

Data Security Center

User Guide

Issue 01
Date 2023-11-30



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. 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 Asset Map.....	6
3 Asset Management.....	12
3.1 Assets.....	12
3.1.1 Allowing or Disallowing Access to Cloud Assets.....	12
3.1.2 Adding Assets in Batches.....	16
3.1.3 OBS Assets.....	18
3.1.3.1 Adding OBS Assets.....	18
3.1.3.2 Deleting OBS Assets.....	20
3.1.4 Database Assets.....	21
3.1.4.1 Authorizing RDS Databases.....	21
3.1.4.2 Adding a Cloud Database.....	24
3.1.4.3 Adding a Self-Built Database.....	26
3.1.4.4 Editing a Database.....	29
3.1.4.5 Deleting a Database.....	30
3.1.5 Big Data Assets.....	32
3.1.5.1 Adding a Cloud ES Data Source.....	32
3.1.5.2 Adding a Self-Built ES Data Source.....	34
3.1.5.3 Adding a DLI Data Source.....	37
3.1.5.4 Adding a Hive Data Source.....	39
3.1.5.5 Adding an HBase Data Source.....	41
3.1.6 MRS Assets.....	43
3.1.6.1 Adding MRS Assets.....	43
3.1.6.2 Deleting MRS Assets.....	45
3.2 Metadata Tasks.....	46
3.2.1 Creating a Metadata Collection Task.....	46
3.2.2 Running a Metadata Collection Task.....	48
3.3 Data Exploration.....	50
3.4 Asset Catalog.....	51
4 Sensitive Data Identification.....	53

4.1 Overview of Sensitive Data Identification.....	53
4.2 Sensitive Data Identification Configuration.....	55
4.2.1 Creating an Identification Template.....	55
4.2.2 Modifying an Identification Template.....	57
4.2.3 Customizing a Rule.....	60
4.2.4 Editing a Rule.....	62
4.2.5 Customizing a Level.....	63
4.2.6 Modifying Level Information.....	64
4.2.7 Disabling a Level.....	65
4.3 Sensitive Data Identification Tasks.....	65
4.3.1 Creating an Identification Task.....	65
4.3.2 Starting a Task.....	68
4.3.3 Identification Tasks.....	69
4.3.4 Viewing the Identification Result.....	73
5 Data Privacy Protection.....	76
5.1 Configuring GaussDB(DWS) and MRS Hive.....	76
5.2 Data Masking.....	78
5.2.1 Overview.....	78
5.2.2 Configuring a Data Masking Rule.....	83
5.2.3 Managing Static Data Masking Tasks.....	91
5.2.3.1 Creating and Running a Database Masking Task.....	91
5.2.3.2 Creating and Running an Elasticsearch Data Masking Task.....	97
5.2.3.3 Creating and Running an MRS Data Masking Task.....	102
5.2.3.4 Creating and Running a Hive Masking Task.....	107
5.2.3.5 Creating and Running an HBase Masking Task.....	111
5.2.4 Dynamic Data Masking.....	115
5.3 Data Watermarking.....	116
5.3.1 Overview.....	116
5.3.2 Database Watermarking.....	117
5.3.2.1 Inserting Watermarks.....	117
5.3.2.2 Extracting Watermarks.....	126
5.3.3 Document Watermarking.....	129
5.3.3.1 Inserting Watermarks.....	129
5.3.3.2 Extracting Watermarks.....	134
6 Data Risk Detection.....	137
6.1 Viewing Abnormal Behaviors Through Data Usage Audit.....	137
6.2 Handling Abnormal Behaviors Found in Data Usage Audit.....	141
6.3 Viewing and Handling Access Key Leaks.....	142
7 Alarm Notifications.....	144
8 Permissions Management.....	146
8.1 Creating a User and Assigning DSC Permissions.....	146

8.2 DSC Custom Policies.....	148
8.3 DSC Permissions and Supported Actions.....	149
9 Key DSC Operations.....	151
9.1 Operations Recorded by CTS.....	151
9.2 Viewing Audit Logs.....	155
A Change History.....	157

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.

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.

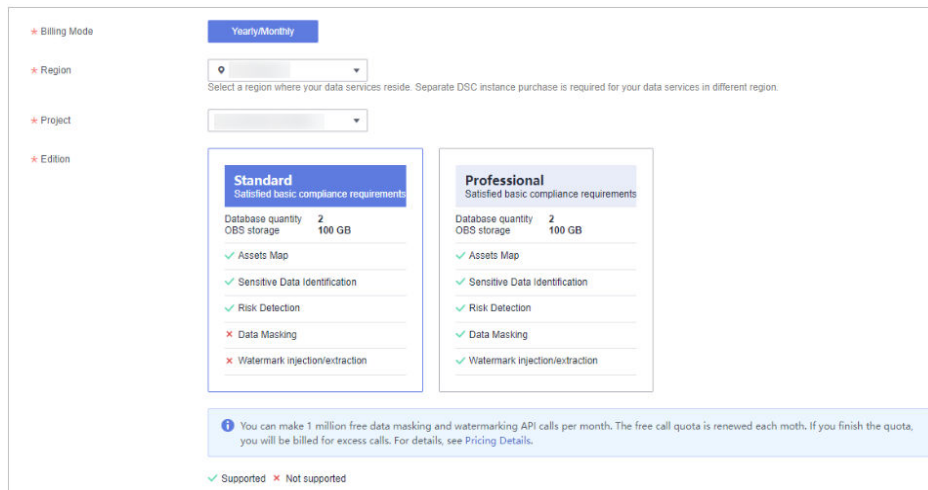
Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 4 If you are a first-time user, click **Buy DSC**.

Step 5 Select a region and edition on the displayed page.

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**.

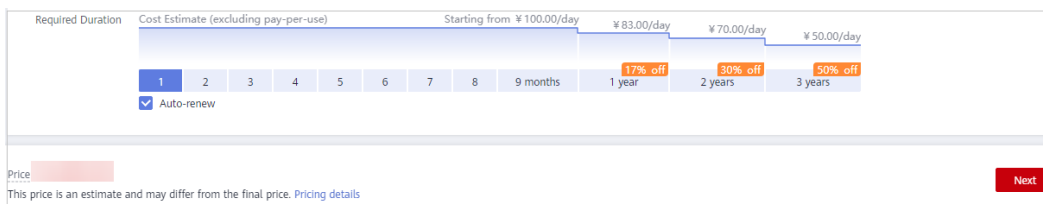
Figure 1-2 Selecting expansion packages



- 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.

Figure 1-3 Setting required duration



NOTE

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

Step 8 Click **Next**.

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

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

Figure 1-4 Viewing details

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

I have read and agree to the Data Security Center Service Statement.

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.
- 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 of the management console and select a region or project.

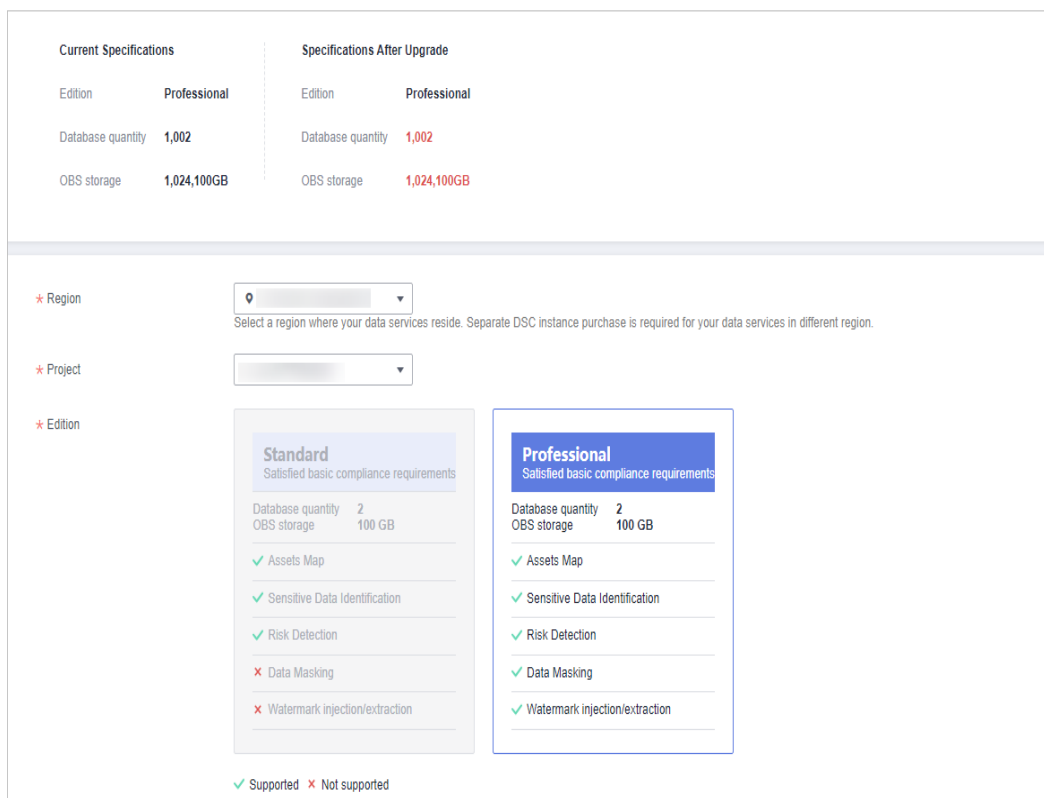
Step 3 In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.

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 1-5 Upgrading edition specifications



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

Figure 1-6 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**.

Figure 1-7 Viewing details

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

I have read and agree to the Data Security Center Service Statement.

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

----End

2 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.

Prerequisites

- Asset access permissions have been granted. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- You have added database assets to DSC. For details, see section [Database Assets](#).

Asset Map Functions

- **Sorted data assets:** Risky cloud data assets are sorted and displayed on an asset map, so that you know where the risky assets are.
- **Sensitive data display:** DSC displays sensitive data by classifications. 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.
- **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. For details about the scoring rules, see [Asset map scoring rules](#).
 - Risk Level: Assets are classified based on the detected risk levels to facilitate viewing and management. You can click the number above a risk level to view asset risk details.

Viewing Risk Statistics



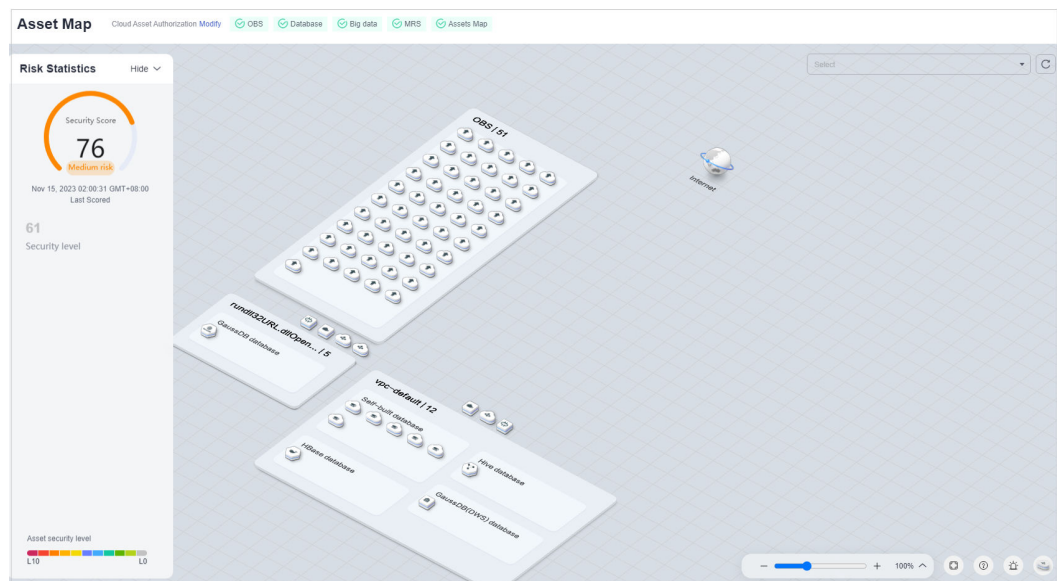
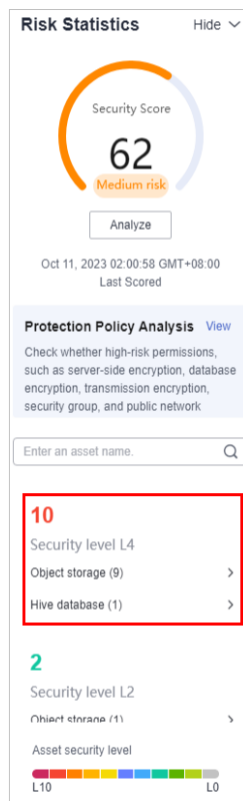
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region or project.
- Step 3** In the navigation tree on the left, click . Choose **Security and Compliance** > **Data Security Center**.
- Step 4** In the navigation pane, choose **Asset Map**.

Figure 2-1 Asset map



- Step 5** When you move the cursor to **Risk Statistics**, asset information under each **Security Level** is displayed.
 - You can click the search box to search for and view the risk level of an asset type.
 - Click **Analyze** to scan again. Move the cursor to the **Risk Statistics** tab to check whether the scanning is complete.
 - Click **View**. The **Protection Policy Analysis** dialog box is displayed. View details about risky configuration items, risk levels, and recommended configuration policies of assets, and click **Modify** or **View Details** in the **Operation** column to handle risky configuration items.

Figure 2-2 Risk Statistics

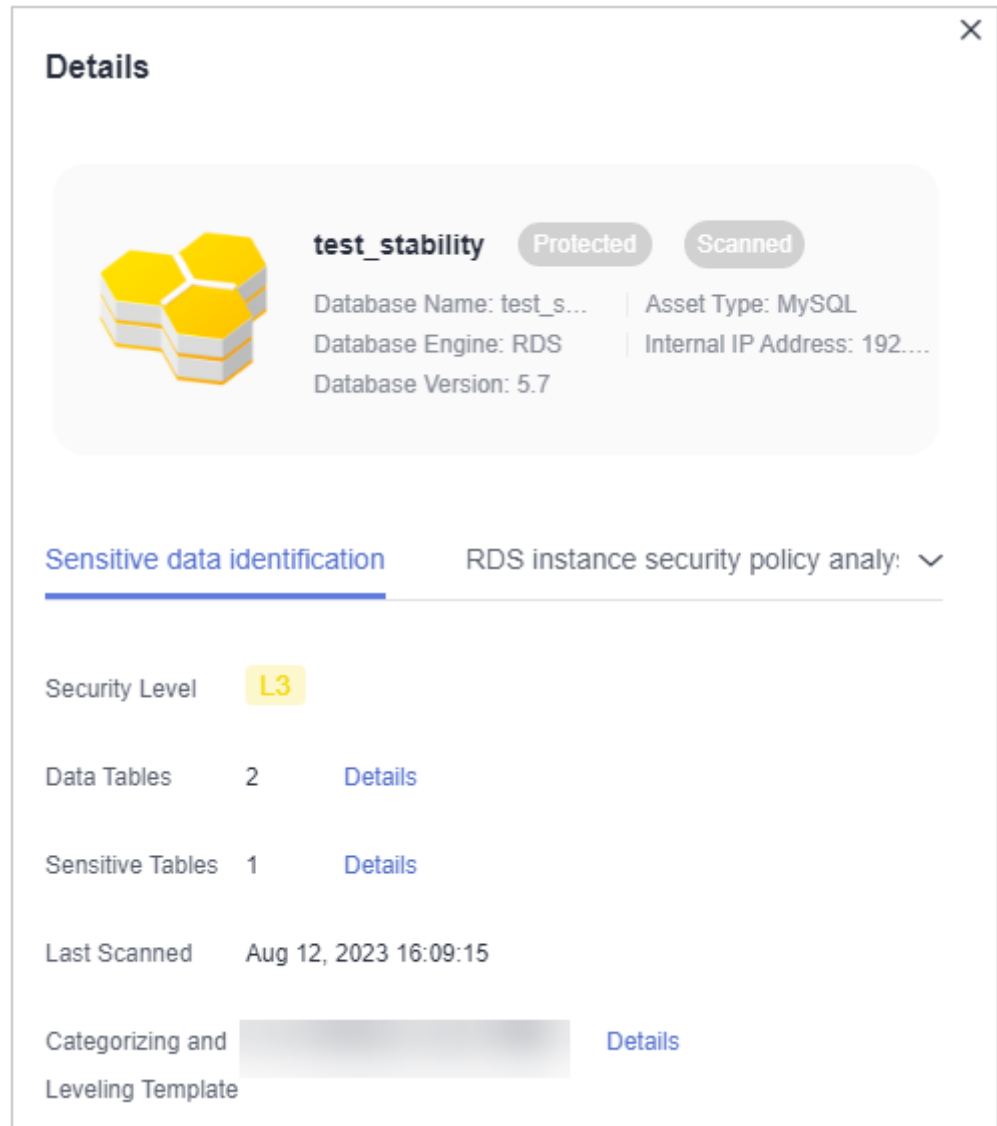


Step 6 Move the cursor to a risk data type on the **Risk Statistics** tab page. All risky assets of the data type are displayed in the dialog box on the right.

Step 7 Click the asset name. The data table details are displayed in the dialog box on the right.

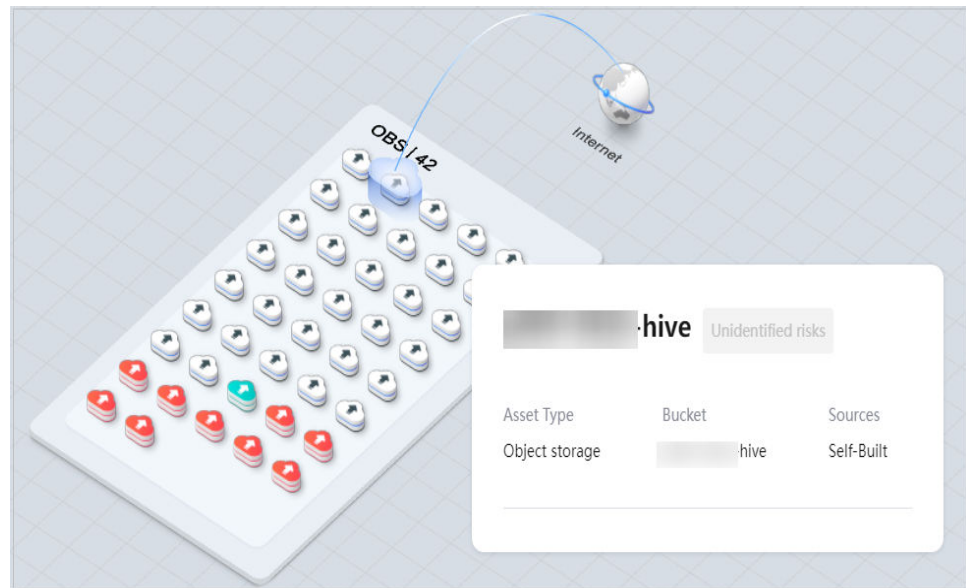
- Sensitive data identification: displays the risk level, total number of data tables, total number of sensitive tables, latest scanning time, and categorization and leveling template of the data table. You can click **Details** to go to the **Sensitive Data Identification** page. For details, see section [Sensitive Data Identification](#).

Figure 2-3 Sensitive object identification details



- 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 permission notifications. You can click **View** or **Modify** to handle the permissions.
- Data exit analysis: You can click the data table name to go to the **Details** dialog box and click the **Data exit analysis** tab to view the data exit details. You can also move the cursor to the data type icon or VPC icon on the asset map to view the data exit gateways.

Figure 2-4 Data exit analysis



----End





Asset map scoring rules

Risk score of an asset = Sensitivity level of the asset x Risk level of the asset x Coefficient score

- The sensitivity level of an asset is calculated as follows:
 - The sensitivity level of an OBS bucket is the maximum sensitivity level of all files in the bucket. The sensitivity level of a database or big data is the maximum sensitivity level of all tables.
 - The mapping between the score ranges (in the old version) and sensitivity levels is as follows: 8–10 points for high sensitivity, 4–7 points for medium sensitivity, and 1–3 points for low sensitivity.
- Asset risk level = MAX(Risk level score of the static asset configuration, Risk level score of the dynamic asset threats)
 - The risk level score of the static asset configuration is the maximum security level in the security protection policy analysis of the asset.
 - The risk level score of the dynamic asset threats is the maximum security level in the threat analysis of the asset.
 - The risk level scores are as follows:
 - Low risk: 1 point
 - Medium risk: 2 points
 - High risk: 3 points
- The coefficient score is related to the total number of assets. It is calculated as follows:
 - Assume that you have X assets, all of which have a high sensitivity and risk level. Your asset security score is 0, and risk score is 100 which is equal to $X \times 3 \times 3 \times Y$. Y is the coefficient score and is equal to $100/9X$.

- If all the X assets have a low sensitivity and risk level, the risk score is 11.1 which is equal to $X \times 1 \times 1 \times 100/9X$, and the security score is 88.9.
- If all the X assets have a medium sensitivity and risk level, the risk score is 44.4 which is equal to $X \times 2 \times 2 \times 100/9X$, and the security score is 55.6.
- According to the preceding calculation rules, the score ranges for high-, medium-, and low-risk assets are as follows:
 - 100: no risk
 - 81-99: low risk
 - 51-80: medium risk
 - 0-50: high risk

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.
- 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 time, so that you can handle the exceptions in time.
- Click  in the lower right corner to display the asset legend.

3 Asset Management

3.1 Assets

3.1.1 Allowing or Disallowing Access to Cloud Assets

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

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

- 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 3-1 Agency policies

Asset	Policy	Scope	Remarks
OBS	OBS Administrator	Global	Used to configure OBS logs, obtain the OBS bucket list, and download items form OBS.
	EVS ReadOnlyAccess	Regional	Used to obtain the EVS disk list.
	OBS Administrator	Global	Used to obtain the logs delivered by OBS.
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	Policy	Scope	Remarks
Asset Map	Tenant Guest	Regional	Used to obtain the list of cloud services used for data storage and processing.
	OBS Administrator	Global	Used to configure OBS logs, obtain the OBS bucket list, and download items form OBS.
	EVS ReadOnlyAccess	Regional	Used to obtain the EVS disk list.
	OBS Administrator	Global	Used for OBS to deliver logs.

Procedure



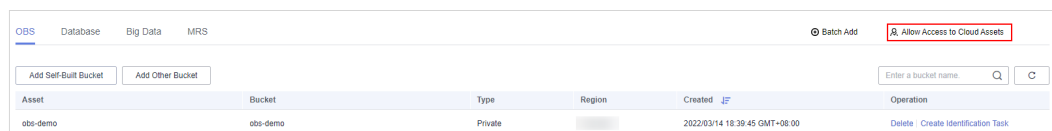
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Asset Management > Assets**.
- Step 5** In the upper right corner of the page, click **Allow Access to Cloud Assets**.

Figure 3-1 Assets



- Step 6** On the displayed page, allow or disallow DSC to access your cloud assets. For details, see [Table 3-2](#).

Figure 3-2 Allowing access to cloud assets

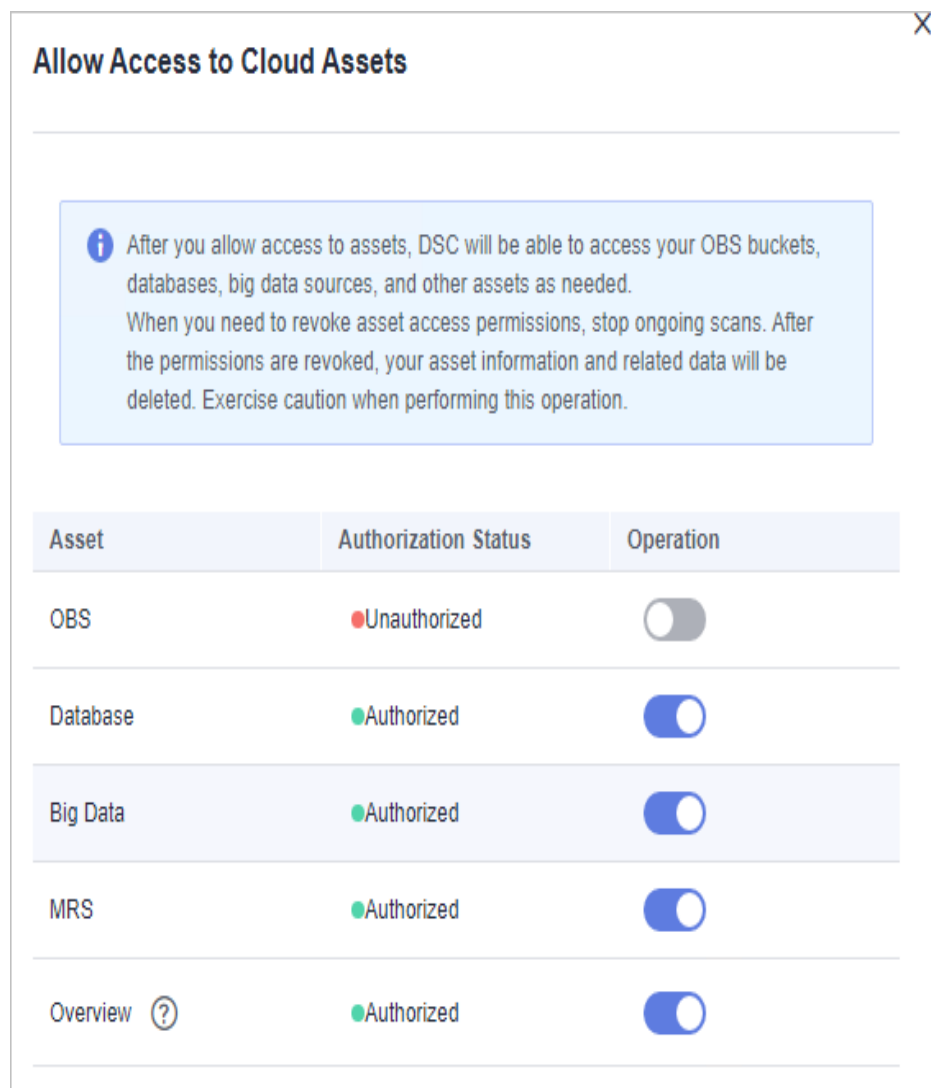




Table 3-2 Parameter description

Parameter	Description
Assets	<p>DSC provides four types of assets:</p> <ul style="list-style-type: none"> • OBS • Database: 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 • Asset map: Allow DSC to access cloud assets. <p>Agency Policies Obtained After Access to Assets Is Allowed describes the agency policies obtained after the access to assets is allowed.</p>

Parameter	Description
Authorization Status	The options are as follows: <ul style="list-style-type: none">• Authorized• Unauthorized
Operation	Click the following toggle buttons to allow or disallow access to your assets: <ul style="list-style-type: none">•  : Unauthorized•  : Authorized

----End

3.1.2 Adding Assets in Batches

Add OBS, database, MRS, and big data assets in batches.

Prerequisites

- DSC has been allowed to access the database assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- The self-built database engine, version, and database server address have been obtained. There are available IP addresses in the corresponding subnet.

Constraints

Only asset types and versions supported by DSC can be added. For details, see [Table 3-3](#).

Table 3-3 Asset types and versions supported by DSC

Asset Type	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
GaussDB for openGauss	1.4
PostgreSQL	11, 10, 9.6, 9.5, 9.4, and 9.1
TDSQL	10.3.X

Asset Type	Version
Oracle	11, 12
DDS	4.2, 4.0, and 3.4
DWS	4.2, 4.0, and 3.4
Elasticsearch	5.x, 6.x, and 7.x
OBS	V3

Procedure



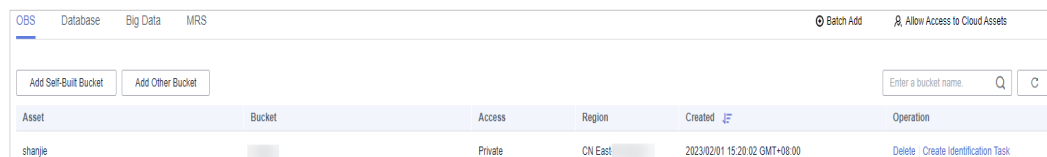
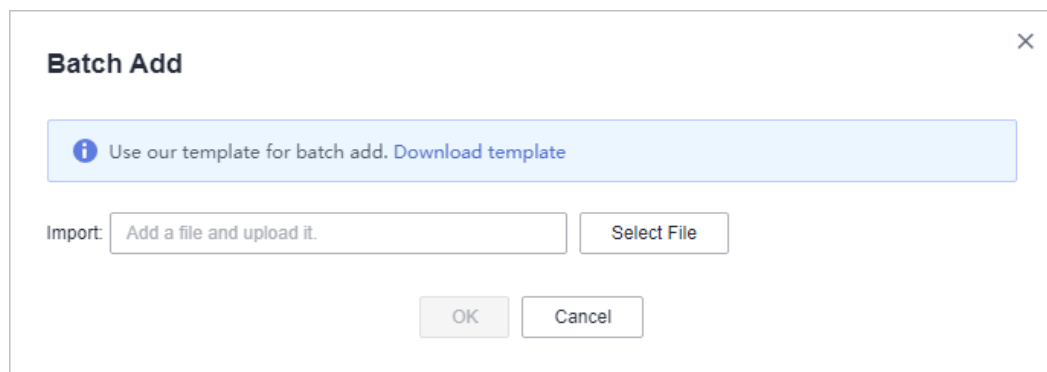
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Asset Management > Assets**.

Figure 3-3 OBS assets

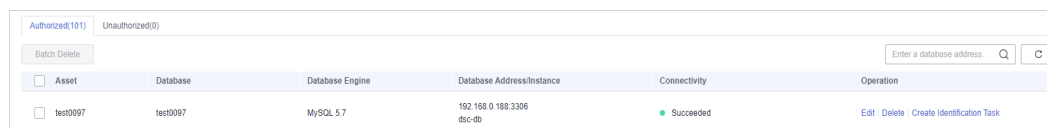


- Step 5** In the upper right corner of the **OBS** tab page, click **Batch Add**.
- Step 6** In the displayed dialog box, click **Select File** and import the sorted assets.
You can click **Download template** to classify assets.

Figure 3-4 Adding assets in batches



- Step 7** Click **OK**.

Figure 3-5 Connectivity test

The screenshot shows a table with columns: Asset, Database, Database Engine, Database Address/Instance, Connectivity, and Operation. A single row is visible with the following data: Asset: test0097, Database: test0097, Database Engine: MySQL 5.7, Database Address/Instance: 192.168.0.188:3306 db-test, Connectivity: Succeeded (indicated by a green dot), and Operation: Edit, Delete, Create Identification Task. Above the table, there are tabs for 'Authorized(101)' and 'Unauthorized(0)', a 'Batch Delete' button, and a search bar labeled 'Enter a database address'.

Asset	Database	Database Engine	Database Address/Instance	Connectivity	Operation
<input type="checkbox"/> test0097	test0097	MySQL 5.7	192.168.0.188:3306 db-test	● Succeeded	Edit Delete Create Identification Task

DSC will check the connectivity of the added database, and the connectivity status of the added database is **Checking**.

- If DSC can access the added database, the connectivity status is **Succeeded**.
- If the DSC cannot access the added database, the connectivity status **Failed**. View the failure cause and follow the instructions described in [How Do I Troubleshoot the Failure in Connecting to the Added Database?](#) to handle the problem.

----End

3.1.3 OBS Assets

3.1.3.1 Adding OBS Assets

After DSC is authorized to access your OBS assets, you can add your OBS assets to DSC protection.

Prerequisites

- OBS asset access permissions are granted. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- OBS has been enabled and used.
- If you want to add a bucket of other types, set the bucket permission to **public** or set the bucket to a private bucket on which the current account has permissions.

Constraints

DSC does not support the parallel file system of OBS.

Procedure



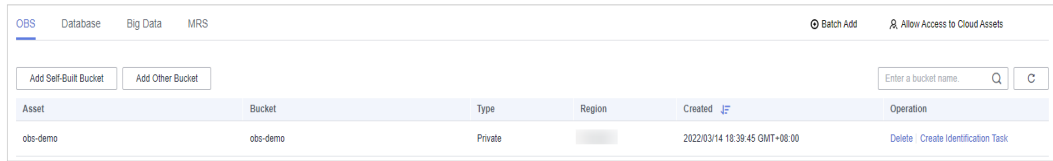
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Asset Management > Assets**.

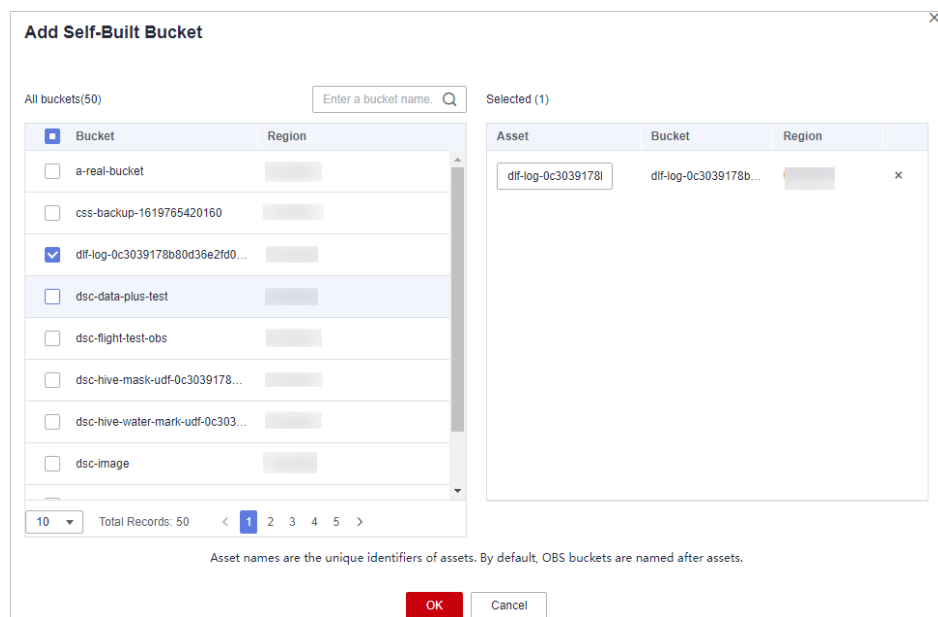
Figure 3-6 OBS assets



Step 5 Add OBS assets.

- Adding self-built OBS buckets
 - a. In the upper left corner of the **OBS** tab page, click **Add Self-Built Bucket**.
 - b. In the displayed dialog box, select the OBS buckets to be added.

Figure 3-7 Adding self-built OBS buckets



- c. Click **OK**.
- Adding other OBS buckets
 - a. In the upper left corner of the **OBS** tab page, click **Add Other Bucket**.
 - b. In the displayed dialog box, enter the name of a bucket to be added.

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

Figure 3-8 Adding other OBS buckets

Asset	Bucket	Operation
obs-01	obs-zh01	Delete

- c. Click **OK**.

----End

Related Operations

- Allow or disallow access to OBS assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- Delete OBS assets. For details, see [Deleting OBS Assets](#).

3.1.3.2 Deleting OBS Assets

This section describes how to delete an OBS bucket that has been added to DSC protection. After the OBS bucket is deleted, the task templates and scanning reports created for it in DSC will also be deleted and cannot be restored.

Prerequisites

- OBS asset access permissions are granted. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- OBS assets to be deleted are not used in any ongoing sensitive data identification tasks.

Constraints

If the OBS assets to be deleted have been used in an ongoing sensitive data identification task, unbind the assets or delete the task, and then delete the OBS assets as instructed.

CAUTION

Deleted assets including related templates, task results, and reports cannot be recovered. Exercise caution when performing this operation.

Procedure



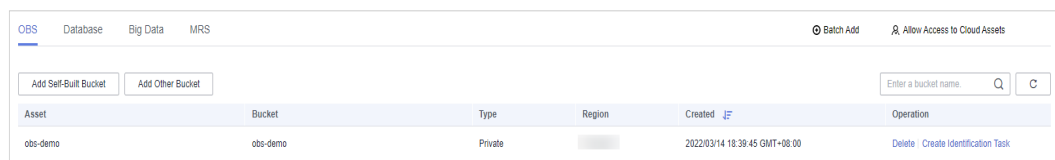
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Asset Management > Assets**.

Figure 3-9 OBS assets



Asset	Bucket	Type	Region	Created	Operation
obs-demo	obs-demo	Private		2022/03/14 18:39:45 GMT+08:00	Delete Create Identification Task

- Step 5** In the OBS asset list, locate the asset to be deleted and click **Delete** in the **Operation** column.
- Step 6** In the displayed dialog box, click **OK**.

----End

3.1.4 Database Assets

3.1.4.1 Authorizing RDS Databases

If you have granted permissions for accessing your database assets to DSC, purchased Huawei Cloud RDS DB instances, and created databases on the DB instances, you can follow the instructions described in this section to authorize permissions for performing relevant operations. Details are as follows:

- 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.

NOTE

DSC cannot scan and mask sensitive data in MySQL databases which SSL has been enabled for on the RDS DB instance.

Prerequisites

- DSC has been allowed to access the database assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- You have subscribed to RDS, and assets are available in RDS. There are available IP addresses in the corresponding subnet.
- The **Status** of the RDS DB instance is **Normal**, and the number of security groups is 1.

Procedure



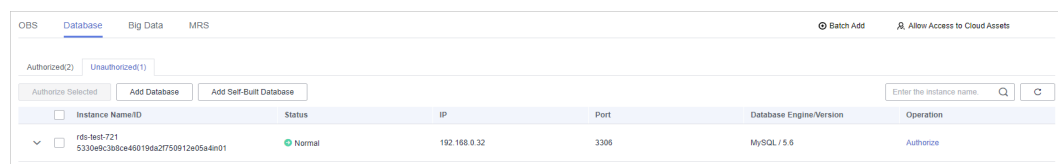
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation tree on the left, choose **Asset Management > Assets**. On the displayed **Assets** page, choose **Database > Unauthorized**. The **Unauthorized Database** page is displayed, as shown in [Figure 3-10](#).


Figure 3-10 Unauthorized database assets



Instance Name/ID	Status	IP	Port	Database Engine/Version	Operation
159-161-721 533049C3808445019842750912e05a4e01	Normal	192.168.0.32	3306	MySQL / 5.6	Authorize

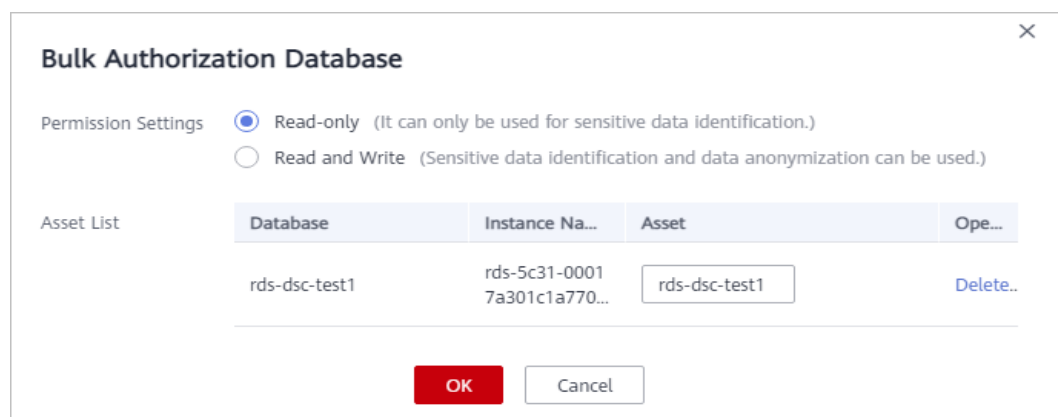
- Step 5** In the row containing the desired RDS DB instance, click **Authorize** in the **Operation** column.

NOTE

If you only need to authorize permissions for a single database in an RDS database instance, click  on the left of instance. In the row containing the desired database, click **Authorize** in the **Operation** column.

- Step 6** In the displayed dialog box, set required parameters based on [Table 3-4](#).

Figure 3-11 Batch permission authorization for databases



Bulk Authorization Database

Permission Settings Read-only (It can only be used for sensitive data identification.)
 Read and Write (Sensitive data identification and data anonymization can be used.)

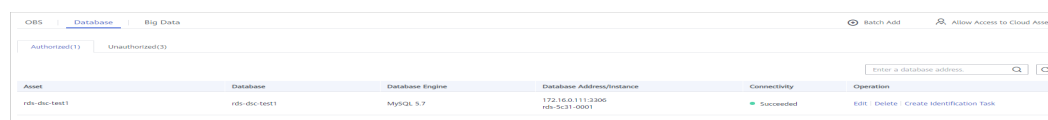
Asset List

Database	Instance Na...	Asset	Ope...
rds-dsc-test1	rds-5c31-0001 7a301c1a770...	rds-dsc-test1	Delete..

Table 3-4 Parameter description

Parameter	Description
Permission Settings	<ul style="list-style-type: none">● Read-only: It can only be used for sensitive data identification. CAUTION After the RDS read-only permission is authorized, DSC creates an account dsc_readonly in RDS.<ul style="list-style-type: none">- 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.● Read and Write: Sensitive data identification and data masking functions can be used.
Asset List	<ul style="list-style-type: none">● If Read-only is selected for Permission Settings, you can change the names of the database assets to be authorized.● If Read and Write is selected for Permission Settings, you can change the names of the database assets to be authorized. The usernames and passwords for accessing the databases must be configured.

Step 7 Click **OK**. The authorized databases are displayed on the **Authorized** tab page.

Figure 3-12 Connectivity test

DSC will check the connectivity of the added database, and the connectivity status of the added database is **Checking**.

- If DSC can access the added database, the connectivity status is **Succeeded**.
- If the DSC cannot access the added database, the connectivity status **Failed**. View the failure cause and follow the instructions described in [How Do I Troubleshoot the Failure in Connecting to the Added Database?](#) to handle the problem.

----End

Related Operations

- Allow or disallow access to database assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- Delete database assets. For details, see [Editing a Database](#).

- Edit database assets. For details, see [Deleting a Database](#).

3.1.4.2 Adding a Cloud Database

If you have subscribed to Huawei Cloud GaussDB(DWS), Document Database Service (DDS), or GaussDB, and created databases in it, you can follow the instructions described in this section to add the created databases DSC.

Prerequisites

- DSC has been allowed to access the database assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- You have subscribed to GaussDB(DWS), DDS, or GaussDB and added assets to it. There are available IP addresses in the corresponding subnet.

Procedure



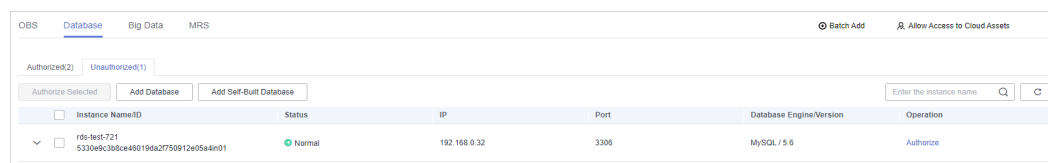
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation tree on the left, choose **Asset Management > Assets**. On the displayed **Assets** page, choose **Database > Unauthorized**. The **Unauthorized Database** page is displayed, as shown in [Figure 3-13](#).

Figure 3-13 Unauthorized database assets



Instance Name/ID	Status	IP	Port	Database Engine/Version	Operation
Instance Name/ID: 18-8e8f721-5330e9c3b8ce4460196a2750912e05a4e01	Normal	192.168.0.32	3306	MySQL / 5.6	Authorize

- Step 5** In the upper left corner of the database asset list, click **Add Database**.

- Step 6** In the displayed dialog box, set database parameters based on [Table 3-5](#).

Figure 3-14 Adding a DWS database

The screenshot shows a dialog box titled "Add Database" with a close button (X) in the top right corner. The dialog contains the following fields:

- Asset**: Text input field with placeholder "Enter an asset name."
- Database Type**: Dropdown menu with "DWS instance" selected.
- Version**: Dropdown menu.
- Port**: Text input field with placeholder "Enter a port."
- Username**: Text input field with placeholder "Enter a username."
- Region**: Dropdown menu with "wx)" selected.
- DWS instance**: Dropdown menu.
- Database Server Address**: Dropdown menu.
- Database**: Text input field with placeholder "Enter a database name."
- Password**: Text input field with placeholder "Enter a password." and a show/hide icon.

At the bottom of the dialog are two buttons: a red "OK" button and a white "Cancel" button.

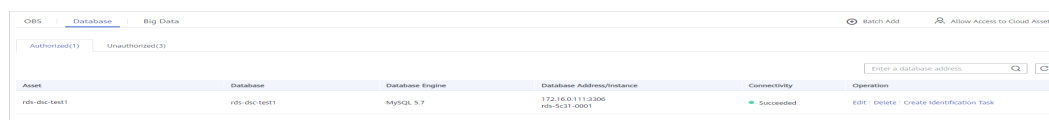
Table 3-5 Parameter description

Parameter	Description	Example Value
Asset	Customized parameter	dsc_test
Region	Region where the account is used for login	N/A
Database Type	You can select DWS instance , DDS instance , or GaussDB instance .	DWS instance
DWS Instance	An option of Database Type . Select a database instance that has been created in GaussDB(DWS) from the drop-down list.	N/A
DDS Instance	An option of Database Type . Select a database instance that has been created in DDS from the drop-down list.	N/A
GaussDB Instance	Select a database instance that has been created in GaussDB from the drop-down list.	N/A
Version	(Default) Version of the selected instance, which cannot be modified	5.7
Database Server Address	IP address of the database server	192.168.0.233
Port	(Default) Port number of the database server, which cannot be modified	3306

Parameter	Description	Example Value
Database	Name of the database created in DWS. You can choose to enter a name or select one from the drop-down list.	N/A
Username	Username for accessing the database you have entered, which must be the same as that set when the database is created in DWS	N/A
Password	Password for accessing the database you have entered, which must be the same as that set when the database is created in DWS	N/A

Step 7 Click **OK**. The authorized databases are displayed on the **Authorized** tab page.

Figure 3-15 Connectivity test



DSC will check the connectivity of the added database, and the connectivity status of the added database is **Checking**.

- If DSC can access the added database, the connectivity status is **Succeeded**.
- If the DSC cannot access the added database, the connectivity status **Failed**. View the failure cause and follow the instructions described in [How Do I Troubleshoot the Failure in Connecting to the Added Database?](#) to handle the problem.

----End

Related Operations

- Allow or disallow access to database assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- Delete database assets. For details, see [Editing a Database](#).
- Edit database assets. For details, see [Deleting a Database](#).

3.1.4.3 Adding a Self-Built Database

Add self-built database assets.

Prerequisites

- DSC has been allowed to access the database assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- The self-built database engine, version, and database server address have been obtained. There are available IP addresses in the corresponding subnet.

Constraints

Only asset types and versions supported by DSC can be added. For details, see [Table 3-6](#).

Table 3-6 Asset types and versions supported by DSC

Asset Type	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
GaussDB for openGauss	1.4
PostgreSQL	11, 10, 9.6, 9.5, 9.4, and 9.1
TDSQL	10.3.X
Oracle	11, 12
DDS	4.2, 4.0, and 3.4
DWS	4.2, 4.0, and 3.4
Elasticsearch	5.x, 6.x, and 7.x
OBS	V3

Procedure



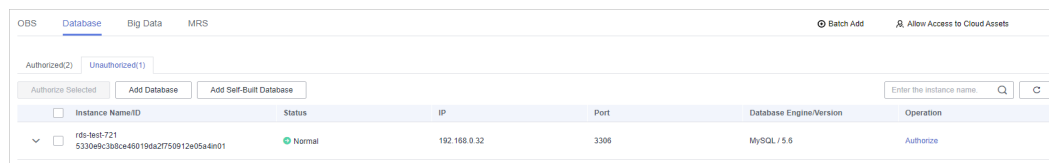
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation tree on the left, choose **Asset Management > Assets**. On the displayed **Assets** page, choose **Database > Unauthorized**. The **Unauthorized Database** page is displayed, as shown in [Figure 3-16](#).

Figure 3-16 Unauthorized database assets



Step 5 In the upper left corner of unauthorized database assets, click **Add Self-Built Database**.

Step 6 In the displayed dialog box, set database parameters. For details, see [Table 3-7](#).

Figure 3-17 Adding a self-built database

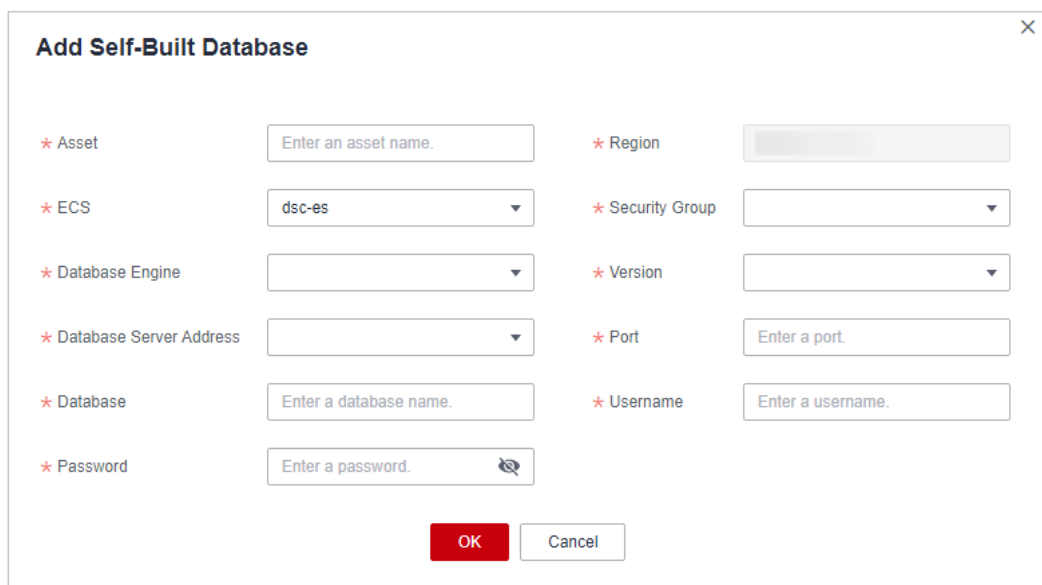


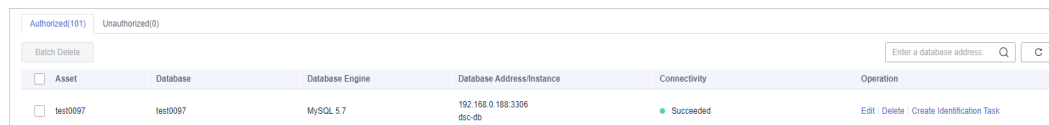
Table 3-7 Parameters for adding a self-built database

Parameter	Description	Example Value
Asset	Database name	N/A
Region	Region where the account is used for login	N/A
ECS	Select an ECS instance created in ECS from the drop-down list.	N/A
Security Group	Name of the security group to which the ECS instance belongs	default
Database Engine	Database engine Value options: MySQL , TDSQL , KingBase , DMDBMS , PostgreSQL , SQLServer , and Oracle	MySQL

Parameter	Description	Example Value
Version	Version number corresponding to the database engine	5.6
Schema Name	Database schema name	N/A
Database Server Address	IP address of the database server	N/A
Port	Port number of the database server	N/A
Database	Self-built database name	N/A
Username	Username for logging in to the database server	N/A
Password	Password for logging in to the database server	N/A

Step 7 Click **OK**. The authorized databases are displayed on the **Authorized** tab page.

Figure 3-18 Connectivity test



The screenshot shows a table with columns: Asset, Database, Database Engine, Database Address/Instance, Connectivity, and Operation. A single row is visible with the following data: Asset: test0097, Database: test0097, Database Engine: MySQL 5.7, Database Address/Instance: 192.168.0.189:3306 dsc-db, Connectivity: Succeeded (indicated by a green dot), and Operation: Edit | Delete | Create Identification Task. Above the table, there are tabs for 'Authorized(101)' and 'Unauthorized(0)', a 'Batch Delete' button, and a search bar with the text 'Enter a database address'.

Asset	Database	Database Engine	Database Address/Instance	Connectivity	Operation
<input type="checkbox"/>	test0097	MySQL 5.7	192.168.0.189:3306 dsc-db	● Succeeded	Edit Delete Create Identification Task

DSC will check the connectivity of the added database, and the connectivity status of the added database is **Checking**.

- If DSC can access the added database, the connectivity status is **Succeeded**.
- If the DSC cannot access the added database, the connectivity status **Failed**. View the failure cause and follow the instructions described in [How Do I Troubleshoot the Failure in Connecting to the Added Database?](#) to handle the problem.

----End

Related Operations

- Allow or disallow access to database assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- Delete database assets. For details, see [Editing a Database](#).
- Edit database assets. For details, see [Deleting a Database](#).

3.1.4.4 Editing a Database

Reset the modified or incorrect username and password of the added database server.

Prerequisites

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

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**.
- Step 4** In the navigation pane, choose **Asset Management > Assets** and click the **Database** tab and then the **Authorized** tab, as shown in [Figure 3-19](#).

Figure 3-19 Authorized database assets

Asset	Database	Database Engine	Database Address/Instance	Connectivity	Operation
rds-dsc-test1	rds-dsc-test1	MySQL 5.7	172.16.0.111:3306 rds-5c31-0001	● Succeeded	Edit Delete Create Identification Task

- Step 5** Locate the database asset to be edited, click **Edit** in the **Operation** column.
- Step 6** In the displayed dialog box, change the username or password of the database server.
- Step 7** Click **OK**.

After the database asset has been edited, the database **Connectivity** status becomes **Checking**. Check whether DSC can access the added database asset using the new username and password.

- If DSC can access the added database, the connectivity status is **Succeeded**.
- If the DSC cannot access the added database, the connectivity status **Failed**. View the failure cause and follow the instructions described in [How Do I Troubleshoot the Failure in Connecting to the Added Database?](#) to handle the problem.

----End

3.1.4.5 Deleting a Database

This section describes how to delete an added database asset. After the OBS bucket is deleted, the task templates and scanning reports created for it in DSC will also be deleted and cannot be restored.

Prerequisites

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

- The database asset to be deleted is not used in any sensitive data identification tasks.

Constraints

- If the database asset to be deleted has been used in a sensitive data identification task, unbind the asset or delete the task and then delete the asset.
- Deleted assets cannot be recovered. After the deletion, the templates, results, and reports related to the asset will be deleted. Exercise caution when performing this operation.

Procedure



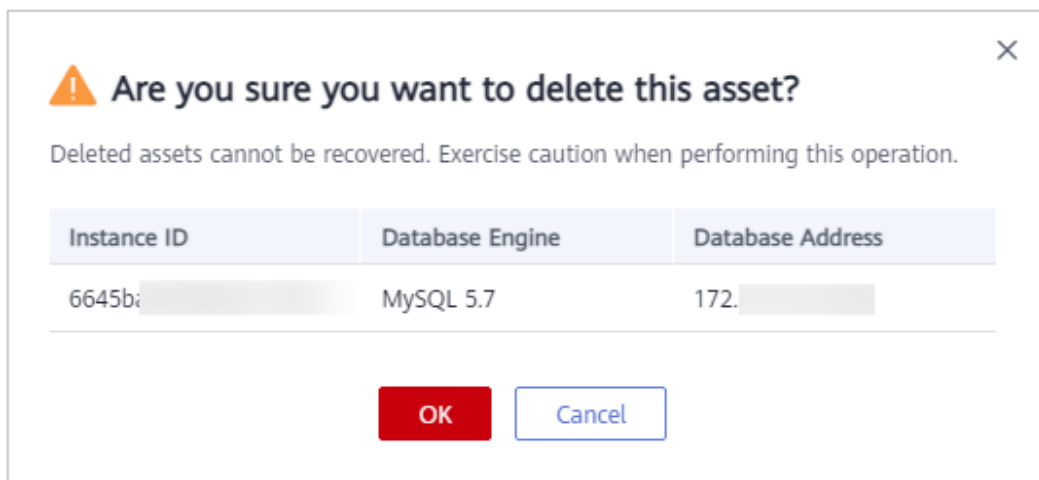
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Asset Management > Assets** and click the **Database** tab and then the **Authorized** tab.

Figure 3-20 Authorized database assets

<input type="checkbox"/> Asset	Database	Database Engine	Database Address/Instance	Connectivity	Operation
<input type="checkbox"/>	gausedb	DWS	192.168.0.226:8000 dsc-dws	● Succeeded	Edit Delete Create Identification Task
<input type="checkbox"/>	thy1	Oracle 11	192.168.0.143:1521	● Succeeded	Edit Delete Create Identification Task

- Step 5** In the database asset list, locate the row that contains the database asset to be deleted and click **Delete** in the **Operation** column.

Figure 3-21 Deleting an asset



- Step 6** In the displayed dialog box, click **OK**.

----End

3.1.5 Big Data Assets

3.1.5.1 Adding a Cloud ES Data Source

This section describes how to add a Cloud ES data source.

Constraints

When you add a cloud ES asset, the created CSS cluster must be a CSS cluster that has not enabled HTTPS authentication.

Prerequisites

- DSC has been allowed to access big data assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- You have subscribed to CSS, and have assets in it. There are available IP addresses in the corresponding subnets.

Procedure



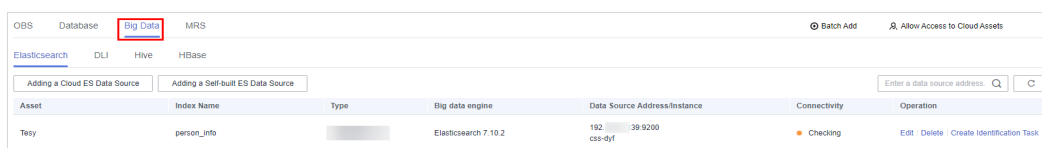
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Asset Management > Assets**, and click the **Big Data** tab. The big data asset list is displayed.

Figure 3-22 Accessing Elasticsearch assets



The screenshot shows the 'Big Data' tab selected in the navigation pane. Below the navigation pane, there are two buttons: 'Adding a Cloud ES Data Source' and 'Adding a Self-built ES Data Source'. A search bar is present with the placeholder text 'Enter a data source address.' and a search icon. Below the search bar is a table with the following columns: Asset, Index Name, Type, Big data engine, Data Source Address/Instance, Connectivity, and Operation. The table contains one row with the following data: Asset: Tesy, Index Name: person_info, Type: [blurred], Big data engine: Elasticsearch 7.10.2, Data Source Address/Instance: 192.168.39.9200 csb-dyt, Connectivity: Checking, Operation: Edit | Delete | Create Identification Task.

Asset	Index Name	Type	Big data engine	Data Source Address/Instance	Connectivity	Operation
Tesy	person_info		Elasticsearch 7.10.2	192.168.39.9200 csb-dyt	Checking	Edit Delete Create Identification Task

- Step 5** In the upper left corner of the Elasticsearch asset list, click **Adding a Cloud ES Data Source**.
- Step 6** In the displayed dialog box, set parameters. For details, see [Table 3-8](#).

Figure 3-23 Adding a cloud ES data source

The screenshot shows a dialog box titled "Adding a Cloud ES Data Source". It contains the following fields and values:

- Asset: Enter an asset name.
- Region: North-Ulanqab203
- Big Data Type: CSS (Elasticsearch)
- Elasticsearch cluster: css-dyf
- Version: 7.10.2
- Database Server Address: 192. .139
- Port: 9200
- Index: Enter an index.
- Username: Enter a username.
- Password: Enter a password.

At the bottom, there are two buttons: "OK" (highlighted in red) and "Cancel".

Table 3-8 Cloud ES data source parameters

Parameter	Description	Example Value
Asset	Enter an asset name containing 4 to 255 characters.	DSCESTest
Big Data Type	Select CSS (ElasticSearch) from the drop-down list box.	--
ElasticSearch cluster	Select an ElasticSearch cluster from the drop-down list box.	--
Version	Version number corresponding to the big data type	5.x
Database Server Address	Select the IP address of the Cloud ES data source server from the drop-down list.	192.168.0.233
Port	Enter the port number of the ES data source server.	9200
Index	Enter the index corresponding to the Cloud ES data source.	--
Username	Enter the username for accessing the ES server.	--
Password	Enter the password for accessing the ES server.	--

Step 7 Click **OK**. The Cloud ES data source is added.

After the cloud ES data source is added, its connectivity status is **Checking**. In this case, DSC tests the connectivity to the data source with your username and password.

- If the connectivity status is **Succeeded**, DSC can access the added data source.
- If the connectivity status is **Failed**, DSC cannot access the added data source. Click **Details** to view the failure cause and enter the correct username and password for accessing the added ES data source.

----End

Related Operations

- Editing and deleting assets
 - In the Elasticsearch asset list, click **Edit** in the **Operation** column of the target asset to modify the asset information.
 - In the Elasticsearch asset list, click **Delete** in the **Operation** column of the target asset to delete the asset.

NOTE

Deleted assets cannot be restored. The deletion operation will also delete the asset-related task templates, task results, and reports. Exercise caution when performing this operation.

- Creating an identification task
In the Elasticsearch asset list, click **Create Identification Task** in the **Operation** column of the target asset. The identification task list is displayed. For details about how to create an identification task, see [Creating an Identification Task](#).

3.1.5.2 Adding a Self-Built ES Data Source

This section describes how to add a self-built ES data source.

Prerequisites

- DSC has been allowed to access big data assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- The type, version, host, and index of the self-built ES big data asset have been obtained. There are available IP addresses in the subnet of the self-built ES big data asset.

Procedure

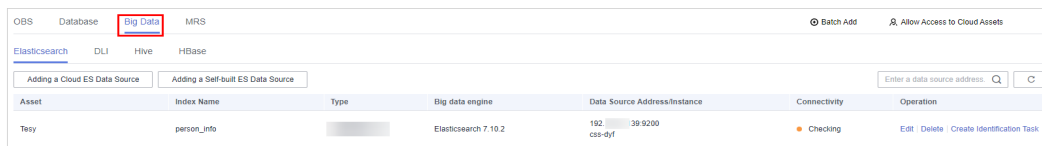
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Asset Management > Assets**, and click the **Big Data** tab. The big data asset list is displayed.

Figure 3-24 Accessing Elasticsearch assets



- Step 5** In the upper left corner of the Elasticsearch asset list, click **Add a Self-built ES Data Source**.
- Step 6** In the displayed dialog box, configure parameters for adding a self-built ES data source. For details, see [Table 3-9](#).

Figure 3-25 Adding a self-built ES data source

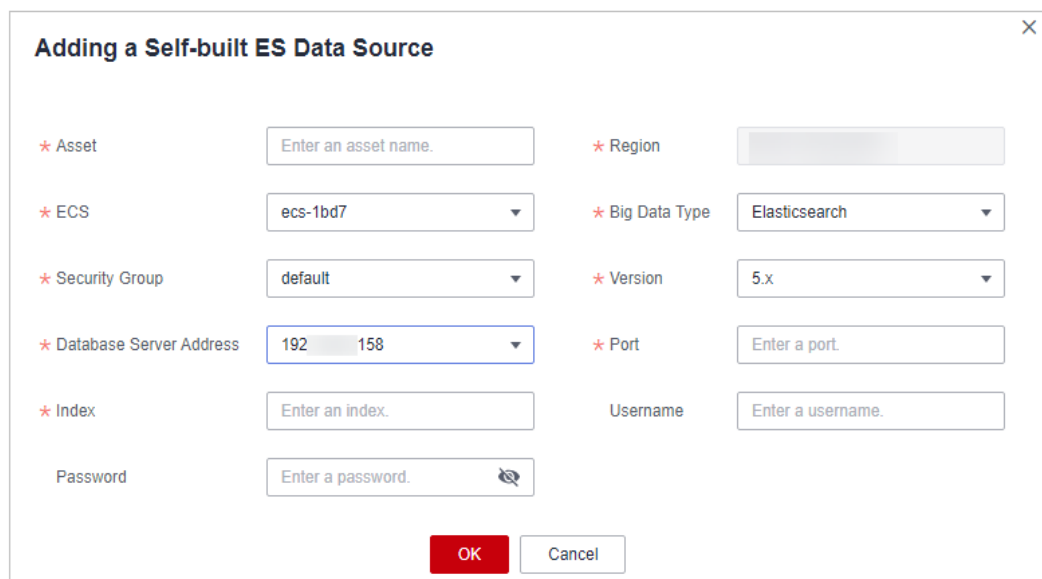


Table 3-9 Parameters for adding a self-built ES data source

Parameter	Description	Example Value
Asset	Enter an asset name containing 4 to 255 characters.	DSCeSTestSelf
Region	Region where the account is used for login	-
ECS	Select an Elasticsearch instance.	--
Big Data Type	Select Elasticsearch .	Elasticsearch
Security Group	Select an existing security group from the drop-down list box.	default
Version	Select the version corresponding to the self-built ES data source version.	5.x

Parameter	Description	Example Value
Database Server Address	Enter the IP address of the self-built Elasticsearch data source server.	192.168.0.233
Port	Enter the port number of the self-built Elasticsearch data source server.	9200
Index	Enter the index corresponding to the self-built ES data source.	--
Username	Enter the username for accessing the self-built Elasticsearch data source server.	--
Password	Enter the password for accessing the self-built Elasticsearch data source server.	--

Step 7 Click **OK**. The self-built Elasticsearch data source is added.

After the self-built ES data source is added, its connectivity status is **Checking**. In this case, DSC tests the connectivity to the data source with your username and password.

- If the connectivity status is **Succeeded**, DSC can access the added data source.
- If the connectivity status is **Failed**, DSC cannot access the added data source. Click **Details** to view the failure cause and enter the correct username and password for accessing the added ES data source.

----End

Related Operations

- Editing and deleting assets
 - In the Elasticsearch asset list, click **Edit** in the **Operation** column of the target asset to modify the asset information.
 - In the Elasticsearch asset list, click **Delete** in the **Operation** column of the target asset to delete the asset.

NOTE

Deleted assets cannot be restored. The deletion operation will also delete the asset-related task templates, task results, and reports. Exercise caution when performing this operation.

- Creating an identification task
In the Elasticsearch asset list, click **Create Identification Task** in the **Operation** column of the target asset. The identification task list is displayed. For details about how to create an identification task, see [Creating an Identification Task](#).

3.1.5.3 Adding a DLI Data Source

This section describes how to add a DLI data source.

Prerequisites

- DSC has been allowed to access big data assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- You have subscribed to DLI, and have assets in it. There are available IP addresses in the corresponding subnets.

Procedure



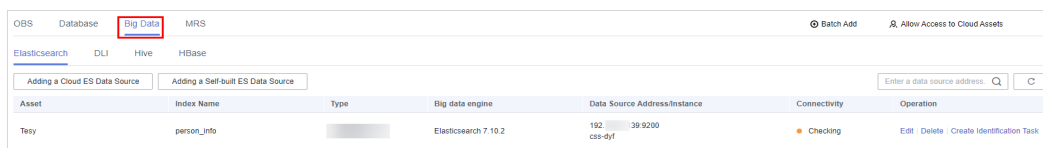
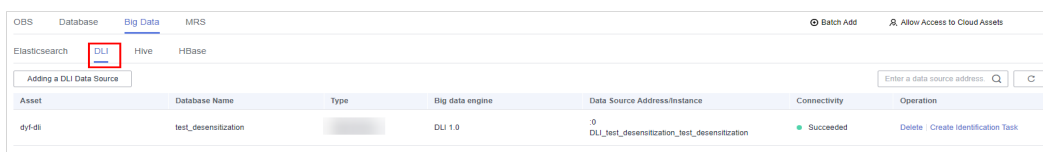
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Asset Management > Assets**, and click the **Big Data** tab. The big data asset list is displayed.

Figure 3-26 Accessing Elasticsearch assets



- Step 5** Click the **DLI** tab.

Figure 3-27 DLI asset tables



- Step 6** In the upper left corner of the DLI asset list, click **Adding a DLI Data Source**.
- Step 7** In the displayed dialog box, set parameters for adding a DLI big data source. For details, see [Table 3-10](#).

Figure 3-28 Adding a DLI data source**Table 3-10** DLI data source parameters

Parameter	Description	Example Value
Asset	Enter an asset name containing 4 to 255 characters.	DSCDLITest
Big Data Type	Select CSS (ElasticSearch) from the drop-down list box.	--
Queue	Select the queue from the drop-down list.	default
DLI Database	Select the database in the queue of DLI.	5.x

Step 8 Click **OK**.

After the DLI data source is added, its connectivity status is **Checking**. In this case, DSC tests the connectivity to the DLI data source with your username and password.

- If the connectivity status is **Succeeded**, DSC can access the added data source.
- If the connectivity status is **Failed**, DSC can access the added data source. Click **Details** to view the failure cause and enter the correct username and password for accessing the added data source.

----End

Related Operations

- Deleting an asset

In the DLI asset list, click **Delete** in the **Operation** column of the target asset to delete the asset.

NOTE

Deleted assets cannot be restored. The deletion operation will also delete the asset-related task templates, task results, and reports. Exercise caution when performing this operation.

- Creating an identification task
In the DLI asset list, click **Create Identification Task** in the **Operation** column of the target asset. The identification task list is displayed. For details about how to create an identification task, see [Creating an Identification Task](#).

3.1.5.4 Adding a Hive Data Source

This section describes how to add a Hive data source.

Prerequisites

- DSC has been allowed to access big data assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- You have obtained the version, host, and index of the Hive data source, and the subnet of the Hive data source has available IP address quotas.

Procedure



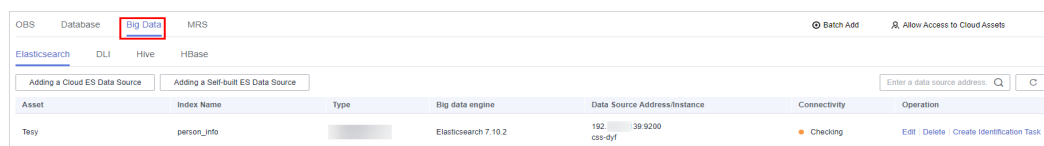
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Asset Management > Assets**, and click the **Big Data** tab. The big data asset list is displayed.

Figure 3-29 Accessing Elasticsearch assets



Asset	Index Name	Type	Big data engine	Data Source Address/Instance	Connectivity	Operation
Tesy	person_info		Elasticsearch 7.10.2	192.168.39.9200 ca-dyt	Checking	Edit Delete Create Identification Task

- Step 5** Click the **Hive** tab. The Hive asset list is displayed.
- Step 6** In the upper left corner of the Hive asset list, click **Adding a Hive Data Source**.
- Step 7** In the displayed dialog box, set big data source parameters by referring to [Table 3-11](#).

Figure 3-30 Adding a Hive data source

Table 3-11 Parameters for adding a Hive data source

Parameter	Description	Example Value
Asset	Enter an asset name containing 4 to 255 characters.	DSCHiveTest
Region	Region where the account is used for login	-
ECS	Select an ECS instance from the drop-down list.	--
Big Data Type	Select Hive .	Hive
Security Group	Select an existing security group from the drop-down list box.	default
Version	In the displayed Select LDT Version dialog box, select the required LDT version.	5.x
Database Server Address	Enter the IP address of the server.	192.168.0.233
Port	Enter the port number of the server.	10000
Database	Enter a database name.	--
Username	Enter the username for accessing the server.	--
Password	Enter the password for accessing the server.	--

Step 8 Click **OK**. The Hive data source is added.

After the Hive data source is added, its connectivity status is **Checking**, which indicates that the DSC is testing the connectivity to the Hive data source with your username and password.

- If the connectivity status is **Succeeded**, DSC can access the added data source.
- If the connectivity status is **Failed**, DSC can access the added data source. Click **Details** to view the failure cause and enter the correct username and password for accessing the added data source.

----End

Related Operations

- Deleting an asset

In the Hive asset list, click **Delete** in the **Operation** column of the target asset to delete the asset.

NOTE

Deleted assets cannot be restored. The deletion operation will also delete the asset-related task templates, task results, and reports. Exercise caution when performing this operation.

- Creating an identification task

In the Hive asset list, click **Create Identification Task** in the **Operation** column of the target asset. The identification task list is displayed. For details about how to create an identification task, see [Creating an Identification Task](#).

3.1.5.5 Adding an HBase Data Source


This section describes how to add an HBase data source.


Prerequisites

- Permissions for accessing to the big data assets have been obtained. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- You have obtained the version, host, and index of the HBase data source, and the subnet of the HBase data source has available IP address quotas.

Procedure

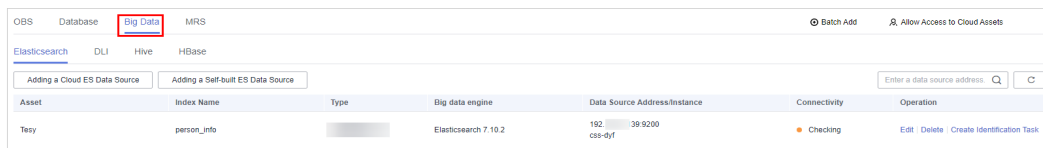
Step 1 Log in to the management console.

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**.

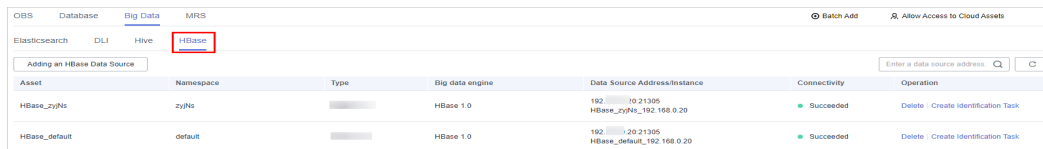
Step 4 In the navigation pane, choose **Asset Management > Assets**, and click the **Big Data** tab. The big data asset list is displayed.

Figure 3-31 Accessing Elasticsearch assets



Step 5 Click the **HBase** tab. The HBase asset list page is displayed.

Figure 3-32 HBase asset list



Step 6 In the upper left corner of the HBase asset list, click **Adding an HBase Data Source**.

Step 7 In the displayed **Adding an HBase Data Source** dialog box, set big data source parameters by referring to [Table 3-12](#).

Figure 3-33 Adding an HBase data source

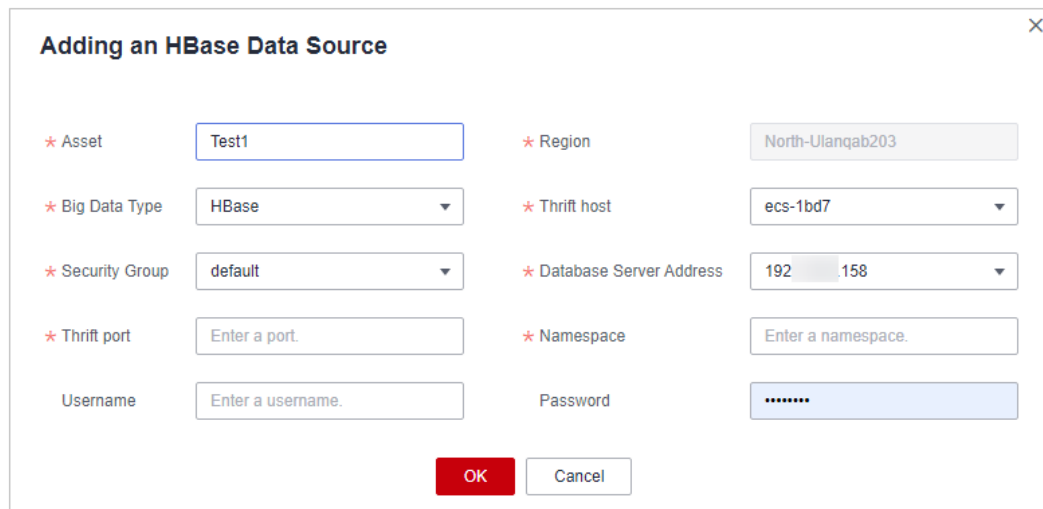


Table 3-12 HBase data source parameters

Parameter	Description
Asset	Enter an asset name containing 4 to 255 characters.
Big Data Type	Select HBase from the drop-down list box.
Thrift host	Select the thrift host in the HBase cluster from the drop-down list box.
Security Group	Select a security group from the drop-down list.

Parameter	Description
Database Server Address	Select a server IP address from the drop-down list box.
Thrift port	Select a thrift node port in the HBase cluster from the drop-down list box.
Username	Enter the username for accessing the server.
Password	Enter the password for accessing the server.

Step 8 Click **OK**. The HBase data source is added.

After the HBase data source is added, its connectivity status is **Checking**, which indicates that the DSC is testing the connectivity to the Hive data source with your username and password.

- If the connectivity status is **Succeeded**, DSC can access the added data source.
- If the connectivity status is **Failed**, DSC can access the added data source. Click **Details** to view the failure cause and enter the correct username and password for accessing the added data source.

----End

Related Operations

- Deleting an asset

In the HBase asset list, click **Delete** in the **Operation** column of the target asset to delete the asset.

NOTE

Deleted assets cannot be restored. The deletion operation will also delete the asset-related task templates, task results, and reports. Exercise caution when performing this operation.

- Creating an identification task

In the HBase asset list, click **Create Identification Task** in the **Operation** column of the target asset. The identification task list is displayed. For details about how to create an identification task, see [Creating an Identification Task](#).

3.1.6 MRS Assets

3.1.6.1 Adding MRS Assets

After you complete MRS authorization, you need to grant permissions to DSC for operating MRS Hive data.

Prerequisites

MRS asset access permissions are granted. 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 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**.
- Step 4** In the navigation pane, choose **Asset Management > Assets** and click the **MRS** tab and then the **Unauthorized** tab.

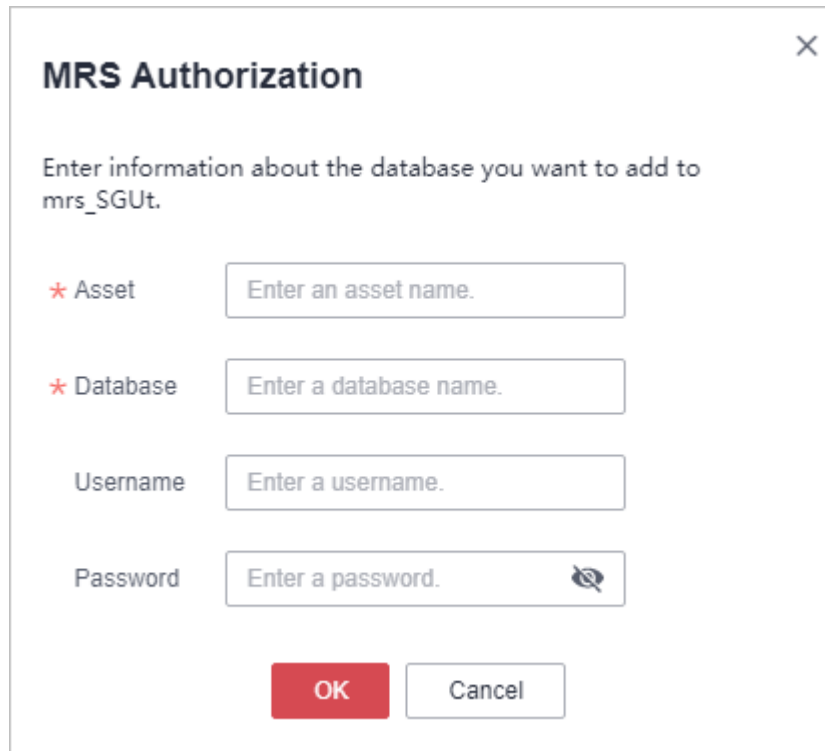
Figure 3-34 MRS assets to be authorized



Instance Name/ID	Cluster Version	Component Version	Subnet	Cluster Status	Operation
mrs_SGUt 9738991-1c77-4f60-946b-9a81852b9eea	MRS 3.1.0_003	Hive/3.1.0	subnet-default	Running	Authorize

- Step 5** In the row containing the desired asset, click **Authorize** in the **Operation** column.
- Step 6** In the displayed **MRS Authorization** dialog, set required parameters based on [Table 3-13](#).

Figure 3-35 MRS Authorization



MRS Authorization

Enter information about the database you want to add to mrs_SGUt.

* Asset

* Database

Username


Password 

Table 3-13 Parameter description

Parameter	Description
Asset	Name of a custom MRS instance
Database	Database name of the MRS instance
Username	Username for accessing the database you have specified, which must be the same as that set when the database is created in MRS
Password	Password for accessing the database you have specified, which must be the same as that set when the database is created in MRS

Step 7 Click **OK**. The authorized MRS assets are displayed in the **Authorized** tab.

----End

3.1.6.2 Deleting MRS Assets

This section describes how to delete an MRS asset. After the OBS bucket is deleted, the task templates and scanning reports created for it in DSC will also be deleted and cannot be restored.

Prerequisites

- MRS asset access permissions are granted. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- The asset to be deleted is not used in any sensitive data identification tasks.

Constraints


If the asset to be deleted has been used in a sensitive data identification task, unbind the asset or delete the task.


⚠ CAUTION

Deleted assets cannot be recovered. After the deletion, the templates, results, and reports related to the asset will be deleted. Exercise caution when performing this operation.

Procedures

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**.

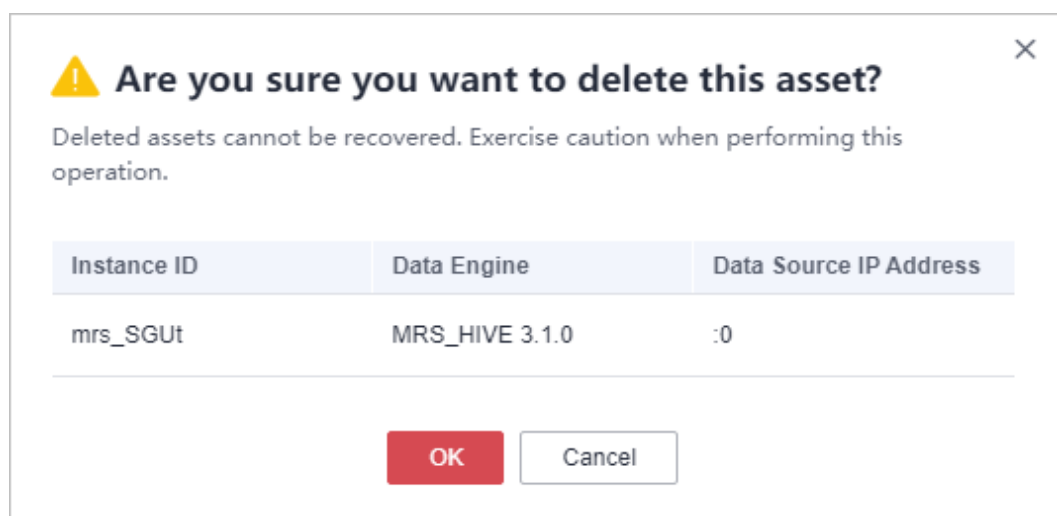
Step 4 In the navigation pane, choose **Asset Management** > **Assets** and click the **MRS** tab and then the **Unauthorized** tab.

Figure 3-36 MRS assets to be authorized

Instance Name/ID	Cluster Version	Component Version	Subnet	Cluster Status	Operation
mrs_SGut 9738901-1d77-4f60-942b-9a81852bfeaa	MRS 3.1.0_003	Hive3.1.0	subnet-default	Running	Authorize

Step 5 In the MRS asset list, locate the asset to be deleted and click **Delete** in the **Operation** column.

Figure 3-37 Deleting an asset



Step 6 In the displayed dialog box, click **OK**.

----End

3.2 Metadata Tasks

3.2.1 Creating a Metadata Collection Task

This topic describes how to create a metadata collection task.

Prerequisites

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

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**.
- 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 3-14 Parameter description

Parameter	Description
Data Source	Select a data source. This parameter can be set to MySQL, PostgreSQL, DMDBMS, KingBase, OpenGuass, DWS, Hive, MRS_HIVE, or TDSQL .
Database Instance	Select a supported database instance.















- Step 6** Click **Next**. The **configure subtasks** page is displayed.
- Click  or  to enable or disable **Scan user tables**.
 - Click  or  to enable or disable **Scan system tables**.
 - Click  or  to enable or disable **Scan column constraints**.
 - Click  or  to enable or disable **Scan views**.
 - Click  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 3-15 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 .

Parameter	Description
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

3.2.2 Running a Metadata Collection Task


You can view and execute a created metadata collection task.


Prerequisites

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

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**.

Step 4 In the navigation pane on the left, choose **Asset Management > Metadata Task**.

Figure 3-38 Metadata Collection Task

Name	Enable/Disable	Sub Tasks	Scheduling Policy	Created	Last Run	Operation
test513	<input checked="" type="checkbox"/>	Scan user tables	Weekly		2023/05/13 17:32:09 GMT+08:00	Running Edit Delete
	<input checked="" type="checkbox"/>	Scan user tables, Scan system tables, Scan column constraints, S...	Once		2023/04/17 11:21:57 GMT+08:00	Running Edit Delete

Table 3-16 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.

Figure 3-39 Running a 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 3-17 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	<p>Running status of the current task. The options are as follows:</p> <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.

Parameter	Description
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

3.3 Data Exploration


You can view details about all the added data assets and add descriptions, tags, security levels, and classifications to databases, tables, and data views to manage data assets by level and classification.


Prerequisites

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

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**.

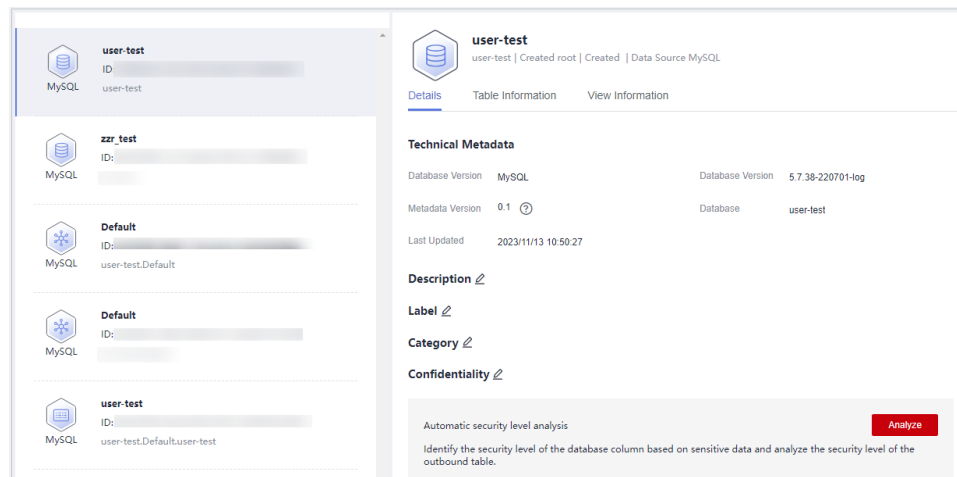
Step 4 In the navigation pane, choose **Asset Management > Data Exploration**.

Step 5 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.

You can also select a template, template category, or security level at the bottom of the search box to filter the database information you want to view.

Step 6 Click a database name to go to the database details page. You can add descriptions, tags, security levels, and classifications to databases, data tables, and data views.

Figure 3-40 Database details



----End



3.4 Asset Catalog

You can view data statistics about different service domains or different types on the **Asset Catalog** page.

Prerequisites

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

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**.
- 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 3-18 Data catalog parameters

Parameter	Description
Statistics	<ul style="list-style-type: none"> ● Sensitive Databases: the percentage of sensitive databases in all databases. ● Sensitive Tables: the percentage of sensitive data tables in all data tables. ● Sensitive 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 Sensitive Columns	Pie chart showing the proportion of sensitive data columns of different security levels in the total data columns
Top 5 Categories	Top 5 data type with the highest proportion
Data Volume	Line chart showing the change of data volume over time
Database Scale Table	<ul style="list-style-type: none"> ● Database instance: database instance name ● Instance ID: instance ID ● Host port: host port number ● User: username

----End

4 Sensitive Data Identification

4.1 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 4-1 Flowchart

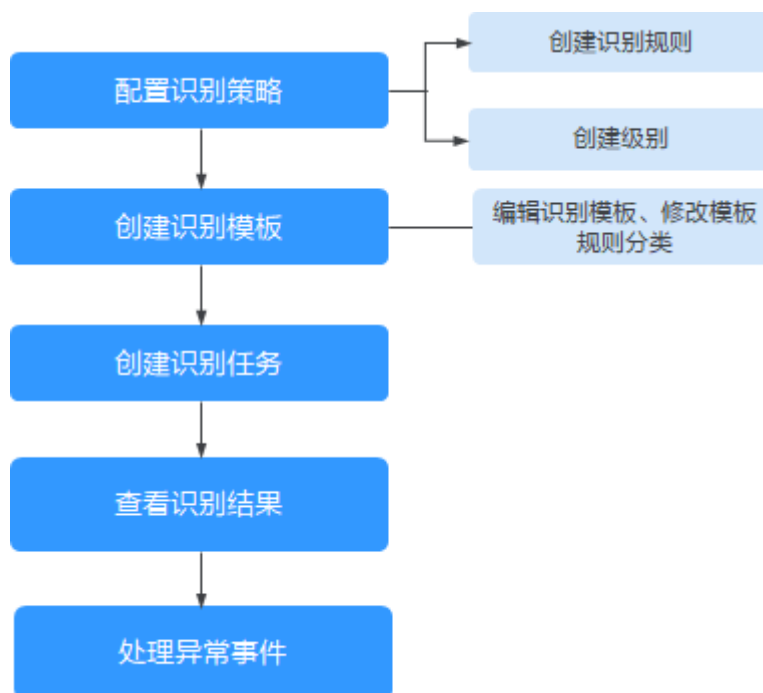


Table 4-1 Functions

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
Identification Template	The built-in templates according to the Huawei Cloud data security classifying and grading standard and best practices are provided. In addition, you can customize new classifying and grading templates to manage scattered rules in a unified manner. These templates are mandatory for creating identification tasks.	Creating an Identification Template

Function	Description	Related Operations
Identification Task	Based on the created identification task, DSC automatically identifies sensitive data in a specified database, OBS bucket, big data source, or MRS, and generates identification results and reports.	Creating an Identification Task
Viewing the Identification Result	After the scanning is complete, you can view the identification result in the identification task list and handle abnormal events based on the identification result.	Viewing the Identification Result

4.2 Sensitive Data Identification Configuration

4.2.1 Creating an Identification Template

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

Constraints

- An identification template cannot be deleted after being created.
- A maximum of 20 identification templates can be created for an account.

Procedure



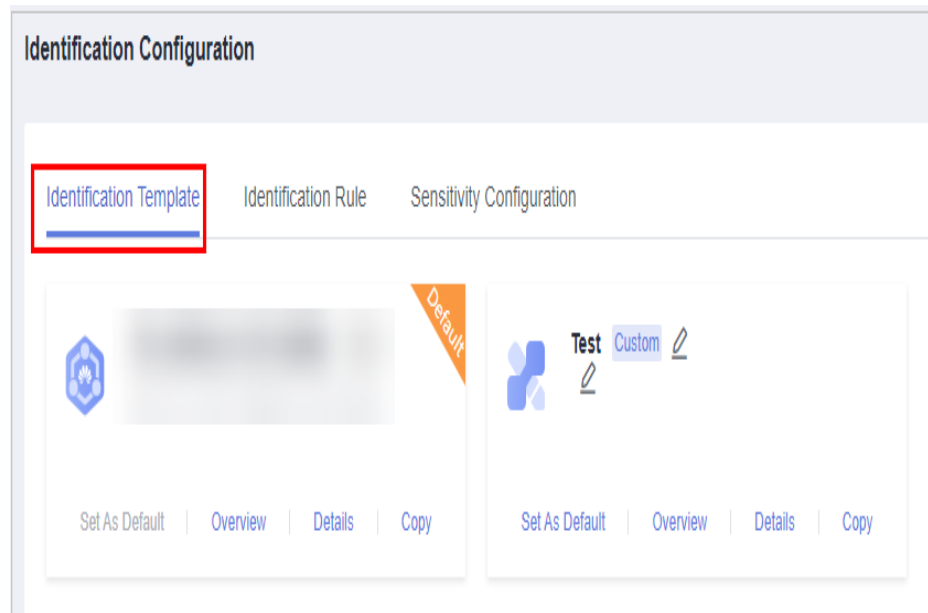
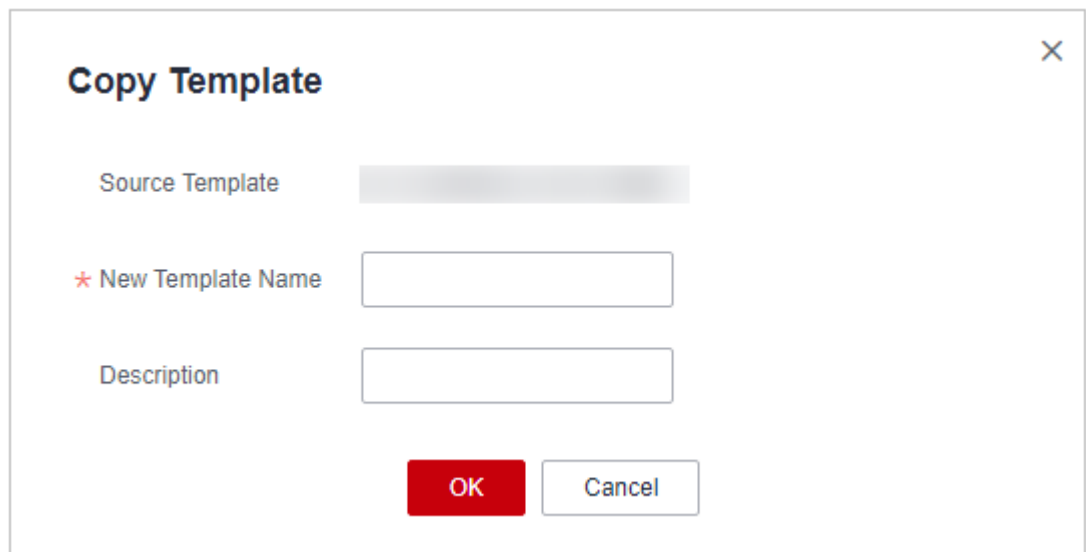
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**, as shown in [Figure 4-2](#).

Figure 4-2 Identification templates



Step 5 Locate the target template, Click **Copy**. In the displayed **Copy Template** dialog box, enter the new template name and description, as shown in [Figure 4-3](#).

Figure 4-3 Replicating a template



Step 6 Click **OK**.

----End

Related Operations

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

4.2.2 Modifying an Identification Template

You can modify a customized template by following the instructions in [Modifying an Identification Template](#).

You can modify the rule category by following the instructions in [Modifying a Template Rule Category](#)

Constraints

A built-in template cannot be modified.

Modifying an Identification Template



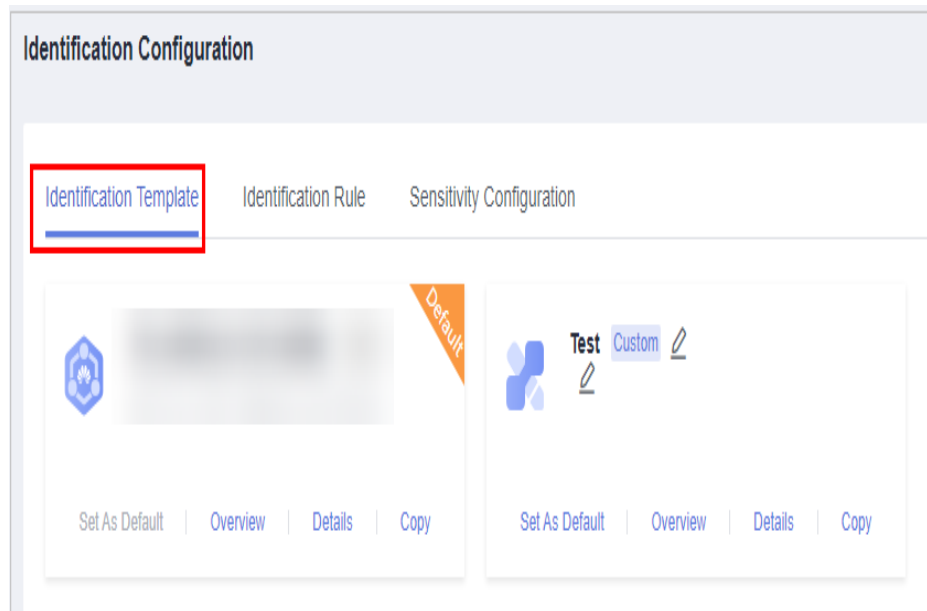
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**, as shown in [Figure 4-4](#).

Figure 4-4 Identification templates







- Step 5** Locate the target template, click **Details**, as shown in [Figure 4-5](#).

Figure 4-5 Template details

The screenshot shows a management console interface. On the left is a navigation pane with a search box 'Enter a category name.' and a tree view showing 'All (4)'. The main area contains a table of rules. At the top of the main area are buttons for 'Add Rule', 'Batch Delete', and 'Modify Class', and a search box 'Enter a rule name.' The table has columns for Rule, Sensitivity Level, Status, Description, and Operation.

Rule	Sensitivity Level	Status	Description	Operation
[Redacted]	L1	<input checked="" type="checkbox"/>	[Redacted]	Details Delete
AWS_ACCESS_KEY	L3	<input checked="" type="checkbox"/>	AWS_ACCESS_KEY	Details Delete
Access_Key_Id	L3	<input type="checkbox"/>	Access_Key_Id	Details Delete

- Move the cursor to a category name:
 - Click  to create a category name.
 - Click  to edit the category name.
 - Click  to delete a category name.
- Click a category name on the left tree and view related category rules on the right. You can select multiple category names.
- 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 the rule.
- Click **Details** in the **Operation** column to edit the rule content.
- Click **Delete** in the **Operation** column to delete a rule.

----End

Modifying a Template Rule Category



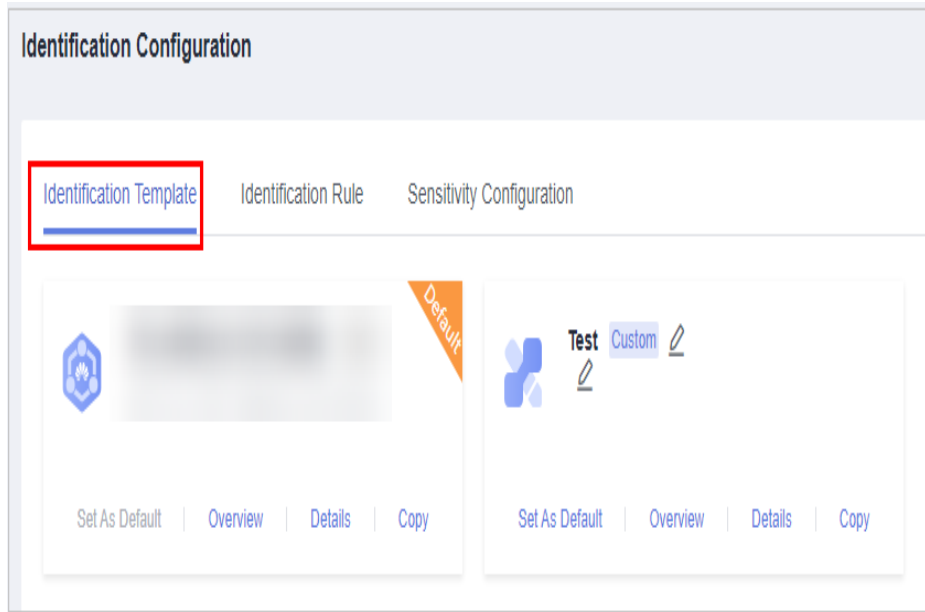
- Step 1** Click  in the upper left corner of the management console and select a region or project.
- Step 2** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 3** In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**, as shown in [Figure 4-6](#).

Figure 4-6 Identification templates



Step 4 Locate the target template, click **Details**.

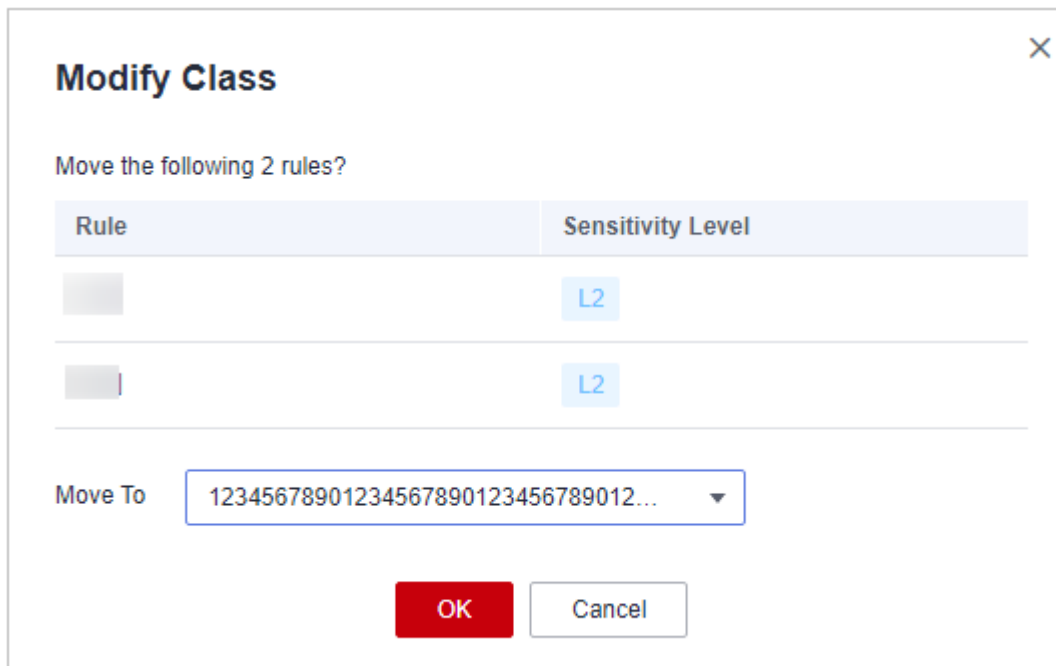
Figure 4-7 Template details



Step 5 Select the rules whose categories are to be modified.

Step 6 Click **Modify Class** in the upper left corner of the rule list. In the displayed dialog box, select the target category.

Figure 4-8 Modifying the category



Step 7 Click **OK**. A message is displayed, indicating that the rule categories are modified.

----End

4.2.3 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



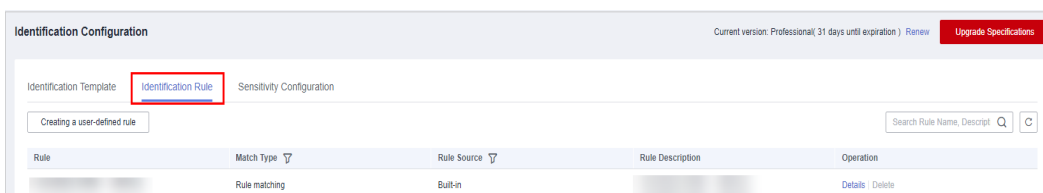
- Step 1** Click  in the upper left corner of the management console and select a region or project.
- Step 2** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 3** In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**.
- Step 4** Click the **Identification Rule** tab, as shown in [Figure 4-9](#).





Figure 4-9 Identification rules




Step 5 Click **Create a user-defined rule** in the upper left corner of the page.

Step 6 In the displayed dialog box, set required parameters based on [Table 4-2](#).

Table 4-2 Parameter description

Parameter	Description
Rule	<p>You can customize a rule name.</p> <p>The rule name must meet the following requirements:</p> <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  to add the rule to multiple templates. • Click  to delete the template. Retain at least one template.
Match Type	<p>This parameter can be set to Rule matching or Keyword matching.</p> <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. <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>
Matching Logic	<p>Select the matching logic:</p> <ul style="list-style-type: none"> • AND: All keywords are included. • OR: Only one keyword is included.
Rule	<ul style="list-style-type: none"> • This parameter is displayed when Match Type is set to Rule Matching. • Click  to add multiple rules. • Click  to delete a rule. Retain at least one rule. <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>
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.

Parameter	Description
Identification Threshold Configuration	Applicable to unstructured data. You can click  to 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 this parameter.

Step 7 Click **OK**.


----End


4.2.4 Editing a Rule

Constraints

Built-in rules cannot be edited.

Procedure

Step 1 Click  in the upper left corner of the management console and select a region or project.

Step 2 In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 3 In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**.

Step 4 Click the **Identification Rule** tab, as shown in [Figure 4-10](#).

Figure 4-10 Identification rules



Step 5 Locate the row that contains the target rule and click **Details** in the **Operation** column to view and modify the rule. You can modify the following information: **Basic Rule Details, Add to Template, Match Condition, and Identification Threshold Configuration**.

----End

Related Operations

If a user-defined sensitive data identification rule is no longer used, locate the rule in the identification rule list, click **Delete** in the **Operation** column.

- Rules in sensitive data identification rule groups cannot be deleted.
- DSC built-in rules cannot be deleted.

4.2.5 Customizing a 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 level cannot be deleted after being 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 pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Sensitive Data Identification > Identification Configuration**.
- 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 4-3](#).

Table 4-3 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.

Figure 4-11 Sensitivity Configuration

Step 7 Click **OK**.

----End

4.2.6 Modifying Level Information


This topic describes how to modify the level information.


Prerequisites

The level to be modified is customized.

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**.

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

Step 5 Click the **Sensitivity Configuration** tab to view the level configuration list, as shown in [Figure 4-12](#).

Figure 4-12 Sensitivity Configuration

Level Name	Level Color	Level Source	Number of References	Description	Operation
L2		Default	247		Edit Enable
L3		Default	211		Edit Enable
L4		Default	220		Edit Enable
L1		Default	120		Edit Enable
		Custom	2		Edit Enable
		Custom	0		Edit Enable

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

4.2.7 Disabling a Level


This topic describes how to disable a level.


Constraints

A built-in level cannot be disabled.

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**.

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

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

Figure 4-13 Sensitivity Configuration



Level Name	Level Color	Level Source	Number of References	Description	Operation
L2		Built-in	247		Enable Disable
L3		Built-in	211		Enable Disable
L4		Built-in	220		Enable Disable
L1		Built-in	128		Enable Disable
		Custom	2		Enable Disable
		Custom	0		Enable Enabled

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

4.3 Sensitive Data Identification Tasks

4.3.1 Creating an Identification Task

Based on the created identification task, DSC automatically identifies sensitive data in a specified database, OBS bucket, big data source, or MRS, and generates identification results and reports.

This topic describes how to create an identification task.

Prerequisites

You have added OBS buckets, databases, or big data sources to the asset list. For details, see [Assets](#).

Procedure



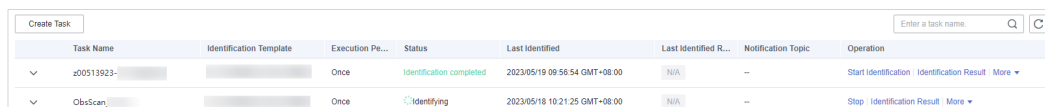
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Sensitive Data Identification > Identification Task**, as shown in [Figure 4-14](#).




Figure 4-14 Identification tasks




Task Name	Identification Template	Execution Pe...	Status	Last Identified	Last Identified R...	Notification Topic	Operation
z00513923-		Once	Identification completed	2023/05/19 09:56:54 GMT+08:00	N/A	--	Start Identification Identification Result More
ObsScan		Once	Identifying	2023/05/18 10:21:25 GMT+08:00	N/A	--	Stop Identification Result More

- 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 4-4](#).

Table 4-4 Parameter description

Parameter	Description	Example Value
Start Task	Indicates whether to enable the sensitive data identification task. By default, the task is started. <ul style="list-style-type: none">  : enabled  : disabled 	
Task Name	You can customize the task name. The task name must meet the following requirements: <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. 	Test task_01

Parameter	Description	Example Value
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 OBS Assets.• Database: DSC is authorized to access your database and identify sensitive data in the database assets. For details about how to add database assets, see Database Assets.• Big Data: DSC is authorized to access your big data source assets and identify sensitive data in the big data source assets. For details about how to add big data source assets, see Big Data Assets.• MRS: DSC is authorized to access your Hive assets and identify sensitive data in the Hive assets. For details, see MRS Assets.	Database
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>	Huawei Cloud Data Security Classifying and Grading Template
Identification Period	<p>Set the execution policy of the data identification task.</p> <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.	Once
When to Execute	<p>This parameter is displayed when Identification Period is set to Once.</p> <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.	Now

Parameter	Description	Example Value
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 Viewing the Identification Result.	None

Step 7 Click **OK**. A message is displayed indicating the task is created successfully.

----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.

4.3.2 Starting a Task

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

Prerequisites

You have added OBS buckets, databases, or big data sources to the asset list. For details, see [Assets](#).

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**.
- Step 4** In the navigation pane, choose **Sensitive Data Identification > Identification Task**, as shown in [Figure 4-15](#).

Figure 4-15 Identification tasks

Task Name	Identification Template	Execution Pe...	Status	Last Identified	Last Identified R...	Notification Topic	Operation
z00513923-		Once	Identification completed	2023/05/19 09:56:54 GMT+08:00	N/A	--	Start Identification Identification Result More
ObsScan		Once	Identifying	2023/05/18 10:21:25 GMT+08:00	N/A	--	Stop Identification Result More

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.

----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.

4.3.3 Identification Tasks

You can view details about the sensitive data identification task in the task list.

Prerequisites

You have added OBS buckets, databases, or big data sources to the asset list. For details, see [Assets](#).

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 pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane on the left, click **Sensitive Data Identification > Identification Task**, as shown in [Figure 4-16](#). [Table 4-5](#) describes the parameters.

Figure 4-16 Identification tasks

Task Name	Identification Template	Execution Pe...	Status	Last Identified	Last Identified R...	Notification Topic	Operation
z00513923-		Once	Identification completed	2023/05/19 09:56:54 GMT+08:00	N/A	--	Start Identification Identification Result More
ObsScan		Once	Identifying	2023/05/18 10:21:25 GMT+08:00	N/A	--	Stop Identification Result More

Table 4-5 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 an identification task.• Click Start Identification to start an identification task.• Click Identification Result to view the identification result.• Click Delete to delete an identification job.
Identification Template	Identification template name
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 task, including the built-in level and custom level. For details, see Customizing a Level .

Parameter	Description
Operation	<p>Operations provided in the Operation column:</p> <ul style="list-style-type: none"> Execute an identification task immediately. For details, see Starting a Task. View the identification result. Click Identification Result to go to the result details page. DSC provides a detailed result analysis report. For details, see Viewing the Identification Result. 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



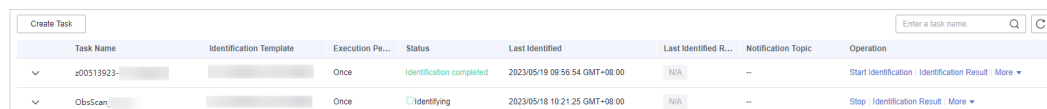
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Sensitive Data Identification > Identification Task**, as shown in [Figure 4-17](#).

Figure 4-17 Identification tasks





Task Name	Identification Template	Execution Pe...	Status	Last Identified	Last Identified R...	Notification Topic	Operation
z00513923		Once	Identification completed	2023/05/19 09:56:54 GMT+08:00	N/A	--	Start Identification Identification Result More ▾
ObsScan		Once	Identifying	2023/05/18 10:21:25 GMT+08:00	N/A	--	Stop Identification Result More ▾

- 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

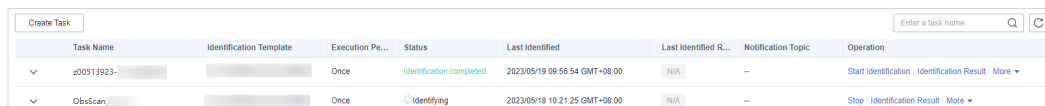
Deleting an Identification Task

- Step 1** Click  in the upper left corner of the management console and select a region or project.

Step 2 In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 3 In the navigation pane, choose **Sensitive Data Identification > Identification Task**, as shown in [Figure 4-18](#).

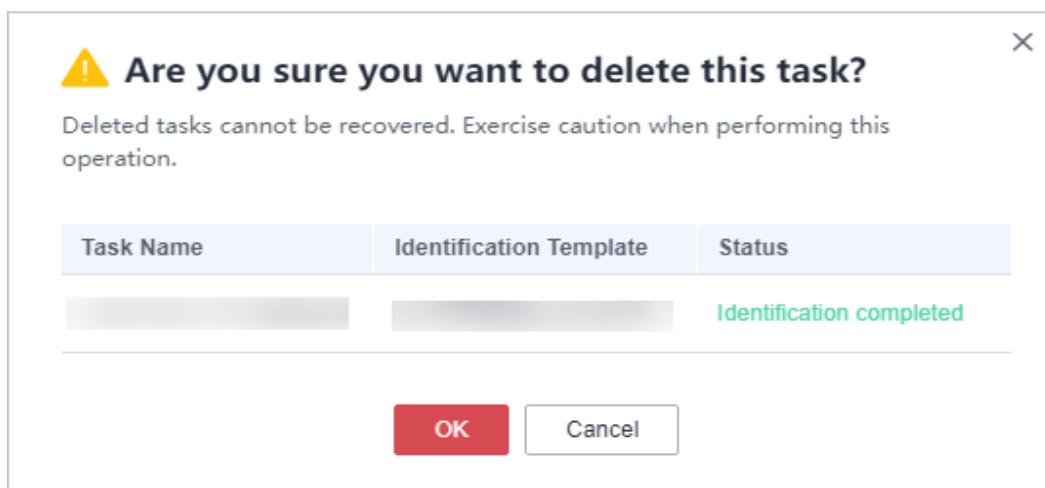
Figure 4-18 Identification tasks



Task Name	Identification Template	Execution Pe...	Status	Last Identified	Last Identified R...	Notification Topic	Operation
s00513923-		Once	Identification completed	2023/05/19 09:56:54 GMT+08:00	N/A	--	Start Identification Identification Result More ▾
ObsScan-		Once	Identifying	2023/05/18 10:21:25 GMT+08:00	N/A	--	Stop Identification Result More ▾

Step 4 Locate the row that contains the target task and choose **More > Delete** in the **Operation** column, as shown in [Figure 4-19](#).

Figure 4-19 Confirming the deletion



Step 5 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

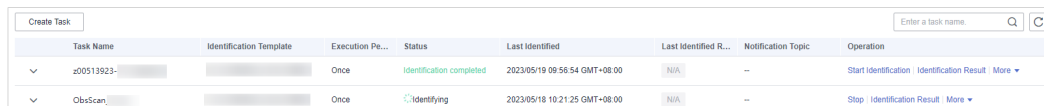
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Sensitive Data Identification > Identification Task**, as shown in [Figure 4-20](#).

Figure 4-20 Identification tasks



Task Name	Identification Template	Execution Pe...	Status	Last Identified	Last Identified R...	Notification Topic	Operation
z00513923-		Once	Identification completed	2023/05/19 09:56:54 GMT+08:00	N/A	--	Start Identification Identification Result More
ObsScan-		Once	Identifying	2023/05/18 10:21:25 GMT+08:00	N/A	--	Stop Identification Result More

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

4.3.4 Viewing the Identification Result


After completing the sensitive data identification task, you can view the results by clicking **Identification Result** in the **Operation** column of the corresponding task in the identification task list. The results will show you the total number of sensitive information items, their risk levels, and their classification and grading results.


Prerequisites

At least one sensitive data identification task has been executed.

Procedure

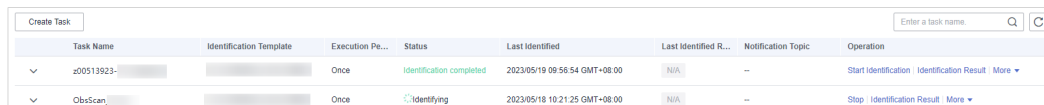
Step 1 Log in to the management console.

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**.

Step 4 In the navigation pane, choose **Sensitive Data Identification > Identification Task**, as shown in [Figure 4-21](#).

Figure 4-21 Identification tasks



Task Name	Identification Template	Execution Pe...	Status	Last Identified	Last Identified R...	Notification Topic	Operation
z00513923-		Once	Identification completed	2023/05/19 09:56:54 GMT+08:00	N/A	--	Start Identification Identification Result More
ObsScan-		Once	Identifying	2023/05/18 10:21:25 GMT+08:00	N/A	--	Stop Identification Result More

Step 5 Click **Identification Result** in the **Operation** column of the target task to view the identification result, as shown in [Figure 4-22](#).

DSC collects statistics on the number and distribution of risk levels for different types of data sources, such as big data, database, OBS, and MRS.

DSC also provides a detailed list of identification results for scanned objects. You can filter the results by task name, asset type, or asset name in the upper left corner of the page. **Table 4-6** describes the parameters in the identification result list.

Figure 4-22 Identification result details



Table 4-6 Identification result parameters

Parameter	Description
Asset	Name of the asset that can be identified
Asset Type	<ul style="list-style-type: none"> • OBS • Database • Big Data • MRS
Asset	Name of the asset containing sensitive information.
Object Path	Path of the sensitive information object.
Level	Sensitive information level.

Step 6 In the row containing the desired scan object, click **View Categorizing and Leveling Result Details** in the **Operation** column. The **Categorizing and Leveling Result Details** dialog box is displayed, as shown in **Figure 4-23**.

Figure 4-23 Categorizing and leveling results

Categorizing and Leveling Results [X]

Identification Object Details

Object [Redacted] Object Path [Redacted]

Asset shanjie Asset Type OBS

Level **L4**

Result Details

Rule	Level	Category	Categorizing and Lev...
[Redacted]	L2	[Redacted]	[Redacted] ...

NOTE

- The **Categorizing and Leveling Result Details** page displays the identification object details and identification result details.
- The result details include the matching rule, leveling result, identification result, and categorizing and leveling template.

----End



5 Data Privacy Protection

5.1 Configuring GaussDB(DWS) and MRS Hive

Before using database watermarks, you have to:

1. **Modifying GaussDB(DWS) Cluster Parameters**
To identify sensitive data and enable privacy protection, you must 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 5-1](#). Retain the default values for other parameters.

Table 5-1 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: *
Allow Conditions	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. You need to configure the Select Group , Select User , and Add Permissions columns. <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. 	Example: <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

5.2 Data Masking

5.2.1 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. [Data Masking Algorithms](#) 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 an 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 precision marketing.

Data Masking Process

Figure 5-1 Static data masking flowchart

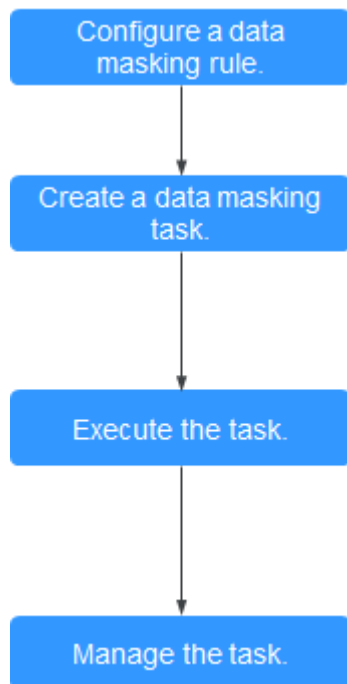
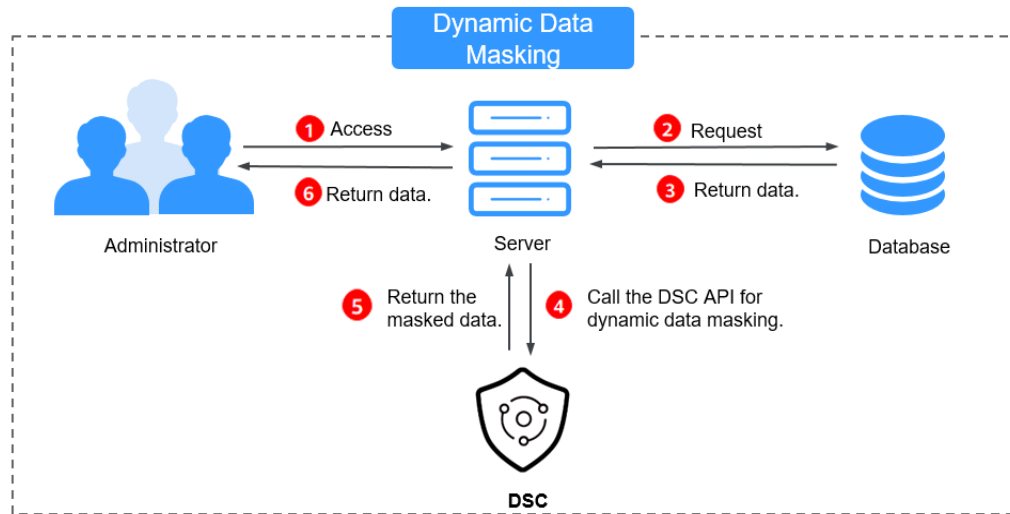


Figure 5-2 Dynamic data masking flowchart



Data Masking Algorithms

Table 5-2 Masking algorithms

Data Masking Algorithms	Description	Application Scenarios
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: Key information Application scenario: data storage
Encryption	<p>Use the encryption algorithms and master key to implement 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 scenario: data storage

Data Masking Algorithms	Description	Application Scenarios
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: 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

Data Masking Algorithms	Description	Application Scenarios
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

Data Masking Algorithms	Description	Application Scenarios
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. 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. 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. 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. 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. 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. Number roundup Rounds a specified number. 	<ul style="list-style-type: none"> Sensitive data: General data Application scenarios: <ul style="list-style-type: none"> Data storage Data usage

5.2.2 Configuring a Data Masking Rule

This section describes how to configure a data masking rule. For more information about masking algorithms, see [Overview](#).

Procedure

Step 1 Log in to the management console.



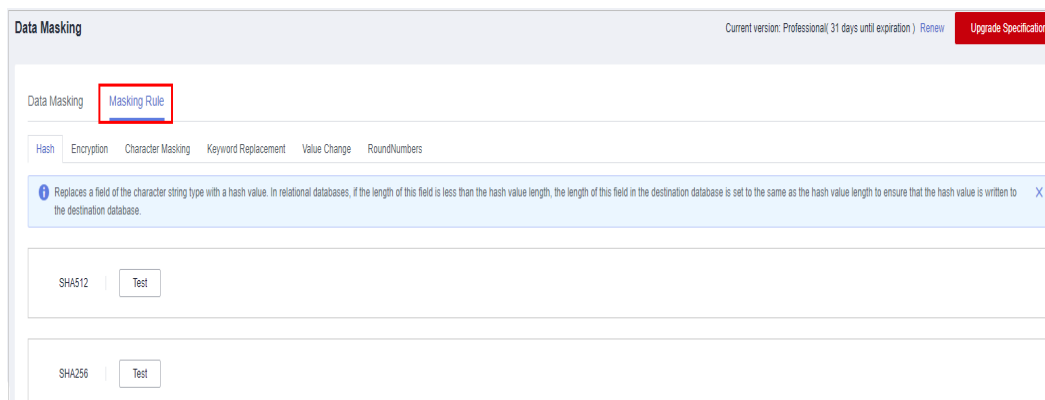
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Data Privacy Protection > Data Masking**. On the page displayed, click the **Masking Rule** tab.

Figure 5-3 Accessing the Masking Rule tab



- Step 5** On the **Masking Rule** tab page, select a proper masking method and configure a masking rule.
- If you select **Hash**, configure a masking rule according to [Hash](#).
 - If you select **Encryption**, configure a masking rule according to [Encryption](#).
 - If you select **Character Masking**, configure a masking rule according to [Character Masking](#).
 - If you select **Keyword Replacement**, configure a masking rule according to [Keyword Replacement](#).
 - If you select **Value Change**, configure a masking rule according to [Value Change](#).
 - If you select **Roundup**, configure a masking rule according to [Roundup](#).

----End

Hash

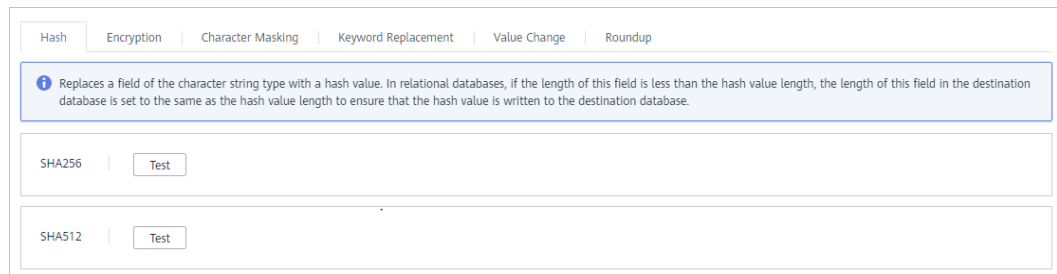
This method is used to replace a field of the string type with a hash value. In a relational database, if the field length is less than the hash length, the length of the field in the destination database is set to be the same as the hash value length to ensure that the hash value is completely written 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** Access the **Masking Rule** page by referring to [Procedure](#).

Step 2 Click the **Hash** tab.

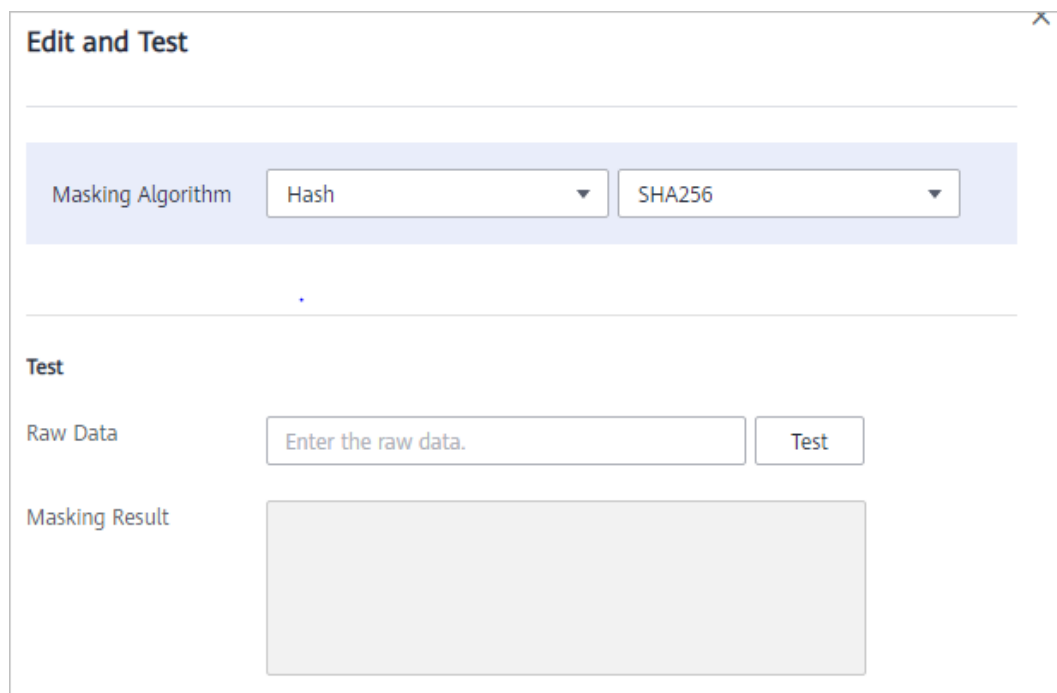
Figure 5-4 Hash



Step 3 In the column where the SHA-256 or SHA-512 algorithm is, click **Test**.

Step 4 On the page displayed, enter the raw data and click **Test**. The masking result will be displayed in the **Masking Result** text box.

Figure 5-5 Hash method



----End

Encryption

This method masks data using encryption algorithms and a master key. In the encryption and data masking result, the first 16 bytes of an encrypted string is the initialization vector (IV), and the rest is the enciphered text.

Step 1 Access the **Masking Rule** page by referring to [Procedure](#).

Step 2 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.


- KMS Key:** If you have created a master key in other Huawei Cloud services, select the created master key from the drop-down list box. If you do not have a master key, click **Create KMS Key** to go to the DEW console and create one. For details, see [Creating a CMK](#).

Figure 5-6 Encryption

Step 3 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 Access the **Masking Rule** page by referring to [Procedure](#).

Step 2 Click the **Character Masking** tab.

Figure 5-7 Character masking method

Name	Rule	Mask	Example	Operation
Landline Number	Retain first 3 and last 4 characters...	*	010****1234	Edit and Test

Step 3 Click **Add** to configure a character masking rule.

Figure 5-8 Adding a character masking rule

Add Character Masking Rule

Name

Rule

Rule Variable N M

Masking Method

Masked with

Test

Raw Data

Masking Result

Step 4 Enter the raw data and click **Test**. The masking result will be displayed in the **Masking Result** text box.

Step 5 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 `abcdefghijklkioij`, the keyword is `bcde`, and the replacement string is `12`, the masking result is `a12fg12fgkioij`.

Step 1 Access the **Masking Rule** page by referring to [Procedure](#).

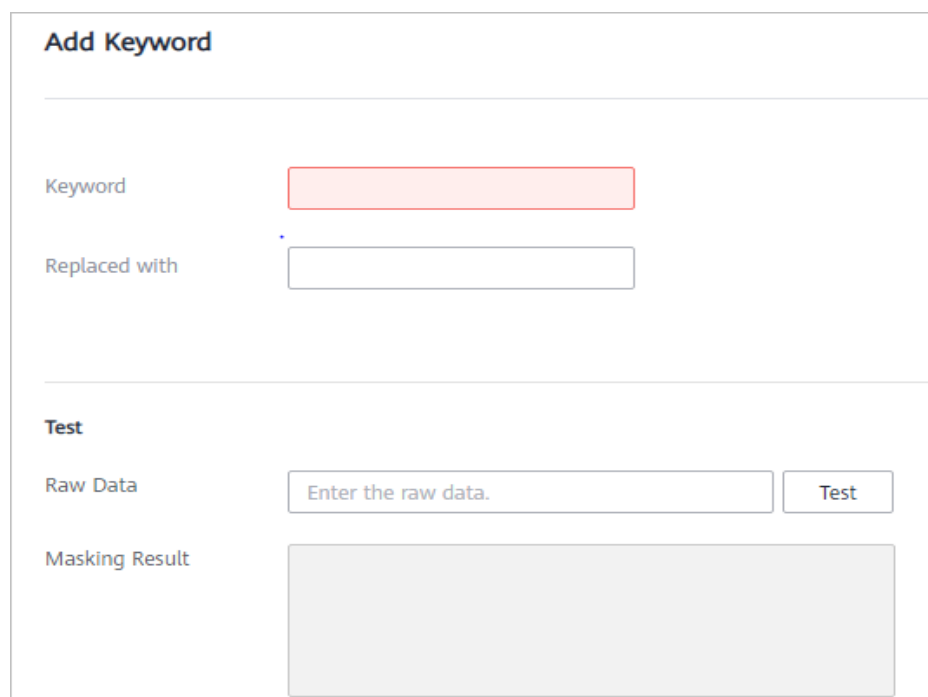
Step 2 Click the **Keyword Replacement** tab.

Figure 5-9 Keyword Replacement

Keyword	Replaced with	Operation
2	3	Edit and Test Delete

Step 3 Set the keyword and the replacement string.

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

Figure 5-10 Adding a keyword

Add Keyword

Keyword

Replaced with

Test

Raw Data

Masking Result

Step 4 Enter the raw data and click **Test**. The masking result will be displayed in the **Masking Result** text box.

Step 5 Verify the testing result and click **Save**.

- To modify a configured masking rule, locate the row containing the rule and click **Edit and Test** in the **Operation** column.
- To delete a configured masking rule, locate the row containing the rule and click **Delete** in the **Operation** column.

----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 a Custom 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 Access the **Masking Rule** page by referring to [Procedure](#).

Step 2 Click the **Value Change** tab.

Figure 5-11 Value Change

Hash	Encryption	Character Masking	Keyword Replacement	Value Change	Roundup
Masking Using the Null Value Sets the target field to Null.					
Masking Using a Custom Value Sets the target field to a default value.					
Numeral Type 1024 -> 0, 0.123 -> 0.0, 0xef -> 0x00					
Character String Type text -> "					
Date/Time Types in the Database Character String Type					
Timestamp Type in the Database "1575604312"->"0"					

----End

Roundup

Step 1 Access the **Masking Rule** page by referring to [Procedure](#).

Step 2 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.

Figure 5-12 Roundup masking algorithms

The screenshot displays the 'Roundup' configuration page. At the top, there are tabs for 'Hash', 'Encryption', 'Character Masking', 'Keyword Replacement', 'Value Change', and 'Roundup'. The 'Date Roundup' section contains the following configurations:

- Roundup of fields after the year field: "2019-05-12 -> 2019-01-01" or "2019-05-12 08:08:08 -> 2019-01-01 00:00:00"
- Roundup of fields after the month field: "2019-05-12 -> 2019-05-01" or "2019-05-12 08:08:08 -> 2019-05-01 00:00:00"
- Roundup of fields after the day field: "2019-05-12 -> 2019-05-12" or "2019-05-12 08:08:08 -> 2019-05-12 00:00:00"
- Roundup of fields after the hour field: "08:08:08 -> 08:00:00" or "2019-05-12 08:08:08 -> 2019-05-12 08:00:00"
- Roundup of fields after the minute field: "08:08:08 -> 08:08:00" or "2019-05-12 08:08:08 -> 2019-05-12 08:08:00"
- Roundup of fields after the second field: "08:08:08.123 -> 08:08:08.000" or "1575612731312 -> 1575612731000"

At the bottom, the 'Number Roundup' section shows 'Roundup Result' as '0.1' and an 'Edit and Test' button.

Step 3 In the **Number Roundup** area, click **Edit and Test** to configure the rounding value.

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 5-13 Number roundup

The screenshot shows the configuration and testing interface for the 'Number Roundup' algorithm. The 'Masking Algorithm' is set to 'Roundup' and the specific algorithm is 'Number Roundup'. The 'Roundup Result' is configured to '0.1'. In the 'Test' section, the 'Raw Data' field contains the placeholder text 'Enter the raw data.', and there is a 'Test' button. Below the 'Raw Data' field is the 'Masking Result' output area, which is currently empty.

Step 4 Enter the raw data and click **Test**. The masking result will be displayed in the **Masking Result** text box.

Step 5 Verify the testing result and click **Save**.

----End

5.2.3 Managing Static Data Masking Tasks

5.2.3.1 Creating and Running a Database Masking Task

Creating a database masking task to mask sensitive information in a specified database. This section describes how to create a database masking task.

Prerequisites


- DSC has been allowed to access cloud assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- Database assets have been added. For details, see [Authorizing RDS Databases](#).
- Sensitive data has been identified by referring to [Creating an Identification Task](#).


Constraints

Supported data sources include **SQLServer, MySQL, PostgreSQL, TDSQL, DMDBMS, KingBase, Oracle, GaussDB(DWS), and OpenGauss.**

Creating and Running a Database Masking Task

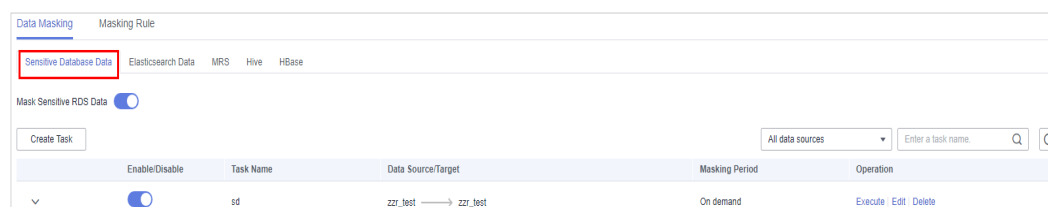
Step 1 Log in to the management console.


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

Step 3 In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 4 In the left navigation pane, choose **Data Privacy Protection > Static Data Masking**.

Figure 5-14 Database data masking



Step 5 On the **Database Masking** tab page, click  to enable database data masking.

Step 6 Click **Create Task**. On the displayed **Configure Data Source** page, configure parameters according to [Table 5-3](#).

Figure 5-15 Configuring a database data masking task

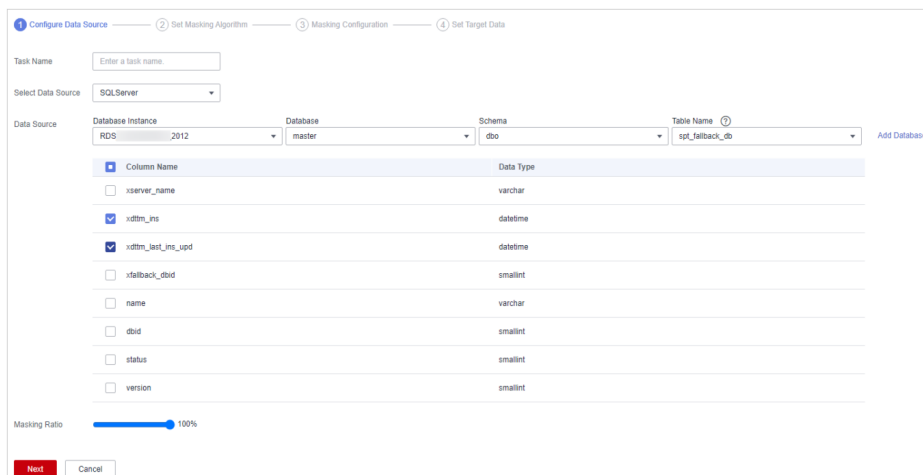
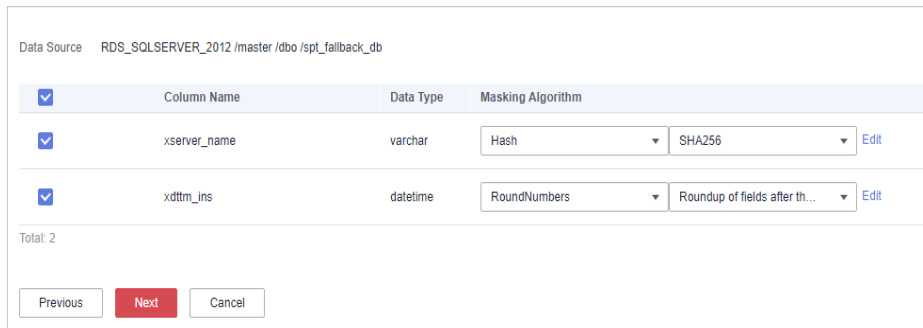


Table 5-3 Datas source parameters

Parameter	Description
Task Name	<p>You can create a custom name for a data masking task.</p> <p>The task name must meet the following requirements:</p> <ul style="list-style-type: none"> It can contain 1 to 255 characters. Only letters, numbers, underscores (_), and hyphens (-) are allowed.
Select Data Source	Select a data source. Possible values are SQLServer , MySQL , TDSQL , PostgreSQL , DMDBMS , KingBase , Oracle , DWS , or OpenGauss .
Data Source	<p>Database instance: Select the database instance where the data you want to mask is.</p> <p>Database: Select the name of the database where the data you want to mask is.</p> <p>Schema: This parameter is available only when SQLServer, KingBase, OpenGauss, PostgreSQL, or DWS is selected for Data Source.</p> <p>Table name: Select the name of the database table where the data you want to mask is.</p> <p>Data Type: Selecting the check box will copy the data in this column to the target database.</p>
NOTE	If no cloud databases are available, click Add Database to add a cloud database. For details, see Adding a Cloud Database .
Masking Ratio	You can drag the slider to select the masking ratio of the data in the database. For example, if the database contains 1000 rows of data and you drag the slider to 80%, the first 800 rows of data in the database are masked.

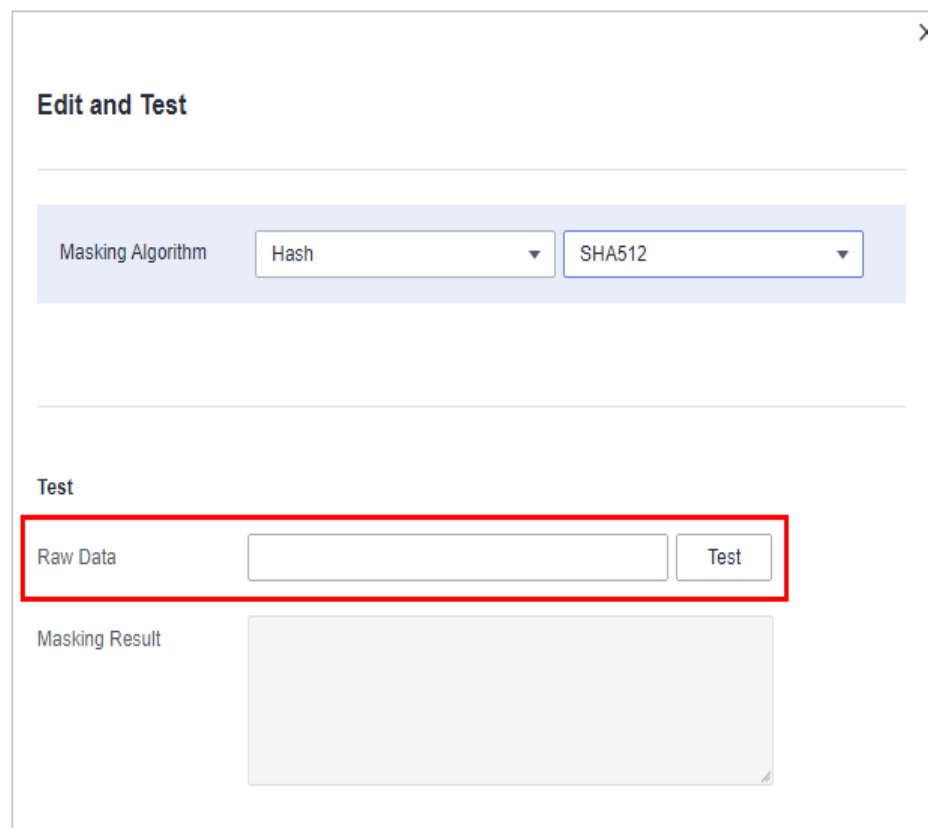
Step 7 Click **Next**.

Figure 5-16 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 a Data Masking Rule](#).
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 a Data Masking Rule](#).

Figure 5-17 Editing test

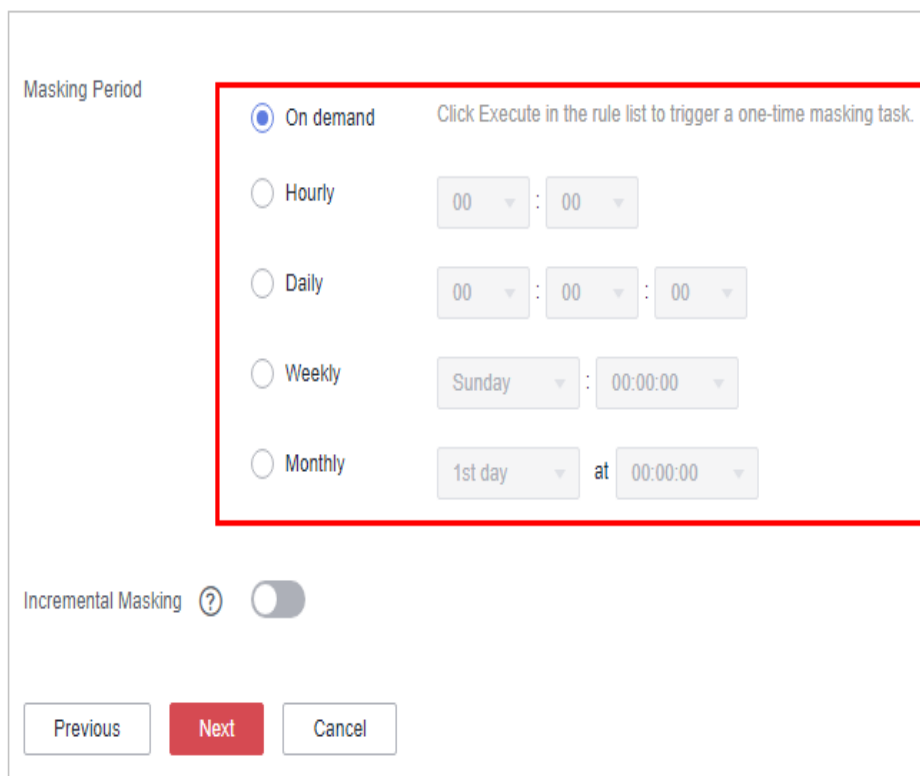


Step 8 Click **Next**.

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

 **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**.

Figure 5-18 Masking period

Masking Period



On demand Click Execute in the rule list to trigger a one-time masking task.

Hourly 00 : 00

Daily 00 : 00 : 00

Weekly Sunday : 00:00:00

Monthly 1st day at 00:00:00

Incremental Masking  

Previous **Next** Cancel

Select and set the execution period of a masking task.

- **Manual:** Manually enable a masking task and execute it based on masking rules.
- **Hourly:** A data masking task is executed every several hours.
For example, to execute a data masking task every two hours, set this parameter to **02:00**.
- **Daily:** A data masking task is executed at a specified time every day.
For example, to execute a data masking task at 12:00 every day, set this parameter to **12:00:00**.
- **Weekly:** A data masking task is executed at a specified time every week.
For example, to execute a data masking task at 12:00 every Monday, set this parameter to 12:00:00 every Monday.

- Monthly:** A data masking task is executed at a specified time on a specified day every month.

For example, to execute a data masking task 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 need to execute a data masking task on the 31st day of each month and the month has fewer than 31 days, the system automatically executes the task on the last day of the month.

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

Figure 5-19 Configuring a target data type

Database Instance RDS_SQLSERVER_2012	Database master	Schema dbo	Table Name Enter a table name.
Data Source Column		Target Column	
xserver_name		xserver_name	
xdtm_ins		xdtm_ins	
Previous		Finish	
		Cancel	

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

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

If the data table name you entered 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.

- 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 **Database** tab. Locate the row containing the target data masking task and click **Execute** in the **Operation** column.


Figure 5-20 Executing a database data masking task

	Enable/Disable	Task Name	Data Source/Target	Masking Period	Operation
▼		test-mysql-1000W	test-tuomin → test-tuomin	On demand	Execute Edit Delete

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

----End


Viewing the Status of a Database Data Masking Task

- On the **Database** tab page, click  of the target data masking task to view its execution status.

The statuses are as follows:

- 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.

Figure 5-21 Data masking task statuses



Enable/Disable	Task Name	Data Source/Target	Masking Period	Operation
	test-mysql-1000W	test-luomin → test-luomin	On demand	Execute Edit Delete
Start Time	End Time	Execution Method	Executed Lines	Status
2023/07/05 18:51:11 GMT+08:00	2023/07/05 19:23:18 GMT+08:00	On demand	10000000	Completed

Editing and Deleting a Database Data Masking Task

A data masking task in the **Pending execution** or **Running** state cannot be edited or deleted.



- In the database data masking task list, locate the row containing the target data masking task and click **Edit** in the **Operation** column to reconfigure masking task information. For details, see [Creating and Running a Database Masking Task](#).

Figure 5-22 Editing a database data masking task

Enable/Disable	Task Name	Data Source/Target	Masking Period	Operation
	encrypt_test	student → student	On demand	Execute Edit Delete
	mask-test	student → student	On demand	Execute Edit Delete

- In the database data masking task list, locate the row containing the target data masking task and click **Delete** in the **Operation** column.

Figure 5-23 Deleting a database data masking task

Enable/Disable	Task Name	Data Source/Target	Masking Period	Operation
	test-mysql-1000W	test-luomin → test-luomin	On demand	Execute Edit Delete
	test-mysql-100W	test-luomin → test-luomin	On demand	Execute Edit Delete



Deleted data masking tasks cannot be recovered.

5.2.3.2 Creating and Running an Elasticsearch Data Masking Task

Create an Elasticsearch data masking task to mask sensitive information in tables or columns in a specified Elasticsearch data source.

This section describes how to create an Elasticsearch data masking task.

Prerequisites


- DSC has been allowed to access cloud assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- Elasticsearch assets have been added by referring to [Big Data Assets](#).
- Sensitive data has been identified by referring to [Creating an Identification Task](#).


Constraints

Currently, only **Elasticsearch** is supported.

Creating and Running an Elasticsearch Data Masking Task

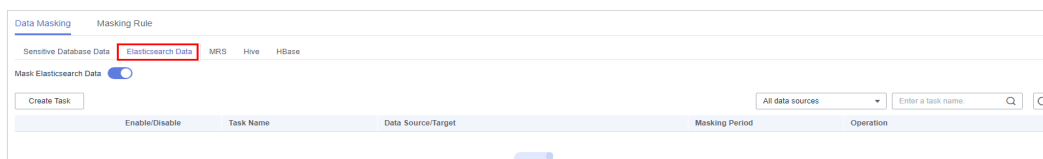
Step 1 Log in to the management console.



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

Step 3 In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 4 In the left navigation pane, choose **Data privacy protection > Perform static data masking** and click the **Elasticsearch** tab. The Elasticsearch masking page is displayed.

Figure 5-24 Elasticsearch data masking



Step 5 Click  and set **Elasticsearch** to  to enable Elasticsearch masking.

Step 6 Click **Create Task** and configure parameters according to [Table 5-4](#).

Figure 5-25 Selecting Elasticsearch as the data source

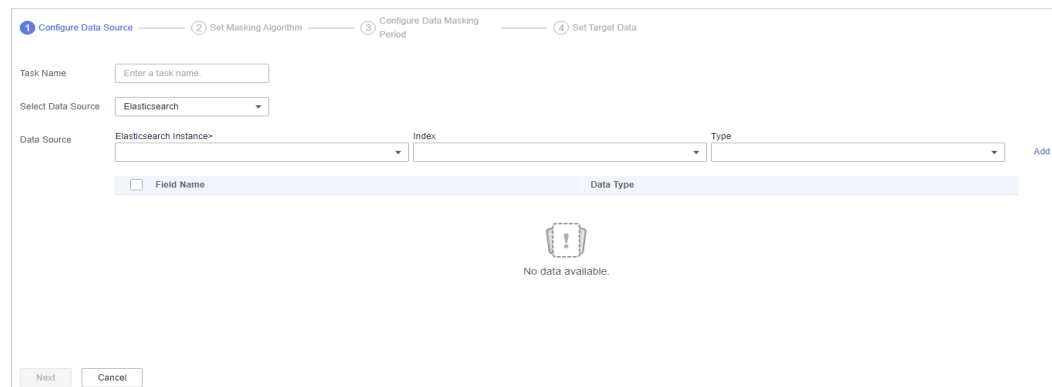
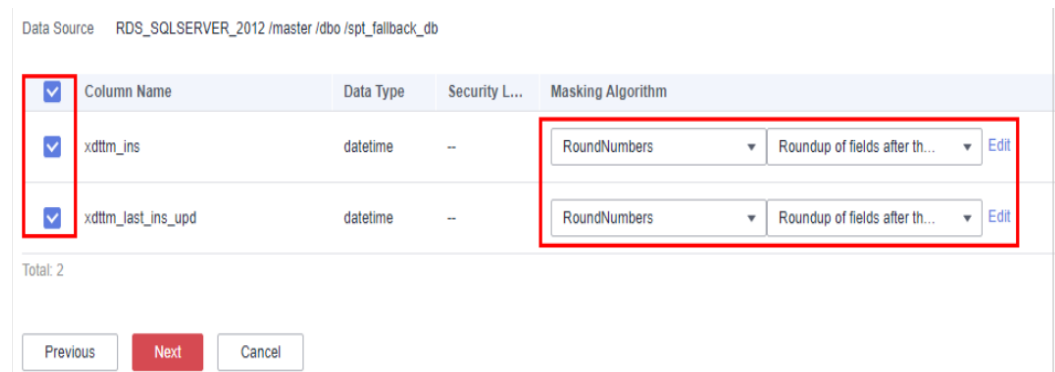


Table 5-4 Datas source parameters

Parameter	Description
Task Name	<p>You can create a custom name for a data masking task.</p> <p>The task name must meet the following requirements:</p> <ul style="list-style-type: none"> • It can contain 1 to 255 characters. • Only letters, numbers, underscores (_), and hyphens (-) are allowed.
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.
<p>NOTE</p> <p>If no Elasticsearch assets are available, click Add to add one. For details, see Big Data Assets.</p>	Index: Select the index where the data to be masked is.
	Type: Select the type of the data to be masked.
	Click Add to add an Elasticsearch asset. For details, see Big Data Assets .

Step 7 Click **Next**.

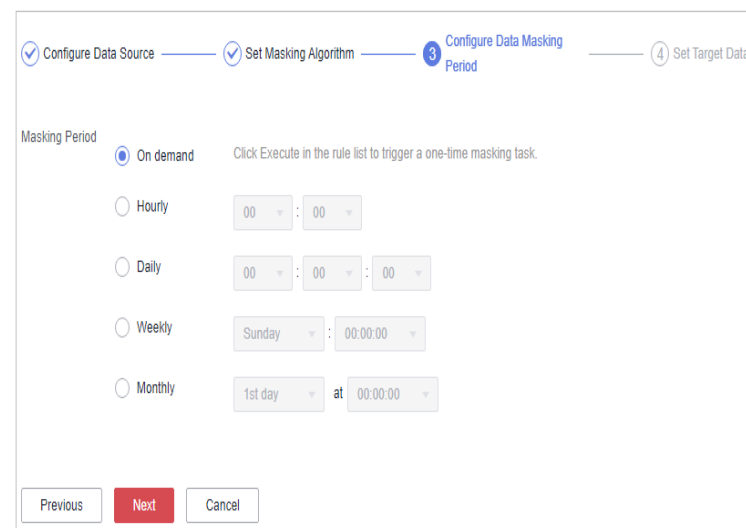
Figure 5-26 Configuring a masking algorithm



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

Step 8 Click **Next**.

Figure 5-27 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:** A data masking task is executed every several hours.
For example, to execute a data masking task every two hours, set this parameter to **02:00**.
- **Daily:** A data masking task is executed at a specified time every day.
For example, to execute a data masking task at 12:00 every day, set this parameter to **12:00:00**.
- **Weekly:** A data masking task is executed at a specified time every week.
For example, to execute a data masking task at 12:00 every Monday, set this parameter to 12:00:00 every Monday.

- Monthly:** A data masking task is executed at a specified time on a specified day every month.

For example, to execute a data masking task 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 need to execute a data masking task on the 31st day of each month and the month has fewer than 31 days, the system automatically executes the task on the last day of the month.

Step 9 Click **Next**.

Figure 5-28 Setting target data

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.

Figure 5-29 Executing an Elasticsearch data masking task

	Enable/Disable	Task Name	Data Source/Target	Masking Period	Operation
▼		test-mysql-1000W	test-tuomin → test-tuomin	On demand	Execute Edit Delete

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


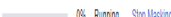

Viewing the Status of an Elasticsearch Data Masking Task

- On the **Elasticsearch** tab page, click  of the target data masking task to view its execution status.

The statuses are as follows:

- 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.

Figure 5-30 Data masking task statuses

Enable/Disable	Task Name	Data Source/Target	Masking Period	Operation
	test-hive-1000V	default → default	On demand	Execute Edit Delete
Start Time ↓				
End Time		Execution Method	Status	
2023/07/06 09:51:46 GMT+08:00	1970/01/01 08:00:00 GMT+08:00	On demand	 0%	Running Stop Masking
2023/07/04 11:35:17 GMT+08:00	2023/07/04 11:37:41 GMT+08:00	On demand		Failed

Editing and Deleting an Elasticsearch Data Masking Task

A data masking task in the **Pending execution** or **Running** state cannot be edited or deleted.

- In the Elasticsearch data masking task list, locate the row containing the target data masking task and click **Edit** in the **Operation** column to modify masking task information. For details, see [Creating and Running an Elasticsearch Data Masking Task](#).

Figure 5-31 Editing an Elasticsearch data masking task

Enable/Disable	Task Name	Data Source/Target	Masking Period	Operation
	wf1gh1gh1j	test → test	01:00 every hour	Execute Edit Delete

- In the Elasticsearch data masking task list, locate the row containing the target data masking task and click **Delete** in the **Operation** column.

Figure 5-32 Deleting an Elasticsearch data masking task**CAUTION**

Deleted data masking tasks cannot be recovered.

5.2.3.3 Creating and Running an MRS Data Masking Task

Create an MRS data masking task to mask sensitive information of specified data.

This section describes how to create an MRS data masking task.

Prerequisites


- DSC has been allowed to access cloud assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- You have added MRS assets. For details, see [Adding MRS Assets](#).
- Permissions on MRS Hive have been configured by referring to [Modifying Hive User Rights](#).
- Sensitive data has been identified by referring to [Creating an Identification Task](#).


Constraints

Currently, only **MRS_HIVE** is supported.

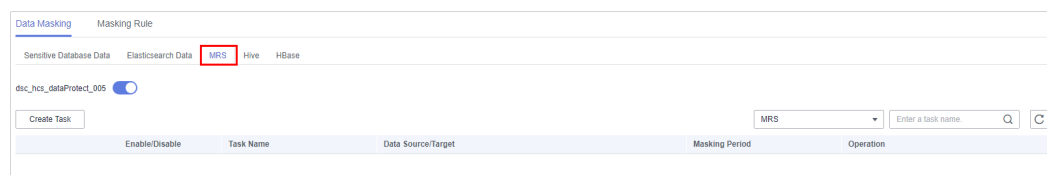
Creating and Running an MRS Data Masking Task

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 pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 4 In the left navigation pane, choose **Data privacy protection > Perform static data masking** and click the **MRS** tab. The MRS masking page is displayed.

Figure 5-33 MRS data masking

Step 5 On the **MRS** tab, click  to enable MRS data masking.

Step 6 Click **Create Task** and configure parameters according to [Table 5-5](#).

Figure 5-34 Configuring the data source

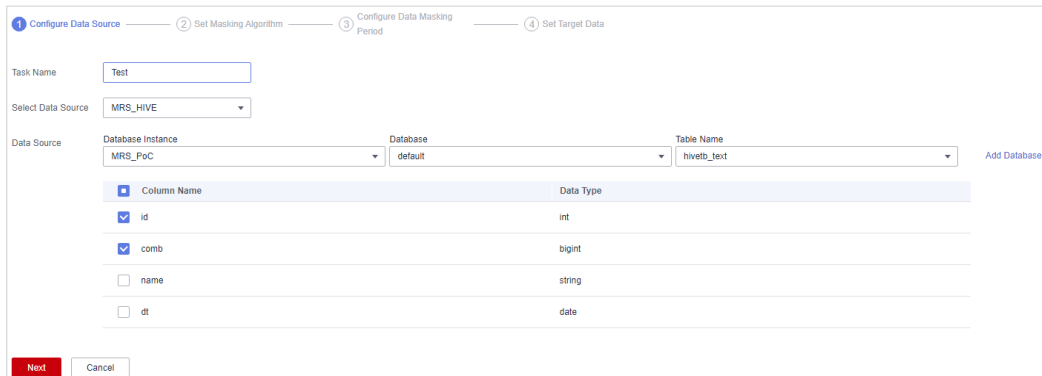


Table 5-5 Datas source parameters

Parameter	Description
Task Name	You can create a custom name for a data masking task. The task name must meet the following requirements: <ul style="list-style-type: none"> It can contain 1 to 255 characters. Only letters, numbers, underscores (_), and hyphens (-) are allowed.
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.
NOTE If no data is available, click Add Database to add database assets. For details, see Adding a Cloud Database .	Database: Select the name of the database where the data you want to mask is.
	Table name: Select the name of the database table where the data you want to mask is.
	Select a column name and copy the data in the column to the target database.

Step 7 Click **Next**.

Figure 5-35 Setting a masking algorithm

<input checked="" type="checkbox"/>	Column Name	Data Type	Masking Algorithm
<input checked="" type="checkbox"/>	name	string	Hash SHA256 Edit
<input checked="" type="checkbox"/>	distance	double	Value Change Masking Using a Custom ... Edit

Total: 2

[Previous](#) [Next](#) [Cancel](#)

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

Step 8 Click **Next**.**Figure 5-36** Masking period

Masking Period

On demand Click Execute in the rule list to trigger a one-time masking task.

Hourly 00 : 00

Daily 00 : 00 : 00

Weekly Sunday : 00:00:00

Monthly 1st day at 00:00:00

[Previous](#) [Next](#) [Cancel](#)

Select and set the execution period of a masking task.

- **Manual:** Manually enable a masking task and execute it based on masking rules.
- **Hourly:** A data masking task is executed every several hours.
For example, to execute a data masking task every two hours, set this parameter to **02:00**.
- **Daily:** A data masking task is executed at a specified time every day.
For example, to execute a data masking task at 12:00 every day, set this parameter to **12:00:00**.
- **Weekly:** A data masking task is executed at a specified time every week.
For example, to execute a data masking task at 12:00 every Monday, set this parameter to 12:00:00 every Monday.

- **Monthly:** A data masking task is executed at a specified time on a specified day every month.

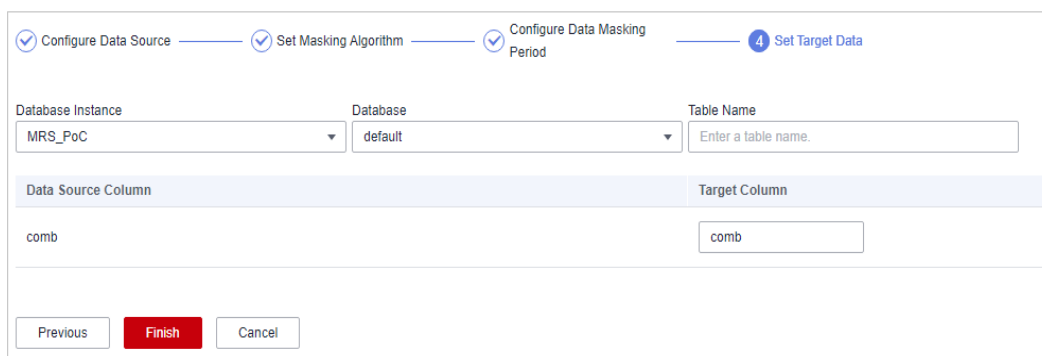
For example, to execute a data masking task at 12:00 on the 12th day of each month, set this parameter to 12:00:00 12th day of every month.

 **NOTE**

If you need to execute a data masking task on the 31st day of each month and the month has fewer than 31 days, the system automatically executes the task on the last day of the month.

Step 9 Click **Next**.

Figure 5-37 Setting target data



Database Instance	Database	Table Name
MRS_PoC	default	Enter a table name.

Data Source Column	Target Column
comb	comb

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

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

If the data table name you entered 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 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 **MRS** 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.

----End






Viewing the Status of an MRS Data Masking Task

- On the **MRS** tab page, click  of the target data masking task to view its execution status.

The statuses are as follows:

- 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.

Figure 5-38 MRS data masking task statuses

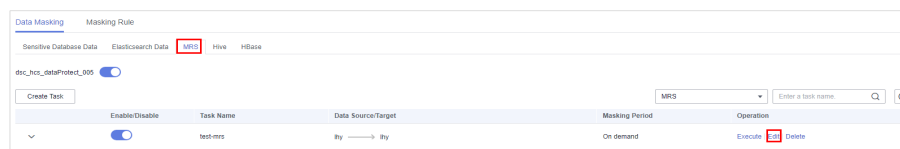
Enable/Disable	Task Name	Data Source/Target	Masking Period	Operation
	test-mrs	lby → lby	On demand	Execute Edit Delete
Start Time ↓ End Time Execution Method Status				
	2023/07/04 11:30:22 GMT+08:00	2023/07/04 11:36:10 GMT+08:00	On demand	 Completed
	2023/06/28 12:37:39 GMT+08:00	2023/06/28 12:41:22 GMT+08:00	On demand	 Completed
	2023/06/28 11:42:40 GMT+08:00	--	On demand	 Stopped
	2023/06/28 11:14:34 GMT+08:00	--	On demand	 Stopped

Editing and Deleting an MRS Data Masking Task

A data masking task in the **Pending execution** or **Running** state cannot be edited or deleted.

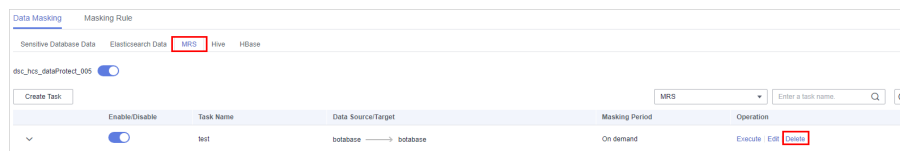
- In the MRS data masking task list, locate the row containing the target data masking task and click **Edit** in the **Operation** column to modify masking task information. For details, see [Creating and Running an MRS Data Masking Task](#).

Figure 5-39 Editing an MRS data masking task



- In the MRS data masking task list, locate the row containing the target data masking task and click **Delete** in the **Operation** column.

Figure 5-40 Deleting an MRS data masking task



Deleted data masking tasks cannot be recovered.

5.2.3.4 Creating and Running a Hive Masking Task

You can mask sensitive Hive data.

This section describes how to create a data masking task for Hive.

Prerequisites

- DSC has been allowed to access cloud assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- Hive assets have been added. For details, see [Big Data Assets](#).
- Sensitive data has been identified by referring to [Creating an Identification Task](#).

Constraints

Currently, only **HIVE** is supported.

Creating and Running a Hive Masking Task




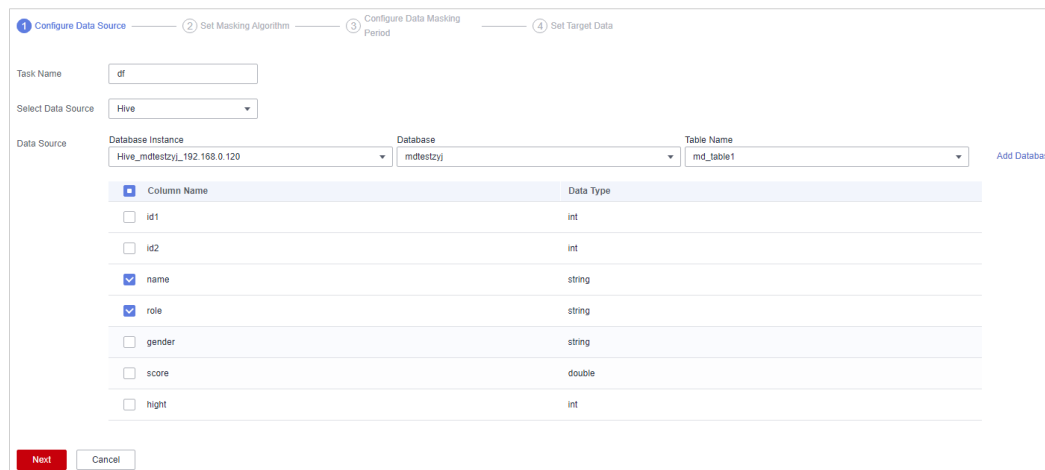
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Data privacy protection > Perform static data masking** and click the **Hive** tab. The **Hive anonymization** page is displayed.
- Step 5** On the **Hive anonymization** tab page, click  and set **Hive anonymization** to enable.
- Step 6** Click **Create Task** and configure required parameters. [Table 5-6](#) describes the parameters.

Figure 5-41 Configuring the data source



The screenshot displays the 'Configure Data Source' step of a Hive masking task configuration. The interface includes a progress bar with four steps: 1. Configure Data Source (active), 2. Set Masking Algorithm, 3. Configure Data Masking Period, and 4. Set Target Data. The 'Task Name' field is set to 'df'. The 'Select Data Source' dropdown is set to 'Hive'. The 'Data Source' section shows the 'Database Instance' as 'Hive_mdtestzy_192.168.0.120', the 'Database' as 'mdtestzy', and the 'Table Name' as 'md_table1'. A table lists columns and their data types, with checkboxes for selection:

Column Name	Data Type
<input type="checkbox"/> id1	int
<input type="checkbox"/> id2	int
<input checked="" type="checkbox"/> name	string
<input checked="" type="checkbox"/> role	string
<input type="checkbox"/> gender	string
<input type="checkbox"/> score	double
<input type="checkbox"/> hight	int

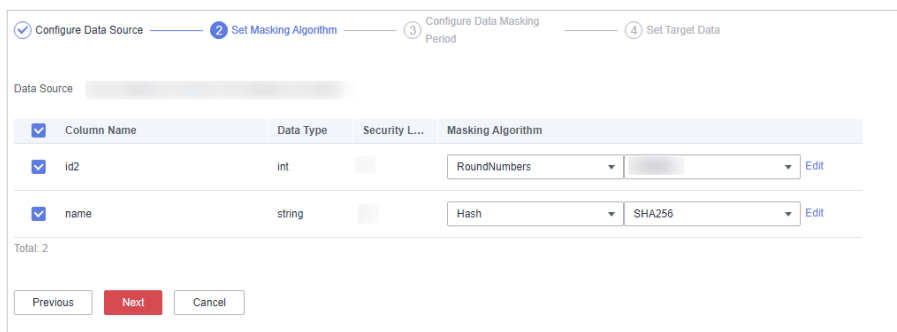
At the bottom, there are 'Next' and 'Cancel' buttons.

Table 5-6 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. Only Hive is supported.
Data Source	<p>Database Instance: Select the database instance where the data you want to mask is located.</p> <p>Database: Select the name of the database where the data you want to mask is located.</p> <p>Table Name: Select the name of the database table where the data you want to mask is located.</p> <p>If you select the check box, data in this column is copied to the Data Type column.</p>
NOTE	If no data is available, click Add Database to add database assets. For details, see Big Data Assets .

Step 7 Click **Next**.

Figure 5-42 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 a Data Masking Rule](#).

Step 8 Click **Next**.

Figure 5-43 Masking period

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

Masking Period

On demand Click Execute in the rule list to trigger a one-time masking task.

Hourly 00 : 00

Daily 00 : 00 : 00

Weekly Sunday : 00:00:00

Monthly 1st day at 00:00:00

Previous Next Cancel

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**.

Figure 5-44 Setting target data

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

Checking the Running Status of a Hive Data Masking Task

- On the **Hive** tab page, view the task running status, as shown in [Running status of the Hive data masking task](#).

The task statuses are described as follows:

- **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.

Figure 5-45 Running status of the Hive data masking task

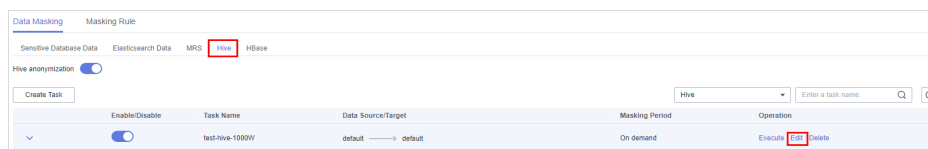
Enable/Disable	Task Name	Data Source/Target	Masking Period	Operation
<input type="checkbox"/>	test-hive-1000W	default -> default	On demand	Execute Edit Delete
Start Time	End Time	Execution Method	Status	
2023/07/09 00:51:46 GMT+08:00	1970/01/01 08:00:00 GMT+08:00	On demand	0% Running	Stop Masking
2023/07/04 11:35:17 GMT+08:00	2023/07/04 11:37:41 GMT+08:00	On demand	Failed	

Editing and Deleting a Hive Data Masking Task

A masking task in the **Waiting** or **Running** status cannot be edited or deleted.

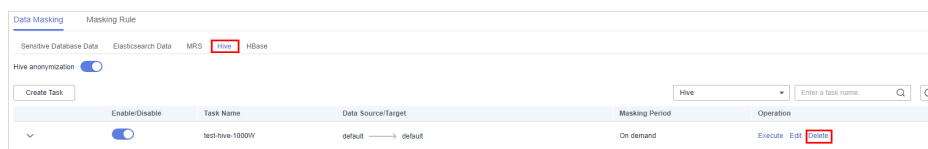
- In the **Hive** data masking task list, click **Edit** in the **Operation** column. For details about how to configure masking task information, see [Creating and Running a Hive Masking Task](#).

Figure 5-46 Editing a Hive data masking task



- In the **Hive** data masking task list, click **Delete** in the **Operation** column.

Figure 5-47 Deleting a Hive data masking task



CAUTION

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

5.2.3.5 Creating and Running an HBase Masking Task

Create a data masking task for a data set to mask sensitive information.

This section describes how to create a data masking task for HBase.

Prerequisites


- DSC has been allowed to access cloud assets. For details, see [Allowing or Disallowing Access to Cloud Assets](#).
- HBase assets have been added. For details, see [Big Data Assets](#).
- Sensitive data has been identified by referring to [Creating an Identification Task](#).

Constraints

Currently, only **HBase** is supported.

Creating and Running an HBase Masking 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 pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation pane, choose **Data privacy protection > Perform static data masking** and click the **HBase** tab. The **HBase anonymization** page is displayed.
- Step 5** On the **HBase anonymization** page, click  to set **HBase anonymization** enabled.
- Step 6** Click **Create Task** and configure required parameters. [Table 5-7](#) describes the parameters.

Figure 5-48 Configuring the data source

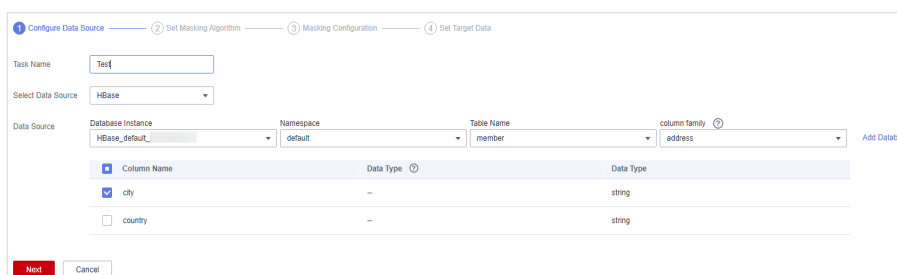


Table 5-7 Parameter description

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 HBase is supported.
Data Source	Database instance: Select the database instance where the data you want to mask is located.
NOTE If no data is available, click Add Database to add database assets. For details, see Big Data Assets .	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 the check box, data in this column is copied to the Data Type column.

- Step 7** Click **Next**.

Figure 5-49 Setting a masking algorithm

Column Name	Data Type	Masking Algorithm	
city	string	Hash	SHA256 Edit

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

Step 8 Click **Next**.

Figure 5-50 Masking period

Masking Period

On demand Click Execute in the rule list to trigger a one-time masking task.

Hourly 00 : 00

Daily 00 : 00 : 00

Weekly Sunday : 00:00:00

Monthly 1st day at 00:00:00

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**.

Figure 5-51 Setting target data

Database Instance	Namespace	Table Name	column family
HBase_default_	default	member	Please enter a column family name.
Data Source Column	Target Column		
city	<input type="text" value="city"/>		
country	<input type="text" value="country"/>		
<input type="button" value="Previous"/> <input type="button" value="Finish"/> <input type="button" value="Cancel"/>			

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

Checking the Running Status of a HBase Data Masking Task

- On the **HBase** page, click  to view the masking task status, as shown in [Figure 5-52](#).

The task statuses are described as follows:

- **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.

Figure 5-52 HBase masking task running status

Start Time	End Time	Execution Method	Status
2023/07/04 11:35:49 GMT+08:00	2023/07/04 11:35:54 GMT+08:00	On demand	Failed
2023/07/03 21:20:02 GMT+08:00	2023/07/03 21:20:13 GMT+08:00	On demand	Failed

Editing and Deleting a HBase Data Masking Task

A masking task in the **Waiting** or **Running** status cannot be edited or deleted.

- In the **HBase** data masking task list, click **Edit** in the **Operation** column. For details about how to configure masking task information, see [Creating and Running an HBase Masking Task](#).

Figure 5-53 Editing an HBase data masking task

Task Name	Data Source/Target	Masking Period	Operation
test_hbase	default -> default	On demand	Execute Edit Delete
HBase_Mask_Test	default -> default	On demand	Execute Edit Delete

- In the **HBase** data masking task list, click **Delete** in the **Operation** column.

Figure 5-54 Deleting an HBase data masking task

Task Name	Data Source/Target	Masking Period	Operation
test_hbase	default -> default	On demand	Execute Edit Delete
HBase_Mask_Test	default -> default	On demand	Execute Edit Delete



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

5.2.4 Dynamic Data Masking

DSC provides a dynamic masking API with which you can input parameters to perform dynamic masking. For details, see [Masking Sensitive Data](#).

5.3 Data Watermarking

5.3.1 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 5-8 Supported database types

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

Table 5-9 Supported file types

Type	Format
Document	PDF, PPT, Word, and Excel
Image	*.jpg, *.jpeg, *.jpe, *.png, *.bmp, *.dib, *.rle, *.tiff, *.tif, *.ppm, *.webp, *.tga, *.tpic, and *.gif
JSON data	The value can be an integer, floating-point number, or string.

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**.

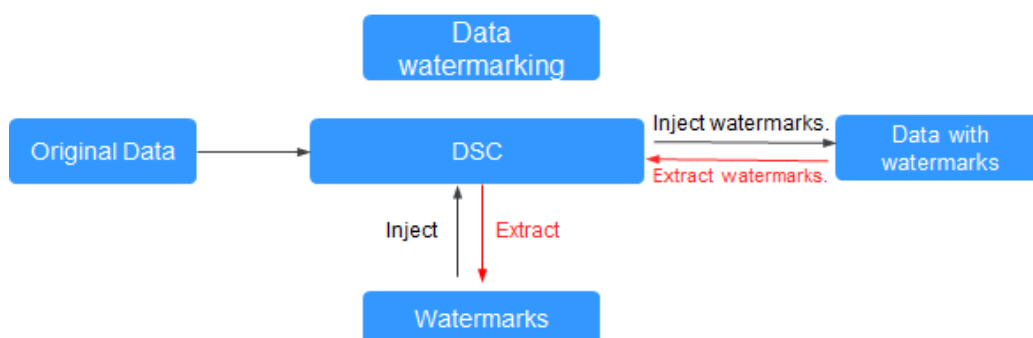
- **Data copyright protection:** In scenarios where digital works are downloaded or copied for use and database services (data mining and analysis) provide data to third parties, digital watermarks can be used to identify the copyright when disputes occur,
- **Source tracing:** Data provided for internal 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 5-55 Data watermarking process



5.3.2 Database Watermarking

5.3.2.1 Inserting Watermarks

Prerequisites

- DSC has been allowed to access cloud assets.
- Database assets have been added. For details, see [Database Assets](#).
- You have added MRS assets. For details, see [Adding MRS Assets](#).
- You have configured the GaussDB(DWS) and MRS_Hive permissions. For details, see [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

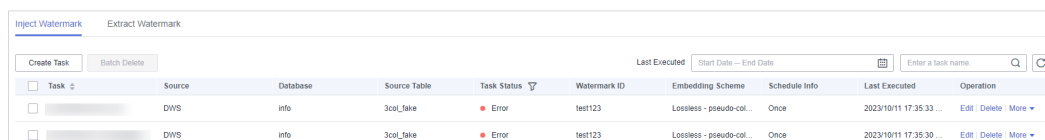
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Data privacy protection > Database Watermark**.

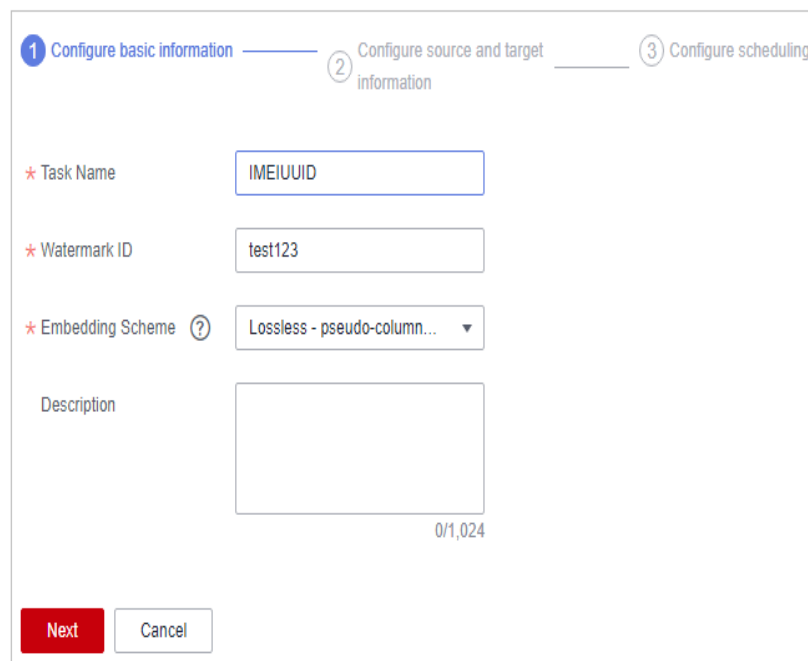
Figure 5-56 Database watermark injection



Task	Source	Database	Source Table	Task Status	Watermark ID	Embedding Scheme	Schedule Info	Last Executed	Operation
<input type="checkbox"/>	DWS	info	3col_fake	Error	test123	Lossless - pseudo-col...	Once	2023/10/11 17:35:33 ...	Edit Delete More
<input type="checkbox"/>	DWS	info	3col_fake	Error	test123	Lossless - pseudo-col...	Once	2023/10/11 17:35:30 ...	Edit Delete More

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

Figure 5-57 Configuring basic information



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

* Task Name:

* Watermark ID:

* Embedding Scheme:

Description:

0/1,024

Next

Table 5-10 Parameters for configuring basic information

Parameter	Description
Task Name	Enter a task name.
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.

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 5-58 Pseudocolumn watermarks

Table 5-11 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">▪ GaussDB(DWS): For details about how to add assets, see Adding a Cloud Database.▪ MRS_HIVE: For details about how to add assets, see Adding MRS Assets.– When Embedding Scheme is set to Lossless-column watermark or Lossless-line watermark, the following data types are supported:<ul style="list-style-type: none">▪ GaussDB(DWS): For details about how to add assets, see Adding a Cloud Database.▪ PostgreSQL: For details about how to add assets, see Adding a Self-Built Database.▪ MySQL: For details about how to add assets, see Adding a Self-Built Database.
Database Instance	Select a Database Instance from the drop-down list.
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 pseudocolumns,
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 5-59 Pseudo-line watermark

The screenshot shows a configuration wizard with three steps: 1. Configure basic information, 2. Configure source and target information (current step), and 3. Configure scheduling information. The 'Source Settings' section includes:

- Data Source Type: DWS
- Database Instance: dsc_test
- Database: info
- Schema: fake
- Source Table: 1col
- Number of pseudo-line spans: 1

The 'Target Settings' section includes:

- Target Table: fd

At the bottom, there are three buttons: 'Previous', 'Next' (highlighted in red), and 'Cancel'.

Table 5-12 Source and destination parameters of pseudo-line watermarks

Parameter	Description	Example Value
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">– GaussDB(DWS): For details about how to add assets, see Adding a Cloud Database.– PostgreSQL: For details about how to add assets, see Adding a Self-Built Database.– MySQL: For details about how to add assets, see Adding a Self-Built Database.	DWS
Database Instance	Select a Database Instance from the drop-down list.	DWS-dsc-Test
Database	Select a Database from the drop-down list.	gaussdb
Mode	This parameter is displayed when Database is DWS or PostgreSQL . Click a Mode as required.	pg_catalog
Source Table	Click and select the corresponding source data table name.	pg_proc
Number of Pseudo-Line Spans	Enter the number of pseudo lines. The value must be a valid integer greater than 1.	10
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.	Test_Table

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

Figure 5-60 Lossy column watermarks

The screenshot displays the configuration interface for lossy column watermarks, specifically the 'Configure source and target information' step. It is divided into three main sections: Source Settings, Watermark Embedding Bar, and Target Settings.

- Source Settings:** Includes dropdown menus for Data Source Type (DWS), Database Instance (DWS-zsy-dscTest), Database (gaussdb), Schema (lhy), and Source Table (table_name_2).
- Watermark Embedding Bar:** A table with columns 'Column Name' and 'Source Data Type'. It lists 'column_name' (integer) and 'column_name2' (character varying), both with checked checkboxes.
- Target Settings:** Includes a text input field for Target Table (fd).

Navigation buttons at the bottom include 'Previous', 'Next' (highlighted in red), and 'Cancel'.

Table 5-13 Source and destination parameters of lossy column watermarks

Parameter	Description	Example Value
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"> GaussDB(DWS): For details about how to add assets, see Adding a Cloud Database. MRS-HIVE: For details about how to add an asset, see Adding MRS Assets. 	DWS
Database Instance	Select a Database Instance from the drop-down list.	DWS-dsc-Test
Database	Select a Database from the drop-down list.	gaussdb

Parameter	Description	Example Value
Mode	This parameter is displayed when the Database is DWS . Click a Mode as required.	pg_catalog
Source Table	Select the corresponding Source Table name.	pg_proc
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.	Test_Table

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

Figure 5-61 Configuring scheduling

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

* Scheduling Parameter Once Daily Weekly Monthly

* Start Time

- 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

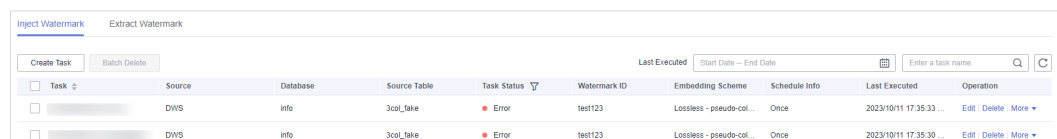
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Data privacy protection > Database Watermark**.

Figure 5-62 Database watermark injection



Task	Source	Database	Source Table	Task Status	Watermark ID	Embedding Scheme	Schedule Info	Last Executed	Operation
<input type="checkbox"/>	DWS	info	3col_like	Error	test123	Lossless - pseudo-col...	Once	2023/10/11 17:35:33 ...	Edit Delete More
<input type="checkbox"/>	DWS	info	3col_like	Error	test123	Lossless - pseudo-col...	Once	2023/10/11 17:35:30 ...	Edit Delete More


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

----End

Enable Task

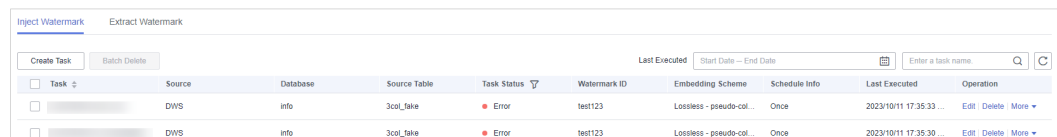
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Data privacy protection > Database Watermark**.

Figure 5-63 Database watermark injection



Task	Source	Database	Source Table	Task Status	Watermark ID	Embedding Scheme	Schedule Info	Last Executed	Operation
<input type="checkbox"/>	DWS	info	3col_like	Error	test123	Lossless - pseudo-col...	Once	2023/10/11 17:35:33 ...	Edit Delete More
<input type="checkbox"/>	DWS	info	3col_like	Error	test123	Lossless - pseudo-col...	Once	2023/10/11 17:35:30 ...	Edit Delete More


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

----End

Stopping a Task

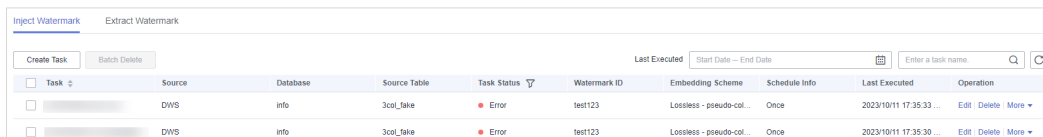
Step 1 Log in to the management console.

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

Step 3 In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Data privacy protection > Database Watermark**.

Figure 5-64 Database watermark injection



Task	Source	Database	Source Table	Task Status	Watermark ID	Embedding Scheme	Schedule Info	Last Executed	Operation
<input type="checkbox"/>	DWS	info	3col_fake	Error	test123	Lossless - pseudo-col...	Once	2023/10/11 17:35:33	Edit Delete More
<input type="checkbox"/>	DWS	info	3col_fake	Error	test123	Lossless - pseudo-col...	Once	2023/10/11 17:35:30	Edit Delete More

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

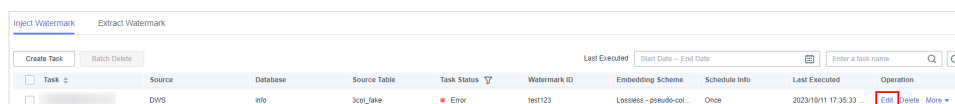
----End

Editing and Deleting an Embedded Watermark Task

The status of embedded watermark task is **Waiting** or **Execution** and the task cannot be edited or deleted.

- Click **Edit** in the **Operation** column to modify the watermark embedding task configuration.

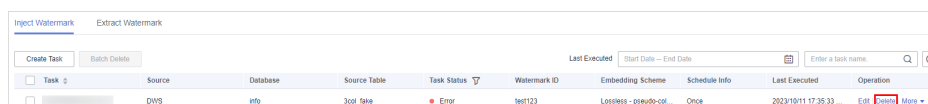
Figure 5-65 Edit embedded watermark task



Task	Source	Database	Source Table	Task Status	Watermark ID	Embedding Scheme	Schedule Info	Last Executed	Operation
<input type="checkbox"/>	DWS	info	3col_fake	Error	test123	Lossless - pseudo-col...	Once	2023/10/11 17:35:33	Edit Delete More

- Click **Delete** in the **Operation** column of the target task. You can also select multiple tasks and click **Batch Delete** to delete them.

Figure 5-66 Deleting a watermark embedding task



Task	Source	Database	Source Table	Task Status	Watermark ID	Embedding Scheme	Schedule Info	Last Executed	Operation
<input type="checkbox"/>	DWS	info	3col_fake	Error	test123	Lossless - pseudo-col...	Once	2023/10/11 17:35:33	Edit Delete More

NOTE

The deletion cannot be undone.

5.3.2.2 Extracting Watermarks

Prerequisites

- DSC has been allowed to access cloud assets.
- Database assets have been added. For details, see [Database Assets](#).
- You have added MRS assets. For details, see [Adding MRS Assets](#).
- You have configured the GaussDB(DWS) and MRS_Hive permissions. For details, see [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.

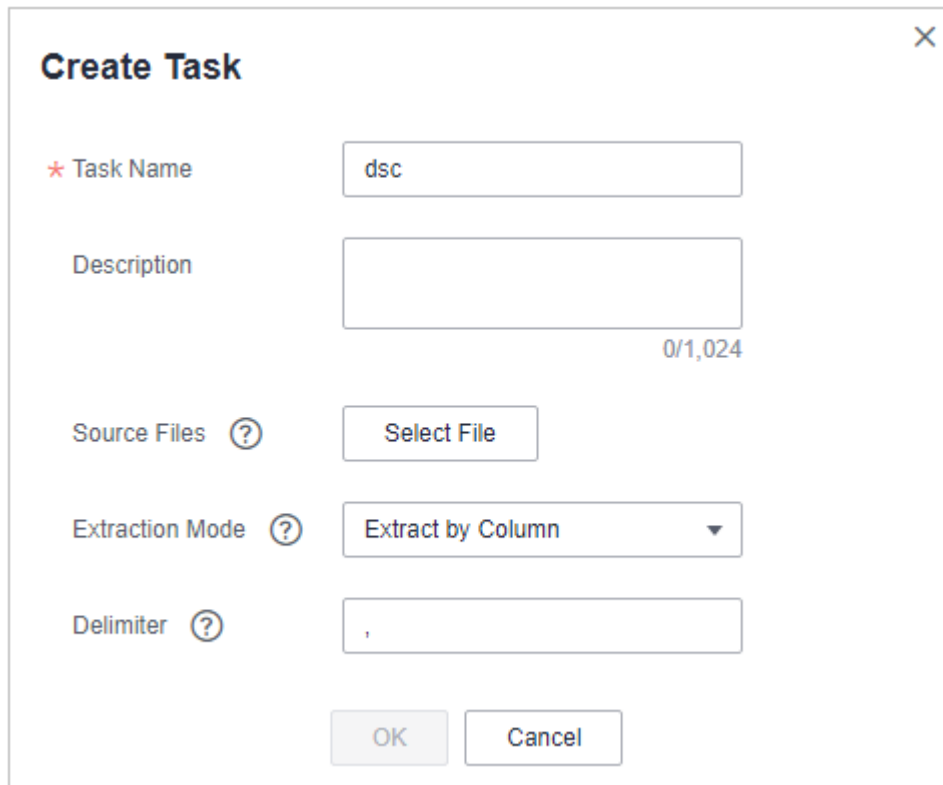
Step 3 In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Data privacy 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 5-14](#).

Figure 5-67 Creating an extraction task



Create Task ✕

* Task Name

Description
0/1,024

Source Files ?

Extraction Mode ? ▾

Delimiter ?

Table 5-14 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 pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Data privacy 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 pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Data privacy 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

5.3.3 Document Watermarking

5.3.3.1 Inserting Watermarks

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

The file format is PDF, PPT, Word, or Excel.


Constraints

If you injected an invisible watermark, extract the watermark from the target file using tools. For details, see [Extracting Watermarks](#).

Creating a Watermark Injection Task for Files in an OBS Bucket

Step 1 Log in to the management console.

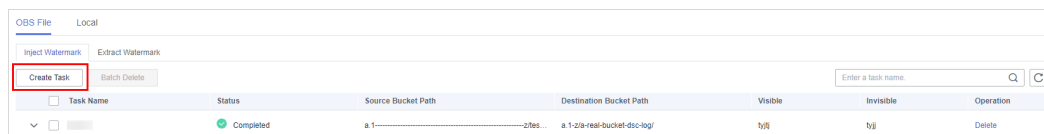
Step 2 Click  in the upper left corner and select a region or project.

Step 3 In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Data Privacy Protection > Document Watermarking**.

Step 5 Click **Create Task** in the upper left corner of the task list to create a task.

Figure 5-68 Creating a task



Step 6 Set the parameters shown in [Table 5-15](#).

Table 5-15 Task parameters

Parameter	Description	Example Value
Task Name	Enter the watermark ingestion task name.	Test_DSC
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: The watermark text is displayed in the file, as shown in Preview Visible Watermark in Figure 5-69. • 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. 	Visible watermark and invisible watermarks
Target Path	Click selecting a file path , and select the watermarked file.	-
Configure Visible Watermark	This parameter is mandatory when Watermark Type is set to Visible . Set Text , Font Size , Font Angle , and Transparency as required.	<ul style="list-style-type: none"> • Text: DSC • Font size: 60 • Font angle: 90 • Transparency: 100
Configure Invisible Watermark	This parameter is mandatory when Watermark Type is set to Invisible . Set Text as required.	Text: Test

Figure 5-69 Inserting Watermarks

* Task Name: Test

Select File: a-real-bucket/dsc_scan_template_classi...
a-real-bucket/dsc_scan_template_classi...
Add File
Only pdf, pptx, docx, and xlsx files are supported.

* Watermark Type: Visible Invisible ?

Target Path: a-real-bucket/a-real-bucket-dsc-log/
Selecting a file path

Configure Visible Watermark

* Text: DSC

Font Size: 1 to 60

Front Angle: 0 to 90

Transparency: 1 to 100

Configure Invisible Watermark

* Text: Test

OK Cancel

Preview Visible Watermark

DSC DSC DSC DSC DSC
DSC DSC DSC DSC DSC
DSC DSC DSC DSC DSC
DSC DSC DSC DSC DSC
DSC DSC DSC DSC DSC
DSC DSC DSC DSC DSC


Step 7 Click **OK**. A message is displayed in the upper right corner, indicating that the watermark injection task is created successfully.

----End

Creating a Local File Data Injection Task

Step 1 Log in to the management console.

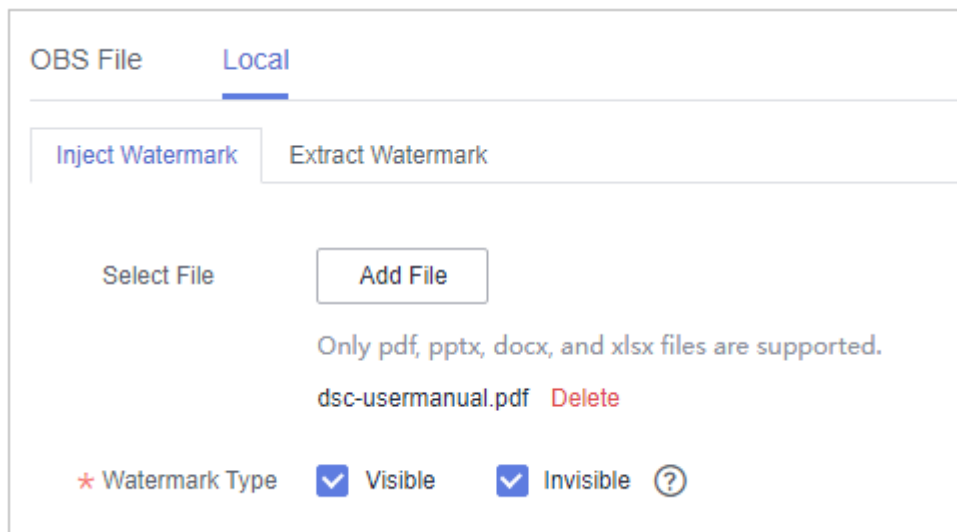
Step 2 Click  in the upper left corner and select a region or project.

Step 3 In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.

Step 4 In the navigation pane, choose **Data Privacy 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.

Figure 5-70 Adding a file

Step 7 After the file is uploaded, configure related parameters, as shown in [Figure 5-71](#). [Table 5-16](#) describes the related parameters.

Table 5-16 Watermarking parameters

Parameter	Description	Example Value
Watermark Type	Both visible and invisible watermarks are supported. You can select multiple values. <ul style="list-style-type: none"> Visible watermark: The watermark text is displayed in the file, as shown in Preview Visible Watermark in Figure 5-71. 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. 	Visible
Configure Visible Watermark	This parameter is mandatory when Watermark Type is set to Visible . Set Text , Font Size , Font Angle , and Transparency as required.	<ul style="list-style-type: none"> Text: DSC Font size: 60 Font angle: 90 Transparency: 100
Configure Invisible Watermark	This parameter is mandatory when Watermark Type is set to Invisible . Set Text as required.	Text: Test

Figure 5-71 Creating a local file data injection task

OBS File Local

Inject Watermark Extract Watermark

Select File

Only pdf, pptx, docx, and xlsx files are supported.
dsc-usermanual.pdf

* Watermark Type Visible Invisible

Configure Visible Watermark

* Text

Font Size

Front Angle

Transparency

Configure Invisible Watermark

* Text

Preview Visible Watermark


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](#).

----End

Related Operations

Click  next to the target watermark injection task name to view or download the status of the OBS file watermark injection task.

- **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.

5.3.3.2 Extracting Watermarks

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

The file format is PDF, PPT, Word, or Excel.

Constraints

The method described in this section applies only to extracting invisible watermarks of a single PDF, PPT, Word, or Excel file.

Creating an OBS Bucket File Watermark Extraction Task



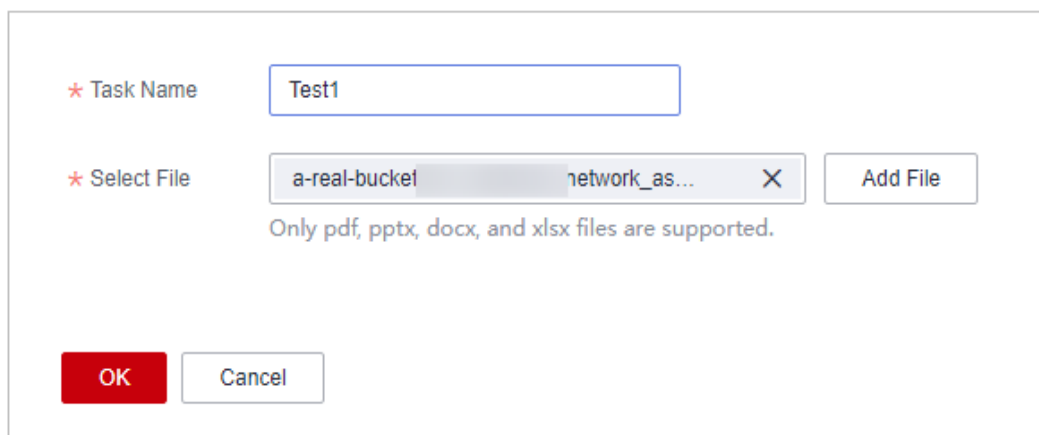
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation tree on the left, choose **Data Privacy 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.

Figure 5-72 Creating a watermark extraction task

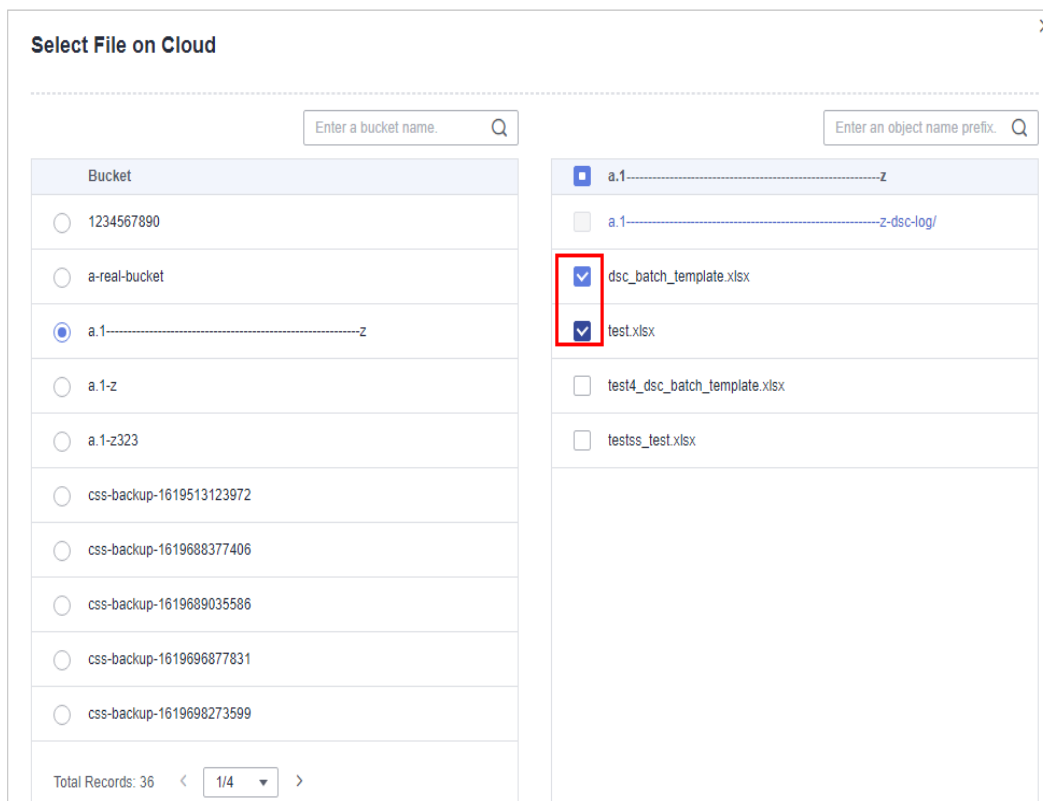


* Task Name


* Select File

Only pdf, pptx, docx, and xlsx files are supported.

- Step 7** Click **Add File** to select the file from which you want to extract watermarks. You can select multiple OBS bucket files.

Figure 5-73 Selecting a file

Step 8 Click **OK**. The watermark extraction task is created.


Step 9 Click  next to the target task name to view the extracted invisible watermark content.

----End

Extracting Watermarks from Local Files

Step 1 Log in to the management console.

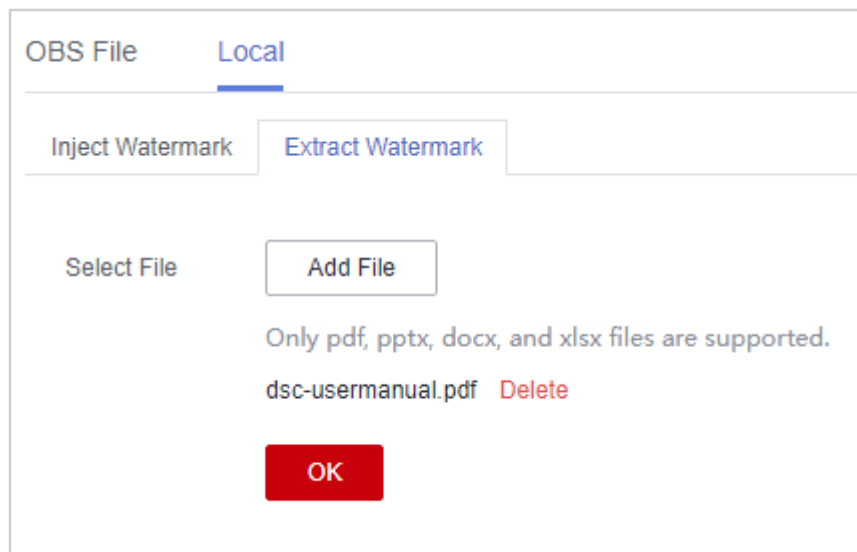
Step 2 Click  in the upper left corner and select a region or project.

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

Step 4 In the navigation tree on the left, choose **Data Privacy Protection** > **Document Watermarking**.

Step 5 On the displayed page, choose **Local** > **Extract Watermark**. The **Extract Watermark** page is displayed.

Figure 5-74 Extracting watermarks



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

Related Operations

Click  next to the target watermark injection task name to view the status of the watermark extraction task.

- **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.

6 Data Risk Detection

6.1 Viewing Abnormal Behaviors Through Data Usage Audit

Report and audit real-time alarms of abnormal data usage in the cloud. You can view abnormal behavior data of last 30 minutes, 3 hours, 24 hours, 7 days, or 30 days. DSC stores abnormal event data for 180 days.

DSC can detect abnormal events related to the access, operation, and management of sensitive data and provide alarm notifications for you to confirm and handle these abnormal events.

The following behaviors are regarded as abnormal events:


- Unauthorized users access and download sensitive data.
- Authorized users access, download, and modify sensitive data, as well as change and delete permissions.
- Authorized users change or delete permissions granted for buckets that contain sensitive data.
- Users who accessed sensitive files fail to log in to the device.


Prerequisites

An abnormal event has been detected and displayed on the page.

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**.

Step 4 In the left navigation pane, choose **Data Risk Detection > Data Usage Audit**, and the **Risky Behavior Detection** tab page is displayed by default. For parameter details, see [Table 6-1](#).

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.

Figure 6-1 Data usage audit list

Table 6-1 Parameters of detected risky behaviors

Parameter	Description
User ID	ID of a resource owner
Event Type	<p>DSC classifies abnormal events into the following three types:</p> <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

Parameter	Description
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.

You can determine whether an abnormal event is a violation according to the event details, and then determine how to handle the event. For details, see [Handling Abnormal Behaviors Found in Data Usage Audit](#).

Figure 6-2 Abnormal event details

Abnormal Event Details	
Asset Owner	ce28abd4fdd44e09a34c78709b413 689
Time	Nov 04, 2020 09:17:55 GMT+08:00
Event Type	Management Exceptions
Event Name	UPDATE.BUCKET.POLICY
Asset Type	OBS
Bucket Name	[REDACTED]n-east-3
Error Code	--
Region	CN East-[REDACTED]
IP Address	[REDACTED]
Log	ce28abd4fdd44e09a34c78709b413 689 [REDACTED]ast-3 [04/Nov/2020:01:17:55 +0000] 121.37.50.1 ce28abd4fdd44e09a34c78709b413 [REDACTED] 8041674e9a8e0ef738afb4ee61 REST.PUT.POLICY - "PUT [REDACTED]ast-3/?policy HTTP/1.1" 204 - - 7 7 "-" "HttpClie

----End

6.2 Handling Abnormal Behaviors Found in Data 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.

Procedure



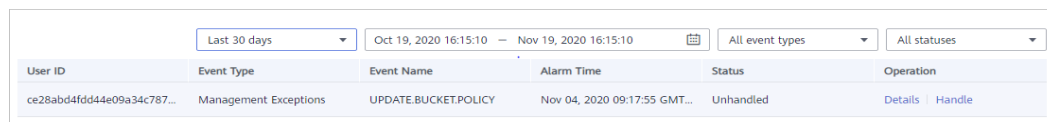
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Data Security Center**.
- Step 4** In the navigation tree on the left, choose **Data Risk Detection > Data Usage Audit**.

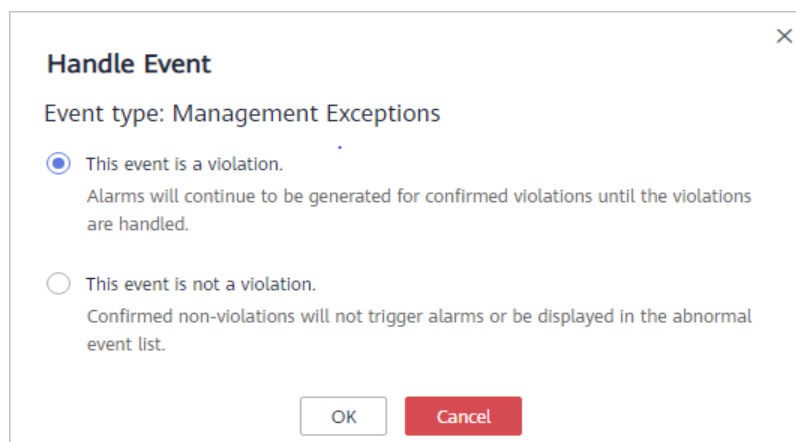
Figure 6-3 Data usage audit list



User ID	Event Type	Event Name	Alarm Time	Status	Operation
ce28abd4fdd44e09a34c787...	Management Exceptions	UPDATE.BUCKET.POLICY	Nov 04, 2020 09:17:55 GMT...	Unhandled	Details Handle

- Step 5** In the abnormal event list, locate the row that contains the abnormal event to be handled, and click **Handle** in the **Operation** column.
- Step 6** In the displayed dialog box, select a handling method, and click **OK**.

Figure 6-4 Handling an abnormal event



Handle Event

Event type: Management Exceptions

This event is a violation.
Alarms will continue to be generated for confirmed violations until the violations are handled.

This event is not a violation.
Confirmed non-violations will not trigger alarms or be displayed in the abnormal event list.

The handling methods are as follows:

- **This event is a violation:** If the identified event is an abnormal event, select this option.
Alarms will continue to be generated for confirmed violations until the violations are handled.
- **This event is not a violation:** If the the identified event is normal and does not need to be handled, select this option.
Confirmed non-violations will not trigger alarms or not be displayed in the abnormal event list.

----End

6.3 Viewing and Handling Access Key Leaks

DSC detects leaks of access keys in the Git code that contain Huawei Cloud AKs and SKs, and displays the detection results in a list. You can handle leak events as required.

Prerequisites

You have obtained credentials for logging in to the management console.

Procedures



- 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**.
- Step 4** In the navigation pane, choose **Risk Detection**. On the displayed page, click the **Access Key Leak Detection** tab.

Table 6-2 Parameters of a detected access key leak event

Parameter	Description
Access Key ID	Access key ID (AK). You can click Go to Access Keys to switch to the access key management page where you can create, modify, enable or disable, or delete an access key.
Intelligence Source	Source of the access key leak event detected, for example, GitHub.
Account Affected	Account affected by the access key leak
Leak Type	Type of the access key leakage event

Parameter	Description
First Detection Time	Time when the leak event is detected for the first time
Status	An access key leak event has the following statuses: <ul style="list-style-type: none">● To be handled indicates the access key leak event has not been handled.● Manually deleted indicates that the leaked access key and the related information have been manually deleted or hidden on GitHub.● Manually disabled indicates that the leaked access key has been disabled and reset (or directly deleted) on the access key management console.● Whitelisted indicates that the leaked access key has been added to the whitelist. An alarm will not be generated for the leak of the access key that has been added to the whitelist.

Step 5 Click **View** in the **Operation** column to view the details about a detected access key lead event, including the details, code snippet, and tips.

Step 6 Handle the event according to the tips. Click **Handle** in the **Operation** column.

Step 7 In the displayed dialog box, select a handling method, and click **OK**.

The handling methods are as follows:

- **Manually Delete Access Key:** Log in to GitHub and manually delete or hide the leaked access key and its related information.
- **Manually Disable Access Key:** Log in to the Access Key management console and disable and reset the access key (or delete it).
- **Add Access Key to Whitelist:** There is no need to handle the event because this event has no security risks. An alarm will not be generated for the leak of the access key that has been added to the whitelist.

----End

7 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 notification, you are advised to create a message topic in the SMN service as an administrator. For details, see [Before You Publish a Message](#).

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**.

Step 4 In the navigation pane, choose **Alarm Notifications**.

Step 5 Configure alarm notifications. [Table 7-1](#) 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 7-1 Configuring alarm notifications

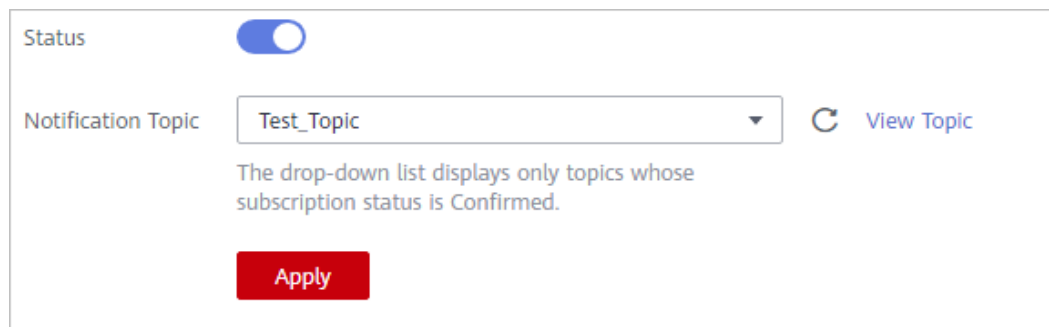





Table 7-1 Alarm notification parameters

Parameter	Description	Example Value
Status	Whether notification is enabled. <ul style="list-style-type: none"> : enabled. : disabled. 	
Notification Topic	Select an existing topic from the drop-down list or click View Topic to create a topic for receiving alarm notifications. Click View Topic and perform the following steps to create a topic: <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. For details about topics and subscriptions, see <i>Simple Message Notification User Guide</i> .	N/A

Step 6 Click **Apply**.

----End

8 Permissions Management

8.1 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 8-1](#)).

Prerequisites

Learn about the permissions supported by DSC in [Table 8-1](#) and choose policies or roles based on your requirements.

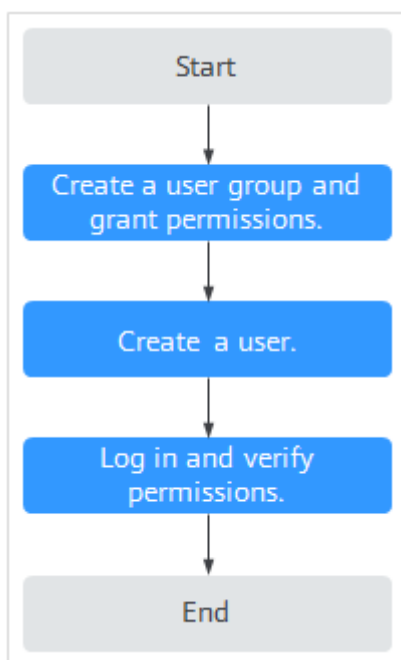
Table 8-1 DSC system permissions

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 8-1 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.

8.2 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"
      ]
    }
  ]
}
```

8.3 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

9 Key DSC Operations

9.1 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 9-1 lists DSC operations recorded by CTS.

Table 9-1 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

9.2 Viewing Audit Logs

After you enable CTS, the system starts recording operations on DSC. Operation records generated during the last seven days can be viewed on the CTS console.

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** Click  in the upper left corner of the page. In the dialog box displayed on the right, choose **Management & Deployment > Cloud Trace Service**.
- Step 4** In the navigation pane, choose **Trace List**.
- Step 5** On the displayed page, you can query traces by setting the filtering criteria. You can select one or more of the following filters to query your traces:
 - **Trace Type, Trace Source, Resource Type, and Search By**
 - Select **Management** for **Trace Type**.
 - Select **DSC** for **Trace Source**.
 - When you select **Resource ID** for **Search By**, enter a resource ID.
 - **Operator**: Select a specific operator (a user rather than tenant).
 - **Trace Status**: Available options include **All trace statuses**, **normal**, **warning**, and **incident**. You can only select one of them.
 - **Time Range**: In the upper right corner of the page, you can query traces in the last one hour, last one day, last one week, or within a customized period.
- Step 6** Click **Query**.
- Step 7** Click  on the left of a trace to expand its details.

Figure 9-1 Trace details



```
View Trace
{
  "request": "/v1/05e3df04478025dc2f79c0005f4271dc/sdg/asset/authorization",
  "code": "200",
  "source_ip": "192.168.1.99",
  "event_type": "system",
  "project_id": "09e3df04478025dc2f79c0005f4271dc",
  "trace_name": "grantOrRevokeToDsc",
  "resource_type": "dscGrant",
  "trace_rating": "normal",
  "api_version": "1.0",
  "service_type": "DSC",
  "tracker_name": "system",
  "time": "Nov 19, 2020 17:32:05 GMT+08:00",
  "record_time": "Nov 19, 2020 17:32:05 GMT+08:00",
  "user": {
    "name": "admin",
    "id": "3496c6e1-3eb817ced344b88b3b",
    "domain": {
      "name": "huawei.com",
      "id": "ce85e11f-f5f55555-78709b413689"
    }
  }
}
```

- Step 8** Click **View Trace** in the **Operation** column. On the displayed dialog box, the trace structure details are displayed.

Figure 9-2 Viewing trace details

```
{
  "request": "/v1/05e3df04478025dc2f79c0005f4271dc/sdg/server/mask/dbs/templates/search",
  "code": "200",
  "source_ip": "192.168.1.2.99",
  "event_type": "system",
  "project_id": "05e3df04478025dc2f79c0005f4271dc",
  "trace_name": "showDBTemplates",
  "resource_type": "dscDBMaskTemplate",
  "trace_rating": "normal",
  "api_version": "1.0",
  "service_type": "DSC",
  "tracker_name": "system",
  "time": "2020/11/19 17:28:25 GMT+08:00",
  "record_time": "2020/11/19 17:28:25 GMT+08:00",
  "user": {
    "name": "admin",
    "id": "8eb817c0d344b88b3b",
    "domain": {
      "name": "admin",
      "id": "09b413689"
    }
  }
}
```

----End

A Change History

Released On	Description
2023-11-30	This issue is the first official release.