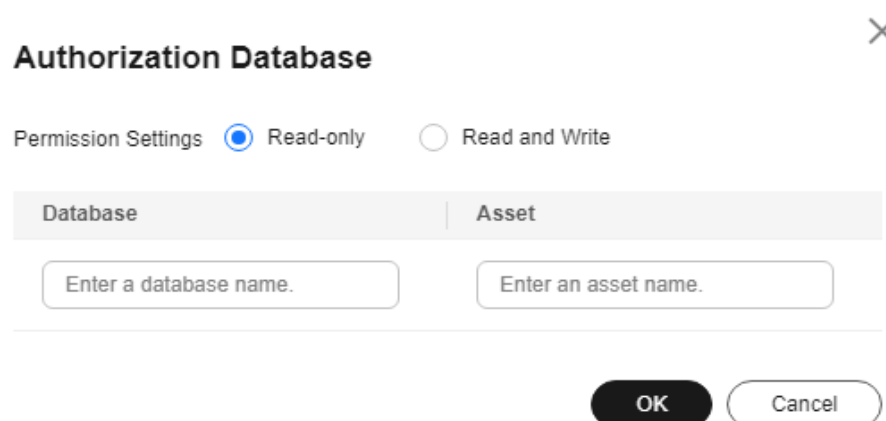


Instance	Status	Type	IP	Port	Engine Version	Authorized Dat...	Created	Operation
rds-1111111111	Normal	Cloud database	192.168.1.6	3306	MySQL 8.0	2 authorized	Nov 19, 2024 01:59...	Authorize Refresh Clear
rds-gomysql8	Normal	Cloud database	192.168.1.21	3306	MySQL 8.0	1 authorized	Nov 29, 2024 02:34...	Authorize Refresh Clear

Step 6 Click the **Database Instances** tab. The **Database Instances** tab page is displayed. Authorization can be performed in either of the following ways:

- Method 1: Click **Authorize** in the **Operation** column of the **database instance** list, and enter the database information for authorization.

Figure 4-5 Authorizing access to databases



Authorization Database ✕

Permission Settings Read-only Read and Write

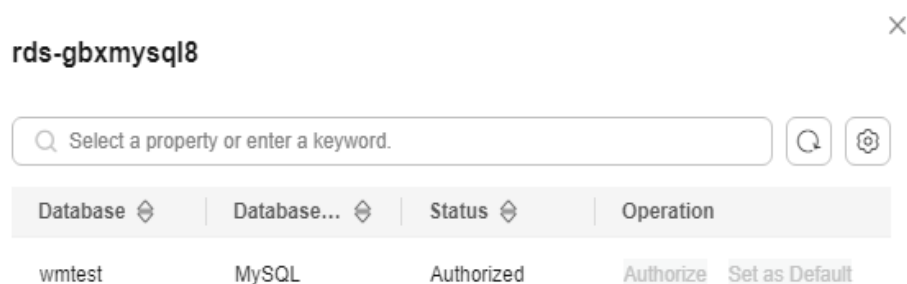
Database	Asset
<input type="text" value="Enter a database name."/>	<input type="text" value="Enter an asset name."/>

- Grant the **read-only permission**: Only the sensitive data identification function can be used.

- Grant the **read and write permission**: The sensitive data identification and data anonymization functions can be used.

CAUTION

- After the RDS read-only permission is authorized, DSC creates an account **dsc_readonly** in RDS.
 - After the password of the **dsc_readonly** account is reset in RDS, it will not be automatically synchronized to DSC. As a result, the sensitive data identification task fails. Therefore, do not reset the password of this account.
 - If you have reset the password of **dsc_readonly** in RDS, delete the authorized RDS DB instance in DSC and re-authorize the instance.
 - DSC cannot scan and mask sensitive data in MySQL databases which SSL has been enabled for on the RDS DB instance.
-
- Method 2: Click an instance name to go to the instance details page. In the **Operation** column, click **Authorize** to authorize access to a database.

Figure 4-6 Instance details

- Step 7** After the authorization is complete, click the **Databases** tab to view the connection status of the authorized database.

After the asset authorization is complete, the **Connection Status** of the asset is **Checking**, which means DSC is checking the database connectivity.

- DSC can access the added database normally if the **Connection Status** of the database is **Succeeded**.
- DSC cannot access the added database normally if the **Connection Status** of the database is **Failed**. Move the cursor to **Failed** to view the failure cause or rectify the fault by referring to section [How Do I Troubleshoot the Failure in Connecting to the Added Database?](#)

----End

Related Operations

- Deleting a DB instance
Only self-built DB instances can be deleted. You can delete an instance only when there are no authorized databases and metadata under it.

Select multiple self-built database instances and click **Batch Delete** in the upper left corner of the instance list to delete the instances. You can also click **Delete** in the **Operation** column of the instance list to delete a single DB instance.

- Drawing metadata of an instance
 - If the number of authorized databases of a cloud database instance is greater than 0, click **Refresh** in the **Operation** column of the instance list to obtain the database, table, and column information of the instance.
Cloud databases that do not support metadata collection, such as DDS, are excluded. For details, see section [Creating a Metadata Collection Task](#).
 - If you enable the function of **automatically creating a metadata task** when adding a self-built database instance, the system automatically creates a metadata task to obtain all metadata of the instance after the instance is created.
Self-built databases that do not support metadata collection, such as SQL Server, are excluded. For details, see section [Creating a Metadata Collection Task](#).
 - Manually create a metadata task by referring to section [Creating a Metadata Collection Task](#).
- Creating an identification task
On the **Databases** tab page, click **Create Identification Task** in the **Operation** column of the asset list to create an identification task for an asset. For details, see section [Creating an Identification Task](#).
- Testing connectivity in batches
You can select multiple database instances and data instances to perform connectivity tests in batches.

4.1.5 Authorizing Access to a Big Data Asset

If your assets are self-built big data, add big data instances to DSC by referring to this section.

If your asset is a DLI database, add it by referring to [Adding a DLI Database](#).

Prerequisites

- DSC has been allowed to access the database assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- You have obtained the version, server, and index information of the self-built ES, HBase, and Hive data sources, and there are available IP addresses in the subnets of these data sources.

Adding a Big Data Instance

Instances of self-built big data types need to be manually added. This section uses Elasticsearch as an example to describe how to add instances of self-built big data types.

Step 1 [Log in to the management console](#).





- Step 2** Click  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** In the navigation tree on the left, choose **Asset Management > Asset Center**. The **Asset Center** page is displayed.
- Step 5** Click **Elasticsearch** and choose the **ElasticSearch Instance** tab.
- Step 6** Click **Elasticsearch instance**. The **Elasticsearch instance** tab page is displayed.
- Step 7** Click **Add** in the upper left corner of the instance list. The **Add Instance** dialog box is displayed.
- Step 8** Set the related parameters according to the [Table 4-5](#), and then click **OK**.

Table 4-5 Parameters for adding an ES instance

Parameter	Description
ECS	Select an ECS from the drop-down list box.
Big Data Type	Big data instance type to be added. In this case, select Elasticsearch .
Security Group	Select a security group from the drop-down list.
Version	Select a version from the drop-down list box. For details about the supported asset types and versions, see section Constraints .
Database Server Address	Select a server address from the drop-down list box.
Database Port	Enter an integer from 0 to 65535.
Index	Enter an index name, which can contain only letters, digits, underscores (_), and hyphens (-).
Username/Password	Enter the username and password of the index.
Asset	Enter a user-defined asset name containing 4 to 255 characters.

----End

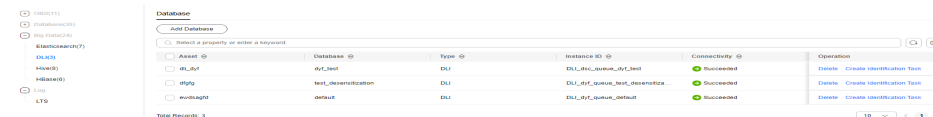
Adding a DLI Database

- Step 1** [Log in to the management console](#).
- Step 2** Click  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 In the navigation tree on the left, choose **Asset Management > Asset Center**. The **Asset Center** page is displayed.

Step 5 Click **DLI**. The **Database** tab page is displayed.

Figure 4-7 DLI database list



Step 6 Click **Adding a database** in the upper left corner of the database list. The **Add Database** dialog box is displayed.

Step 7 Set parameters according to [Table 4-6](#) and click **OK**.

Table 4-6 Parameters for adding a database

Parameter	Description
Asset	Enter a user-defined asset name containing 4 to 255 characters.
Big Data Type	Select DLI from the drop-down list box.
Queue	Select a queue from the drop-down list box.
DLI Database	Select the DLI database to be added from the drop-down list box.

Step 8 After the asset authorization is complete, the **Connectivity** of the asset is **Checking**, which means DSC is checking the asset connectivity.

- If DSC can access the added asset, the **Connectivity** is **Succeeded**.
- If the DSC cannot access the added asset, the **Connectivity** is **Failed**. Move the cursor to **Failed** to view the failure cause or rectify the fault by referring to section [How Do I Troubleshoot the Failure in Connecting to the Added Database?](#)

----End

Related Operations

- Deleting an instance
A big data instance can be deleted only when the big data instance is a self-built instance and the number of authorized databases in it is 0.
Select multiple self-built instances and click **Batch Delete** in the upper left corner of the instance list to delete the instances. You can also click **Delete** in the **Operation** column of the instance list to delete a single instance.
- Drawing metadata of an instance
 - If the number of authorized databases in the MRS_Hive instance is greater than 0, click **More > Refresh** in the **Operation** column of the Hive instance list to automatically create a metadata task to obtain the database, table, and column information of the instance.

- If you enable the function of automatically creating a metadata task when adding a Hive instance, the system automatically creates a metadata task to obtain all metadata of the instance after the instance is created.
- For details about the big data types that support metadata collection, see section [Creating a Metadata Collection Task](#).
- You can refer to section [Creating a Metadata Collection Task](#) to manually create a metadata collection task.
- Creating an identification task
On the **Databases** tab page, click **Create Identification Task** in the **Operation** column of the asset list to create an identification task for an asset. For details, see section [Creating an Identification Task](#).

4.1.6 Authorizing Access to a Big Data Asset

To identify sensitive data or mask data of a big data instance, you need to authorize access to databases in the instance. This section describes how to authorize access to a database.

Prerequisites


You have subscribed to DLI and CSS, and have assets in them. There are available IP addresses in the corresponding subnets.

Authorizing Access to a Big Data Asset

The Elasticsearch big data type is used as an example to describe how to authorize access to big data assets. To authorize access to other types of big data assets, click the corresponding big data type.

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation tree on the left, choose **Asset Management > Asset Center**. The **Asset Center** page is displayed.

Step 5 Click **Elasticsearch** and choose the **ElasticSearch Instance** tab.

Step 6 Click **Elasticsearch instance**. The **Elasticsearch instance** tab page is displayed. Authorization can be performed in either of the following ways:

- Method 1: Click **Authorize** in the **Operation** column of the ElasticSearch instance list, and enter the Elasticsearch index information to perform authorization.
- Method 2: Click an instance name to go to the instance details page and view the status of all indexes of the instance.

Then click **Authorize** in the **Operation** column to authorize unauthorized indexes.

 NOTE

Click **Set as Default**. The metadata task creates a connection with the default database and draws the metadata of the instance.

Step 7 Click the **Index** tab to view the connection status of authorized assets.

After the asset authorization is complete, the **Connectivity** of the asset is **Checking**, which means DSC is checking the database connectivity.

- If DSC can access the added asset, the **Connectivity** is **Succeeded**.
- If the DSC cannot access the added asset, the **Connectivity** is **Failed**. Move the cursor to **Failed** to view the failure cause or rectify the fault by referring to section [How Do I Troubleshoot the Failure in Connecting to the Added Database?](#)

----End

Related Operations

- Deleting an instance
A big data instance can be deleted only when the big data instance is a self-built instance and the number of authorized databases in it is 0.
Select multiple self-built instances and click **Batch Delete** in the upper left corner of the instance list to delete the instances. You can also click **Delete** in the **Operation** column of the instance list to delete a single instance.
- Drawing metadata of an instance
 - If the number of authorized databases in the MRS_Hive instance is greater than 0, click **More** > **Refresh** in the **Operation** column of the Hive instance list to automatically create a metadata task to obtain the database, table, and column information of the instance.
 - If you enable the function of automatically creating a metadata task when adding a Hive instance, the system automatically creates a metadata task to obtain all metadata of the instance after the instance is created.
 - For details about the big data types that support metadata collection, see section [Creating a Metadata Collection Task](#).
 - You can refer to section [Creating a Metadata Collection Task](#) to manually create a metadata collection task.
- Creating an identification task
On the **Databases** tab page, click **Create Identification Task** in the **Operation** column of the asset list to create an identification task for an asset. For details, see section [Creating an Identification Task](#).

4.1.7 Adding a Log Stream

Add cloud log assets to DSC.

Prerequisites


- DSC has been allowed to access the LTS assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).

- LTS has been enabled and there are logs on it.

Adding a Log Stream

Step 1 Log in to the management console.

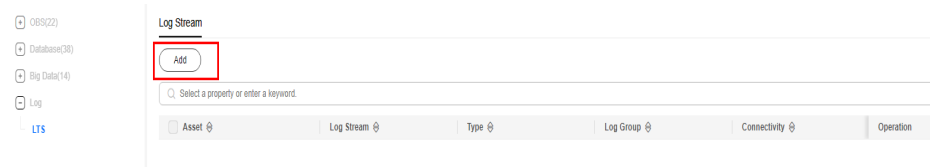
Step 2 Click  in the upper left corner and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation tree on the left, choose **Asset Management > Asset Center**. The **Asset Center** page is displayed.

Step 5 Choose **Log < LTS**. The **Log Stream** tab page is displayed.

Figure 4-8 LTS database list



Step 6 Click **Add** in the upper left corner of the database list. The **Add Log Stream** dialog box is displayed.

Step 7 Set parameters according to [Table 4-7](#) and click **OK**.

Table 4-7 Parameters for adding a database

Parameter	Description
Asset	Enter a user-defined asset name containing 4 to 255 characters.
Big Data Type	Select LTS from the drop-down list box.
Log Group	Select a log group from the drop-down list box.
Log Stream	Select the log stream to be added from the drop-down list box.

Step 8 After the asset authorization is complete, the **Connectivity** of the asset is **Checking**, which means DSC is checking the asset connectivity.

- If DSC can access the added asset, the **Connectivity** is **Succeeded**.
- If the DSC cannot access the added asset, the **Connectivity** is **Failed**. Move the cursor to **Failed** to view the failure cause or rectify the fault by referring to section [How Do I Troubleshoot the Failure in Connecting to the Added Database?](#)

----End

4.2 Managing Asset by Group

Database and big data assets in the asset center can be easily maintained and managed by group. This topic describes how to manage assets by group.

Prerequisites


- Access to cloud assets has been authorized. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- Access to the target assets has been authorized. For details, see asset authorization in section [Asset Center](#).

Creating a Database Group

You can create labels to categorize your assets, making them easier to manage and view.

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation pane on the left, choose **Asset Management > Asset Group Management**.


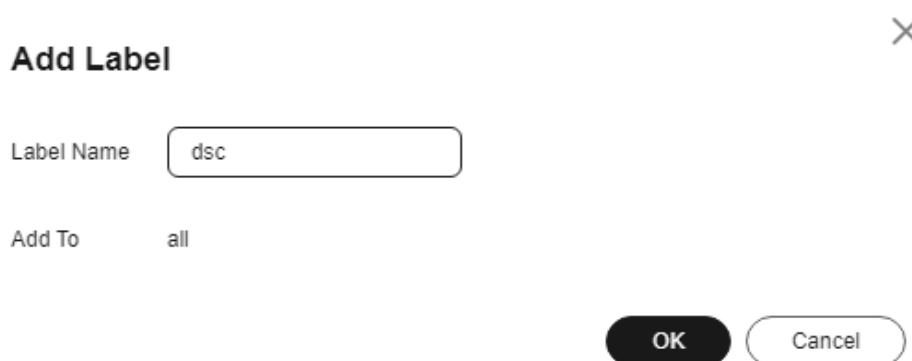
Step 5 Move the cursor to **all** or the newly created label and click . The **Add Label** dialog box is displayed.

Figure 4-9 Adding a label



Add Label ✕

Label Name

Add To

OK **Cancel**

Step 6 Set the label name (group name) and click **OK**. A label is created.


----End

Managing Database Groups


You can regroup databases by moving them to another group.

Step 1 [Log in to the management console.](#)

Step 2 Click  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 In the navigation pane on the left, choose **Asset Management > Asset Group Management**.

Step 5 In the **All Data** tree, select the group to be managed. On the right page, click  on the left of a database instance to expand the database instance details.

Step 6 Select the database to be moved and click **Move** in the **Operation** column. In the **Move** dialog box, select the target label.

Step 7 Click **OK**.


----End

Deleting a Database Group


The **ungrouped** group provided by the system cannot be deleted.

Step 1 [Log in to the management console.](#)

Step 2 Click  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 In the navigation pane on the left, choose **Asset Management > Asset Group Management**.

Step 5 Move the cursor to a label name in the **All Data** tree and click  to delete the label.

Step 6 Click **OK**.

After the label is deleted, assets under the label are moved to **Ungrouped**.

----End

4.3 Metadata Tasks

4.3.1 Creating a Metadata Collection Task

After a metadata task is created, the task creates a connection with the default database to obtain the metadata of the instance. This topic describes how to create a metadata collection task.


Prerequisites

Access to cloud assets has been authorized. For details, see [Allowing or Disallowing Access to Cloud Assets](#).

Procedure

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation pane on the left, choose **Asset Management > Metadata Task**.

Step 5 On the **Metadata Collection Task** page, click **Create**. [Parameter description](#) describes the parameters required for data source configuration.

Table 4-8 Parameter description



Parameter	Description
Data Source	Select a data source. Available options are MySQL, TDSQL, PostgreSQL, DMDBMS, Kingbase, OpenGuass, DWS, Hive, and MRS_HIVE .
Database Instance	Select a database instance from the drop-down list box.
Add Configuration	You can click Add Configuration to add a configuration item.

Step 6 Click **Next**. The **configure subtasks** page is displayed.

- Choose  or  to enable or disable **Scan user tables**.
- Choose  or  to enable or disable **Scan systems tables**, including **information_schema**.
- Choose  or  to enable or disable **Scan column constraints** to check whether the constraints contain primary keys or whether there are unique constraints.
- Choose  or  to enable or disable **Scan views** to check whether metadata contains views.
- Choose  or  to enable or disable **Scan column comments**.
- Click  or  to enable or disable **Scan permissions**.

Step 7 Click **Next** to configure the task information. [Parameter description](#) describes the parameters required for configuring task information.

Table 4-9 Parameters description

Parameter	Description
Task Details	<ul style="list-style-type: none">• Task: You can customize the name of a collection task. This parameter is mandatory.• Task Description: Task description. This parameter is optional.
Task Settings	Click  or  to enable or disable Delete disconnected metadata .
When to Execute	<ul style="list-style-type: none">• Identification Period: You can select Once, Daily, Weekly, or Monthly.• When to Execute: You can select Now or As scheduled.

Step 8 Click **Next**. On the configuration confirmation page that is displayed, confirm the parameters.

Step 9 Click **Finish**. A new metadata collection task is created.

----End

4.3.2 Running a Metadata Collection Task

You can view and execute a created metadata collection task.


Prerequisites

A metadata collection task has been created. For details, see [Creating a Metadata Collection Task](#).

Procedure

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation tree on the left, choose **Asset Management > Metadata Task**. The metadata collection task page is displayed.

Table 4-10 Parameters of a metadata collection task

Parameter	Description
Name	Metadata collection task name
Enable/Disable	Enabling or disabling the current task

Parameter	Description
Sub Tasks	Sub-task name
Scheduling Policy	You can select Once , Daily , Weekly , or Monthly .
Created	ID of user who created the task
Last Run	Last running time of a task

Step 5 Click **Running** in the **Operation** column to run the created metadata collection task.


Step 6 Click  on the left of a metadata collection task to view the task running details. **Parameter description** describes the parameters of the running details of a metadata collection task.

Table 4-11 Parameter description

Parameter	Description
Start Time	Time when a task starts to be executed
End Time	Time when a task ends.
Execution Method	Once , Daily , Weekly , or Monthly
Status	Running status of the current task. The options are as follows: <ul style="list-style-type: none">● Completed: The metadata collection task has been completed.● Running: The metadata collection task is running.● Failed: The metadata collection task fails to be executed.● Scheduling: The metadata collection task has been added and is to be executed.● Partially completed: The metadata collection task has been partially completed.
Duration	Duration from the time when a task starts to run to the time when the task ends.

----End

Related Operations

You can click **Edit** or **Delete** in the **Operation** column to edit or delete a metadata collection task

4.4 Data Exploration

The data exploration page displays the databases, data tables, and data views obtained through metadata tasks. You can add descriptions, tags, security levels, and classifications to manage data assets by level and classification.


Prerequisites

- DSC has been allowed to access the database assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- Metadata has been scanned. For details, see [Metadata Tasks](#).

Procedure

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation pane, choose **Asset Management > Data Exploration**.

Step 5 Select a display mode from the drop-down list box in the upper left corner.

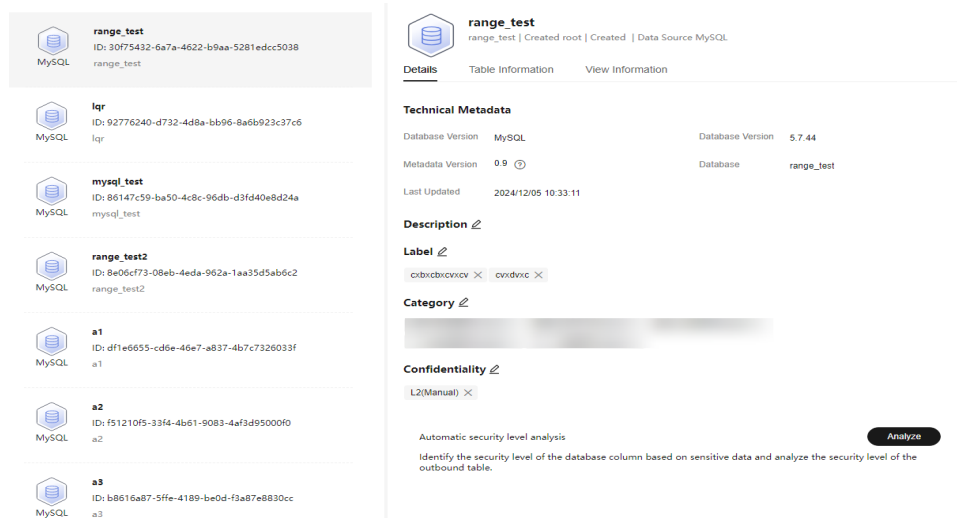
- **Database**
- **Schema**
- **Table**
- **Data Column**

Step 6 Click a database name.

You can add descriptions, labels, security levels, and categories to databases, data tables, and data views.

Click **Analyze** to perform automatic security level analysis. The security levels of databases and tables are determined based on their column security levels generated in the sensitive data identification results.

Figure 4-10 Database details

**Step 7** View detailed information about the database.

- On the data details page, click the **Table Information** tab.
 - Click a table name to view its details.
 - Select a table and click **Identifier** in the upper left corner to add a table identifier. You can select a label or security level..
 - **Label:** Click the **Select Label** text box to select an added label or enter text and press Enter to add a label temporarily, and click **OK**.
 - **Security Level :** Select a security level from the **Select Security Level** drop-down list. The security levels include built-in levels and custom levels. To create a security level, see [Adding a Sensitive Level](#). Select a security level and click **OK**.
 - You can also click the edit button to add information such as the category, security level, label, and description for a single table.
- On the data details page, click the **View Information** tab.
 - Click the view name to view the view details.
 - Click the **View Information** tab, select a view, and click **Identifier** in the upper left corner to add a view identifier.
 - **Label:** Click the **Select Label** text box to select an added label or enter text and press Enter to add a label temporarily, and click **OK**.
 - **Security Level :** Select a security level from the **Select Security Level** drop-down list. The security levels include built-in levels and custom levels. To create a security level, see [Adding a Sensitive Level](#). Select a security level and click **OK**.
 - You can also click the edit button to add information such as the category, security level, label, and description to the view.
- Click the **Schema Information** tab (this tab is displayed only when the database has schemas).
 - Select a schema and click **Identifier** in the upper left corner to add a column identifier. The identifier may be a label or a security level.

- **Label:** Click the **Select Label** text box to select an added label or enter text and press Enter to add a label temporarily, and click **OK**.
- **Security Level :** Select a security level from the **Select Security Level** drop-down list. The security levels include built-in levels and custom levels. To create a security level, see [Adding a Sensitive Level](#). Select a security level and click **OK**.
- You can also click the edit button to add information such as the category, security level, label, and description to the schema.

----End

Related Operations

Enter a database name, database table name, data table column name, or template name in the search box to search for the database information you want to view.

4.5 Asset Catalog

The asset catalog collects statistics on sensitive information about assets from two dimensions: **service domain** and **data type**. It allows users to view sensitive information from three dimensions: **database**, **table**, and **column**.

- The labels of **Service Domain** are created on the [Asset Group Management](#) page. You can modify the category label on the [Asset Group Management](#) page.
- **Data Types**
Structured data: The following data types are supported: DWS, **PostgreSQL**, **DMDBMS (Dameng)**, **MySQL**, **OpenGauss**, **KingBase (KingBase)**, **TDSQL**, **SQLServer**, **Hive**, and **MRS_HIVE**.


Prerequisites

- Access to cloud assets has been authorized. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- Specific assets have been added or authorized. For details, see [Asset Center](#).

Viewing the Asset Catalog

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation pane, choose **Asset Management > Asset Catalog**.

Step 5 On the **Service Domain** or **Data Type** tab page, view the added data asset information. [Data catalog parameters](#) describes related parameters.

You can select a group of data asset on the left to view statistics of a specific data asset on the **Service Domain** tab page, or select a data type on the left tree to view data asset of a data type on the **Data Type** tab.

Table 4-12 Data catalog parameters

Parameter	Description
Statistics	<p>Click View Details. On the Sensitive Data Statistics page, statistics are displayed in three dimensions: category, level, and database.</p> <ul style="list-style-type: none"> • Sensitive databases/Total databases: the percentage of sensitive databases in all databases. • Sensitive tables/Total tables: the percentage of sensitive data tables in all data tables. • Sensitive data columns/Total columns: the percentage of sensitive data columns in all data columns. <p>NOTE WoW indicates the data changes compared with the previous week.</p>
Percentage of Different Levels of Data	<p>Pie chart showing the proportion of sensitive data columns of different security levels in the total data columns</p> <p>Click View Details. On the Sensitive Data Statistics page, statistics are displayed in three dimensions: category, level, and database.</p>
Top 5 Categories	<p>Top 5 data type with the highest proportion</p> <p>Click View Details. On the Categorization Result Details page, view the statistics.</p>
Data Volume	<p>Line chart showing the change of data volume over time</p> <p>Click View Details. On the Sensitive Data Statistics page, statistics are displayed in three dimensions: category, level, and database.</p>


Parameter	Description
Database Scale Table	<p>Displays the number of databases, tables, and columns that contain sensitive data in a database instance. For details, see Viewing Database Instance Details.</p> <ul style="list-style-type: none">● Database Instance/ID: Database instance name or ID.● Host port: host port number● User: username● Sensitive Databases: Number of databases in the instance that contain sensitive data.● Sensitive Tables: Number of tables in the instance that contain sensitive data.● Sensitive Columns: Number of columns in the instance that contain sensitive data.

----End

Viewing Database Instance Details

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation pane, choose **Asset Management > Asset Catalog**.

Step 5 Click the **Service Domain** or **Data Type** tab.

Step 6 Select a group label or data type on the left and click the database instance name in the **Database Scale Table** list. The **instance Details** page is displayed.

View information about all databases in the instance, including the **Database Name, Total Tables, Sensitive Tables, Sensitivity Level, Tag, and Last Scan Time**.

Click the database name. The **Database Details** page is displayed, including the **Basic Information** and **Database Tables** tab pages.

- The **Basic Information** tab page displays information such as the database type, version, and name. Click **Analyze** to perform automatic security level analysis. The security levels of databases and tables are determined based on their column security levels generated in the sensitive data identification results.

- The **Database Tables** tab page displays the data table name, number of table columns, associated schema, category, and sensitivity level. Click to view details.

Figure 4-11 Instance details

Database	Total Tables	Sensitive Tables	Sensitivity Level	Label	Last Scanned
test_dbms c214489c7-95e2-482b-a481-c09c396420ed	2	2	1550	mm	Dec 05, 2024 10:33:09 GMT+08:00

----End

5 Sensitive Data Identification

5.1 Overview of Sensitive Data Identification

Sensitive data identification automatically identifies sensitive data and analyzes the usage of such data. With data identification engines, structured data (RDS and DWS) and unstructured data (OBS) is scanned and classified. It then automatically identifies sensitive data and analyzes the usage of such data for further ensuring security.

Constraints

For Hive data in MRS, sensitive data can be identified only when **Match Type** is Rule **matching** and **Rule** is **Content > Include**.

Process

Figure 5-1 Flowchart

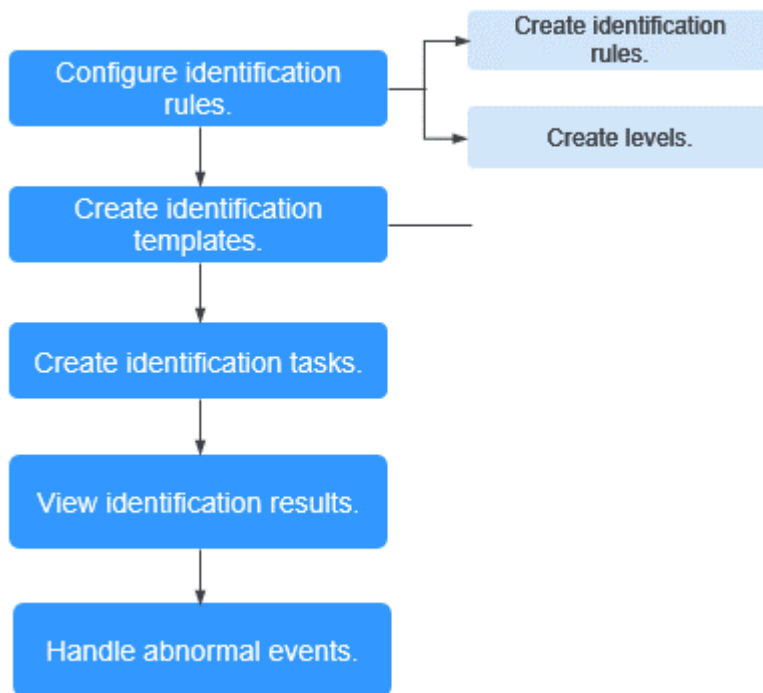


Table 5-1 Functions

Function	Description	Related Operations
Identification Rule	Built-in data identification rules of Data Security Center of Huawei Cloud can be used. In addition, you can also customize new rules to classify scattered data based on identification rules. These rules are mandatory for creating identification templates.	Customizing a Rule
Sensitivity Configuration	The built-in data security levels of Huawei Cloud Data Security Center are available. In addition, you can also customize new levels to classify rules.	Customizing a Level

Function	Description	Related Operations
Identification Template	The built-in templates according to the Huawei Cloud data security classification and grading standard and best practices are provided. In addition, you can customize new classification and grading templates to manage scattered rules in a unified manner. These templates are mandatory for creating identification tasks.	Creating an Identification Template
Identification Task	Based on the created identification task, DSC automatically identifies sensitive data in a specified database, OBS bucket, big data source, LTS, or MRS, and generates identification results and reports.	Creating a Sensitive Data Identification Task
Viewing or Downloading the Identification Result	After the scanning is complete, you can view the identification result in the identification task list or download the identification result to the local PC.	Identification Results

5.2 Sensitive Data Identification Configuration

5.2.1 Creating an Identification Template


By default, DSC provides a built-in identification template. You can create or copy a template to customize a new identification template. This topic describes how to add an identification template.


Constraints

A maximum of 20 identification templates can be created for an account.

Copying the Identification Template

Step 1 [Log in to the management console.](#)

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**. The **Identification Template** tab page is displayed.


Step 5 Locate the target template, Click **Copy**. In the displayed **Copy Template** dialog box, enter the new template name and description.


Step 6 Click **OK**.

----End

Creating an Identification Template

Step 1 [Log in to the management console](#).

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**.

Step 5 Click **Create Template** in the upper left corner of the page to create a template. In the **Create Template** dialog box, enter the **Template Name** and **Description**.

Step 6 Click **OK**. The new identification template is displayed in the identification template list.

----End

Related Operations

- Click **Set As Default** to set the template as the default template.
- Click **Overview** to view the template type and level.

5.2.2 Managing Identification Templates

You can modify the content of a custom template. For details, see [Editing a Classification and Grading Template](#).


The rule category of a template can be modified. The [Modifying a Rule Category](#) section describes how to modify a rule category.




Constraints

A built-in template and the default identification template cannot be deleted.



Modifying an Identification Template

Step 1 [Log in to the management console](#).

Step 2 Click  in the upper left corner of the management console and select a region or project.



- Step 3** In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**. The **Identification Template** tab page is displayed.
- Step 5** Locate the target template, click **Details**. The template details page is displayed.
- Click  after **All** to create a category.
 - Move the cursor to a category name:
 - Click the edit button to edit the category name.
 - Click **Delete** to delete a category name.
 - Click a category name on the left tree and view related category rules on the right.
 - Click **Add Rule** in the upper left corner. For details, see [Customizing a Rule](#).
 - Click **Batch Delete** to delete the selected rules.
 - Click  in the **Status** column to enable or disable a rule. After the rule is disabled, it will not take effect during identification using the template.
 - Click **Details** in the **Operation** column to edit the rule content.
 - Click **Delete** in the **Operation** column to delete a rule.
- End

Modifying a Rule Category

- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**. The **Identification Template** tab page is displayed.
- Step 5** Locate the target template, click **Details**. The template details page is displayed.
- Step 6** Select the rules whose categories are to be modified.
- Step 7** Click **Modify Category** in the upper left corner of the rule list. In the displayed dialog box, select the target category.
- Step 8** Click **OK**. A message is displayed, indicating that the rule categories are modified.
- End

Deleting an Identification Template

- Step 1** [Log in to the management console](#).

- Step 2** Click  in the upper left corner of the management console and select a region or project.
 - Step 3** In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.
 - Step 4** In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**. The **Identification Template** tab page is displayed.
 - Step 5** Click **Delete** under the corresponding classification and grading template to delete the template.
 - Step 6** Click **OK**. The classification and grading template in use cannot be deleted. Delete the corresponding identification task first and then delete the classification and grading template.
- End

5.2.3 Customizing a Rule

Sensitive data identification rules include built-in rules and user-defined rules. You can select built-in or customized identification rules when creating or editing an identification template.

Procedure



- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**. The **Identification Template** tab page is displayed.
- Step 5** Click the **Identification Rule** tab. The **Identification Rule** page is displayed.
- Step 6** Click **Create a user-defined rule** in the upper left corner of the page.
- Step 7** In the displayed dialog box, set required parameters based on [Table 5-2](#).

Table 5-2 Parameter description

Parameter	Description
Rule	You can customize a rule name. The rule name must meet the following requirements: <ul style="list-style-type: none">• Contain 1 to 255 characters.• Consist of letters, digits, underscores (_), hyphens (-), and brackets.• Be unique.
Description	Enter a rule description.
Add to Template	<ul style="list-style-type: none">• Select the template name, template rule category, and level from the drop-down list boxes to add the rule to a rule template.• Click Add to add the rule to multiple templates.• Click the deletion button to delete the template. Retain at least one template.
Match Type	This parameter can be set to Rule matching or Keyword matching . <ul style="list-style-type: none">• Keyword matching indicates that the rule can be executed using keywords.• Regular matching is used to match (specify and identify) characters, words, and patterns. NOTE For Hive data in MRS, sensitive data can be identified only when Match Type is Rule matching and Rule is Content > Include .
Matching Logic	Select the matching logic: <ul style="list-style-type: none">• AND: All keywords are included.• OR: Only one keyword is included.



Parameter	Description
Rule	<p>This parameter is displayed when Match Type is set to Rule matching. Select the rule content from the drop-down list.</p> <ul style="list-style-type: none"> Choose Column Name > Include or Column Comment > Include. Enter a keyword to check whether the column name or column comment contains the keyword. Choose Column Name > Regex or Column Comment > Regex and enter a regular expression to check whether it matches. Choose Content > Include. Enter a keyword to check whether the keyword is contained in the content. Choose Content > Regex. Enter a regular expression to check whether the regular expression matches. Choose Content > Keyword and enter multiple keywords. The relationship between the keywords is OR, meaning if any keyword is found in the content, it will be matched. <p>NOTE For Hive data in MRS, sensitive data can be identified only when Match Type is Rule matching and Rule is Content > Include.</p>
Test Rule	<ul style="list-style-type: none"> This parameter is displayed when Match Type is set to Rule Matching. Enter the rule content and click Test. The test result of the rule is displayed in the Test Result area. You can click Add to add multiple rules for test. Both built-in rules and user-defined rules support rule tests. To test a built-in rule, click Details in the Operation column of the rule list. On the Edit Rule page, enter the rule for test. <p>NOTE</p> <ul style="list-style-type: none"> Image rules cannot be tested. The rule test is not supported when the Match Type is Keyword matching. Only the first matching result of the test content is displayed.
Content	<ul style="list-style-type: none"> This parameter is displayed when Match Type is set to Keyword Matching. Multiple keywords are separated by line breaks.
Identification Threshold Configuration	Applicable to unstructured data. You can select a low, medium, or high threshold. A higher threshold requires more hits.
Hit Rate	Applicable to structured data. You can drag the slider to set the value. A larger value indicates a higher hit rate.

Step 8 Click **OK**.

----End

5.2.4 Editing a Rule

Procedure

- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**. The **Identification Template** tab page is displayed.
- Step 5** Click the **Identification Rule** tab. The **Identification Rule** page is displayed.
- Step 6** In the **Operation** column of the target rule, click **Edit** to view and modify the rule. You can modify the values of the following parameters in a built-in rule: **Add to Template**.

----End

5.2.5 Viewing Built-in Rules

DSC provides seven types of built-in rules for sensitive information in various industries, including sensitive image information, sensitive personal information, and sensitive enterprise information. This section describes how to view the built-in rules of DSC.

Constraints

Currently, OCR can recognize business license images only in some regions. For details about the supported regions, see [Regions Supported by OCR](#).

The restrictions on using other built-in image rules are as follows:


Restrictions on Passport OCR


- All fields on Chinese mainland passports can be recognized.
- Passports that are issued by China, Hong Kong (China), Macao (China), Taiwan (China), and other countries and regions and that are with complete machine-readable codes can be recognized.
- Only images in PNG, JPG, JPEG, BMP, or TIFF format can be recognized.
- No side of the image can be smaller than 15 or larger than 4,0968,192 pixels.
- The information page of the passport to be recognized must occupy more than 25% of the image. When scanning a passport, ensure that the entire page is displayed in the image.
- A passport can be rotated to any angle.
- The passport in the image can be moderately distorted, but the aspect ratio cannot be distorted by more than 10%.

- Illuminated or dark images can be recognized, but the accuracy may be compromised.

Viewing Built-in Rules

Step 1 [Log in to the management console.](#)

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**. The **Identification Template** tab page is displayed.

Step 5 Click the **Identification Rule** tab. The **Identification Rule** page is displayed. The built-in rules are shown in [Table 5-3](#).

Click the search box above the rule list and select a filter.

Table 5-3 Built-in rules

Category	Sensitive Information
Personal sensitive image information	<ul style="list-style-type: none">• Driving license image (Chinese mainland)• Bank card image (Chinese mainland)• ID card image (Chinese mainland)• Image of motor vehicle registration certificate (Chinese mainland)• Passport image (Chinese mainland)• Auto insurance policy image (Chinese mainland)• Motor vehicle license image (Chinese mainland)

Category	Sensitive Information
Personal privacy	<ul style="list-style-type: none"> ● ID card No. (Chinese mainland) ● Passport No. (Chinese mainland) ● Driver's license No. (Chinese mainland) ● Exit-Entry Permit for Traveling to and from Hong Kong and Macau (EEP) ● Car license plate number (Chinese mainland) ● Military ID card number ● American social security number (SSN) ● ITIN ● Social security information ● Vehicle identification number ● Name (Simplified Chinese) ● Name (English) ● Nationality ● Gender ● Ethnicity ● Birthday ● Birth place ● Education level ● Company ● Industry ● Telephone number (Chinese mainland) ● Mobile number (Chinese mainland) ● Email ● Marital status ● Family member relationship ● Religion ● Bank account number ● Credit card number ● MasterCard credit card number ● VISA credit card number ● Credit card security code

Category	Sensitive Information
Enterprise information	<ul style="list-style-type: none"> ● Business registration number ● Unified social credit code ● Taxpayer identification number (tax number) ● Organization code ● Enterprise type ● Operation status ● Enterprise delivery information ● Enterprise requirement information
Device information	<ul style="list-style-type: none"> ● International mobile equipment identity (IMEI) ● Mobile equipment identity (MEID) ● MAC address ● SIM card IMSI information. ● IPv4 address ● IPv6 address ● Linux-Passwd file ● Linux-Shadow file
Key credential information	<ul style="list-style-type: none"> ● SSL certificate ● Access_Key_Id ● Secret_Access_Key ● AWS_ACCESS_KEY ● AWS_SECRET_KEY ● Facebook_SECRET ● IAM op_service account and password ● GitHub_KEY ● DSA private key ● EC private key ● Encryption private key ● RSA private key
Location	<ul style="list-style-type: none"> ● GPS data ● Exact address (China) ● Province (Chinese mainland) ● Postal code (Chinese mainland) ● City (Chinese mainland) ● Municipality (China) ● Address (Chinese mainland)

Category	Sensitive Information
System network information	<ul style="list-style-type: none">• URL link• LDAP• OS
Time information	<ul style="list-style-type: none">• Date• Time

----End

5.2.6 Adding a Sensitive Level

DSC provides four built-in sensitive data levels: L1 to L4. You can customize a level by following the instructions in this topic.

Constraints

A maximum of 20 security levels can be created.

Procedure



- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**. The **Identification Template** tab page is displayed.
- Step 5** Click the **Sensitivity Configuration** tab and click **Adding a Level** in the upper left corner.
- Step 6** In the displayed dialog box, set required information based on [Table 5-4](#).

Table 5-4 Parameter description

Parameter	Description
Level	Enter a user-defined level name.
Level Color	You can select a color based on the sensitivity level. A higher level color value indicates a higher sensitivity. For example, name and gender are low-sensitivity data, and the ID card number and encryption key are high-sensitivity data.

Step 7 Click **OK**.

----End


5.2.7 Managing Levels


This section describes how to modify, delete, or disable a sensitivity level.

Editing a Level

A built-in sensitivity level cannot be edited.

Step 1 [Log in to the management console](#).

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**. The **Identification Template** tab page is displayed.

Step 5 Click the **Sensitivity Configuration** tab to view the sensitivity level configuration list.

Step 6 Locate the target level to be modified, click **Edit** in the **Operation** column, and modify the level information.


Step 7 Click **OK** to save the modification.


----End

Deleting a Level

Only custom levels that are not referenced can be deleted.

Step 1 [Log in to the management console](#).

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**. The **Identification Template** tab page is displayed.

Step 5 Click the **Sensitivity Configuration** tab to view the sensitivity level configuration list.

Step 6 In the **Operation** column of the target level, click **Delete** to delete the level content.


Step 7 Click **OK**.


----End

Disabling a Level

A built-in level cannot be disabled.

Step 1 [Log in to the management console.](#)

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**. The **Identification Template** tab page is displayed.

Step 5 Click the **Sensitivity Configuration** tab to view the sensitivity level configuration list.

Step 6 Locate the target level to be disabled, click **Disable** in the **Operation** column.

NOTE

- Disabled levels are not displayed when you create or edit a template.
- To enable a level, click **Enabled** in the **Operation** column of the row that contains the level.

----End

5.3 Sensitive Data Identification Tasks

5.3.1 Creating an Identification Task


Based on the created identification task, DSC automatically identifies sensitive data in a specified database, OBS bucket, big data source, LTS, or MRS, and generates identification results and reports. This topic describes how to create an identification task.


Prerequisites

- Access to cloud assets has been authorized. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- OBS assets or authorized database/big data assets have been added. For details, see the operations of adding and authorizing assets in [Asset Center](#).

Creating an Identification Task

Step 1 [Log in to the management console.](#)

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane on the left, choose **Sensitive Data Identification > Identification Task**.

Step 5 In the upper left corner of the task list, click **Create Task**.

Step 6 In the displayed dialog box, set required parameters based on [Table 5-5](#).

Figure 5-2 Creating a sensitive data identification task

Edit Task ×

* Task Name

* Data Type

- OBS ▼
- Database ▼
- Big Data ▼
- MRS ▼
- LTS ▼

* Identification Template ▼

* Identification Period Once Daily Weekly Monthly

* When to Execute Now As scheduled

Notification Topic ▼ [View Topic](#)

The drop-down list displays only topics whose subscription status is Confirmed.

Table 5-5 Parameter description

Parameter	Description
Task Name	<p>You can customize the task name.</p> <p>The task name must meet the following requirements:</p> <ul style="list-style-type: none">• Contain 4 to 255 characters.• Consist of letters, digits, underscores (_), and hyphens (-).• The name must start with a letter.• Be unique.
Sensitive Data	<p>Type of data to be identified. You can select multiple types.</p> <ul style="list-style-type: none">• 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.• Database: DSC identifies sensitive data of authorized database assets. For details about how to authorize DSC to access your database assets, see Authorizing Access to a Database Asset.• Big data: DSC identifies sensitive data of authorized big data assets. For details about how to authorize DSC to access your big data assets, see Authorizing Access to a Big Data Asset.• MRS: DSC identifies sensitive data of authorized big data assets. For details about how to authorize DSC to access your MRS assets, see Authorizing Access to a Big Data Asset.• LTS: DSC identifies sensitive data of authorized LTS assets. For details about how to add log streams, see Adding a Log Stream.
Identification Template	<p>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 Creating an Identification Template.</p>
Identification Scope	<p>This parameter is displayed when Data Type is set to LTS. Set this parameter to 1 day, 2 days, or 3 days.</p>
Identification Intensity	<p>This parameter is displayed when Data Type is set to LTS. Select the log identification intensity, which can be High, Medium, or Low. A higher intensity indicates more sampled data.</p>

Parameter	Description
Identification Period	Set the execution policy of the data identification task. <ul style="list-style-type: none">● Once: The task will be executed once at a specified time.● Daily: The task is executed at a fixed time every day.● Weekly: The task is executed at a specified time every week.● Monthly: The task is executed at a specified time every month.
When to Execute	This parameter is displayed when Identification Period is set to Once . <ul style="list-style-type: none">● Now: Select the option and click OK, the system executes the data identification task immediately.● As scheduled: The task will be executed at a specified time.
Start Time	This parameter is displayed when Identification Period is set to Daily , Weekly , or Monthly . Select the time when the task is being executed. After the time is selected, the task is executed every day, every week, every month, or at the specified time.
(Optional) Topic	<ul style="list-style-type: none">● Select an existing topic from the drop-down list or click View Topic to create a topic for receiving alarm notifications.● If you do not configure a topic, you can view the identification result in the identification task list. For details, see Identification Results.

Step 7 (Optional) If you need to set the scan scope for the added assets, see section [Adding an Identification Scope](#).


Step 8 Click **OK**. A message is displayed indicating the task is created successfully.


----End

Adding an Identification Scope

By default, DSC performs a global scan on the selected assets. You can also add a scan scope by referring to this section.

Step 1 [Log in to the management console](#).

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

- Step 4** In the navigation pane on the left, choose **Sensitive Data Identification > Identification Task**.
- Step 5** Click **Create Task**. The **Create Task** page is displayed.
- Step 6** Select the data type, select the name of the asset to be scanned, and click **OK**.
- Step 7** In the lower left corner of the page, click the button to add an identification scope. You can add multiple scopes at the same time. For details about the parameter settings, see [Table 5-6](#).

Table 5-6 Parameters for configuring the scan scope

Asset Type	Configuration Parameter	Description
OBS	Asset	Select the bucket to be scanned from the drop-down list. You can select multiple buckets.
	Scan Scope	<ul style="list-style-type: none">• File name prefix: For example, if the prefix is <i>dsc_</i>, all files with the prefix <i>dsc_</i> are scanned. A maximum of one inclusion condition can be added for the file name prefix.• File name extension: The file name extension contains the file type following the dot (.). For example, the file name extension <i>dsc_security.txt</i> can be <i>security.txt</i> or <i>.txt</i>. Only the files that meet all the filtering conditions are scanned. A maximum of one inclusion condition can be added for the file name extension.• Directory name: Specifies the directory to be scanned. All files in the specified directory are scanned. A maximum of one inclusion condition can be added for the directory. <p>After entering the file name prefix/suffix/directory name, click Add as Inclusion Condition to add it as an inclusion condition.</p> <p>For example, if you select the File name prefix, enter the prefix <i>dsc_</i>, and click Add as Inclusion Condition, only the files whose file name prefix is <i>dsc_</i> are scanned. If you click Add as Exclusion Condition to as the prefix as an exclusion condition, only files whose prefixes are not <i>dsc_</i> are scanned.</p>

Asset Type	Configuration Parameter	Description
	Scan Depth	<ul style="list-style-type: none">● Global Scan: If this parameter is selected, all data is scanned.● Specify Scan Scope: Select Specify Scan Scope and enter the Scan Depth. The depth of the root directory starts at 1 and increases incrementally. However, it must not surpass a depth of 10.
Database/Big Data/MRS	Asset	Select an instance name from the drop-down list. You can select multiple instances.
	Scan Scope	<ul style="list-style-type: none">● Table name prefix: A maximum of one inclusion condition can be added for the table name prefix. For example, if you enter <i>dsc_</i> as the prefix of a table name and click Add as Inclusion Condition only the table data whose prefix is <i>dsc_</i> is scanned. If you click Add as Exclusion Condition to as the prefix as an exclusion condition, only tables whose prefixes are not <i>dsc_</i> are scanned.● Table name suffix: A maximum of one inclusion condition can be added for the table name suffix. The principle is the same as that of the prefix.
LTS	Asset	Select an instance name from the drop-down list. You can select multiple instances.
	Scan Scope	<ul style="list-style-type: none">● Key prefix: If this parameter is added as an inclusion condition, the log content that contains the key prefix is scanned. If this parameter is added as an exclusion condition, the log content except the key prefix is scanned.● Key suffix: The principle is the same as that of the key prefix. <p>NOTE</p> <ul style="list-style-type: none">- A maximum of one inclusion condition can be added for each of the key prefix and suffix.- A maximum of 10 exclusion conditions can be added for key prefixes and suffixes.

Figure 5-3 Configuring the scan scope

+ Add Database Identification Scope

Database Scan Configuration1 × Cancel

Asset --Select--

Scan Scope Specify Scan Scope ?

prefix

Add as Inclusion Condition Add as Exclusion Condition

Inclusion Co...	Type	O..	Exclusion Co...	Type	O..

+ Add Big Data Identification Scope

OK Cancel

----End

Follow-up Procedure

Viewing the Identification Result: After the sensitive data identification task is complete, you can click **Identification Result** in the **Operation** column of the row containing the target task to view the total number of sensitive information items, risk level, and sensitive information classification and grading result of the data assets. You can also download these statistics as a report.

5.3.2 Starting a Task


DSC can repeatedly execute an identification task. You can start an identification task by following the instruction in this topic.


Prerequisites

- Access to cloud assets has been authorized. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- OBS assets or authorized database/big data assets have been added. For details, see the operations of adding and authorizing assets in [Asset Center](#).

Procedure

Step 1 [Log in to the management console](#).

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane on the left, choose **Sensitive Data Identification > Identification Task**.

Step 5 Locate the task to be started and click **Start Identification** in the **Operation** column. If a message is displayed in the upper right corner, indicating that the scan task starts, the operation is successful.

NOTE

If you want to stop an ongoing task, click **Stop** in the **Operation** column of the row containing the target task.

To disable a scheduled task, choose **More > Stop Task** in the **Operation** column of the target task.

----End

Follow-up Procedure

Viewing the Identification Result: After the sensitive data identification task is complete, you can click **Identification Result** in the **Operation** column of the row containing the target task, to view the total number of sensitive information items, risk level, and sensitive information classification and grading result of the data assets.

5.3.3 Identification Tasks

This section describes how to view, edit, and delete a sensitive data identification task in the task list.

Prerequisites

An identification task has been created and executed.

Viewing the Identification Task List

Step 1 [Log in to the management console](#).




- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane on the left, click **Sensitive Data Identification > Identification Task**. [Table 5-7](#) describes the parameters.

Table 5-7 Identification task parameters


Parameter	Description
Task Name	Identification task name Click  on the left of a task name to view the scanning time and task status. In the Operation column of a specific object, you can perform the following operations: <ul style="list-style-type: none">• Click Stop to stop scanning on the object.• Click Start Identification to start scanning on the object.• Click Identification Result to view the scanning result.• Click Delete to delete the identification task of the object.
Identification Template	Name of the identification template used by the task.
Execution Period	Execution period of an identification task. The value can be: <ul style="list-style-type: none">• Once: The task is executed only once.• Daily: The task is executed at a fixed time every day.• Weekly: The task is executed at a fixed time every week.• Monthly: The task is executed at a fixed time every month.
Status	Execution status of an identification task <ul style="list-style-type: none">• Pending identification: The task is waiting to be started.• Identifying: The task is being executed.• Identification completed: All objects of the target task have been scanned.• Identification failed: At least one object of the target task fails to be scanned.• Identification terminated: The task that is being executed is forcibly stopped.
Last Identified	Last execution time of the task.
Last Identified Result	Last scan result of the job.


Parameter	Description
Operation	<p>Operations provided in the Operation column:</p> <ul style="list-style-type: none">● Start Identification: Execute an identification task immediately. For details, see Starting a Task.● Identification Result: View and download the identification result. Click Identification Result to go to the result details page. DSC provides a detailed result analysis report. For details, see Identification Results.● Start a task. When the task is closed, choose More > Start Task. For details, see Starting a Task.● Stop a task. When the task is started, choose More > Stop Task. For details, see Stopping an Identification Task.● Edit a task. Choose More > Edit. For details, see Editing an Identification Task.● Delete a task. Choose More > Delete. For details, see Deleting an Identification Task.

----End

Editing an Identification Task

Step 1 [Log in to the management console](#).

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane on the left, choose **Sensitive Data Identification > Identification Task**.


Step 5 Locate the row that contains the target task and choose **More > Edit** in the **Operation** column.


Step 6 In the displayed dialog box, modify the task information and click **OK**.

----End

Deleting an Identification Task

Step 1 [Log in to the management console](#).

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.



- Step 4** In the navigation pane on the left, choose **Sensitive Data Identification > Identification Task**.
- Step 5** Locate the row that contains the target task and choose **More > Delete** in the **Operation** column.
- Step 6** In the displayed dialog box, click **OK**.

⚠ CAUTION

- If an identification task is running, stop the task or wait until the task is complete, then delete it.
 - The deletion cannot be undone.
-

----End

Stopping an Identification Task

- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane on the left, choose **Sensitive Data Identification > Identification Task**.
- Step 5** Locate the row that contains the target task and choose **More > Stop Task** in the **Operation** column.

📖 NOTE

- A task in the **Identifying** status cannot be closed.
- The name of a closed task is displayed in gray, indicating that the task is closed.
- To start this task, click **More > Start Task** in the **Operation** column of the row containing the target task

----End



5.3.4 Identification Results

After a sensitive data identification task is complete, you can view the result on the result details page. You can also download the generated identification result to your local PC. This section explains how to view and download the identification result.

Prerequisites

At least one sensitive data identification task has been executed. For details about how to create a sensitive data identification task, see [Creating an Identification Task](#).

Viewing the Identification Result

- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane on the left, choose **Sensitive Data Identification > Identification Task**.
- Step 5** Click **Identification Result** in the **Operation** column of the target task. The result details page is displayed.
- Step 6** DSC collects statistics on the total number of sensitive information records, risk level distribution, and top 10 matched rules.

DSC also provides a detailed identification result list. Click the filter box in the upper left corner of the list and select one or more filters, such as **Column Name**, **Object Name**, **Database Name**, and **Table Name**, to filter the identification results. For details about the parameters in the identification result list, see [Table 5-8](#).

Table 5-8 Identification result parameters

Parameter	Description
Column Name	Name of the column whose data is identified
Asset	Name of the asset that can be identified
Asset Type	<ul style="list-style-type: none">• OBS• Database• Big Data• MRS• LTS
Asset	Name of the asset containing sensitive information.
Database Name	Name of the database where sensitive information is identified.
Table Name	Name of the table where sensitive information is identified.
Bucket Name	The bucket name is displayed when the asset type is OBS.
Object Path/ Collection Time	Path for storing sensitive information and collection time.
Level	Sensitive information level.

Step 7 In the row containing the desired scan object, click **View Classification and Grading Result Details** in the **Operation** column. The **Classification and Grading Result Details** dialog box is displayed. View the result details and sample data.

- Click **Add Rule** in the upper left corner of the result details list. In the displayed **Add Rule** dialog box, select a new rule from the **New rule** drop-down list and click **OK**. A message is displayed, indicating that the original rule has been replaced with the new rule.
- Click **Replace** in the **Operation** column. In the dialog box that is displayed, select a new rule from the **New rule** drop-down list to replace the rule in the identification result. Click **OK**. A message is displayed, indicating that the original rule has been replaced with the new rule.
- Click **Remove** in the **Operation** column to delete unnecessary rules.


 **NOTE**


- The **Categorization and leveling result details** page displays the **identification object details**, **result details**, and **sample data**.
- The **Result Details** area displays the matching rule, number of hits/hit rate, grading result, and classification and grading template.
- Click the **Sample Data** tab to view the sample data that matches the rule. Currently, sample data of the big data and LTS types cannot be viewed.

----End

Downloading the Identification Result

Step 1 [Log in to the management console](#).

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane on the left, choose **Sensitive Data Identification > Identification Task**.

Step 5 Click **Identification Result** in the **Operation** column of the target task. The result details page is displayed.

Step 6 Click **Generate Result File** in the upper left corner. The **Generate Result File** dialog box is displayed.

- **Identification task:** Name of the scan task.
- **Object Type:** Type of the object to be scanned.
- **Scan object:** Object to be scanned.
- **Export Target Bucket:** Select a bucket for storing the identification result from the drop-down list box. If no bucket is available in the drop-down list box, create a bucket by referring to [Creating an OBS Bucket](#). The *scan-results* folder is created in the root directory of the bucket to store the identification result.
- **Sample data masking:** The sample data masking function is applicable only to assets that support sample data viewing, such as databases and OBS. If

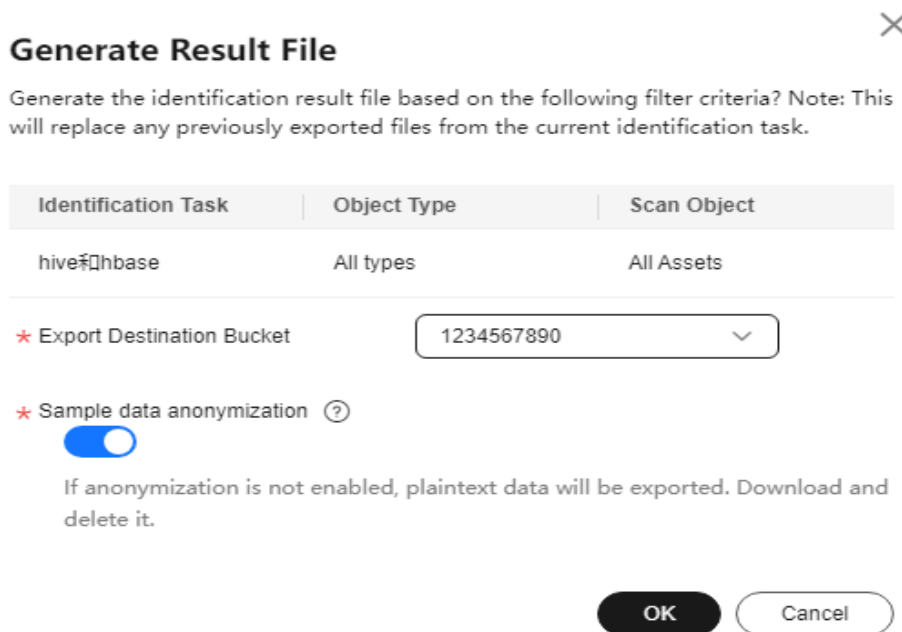
sample data masking is not enabled, the identification result sample data will be exported in plaintext. Download the data and delete it in a timely manner.

NOTE

The identification result list supports filtering.

OBS storage occupies certain storage space, which may incur fees. For details, see [OBS Billing Overview](#).

Figure 5-4 Confirming the generation of the result file



Step 7 Select **OK** to initiate the generation of the sensitive data scan report for the selected asset. A notification will appear in the upper right corner confirming the successful export of the identification result file. Subsequently, the status of the result file will be updated to **Queuing** or **Running**.

- The status of the generated result file is as follows:
 - **Running**: The result report is being generated.
 - **Queuing**: The generated task is queuing.
- If the **Download Identification Result from OBS** button is dimmed and the message "No file available. Please generate a file first." is displayed, click **Generate Result File** and download it again.

NOTE

Result files from various subtasks within the same identification task will replace one another upon generation.

Step 8 Click **Download the result file from the OBS bucket**. In the displayed dialog box, view the file path and other information. Click **OK** to go to the **OBS Buckets** page. Find the corresponding bucket based on the bucket name in the **File Path**, click the bucket name to go to the bucket, and select the identification result file, click **Download** in the **Operation** column to download the identification result file to the local PC.

Step 9 On the identification result report Excel file, identification results are displayed on the **Asset Name** and **Asset Type** sheets. The key fields include **Rule**, **Level**, **Category**, and **Classification and Grading Template**.

Figure 5-5 Example of the identification result report

SCAN_RESULT_HEADER ASSETNAME_NAME	Database	Datatable	Datatable Column	Rule	Level	Category	Categorizing and Leveling Template	Sample Data
dm_test	DMTEST	dm_test	null	N/A	N/A	N/A	N/A	
dm_test	DMTEST	dm_test	name	N/A	N/A	N/A	N/A	

----End

6 Policy Center

6.1 Policy Baseline

6.1.1 Policy Baseline Overview

The policy baseline is a comprehensive data security policy framework that incorporates data security management regulations, data classification and grading standards, cross-border data transfer management regulations, and critical and core data requirements. DSC offers pre-configured policy templates grounded in Huawei Cloud's extensive data security governance expertise, as well as support for policy creation, deletion, modification, querying, structured presentation, and filtered query functionality.


Enterprises can configure and implement unified data security protection policies to establish integrated collaborative protection measures, covering sensitive data discovery, identification, protection, supervision, and governance. This approach meets data security and personal information protection compliance requirements, simplifies data security management, and enhances the security and efficiency of enterprise data.

Application Scenarios

During the initialization phase, the enterprise administrator navigates to the DSC policy center page to establish the enterprise's data security protection policy baseline. Policies can be configured for the entire data lifecycle.

- Go to the **Asset Map** page and click an asset name. On the displayed page, click the **Protection Policy Analysis** tab. On this page, you can view the security configurations (such as encryption, backup, and audit) and their policy baseline requirements. You can click **View** or **Policy baseline** to go to the management console of the corresponding data source and configure related permissions based on policy requirements.

Figure 6-1 Protection policy analysis



rds-z [redacted] ○ Scanned Protected L4

Instance ID: 866d4dcfc0f84bc1a9ac932fcd34ed27in03

Created: Dec 19, 2024 02:05:57 GMT+08:00

×

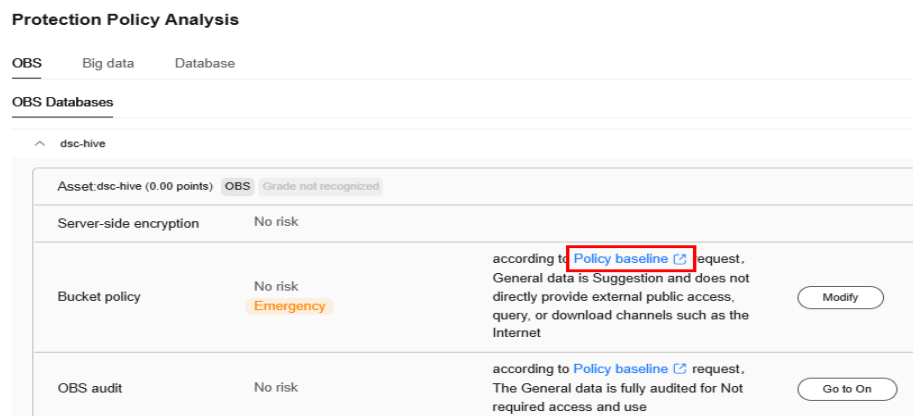
Basic Info

Type	Private IP Address
RDS	10 [redacted] 9
Port	Engine Type
5432	PostgreSQL
Version	
15	

Analysis of security protection policies
Data Egress Analysis ...

Storage encryption	To be started View	No risk
	according to Policy baseline request, L4 data enables encrypted storage for Not required to ensure the confidentiality of data storage	
Mode of operation	Modify	No risk
	according to Policy baseline request, L4 data is Required The active and standby and cluster methods are used to ensure the high availability of stored data	

- Go to the **Asset Map** page and click **Rating Details** to view the security configurations (such as encryption, backup, and audit) of all assets and the policy baseline requirements. You can click **View/Enable** or **Policy Baseline** to go to the management console of the corresponding data source and configure related permissions based on the policy requirements.

Figure 6-2 Protection policy analysis

Built-in Measures

DSC provides built-in measures for each phase of the data lifecycle.

Collection Phase

- Classification and grading: Classify and grade data, and implement corresponding security policies and assurance measures based on the data security level.
- Trace record: Trace and record the data collection process, including source, time, type, and quantity.
- Data source security authentication: Verify the security of data collection devices or systems using factors such as passwords, certificates, physical locations, and network access modes.
- Encryption: Encrypt the collected data.

Transmission Phase

- Integrity check: Verify data integrity during transmission.
- Availability assurance: Implement measures like device redundancy and line redundancy to ensure data transmission availability.
- Identity authentication and authorization: Perform identity authentication and authorization on both communication parties to ensure trustworthiness during transmission.
- Encryption: Use data encryption, secure transmission channels, or secure transmission protocols for data transmission.
- Approval and audit: Secure approval and authorization in advance, and retain data transfer logs for audit purposes.

Storage Phase

- Classification and grading: Classify and grade the statically stored data, and implement corresponding security policies and assurance measures based on the data security level.
- Storage isolation: Store data of different levels separately, and use physical or logical isolation mechanisms to control data flow between regions.

- Integrity protection: Ensure data integrity using measures such as cryptographic technologies and integrity monitoring.
- Reliability assurance: Use active/standby and cluster modes to ensure high availability of stored data.
- Security management: Perform necessary security management on data storage devices and systems, including authentication mechanisms for operation terminals, system access control, and security baselines for system configurations.
- Backup and restoration: Establish a data backup and restoration mechanism and prepare a data DR emergency plan to detect and restore data promptly if lost or damaged.
- Encryption: Use data encryption and disk encryption to ensure storage confidentiality.

Use Phase

- Identity authentication and access control: Authenticate the identity of visitors and assign data access permissions to the identities or roles of the actual visitors to prevent unauthorized data access.
- Audit: Retain operation logs during data access for real-time or post-event audit.
- Review and secondary authorization: Establish an access permission application, review, and approval mechanism; verify actual operations and application operations; and establish multi-factor authentication or secondary authorization mechanisms.
- Masking: Implement technical measures such as masking and anonymization during data access, display, processing, development, and testing to prevent sensitive information leakage.
- Blocking: Use technical measures such as database firewalls to monitor and block malicious attacks, including SQL injection and vulnerability exploitation, in real-time.
- Public network protection: Prohibit external query and download channels, such as the Internet.

Sharing Phase


- Security audit: Record logs during data sharing to audit the security of shared data.
- Blocking: Establish an emergency response mechanism or technical means to cut off data sharing in a timely manner if necessary.
- Masking: Mask data containing sensitive fields.
- Encryption: If masking is not possible due to service requirements, encrypt the data, use secure and reliable transmission protocols, or share the data in a secure and controllable environment.
- Watermarking: Add watermarks to shared data and establish a watermark source tracing mechanism to determine responsibility in case of data leakage.
- Review and supervision: Establish a data sharing approval mechanism and adopt a pre-sharing approval policy. Obtain the approval of the data owner or authorized approver. Perform routine security supervision and review of shared data.


Destruction Phase

- Review and supervision: Establish a destruction approval and supervision process. Adopt a pre-destruction approval mechanism. Obtain the approval of the data owner or authorized approver. Supervise the destruction implementation process.
- Destruction evidence retention: Record data destruction operations so administrators can view, track, confirm, and collect evidence of the destruction.
- Physical destruction: Physically destroy storage media using methods such as degaussing, magnetic media destruction, crushing, and melting.
- Copy destruction: Destroy data on storage media that stores data copies to ensure the data cannot be restored.

Procedure

Step 1 [Log in to the management console.](#)

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation tree on the left, choose **Policy Center > Policy Baseline**. The **Policy Baseline** page is displayed.

----End

6.1.2 Data Collection

Configuring Measures

Step 1 Go to the **Policy Baseline** page by referring to [Procedure](#).

Step 2 Click the **Collection** tab.

Step 3 Click **Configure Measures**. The **Configure Measure** page is displayed.

- **Built-in Measures:** DSC offers built-in measures for various data periods, leveraging Huawei Cloud's data security governance expertise. You can hover over a measure name to view its description.
- **Custom Measures:** The added custom measures are displayed in the baseline policy list.

Step 4 You can uncheck the box to deselect unnecessary measures. The deselected measures will not be displayed in the policy baseline list.

Step 5 Click **Add**. The **Add Custom Protection Measure** page is displayed.

1. Enter the **measure name** and **measure description**. Click **OK** to return to the **Configure Measure** page, where you can see the added measure.
2. Click **Edit** in the **Operation** column to modify a measure, or click **Delete** to delete an unnecessary measure.

Step 6 Click **OK** to view the configured measures in the policy baseline list.

----End

Configuring Data Protection Type

Step 1 Go to the **Policy Baseline** page by referring to [Procedure](#).

Step 2 Choose **Configure Data Protection Type**. The **Configure Data Protection Type** page is displayed.

Step 3 Built-in Data Protection Type: If a protection type is deselected, the type will not appear in the baseline policy list, and the default policy requirements of this type will be cleared. You will need to customize the policy requirements for the protection type the next time.

- **General Data Protection:** This type of protection is applied to data that has not been classified based on sensitive data identification.
- **Leveled Data Protection Type:** Leveled data protection is applicable to data that has been classified and graded. DSC includes built-in sensitive data levels from L1 to L4. If this option is deselected, it will not be displayed in the policy baseline list.

Step 4 Custom Data Protection Type: The added custom data protection types are displayed in the policy baseline list.

Select a custom level from the drop-down list box. If no custom level is available, create one by referring to [Adding a Sensitive Level](#).

Step 5 Click **OK**. In the policy baseline table, view the data protection type.

----End

Modifying Protection Requirements

Step 1 Go to the **Policy Baseline** page by referring to [Procedure](#).

Step 2 Choose **Modify Protection Requirements** to modify the protection requirements of the measure corresponding to a data protection type.

Step 3 For example, select one of the following values for **Classification and Grading** in the **General Data Protection** row:

- **Not required**
- **Suggestion**
- **Required**

Figure 6-3 Modifying Protection Requirements

Data Protection Type	Data Transmission Integrity...	Data Transmission Availab...	Transmission Party Authen...	Data Encryption	Transmission Approval and...	密保	水印
Leveled data protection	Required	Required	Not required	Not required	Not required	Not required	Not required
Hierarchical data protection	Not required	Not required	Not required	Not required	Not required	Not required	Not required
L1	Suggestion	Not required	Not required	Not required	Not required	Not required	Not required
L3	Required	Not required	Not required	Not required	Not required	Not required	Not required
L4	Not required	Not required	Not required	Not required	Not required	Not required	Not required
L2	Not required	Not required	Not required	Not required	Not required	Not required	Not required

Step 4 Click **Save Changes**. You can also click **Cancel Changes** in the upper left corner to cancel the modification and return to the previous protection requirements.

----End

6.1.3 Data Transmission

Configuring Measures

Step 1 Go to the **Policy Baseline** page by referring to [Procedure](#).

Step 2 Click the **Transmission** tab.

Step 3 Click **Configure Measures**. The **Configure Measure** page is displayed.

- **Built-in Measures:** DSC offers built-in measures for various data periods, leveraging Huawei Cloud's data security governance expertise. You can hover over a measure name to view its description.
- **Custom Measures:** The added custom measures are displayed in the baseline policy list.

Step 4 You can uncheck the box to deselect unnecessary measures. The deselected measures will not be displayed in the policy baseline list.

Step 5 Click **Add**. The **Add Custom Protection Measure** page is displayed.

1. Enter the **measure name** and **measure description**. Click **OK** to return to the **Configure Measure** page, where you can see the added measure.
2. Click **Edit** in the **Operation** column to modify a measure, or click **Delete** to delete an unnecessary measure.

Step 6 Click **OK** to view the configured measures in the policy baseline list.

----End

Configuring Data Protection Type

Step 1 Go to the **Policy Baseline** page by referring to [Procedure](#).

Step 2 Click the **Transmission** tab.

Step 3 Choose **Configure Data Protection Type**. The **Configure Data Protection Type** page is displayed.

Step 4 Built-in Data Protection Type: If a protection type is deselected, the type will not appear in the baseline policy list, and the default policy requirements of this type will be cleared. You will need to customize the policy requirements for the protection type the next time.

- **General Data Protection:** This type of protection is applied to data that has not been classified based on sensitive data identification.
- **Leveled Data Protection Type:** Leveled data protection is applicable to data that has been classified and graded. DSC includes built-in sensitive data levels from L1 to L4. If this option is deselected, it will not be displayed in the policy baseline list.

Step 5 Custom Data Protection Type: The added custom data protection types are displayed in the policy baseline list.

Select a custom level from the drop-down list box. If no custom level is available, create one by referring to [Adding a Sensitive Level](#).

Step 6 Click **OK**. In the policy baseline table, view the data protection type.

----End

Modifying protection requirements

Step 1 Go to the **Policy Baseline** page by referring to [Procedure](#).

Step 2 Click the **Transmission** tab.

Step 3 Choose **Modify Protection Requirements** to modify the protection requirements of the measure corresponding to a data protection type.

Step 4 For example, select one of the following values for **Classification and Grading** in the **General Data Protection** row:

- **Not required**
- **Suggestion**
- **Required**

Figure 6-4 Modifying protection requirements

The screenshot shows a web interface for configuring data protection requirements. At the top, there are buttons for 'Save Changes', 'Cancel Changes', 'Configure Measures', and 'Configure Data Protection Type'. Below these is a search bar with the text 'Select a property or enter a keyword'. The main area is a table with columns for different protection types and classification levels. The 'Leveled data protection' row is highlighted, and a red box highlights the 'Required' option in the 'Data Transmission Integrity...' column. Other options in this column include 'Not required', 'Suggestion', and 'Required' (highlighted in blue). The table also includes rows for 'Hierarchical data protection' and classification levels L1, L3, and L4.

Data Protection Type	Data Transmission Integrity...	Data Transmission Availabi...	Transmission Party Authen...	Data Encryption	Transmission Approval and...	DRP	sdipdg
Leveled data protection	Required	Required	Not required	Not required	Not required	Not required	Not required
<input type="checkbox"/> Hierarchical data protection	Not required						
L1	Not required	Not required	Not required	Not required	Not required	Not required	Not required
L3	Suggestion	Not required	Not required	Not required	Not required	Not required	Not required
L4	Required	Not required	Not required	Not required	Not required	Not required	Not required

Step 5 Click **Save Changes**. You can also click **Cancel Changes** in the upper left corner to cancel the modification and return to the previous protection requirements.

----End

6.1.4 Data Storage

Configuring Measures

Step 1 Go to the **Policy Baseline** page by referring to [Procedure](#).

Step 2 Click the **Storage** tab.

Step 3 Click **Configure Measures**. The **Configure Measure** page is displayed.

- **Built-in Measures:** DSC offers built-in measures for various data periods, leveraging Huawei Cloud's data security governance expertise. You can hover over a measure name to view its description.
- **Custom Measures:** The added custom measures are displayed in the baseline policy list.

Step 4 You can uncheck the box to deselect unnecessary measures. The deselected measures will not be displayed in the policy baseline list.

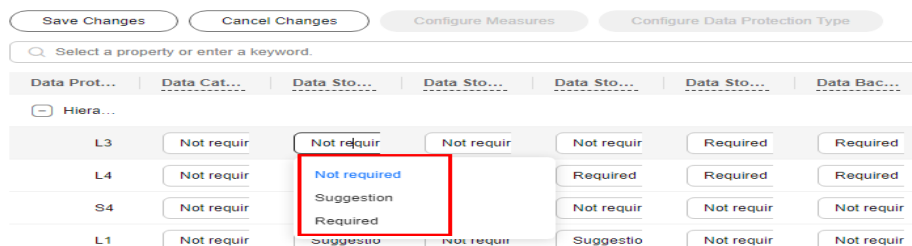
- Step 5** Click **Add**. The **Add Custom Protection Measure** page is displayed.
1. Enter the **measure name** and **measure description**. Click **OK** to return to the **Configure Measure** page, where you can see the added measure.
 2. Click **Edit** in the **Operation** column to modify a measure, or click **Delete** to delete an unnecessary measure.
- Step 6** Click **OK** to view the configured measures in the policy baseline list.
- End

Configuring Data Protection Type

- Step 1** Go to the **Policy Baseline** page by referring to [Procedure](#).
- Step 2** Click the **Storage** tab.
- Step 3** Choose **Configure Data Protection Type**. The **Configure Data Protection Type** page is displayed.
- Step 4** **Built-in Data Protection Type**: If a protection type is deselected, the type will not appear in the baseline policy list, and the default policy requirements of this type will be cleared. You will need to customize the policy requirements for the protection type the next time.
- **General Data Protection**: This type of protection is applied to data that has not been classified based on sensitive data identification.
 - **Leveled Data Protection Type**: Leveled data protection is applicable to data that has been classified and graded. DSC includes built-in sensitive data levels from L1 to L4. If this option is deselected, it will not be displayed in the policy baseline list.
- Step 5** **Custom Data Protection Type**: The added custom data protection types are displayed in the policy baseline list.
- Select a custom level from the drop-down list box. If no custom level is available, create one by referring to [Adding a Sensitive Level](#).
- Step 6** Click **OK**. In the policy baseline table, view the data protection type.
- End

Modifying protection requirements

- Step 1** Go to the **Policy Baseline** page by referring to [Procedure](#).
- Step 2** Click the **Storage** tab.
- Step 3** Choose **Modify Protection Requirements** to modify the protection requirements of the measure corresponding to a data protection type.
- Step 4** For example, select one of the following values for **Classification and Grading** in the **General Data Protection** row:
- **Not required**
 - **Suggestion**
 - **Required**

Figure 6-5 Modifying protection requirements

Step 5 Click **Save Changes**. You can also click **Cancel Changes** in the upper left corner to cancel the modification and return to the previous protection requirements.

----End

6.1.5 Data Use

Configuring Measures

Step 1 Go to the **Policy Baseline** page by referring to [Procedure](#).

Step 2 Click the **Use** tab.

Step 3 Click **Configure Measures**. The **Configure Measure** page is displayed.

- **Built-in Measures:** DSC offers built-in measures for various data periods, leveraging Huawei Cloud's data security governance expertise. You can hover over a measure name to view its description.
- **Custom Measures:** The added custom measures are displayed in the baseline policy list.

Step 4 You can uncheck the box to deselect unnecessary measures. The deselected measures will not be displayed in the policy baseline list.

Step 5 Click **Add**. The **Add Custom Protection Measure** page is displayed.

1. Enter the **measure name** and **measure description**. Click **OK** to return to the **Configure Measure** page, where you can see the added measure.
2. Click **Edit** in the **Operation** column to modify a measure, or click **Delete** to delete an unnecessary measure.

Step 6 Click **OK** to view the configured measures in the policy baseline list.

----End

Configuring Data Protection Type

Step 1 Go to the **Policy Baseline** page by referring to [Procedure](#).

Step 2 Click the **Use** tab.

Step 3 Choose **Configure Data Protection Type**. The **Configure Data Protection Type** page is displayed.

Step 4 Built-in Data Protection Type: If a protection type is deselected, the type will not appear in the baseline policy list, and the default policy requirements of this type will be cleared. You will need to customize the policy requirements for the protection type the next time.

- **General Data Protection:** This type of protection is applied to data that has not been classified based on sensitive data identification.
- **Leveled Data Protection Type:** Leveled data protection is applicable to data that has been classified and graded. DSC includes built-in sensitive data levels from L1 to L4. If this option is deselected, it will not be displayed in the policy baseline list.

Step 5 Custom Data Protection Type: The added custom data protection types are displayed in the policy baseline list.

Select a custom level from the drop-down list box. If no custom level is available, create one by referring to [Adding a Sensitive Level](#).

Step 6 Click **OK**. In the policy baseline table, view the data protection type.

----End

Modifying protection requirements

Step 1 Go to the **Policy Baseline** page by referring to [Procedure](#).

Step 2 Click the **Use** tab.

Step 3 Choose **Modify Protection Requirements** to modify the protection requirements of the measure corresponding to a data protection type.

Step 4 In the **General Data Protection** row, click the **Access Authentication and Control** drop-down list and select one of the following:

- **Not required**
- **Suggestion**
- **Required**

Step 5 Click **Save Changes**. You can also click **Cancel Changes** in the upper left corner to cancel the modification and return to the previous protection requirements.

----End

6.1.6 Data Sharing

Configuring Measures

Step 1 Go to the **Policy Baseline** page by referring to [Procedure](#).

Step 2 Click the **Sharing** tab.

Step 3 Click **Configure Measures**. The **Configure Measure** page is displayed.

- **Built-in Measures:** DSC offers built-in measures for various data periods, leveraging Huawei Cloud's data security governance expertise. You can hover over a measure name to view its description.
- **Custom Measures:** The added custom measures are displayed in the baseline policy list.

Step 4 You can uncheck the box to deselect unnecessary measures. The deselected measures will not be displayed in the policy baseline list.

- Step 5** Click **Add**. The **Add Custom Protection Measure** page is displayed.
1. Enter the **measure name** and **measure description**. Click **OK** to return to the **Configure Measure** page, where you can see the added measure.
 2. Click **Edit** in the **Operation** column to modify a measure, or click **Delete** to delete an unnecessary measure.
- Step 6** Click **OK** to view the configured measures in the policy baseline list.
- End

Configuring Data Protection Type

- Step 1** Go to the **Policy Baseline** page by referring to [Procedure](#).
- Step 2** Click the **Sharing** tab.
- Step 3** Choose **Configure Data Protection Type**. The **Configure Data Protection Type** page is displayed.
- Step 4** **Built-in Data Protection Type**: If a protection type is deselected, the type will not appear in the baseline policy list, and the default policy requirements of this type will be cleared. You will need to customize the policy requirements for the protection type the next time.
- **General Data Protection**: This type of protection is applied to data that has not been classified based on sensitive data identification.
 - **Leveled Data Protection Type**: Leveled data protection is applicable to data that has been classified and graded. DSC includes built-in sensitive data levels from L1 to L4. If this option is deselected, it will not be displayed in the policy baseline list.
- Step 5** **Custom Data Protection Type**: The added custom data protection types are displayed in the policy baseline list.
- Select a custom level from the drop-down list box. If no custom level is available, create one by referring to [Adding a Sensitive Level](#).
- Step 6** Click **OK**. In the policy baseline table, view the data protection type.
- End

Modifying protection requirements

- Step 1** Go to the **Policy Baseline** page by referring to [Procedure](#).
- Step 2** Click the **Sharing** tab.
- Step 3** Choose **Modify Protection Requirements** to modify the protection requirements of the measure corresponding to a data protection type.
- Step 4** For example, select one of the following values for **Security Auditing** in the **Leveled data protection** row:
- **Not required**
 - **Suggestion**
 - **Required**

Figure 6-6 Modifying protection requirements

Data Protection Type	Access Authentication and Control	Data Masking	Data Access Blocking
Leveled data protection	Not required ^	Not required v	Not required v
<input type="checkbox"/> Hierarchical data protection	Not required		
L1	Suggestion	Not required v	Suggestion v
L2	Required	Suggestion v	Required v
L3	Required v	Required v	Required v
L4	Required v	Required v	Required v

Step 5 Click **Save Changes**. You can also click **Cancel Changes** in the upper left corner to cancel the modification and return to the previous protection requirements.

----End

6.1.7 Data Destruction

Configuring Measures

Step 1 Go to the **Policy Baseline** page by referring to [Procedure](#).

Step 2 Choose the **Destruction** tab.

Step 3 Click **Configure Measures**. The **Configure Measure** page is displayed.

- **Built-in Measures:** DSC offers built-in measures for various data periods, leveraging Huawei Cloud's data security governance expertise. You can hover over a measure name to view its description.
- **Custom Measures:** The added custom measures are displayed in the baseline policy list.

Step 4 You can uncheck the box to deselect unnecessary measures. The deselected measures will not be displayed in the policy baseline list.

Step 5 Click **Add**. The **Add Custom Protection Measure** page is displayed.

1. Enter the **measure name** and **measure description**. Click **OK** to return to the **Configure Measure** page, where you can see the added measure.
2. Click **Edit** in the **Operation** column to modify a measure, or click **Delete** to delete an unnecessary measure.

Step 6 Click **OK** to view the configured measures in the policy baseline list.

----End

Configuring Data Protection Type

Step 1 Go to the **Policy Baseline** page by referring to [Procedure](#).

Step 2 Choose the **Destruction** tab.

- Step 3** Choose **Configure Data Protection Type**. The **Configure Data Protection Type** page is displayed.
- Step 4 Built-in Data Protection Type:** If a protection type is deselected, the type will not appear in the baseline policy list, and the default policy requirements of this type will be cleared. You will need to customize the policy requirements for the protection type the next time.
- **General Data Protection:** This type of protection is applied to data that has not been classified based on sensitive data identification.
 - **Leveled Data Protection Type:** Leveled data protection is applicable to data that has been classified and graded. DSC includes built-in sensitive data levels from L1 to L4. If this option is deselected, it will not be displayed in the policy baseline list.
- Step 5 Custom Data Protection Type:** The added custom data protection types are displayed in the policy baseline list.
- Select a custom level from the drop-down list box. If no custom level is available, create one by referring to [Adding a Sensitive Level](#).
- Step 6** Click **OK**. In the policy baseline table, view the data protection type.

----End

Modifying protection requirements

- Step 1** Go to the **Policy Baseline** page by referring to [Procedure](#).
- Step 2** Choose the **Destruction** tab.
- Step 3** Choose **Modify Protection Requirements** to modify the protection requirements of the measure corresponding to a data protection type.
- Step 4** For example, select one of the following values for **Data Destruction Oversight** in the **Leveled Data Protection** row:
- **Not required**
 - **Suggestion**
 - **Required**

Figure 6-7 Modifying protection requirements

Data Protection Type	Data Destruction Oversight	Record of Destruction	Physical Media Destruction	Test
Leveled data protection	Not required	Not required	Not required	Not required
<input type="checkbox"/> Hierarchical data protection	Not required			
L1	Suggestion	Required	Not required	Not required
L2	Required	Required	Suggestion	Not required
L3	Required	Required	Required	Not required
L4	Required	Required	Required	Not required
S4	Not required	Not required	Not required	Not required

- Step 5** Click **Save Changes**. You can also click **Cancel Changes** in the upper left corner to cancel the modification and return to the previous protection requirements.

----End

6.2 Policy Management

The administrator creates policies for database audit, watermarking, and static masking on the policy management page of the policy center, and then deploys these policies to the relevant services or instances.

Policy Types

- **Database audit:** Monitor and records database activities to ensure data integrity, security, and compliance.
- **Database watermarking:** Embed invisible identifiers into data to verify data authenticity and ownership and trace data leakage sources.
- **Static database masking:** Mask sensitive data to ensure privacy and security while retaining the data structure and statistics features.

Creating a Policy

The following part describes how to create a policy.

Creating a Database Audit Policy


Connect to the DBSS service to monitor and record database instances that do not require agent audits, ensuring data integrity, security, and compliance.

Prerequisites

DBSS has been enabled and an instance has been added.

Step 1 [Log in to the management console.](#)

Step 2 Click  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 Choose **Policy Center > Policy Management**. The **Policy Management** page is displayed.

Step 5 Click **Create Policy** in the upper left corner. The **Create Policy** page is displayed.

Step 6 Select the **Database audit** policy type.

Step 7 Click **Start configuring**. The page for configuring the database audit policy type is displayed.

Step 8 Set the parameters by referring to [Table 6-1](#).

Table 6-1 Parameters for configuring a database audit policy

Parameter	Description
Policy Name	Enter a policy name. The name can contain a maximum of 255 characters, including letters, digits, underscores (_), and hyphens (-).
Associated Instance	Select a database audit instance from the drop-down list.
Target Data Source	Select the target data source from the drop-down list. Only database instances that do not require agent audit are supported.
Display Result Set	When the function for recording result sets is enabled, the system logs the SQL result content. You can view this content in the logs. If the function is disabled, the SQL result in the log details will be empty. Recording result sets may lead to information leakage. Therefore, it is recommended not to enable this function.
Mask Privacy Data	You are advised to set masking rules to prevent sensitive data leakage.

Step 9 Click **Save and Deliver**. The policy list is displayed, showing the newly created policy.


----End

Creating a Database Watermarking Policy

Embed invisible identifiers into data to verify data authenticity and ownership and trace data leakage sources.

Step 1 [Log in to the management console](#).

Step 2 Click  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 Choose **Policy Center > Policy Management**. The **Policy Management** page is displayed.

Step 5 Click **Create Policy** in the upper left corner. The **Create Policy** page is displayed.

Step 6 Select the **Database Watermark** policy type.

Step 7 Click **Start configuring**. On the **Database Watermarking** page that is displayed, create a watermark injection or watermark extraction task. For details, see [Injecting Watermarks to Databases](#) and [Extracting Watermarks from Databases](#).


----End

Creating a Static Database Masking Policy

Mask sensitive data to ensure privacy and security while retaining the data structure and statistics features.

Step 1 [Log in to the management console](#).

Step 2 Click  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 Choose **Policy Center > Policy Management**. The **Policy Management** page is displayed.

Step 5 Click **Create Policy** in the upper left corner. The **Create Policy** page is displayed.

Step 6 Select the **Static database masking** policy type.

Step 7 Click **Start configuring**. On the displayed data masking page, create a data masking task. For details, see [Static Data Masking](#).

----End

Related Operations

- **Disabling a policy:** You can click **Disable** in the **Operation** column of a policy that is enabled and successfully delivered to disable the policy. After you click **Disable**, the policy status changes to **Disabled (Delivering)**. When the policy status changes to **Disabled (Delivered)**, the policy is disabled.

NOTE

- After an encryption policy is enabled and delivered, it cannot be disabled or deleted. You can click **Decrypt** under **Operation > More** to decrypt the corresponding encryption policy. After decryption, a suffix is appended to the encryption policy name. A new decryption policy will not be generated.
- **Deleting a policy:** Click **Delete** in the **Operation** column of a policy that is successfully delivered to delete the policy. After you click **Delete**, a message is displayed in the upper right corner of the page, indicating that the policy is successfully deleted.

6.3 Transfer Log Collection


DSC collects logs from applications (including DBSS) to assist in tracking data flow and promptly identifying exceptions and risks.


Prerequisites

- DBSS has been enabled and the database instance has been installed. For details about how to enable DBSS, see [Purchasing Database Audit](#) ..

Enabling Transfer Log Collection

Step 1 [Log in to the management console](#).


Step 2 Click  in the upper left corner of the management console and select a region or project.


Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center** .

Step 4 In the navigation pane, choose **Policy Center > Transfer Log Collection**. The **Data Transfer** page is displayed.

Step 5 [Table 6-2](#) describes the parameters in the instance list.

Table 6-2 Instance list

Parameter	Description
Instance Name/ID	Instance name of the interconnected microservice, for example, DBSS. If no instance is available, buy one.
Instance Type	Instance type, which can be DBSS .
Instance Status	Status of an instance <ul style="list-style-type: none">• Not Opened: Data transfer log collection is not enabled.• Opening: Data transfer log collection is being enabled.• Open Failed: Failed to enable data transfer log collection.• Running: Data transfer log collection is enabled successfully.• Offline: The instance status is abnormal and no heartbeat message is received.• Disabling Failed: Failed to disable data transfer log collection.• Disabling: Data transfer log collection is being disabled.• Abnormal: The instance status is abnormal.
Last Heartbeat Time	Time when DSC was connected to the instance last time.
Data Transfer Log Collection Status	Click  to enable log collection.


Step 6 Click  to enable log collection.


Step 7 Click **Batch Enable Transfer Collection** in the upper left corner to enable transfer log collection in batches.

----End

Disabling Transfer Log Collection

Step 1 [Log in to the management console.](#)

Step 2 Click  in the upper left corner of the management console and select a region or project.


Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.


Step 4 In the navigation pane, choose **Policy Center > Transfer Log Collection**. The **Data Transfer** page is displayed.

Step 5 [Table 6-3](#) describes the parameters in the instance list.

Table 6-3 Instance list

Parameter	Description
Instance Name/ID	Instance name of the interconnected microservice, for example, DBSS. If no instance is available, buy one.
Instance Type	Instance type, which can be DBSS .
Instance Status	Status of an instance <ul style="list-style-type: none">● Not Opened: Data transfer log collection is not enabled.● Opening: Data transfer log collection is being enabled.● Open Failed: Failed to enable data transfer log collection.● Running: Data transfer log collection is enabled successfully.● Offline: The instance status is abnormal and no heartbeat message is received.● Disabling Failed: Failed to disable data transfer log collection.● Disabling: Data transfer log collection is being disabled.● Abnormal: The instance status is abnormal.

Parameter	Description
Last Heartbeat Time	Time when DSC was connected to the instance last time.
Data Transfer Log Collection Status	Click  to enable log collection.

Step 6 Click  to disable log collection.

Click **Disabling Transfer Collection in Batches** in the upper left corner to disable transfer log collection in batches.

----End

7 Data Asset Protection

7.1 Data Masking

7.1.1 Data Masking Overview

DSC supports static data masking and dynamic data masking. You can configure masking rules for specified data assets to implement static masking or use the [API for dynamic data masking](#) to implement dynamic data masking, ensuring that sensitive information is not disclosed. [Masking Algorithms and Application Scenarios](#) lists the data masking algorithms supported by DSC.

Static data masking: DSC can help mask a large amount of data at one time based on the configured data masking rules. Static data masking is used when sensitive data in the production environment is delivered to the development, testing, or external environment for development and testing and data sharing and research. You can create a data masking task on the DSC console to quickly mask sensitive data in databases and big data assets.

Dynamic data masking: DSC provides dynamic data masking APIs to mask the data accessed from the external systems. Dynamic data masking applies to scenarios where data is queried from the external system, such as production applications, data exchange, O&M applications, and marketing. For details, see [API for dynamic data masking](#).

Procedure

Figure 7-1 Static data masking flowchart

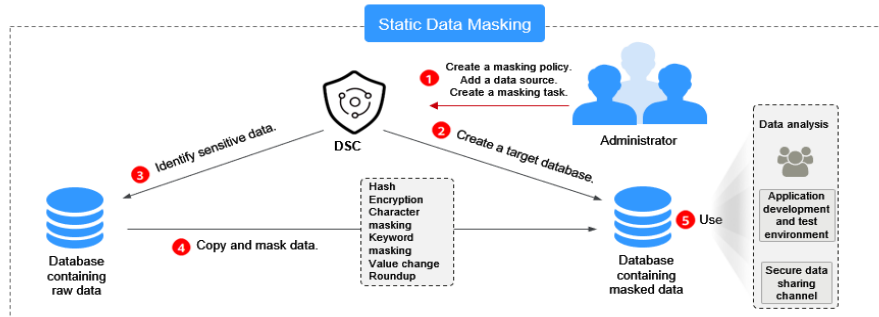
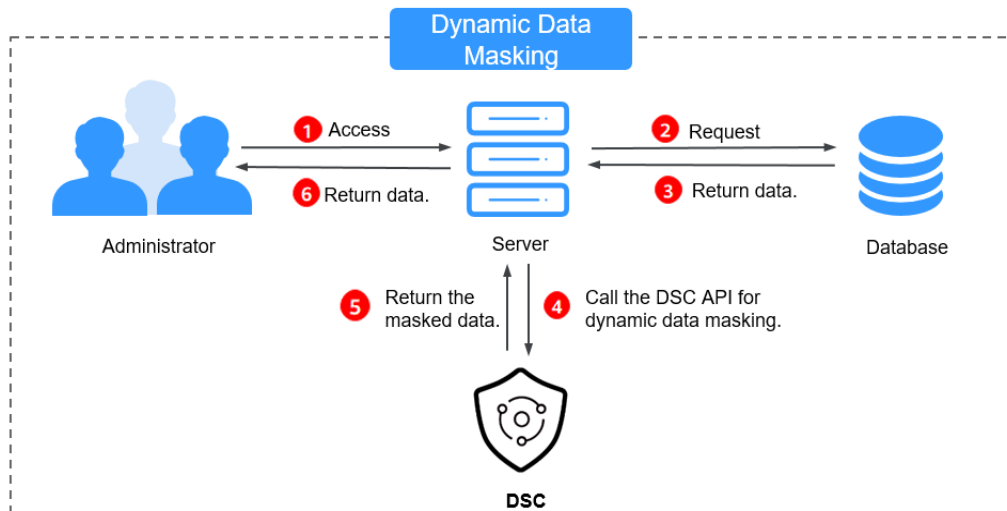


Figure 7-2 Dynamic data masking flowchart



7.1.2 Configuring and Viewing Masking Rules

Masking Algorithms and Application Scenarios

Table 7-1 Masking algorithms

Algorithm	Description	Application Scenario
Hash	<p>Use Hash functions to mask sensitive data. DSC supports SHA-256 and SHA-512.</p> <ul style="list-style-type: none">• SHA256 SHA-256, a message-digest algorithm, is used by DSC to compute a digest from a string in the database table. It takes a block of data and returns a fixed-size bit string (hash value). As the value length may exceed the maximum column width allowed in the original table, you can adjust the column width to adapt to the returned SHA-256 hash values.• SHA512 SHA-512, a message-digest algorithm, is used by DSC to compute a digest from a string in the database table. It takes a block of data and returns a fixed-size bit string (hash value). As the value length may exceed the maximum column width allowed in the original table, you can adjust the column width to adapt to the returned SHA-512 hash values.	<ul style="list-style-type: none">• Sensitive data: Keys• Application scenarios: Data storage
Encryption	<p>Use an encryption algorithm and an encryption master key to generate a specified Data Encryption Key (DEK). This DEK is then used to encrypt sensitive data, thereby achieving data masking.</p> <p>DSC supports two encryption algorithms: AES256 and SM4.</p>	<ul style="list-style-type: none">• Sensitive data:<ul style="list-style-type: none">– Personal data– Enterprise data• Application scenarios: Data storage

Algorithm	Description	Application Scenario
Character Masking	<p>Use the specified character * or random characters (including numbers, letters, and both number and letters) to cover part of the original content. The following six data masking approaches are supported:</p> <ul style="list-style-type: none">• Retain first N and last M• Retain from X to Y• Mask first N and last M• Mask from X to Y• Mask data ahead of special characters• Mask data followed by special characters <p>NOTE DSC has multiple character masking templates.</p>	<ul style="list-style-type: none">• Sensitive data:<ul style="list-style-type: none">- Personal data• Application scenarios:<ul style="list-style-type: none">- Data usage- Data sharing
Keyword Replacement	<p>Search for keywords in a specified column and replace them.</p> <p>For example, the specified characters are "Zhang San eats at home". After replacement, the characters become "Mr. Zhang eats at home". In the example, "Zhang San" is replaced with "Mr. Zhang".</p> <p>After this algorithm is executed, the value length may exceed the maximum length allowed by the database. In this case, the excess part will be truncated and inserted into the database.</p>	<ul style="list-style-type: none">• Sensitive data:<ul style="list-style-type: none">- Personal data- Enterprise data- Device data• Application scenarios:<ul style="list-style-type: none">- Data storage- Data sharing

Algorithm	Description	Application Scenario
Value Change	<p>Set a specified field to Null or left it blank for data masking.</p> <ul style="list-style-type: none">• Masking Using the Null Value Set a field of any type to NULL. If a field is set to NOT NULL, this algorithm changes the attribute of the file to NULL when copying the column.• Masking Using a Custom Value Set the target field to a default value. Specifically, a character field is left blank, a numeric field is set to 0, a date field is set to 1970, and time field is set to 00:00.	<ul style="list-style-type: none">• Sensitive data:<ul style="list-style-type: none">- Personal data- Enterprise data- Device data• Application scenarios:<ul style="list-style-type: none">- Data storage- Data sharing

Algorithm	Description	Application Scenario
Roundup	<p>Round a date or number.</p> <ul style="list-style-type: none">• Date Roundup Roundup of fields after the year field For example, 2019-05-12 will be converted to 2019-01-01, and 2019-05-12 08:08:08 will be converted to 2019-01-01 00:00:00.<p>Roundup of fields after the month field For example, 2019-05-12 will be converted to 2019-05-01, and 2019-05-12 08:08:08 will be converted to 2019-05-01 00:00:00.</p><p>Roundup of fields after the day field For example, 2019-05-12 will be converted to 2019-05-12, and 2019-05-12 08:08:08 will be converted to 2019-05-12 00:00:00.</p><p>Roundup of fields after the hour field For example, 08:08:08 will be converted to 08:00:00, and 2019-05-12 08:08:08 will be converted to 2019-05-12 08:00:00.</p><p>Roundup of fields after the minute field For example, 08:08:08 will be converted to 08:08:00, and 2019-05-12 08:08:08 will be converted to 2019-05-12 08:08:00.</p><p>Roundup of fields after the second field For example, 08:08:08.123 will be converted to 08:08:08.000, and 1575612731312 will be converted to 1575612731000.</p>• Number roundup Rounds a specified number.	<ul style="list-style-type: none">• Sensitive data: General sensitive data• Application scenarios:<ul style="list-style-type: none">- Data storage- Data usage

Configuring and Viewing Masking Rules

You can configure masking rules for specified data types to implement static masking of sensitive data. This section describes the data types supported by each masking algorithm and how to add and test masking algorithms.

Hash


This method is used to replace a field of the string type with a hash value. In a relational database, if the field length is less than the hash length, the length of the field in the destination database is set to be the same as the hash value

length to ensure that the hash value is completely written to the destination database. By default, two hash algorithms, SHA-256 and SHA-512, are configured for DSC.

Hash algorithms are built-in and do not need to be configured. If you want to test the masking effect, perform the following steps:

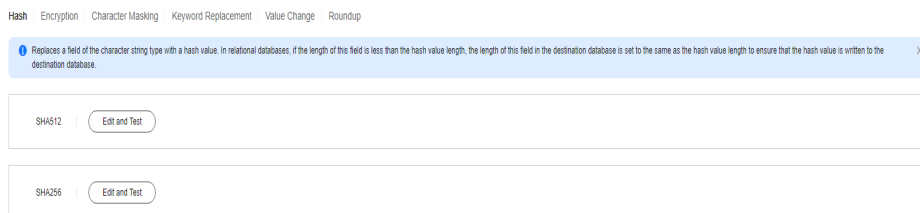
Step 1 [Log in to the management console.](#)

Step 2 Click  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 In the navigation pane, choose **Data Asset Protection > Static Data Masking**. On the page displayed, click the **Masking Rule** tab.

Figure 7-3 Hash masking



Step 5 In the column where the SHA-256 or SHA-512 algorithm is, click **Edit and Test**.

Step 6 On the **Edit and Test** page, set **Masking Algorithm** to **Hash**, enter **Raw Data**, and click **Test**. The masked data is displayed in the **Masking Result** text box.

Figure 7-4 Hash method

Edit and Test

Masking Algorithm Hash SHA512

Test

Raw Data Test

Masking Result

```
a283e0f722769899e7774ca32d5e57f1ee0e712d6faadb6ae8
da2c95fe9a1486a5ebb6cb1865e72fe11ef85d3ca5d812e298
19355b1bfa05b4e6720ac7f1f105b
```

Cancel


----End

Encryption

This method masks data using encryption algorithms and a master key.

Step 1 [Log in to the management console.](#)

Step 2 Click  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 In the navigation pane, choose **Data Asset Protection > Static Data Masking**. On the page displayed, click the **Masking Rule** tab.

Figure 7-5 Hash masking

Hash Encryption Character Masking Keyword Replacement Value Change Roundup

! Replaces a field of the character string type with a hash value. In relational databases, if the length of this field is less than the hash value length, the length of this field in the destination database is set to the same as the hash value length to ensure that the hash value is written to the destination database. X

SHA512 Edit and Test

SHA256 Edit and Test

Step 5 Click the **Encryption** tab.

- **Master Key Algorithm:** Select an encryption algorithm from the drop-down list box. Two encryption algorithms are available: **AES256** and **SM4**.

Table 7-2 Master key algorithms

Key Type	Algorithm Type	Key Specifications	Description	Usage
Symmetric key	AES	AES_256	AES symmetric key	Encrypts and decrypts a small amount of data or data keys.
Symmetric key	SM4	SM4	SM4 symmetric key	Encrypts and decrypts a small amount of data or data keys.

- For KMS encryption, the KMS key can be either selected from the drop-down list or entered:
 - **Select from Keys:** Select an existing master key from the drop-down list. If no master key is available, click **Create KMS Key** to create one. For details about how to create a KMS key, see [Creating a Key](#).

 **NOTE**


By default, the master key **csmd/default** is used for encryption.

- **Enter a KMS key ID:** Enter the ID of the KMS key in the current region.
- Select the **Data Key Length** from the drop-down list box. The options are 128, 192, and 256.

Step 6 After the configuration is complete, click **Generate Encryption Configuration**.

If you want to delete a configured encryption configuration, click **Delete** in the **Operation** column.

 **NOTE**

Click  to enable the rotation policy. After rotation, the current encryption configuration is updated to improve security.

----End


Character Masking

This method uses the specified character * or a random character to cover part of the content.

There are six masking methods available, including retaining first *N* and last *M*, retaining from *X* to *Y*, masking first *N* and last *M*, masking from *X* to *Y*, masking data ahead of special characters, and masking data followed by special characters.

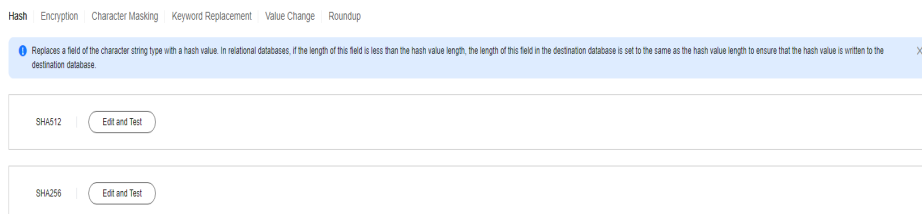
Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation pane, choose **Data Asset Protection > Static Data Masking**. On the page displayed, click the **Masking Rule** tab.

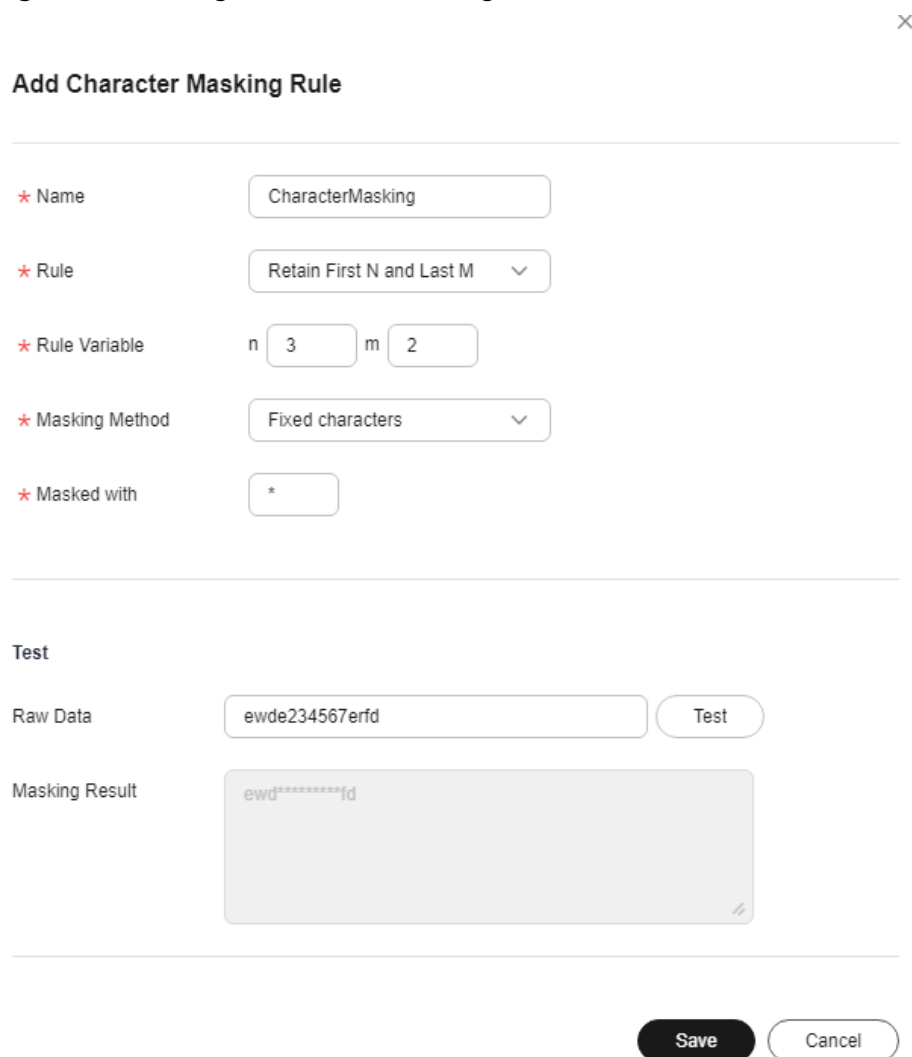
Figure 7-6 Hash masking



Step 5 Click the **Character Masking** tab.

Step 6 Click **Add** to configure a character masking rule.

Figure 7-7 Adding a character masking rule



Step 7 Configure the parameters by referring to [Table 7-3](#). Enter the raw data and click **Test**. The masking result will be displayed in the **Masking Result** text box.

Table 7-3 Character masking parameters

Parameter	Description
Name	Enter a character masking rule name. The name can contain only letters, digits, underscores (_), and hyphens (-), and cannot exceed 255 characters.
Rule	The following rules are available: <ul style="list-style-type: none">● Retain first <i>N</i> and last <i>M</i>● Retain from <i>X</i> to <i>Y</i>● Mask first <i>N</i> and last <i>M</i>● Mask from <i>X</i> to <i>Y</i>● Mask data ahead of special characters● Mask data followed by special characters
Rule Variable	Enter the value of the corresponding rule. For example, if you select Retain from <i>x</i> to <i>y</i> , set <i>x</i> to 3 , and set <i>y</i> to 6 , meaning the third to sixth characters are retained.
Masking Method	The optional masking methods are as follows: <ul style="list-style-type: none">● Fixed characters: Replace specified characters with fixed characters.● Random characters: Replace specified characters with random characters.
Masked with	This parameter is displayed when Masking Method is set to Fixed Characters . You need to enter the specified characters used to mask data.
Random Character Type	The random characters include: <ul style="list-style-type: none">● Random letters● Random digits● Combination of random digits and letters

Step 8 Verify the testing result and click **Save**.

 **NOTE**


- Multiple character masking rules have been preset in DSC. Built-in masking rules cannot be deleted. To delete a custom masking rule, click **Delete** in the **Operation** column of the target rule.
- All rules can be edited. To edit a rule, locate the row containing the rule and click **Edit** in the **Operation** column.


----End

Keyword Replacement

This method masks data by replacing matched keywords with custom strings. For example, if the original characters are **abcdefgbcdefgkjkoij**, the keyword is **bcde**, and the replacement string is **12**, the masking result is **a12fg12fgkjkoij**.

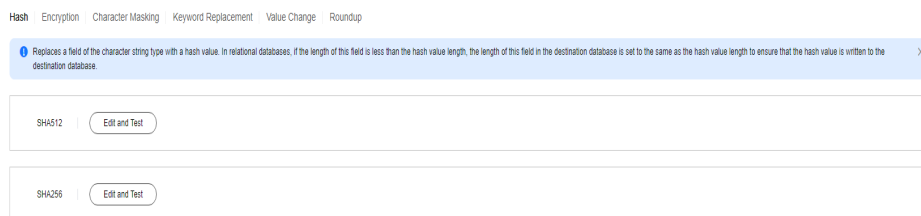
Step 1 Log in to the management console.

Step 2 Click  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 In the navigation pane, choose **Data Asset Protection > Static Data Masking**. On the page displayed, click the **Masking Rule** tab.

Figure 7-8 Hash masking



Step 5 Click the **Keyword Replacement** tab.

Step 6 Click **Add** in the upper left corner. The **Add Keyword** page is displayed.

Step 7 Set the keyword and the replacement string.

Then, the keywords matched in raw characters will be replaced with the replacement string.

Figure 7-9 Adding a keyword

Add Keyword

* Keyword

* Replaced with

Test

Raw Data

Masking Result

Step 8 Enter the raw data and click **Test**. The masking result will be displayed in the **Masking Result** text box.

Step 9 Verify the testing result and click **Save**.

- In the **Operation** column of the keyword replacement rule list, click **Edit and Test** to modify a masking rule.
- In the **Operation** column of the keyword replacement rule list, click **Delete** to delete a masking rule.

----End

Value Change


The following algorithms have been built in:

- **Masking Using the Null Value:** Set fields of any type to **NULL**. For a field whose attribute is set to **NOT NULL**, the algorithm changes the attribute to **NULL** during copy.
- **Masking Using the Empty Value:** Set the specified field to an empty value. Specifically, a character field is left blank, a numeric field is set to **0**, a date field is set to **1970**, and time field is set to **00:00**.

It is a built-in masking rule of DSC and does not need to be configured. To view the masking rule, perform the following steps:

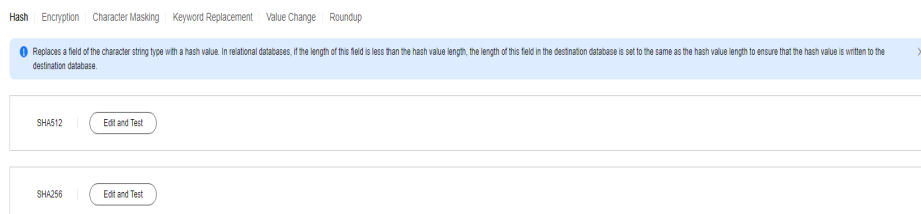
Step 1 [Log in to the management console.](#)

Step 2 Click  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 In the navigation pane, choose **Data Asset Protection > Static Data Masking**. On the page displayed, click the **Masking Rule** tab.

Figure 7-10 Hash masking




Step 5 Click the **Value Change** tab.

----End

Roundup

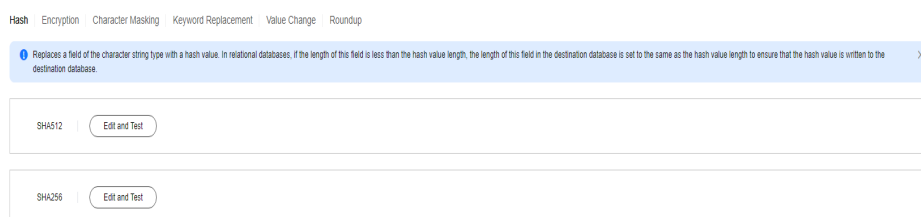
Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation pane, choose **Data Asset Protection > Static Data Masking**. On the page displayed, click the **Masking Rule** tab.

Figure 7-11 Hash masking



Step 5 Click **Round**.

There are two built-in data masking algorithms available:

- **Date Roundup:** Used for time-related fields such as **timestamp**, **time**, **data**, and **datetime** in RDS.
- **Number Roundup:** Used for value types fields such as **double**, **float**, **int**, and **long**. After data masking, the original field type does not change.

Step 6 Click **Edit and Test**. On the **Edit and Test** page, select **Roundup** for **Masking Algorithm** and set the **Roundup result**.

Masking Result: Rounds a given value downwards to a multiple value closest to the raw data. For example, if the given value is **5** and the raw data is **14**, the multiple of **5** that is closest to **14** is **10**. That is, the masking result is **10**.

Figure 7-12 Number roundup

Edit and Test

Masking Algorithm Roundup Number Roundup

★ Roundup Result 5

Test

Raw Data 14 Test

Masking Result

10

Save Cancel

Step 7 Enter the raw data and click **Test**. The masking result will be displayed in the **Masking Result** text box.

Step 8 Verify the testing result and click **Save**.

----End

Simulation Masking

Once sensitive data is identified, it is replaced with simulated data. At present, this functionality is limited to OBS masking tasks.

Table 7-4 Supported simulation masking types

No.	Sensitive Data Rule	Simulation Masking Type
1	ID card No. (Chinese mainland)	ID card number
2	Birthday	Random date (specified range)
3	Date	Random date (specified range)
4	Mobile number (Chinese mainland)	Mobile number

No.	Sensitive Data Rule	Simulation Masking Type
5	Email address	Email address
6	Postal code (Chinese mainland)	Postal code
7	Address (Chinese mainland)	Address
8	Exact address (China)	Address
9	International mobile equipment identity (IMEI)	IMEI
10	IPv4 address	IPv4 address
11	IPv6 address	IPv6 address
12	Bank account number	Bank account number
13	Person name (Simplified Chinese)	Person name
14	Car license plate number (Chinese mainland)	Car license plate number
15	Passport No. (Chinese mainland)	Passport No.

7.1.3 Static Data Masking

7.1.3.1 Creating a Static Data Masking Task

DSC supports masking of database, big data, and OBS data. For details about the supported data types, see [Constraints](#). This section describes how to create masking tasks of different data types.

Prerequisites

- Access to cloud assets has been authorized. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- An OBS bucket or database/big data asset has been added and authorized. For details, see the operations of adding and authorizing assets in [Asset Center](#).
- Sensitive data has been identified by referring to [Creating an Identification Task](#).
- Related MRS_Hive permission needs to be configured for MRS masking. For details, see [Modifying Hive User Rights](#).

Constraints

- Database masking:
The following data sources are supported: **SQLServer, MySQL, TDSQL, PostgreSQL, Dameng, Kingbase, GaussDB, Oracle, and DWS**.

- Big data masking:
The value can be **Elasticsearch**, **MRS_HIVE**, **Hive**, **HBase**, or **DLI**.
- OBS bucket masking:
 - DSC does not support the parallel file system of OBS.
 - DSC supports files such as .txt, .log, .xml, .ini, .sql, .inf, .java and .json or files whose mime type starts with text.


Creating a Static Data Masking Task

You can create a static data masking task on the DSC console and mask data sources based on the selected masking rule. For details about how to view and test masking rules, see [Configuring and Viewing Masking Rules](#).

Creating and Running a Database Masking Task

Step 1 [Log in to the management console](#).

Step 2 Click  in the upper left corner and select a region or project.

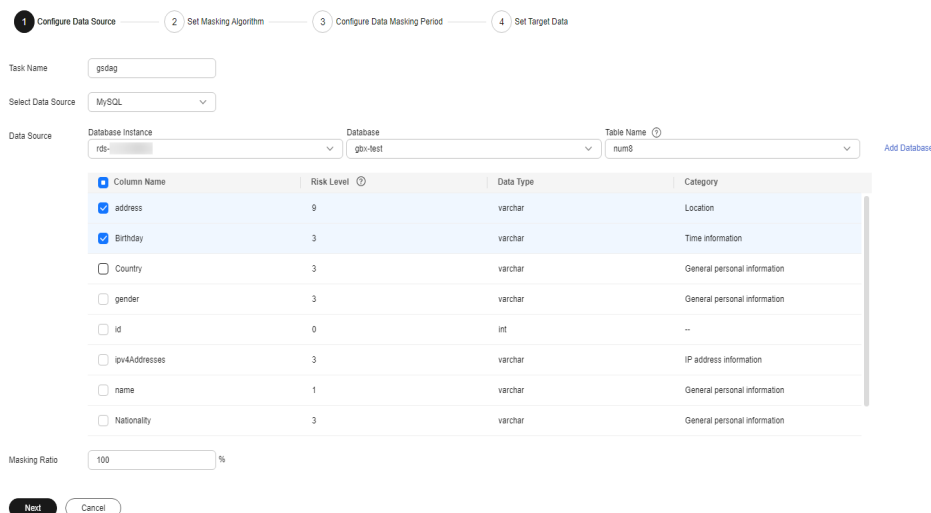
Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the left navigation pane, choose **Data Asset Protection > Static Data Masking**. The **Static Data Masking** page is displayed.

Step 5 On the **Databases** tab page, set **Mask Sensitive Database Data** to .

Step 6 Click **Create Task**. On the displayed **Configure Data Source** page, configure parameters according to [Table 7-5](#).

Figure 7-13 Configuring a database data masking task

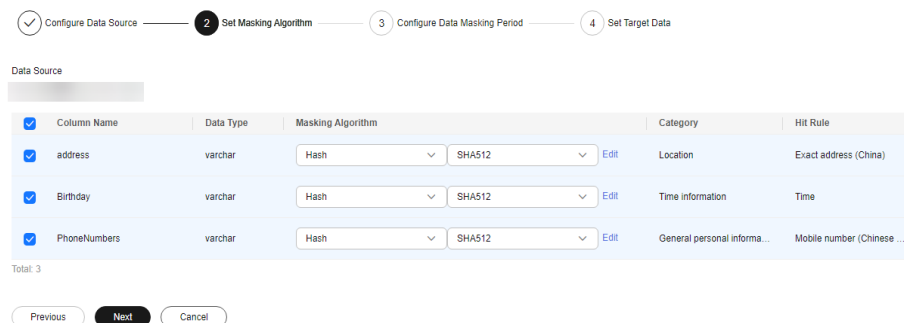


Column Name	Risk Level	Data Type	Category
<input checked="" type="checkbox"/> address	9	varchar	Location
<input checked="" type="checkbox"/> Birthday	3	varchar	Time information
<input type="checkbox"/> Country	3	varchar	General personal information
<input type="checkbox"/> gender	3	varchar	General personal information
<input type="checkbox"/> id	0	int	--
<input type="checkbox"/> ipv4Addresses	3	varchar	IP address information
<input type="checkbox"/> name	1	varchar	General personal information
<input type="checkbox"/> Nationality	3	varchar	General personal information

Table 7-5 Parameter description

Parameter	Description
Task Name	You can customize the name of a data masking task. The task name must meet the following requirements: <ul style="list-style-type: none"> Contain 1 to 255 characters. Consist of letters, digits, underscores (_), and hyphens (-).
Select Data Source	Select a data source. Available options are SQLServer, MySQL, TDSQL, PostgreSQL, Dameng, Kingbase, OpenGauss, Oracle, and DWS .
Data Source	Database Instance: Select the database instance to be masked.
NOTE If no database instance is available, click Add Database to add or authorize a database. For details, see Adding Self-Built Database Instances and Authorizing Access to a Database Asset .	Database: Select the name of the database to be masked.
	Schema: This parameter is available only when SQLServer, KingBase, OpenGauss, PostgreSQL, or DWS is selected for Data Source .
	Table name: Select the name of the database table where the data you want to mask is located.
Column Information	The column information includes Column Name, Risk Level, Data Type, and Category .
Masking Ratio	Specify the database's masking ratio. For instance, setting it to 80% will mask the initial 800 rows in a database with 1000 rows.

Step 7 Click **Next**. The **Set Masking Algorithm** page is displayed.

Figure 7-14 Configuring the data masking algorithm

1. Select the data columns you want to mask.
2. Select a proper masking algorithm based on the **data type**. For details about data masking algorithms, see [Configuring and Viewing Masking Rules](#).

 NOTE

If the decryption masking algorithm is selected for encrypted data, the encrypted data will be decrypted then masked.

If the masking algorithm is selected for unencrypted data, data remains unchanged after masking.

3. Click **Edit**. On the editing test page displayed, test the masking algorithm you selected. Enter the replacement string and raw data, click **Test**, and view the masking result. For details about masking rules, see [Configuring and Viewing Masking Rules](#).

Step 8 Click **Next**. On the **Configure Data Masking Period** page that is displayed, configure the masking period.

Click  next to **Incremental Masking** to enable incremental masking.

Incremental Key Value: Select an incremental key value from the drop-down list box, for example, **id**.

 NOTE

- After incremental masking is enabled, the data added after the last masking task is completed is masked. Select a field that increases with time in the source data as the incremental column, such as the creation time and auto-increment ID.
- Currently, incremental masking supports the following database field types: **int**, **bigint**, **integer**, **date**, and **datetime**.

Select and set the execution period of a masking task.

- **Manual:** Manually enable a masking task and execute it based on masking rules.
- **Hourly:** Execute a data masking task every several hours.
Example: If the masking task needs to be executed every two hours, set this parameter to **02:00**.
- **Daily:** Execute a data masking task at a specified time every day.
Example: If the masking task needs to be executed at 12:00 every day, set this parameter to **12:00:00**.
- **Weekly:** Execute a data masking task at a specified time every week.
Example: If the masking task needs to be executed at 12:00 every Monday, set this parameter to 12:00:00 every Monday.
- **Monthly:** Execute a data masking task at a specified time on a specified day every month.
Example: If the masking task needs to be executed at 12:00 on the 12th day of each month, set this parameter to 12:00:00 12th day of every month.

 NOTE

If you want to execute a data masking task on the 31st day of each month, the system automatically executes the task on the last day of every month.

Step 9 Click **Next**. The **Set Target Data** page is displayed.

Figure 7-15 Configuring a target data type

✓ Configure Data Source ✓ Set Masking Algorithm ✓ Configure Data Masking Period 4 Set Target Data

Database Instance: Database: Table Name:

Data Source Column	Risk Level	Target Column
address	9	<input type="text" value="address"/>
Birthday	3	<input type="text" value="Birthday"/>
PhoneNumbers	6	<input type="text" value="PhoneNumbers"/>

1. Select a database instance, database name, schema (if any), and enter the table name.

If the entered data table name already exists, the system updates the data table in the target database.

If the entered data table name does not exist, the system automatically creates a data table with the same name in the target database.

CAUTION

- Do not fill in an existing service data table. Otherwise, services may be affected.
- Do not select an original data table as the target data table. Otherwise, the original data may be overwritten.

2. Set the column name of the target data type.

By default, the system generates a name that is the same as the name of the data source column. You can retain the default name or change it as required.

Step 10 Click **Finish**.

Step 11 Click the **Database** tab and turn on the button under **Enable/Disable** to enable the task. In the **Operation** column of the target masking task, click **Execute**.


The data masking task is executed as configured.

----End

Creating and Running an Elasticsearch Data Masking Task

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the left navigation pane, choose **Data Asset Protection > Data Masking** and click the **Elasticsearch** tab. The Elasticsearch masking page is displayed.

Step 5 Click **Authorizing Access to a Database Asset** and set **Elasticsearch** to  to enable Elasticsearch masking.

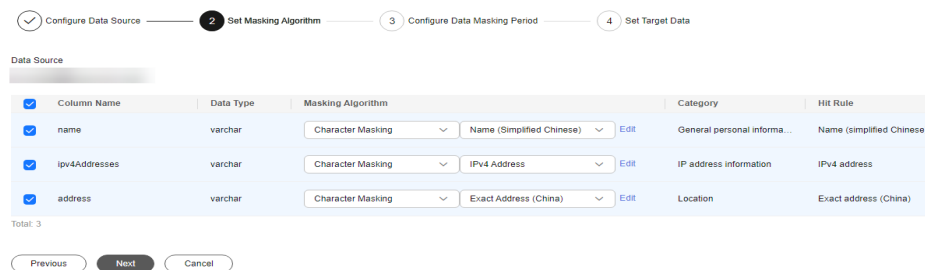
Step 6 Click **Create Task**. On the displayed **Configure Data Source** page, configure parameters according to **Table 7-6**.

Table 7-6 Parameter description

Parameter	Description
Task Name	You can customize the name of a data masking task. The task name must meet the following requirements: <ul style="list-style-type: none"> Contain 1 to 255 characters. Consist of letters, digits, underscores (_), and hyphens (-).
Select Data Source	Select a data source. Currently, the value can only be Elasticsearch .
Data Source	Elasticsearch: Select the Elasticsearch instance where the data to be masked is.
NOTE If no Elasticsearch instance is available, click Add to add Elasticsearch indexes. For details, see Authorizing Access to a Big Data Asset .	Index: Select the index where the data to be masked is.
	Type: Select the type of the data to be masked.
Field Information	The field information includes Field Name , Risk Level , Data Type , and Category .

Step 7 Click **Next**. The **Set Masking Algorithm** page is displayed.

Figure 7-16 Configuring a masking algorithm



1. Select the data columns you want to mask.
2. Select a data masking algorithm. For details about data masking algorithms, see [Configuring and Viewing Masking Rules](#).

Step 8 Click **Next** to switch to the **Configure Data Masking Period** page and configure the data masking period.

Select and set the execution period of a masking task.

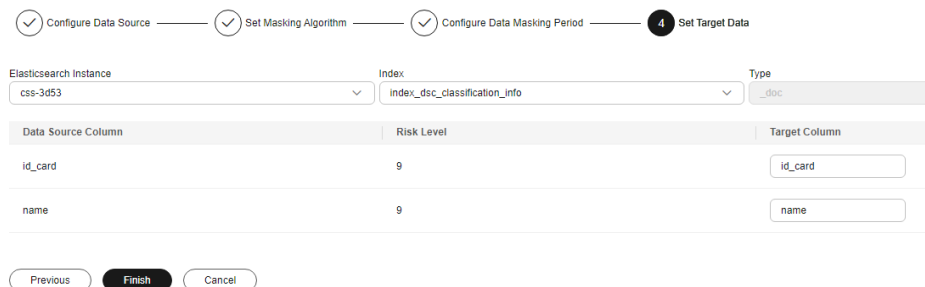
- **Manual:** Manually enable a masking task and execute it based on masking rules.
- **Hourly:** Execute a data masking task every several hours.
Example: If the masking task needs to be executed every two hours, set this parameter to **02:00**.
- **Daily:** Execute a data masking task at a specified time every day.
Example: If the masking task needs to be executed at 12:00 every day, set this parameter to **12:00:00**.
- **Weekly:** Execute a data masking task at a specified time every week.
Example: If the masking task needs to be executed at 12:00 every Monday, set this parameter to 12:00:00 every Monday.
- **Monthly:** Execute a data masking task at a specified time on a specified day every month.
Example: If the masking task needs to be executed at 12:00 on the 12th day of each month, set this parameter to 12:00:00 12th day of every month.

 **NOTE**

If you want to execute a data masking task on the 31st day of each month, the system automatically executes the task on the last day of every month.

Step 9 Click **Next**. The **Set Target Data** page is displayed.

Figure 7-17 Setting target data



Data Source Column	Risk Level	Target Column
id_card	9	id_card
name	9	name

1. Select an Elasticsearch instance and index, and set **Type**.

If the type you entered already exists, the system updates the data of the type in the target data source.

If the type you entered does not exist, the system automatically creates a type with the same name in the target data source.

 **CAUTION**

If you want to use an existing type, do not set **Type**. Otherwise, services may be affected.

2. Set the column name of the target data type.


By default, the system generates the same name as the data source column. You can retain the default name or change it as needed.

Step 10 Click **Finish**.

Step 11 Click the **Elasticsearch** tab. Locate the row containing the target data masking task and click **Execute** in the **Operation** column.

Step 12 The system starts to execute the data masking task as configured.

 **NOTE**


If  is displayed in the **Enable/Disable** column, the task is disabled, and you are not allowed to click **Execute**.

----End

Creating and Running an MRS Data Masking Task

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the left navigation pane, choose **Data asset protection > Static Data Masking** and click the **MRS** tab. The MRS masking page is displayed.

Step 5 Click  and set **Mask Sensitive MRS Data** to  to enable MRS masking.

Step 6 Click **Create Task**. On the displayed **Configure Data Source** page, configure parameters according to [Table 7-7](#).

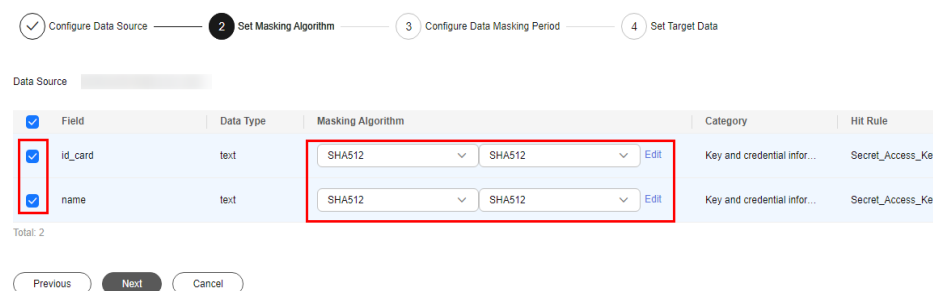
Table 7-7 Parameter description

Parameter	Description
Task Name	You can customize the name of a data masking task. The task name must meet the following requirements: <ul style="list-style-type: none"> Contain 1 to 255 characters. Consist of letters, digits, underscores (_), and hyphens (-).
Select Data Source	Select a data source. Only MRS_HIVE is available.
Data Source	Database Instance: Select the database instance where the data you want to mask is located.
NOTE If no Hive database instance is available, click Authorize Database to add a big data instance asset. For details, see Authorizing Access to a Big Data Asset .	Database: Select the name of the database where the data you want to mask is located.
	Table Name: Select the name of the database table where the data you want to mask is located.

Parameter	Description
	Select a column name to copy the data in the column to the target database.
Column Information	The column information includes Column Name , Risk Level , Data Type , and Category .

Step 7 Click **Next**. The **Set Masking Algorithm** page is displayed.

Figure 7-18 Setting a masking algorithm



1. Select the data columns you want to mask.
2. Select a data masking algorithm. For details about data masking algorithms, see [Configuring and Viewing Masking Rules](#).

Step 8 Click **Next** to switch to the **Configure Data Masking Period** page and configure the data masking period.

Select and set the execution period of a masking task.

- **Manual:** Manually enable a masking task and execute it based on masking rules.
- **Hourly:** Execute a data masking task every several hours.
Example: If the masking task needs to be executed every two hours, set this parameter to **02:00**.
- **Daily:** Execute a data masking task at a specified time every day.
Example: If the masking task needs to be executed at 12:00 every day, set this parameter to **12:00:00**.
- **Weekly:** Execute a data masking task at a specified time every week.
Example: If the masking task needs to be executed at 12:00 every Monday, set this parameter to **12:00:00 every Monday**.
- **Monthly:** Execute a data masking task at a specified time on a specified day every month.
Example: If the masking task needs to be executed at 12:00 on the 12th day of each month, set this parameter to **12:00:00 12th day of every month**.

NOTE

If you want to execute a data masking task on the 31st day of each month, the system automatically executes the task on the last day of every month.

Step 9 Click **Next**. The **Set Target Data** page is displayed.

Figure 7-19 Setting target data

Data Source Column	Risk Level	Target Column
address	9	address
Birthday	3	Birthday

1. Select a database instance and database name, and enter the database table name.

If the entered data table name already exists, the system updates the data table in the target database.

If the entered data table name does not exist, the system automatically creates a data table with the same name in the target database.

CAUTION

Do not fill in an existing service data table. Otherwise, services may be affected.

2. Set the column name of the target data type.

By default, the system generates a name that is the same as the name of the data source column. You can retain the default name or change it as required.

Step 10 Click **Finish**.

Step 11 Click the **MRS** tab. Locate the row containing the target data masking task and click **Execute** in the **Operation** column.


Step 12 The data masking task is executed as configured.

----End

Creating and Running a Hive Masking Task

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the left navigation pane, choose **Data Asset Protection** > **Static Data Masking** and click the **Hive** tab. The Hive masking page is displayed.

Step 5 Click  and set **Mask Sensitive Hive Data** to  to enable Hive masking.

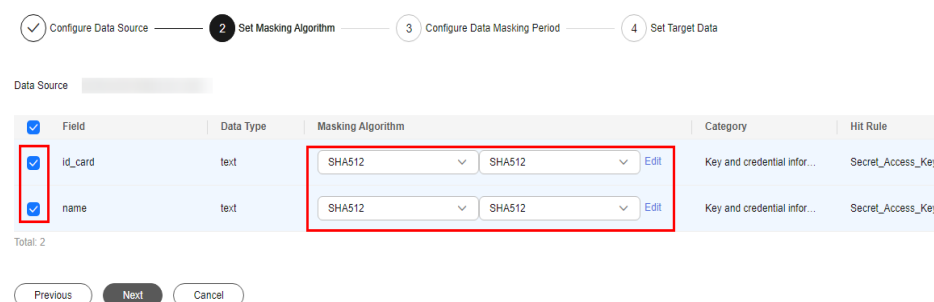
Step 6 Click **Create Task**. On the displayed **Configure Data Source** page, configure parameters according to [Table 7-8](#).

Table 7-8 Parameter description

Parameter	Description
Task Name	You can customize the name of a data masking task. The task name must meet the following requirements: <ul style="list-style-type: none"> Contain 1 to 255 characters. Consist of letters, digits, underscores (_), and hyphens (-).
Select Data Source	Select a data source. Only Hive is supported.
Data Source	Database Instance: Select the database instance where the data you want to mask is located.
NOTE If no Hive database instance is available, click Add Database to add a big data asset. For details, see Authorizing Access to a Big Data Asset .	Database: Select the name of the database where the data you want to mask is located.
	Table name: Select the name of the database table where the data you want to mask is located. If you select the check box, data in this column is copied to the Data Type column.
Column Information	The column information includes Column Name , Risk Level , Data Type , and Category .

Step 7 Click **Next**. The **Set Masking Algorithm** page is displayed.

Figure 7-20 Setting a masking algorithm



1. Select the data columns you want to mask.
2. Select a data masking algorithm. For details about data masking algorithms, see [Configuring and Viewing Masking Rules](#).

Step 8 Click **Next** to switch to the **Configure Data Masking Period** page and configure the data masking period.

Select and set the execution period of a masking task.

- **Manual:** Manually enable a masking task and execute it based on masking rules.
- **Hourly:** Execute a data masking task every several hours.
Example: If the masking task needs to be executed every two hours, set this parameter to **02:00**.
- **Daily:** Execute a data masking task at a specified time every day.
Example: If the masking task needs to be executed at 12:00 every day, set this parameter to **12:00:00**.
- **Weekly:** Execute a data masking task at a specified time every week.
Example: If the masking task needs to be executed at 12:00 every Monday, set this parameter to 12:00:00 every Monday.
- **Monthly:** Execute a data masking task at a specified time on a specified day every month.
Example: If the masking task needs to be executed at 12:00 on the 12th day of each month, set this parameter to 12:00:00 12th day of every month.

NOTE

If you want to execute a data masking task on the 31st day of each month, the system automatically executes the task on the last day of every month.

Step 9 Click **Next**. The **Set Target Data** page is displayed.

Figure 7-21 Setting target data

Progress: Configure Data Source — Set Masking Algorithm — Configure Data Masking Period — **4** Set Target Data

Database Instance	Database	Table Name
<input type="text"/>	<input type="text"/>	<input type="text" value="test"/>

Data Source Column	Risk Level	Target Column
name	1	<input type="text" value="name"/>
address	9	<input type="text" value="address"/>

1. Select a database instance and database name, and enter the database table name.

If the entered data table name already exists, the system updates the data table in the target database.

If the entered data table name does not exist, the system automatically creates a data table with the same name in the target database.

CAUTION

Do not fill in an existing service data table. Otherwise, services may be affected.

2. Set the column name of the target data type.

By default, the system generates a name that is the same as the name of the data source column. You can retain the default name or change it as required.

Step 10 Click **Finish**.

Step 11 On the **Hive** page. In the **Operation** column of the target anonymization task, click **Execute**.


Step 12 The data masking task is executed as configured.

----End

Creating and Running an HBase Masking Task

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation pane, choose **Data Asset Protection > Static Data Masking** and click the **HBase** tab. The HBase masking page is displayed.

Step 5 Click  and set **Mask Sensitive HBase Data** to  to enable HBase masking.

Step 6 Click **Create Task**. On the displayed **Configure Data Source** page, configure parameters according to [Table 7-9](#).

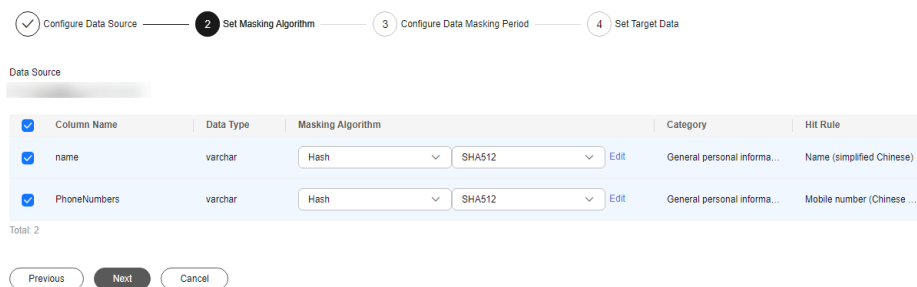
Table 7-9 Parameter description

Parameter	Description
Task Name	You can customize the name of a data masking task. The task name must meet the following requirements: <ul style="list-style-type: none"> Contain 1 to 255 characters. Consist of letters, digits, underscores (_), and hyphens (-).
Select Data Source	Select a data source. Only HBase is supported.
Data Source	Database Instance: Select the database instance where the data you want to mask is located.
NOTE If no database instance is available, click Add Database to add a big data asset. For details, see Authorizing Access to a Big Data Asset .	Namespace: Select the namespace where the data to be masked is located.
	Table name: Select the name of the database table where the data you want to mask is located.
	Column Family: Select the column where the data to be masked is located.
	If you select a column, data in this column will be copied to the target database.

Parameter	Description
Column Information	The column information includes Column Name , Risk Level , Data Type , and Category .

Step 7 Click **Next**. The **Set Masking Algorithm** page is displayed.

Figure 7-22 Setting a masking algorithm



1. Select the data columns you want to mask.
2. Select a data masking algorithm. For details about data masking algorithms, see [Configuring and Viewing Masking Rules](#).

Step 8 Click **Next**. On the **Configure Data Masking Period** page that is displayed, configure the masking period.

Select and set the execution period of a masking task.

- **Manual:** Manually enable a masking task and execute it based on masking rules.
- **Hourly:** Execute a data masking task every several hours.
Example: If the masking task needs to be executed every two hours, set this parameter to **02:00**.
- **Daily:** Execute a data masking task at a specified time every day.
Example: If the masking task needs to be executed at 12:00 every day, set this parameter to **12:00:00**.
- **Weekly:** Execute a data masking task at a specified time every week.
Example: If the masking task needs to be executed at 12:00 every Monday, set this parameter to **12:00:00 every Monday**.
- **Monthly:** Execute a data masking task at a specified time on a specified day every month.
Example: If the masking task needs to be executed at 12:00 on the 12th day of each month, set this parameter to **12:00:00 12th day of every month**.

NOTE

If you want to execute a data masking task on the 31st day of each month, the system automatically executes the task on the last day of every month.

Step 9 Click **Next**. The **Set Target Data** page is displayed.

Figure 7-23 Setting target data

Progress: Configure Data Source — Set Masking Algorithm — Configure Data Masking Period — **4** Set Target Data

Database Instance	Namespace	Table Name	column family
hbase	zyj	student	Please enter a column family name.
Data Source Column	Risk Level	Target Column	
name	0	<input type="text" value="name"/>	
email	6	<input type="text" value="email"/>	

1. Select the database instance, namespace, and data table name, and enter the column family.

If the entered column name already exists, the system updates the data in the column.

If the entered column name does not exist, the system automatically creates the column in the target data table.

CAUTION

Do not fill in an existing service data table. Otherwise, services may be affected.

2. Set the column name of the target data type.
By default, the system generates a name that is the same as the name of the data source column. You can retain the default name or change it as required.

Step 10 Click **Finish**.

Step 11 On the **HBase** page. In the **Operation** column of the target anonymization task, click **Execute**.


Step 12 The data masking task is executed as configured.

----End

Creating and Running a DLI Masking Task

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation pane, choose **Data Asset Protection > Static Data Masking** and click the **DLI** tab. The DLI masking page is displayed.

Step 5 Click  and set **Masking Sensitive DLI Data** to  to enable DLI masking.


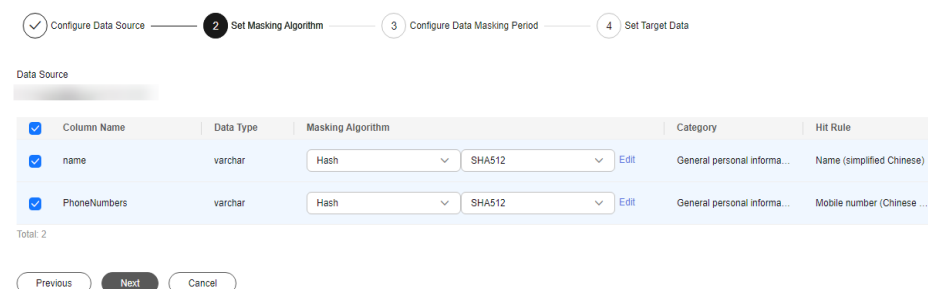
Step 6 Click **Create Task**. On the displayed **Configure Data Source** page, configure parameters according to .

Table 7-10 Parameter description

Parameter	Description
Task Name	You can customize the name of a data masking task. The task name must meet the following requirements: <ul style="list-style-type: none"> Contain 1 to 255 characters. Consist of letters, digits, underscores (_), and hyphens (-).
Select Data Source	Select a data source. Only DLI is supported.
Data Source (If no database instance is available, click Add Database to add a database. For details, see Authorizing Access to a Big Data Asset.)	<p>Database Instance: Select the database instance where the data you want to mask is located.</p> <p>Database Name: Enter the name of the database for masking.</p> <p>Table Name: Enter the name of the table to be masked.</p> <p>NOTE Only assets with read and write permissions can use the masking function.</p> <p>Select the columns to be masked. You can select multiple columns.</p>
AK/SK	Enter an access key. For details, see Access Keys . You can obtain the AK from the access key list and SK from the downloaded CSV file.
Column Information	The column information includes Column Name , Risk Level , Data Type , and Category .

Step 7 Click **Next**. The **Set Masking Algorithm** page is displayed.

Figure 7-24 Setting a masking algorithm



1. Select the data columns you want to mask.
2. Select a data masking algorithm. For details about data masking algorithms, see [Configuring and Viewing Masking Rules](#).

Step 8 Click **Next** to switch to the **Configure Data Masking Period** page and configure the data masking period.

Select and set the execution period of a masking task.

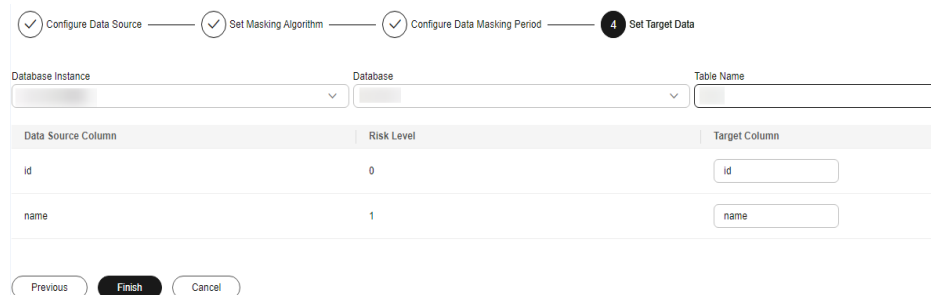
- **Manual:** Manually enable a masking task and execute it based on masking rules.
- **Hourly:** Execute a data masking task every several hours.
Example: If the masking task needs to be executed every two hours, set this parameter to **02:00**.
- **Daily:** Execute a data masking task at a specified time every day.
Example: If the masking task needs to be executed at 12:00 every day, set this parameter to **12:00:00**.
- **Weekly:** Execute a data masking task at a specified time every week.
Example: If the masking task needs to be executed at 12:00 every Monday, set this parameter to 12:00:00 every Monday.
- **Monthly:** Execute a data masking task at a specified time on a specified day every month.
Example: If the masking task needs to be executed at 12:00 on the 12th day of each month, set this parameter to 12:00:00 12th day of every month.

 **NOTE**

If you want to execute a data masking task on the 31st day of each month, the system automatically executes the task on the last day of every month.

Step 9 Click **Next**. The **Set Target Data** page is displayed.

Figure 7-25 Setting target data



Data Source Column	Risk Level	Target Column
id	0	id
name	1	name

1. Select a database instance and database name, and enter the table name.
If the entered table name already exists, the system will update the data in the existing table.
If the table name is new, it will automatically create and name the table in the target database.

 **CAUTION**

Do not fill in an existing service data table. Otherwise, services may be affected.

2. Set the column name of the target data type.
By default, the system generates a name that is the same as the name of the data source column. You can retain the default name or change it as required.

Step 10 Click **Finish**.

Step 11 On the **DLI** page. In the **Operation** column of the target anonymization task, click **Execute**.


Step 12 The data masking task is executed as configured.

----End

Creating and Running an OBS Masking Task

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation pane, choose **Data Asset Protection > Static Data Masking** and click the **OBS** tab. The OBS masking page is displayed.

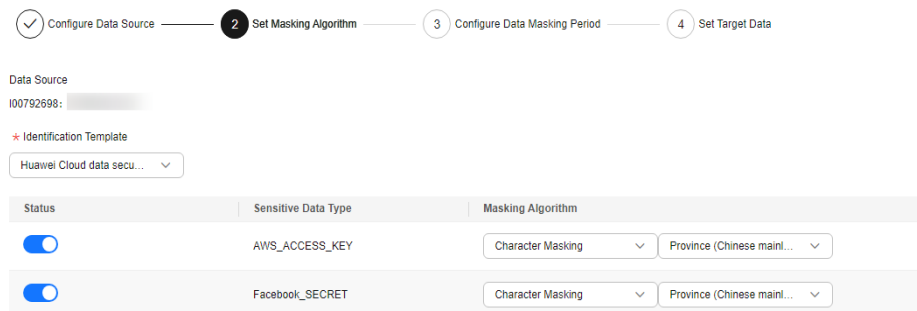
Step 5 Click  and set **Mask Sensitive OBS Data** to  to enable OBS masking.

Step 6 Click **Create Task**. On the displayed **Configure Data Source** page, configure parameters according to [Table 7-11](#).

Table 7-11 Parameter description

Parameter	Description
Task Name	You can customize the name of a data masking task. The task name must meet the following requirements: <ul style="list-style-type: none">Contain 1 to 255 characters.Consist of letters, digits, underscores (_), and hyphens (-).
Select Data Source	Select a data source. Only OBS is supported.
Data Source	Bucket Name: Select an OBS bucket name from the drop-down list box. OBS Storage Path: Select the path of the OBS bucket file from the drop-down list box. File Type: Currently, only the text type is supported. NOTE Only assets with read and write permissions can use the masking function.

Step 7 Click **Next**. The **Set Masking Algorithm** page is displayed.

Figure 7-26 Setting a masking algorithm

1. **Identification Template:** Select an identification template from the drop-down list box.

If a sensitive data identification rule is disabled in the sensitive data identification template, the corresponding sensitive information is not displayed.

2. Click the switch in the **Status** column to disable masking for the sensitive data type.

If the **Status** button is disabled, the identification rule is enabled but masking is not performed after identification.

3. Data masking algorithms:

By default, **Simulation masking** is selected, meaning the amount of information is not lost and the data format is not changed after masking. For details about the sensitive data types supported by simulation masking, refer to [Simulation Masking](#). You can also choose the following masking algorithms from the drop-down list:

Hash: For details, see [Hash](#).

Character masking: For details, see [Character Masking](#).

Keyword replacement: For details, see [Keyword Replacement](#).

Value change: For details, see [Value Change](#).

Step 8 Click **Next**. The **Configure Data Masking Period** page is displayed.

- **Traverse Sub-directories:** If you enable this option, the subdirectories in the source directory will be masked.
- **Rename File:** If you enable this option, the masked files will be renamed.
 - **File Prefix/File Suffix:** The value can contain only letters, digits, underscores (_), and hyphens (-), and cannot exceed 16 characters.
 - Example of renaming a file: The original file name is **Test.txt**, the prefix is **DSC_**, and the suffix is **1**. The renamed file is **DSC_Test1.txt**.

Step 9 Click **Next**. The **Set Target Data** page is displayed.

Figure 7-27 Setting target data

Configure Data Source — Set Masking Algorithm — Configure Data Masking Period — **4** Set Target Data

Bucket Name: dsc-test-dy2

OBS Storage Path: 1000_bxt

Previous Finish Cancel

1. **Bucket Name:** Select a bucket from the drop-down list for storing the masked file.
2. **OBS Storage Path:** Click to select an OBS file path.

CAUTION

The path of the target OBS bucket cannot be the same as that of the source OBS bucket or the subdirectory of the source OBS bucket.

Step 10 Click **Finish**. The OBS masking task is created.

Step 11 Go to the **OBS** tab page, locate the target masking task, click **Enable/Disable** to enable the task, and click **Execute** in the **Operation** column.

Step 12 After the task is executed, the system starts to perform masking based on the settings.

----End


7.1.3.2 Checking the Running Status of a Static Data Masking Task


Prerequisites

A static data masking task has been created. For details, see section [Creating a Static Data Masking Task](#).


Checking the Running Status of a Static Data Masking Task

Step 1 [Log in to the management console](#).


Step 2 Click  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 In the left navigation pane, choose **Data Asset Protection** > **Static Data Masking**. The **Static Data Masking** page is displayed.

Step 5 Click the **Masking Task** tab, select the masking task type, such as database, Elasticsearch, or MRS, and click  before the target masking task to view the running status of the masking task.

The statuses are as follows:

- **Queuing:** The masking task is in the queue.
- **Completed:** The data masking task has been successfully executed.
- **Running:** The data masking task is being executed.
- **Pending execution:** The data masking task is not executed.
- **Stopped:** The data masking task has been manually stopped.
- **Failed:** The data masking task fails to be executed. Move the cursor to  to view the failure cause.

----End


7.1.3.3 Editing and Deleting a Static Data Masking Task

Editing and Deleting a Static Data Masking Task

You can edit and delete a masking task executed on the console. For a running masking task, you can stop it then edit and delete it.

Step 1 [Log in to the management console.](#)

Step 2 Click  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 In the left navigation pane, choose **Data Asset Protection > Static Data Masking**. The **Static Data Masking** page is displayed.

Step 5 Click the **Masking Task** tab and select the masking task type, for example, database, Elasticsearch, or MRS. In the masking task list, click **Edit** in the **Operation** column of the target masking task to reconfigure the masking task information. For details, see [Creating and Running a Database Masking Task](#).

Step 6 Click **Delete** in the **Operation** column of the target masking task to delete the task.

 CAUTION

Deleted masking tasks cannot be restored. Exercise caution when performing this operation.

----End

7.2 Data Watermarking

7.2.1 Data Watermarking Overview

If data leakage occurs, you can use DSC to extract the watermark information. In this case, the organization or person that is accountable for the leakage problem

can be easily found. Adding watermarks does not affect the distributed data usage.

Table 7-12 Supported database types

Database Type	Data Type
DWS	smallint, integer, bigint, float4, float8, varchar, text, and char
MRS-HIVE	smallint, int, long, float, double, and string

Table 7-13 Supported file types

Type	Format
Document	pdf, pptx, docx, and xlsx
JSON data (invoking data watermark APIs)	The value can be an integer, floating-point number, or string.

Table 7-14 Supported image watermark types

Type	Format
Images (or invoking image watermark APIs)	*.jpg, *.jpeg, *.jpe, *.png, *.bmp, *.dib, *.rle, *.tiff, *.tif, *.ppm, *.webp, *.tga, *.tpic, *.gif

Application Scenarios

Data watermarking is widely used in government departments, healthcare agencies, finance institutions, academic institutes, and other organizations. It is generally used for **copyright protection** and **source tracing**.

- **Data copyright protection:** In scenarios where digital works are downloaded or copied for use and database services (data mining and analysis) provide data to third parties, digital watermarks can be used to identify the copyright when disputes occur,
- **Source tracing:** Data provided for internal employees or third parties can be injected with watermarks to identify the ownership and remind them of keeping the data secure. When the data leaked, the watermarks can be used to trace the source of data leak and identify the root cause.

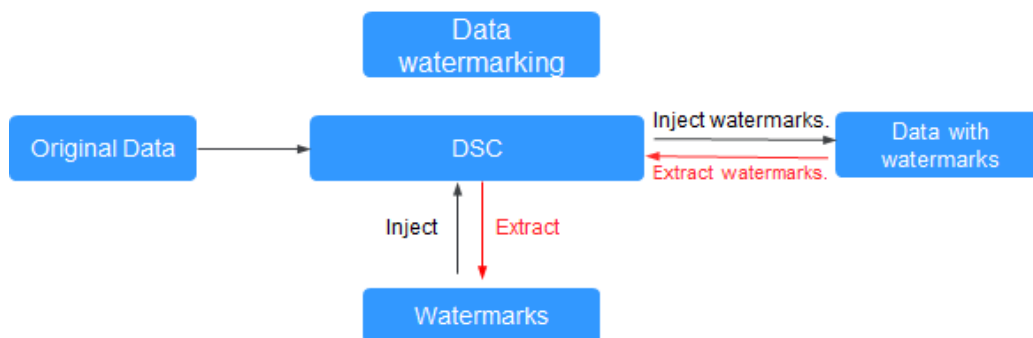
Advantages and Highlights

- **Visible and invisible watermarks:** You can inject visible or invisible watermarks into the data as needed to efficiently cope with data theft through image process tools, picture taking, or screenshots.

- **Detectable and tamper-proofing:** Watermarks injected into the data can be detected and will not be lost, fabricated, and tampered with.
- **High robustness:** Watermarks are not easily removed during transmission or use. Even if the data carrier is tampered with or damaged, there is a high probability that watermarks are extracted.

Procedure

Figure 7-28 Data watermarking process



7.2.2 Injecting Watermarks

7.2.2.1 Injecting Watermarks to Databases

Prerequisites

- Access to cloud assets has been authorized. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- An RDS or GaussDB(DWS) database has been authorized. For details, see [Adding Self-Built Database Instances](#).
- An MRS database has been authorized. For details, see [Authorizing Access to a Big Data Asset](#).
- You have configured the GaussDB(DWS) and MRS_Hive permissions. For details, see [\(Optional\) Configuring GaussDB\(DWS\) and MRS Hive](#).


Constraints

- GaussDB(DWS) data supports the following watermarks: smallint, integer, bigint, float4, float8, varchar, text, and char.
- MRS Hive data supports the following watermarks: smallint, int, long, float, double, and string.
- A single column in the embedding target cannot have more than 30% redundant data.
- The database encoding is UTF-8.
- The database injection is a non-primary key column.
- It is recommended that the number of data rows in a data table be greater than 1500.

Creating a Sensitive Data Identification Task

Step 1 [Log in to the management console.](#)

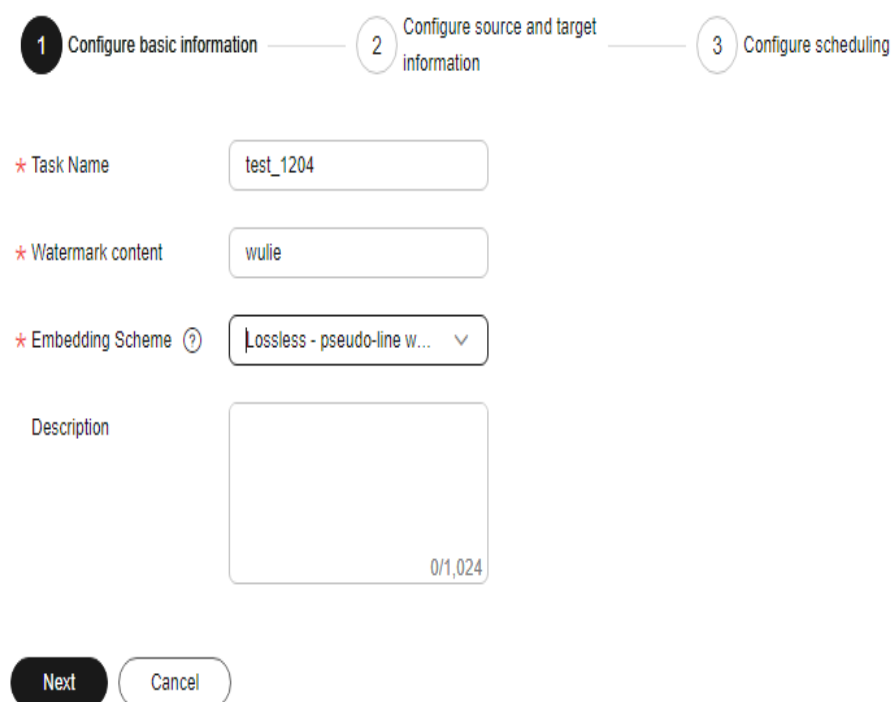
Step 2 Click  in the upper left corner and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Data Asset Protection > Database Watermark**.

Step 5 Click **Create Task**. The **Configure basic information** page is displayed.


Figure 7-29 Configuring basic information



1 Configure basic information — 2 Configure source and target information — 3 Configure scheduling

* Task Name

* Watermark content

* Embedding Scheme 

Description

0/1,024

Next

Table 7-15 Parameters for configuring basic information

Parameter	Description
Task Name	Enter a task name. The value can contain only letters, digits, underscores (_), and hyphens (-), and cannot exceed 255 characters.
Watermark ID	Enter the watermark identifier to be injected.

Parameter	Description
Embedding Scheme	<p>Click the drop-down list box to select a watermark embedding scheme. The options are as follows:</p> <ul style="list-style-type: none"> • Lossless - pseudo-column watermark: A pseudocolumn related to other attributes of the relationship table is generated. The pseudocolumn is deceptive to attackers. Watermarks are embedded into the pseudocolumn to reduce damage to the original data. • Lossless - pseudo-line watermark: Pseudo lines are generated based on the data type, data format, and value range. Watermarks are embedded into these pseudo lines to reduce damage to the original data. • Lossy - column watermark: If you directly add watermarks to column data, the data will be modified or damaged. <p>NOTE A higher error correction level indicates more watermark bits and a lower bit error rate (BER) during source tracing. Note that a higher error correction level requires more data as the embedding target to ensure embedding integrity. The default value is 1.</p>

Step 6 Click **Next**. On the **Configure source and target information** page, set related parameters.

- **Lossless - pseudocolumn watermark:** Embed watermarks to newly created columns to avoid data loss.

Figure 7-30 Pseudocolumn watermarks

Table 7-16 Source and destination parameters of pseudocolumn watermarks

Parameter	Description
Data Source Type	Select a data source type from the drop-down list box. <ul style="list-style-type: none">– When Embedding Scheme is set to Lossy - Column Watermark, the following data source types are supported:<ul style="list-style-type: none">▪ DWS▪ MRS_HIVE– When Embedding Scheme is set to Lossless pseudo-column watermarking or Lossless pseudo-line watermarking, the following data types are supported:<ul style="list-style-type: none">▪ DWS▪ PostgreSQL▪ MySQL
Database Instance	Select a Database Instance from the drop-down list. If no database instance is available, add databases by following the instructions provided in sections Adding Self-Built Database Instances and Authorizing Access to a Big Data Asset .
Database	Select a Database from the drop-down list.
Schema	This parameter is displayed when Database is DWS or PostgreSQL . Click a Mode as required.
Source Table	Select the corresponding Source Table name.
Column Name	Only letters, numbers, underscores (_), and hyphens (-) are allowed (255 characters max).
Column Data Type	Click to select the data type of the embedded pseudocolumn. <ul style="list-style-type: none">– Numeric– String– Date
Example Value	Choose Setting Field Rules . The embedded pseudocolumn data example is displayed.

Parameter	Description
Setting Field Rules	<ul style="list-style-type: none">– If Column Data Type is set to Numeric, this parameter is a random number. You can specify the range and precision of the random number. If the range and precision are not specified, pseudo data will be randomly generated.– When Column Data Type is set to String, you can select pseudo data such as the person name, ID card number, and mobile number from the drop-down list box.– When the Column Data Type is set to Date, you can specify a date range. If no date range is specified, pseudo data is randomly generated.
Add a Pseudo Column	You can click Add a Pseudo Column to add two pseudo-columns,
Target Table	Enter the target table name. The name can contain only letters, digits, underscores (_), and hyphens (-) and cannot exceed 255 characters.

- **Lossless - pseudo-line watermark:** Watermarks are embedded into line copies to avoid data loss.

Figure 7-31 Pseudo-line watermark

1 Configure basic information — **2 Configure source and target information** — 3 Configure scheduling information

Source Settings

- * Data Source Type: DWS
- * Database Instance: testgy
- * Database: testwm
- * Schema: wmtest
- * Source Table [?]: info1
- * Number of pseudo-line spans: 12

Target Settings

- * Target Table: table

Table 7-17 Source and destination parameters of pseudo-line watermarks

Parameter	Description
Data Source Type	Select a Data Source Type from the drop-down list. The following data source types are supported: <ul style="list-style-type: none"> - DWS - PostgreSQL - MySQL
Database Instance	Select a Database Instance from the drop-down list. If no database instance is available, add databases by following the instructions provided in sections Adding Self-Built Database Instances and Authorizing Access to a Big Data Asset .

Parameter	Description
Database	Select a Database from the drop-down list.
Mode	This parameter is displayed when Database is DWS or PostgreSQL . Click a Mode as required.
Source Table	Click and select the corresponding source data table name.
Number of Pseudo-Line Spans	Enter a valid integer greater than 1 to specify the number of pseudo-rows inserted into the original data.
Target Table	Enter the name of the data storage table with watermarks embedded. The name can contain only letters, digits, underscores (_), and hyphens (-), and cannot exceed 255 characters.

- **Lossy - column watermark:** Embed watermarks directly to the column data.

Figure 7-32 Lossy column watermarks

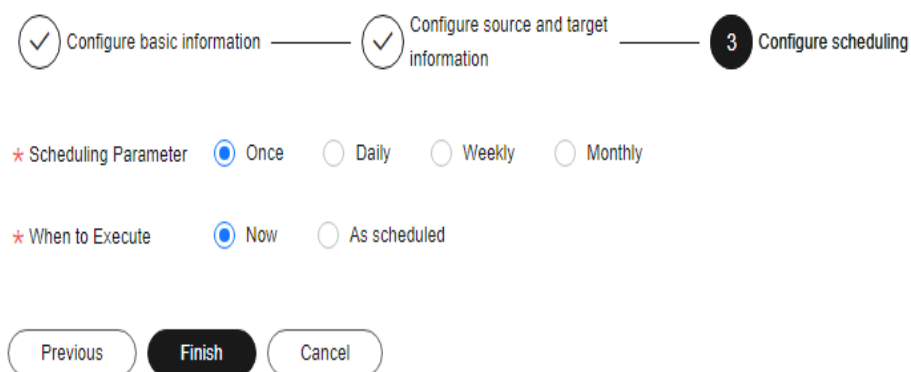
Table 7-18 Source and destination parameters of lossy column watermarks

Parameter	Description
Data Source Type	Select a Data Source Type from the drop-down list. The following data source types are supported: <ul style="list-style-type: none"> - DWS - MRS-HIVE

Parameter	Description
Database Instance	Select a Database Instance from the drop-down list. If no database instance is available, add databases by following the instructions provided in sections Adding Self-Built Database Instances and Authorizing Access to a Big Data Asset .
Database	Select a Database from the drop-down list.
Mode	This parameter is displayed when the Database is DWS . Click a Mode as required.
Source Table	Select the corresponding Source Table name.
Watermark Embedding Bar	Click to select the column data to which watermarks are embedded. You can select multiple columns. NOTE <ul style="list-style-type: none">- The source database character set must be UTF-8.- A single column in the embedding target cannot have more than 30% redundant data.
Target Table	Enter the name of the data storage table with watermarks embedded. The name can contain only letters, digits, underscores (_), and hyphens (-), and cannot exceed 255 characters.

Step 7 Click **Next**. The **Configuring scheduling** page is displayed.

Figure 7-33 Configuring scheduling



- If the **Scheduling Parameter** is set to **Once**, you can select **Now** or **As scheduled** to start the watermark embedding task.

- If the **Scheduling Parameter** is set to **Daily**, **Weekly**, or **Monthly**, start the watermark embedding task at a specified time daily, weekly, or monthly.


Step 8 Click **Finish**.

----End

Running Tasks

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation pane, choose **Data Asset Protection > Database Watermark**.

Step 5 In the **Operation** column of the target task, choose **More > Running**.


----End

Starting a Task

This parameter is displayed when the watermarking task is a scheduled task.

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation pane, choose **Data Asset Protection > Database Watermark**.

Step 5 In the **Operation** column of the target task, choose **More > Start Task**.


----End

Stopping a Task

This parameter is displayed when the watermarking task is a scheduled task.

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation pane, choose **Data Asset Protection > Database Watermark**.

Step 5 In the **Operation** column of the target task, choose **More > Stop Task**.

----End

Editing and Deleting an Embedded Watermark Task

A running watermark embedding task cannot be edited or deleted.

- Click **Edit** in the **Operation** column to modify the watermark embedding task configuration.
- Click **Delete** in the **Operation** column of the target task. You can also select multiple tasks and click **Batch Delete** to delete them.

NOTE

The deletion cannot be undone.

7.2.2.2 Injecting Watermarks to Documents

On the DSC console, you can insert custom watermarks in PDF, PPT, Word, and Excel documents. This section describes how to insert customized watermarks into local files or cloud files (files stored in the OBS bucket).

Prerequisites

- OBS asset access permissions are granted. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- You have enabled and created assets on OBS. For details about how to enable OBS, see [Enabling and Using OBS Buckets](#).
- The document format is PDF, PPTX, DOCX, or XLSX.


Constraints

- The maximum size of a PDF or Word file is 50 MB.
- The maximum size of an Excel file is 70 MB.
- The maximum size of a PPT file is 20 MB.

Creating a Watermark Injection Task for Files in an OBS Bucket

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation pane, choose **Data Asset Protection** > **Document Watermarking**.

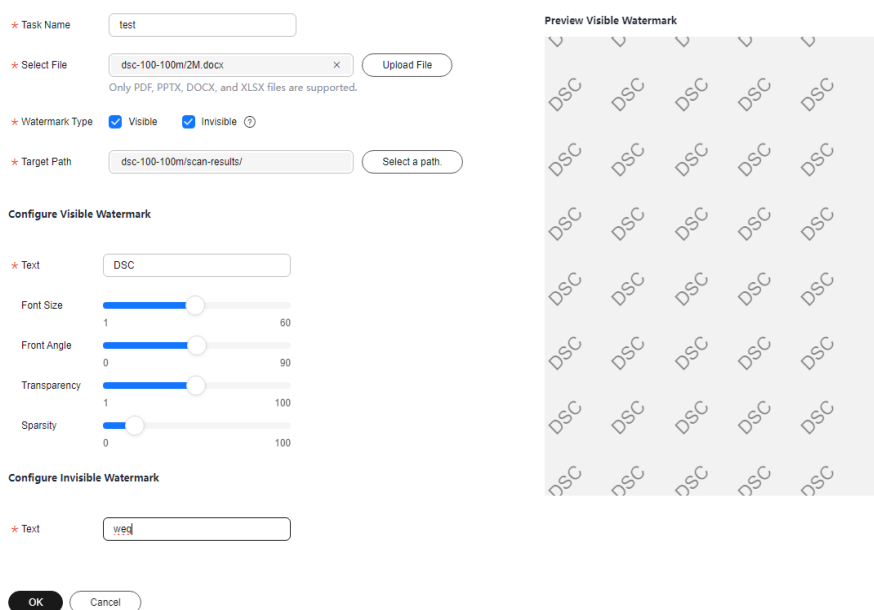
Step 5 Click **Create Task** in the upper left corner of the task list to create a task.


Step 6 Set the parameters shown in [Table 7-19](#).

Table 7-19 Task parameters

Parameter	Description
Task Name	Enter the watermark ingestion task name. The value can contain only letters, digits, underscores (_), and hyphens (-), and cannot exceed 255 characters.
Select File	Click Add File . In the right pane, select the name of the bucket to which you want to add a watermark. In the left pane, select a file. You can select multiple files.
Watermark Type	Both visible and invisible watermarks are supported. You can select multiple values. <ul style="list-style-type: none"> • Visible watermark: Watermarks are visible on documents. • Invisible watermark: The watermark text is invisible and needs to be extracted using tools. For details about how to extract an invisible watermark, see Extracting Watermarks from Documents.
Target Path	Click selecting a file path , and select the watermarked file.
Configure Visible Watermark	Set the Watermark Type to Visible Watermark . Then, enter the watermark content and drag the slider to set the Text , Font Size , Font Angle , Sparseness , and Transparency .
Configure Invisible Watermark	This parameter is mandatory when Watermark Type is set to Invisible . Set Text as required.

Figure 7-34 Inserting Watermarks



- Step 7** Click **OK**. A message is displayed in the upper right corner, indicating that the watermark injection task is created successfully.
- Step 8** In the watermark task list, click the task name to view the task running status.
- **Running**: You can view the progress of the watermark ingestion task.
 - **Finished**: You can click **Download** in the **Operation** column to download the watermarked OBS bucket file.
 - **Failed**: The watermark injection task fails to be executed. You can move the cursor to  to view the failure cause.
- Step 9** If the injected watermark is a visible watermark, click **Download** to obtain the watermark file.

If you injected an invisible watermark, extract the watermark from the target file using tools. For details, see [Extracting Watermarks from Documents](#).

----End

Creating a Local File Data Injection Task



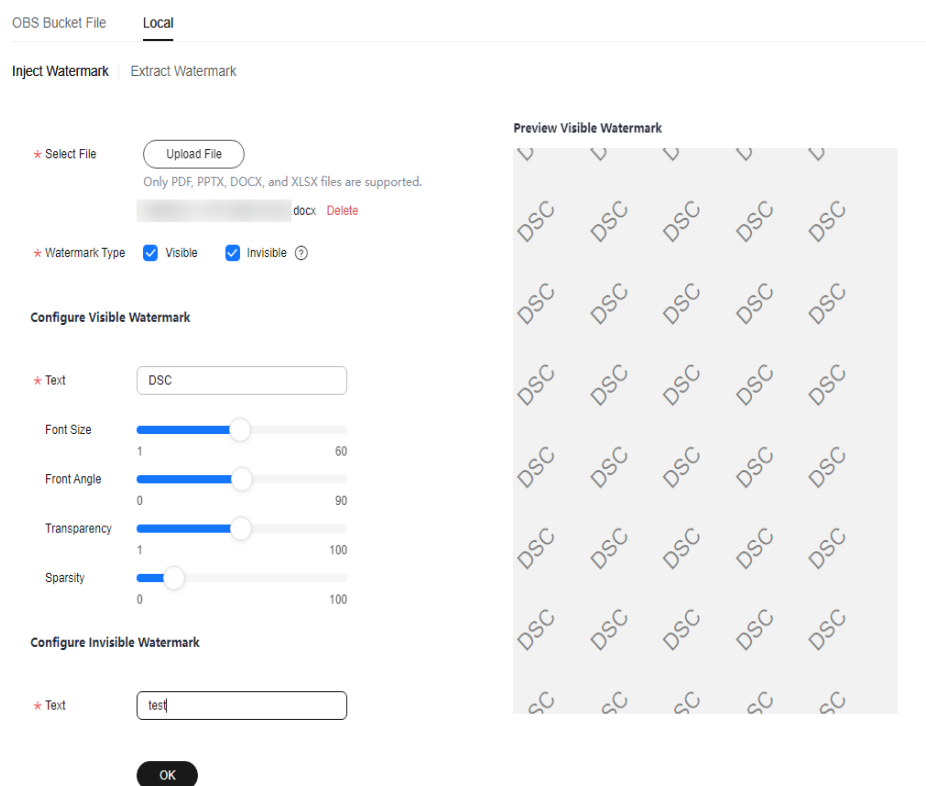
- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner and select a region or project.
- Step 3** In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Data Asset Protection > Document Watermarking**.
- Step 5** Click the **Local File** tab. The **Watermark Injection** page is displayed.
- Step 6** Click **Select File**, and select the file to which the watermark is to be injected.
- Step 7** After the file is uploaded, configure related parameters. [Table 7-20](#) describes the related parameters.

Table 7-20 Watermarking parameters

Parameter	Description
Watermark Type	Both visible and invisible watermarks are supported. You can select multiple values. <ul style="list-style-type: none">• Visible watermark: Watermarks are visible on documents.• Invisible watermark: The watermark text is invisible and needs to be extracted using tools. For details about how to extract an invisible watermark, see Extracting Watermarks from Documents.

Parameter	Description
Configure Visible Watermark	Set the Watermark Type to Visible Watermark . Then, enter the watermark content and drag the slider to set the Text , Font Size , Font Angle , Sparseness , and Transparency .
Configure Invisible Watermark	This parameter is mandatory when Watermark Type is set to Invisible . Set Text as required.

Figure 7-35 Creating a Local File Data Injection Task



Step 8 After parameters are configured, click **OK**. The file with watermark injected is automatically downloaded to the specified path on the local PC.

NOTICE

- If you injected a visible watermark, open the target file to view the watermark.
- If you injected an invisible watermark, extract the watermark from the target file using tools. For details, see [Extracting Watermarks from Documents](#).

----End

7.2.2.3 Injecting Watermarks to Images

The DSC console offers a feature for injecting watermarks into JPG or JPEG files. You can refer to this section to apply customized watermarking to your cloud-stored files in OBS buckets or to images on your local device.

Prerequisites


- OBS asset access permissions are granted. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- You have enabled and created assets on OBS. For details about how to enable OBS, see [Enabling and Using OBS Buckets](#).
- Currently, the following image format is supported: .jpg, .jpeg, .jpe, .png, .bmp, .dib, .rle, .tiff, .tif, .ppm, .webp, .tga, .tpic, .gif.


Constraints

- The maximum size of an image is 20 MB.
- The resolution of the image to be watermarked must be greater than 128 x 128 pixels.
- The maximum length of the invisible text watermark is 32 characters.

Injecting Watermarks into OBS Bucket Files

Step 1 [Log in to the management console](#).

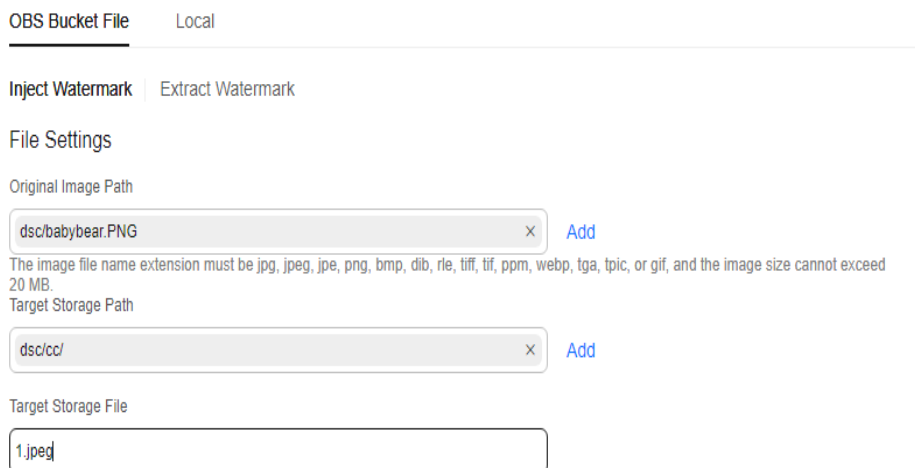
Step 2 Click  in the upper left corner and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation tree on the left, choose **Data Asset Protection > Image Watermarking**. The **Image Watermarking** page is displayed.

Step 5 On the **OBS Bucket Files** tab page, set the path in the **File Settings** area.

Figure 7-36 File settings



OBS Bucket File Local

Inject Watermark Extract Watermark

File Settings

Original Image Path

dsc/babybear.PNG x Add

The image file name extension must be jpg, jpeg, jpe, png, bmp, dib, rle, tiff, tif, ppm, webp, tga, tpic, or gif, and the image size cannot exceed 20 MB.

Target Storage Path

dsc/cc/ x Add

Target Storage File

1.jpeg

1. Click **Add** next to **Original image path** to select the cloud path of the original images. The size of the selected image cannot exceed 20 MB.
2. Click **Add** next to **Storage destination path** to select the destination storage path.
3. Click the **Save Target File Name** text box and enter the name of the watermarked image file. The file name contains a maximum of 32 characters, and the file name extension is *.jpg, *.jpeg, *.jpe, *.png, *.bmp, *.dib, *.rle, *.tiff, *.tif, *.ppm, *.webp, *.tga, *.tpic, or *.gif.

Step 6 Watermark type can be **visible watermark** and **invisible watermark**.

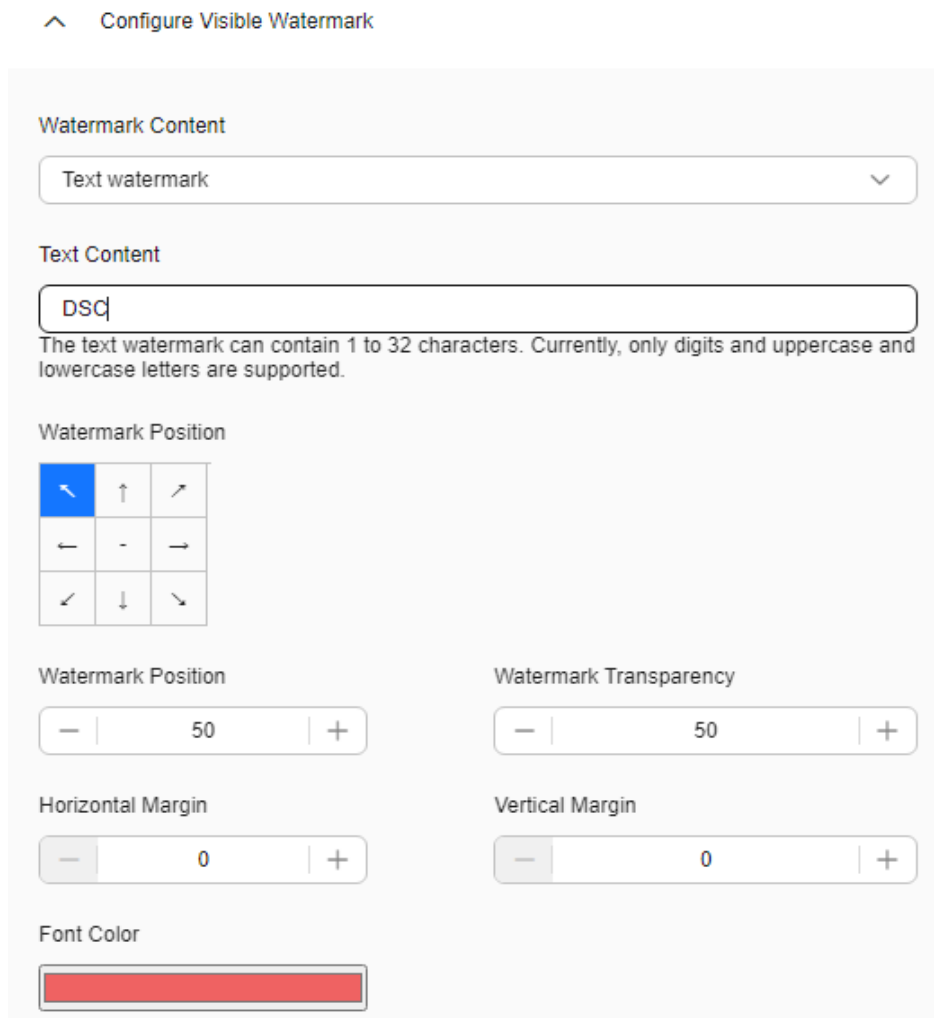
- Visible watermark: The watermark can be displayed on the image. For details about the related parameters, see [Table 7-21](#).

Table 7-21 Configuring a visible watermark

Parameter	Description
Watermark Content	Select the Watermark Content from the drop-down list box. <ul style="list-style-type: none">- Image watermark- Text watermark.
Image Path	If Watermark Content is set to Image watermark , click Add to select an image on the cloud as the watermark. The watermark image must be in the same area as the original image. Otherwise, the preview fails.
Text Content	If Watermark Content is set to Text Watermark , click the text box and enter the text watermark content. The value contains 1 to 32 characters, including only digits and case-sensitive letters.
Watermark Position	Select the position where the watermark is injected.
Image Size	Absolute size of the image to be injected. This parameter is displayed when Watermark Content is set to Image watermark . The value ranges from 0 to 100.
Watermark Size	Size of the text watermark to be injected. This parameter is displayed when Watermark Content is set to Text watermark . The value ranges from 1 to 100.
Watermark Transparency	Transparency of the watermark to be injected. The value ranges from 1 to 100.
Horizontal Margin	Horizontal margin of the watermark to be injected relative to the image. The value ranges from 0 to 100.

Parameter	Description
Vertical Margin	Vertical margin of the watermark to be injected relative to the image. The value ranges from 0 to 100.
Font Color	This parameter is displayed when Watermark Content is set to Text watermark . You can click the color bar to select the font color of the text watermark to be injected.

Figure 7-37 Configuring a visible watermark



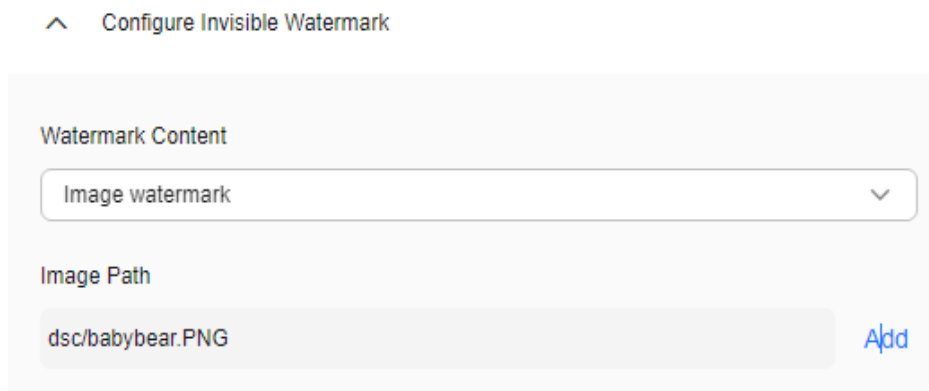
- Invisible watermark: The watermark text is invisible and needs to be extracted using tools. For details about how to extract an invisible watermark, see [Extracting Watermarks from Images](#).

NOTE

For effective watermark embedding, the resolution of the watermark image should be at least 64 x 64 pixels. Upon extraction, the watermark will be displayed as a downscaled version, resized to precisely 64 x 64 pixels.

Table 7-22 Configuring an invisible watermark

Parameter	Description
Watermark Content	Select the Watermark Content from the drop-down list box. <ul style="list-style-type: none">- Image watermark- Text watermark.
Text Content	If Watermark Content is set to Text Watermark , click the text box and enter the text watermark content. The value contains 1 to 32 characters.
Image path	If Watermark Content is set to Image watermark , click Add to select an image on the cloud as the watermark.

Figure 7-38 Configuring an invisible watermark

Step 7 After parameters are configured, click **OK**. The file with watermark injected is automatically downloaded to the specified path on the local PC.

NOTICE

- If you injected a visible watermark, open the target file to view the watermark.
- If you injected an invisible watermark, extract the watermark from the target file using tools. For details, see [Extracting Watermarks from Images](#).

Step 8 Click **Preview** in the lower left corner of the page and preview the watermark effect in the visible watermark preview area on the right. The invisible watermark cannot be previewed.


Step 9 Click **OK** to complete watermark injection.

----End

Creating a Local File Watermark Injection Task

Step 1 [Log in to the management console.](#)

Step 2 Click  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 In the navigation tree on the left, choose **Data Asset Protection > Image Watermarking**. The **Image Watermarking** page is displayed.

Step 5 Click the **Local File** tab. The **Watermark Injection** page is displayed.

Step 6 Click **Add File** and select the local image file to which you want to add watermarks.

Step 7 **Watermark type** can be **visible watermark** and **invisible watermark**.

- Visible watermark: Watermarks are visible on images.
- Invisible watermark: The watermark text is invisible and needs to be extracted using tools. For details about how to extract an invisible watermark, see [Extracting Watermarks from Images](#).

Step 8 Set the watermark parameters according to [Table 7-23](#).

Table 7-23 Watermark settings

Water mark Type	Parameter	Description
Visible water mark	Watermark Content	Select the watermark content from the drop-down list box. <ul style="list-style-type: none">• Image watermark• Text watermark.
	Watermark Image	When Watermark Content is set to Image watermark , click Add File to add an image as the watermark. The watermark image must be in the same area as the original image. Otherwise, the preview fails.
	Text Content	This parameter is displayed when Watermark content is set to Text watermark . Click the text box to enter the text watermark content. The text watermark contains 1 to 32 characters, including only digits and case-sensitive letters.

Water mark Type	Parameter	Description
	Watermark Position	Select the position where the watermark is injected.
	Image Size	Absolute size of the image to be injected. This parameter is displayed when Watermark Content is set to Image watermark . The value ranges from 0 to 100.
	Watermark Size	Size of the text watermark to be injected. This parameter is displayed when Watermark Content is set to Text watermark . The value ranges from 1 to 100.
	Watermark Transparency	Transparency of the watermark to be injected. The value ranges from 1 to 100.
	Horizontal Margin	Horizontal margin of the watermark to be injected relative to the image. The value ranges from 0 to 100.
	Vertical Margin	Vertical margin of the watermark to be injected relative to the image. The value ranges from 0 to 100.
	Font Color	This parameter is displayed when Watermark Content is set to Text watermark . You can click the color bar to select the font color of the text watermark to be injected.
Invisible watermark	Watermark Content	Select the watermark content from the drop-down list box. <ul style="list-style-type: none"> ● Image watermark ● Text watermark.
	Watermark Image	This parameter is displayed when Watermark Content is set to Image watermark . Click Add File to select a local image as the watermark.
	Text Content	This parameter is displayed when Watermark Content is set to Text watermark . Click the text box to enter the watermark text content.

Figure 7-39 Watermark settings

The image shows two panels for configuring watermarks. The top panel is titled 'Configure Visible Watermark' and includes the following settings:

- Watermark Content:** A dropdown menu set to 'Image watermark'.
- Watermark Image:** An 'Upload File' button.
- Watermark Position:** A 3x3 grid of directional arrows. The top-left arrow (pointing up and left) is highlighted in blue.
- Image Size (%):** A slider set to 50.
- Watermark Transparency:** A slider set to 50.
- Horizontal Margin:** A slider set to 0.
- Vertical Margin:** A slider set to 0.

The bottom panel is titled 'Configure Invisible Watermark' and includes the following settings:

- Watermark Content:** A dropdown menu set to 'Image watermark'.
- Watermark Image:** An 'Upload File' button.

Step 9 After parameters are configured, click **OK**. The file with watermark injected is automatically downloaded to the specified path on the local PC.

NOTICE

- If you injected a visible watermark, open the target file to view the watermark.
- If you injected an invisible watermark, extract the watermark from the target file using tools. For details, see [Extracting Watermarks from Images](#).

----End

7.2.3 Extracting Watermarks

7.2.3.1 Extracting Watermarks from Databases

Prerequisites

- Access to cloud assets has been authorized. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- An RDS or GaussDB(DWS) database has been authorized. For details, see [Adding Self-Built Database Instances](#).
- An MRS database has been authorized. For details, see [Authorizing Access to a Big Data Asset](#).
- You have configured the GaussDB(DWS) and MRS_Hive permissions. For details, see [\(Optional\) Configuring GaussDB\(DWS\) and MRS Hive](#).


Constraints

- The source file must be in CSV format and cannot be larger than 20 MB.
- The table may contain more than 1,500 rows of data.
- The CSV file content is encoded in UTF-8 mode. Ensure that the data is complete and correct.

Creating a Task

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation pane, choose **Data Asset Protection > Database Watermark**.

Step 5 Click the **Extract Watermark** tab.

Step 6 Click **Create Task**. In the displayed dialog box, set parameters based on [Table 7-24](#).

Figure 7-40 Creating an extraction task

Create Task ✕

* Task Name

Description

* Source Files

* Extraction Mode

* Delimiter

Table 7-24 Creating a watermark extraction task



Parameter	Description
Task Name	Enter a task name.
Source Files	The source file must be in CSV format and cannot be larger than 20 MB. The table may contain more than 1,500 rows of data. The CSV file content is encoded in UTF-8 mode. Ensure that the data is complete and correct.
Extraction Mode	Select a watermark extraction mode from the drop-down list box. For lossy column embedding and lossless column embedding, extract watermarks by column. For lossless line embedding, extract watermarks by row.
Delimiter	Delimiters in a file. For example: comma (,)

Step 7 Click **OK**.

----End



Viewing Results

Step 1 [Log in to the management console.](#)

- Step 2** Click  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** In the navigation pane, choose **Data Asset Protection > Database Watermark**.
- Step 5** Click the **Extract Watermark** tab.
- Step 6** Locate a task and click **View Result** in the **Operation** column.
- End

Deleting a Watermark Extraction Task

Watermark extraction tasks that are being executed cannot be deleted.

- Step 1** [Log in to the management console](#).
- Step 2** Click  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** In the navigation pane, choose **Data Asset Protection > Database Watermark**.
- Step 5** Click the **Extract Watermark** tab.
- Step 6** Click **Delete** in the **Operation** column of the target task. You can also select multiple tasks and click **Batch Delete** to delete them.

NOTE

The deletion cannot be undone.

----End

7.2.3.2 Extracting Watermarks from Documents

The content of invisible watermarks cannot be seen and needs to be extracted using tools. This section describes how to extract watermarks from a PDF, PPT, Word, or Excel file stored on the cloud (OBS buckets) or local PC.

Prerequisites

- OBS asset access permissions are granted. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- You have enabled and created assets on OBS. For details about how to enable OBS, see [Enabling and Using OBS Buckets](#).
- The file format is PDF, PPT, Word, or Excel.

Constraints


- This section focuses on the extractions of invisible watermarks from a single PDF, PPT, Word, or Excel file.

- The maximum size of a PDF or Word file is 50 MB.
- The maximum size of an Excel file is 70 MB.
- The maximum size of a PPT file is 20 MB.

Creating an OBS Bucket File Watermark Extraction Task

Step 1 [Log in to the management console.](#)

Step 2 Click  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 In the navigation tree on the left, choose **Data Asset Protection > Document Watermarking**. On the displayed page, click the **OBS File** tab.


Step 5 Click the **Watermark Extraction** tab. The **Watermark Extraction** page is displayed.

Step 6 Click **Create Task** in the upper left corner. The **Create Task** page is displayed.

Step 7 Click **Add File** to select the file from which you want to extract watermarks. You can select multiple OBS bucket files.

Step 8 Click **OK**. The watermark extraction task is created.

Step 9 Click the target task name. In the dialog box that is displayed, view the watermark extraction task status and the invisible watermark content of the OBS bucket file.


- **Running:** You can view the progress of the watermark extraction task.
- **Completed:** The watermark content is displayed in the **Invisible Watermarks** column. If there are no invisible watermarks, -- is displayed.
- **Failed:** The watermark extraction task fails to be executed. You can move the cursor to  to view the failure cause.

----End

Extracting Watermarks from Local Files

Step 1 [Log in to the management console.](#)

Step 2 Click  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 In the navigation tree on the left, choose **Data Asset Protection > Document Watermarking**. On the displayed page, click the **OBS File** tab.

Step 5 On the displayed page, choose **Local > Extract Watermark**. The **Extract Watermark** page is displayed.

Step 6 Upload the local file from which you want to extract the watermark text.

 NOTE

Only PDF, PPT, Word, and Excel files are supported.

Step 7 After the file is uploaded, click **OK**. The invisible watermark content is displayed in the dialog box.

----End

7.2.3.3 Extracting Watermarks from Images

The content of an invisible watermark remains unseen until it is retrieved through a specialized watermark extraction tool. The DSC console facilitates this process by offering a watermark extraction feature for images. Detailed instructions on how to extract watermarks from files stored in OBS buckets or from local files are provided in this section.

Prerequisites

- OBS asset access permissions are granted. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- You have enabled and created assets on OBS. For details about how to enable OBS, see [Enabling and Using OBS Buckets](#).
- Currently, the following image format is supported: .jpg, .jpeg, .jpe, .png, .bmp, .dib, .rle, .tiff, .tif, .ppm, .webp, .tga, .tpic, .gif.
- The resolution of the original image must be greater than 128 x 128 pixels.


Constraints

- Extract invisible watermarks from a single image file.
- The maximum size of an image is 20 MB.
- The invisible watermark content contains a maximum of 32 bytes.

Extracting Watermarks from an OBS Bucket File

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation tree on the left, choose **Data Asset Protection > Document Watermarking**. On the displayed page, click the **OBS File** tab.

Step 5 Click the **Watermark Extraction** tab. The **Watermark Extraction** page is displayed.

Step 6 Select the content to be extracted.

- If **Extract Content** is set to **Text**, click **Add** to select the image from which the watermark is to be extracted.

Figure 7-41 Extracting text content

The screenshot shows the 'Extract Watermark' dialog box with the 'Extracted Content' set to 'Text'. The 'Select File' field contains 'a-real-bucket/1123.jpg' and an 'Add' button is visible to its right. Below the field, a note states: 'The image file name extension must be jpg, jpeg, jpe, png, bmp, dib, rle, tiff, tif, ppm, webp, tga, tpic, or gif, and the image size cannot exceed 20 MB.' An 'OK' button is at the bottom.

- If **Extract Content** is set to **Image**:
 - Click **Add** next to **Select File** and select the image from which you want to extract watermarks.
 - Click **Add** next to **Storage Destination Path** and select the path for storing the extracted watermark image.
 - Click **Save Target File Name** and enter the file name of the watermark image to be extracted.

Figure 7-42 Extracting image content

The screenshot shows the 'Extract Watermark' dialog box with the 'Extracted Content' set to 'Image'. The 'Select File' field contains 'dsc/babybear.PNG' and an 'Add' button (2) is to its right. The 'Target Storage Path' field contains 'dsc/dameng/' and an 'Add' button (3) is to its right. The 'Target Storage File' field contains '1.jpg' (4). A red box (1) highlights the 'Image' radio button. A note below the 'Select File' field states: 'The image file name extension must be jpg, jpeg, jpe, png, bmp, dib, rle, tiff, tif, ppm, webp, tga, tpic, or gif, and the image size cannot exceed 20 MB.' An 'OK' button is at the bottom.


Step 7 Click **OK**. If the **Extract Content** is **Text**, the invisible watermark content is displayed in the dialog box. If the **Extract Content** is **Image**, view the image in the target storage path.

----End

Extracting Watermarks from a Local File

Step 1 [Log in to the management console.](#)

Step 2 Click  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 In the navigation tree on the left, choose **Data Asset Protection > Document Watermarking**. On the displayed page, click the **OBS File** tab.

Step 5 On the displayed page, choose **Local > Extract Watermark**. The **Extract Watermark** page is displayed.

Step 6 Select the **Extract Content**.

- If the **Extract Content** is **Text**, click **Upload File** to upload the local image whose invisible watermark needs to be extracted to the DSC platform.
- If the **Extract Content** is **Image**, click **Upload File** to upload the image whose invisible watermark needs to be extracted from the local host to the DSC platform.

Step 7 After the file is uploaded, click **OK**. The invisible watermark content is displayed in the dialog box.

----End

7.3 (Optional) Configuring GaussDB(DWS) and MRS Hive

Before using database watermarks, you have to:

1. **Modify GaussDB(DWS) cluster parameters.**

To identify sensitive data and enable privacy protection, you must [submit a service ticket](#) to adjust the parameter **javaudf_disable_feature** of the GaussDB(DWS) cluster. If GaussDB(DWS) data is not involved, you do not need to change the value.


2. **Modify Hive User Rights**

To perform data watermark operations on MRS Hive data, you must assign related permissions to Hive users as the administrator **Ranger**.

Modifying Hive User Rights

Step 1 [Log in to the management console.](#)

Step 2 Click  in the upper left corner and select a region or project.

Step 3 In the navigation tree on the left, click , and choose **Analytics > MapReduce Service**. The **Dashboard** page is displayed.

Step 4 In the cluster list, click the name of the target cluster. The cluster information page is displayed.

- Step 5** Click **Access Manager** next to **MRS Manager**. In the dialog box that is displayed, click **OK**. The Manager login page is displayed.
- Step 6** Enter the default username **admin** and the password set during cluster creation, and click **Log In**. The Manager page is displayed.
- Step 7** Choose **Cluster > Service > Ranger**. The Ranger service overview page is displayed.
- Step 8** Click **RangerAdmin** in the **Basic Information** area to go to the Ranger web UI. The type of the **admin** user in the Ranger is **User**. Therefore, only the **Access Manager** and **Security Zone** pages can be viewed. You need to switch to the **rangeradmin** user or another user who has the Ranger administrator rights.
1. On the Ranger WebUI, click the username in the upper right corner and choose **Log Out** to log out the current user.
 2. Log in to the system again as user **rangeradmin** or another user who has the Ranger administrator rights.
- Step 9** On the home page, click the plug-in name in the **HADOOP SQL** area, for example, **Hive**.
- Step 10** On the **Access** tab page, click **Add New Policy** to add a Hive permission control policy.
- Step 11** Set related parameters based on permission requirements. Set the key parameters described in [Table 7-25](#). Retain the default values for other parameters.

Table 7-25 Hive permission parameters

Parameter	Description	Example Value
Policy Name	Policy name, which can be customized and must be unique in the service.	dataarts_dsc
Database	Name of the Hive database to which the policy applies Change database to global . *, the policy takes effect globally.	global: *

Parameter	Description	Example Value
Allow Conditions	<p>Policy allowed condition. You can configure permissions and exceptions allowed by the policy. In the Select Role, Select Group, and Select User columns, select the role, user group, or user to which the permission is to be granted, click Add Conditions, add the IP address range to which the policy applies, and click Add Permissions to add the corresponding permission.</p> <p>You need to configure the Select Group, Select User, and Add Permissions columns.</p> <ul style="list-style-type: none"> • Select Group: Select the user group you want to use to watermark MRS Hive data. • Select User: Select the user you want to use to watermark MRS Hive data. If the user is already in the selected user group, you do not need to select it again. • Add Permissions: Select Select/Deselect All to select all permissions. 	<p>Example:</p> <ul style="list-style-type: none"> • Select Group: dayu_user • Select User: dgc_test • Add Permissions: All

Step 12 Click **Add** to view the basic policy information.

----End

8 Data Security Operations

8.1 Situational Awareness Dashboard

There are always such scenarios as presentation, reporting, or real-time monitoring where you need to present the analysis results of DSC on large screens to achieve better demonstration effect. It is not ideal to just zoom in the console. Now, DSC **Dashboard** is a good choice for you to display the service console on bigger screens for a better visual effect.

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.


Prerequisites

- Cloud asset access permissions are granted. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- The DBSS service has been enabled. For details, see [Purchasing Database Audit](#).

Procedure

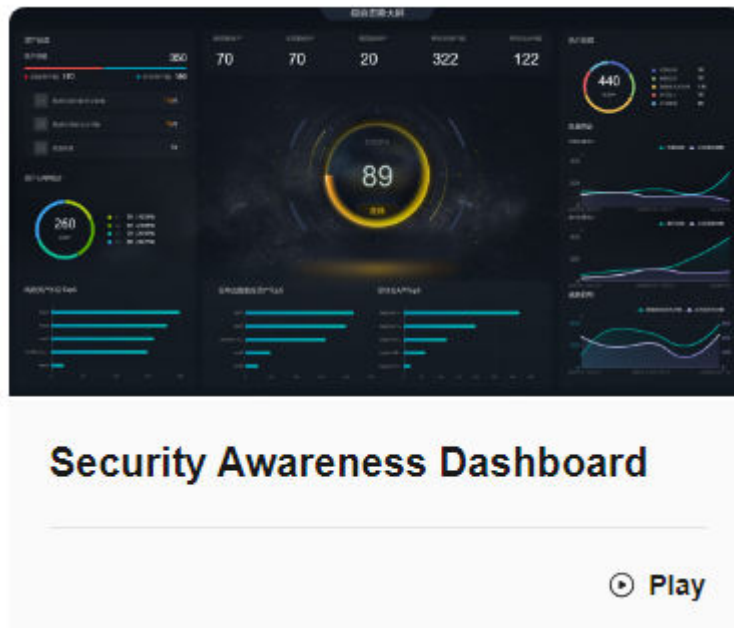
Step 1 [Log in to the management console](#).

Step 2 Click  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**.

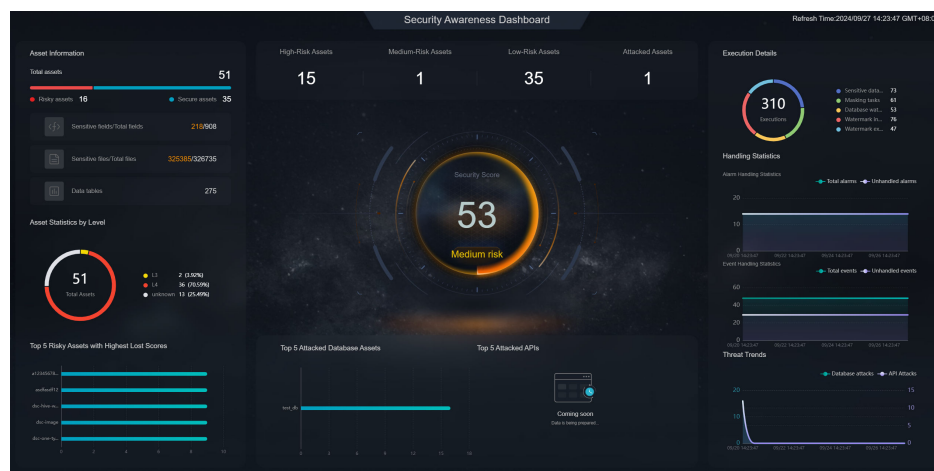
Step 4 In the navigation tree on the left, choose **Data Security Operations > Dashboard**. The **Dashboard** page is displayed.

Figure 8-1 Situational Awareness Dashboard



Step 5 Click the **Dashboard** image. The **Dashboard** page is displayed.
This dashboard includes many graphs.

Figure 8-2 Security awareness dashboard



----End

Security Score

The security scores of all assets are displayed, as shown in [Figure 8-3](#).

Table 8-1 Secure score

Parameter	Source	Description
Security Score	Score on the asset map	<p>For details about the score calculation rules, see Viewing Scoring Rules. The criteria for classifying high, medium, and low risks in the final score are as follows:</p> <ul style="list-style-type: none"> • 100: no risk • 81-99: low risk • 51-80: medium risk • 0-50: high risk

Figure 8-3 Security score



Risky Asset Statistics

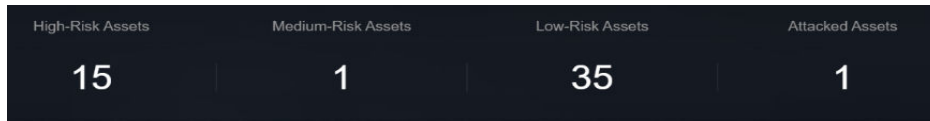
Risk statistics of authorized assets are displayed, as shown in [Figure 8-4](#).

Risky asset statistics come from the **asset map**. To view asset details, go to this [page](#).

Table 8-2 Security score

Parameter	Source	Description
High/Medium/Low-risk assets	Risk level in Protection Policy Analysis	For details about the calculation rules, see Risk Statistics .
Attacked assets	Alarms in Data Security Operations > Alarm Management	Analyze the number of attacked assets based on alarms in Alarm Management .

Figure 8-4 Risky asset statistics



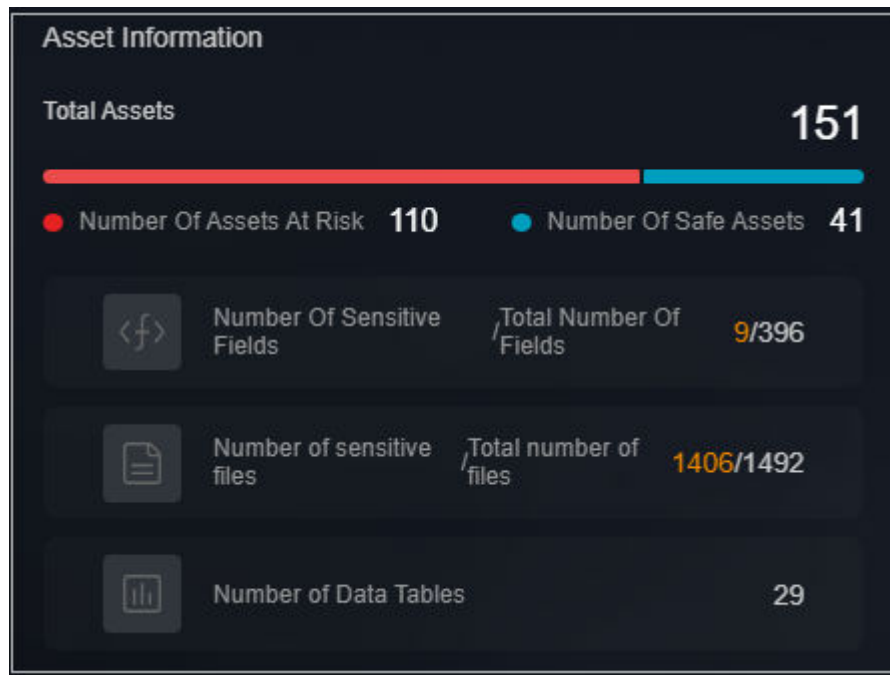
Information

The total number of assets and the identified high-, medium, and low-risk assets are displayed, as shown in [Figure 8-5](#).

Table 8-3 Asset information

Parameter	Source	Description
Total assets	Sum of high-risk, medium-risk, and low-risk assets.	-
Risky assets	Sum of high- and medium-risk assets.	-
Secure assets	Number of low-risk assets.	-
Sensitive fields/Total fields	Sensitive data identification	Total number of sensitive data fields/Total number of fields.
Sensitive files/Total files	Sensitive data identification	Total number of sensitive data files in OBS assets/ Total number of files.
Data tables	Total number of sensitive data tables.	Total number of sensitive data tables.

Figure 8-5 Asset information



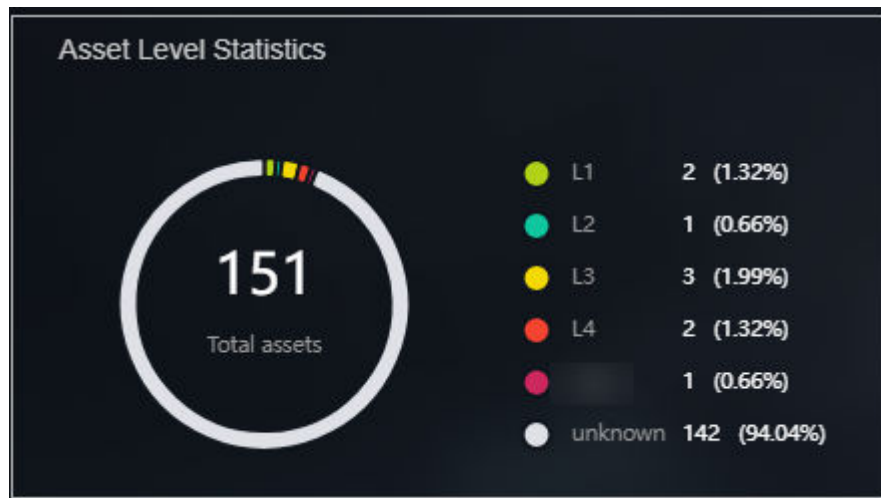
Asset Statistics by Level

The total number of assets that have been categorized and leveled through sensitive data identification, and the number and proportion of assets at each level are displayed, as shown in [Figure 8-6](#).

Table 8-4 Asset information

Parameter	Data Scope	Description
Total assets	Asset map	Total number of assets that are categorize and leveled using the sensitive data identification function.
Level	Sensitive data identification	Number of assets at each level and the proportion of each asset to the total assets.

Figure 8-6 Asset statistics by level



Top 5 Risky Assets with Highest Lost Scores

The top 5 assets with the highest lost scores are displayed. When you move the cursor to the bar chart, the asset name, asset type, data source, and score loss are displayed, as shown in [Figure 8-7](#).

Table 8-5 Asset information

Parameter	Source	Description
Risky asset score loss	Asset map	The asset name , asset type , data source , and score deduction of a single asset are displayed based on the score loss rules in the asset scoring rules. The details about the score deduction rules are described on the console. For details, see Viewing Scoring Rules .

Figure 8-7 Top 5 Risky Assets with Highest Lost Scores



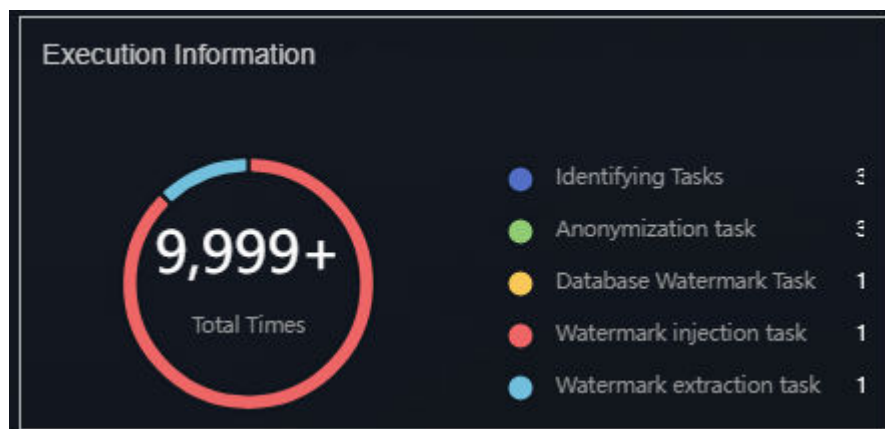
Execution Information

The total number of executed tasks is displayed, including sensitive data identification, static data masking, and data watermarking tasks are displayed, as shown in [Figure 8-8](#).

Table 8-6 Task execution information

Parameter	Source	Description
Total executions	Sensitive data identification, static data masking, and data watermarking	Total number of executed tasks.

Figure 8-8 Task execution information



Handling Statistics

- Alarm Handling Statistics

Displays the total number of alarms and the number of unhandled alarms from the **Alarm Management** page by time.

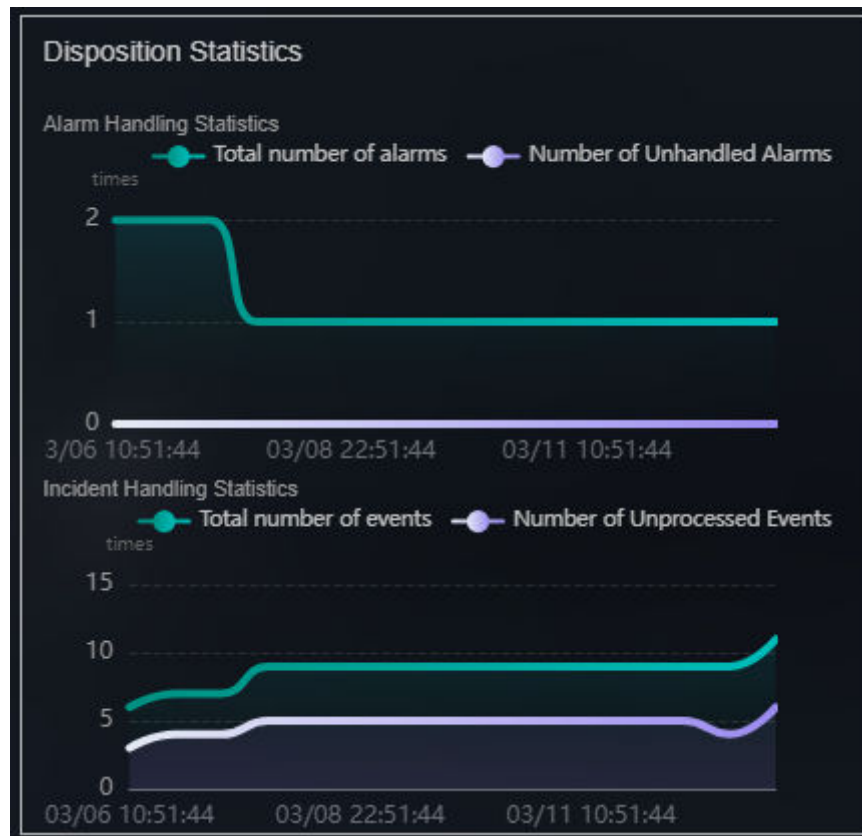
- Event Handling Statistics

Displays the total number of events and the number of unhandled events from the **Event Management** page by time.

Table 8-7 Task execution information

Parameter	Source	Description
Total alarms	Alarm Management module	Total number of alarms in the alarm list on the Alarm Management page
Unhandled alarms	Alarm Management	Number of alarms whose status is enabled in the alarm list on the Alarm Management page
Total events	Event Management module	Total number of events in the event list on the Event Management page
Unhandled events	Event Management module	Number of events whose status is enabled and blocked in the alarm management list.

Figure 8-9 Handling Statistics



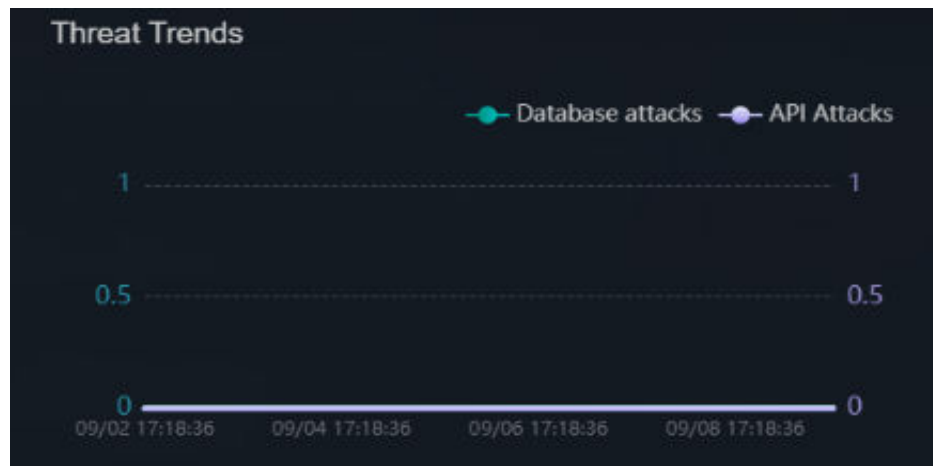
Threat Trends

The number of database attacks and the number of API attacks are displayed by time, as shown in [Figure 8-10](#).

Table 8-8 Task execution information

Parameter	Source	Description
Database attacks	Alarm Management module	Analyze the number of database attacks based on the alarms on the Alarm Management page.

Figure 8-10 Threat Trends



Top 5 Attack Targets

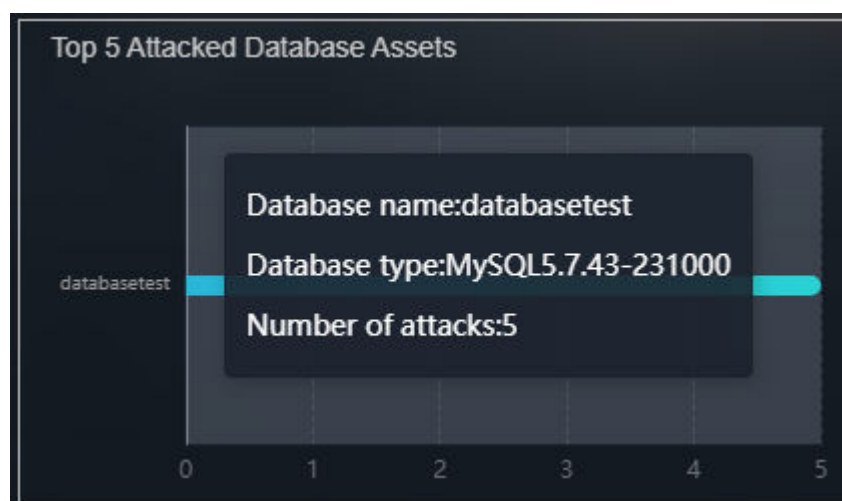
Table 8-9 Top 5 attack targets

Parameter	Source	Description
Top 5 attacked database assets	Alarm Management module	Analyze and display top 5 attacked database assets based on alarms on the Alarm Management page.

Top 5 Attacked Database Assets

The top 5 attacked database assets are displayed. When you move the cursor to the bar chart, the **Database**, **Database type**, and **Number of attacks** are displayed, as shown in [Figure 8-11](#).


Figure 8-11 Top 5 attacked database assets



8.2 Data Transfer Details


Full-link cloud data flow monitoring includes the following phases:


- Analyze the transfer paths between the cloud database, the data source, and the destination host based on the database audit logs.
- Finally, use full-link association analysis to measure and map the complete data transfer path on the cloud in real time.

After you enable the collection of data flow logs of an instance in , DSC performs data flow analysis on the collected logs and draws a flow diagram. It calculates various metrics based on the log data and saves the results.

Viewing Data Transfer Analysis

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

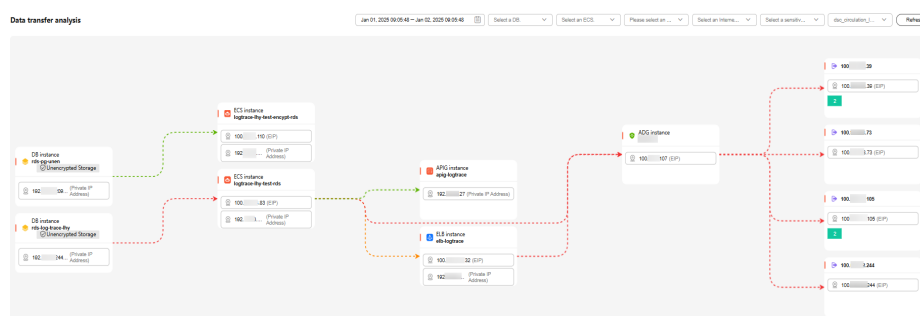
Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation tree on the left, choose **Data Security Operations > Data Transfer Details**. The **Data Transfer Analysis** page is displayed.

When you hover over the transfer stream, the system shows whether the data is encrypted for transmission and the total number of access instances. A red arrow signifies that data is not encrypted, a green arrow means that data is encrypted, and a yellow arrow indicates that data is partially encrypted. The encryption status of the connection line indicates the current encryption status.

Figure 8-12 Data transfer analysis



Step 5 **Select a time range:** Click to select a time range.

Select a DB: Select the database to be viewed.

Select an ECS: Select an ECS from the drop-down list box.

Select an egress type: Select ELB or APIG from the drop-down list box.

Select an external IP address: Select an external IP address from the drop-down list.

Select a sensitivity level: Select a sensitivity level from the drop-down list.

Select a sensitivity label: Select a sensitivity label from the drop-down list.

----End

8.3 Event Management

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.

Prerequisites

The DBSS service has been enabled and there are available assets on it. For details, see [Purchasing Database Audit](#).

Creating an Event



- Step 1** [Log in to the management console](#).
- Step 2** Click  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** In the navigation tree on the left, choose **Data Security Operations > Event Management**. The **Event Management** page is displayed.
- Step 5** Click **Create** in the upper left corner. The page for creating an event is displayed.
- Step 6** Set the event parameters based on [Table 8-10](#).

Table 8-10 Event parameters

Parameter	Description
Event Name	The value can contain 4 to 255 characters, including letters, digits, hyphens (-), and underscores (_), and must start with a letter.

Parameter	Description
Type	Select an event type from the drop-down list box. <ul style="list-style-type: none">• Databases<ul style="list-style-type: none">- SQL Injection- Risky operations• Application APIs<ul style="list-style-type: none">- Unauthorized access- Login security- Interface security- Service security- Data security
Event Level	Select an event level from the drop-down list box. <ul style="list-style-type: none">• Suggestion• Low• Medium• High• Critical
Status	Select a status from the drop-down list box. <ul style="list-style-type: none">• Open• Blocked• Closed
Module	Select a source function module from the drop-down list box. <ul style="list-style-type: none">• Database auditor• Cloud bastion host
Instance	Select an event source instance from the drop-down list box.
Owner	Select an event handling owner from the drop-down list box.
Affected Assets (Optional)	Enter the information about the assets affected by the event.
Occurred On	Time when an event occurs for the first time.
Planned Closure Time	Time when an event is planned to be closed.
Recommended Handling Method (Optional)	Enter the recommended event handling method. A maximum of 1000 characters can be entered.

Parameter	Description
Verification Status	Select an event verification status from the drop-down list box. <ul style="list-style-type: none"> • Unknown • Confirmed • False
Description	Enter the event description.


Step 7 Click **OK**.

----End

Viewing the Event Management List

Step 1 [Log in to the management console](#).

Step 2 Click  in the upper left corner and select a region or project.

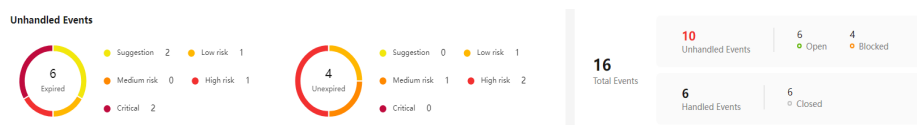
Step 3 In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation tree on the left, choose **Data Security Operations > Event Management**. The **Event Management** page is displayed.

Step 5 View the number of unhandled events and the total number of events.

The doughnut chart displays the number of expired and unexpired events.

Figure 8-13 Event handling statistics



Step 6 View the alarm list. For details about the parameters, see [Table 8-11](#).

Table 8-11 Data risk event parameters

Parameter	Description
Event Name/ID	<ul style="list-style-type: none"> • Name of an event. The event name should denote the content of the event. You can click the event name on the right of the event name to view the basic information, handling suggestions, and associated alarms of the event. • Click the event name to view the event details.

Parameter	Description
Event Level	There are five event levels: <ul style="list-style-type: none">• Suggestion• Low• Medium• High• Critical
Subcategory/Category	Event sources are classified into the following categories: <ul style="list-style-type: none">• Database attacks• API attacks
Source	Database Audit, Database Security Gateway, and API Security Gateway instances
Status	The status options are: <ul style="list-style-type: none">• Open• Blocked• Closed
Affected Assets	Affected database assets or APIs.
Verification Status	Its value can be: <ul style="list-style-type: none">• Unknown• Confirmed• False
Owner	Username.
Created	Event creation time
Occurred On	Time when an event occurs for the first time.
Planned Closure Time	Time when an event is planned to be closed.

----End

Related Operations

- Close
 - Click **Close** in the Operation column of the alarm list to disable the alarm.
- Edit
 - Click **Edit** in the **Operation** column of the alarm list to edit the alarm.
- Delete
 - Click **Delete** in the **Operation** column of the alarm list to delete the alarm.

8.4 Alarm Management

When a system or service alarm is generated from the DBSS service, the alarm is pushed to the DSC in real time. Users can check and handle the alarm. Alarms are stored in the DSC for 30 days.

Prerequisites

The DBSS service has been enabled and there are available assets on it. For details, see [Purchasing Database Audit](#).

Procedure



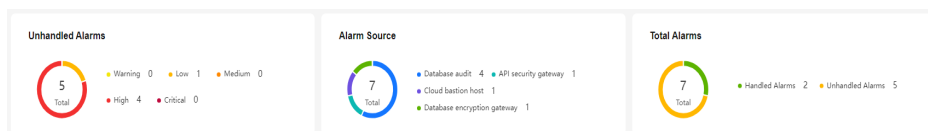
- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner and select a region or project.
- Step 3** In the navigation tree on the left, click . Choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation tree on the left, choose **Data Security Operations > Alarm Management**. The **Alarm Management** page is displayed.
- Step 5** You can view the unhandled alarms, alarm sources, and total number of alarms.

Figure 8-14 Alarm doughnut chart



- Step 6** View the alarm list. For details about the parameters, see [Table 8-12](#).

Table 8-12 Data risk alarm parameters

Parameter	Description
Alarm Name/ID	Indicates the name of the alarm source. An alarm should denote the content of the alarm. You can click an alarm name to view details about the alarm, including basic alarm information, handling suggestions, and attack information.
Alarm Level	There are 5 alarm severity levels: <ul style="list-style-type: none"> ● Suggestion ● Low ● Medium ● High ● Critical

Parameter	Description
Subcategory/Category	Alarm source types are as follows: <ul style="list-style-type: none">• Database attacks• API attacks
Source	Database Audit instances
Status	The status options are: <ul style="list-style-type: none">• Open• Blocked• Closed
Affected Assets	Affected database assets.
Verification Status	Its value can be: <ul style="list-style-type: none">• Unknown• Confirmed• False
Owner	Username.
Created	Time the alarm was created.
Occurred On	Time when an alarm occurs for the first time.

----End

Related Operations

- Convert to event.
 - a. Click **Convert to Event** in the **Operation** column of the alarm list. The **Convert to Event** page is displayed.
 - b. Enter the parameters, as shown in [Table 8-13](#).

Table 8-13 Parameters for converting an alarm to an event

Parameter	Description
Event Name	Enter the event name.
Event Type	Select an event type from the drop-down list box.
Planned Closure Time	Select the time when the event is closed.

- c. Click **OK** to convert an alarm to an event. You can view the converted event on the **Event Management** page.
- Close
Click **Close** in the Operation column of the alarm list to disable the alarm.

- Edit
Click **More** > **Edit** in the **Operation** column of the alarm list to edit the alarm.
- Delete
Click **More** > **Delete** in the **Operation** column of the alarm list to delete the alarm.

8.5 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.

Prerequisites

- An abnormal event has been detected and displayed on the page.
- The OBS audit function has been enabled in the asset center.


NOTE

- After OBS audit is enabled, you will be charged for reading and writing logs using the logging function of OBS. For details about the fees, see [Requests](#).
- Sensitive data of OBS assets has been identified. For details about how to identify sensitive data, see [Creating an Identification Task](#).

Procedure

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation tree on the left, choose **Data Security Operation** > **OBS Usage Audit**. The **OBS Usage Audit** page is displayed. For details about the parameters, see [Table 8-14](#).

In the upper right corner of the list, select a time range, set the time period, and select an event type and status to query the abnormal behaviors you want to view.

Table 8-14 Parameters of detected risky behaviors

Parameter	Description
User ID	ID of a resource owner

Parameter	Description
Event Type	DSC classifies abnormal events into the following three types: <ul style="list-style-type: none">• Unauthorized data access<ul style="list-style-type: none">- Access sensitive files without granted permissions.- Download sensitive files.• Abnormal data operations<ul style="list-style-type: none">- Update sensitive files.- Append data to sensitive files.- Delete sensitive files.- Copy sensitive files.• Abnormal data management<ul style="list-style-type: none">- When a bucket is added, the system detects that the bucket is a public read or a public read/write bucket.- When a bucket is added, the system detects that the access/ACL access permissions of a private bucket are granted for anonymous users or registered user groups.- The policy of a bucket containing sensitive files is changed or deleted.- The ACL of a bucket containing sensitive files is changed or deleted.- The cross-region replication configuration of a bucket containing sensitive files is modified or deleted.- The ACL of a sensitive file is modified or deleted.
Event Name	Event that causes an exception
Alarm Time	Time when an exception occurs
Status	Status description is as follows: <ul style="list-style-type: none">• Unhandled: indicates that an abnormal event is not handled.• Confirmed Violation: indicates that a handled abnormal event causes an exception.• Confirmed Non-violation: indicates that a handled abnormal event does not cause any exceptions.

Step 5 Click **View Details** in the **Operation** column of an abnormal event to view details about the event.

- Step 6** In the **Operation** column of the abnormal event, click **Handle** to handle the event. The handling method is as follows:
- The event is confirmed as a violation.
Should a policy violation occur and remain unhandled, DSC will persistently alert the event.
 - The event is deemed normal and requires no action.
It can be configured to be ignored. Once set, DSC will cease alerts for this event, and it will not appear in the list of abnormal events.

----End

8.6 Watermarks

8.6.1 Extracting Watermarks from Databases

Prerequisites

- Access to cloud assets has been authorized. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- An RDS or GaussDB(DWS) database has been authorized. For details, see [Adding Self-Built Database Instances](#).
- An MRS database has been authorized. For details, see [Authorizing Access to a Big Data Asset](#).
- You have configured the GaussDB(DWS) and MRS_Hive permissions. For details, see [\(Optional\) Configuring GaussDB\(DWS\) and MRS Hive](#).


Constraints

- The source file must be in CSV format and cannot be larger than 20 MB.
- The table may contain more than 1,500 rows of data.
- The CSV file content is encoded in UTF-8 mode. Ensure that the data is complete and correct.

Creating a Task

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation tree on the left, choose **Data Security Operations > Watermark Tracing**. The **Database Watermark Extraction** tab page is displayed.

Step 5 Click **Create Task**. In the displayed dialog box, set parameters based on [Table 8-15](#).

Table 8-15 Creating a watermark extraction task


Parameter	Description
Task Name	Enter a task name.
Source Files	The source file must be in CSV format and cannot be larger than 20 MB. The table may contain more than 1,500 rows of data. The CSV file content is encoded in UTF-8 mode. Ensure that the data is complete and correct.
Extraction Mode	Select a watermark extraction mode from the drop-down list box. For lossy column embedding and lossless column embedding, extract watermarks by column. For lossless line embedding, extract watermarks by row.
Delimiter	Delimiters in a file. For example: comma (,)


Step 6 Click **OK**.

----End

Viewing Results

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation tree on the left, choose **Data Security Operations > Watermark Tracing**. The **Database Watermark Extraction** tab page is displayed.

Step 5 Locate a task and click **View Result** in the **Operation** column.


----End

Deleting a Watermark Extraction Task

Watermark extraction tasks that are being executed cannot be deleted.

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation tree on the left, choose **Data Security Operations > Watermark Tracing**. The **Database Watermark Extraction** tab page is displayed.

Step 5 Click **Delete** in the **Operation** column of the target task. You can also select multiple tasks and click **Batch Delete** to delete them.

 NOTE

The deletion cannot be undone.

----End

8.6.2 Extracting Watermarks from an OBS Bucket File

The content of invisible watermarks cannot be seen and needs to be extracted using tools. This section describes how to extract watermarks from a PDF, PPT, Word, or Excel file stored on the cloud (OBS buckets).

Prerequisites

- OBS asset access permissions are granted. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- OBS has been enabled and used.
- The file format is PDF, PPT, Word, or Excel.


Constraints

- This section describes how to extract invisible watermarks from PDF, PPT, Word, or Excel documents.
- The maximum size of a PDF or Word file is 50 MB.
- The maximum size of an Excel file is 70 MB.
- The maximum size of a PPT file is 20 MB.

Creating an OBS Bucket File Watermark Extraction Task

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation tree on the left, choose **Data Security Operations > Watermark Tracing**. The **Database Watermark Extraction** tab page is displayed.

Step 5 Click the **OBS File Watermark Extraction** tab.


Step 6 Click **Create Task** in the upper left corner. The **Create Task** page is displayed.

Step 7 Click **Add File** to select the file from which you want to extract watermarks. You can select multiple OBS bucket files.

Step 8 Click **OK**. The watermark extraction task is created.

Step 9 Click the target task name. In the dialog box that is displayed, view the watermark extraction task status and the invisible watermark content of the OBS bucket file.

- **Running**: You can view the progress of the watermark extraction task.
- **Completed**: The watermark content is displayed in the **Invisible Watermarks** column. If there are no invisible watermarks, -- is displayed.

- **Failed:** The watermark extraction task fails to be executed. You can move the cursor to  to view the failure cause.

----End

8.6.3 Extracting Watermarks from a Local File

The content of invisible watermarks cannot be seen and needs to be extracted using tools. This section describes how to extract watermarks from a local PDF, PPT, Word, or Excel file.

Prerequisites

- OBS asset access permissions are granted. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- OBS has been enabled and used.
- The file format is PDF, PPT, Word, or Excel.


Constraints

- This section describes how to extract invisible watermarks from PDF, PPT, Word, or Excel documents.
- The maximum size of a PDF or Word file is 50 MB.
- The maximum size of an Excel file is 70 MB.
- The maximum size of a PPT file is 20 MB.

Extracting Watermarks from a Local File

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation tree on the left, choose **Data Security Operations > Watermark Tracing**. The **Database Watermark Extraction** tab page is displayed.

Step 5 Click the **Local File Watermark Extraction** tab.

Step 6 Click **Upload File** to upload the local file from which you want to extract invisible watermarks.

NOTE

Only PDF, PPT, Word, and Excel files are supported.

Step 7 After the file is uploaded, click **OK**. The invisible watermark content is displayed in the dialog box.

----End

9 Alarm Notifications

DSC sends notifications through the notification method configured by users when sensitive data identification is completed or abnormal events are detected.

Prerequisites

The SMN service has been enabled.


Constraints

- Before using the alarm notification function, ensure that SMN has been enabled. The SMN service is a paid service. For price details, see [SMN Pricing Details](#).
- Before setting alarm notifications, you are advised to create a **message topic** in **Simple Message Notification** as the administrator. For details, see [Creating a Topic](#).

Procedure

Step 1 [Log in to the management console](#).

Step 2 Click  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 In the navigation pane, choose **Alarm Notifications**.

Step 5 Configure alarm notifications.  describes the parameters.

NOTE

The alarm notification is the default notification. If no topics have been, the default notification is used for data usage audit alarms.

Figure 9-1 Configuring alarm notifications

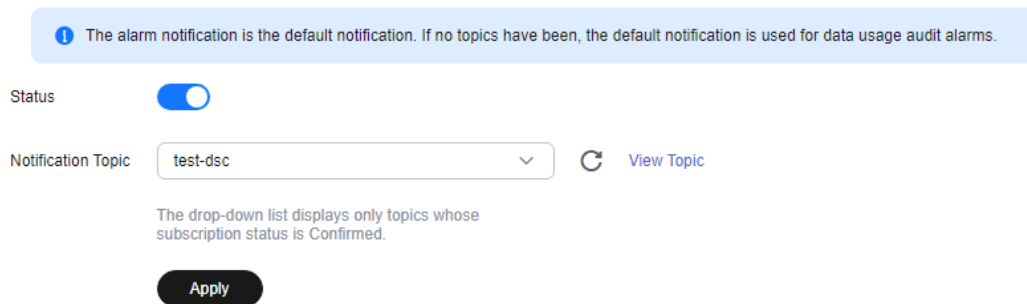




Table 9-1 Alarm notification parameters

Parameter	Description
Status	<p>Whether notification is enabled.</p> <ul style="list-style-type: none"> : enabled. : disabled.
Notification Topic	<p>Select an existing topic from the drop-down list or click View Topic to create a topic for receiving alarm notifications.</p> <p>Click View Topic and perform the following steps to create a topic:</p> <ol style="list-style-type: none"> Create a topic. For details, see Creating a Topic. You can add one or more subscriptions to a topic by configuring the phone number, email address, function, platform application endpoint, DMS endpoint, or HTTP/HTTPS endpoint for receiving alarm notifications. For details, see Adding a Subscription. Confirm the subscription. After the subscription is added, confirm the subscription. <p>For details about topics and subscriptions, see <i>Simple Message Notification User Guide</i>.</p>

Step 6 Click **Apply**.

----End

10 Multi-Account Management

10.1 Multi-Account Management Overview

With DSC, you can securely and reliably aggregate data and access resources across accounts. If your account is managed by an organization, you can also protect the data security of all member accounts without logging in to each one.

To use DSC to protect data security of organization member accounts, follow the following steps (using account A to show how to manage account B's assets):

1. If account A is an organization administrator, skip this step. If account A is not an organization administrator, the organization administrator should add account A as a delegated administrator. For details, see [Specifying a Delegated Administrator](#).

NOTE

The administrator can delegate the administrator rights to a member and revoke them. The right change takes effect after you refresh the page 1-2 minutes later.

2. The organization administrator or delegated administrator invites account B to join the organization. For details, see [Inviting an Account to Join Your Organization](#).
3. After account B is added to the organization, log in to DSC as account A and choose **Multi-Account Management** to view the asset information of account B.

For details, see [Overview of Organizations](#).

NOTE

To access the data asset information of account B, DSC automatically creates a service agency in account B.

- The agency is a cloud service associated agency. The **Identity Policy** in use is **DSCServiceLinkedAgencyPolicy**, and the agency is named **ServiceLinkedAgencyForDataSecurityCenter**. The authorization scope is **Creating, deleting, and querying a service agency, and binding the identity policy (DSCServiceAgencyPolicy) to the agency. (The creation and deletion of the agency are restricted to dsc_depend_agency_v5.)**
- If account B is deleted, DSC automatically deletes the DSC agency in account B.

10.2 Enable Multi-account Management

After the multi-account management function is enabled, the security administrator can protect the data of all member accounts without logging in to them. This section describes how to enable the multi-account management function.

Prerequisites

- The organization service has been enabled. For details see [Creating an Organization](#).
- DSC has been authorized as a trusted service. For details, see [Enabling or Disabling a Trusted Service](#).
- The account is an administrator or delegated administrator. If the account is not an administrator or delegated administrator, see section [Specifying a Delegated Administrator](#).


Constraints

After joining the organization, the administrator or service agency administrator can view and manage the assets of member accounts in the organization. You can switch accounts in the upper left corner of the menu bar to manage assets under a member account.

Procedure

Step 1 [Log in to the management console](#).

Step 2 Click  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 Choose **Multi-Account Management**.

Step 5 Choose **Enable Multi-Account Management** to enable the multi-account management function.

----End

10.3 Viewing Multi-Account Management

Prerequisites


- The organization service has been enabled. For details see [Creating an Organization](#).
- DSC has been authorized as a trusted service. For details, see [Enabling or Disabling a Trusted Service](#).

- The account is an administrator or delegated administrator. If the account is not an administrator or delegated administrator, see section [Specifying a Delegated Administrator](#).

Procedure

Step 1 [Log in to the management console](#).

Step 2 Click  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 Choose **Multi-Account Management**.

Step 5 The **Accounts** page is displayed. [Table 10-1](#) describes the parameters on the page.

Table 10-1 Account list

Parameter	Description
Account name	Name of the account that is invited to join the organization. For details, see Inviting an Account to Join Your Organization .
DomainId	Domain ID of the current account.
OBS assets	Number of OBS assets.
Database assets	Number of database assets.
Big data asset	Number of big data assets.
Operation	Click Go to View to go to the Asset Center page and view and manage related assets.

----End

11 Permissions Management

11.1 Creating a User and Assigning DSC Permissions

This section describes IAM's fine-grained permissions management for your DSC resources. With [IAM](#), you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to DSC resources.
- Grant only the permissions required for users to perform a task.
- Entrust a Huawei Cloud account or cloud service to perform professional and efficient O&M on your DSC resources.

If your Huawei Cloud account does not require individual IAM users, skip this section.

This section describes the procedure for granting permissions (see [Figure 11-1](#)).

Prerequisites

Learn about the permissions supported by DSC in [Table 11-1](#) and choose policies or roles based on your requirements.

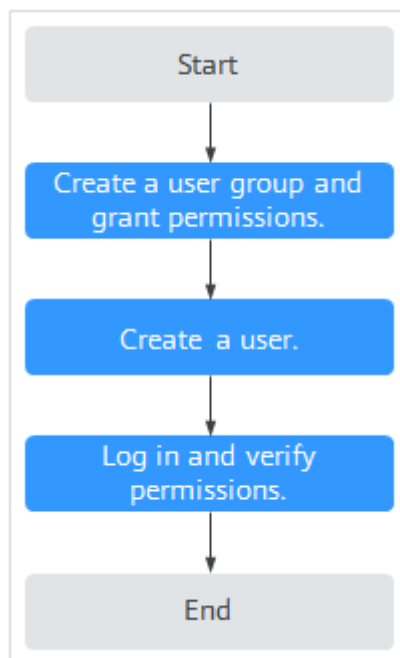
Table 11-1 DSC system permissions

Policy	Description	Type	Dependency
DSC DashboardReadOnlyAccess	Read-only permissions for the overview page of DSC	System-defined policy	None

Policy	Description	Type	Dependency
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

Process Flow

Figure 11-1 Process for granting permissions



1. **Create a user group and assign permissions..**
Create a user group on the IAM console, and assign the **DSC FullAccess** permissions to the group.
2. **Creating an IAM User.**
Create a user on the IAM console and add it to the group created in **1**.
3. **Logging In as an IAM User** and verify permissions.
Log in to the DSC console using the created user and verify that the user has administrator permissions for DSC.
Assume you are granted only the **DSC FullAccess** permission. Choose any other service in the **Service List**. If a message appears indicating insufficient

permissions to access the service, the permission setting has already taken effect.

11.2 DSC Custom Policies

Custom policies can be created to supplement the system-defined policies of DSC.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see [Creating a Custom Policy](#). The following section contains examples of common DSC custom policies.

Example Custom Policies

- Example 1: Allowing a user to query the big data assets

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dsc:bigdataAsset:list"
      ]
    }
  ]
}
```

- Example 2: Disallowing a user to query the OBS assets

A deny policy must be used together with other policies. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

The following method can be used if you need to assign permissions of the **DSC FullAccess** policy to a user but also forbid the user from querying the OBS asset list (`dsc:obsAsset:list`). Create a custom policy with the same action for denying querying the OBS asset list, and assign both policies to the group the user belongs to. Then, the user can perform all operations on DSC except querying the OBS asset list. The following is an example policy for denying querying OBS asset list.

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "dsc:obsAsset:list"
      ]
    },
  ]
}
```

- Multi-action policy

A custom policy can contain the actions of multiple services that are of the project-level type. The following is an example policy containing actions of multiple services:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dsc:obsAsset:list",
        "dsc:scanRule:list"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "hss:hosts:switchVersion",
        "hss:hosts:manualDetect",
        "hss:manualDetectStatus:get"
      ]
    }
  ]
}
```

11.3 DSC Permissions and Supported Actions

This section describes how to use IAM for fine-grained DSC permissions management. If your Huawei Cloud account does not need individual IAM users, skip over this section.

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

You can grant users permissions by using [roles](#) and [policies](#). Roles are provided by IAM to define service-based permissions depending on user's job responsibilities. Policies are a type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions

Supported Actions

DSC provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control.

- Permissions: Statements in a policy that allow or deny certain operations
- Actions: Added to a custom policy to control permissions for specific operations

Permission	Action
Querying the OBS asset list	dsc:obsAsset:list
Updating identification rules	scanRule:update
Adding big data assets	dsc:bigdataAsset:create
Viewing the identification rule list	dsc:scanRule:list

Permission	Action
Adding OBS assets	dsc:obsAsset:create
Querying the RDS DB instance list	dsc:rds:list
Deleting databases	dsc:databaseAsset:delete
Adding identification rules	dsc:scanRule:create
Deleting identification tasks	dsc:scanTask:delete
Querying DSC permissions	dsc:authorization:get
Querying RDS database list	dsc:rdsDatabase:list
Modifying identification tasks	dsc:scanTask:update
Querying the Cloud Search Service (CSS) list	dsc:css:list
Creating identification tasks	dsc:scanTask:create
Granting operation permissions to DSC users	dsc:authorization:grant
Querying the big data asset list	dsc:bigdataAsset:list
Querying the identification task list	dsc:scanTask:list
Adding databases	dsc:databaseAsset:create
Deleting identification tasks	dsc:scanRule:delete
Querying the database list	dsc:databaseAsset:list
Deleting OBS assets	dsc:obsAsset:delete
Deleting big data assets	dsc:bigdataAsset:delete
Operating DSC common resources	dsc:common:operate
Querying DSC common resources	dsc:common:list

12 Key DSC Operations

12.1 Operations Recorded by CTS

Cloud Trace Service (CTS) provides you with DSC operation records. After enabling CTS, you can view all generated traces to review and audit performed DSC operations. For details, see *Cloud Trace Service User Guide*.

Table 12-1 lists DSC operations recorded by CTS.

Table 12-1 DSC operations supported by CTS

Operation	Resource Type	Trace Name
Assign or revoke permissions for DSC	dscGrant	grantOrRevokeTodsc
Add an OBS bucket	dscObsAsset	addBuckets
Delete an OBS bucket	dscObsAsset	deleteBucket
Add a database	dscDatabaseAsset	addDatabase
Modify a database	dscDatabaseAsset	updateDatabase
Delete a database	dscDatabaseAsset	deleteDatabase
Add a big data source	dscBigdataAsset	addBigdata
Modify a big data source	dscBigdataAsset	updateBigdata
Delete a big data source	dscBigdataAsset	deleteBigdata

Operation	Resource Type	Trace Name
Update the object name	dscAsset	updateAssetName
Download a template for batch import	dscBatchImportTemplate	downloadBatchImportTemplate
Add databases in batches	dscAsset	batchAddDatabase
Add assets in batches	dscAsset	batchAddAssets
Display abnormal events	dscExceptionEvent	listExceptionEventInfo
Obtain the abnormal event details	dscExceptionEvent	getExceptionEventDetail
Add alarm configurations	dscAlarmConfig	addAlarmConfig
Change alarm configurations	dscAlarmConfig	updateAlarmConfig
Download a report	dscReport	downloadReport
Delete a report	dscReport	deleteReport
Add a scan rule	dscRule	addRule
Modify a scan rule	dscRule	editRule
Delete a scan rule	dscRule	deleteRule
Add a scan rule group	dscRuleGroup	addRuleGroup
Modify a scan rule group	dscRuleGroup	editRuleGroup
Delete a scan rule group	dscRuleGroup	deleteRuleGroup
Add a scan task	dscScanTask	addScanJob
Modify a scan task	dscScanTask	updateScanJob
Delete a scan subtask	dscScanTask	deleteScanTask
Delete a scan task	dscScanTask	deleteScanJob

Operation	Resource Type	Trace Name
Start a scan task	dscScanTask	startJob
Stop a scan task	dscScanTask	stopJob
Start a scan subtask	dscScanTask	startTask
Stop a scan subtask	dscScanTask	stopTask
Enable/disable data masking for Elasticsearch	dscBigDataMaskSwitch	switchBigDataMaskStatus
Obtain the Elasticsearch field	dscBigDataMetaData	getESField
Add an Elasticsearch data masking template	dscBigDataMaskTemplate	addBigDataTemplate
Modify an Elasticsearch data masking template	dscBigDataMaskTemplate	editBigDataTemplate
Delete an Elasticsearch data masking template	dscBigDataMaskTemplate	deleteBigDataTemplate
Query the Elasticsearch data masking template list	dscBigDataMaskTemplate	showBigDataTemplates
Enable or disable an Elasticsearch data masking template	dscBigDataMaskTemplate	operateBigDataTemplate
Switch the status of an Elasticsearch data masking template	dscBigDataMaskTemplate	switchBigDataTemplate
Enable or disable data masking for databases	dscDBMaskSwitch	switchDBMaskStatus
Obtain the database fields	dscDBMetaData	getColumn
Add a database masking template	dscDBMaskTemplate	addDBTemplate

Operation	Resource Type	Trace Name
Modify a database masking template	dscDBMaskTemplate	editDBTemplate
Delete a database masking template	dscDBMaskTemplate	deleteDBTemplate
Query the database masking template list	dscDBMaskTemplate	showDBTemplates
Start or stop a database data masking template	dscDBMaskTemplate	operateDBTemplate
Switch the status of a database data masking template	dscDBMaskTemplate	switchDBTemplate
Add a masking algorithm	dscMaskAlgorithm	addMaskAlgorithm
Edit a masking algorithm	dscMaskAlgorithm	editMaskAlgorithm
Delete a masking algorithm	dscMaskAlgorithm	deleteMaskAlgorithm
Test a masking algorithm	dscMaskAlgorithm	testMaskAlgorithm
Obtain the mapping between fields and masking algorithms	dscMaskAlgorithm	getFieldAlgorithms
Add encryption algorithm configurations	dscEncryptMaskConfig	addEncryptConfig
Modify encryption algorithm configurations	dscEncryptMaskConfig	editEncryptConfig
Delete encryption algorithm configurations	dscEncryptMaskConfig	deleteEncryptConfig

12.2 Viewing CTS Traces in the Trace List

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in Object Storage Service (OBS) buckets. Cloud Trace Service (CTS) stores operation records (traces) generated in the last seven days.

NOTE

These operation records are retained for seven days on the CTS console and are automatically deleted upon expiration. Manual deletion is not supported.


This section describes how to query or export operation records of the last seven days on the CTS console.




- [Viewing Real-Time Traces in the Trace List of the New Edition](#)
- [Viewing Real-Time Traces in the Trace List of the Old Edition](#)

Constraints


- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for longer than seven days, you must configure transfer to OBS or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.
- After performing operations on the cloud, you can query management traces on the CTS console one minute later and query data traces five minutes later.
- Data traces are not displayed in the trace list of the new version. To view them, you need to go to the old version.

Viewing Real-Time Traces in the Trace List of the New Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** **Management & Deployment** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
 - **Trace Name:** Enter a trace name.
 - **Trace ID:** Enter a trace ID.
 - **Resource Name:** Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API

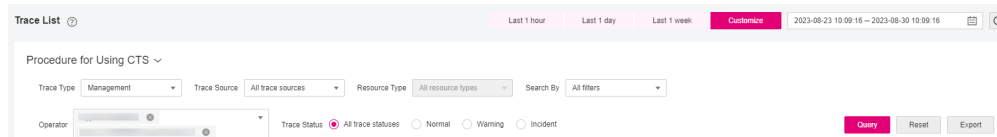
- operation does not involve the resource name parameter, leave this field empty.
- **Resource ID:** Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
 - **Trace Source:** Select a cloud service name from the drop-down list.
 - **Resource Type:** Select a resource type from the drop-down list.
 - **Operator:** Select one or more operators from the drop-down list.
 - **Trace Status:** Select **normal**, **warning**, or **incident**.
 - **normal:** The operation succeeded.
 - **warning:** The operation failed.
 - **incident:** The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
 - **Enterprise Project ID:** Enter an enterprise project ID.
 - **Access Key:** Enter a temporary or permanent access key ID.
 - **Time range:** Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
5. On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.
- Enter any keyword in the search box and press **Enter** to filter desired traces.
 - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
 - Click  to view the latest information about traces.
 - Click  to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled () , excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see [Trace Structure](#) section "Trace References" > "Trace Structure" and [Example Traces](#) section "Trace References" > "Example Traces".
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.



Viewing Real-Time Traces in the Trace List of the Old Edition

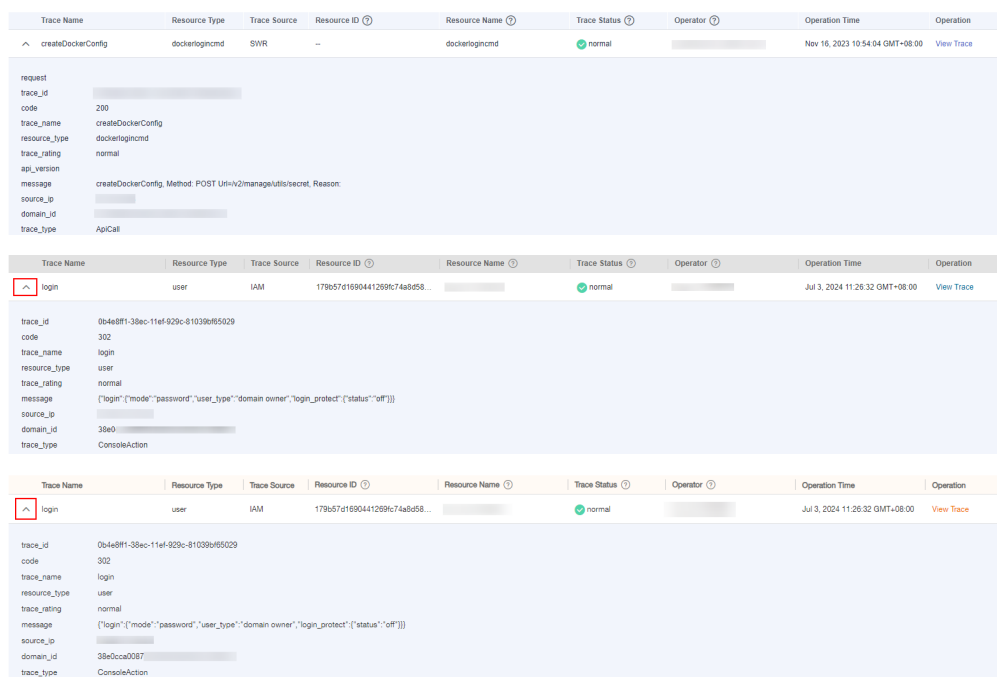
1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** **Management & Deployment** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.

- Set filters to search for your desired traces, as shown in **Figure 12-1**. The following filters are available.

Figure 12-1 Filters



- **Trace Type, Trace Source, Resource Type, and Search By:** Select a filter from the drop-down list.
 - If you select **Resource ID** for **Search By**, specify a resource ID.
 - If you select **Trace name** for **Search By**, specify a trace name.
 - If you select **Resource name** for **Search By**, specify a resource name.
 - **Operator:** Select a user.
 - **Trace Status:** Select **All trace statuses, Normal, Warning, or Incident**.
 - Time range: Select **Last 1 hour, Last 1 day, or Last 1 week**, or specify a custom time range within the last seven days.
- Click **Query**.
 - On the **Trace List** page, you can also export and refresh the trace list.
 - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.
 - Click  to view the latest information about traces.
 - Click  on the left of a trace to expand its details.



9. Click **View Trace** in the **Operation** column. The trace details are displayed.

View Trace ×

```
{
  "request": "",
  "trace_id": "XXXXXXXXXXXXXXXXXXXX",
  "code": "200",
  "trace_name": "createDockerConfig",
  "resource_type": "dockerlogincmd",
  "trace_rating": "normal",
  "api_version": "",
  "message": "createDockerConfig, Method: POST Url=/v2/manage/utis/secret, Reason:",
  "source_ip": "XXXXXXXXXXXX",
  "domain_id": "XXXXXXXXXXXXXXXXXXXX",
  "trace_type": "ApiCall",
  "service_type": "SWR",
  "event_type": "system",
  "project_id": "XXXXXXXXXXXXXXXXXXXX",
  "response": "",
  "resource_id": "",
  "tracker_name": "system",
  "time": "Nov 16, 2023 10:54:04 GMT+08:00",
  "resource_name": "dockerlogincmd",
  "user": {
    "domain": {
      "name": "XXXXXXXXXXXX",
      "id": "XXXXXXXXXXXXXXXXXXXX"
    }
  }
}
```

10. For details about key fields in the trace structure, see [Trace Structure](#) section "Trace References" > "Trace Structure" and [Example Traces](#) section "Trace References" > "Example Traces" in the *CTS User Guide*.
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.