Data Security Center

User Guide

Issue	01
Date	2022-12-20

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.

Contents

1 Service Overview

1.1 What Is DSC?

Data Security Center (DSC) is a latest-generation cloud data security management platform that protects your data assets by leveraging its data protection capabilities such as data classification, risk identification, data masking, and watermark-based source tracking. DSC gives you an insight into the security status of each stage in data security lifecycle and provides constant visibility of the security status of your data assets.

NOTICE

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

1.2 Specifications of Different DSC Editions

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

Table 1-1 Specifications of different DSC editions

Edition	Database Quantity	OBS Storage (GB)	API Calling Quota	Function
Standard	2	100	Not supported	• Data security overview • Sensitive data identification

Edition	Database Quantity	OBS Storage (GB)	API Calling Quota	Function
Professional	2	100	1,000,000 times	• Data security overview • Sensitive data identification • Data masking • Data watermark injection/extraction • API calling

1.3 Functions

Table 1-2 describes the functions provided by DSC.

Table 1-2 DSC functions

Function	Description	Reference Document
Data Security Overview	DSC provides constant visibility of the security status of your data and displays the security status in data collection, transmission, storage, usage, exchange, and deletion.	OverviewData Security Overview
Asset List	DSC manages the data assets added in DSC, including OBS, databases, MRS, and big data. For details about the restrictions on adding assets, see Constraints.	Adding Assets in Batches

Function	Description	Reference Document
Sensitive Data Identification	• **Automatic data classification**: DSC precisely and efficiently identifies sensitive data from structured data stored in Relational Database Service (RDS) and unstructured data stored in Object Storage Service (OBS), covering all data on the cloud. – File types: DSC can identify sensitive data from over 200 types of unstructured files. – Data types: DSC is able to identify dozens of personal privacy data types (Chinese or English). – Image types: DSC is able to identify sensitive words (Chinese and English) in eight types of images such as PNG, JPEG, x-portable-pixmap, TIFF, BMP, GIF, JPX, and JP2. – Compliance templates: Various	**Creating a Sensitive Data Identification Task**

Function	Description	Reference Document
	templates built in DSC are used to check whether data is compliant with regulations and standards such as General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), and Health Insurance Portability and Accountability Act (HIPAA). ● **Automatic identification of sensitive data** – Automatic identification of sensitive data and personal privacy data – Customized identification rules to meet various requirements of different industries – File framework sort-out to precisely identify sensitive data. – Clear and intuitive compliance reports that can be downloaded	

Function	Description	Reference Document
Data Masking	Supports static data masking and dynamic data masking. Data masking has the following features: • **Zero impact**: DSC reads data from original databases, statically masks sensitive data using precise masking engines, and saves the masked data separately without affecting your data assets. • **Various data sources**: Data of various sources on the cloud, such as RDS, self-built databases on ECSs, or big data, can be masked to meet security requirements. • **Custom data masking policies**: DSC provides you with over 20 preset data masking rules. You can use the default masking rules or customize the masking rules to mask sensitive data in the specified database table. For details about the data masking algorithms	**Configuring a Data Masking Rule**

Function	Description	Reference Document
	supported by DSC, see . • **Easy and quick masking rule configuration for security compliance**: Easy and quick data masking rule configuration can be achieved based on data scanning results. DSC uses built-in and customized masking algorithms to mask RDS and Elasticsearch data.	
Data Watermarking	Adds watermarks to or extracts watermarks from PDF, PPT, Word, and Excel files. • **Copyright proof**: The owner information is added to the assets to specify the ownership, achieving copyright protection. • **Automated monitoring**: The user information is added to the assets for tracing data leak.	**Watermark Injection**
Alarm Notifications	Sends notifications through the notification method configured by users when sensitive data identification is completed or abnormal events are detected.	**Alarm Notifications**

1.4 Advantages

Actionable Insights into Data Security

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

Extensive Range of Data Sources

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

Precise Identification of Sensitive Data

DSC precisely and efficiently identifies sensitive data sources based on the expert expertise and Natural Language Processing (NLP).

Flexible Data Masking

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

1.5 Billing

WAF instances are billed on a pay-per-use basis, which is postpaid.

Billing Item

Table 1-3 Billing items

Billing Mode	Billing Item	Billing
Pay-Per-Use	(Mandatory) Edition specifications	Billed based on the specifications of purchased DSC edition (standard or professional). For details about specifications and functions of each edition, see **Specifications of Different DSC Editions**.
	(Optional) Database expansion package	Billed based on the number of purchased packages.
	(Optional) OBS expansion package	Billed based on the number of purchased packages.

Billing Mode	Billing Item	Billing
	APIs (data masking and watermarking)	This feature is supported only by the professional edition and is charged based on the number of API calls.

Billing Mode

Pay-per-use billing: you can enable or disable a WAF instance anytime you want.

The billing starts when you enable DSC and ends when you disable it. You are charged based on the service edition, number of database and OBS expansion packages, and number of API requests.

1.6 Applicable Scenarios

Automatic Identification and Classification of Sensitive Data

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

Abnormal Behavior Analysis

DSC establishes a user behavior library through deep learning of user behaviors. Any behavior uncovered in the library is deemed abnormal and an alarm will be reported on a real-time basis. You can then trace user behaviors and correlate the events with the users to identify who performed the risky operations. It also detects data security breaches and generates alarms so that you can take immediate protective actions.

Data Masking

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

Data Compliance

DSC provides dozens of templates that can be used to check for compliance with regulations and standards such as GDPR, PCI DSS, and HIPAA. DSC checks your data protection measures against multiple rules in the templates and generates reports to propose corrective measures

1.7 DSC and Related Services

OBS

Object Storage Service (OBS) is a stable, secure, efficient, and easy-to-use cloud storage service that can store any amount and form of unstructured data. After

OBS access permissions are granted, DSC is allowed to automatically identify and classify sensitive data, analyze abnormal user behaviors, and protect data stored in OBS.

RDS

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

DWS

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

DDS

Document Database Service (DDS) is a database service compatible with the MongoDB protocol and is secure, highly available, reliable, scalable, and easy to use. It provides DB instance creation, scaling, redundancy, backup, restoration, monitoring, and alarm reporting functions with just a few clicks on the DDS console. After DDS access permissions are granted, DSC is allowed to automatically identify and classify sensitive data and protect data stored in DDS.

ECS

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

Bare Metal Server (BMS)

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

CSS

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

DLI

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

MRS

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

ELB

DSC is bound to Elastic Load Balance (ELB) to query the encryption communications status.

SMN

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

CTS

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

Table 1-4 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

Operation	Resource Type	Trace Name
Add a big data source	dscBigdataAsset	addBigdata
Modify a big data source	dscBigdataAsset	updateBigdata
Delete a big data source	dscBigdataAsset	deleteBigdata
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

Operation	Resource Type	Trace Name
Add a scan task	dscScanTask	addScanJob
Modify a scan task	dscScanTask	updateScanJob
Delete a scan subtask	dscScanTask	deleteScanTask
Delete a scan task	dscScanTask	deleteScanJob
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	dscBigDataMaskTem-plate	addBigDataTemplate
Modify an Elasticsearch data masking template	dscBigDataMaskTem-plate	editBigDataTemplate
Delete an Elasticsearch data masking template	dscBigDataMaskTem-plate	deleteBigDataTemplate
Query the Elasticsearch data masking template list	dscBigDataMaskTem-plate	showBigDataTemplates
Enable or disable an Elasticsearch data masking template	dscBigDataMaskTem-plate	operateBigDataTemplate
Switch the status of an Elasticsearch data masking template	dscBigDataMaskTem-plate	switchBigDataTemplate

Operation	Resource Type	Trace Name
Enable or disable data masking for databases	dscDBMaskSwitch	switchDBMaskStatus
Obtain the database fields	dscDBMetaData	getColumn
Add a database masking template	dscDBMaskTemplate	addDBTemplate
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

Operation	Resource Type	Trace Name
Delete encryption algorithm configurations	dscEncryptMaskConfig	deleteEncryptConfig

VPC

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

IAM

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

1.8 Constraints

Supported Data Sources

- Relational Database Service (RDS)
- Object Storage Service (OBS)
- Data Warehouse Service (DWS)
- Document Database Service (DDS)
- MapReduce Service (MRS)
- Cloud Search Service (CSS)
- Data Lake Insight (DLI)
- Databases on Elastic Cloud Servers (ECSs)
- Databases on Bare Metal Servers (BMSs)

Supported Database Versions

Table 1-5 lists the database types and versions supported by DSC.

Table 1-5 Supported database types and versions

Database Type	Version
MySQL	5.6, 5.7, 5.8, and 8.0

Database Type	Version
SQL Server	• 2017_SE, 2017_EE, and 2017_WEB • 2016_SE, 2016_EE, and 2016_WEB • 2014_SE and 2014_EE • 2012_SE, 2012_EE, and 2012_WEB • 2008_R2_EE and 2008_R2_WEB
PostgreSQL	11, 10, 9.6, 9.5, 9.4, and 9.1
Oracle	10 and 12

1.9 Permissions Management

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

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

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

DSC Permissions

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

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

You can grant users permissions by using roles and policies.

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

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

Table 1-6 describes the system-defined policies of DSC.

Table 1-6 DSC system-defined policies

Policy	Description	Type	Dependency
DSC DashboardReadOnlyAccess	Read-only permissions for the overview page of DSC	System-defined policy	None
DSC FullAccess	All permissions for DSC	System-defined policy	None
DSC ReadOnlyAccess	Read-only permissions for Data Security Center	System-defined policy	None

2 Service Provisioning

2.1 Buying DSC

DSC can be billed on a pay-per-use basis. DSC provides the database and OBS expansion packages. Apply for a 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.

Specification Limitations

- One expansion package offers one database instance. RDS and DWS databases, self-built databases on ECSs, 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.

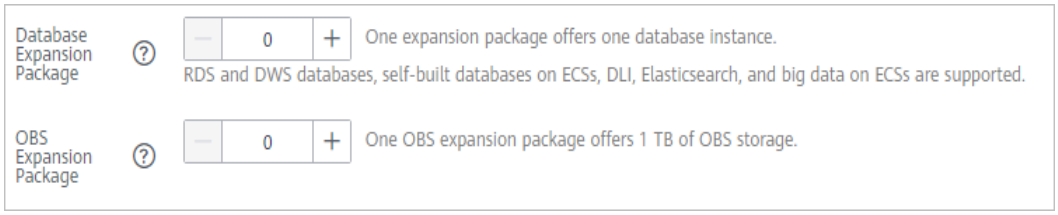
Step 3 In the navigation pane on the left, click and choose **Security** > **Data Security Center**.

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

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

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

Figure 2-1 Selecting expansion packages



- One expansion package offers one database instance. RDS and DWS databases, self-built databases on ECSs, Elasticsearch, and big data on ECSs are supported.
- One OBS expansion package offers 1 TB (1024 GB) of OBS storage.

Step 7 Click **Apply for DSC**.

----End

2.2 Upgrading Specifications

After applying for 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.

Specification Limitations

- One expansion package offers one database instance. RDS and DWS databases, self-built databases on ECSs, 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.

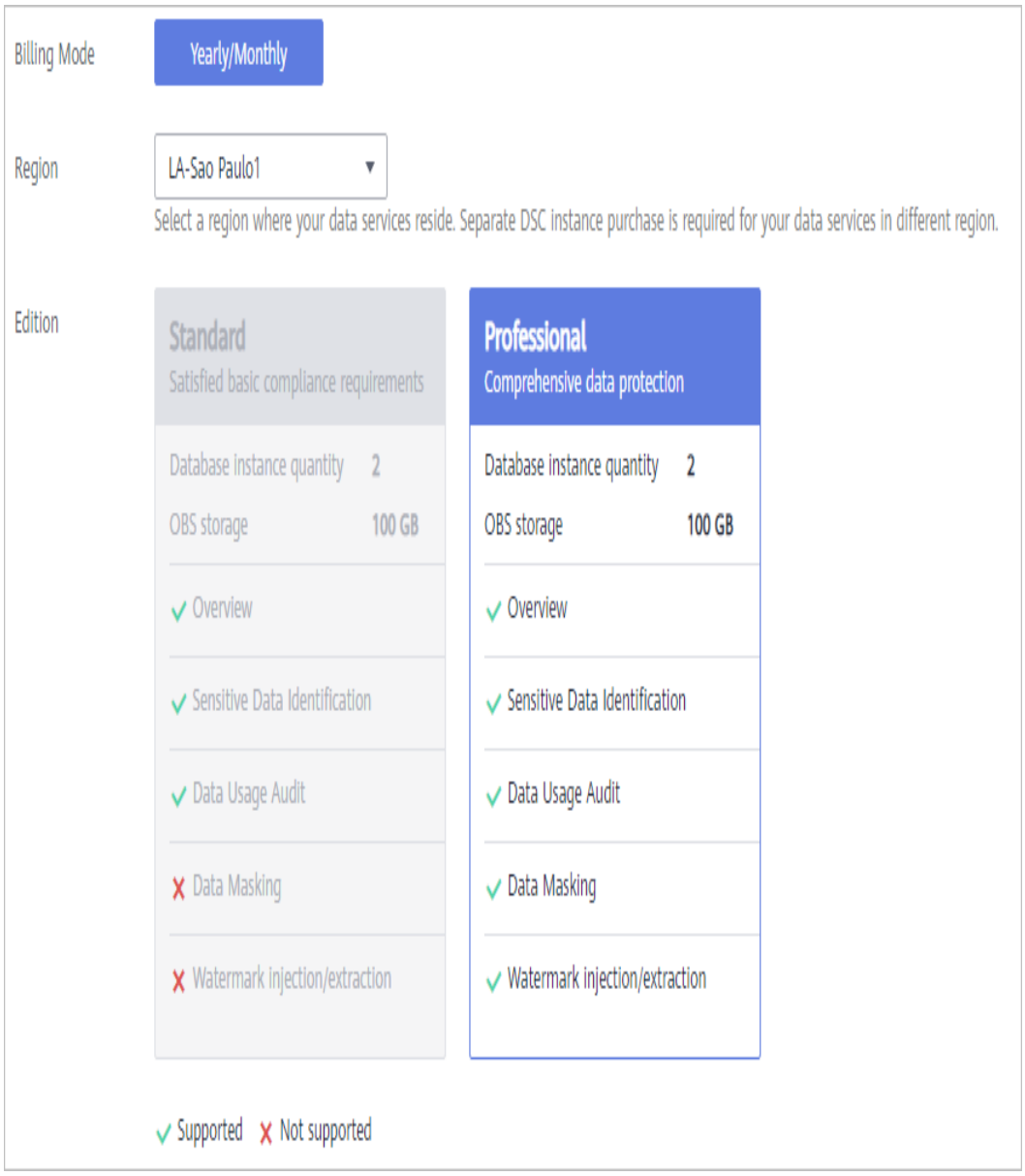
Step 3 In the navigation pane on the left, click and choose **Security** > **Data Security Center**.

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.

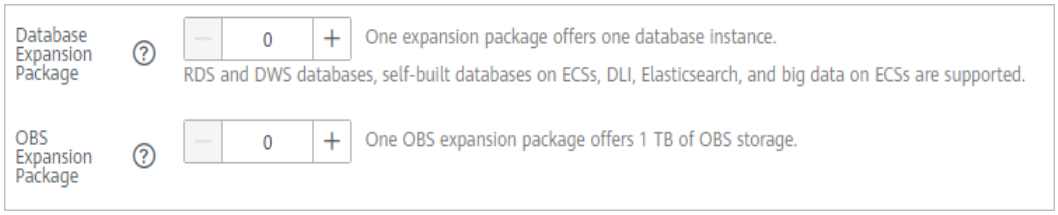
The edition listed on the right side of the current one is a more feature-rich edition.

Figure 2-2 Upgrading edition specifications



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

Figure 2-3 Selecting expansion packages



- One expansion package offers one database instance. RDS and DWS databases, self-built databases on ECSs, Elasticsearch, and big data on ECSs are supported.

- One OBS expansion package offers 1 TB (1024 GB) of OBS storage.

Step 7 Click **Apply for DSC**.

----End

2.3 Unsubscribing from DSC

This section describes how to unsubscribe from DSC.

Prerequisites

You have applied for DSC.

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 and choose **Security** > **Data Security Center**.

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

Step 5 Click **OK**.

----End

3 Assets

3.1 Allowing or Disallowing Access to Cloud Assets

This section describes how to grant or revoke permissions for accessing OBS bucket, database, big data, MRS, and data security overview. 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.
- 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.

Procedure

Step 1 Log in to the management console.

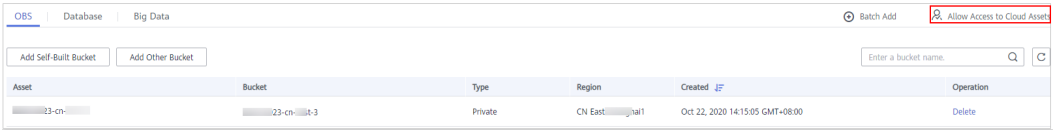
Step 2 Click in the upper left corner of the management console and select a region or project.

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

Step 4 In the navigation pane, choose **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 3-1**.

Figure 3-2 Allowing access to cloud assets

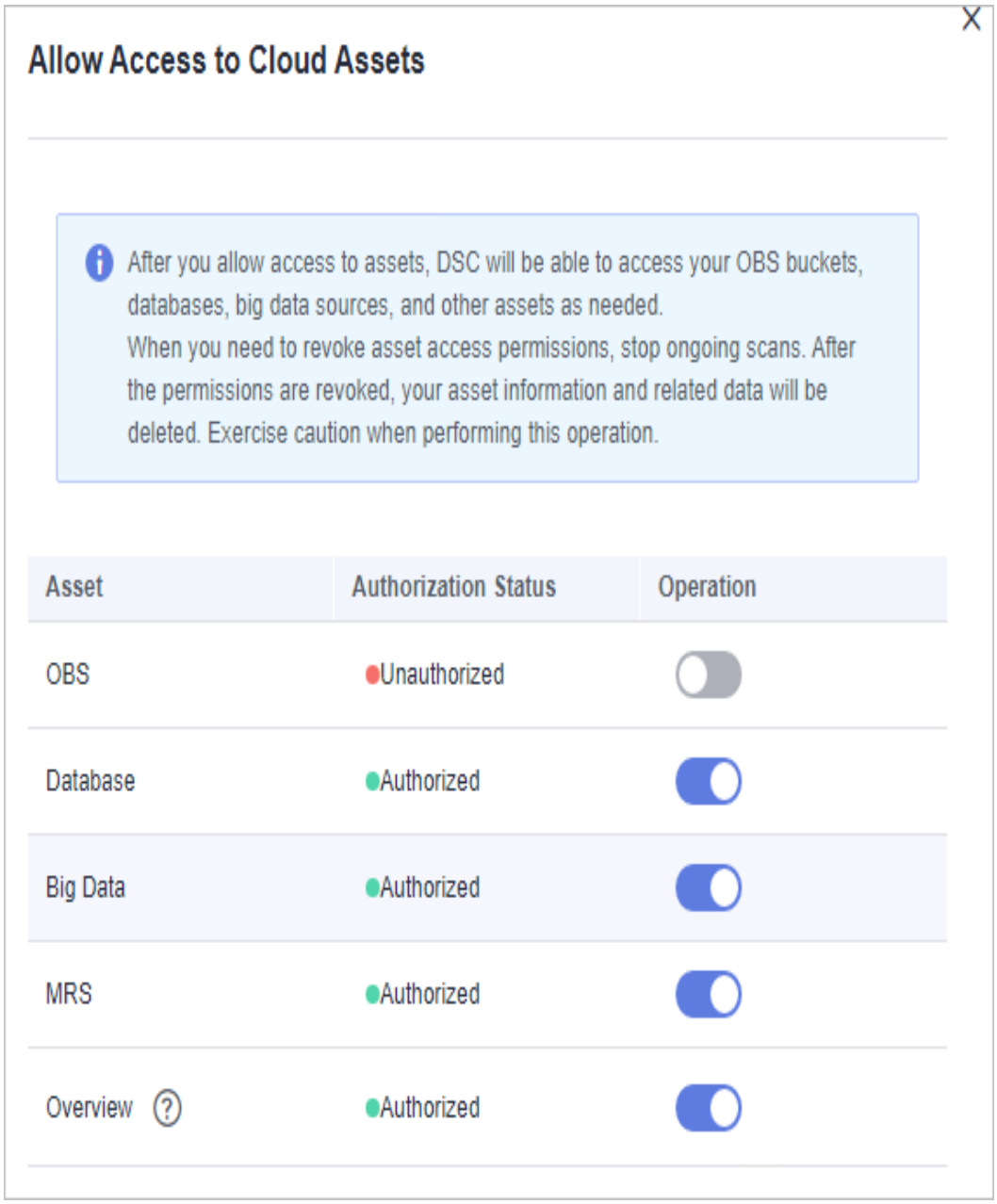


Table 3-1 Parameter description

Parameter	Description
Assets	DSC provides four types of assets: • OBS • Database: For details about the database types and versions supported by DSC, see **Constraints**. • Big Data: assets in Cloud Search Service (CSS) and Data Lake Insight (DLI) • MapReduce Service (MRS) • Overview: Allow DSC to access and collect stored, transferred, used, exchanged, and deleted data of cloud services.
Authorization Status	The options are as follows: • Authorized • Unauthorized
Operation	Click the following toggle buttons to allow or disallow access to your assets: •  : Unauthorized •  : Authorized

----End

3.2 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

Database types and versions supported by DSC can be added. For details, see **Table 3-2**.

Table 3-2 Supported database types and versions

Database Type	Version
MySQL	5.6, 5.7, 5.8, and 8.0

Database Type	Version
SQL Server	• 2017_SE, 2017_EE, and 2017_WEB • 2016_SE, 2016_EE, and 2016_WEB • 2014_SE and 2014_EE • 2012_SE, 2012_EE, and 2012_WEB • 2008_R2_EE and 2008_R2_WEB
PostGreSQL	11, 10, 9.6, 9.5, 9.4, and 9.1
Oracle	10 and 12

Procedure

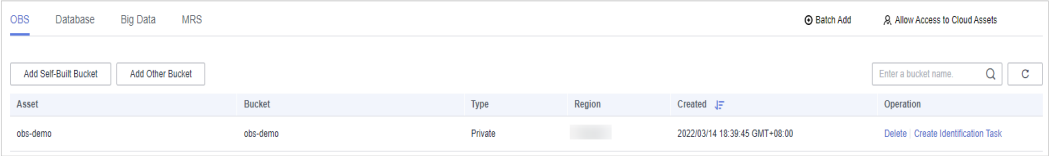
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Assets**.

Figure 3-3 OBS assets

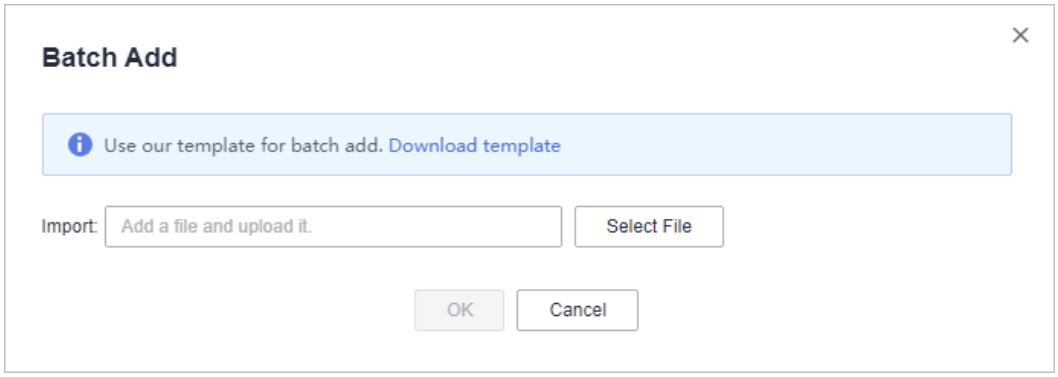


Step 5 In the upper right corner of the **OBS** tab page, click **Batch Add**.

Step 6 In the displayed dialog box, click **Select File** and import the sorted assets.

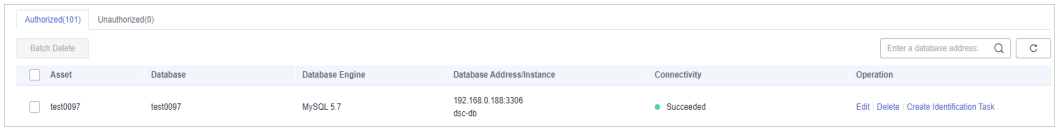
You can click **Download template** to classify assets.

Figure 3-4 Adding assets in batches



Step 7 Click **OK**.

Figure 3-5 Connectivity test



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**. Click **Cause** to view the failure cause.

----End

3.3 OBS Assets

3.3.1 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.
- The OBS buckets to be added are public.

Procedure

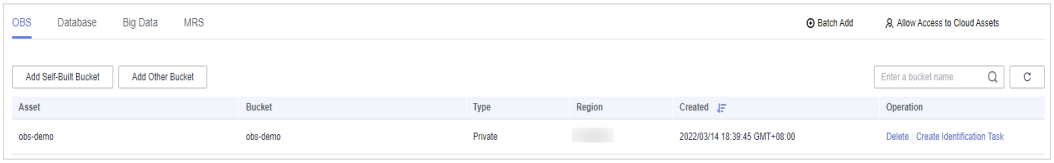
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Assets**.

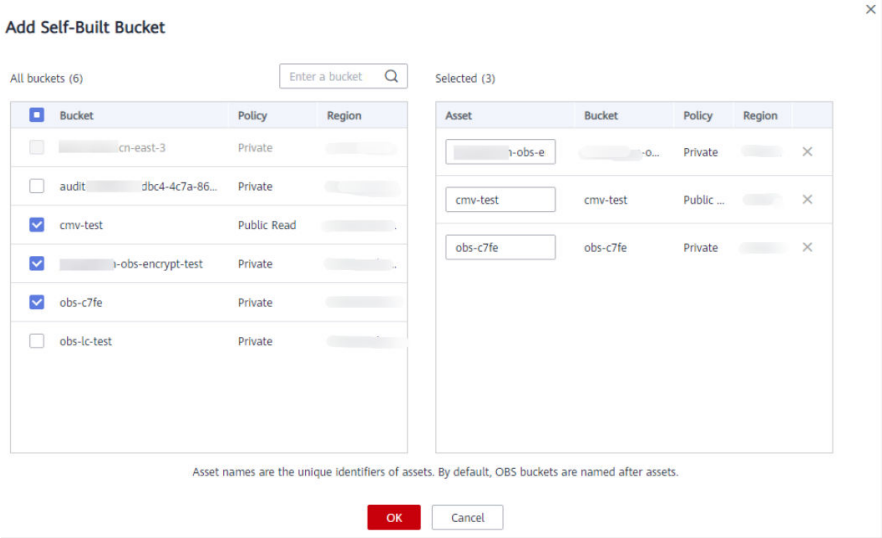
Figure 3-6 OBS assets



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



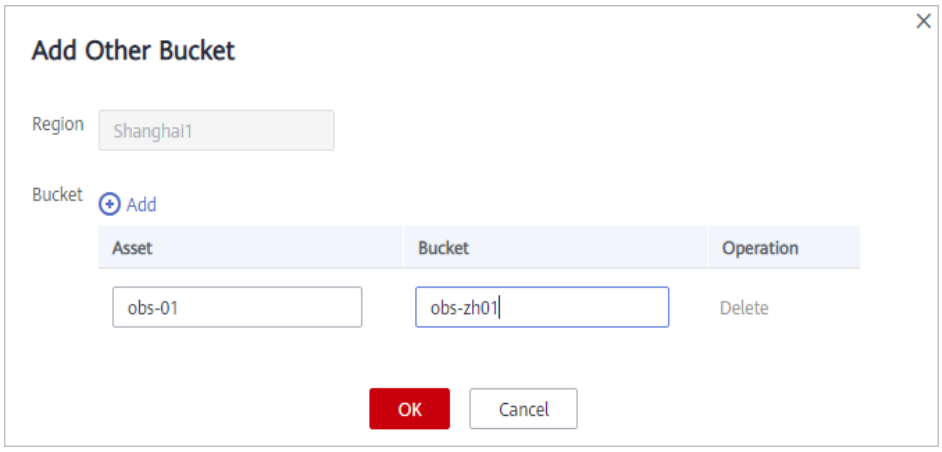
  c. Click **OK**.

- 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 

.

  Figure 3-8 Adding other OBS buckets



  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**.

3.3.2 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.
- Deleted assets including related templates, task results, and reports cannot be recovered. Exercise caution when performing this operation.

Procedure

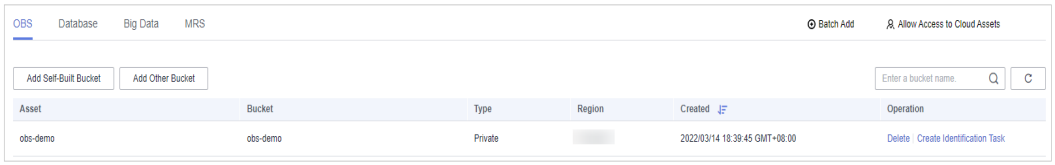
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Assets**.

Figure 3-9 OBS assets



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

3.4 Database Assets

3.4.1 Adding an RDS Database

If you have granted permissions for accessing your database assets to DSC, purchased 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 RDS DB instance is in the **Normal** state.

Procedure

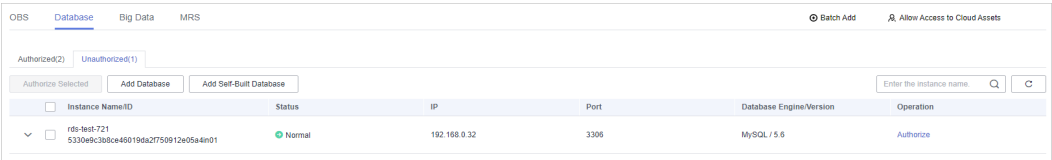
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Assets** and select the **Database** tab and then the **Unauthorized** tab.

Figure 3-10 Unauthorized database assets



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 3-3**.

Figure 3-11 Batch permission authorization for databases

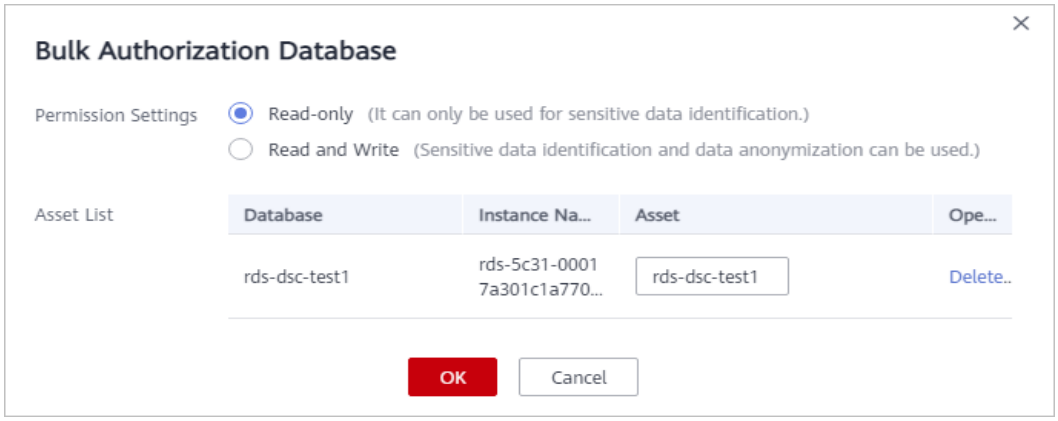
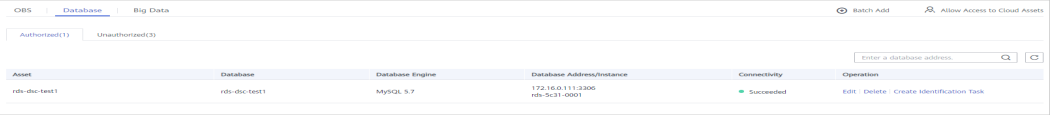


Table 3-3 Parameter description

Parameter	Description
Permission Settings	• **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. – 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	• 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**. Click **Cause** to view the failure cause.

----End

3.4.2 Adding a Database

If you have subscribed to GaussDB(DWS) or Document Database Service (DDS), and created databases in it, you can follow the instructions described in this section to add the created databases to 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 DDS or GaussDB(DWS) and added assets to it. There are available IP addresses in the corresponding subnet.

Procedure

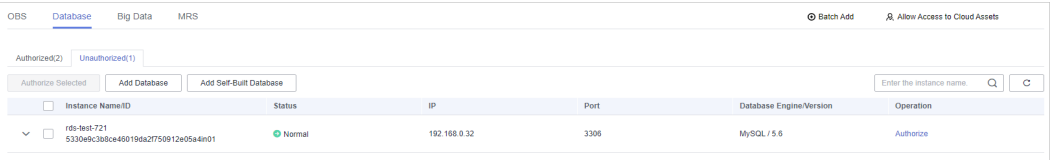
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Assets** and select the **Database** tab and then the **Unauthorized** tab.

Figure 3-13 Unauthorized database assets



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 3-4**.

Figure 3-14 Adding a DWS database

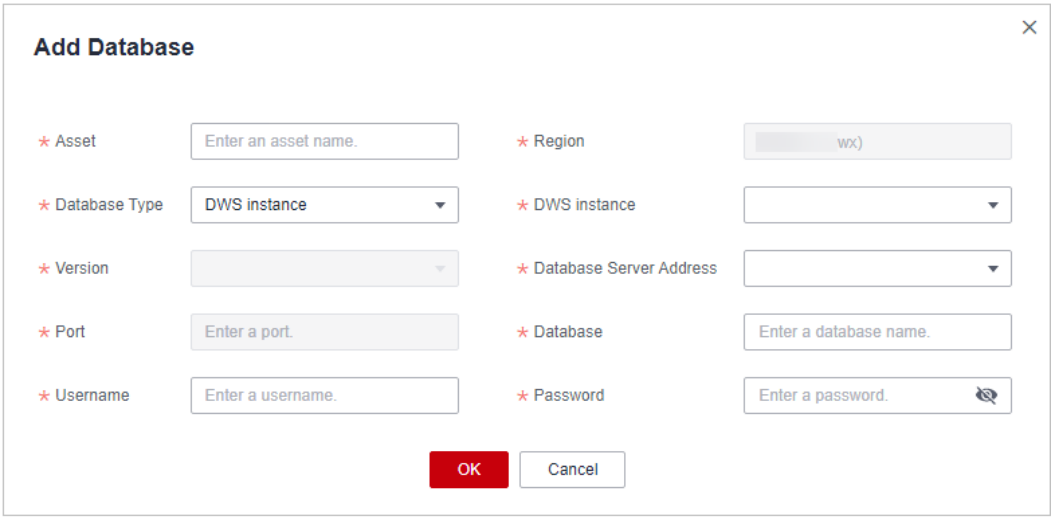


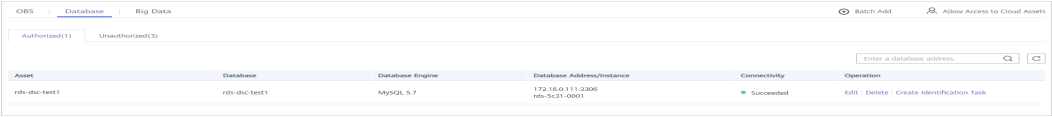
Table 3-4 Parameter description

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** or **DDS 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 instances	An option of **Database Type**. Select a database instance that has been created in DDS 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
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

Parameter	Description	Example Value
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**. Click **Cause** to view the failure cause.

----End

3.4.3 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

Database types and versions supported by DSC can be added. For details, see **Table 3-5**.

Table 3-5 Supported database types and versions

Database Type	Version
MySQL	5.6, 5.7, 5.8, and 8.0

Database Type	Version
SQL Server	• 2017_SE, 2017_EE, and 2017_WEB • 2016_SE, 2016_EE, and 2016_WEB • 2014_SE and 2014_EE • 2012_SE, 2012_EE, and 2012_WEB • 2008_R2_EE and 2008_R2_WEB
PostGreSQL	11, 10, 9.6, 9.5, 9.4, and 9.1
Oracle	10 and 12

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Assets** and select the **Database** tab and then the **Unauthorized** tab.

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 3-6**.

Figure 3-17 Adding a self-built database

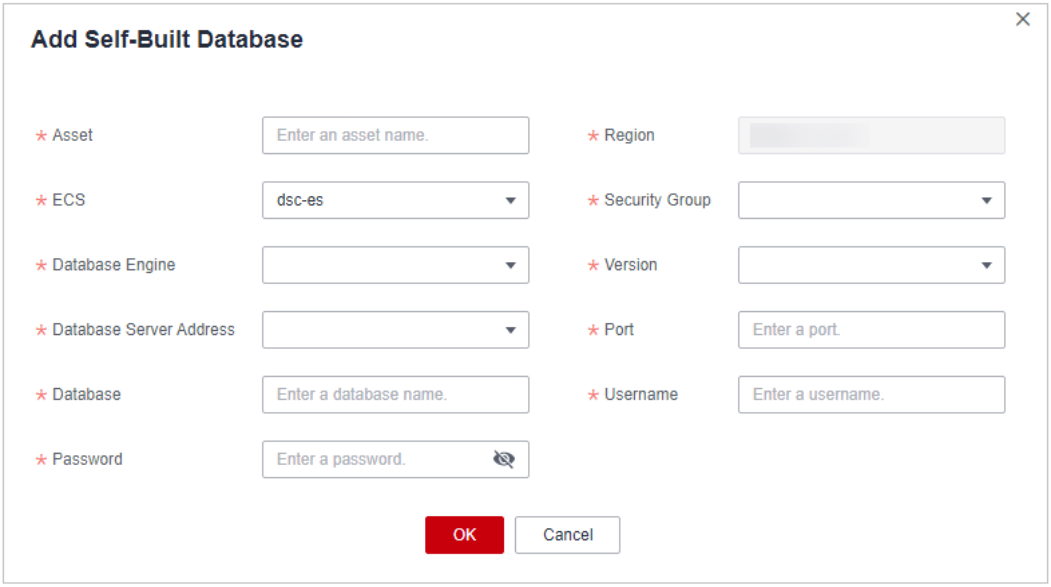


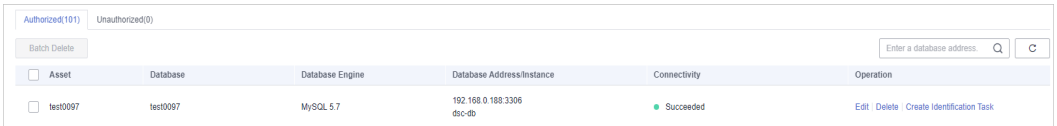
Table 3-6 Parameters for adding a self-built database

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**, **PostgreSQL**, **SQLServer**, and **Oracle**	MySQL
Version	Version number corresponding to the database engine	5.6
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

Parameter	Description	Example Value
Password	Password for logging in to the database server	N/A

Step 7 Click **OK**.

Figure 3-18 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**. Click **Cause** to view the failure cause.

----End

3.4.4 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

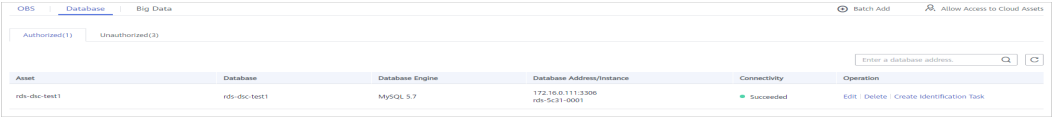
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Assets** and select the **Database** tab and then the **Authorized** tab.

Figure 3-19 Authorized database assets



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**. Click **Cause** to view the failure cause.

----End

3.4.5 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

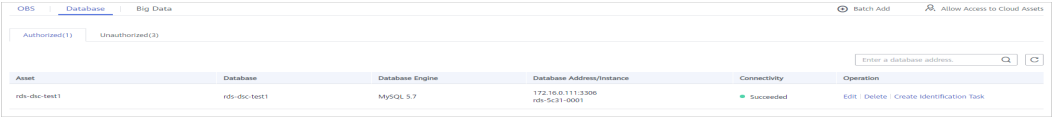
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Assets** and select the **Database** tab and then the **Authorized** tab.

Figure 3-20 Authorized database assets



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.

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

----End

3.5 Big Data Assets

3.5.1 Adding a Big Data Source

Add big data assets stored in CSS, DLI, and Hive.

Prerequisites

- Permissions for accessing to the big data assets have been obtained. For details, see **Allowing or Disallowing Access to Cloud Assets**.

Procedure

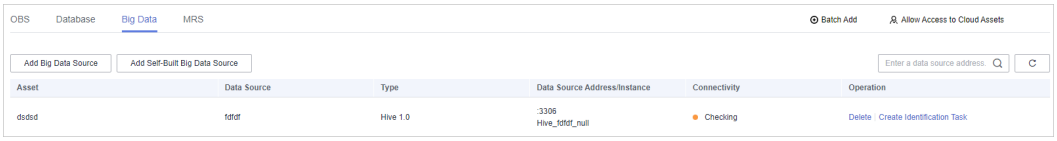
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Assets** and click the **Big Data** tab.

Figure 3-21 Big data assets



Step 5 In the upper left corner of the big data asset list, click **Add Big Data Source**.

Step 6 In the displayed dialog box, set parameters for adding a big data source. For details, see **Table 3-7**.

Figure 3-22 Adding a big data source

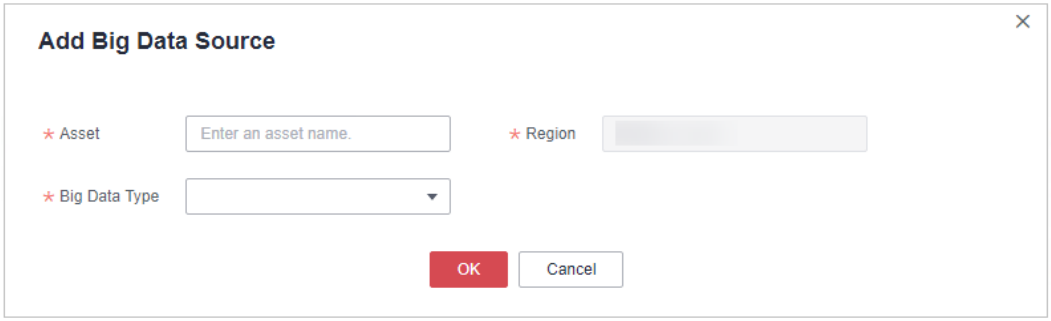


Table 3-7 Parameters for adding a big data source

Parameter	Description	Example Value
Asset	Customized parameter	N/A
Region	Region where the account is used for login	N/A
Big Data Type	Type of a big data asset. The options are as follows: ● When you select **Elasticsearch**, refer to **Table 3-8** for descriptions about the parameters required. ● When you select **DLI**, refer to **Table 3-9** for descriptions about the parameters required. ● When you select **Hive**, refer to **Table 3-10** for descriptions about the parameters required.	Elasticsearch

Table 3-8 Parameters required for adding Elasticsearch big data source

Parameter	Description	Example Value
Elasticsearch Instance	Elasticsearch instance	N/A
Version	Version number corresponding to the big data type	5.x
Database Server Address	IP address of the big data source server	192.168.0.233
Port	Port number of the big data source server	3306
Index	Index corresponding to the big data source	N/A
Username	Username for accessing the big data server	N/A
Password	Password for accessing the big data server	N/A

Table 3-9 Parameters required for adding DLI big data source

Parameter	Description	Example Value
Queue	Select the queue from the drop-down list.	default
DLI Database	Select the database in the queue of DLI.	5.x

Table 3-10 Parameters required for adding Hive big data source

Parameter	Description	Example Value
VPC	Select a VPC from the drop-down list.	N/A
Subnet	Select the subnet of the VPC.	N/A
Security Group	Select an available security group from the drop-down list.	N/A
Database Server Address	IP address of the big data source server	192.168.0.233
Port	Port number of the big data source server	3306
Database	Enter a database name.	N/A

Step 7 Click **OK**.

After the big data source has been added, the connectivity status becomes **Checking** to check whether DSC can access the added big data asset using the new username and password.

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

----End

3.5.2 Adding a Self-Built Big Data Source

Add a self-built big data source asset to DSC.

Prerequisites

- Permissions for accessing to the big data assets have been obtained. For details, see **Allowing or Disallowing Access to Cloud Assets**.

- The type, version, host, and index of other self-built big data assets have been obtained. There are available IP addresses in the subnet of self-built big data assets.

Procedure

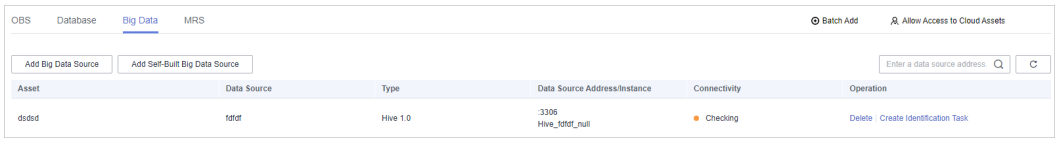
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Assets** and click the **Big Data** tab.

Figure 3-23 Big data assets



Step 5 In the upper left corner of the big data asset list, click **Add Self-Built Big Data Source**.

Step 6 In the displayed dialog box, configure parameters for adding a self-built big data source. For details, see **Table 3-11**.

Figure 3-24 Adding a self-built big data source

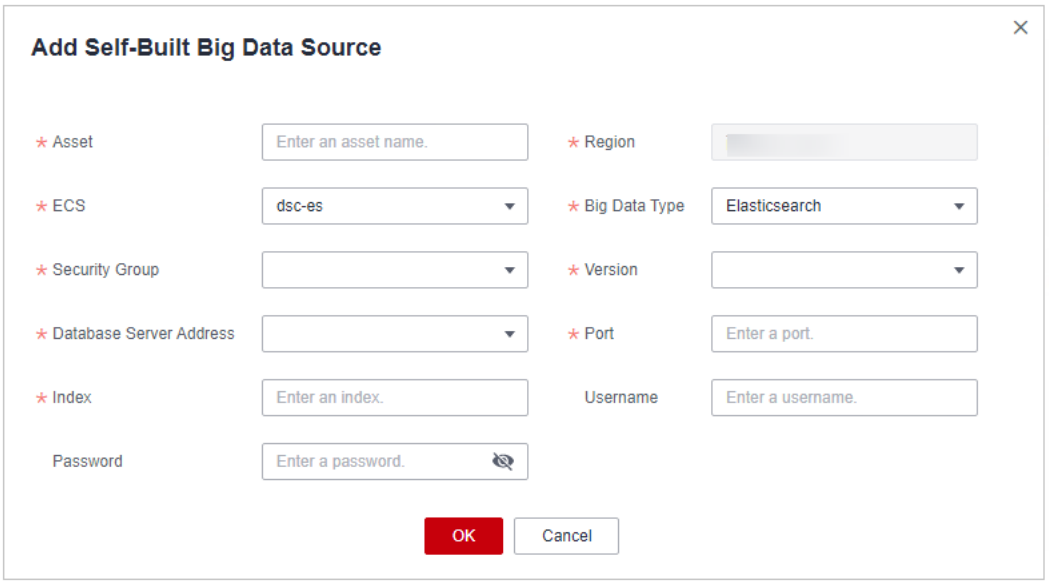


Table 3-11 Parameters for adding a self-built big data source

Parameter	Description	Example Value
Asset	Customized parameter	N/A
Region	Region where the account is used for login	N/A
ECS	Select an Elasticsearch instance.	N/A
Big Data Type	Type of a big data asset Currently, only **Elasticsearch** is supported.	Elasticsearch
Security Group	Select an existing security group from the drop-down list box.	default
Version	Version number corresponding to the big data type	5.x
Database Server Address	IP address of the big data asset server	192.168.0.233
Port	Port number of the big data asset server	3306
Index	Index corresponding to the big data asset	N/A
Username	Username for accessing the big data server	N/A
Password	Password for accessing the big data server	N/A

Step 7 Click **OK**.

After the big data source has been added, the connectivity status becomes **Checking** to check whether DSC can access the added big data asset using the new username and password.

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

----End

3.5.3 Editing a Big Data Source

Reset the modified or incorrect username and password of the added big data asset server.

Prerequisites

- Big data assets have been allowed to access. For details, see **Allowing or Disallowing Access to Cloud Assets**.
- Big data assets have been added.

Procedure

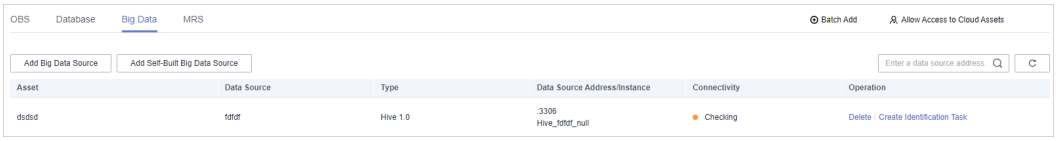
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Assets** and click the **Big Data** tab.

Figure 3-25 Big data assets



Step 5 Locate the row that contains the big data asset to be edited, click **Edit** in the **Operation** column.

Step 6 In the displayed dialog box, change the username or password for accessing the big data asset.

Step 7 Click **OK**.

After the big data asset has been edited, the connectivity status becomes **Checking** to check whether DSC can access the added big data asset using the new username and password.

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

----End

3.5.4 Deleting a Big Data Asset

This section describes how to delete a big data 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

- Big data assets have been allowed to access. For details, see **Allowing or Disallowing Access to Cloud Assets**.

- The big data asset to be deleted is not used in any sensitive data identification jobs.

Constraints

- If the big data asset to be deleted has been used in a sensitive data identification job, unbind the asset or delete the job 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

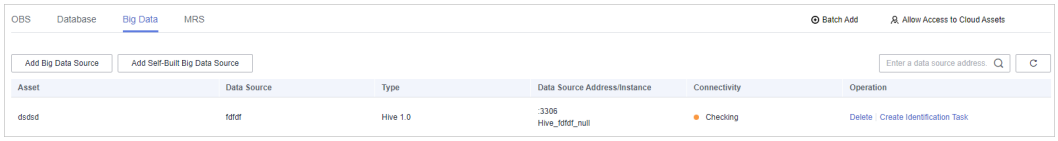
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Assets** and click the **Big Data** tab.

Figure 3-26 Big data assets



Step 5 Locate the row that contains the big data asset to be deleted, click **Delete** in the **Operation** column.

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

----End

3.6 MRS Assets

3.6.1 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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Assets** and select the **MRS** tab and then the **Unauthorized** tab.

Figure 3-27 MRS assets to be authorized

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 3-12.

Figure 3-28 MRS Authorization

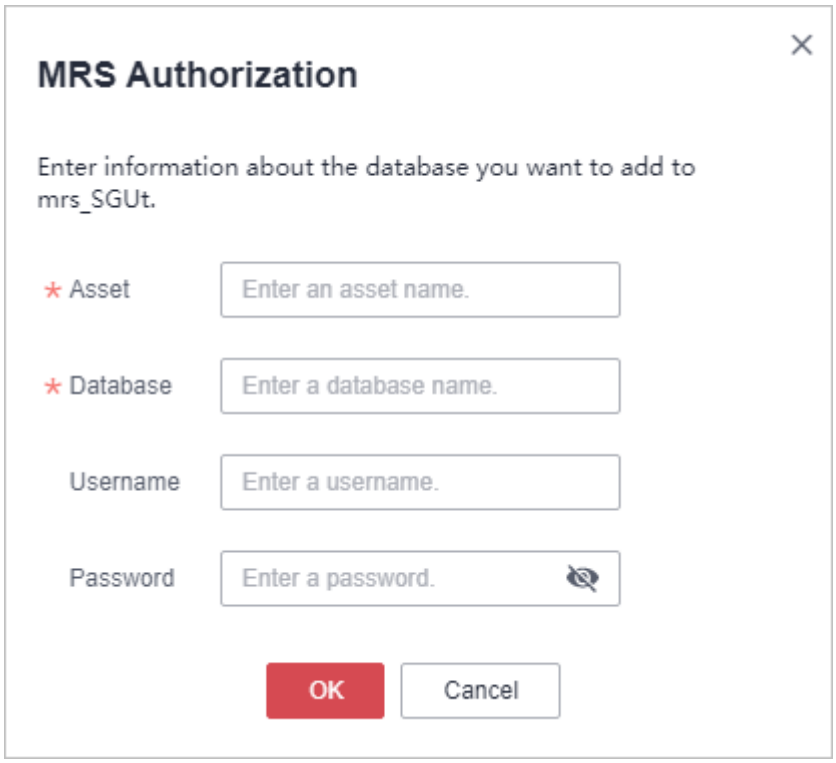


Table 3-12 Parameter description

Parameter	Description
Asset	Name of a custom MRS instance

Parameter	Description
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

3.6.2 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.
- 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.

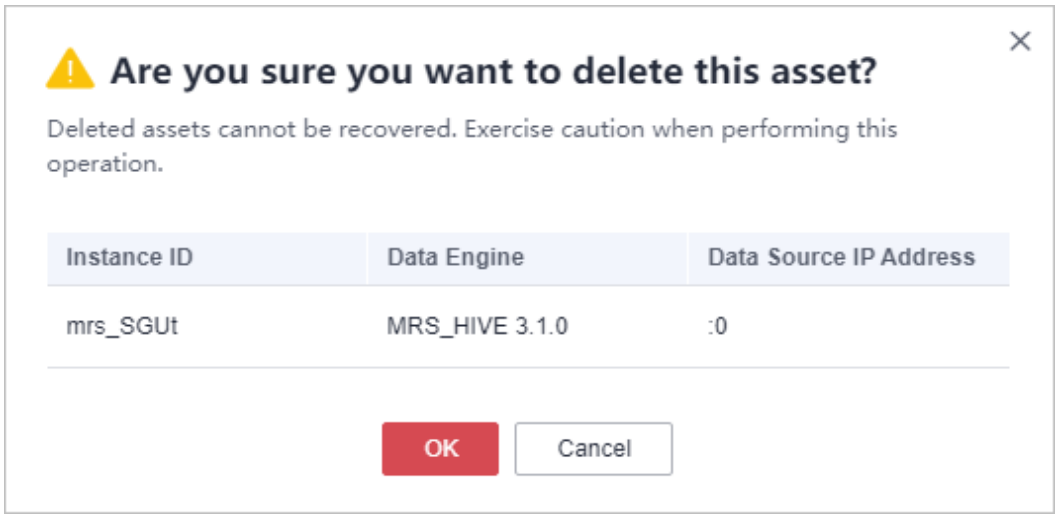
Step 3 In the navigation pane on the left, click and choose **Security** > **Data Security Center**.

Step 4 In the navigation pane, choose **Assets** and select the **MRS** tab and then the **Unauthorized** tab.

Figure 3-29 MRS assets to be authorized

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

Figure 3-30 Deleting an asset



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

----End

4 Overview

The **Overview** (asset map) page provides an overview of service security status and the constant visibility of the data security status in collection, transmission and storage, usage, exchange, and deletion.

Prerequisites

- Asset access permissions are granted.
- 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** > **Data Security Center**.

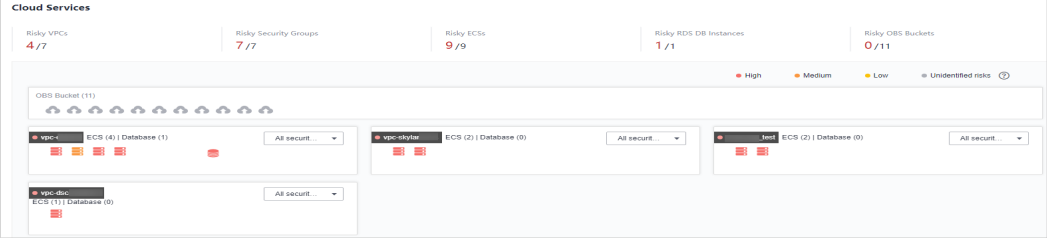
Step 4 On the **Overview** page, view the **Cloud Services** module.

This page provides a data asset map to help you build a panoramic view of your data assets. It displays the data asset distribution, data sensitivity, and risk levels in an intuitive way.

- **Sorted data assets**: Risky cloud data assets are sorted and displayed on an asset map, so that you know where the risky resources 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 assets are displayed by numbers of **risky VPCs**, **risky security groups**, **risky ECSs**, **risky RDS DB instances**, and **risky OBS buckets**.
  - Sensitive data of each type of assets is classified by **high**, **medium**, **low**, and **unidentified risks**.

- **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.

Figure 4-1 Cloud services



NOTE

- You can move the cursor to the data asset icon to view the asset information.
- If you click the data asset icon, in the dialog box displayed on the right, you can view the basic information, risk information, and risky security group rules related to this asset.

Step 5 Go to the **Data Collection Security** module, as shown in **Figure 4-2**.

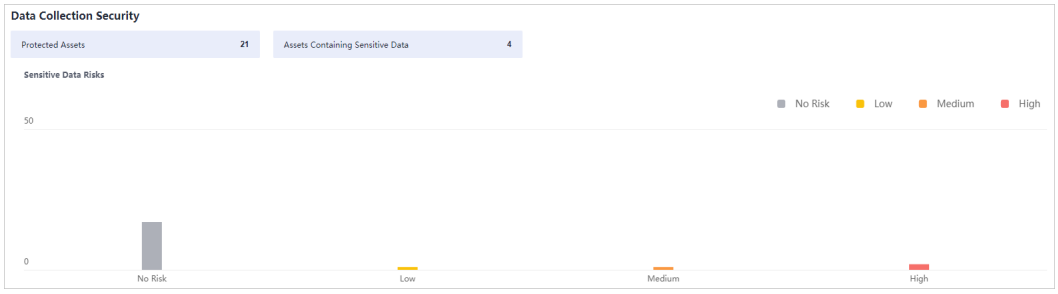
DSC identifies and classifies sensitive data based on data masking rules. You can view the distribution of data with different risk levels in your asset on the **Overview** page.

The sensitivity of a file is determined by the number of times that sensitive fields appear in the file and sensitive associations. Sensitive fields are classified into four risk levels based on their sensitivity: **Unidentified risks**, **Low**, **Medium**, and **High** risks. The risk levels increase in ascending order. Risk levels are described as follows:

- Unidentified (level 0)
- Low (level 1–3)
- Medium (level 4–7)
- High (level 8–10)

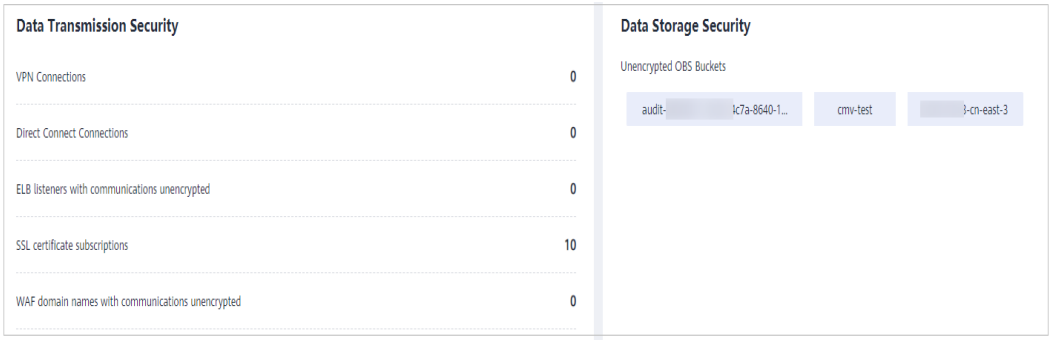
In the bar chart, different heights represent the number of assets of the corresponding risk level. Move the cursor to the bar chart to view the number of assets of the corresponding risk level.

Figure 4-2 Data collection security



Step 6 Go to the **Data Transmission Security** and **Data Storage Security** modules.

Figure 4-3 Data transmission and storage security



- **Data Transmission Security**: DSC displays the following items that may have transmission security risks (click an item to view details):
  - **VPN connections**: indicates the number of VPN connections that have been created in your assets. For details, see *Virtual Private Network User Guide*.
  - **Direct Connect connections**: indicates the number of Direct Connect connections have been created in your assets. For details, see *Direct Connect User Guide*.
  - **ELB listeners with communications unencrypted**: indicates the number of added listeners that do not use HTTPS for encryption. You are advised to enhance communications security using HTTPS.
  - **SSL certificate subscriptions**: indicates the number of purchased or uploaded certificates in your assets. For details about SSL certificates, see *SSL Certificate Manager User Guide*.
  - **WAF domain names with communications unencrypted**: indicates the number of added WAF domain names that do not use HTTPS for encryption. You are advised to enhance communications security using HTTPS.
- **Data Storage Security**: This module lists the OBS buckets that are not encrypted. To protect your assets from avoidable storage security risks, you are advised to click the unencrypted OBS bucket to go to the OBS console and encrypt the bucket. .

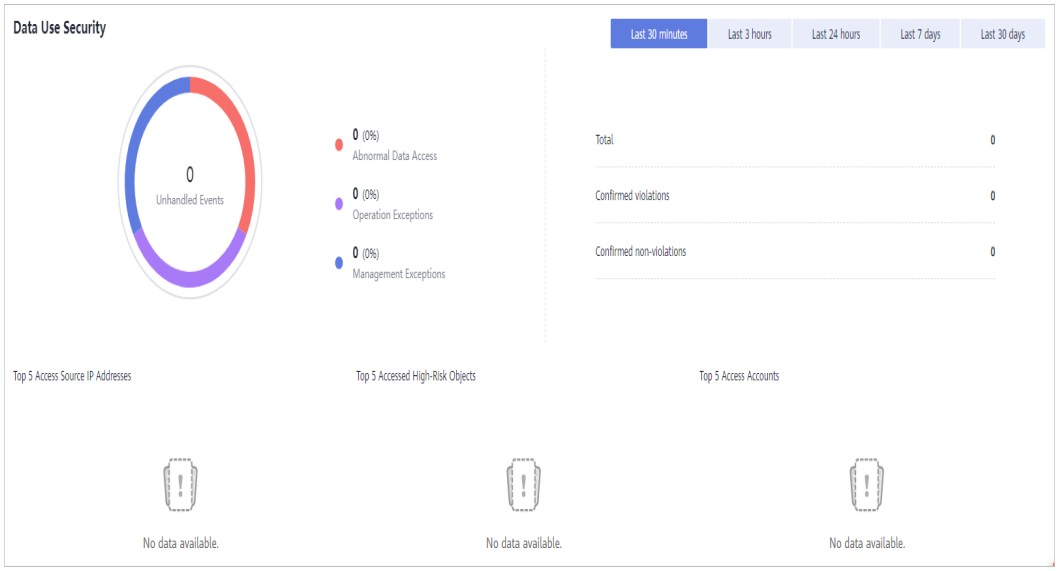
Step 7 Go to the **Data Usage Security** module.

This module displays data usage security information within the last 30 minutes, last 3 hours, last 24 hours, last 7 days, and last 30 days.

- **Unhandled Events**: displays the proportion of data access exceptions, operation exceptions, and management exceptions. In addition, the total number of abnormal events, confirmed violations, and confirmed non-violations are displayed.
  - Click a color area in **Unhandled Events** to view the proportion of abnormal events of a specified data type.
  - To stop displaying information about an unhandled event, click the legend with the same color to the right of the circle.
- **Top 5 Access Source IP Addresses**: displays statistics on the top 5 access source IP addresses.

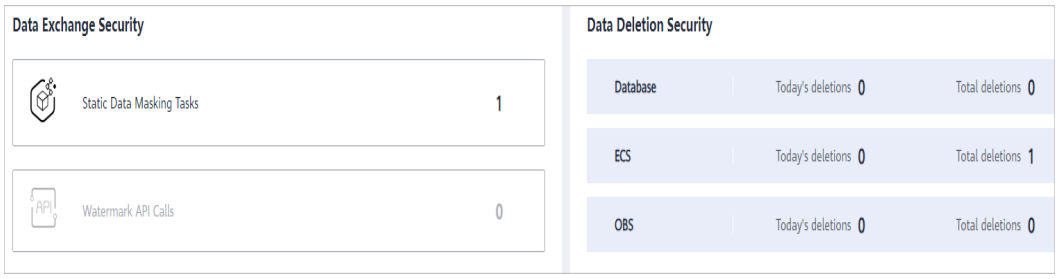
- **Top 5 Accessed High-Risk Objects**: displays statistics on the top 5 accessed high-risk objects.
- **Top 5 Access Accounts**: displays statistics on the top 5 access accounts.

Figure 4-4 Data Use Security



Step 8 Go to the **Data Exchange Security** and **Data Deletion Security** modules.

Figure 4-5 Data exchange and deletion security



- **Data Exchange Security**: DSC displays the number of created static data masking tasks and watermark API calls. For details about how to create a data masking task, see **Creating a Data Masking Task**.
- **Data Deletion Security**: DSC collects statistics on the number of daily and total deleted database, ECS, and OBS assets.

----End

5 Sensitive Data Identification

5.1 Identification Rules

5.1.1 Adding a Rule

An identification rule group, as a service logic group, includes scattered rules. A rule group is the prerequisite for operating a sensitive data identification task.

Constraints

You can add a built-in rule or customized rule. Built-in rules cannot be added, edited, and deleted.

Procedure

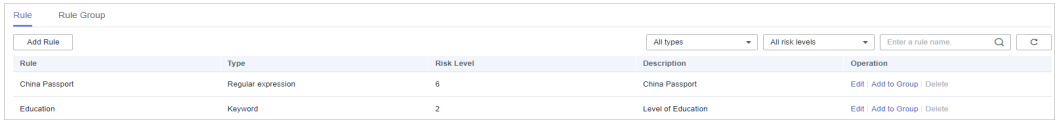
Step 1 Log in to the management console.

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** > **Data Security Center**.

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

Figure 5-1 Rules



Step 5 In the upper left corner of the rule list, click **Add Rule**.

Step 6 In the displayed dialog box, configure basic parameters. For parameter details, see **Table 5-1**.

Figure 5-2 Adding an identification rule

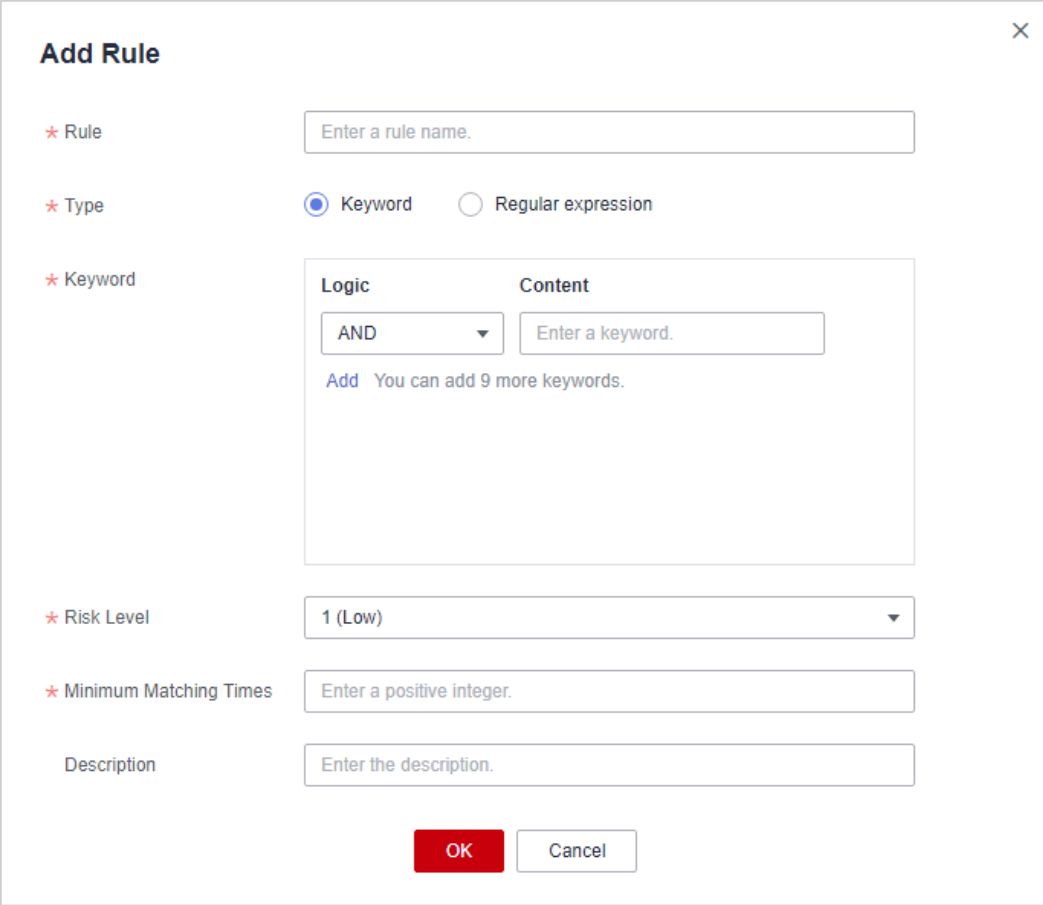


Table 5-1 Parameters for adding an identification rule

Name	Description	Example Value
Rule	You can customize a rule name. The rule name must meet the following requirements: ● Contain 1 to 255 characters. ● Consist of letters, digits, underscores (_), and hyphens (-). ● Be unique.	N/A
Type	Set it to **Keyword** or **Regular expression**. ● **Keyword**: Indicates that the rule can be executed using keywords. ● **Regular expression**: A regex follows concise, flexible principles to match (specify and identify) characters, words, and patterns.	Keyword

Name	Description	Example Value
Keyword	This parameter is displayed when **Type** is set to **Keyword**. ● **Logic**: Select a logical relationship for keywords. – **AND**: All keywords are included. – **OR**: Only one keyword is included. ● **Content**: Enter a keyword. You can click Add to add a maximum of 10 keywords.	and, Zhang San
Regular Expression	This parameter is displayed when **Type** is set to **Regular expression**.	N/A
Risk Level	Select the risk level for the rule. The risk level ranges from 1 to 10. Levels 1 to 3 indicate low risks, 4 to 7 indicate medium risks, and 8 to 10 indicate high risks.	5 (Medium)
Minimum Matching Times	Number of rule hits. If the number of rule hits reaches the set value, the information will be marked as sensitive information.	2
Description	(Optional) This parameter is used to differentiate this rule from others.	N/A

Step 7 Click **OK**.

----End

5.1.2 Viewing the Rule List

View the sensitive data identification rule list.

Prerequisites

Identification rules have been added.

Procedure

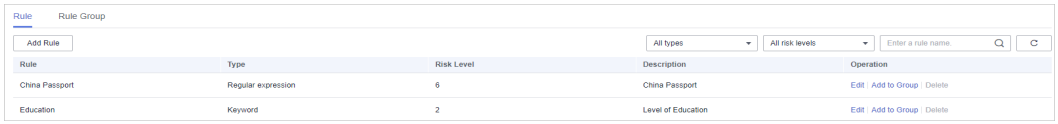
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Sensitive Data Identification** > **Identification Rule**. Table 5-2 describes the parameters.

Figure 5-3 Rules



NOTE

- In the upper right corner of the page, select a rule type and risk level to view the corresponding rules.
- In the search box, enter a rule name or keyword and click 🔍 or press **Enter** to search for the specified rule.

Table 5-2 Rule parameters

Parameter	Description
Rule	Rule name
Type	Rule types: • **Keyword**: Keyword used to execute a rule • **Regular expression**: Regular expression used to execute a rule
Risk Level	Risk level of an identification rule The risk level ranges from 1 to 10. Levels 1 to 3 indicate low risks, 4 to 7 indicate medium risks, and 8 to 10 indicate high risks.
Description	Rule description

----End

5.1.3 Editing a Rule

Edit a sensitive data identification rule, for example, editing the rule name, type, and description.

Prerequisites

Identification rules have been added.

Constraints

DSC built-in identification rules cannot be edited.

Procedure

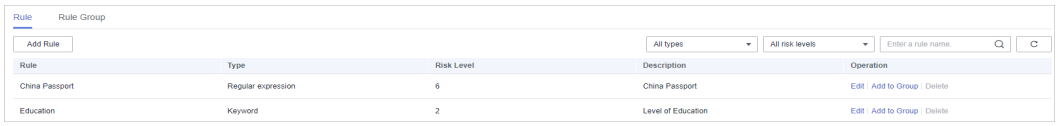
Step 1 Log in to the management console.

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** > **Data Security Center**.

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

Figure 5-4 Rules



Step 5 In the rule list, locate the row that contains the rule to be edited, and click **Edit** in the **Operation** column.

Step 6 In the displayed dialog box, edit rule parameters as required. **Table 5-3** describes the parameters.

Figure 5-5 Editing a rule

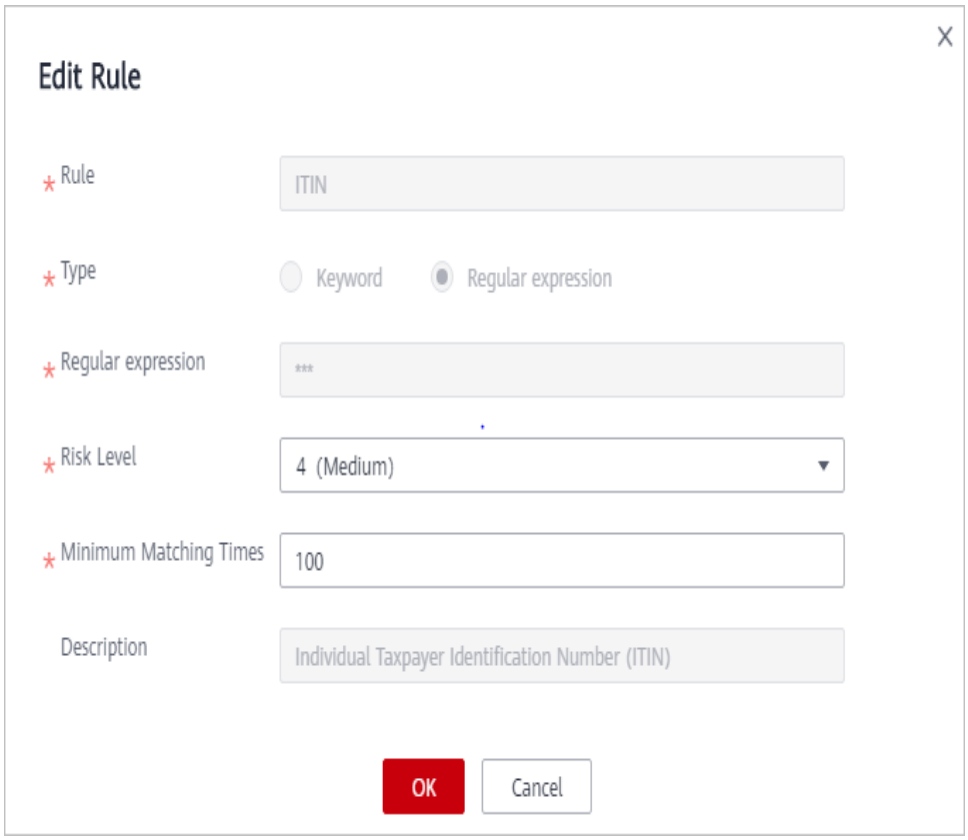


Table 5-3 Parameters for adding an identification rule

Name	Description	Example Value
Rule	You can customize a rule name. The rule name must meet the following requirements: ● Contain 1 to 255 characters. ● Consist of letters, digits, underscores (_), and hyphens (-). ● Be unique.	N/A
Type	Set it to **Keyword** or **Regular expression**. ● **Keyword**: Indicates that the rule can be executed using keywords. ● **Regular expression**: A regex follows concise, flexible principles to match (specify and identify) characters, words, and patterns.	Keyword
Keyword	This parameter is displayed when **Type** is set to **Keyword**. ● **Logic**: Select a logical relationship for keywords. – **AND**: All keywords are included. – **OR**: Only one keyword is included. ● **Content**: Enter a keyword. You can click Add to add a maximum of 10 keywords.	and, Zhang San
Regular Expression	This parameter is displayed when **Type** is set to **Regular expression**.	N/A
Risk Level	Select the risk level for the rule. The risk level ranges from 1 to 10. Levels 1 to 3 indicate low risks, 4 to 7 indicate medium risks, and 8 to 10 indicate high risks.	5 (Medium)
Minimum Matching Times	Number of rule hits. If the number of rule hits reaches the set value, the information will be marked as sensitive information.	2
Description	(Optional) This parameter is used to differentiate this rule from others.	N/A

Step 7 Click **OK**.

----End

5.1.4 Deleting a Rule

User-defined sensitive data rules that are no longer used can be deleted from the sensitive data rule list.

- Rules that have been added to rule groups cannot be deleted.
- DSC built-in rules cannot be deleted.

Prerequisites

- Identification rules have been added.
- Rules to be deleted are not added to a rule group.

Constraints

- DSC built-in rules cannot be deleted.
- If the rule to be deleted has been added to a rule group, remove the rule from the group by following the instructions provided in **Editing a Rule Group** and then delete the rule.
- Deleted rules cannot be recovered. Exercise caution when performing this operation.

Procedure

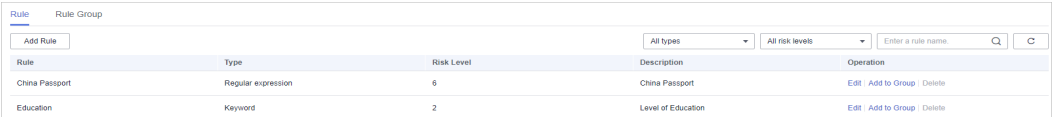
Step 1 Log in to the management console.

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** > **Data Security Center**.

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

Figure 5-6 Rules



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

Step 6 Click **OK**.

----End

5.1.5 Adding a Rule to a Rule Group

Add an identification rule to a rule group. You can select a rule group for a specific sensitive data identification task.

Prerequisites

- Identification rules have been added.
- Identification rule groups have been created.

Procedure

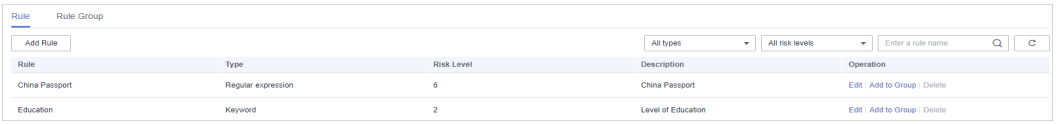
Step 1 Log in to the management console.

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** > **Data Security Center**.

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

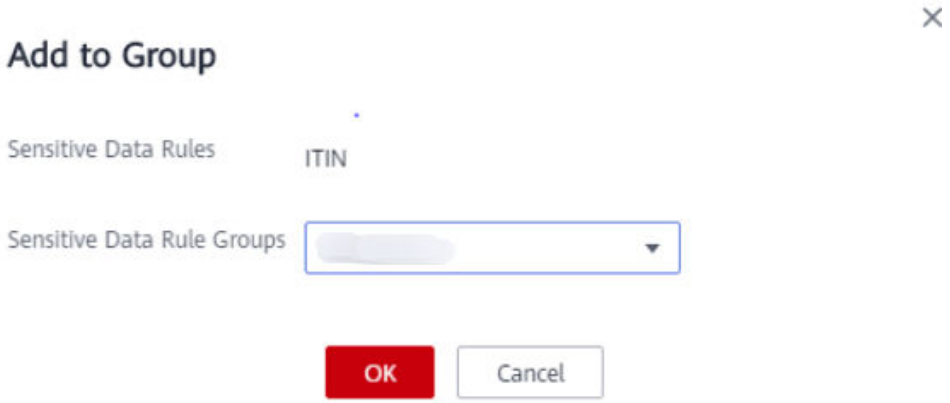
Figure 5-7 Rules



Step 5 In the rule list, locate the row that contains the rule to be added to a group, and click **Add to Group** in the **Operation** column.

Step 6 In the displayed dialog box, select a rule group.

Figure 5-8 Adding a rule to a rule group



Step 7 Click **OK**.

----End

5.2 Identification Rule Groups

5.2.1 Adding a Rule Group

If the built-in rule groups provided by DSC cannot meet your sensitive data identification scenarios, you can refer to this section to customize sensitive data rule groups and flexibly combine rules to identify sensitive data in various scenarios.

Constraints

You can add a built-in or customized rule group. Built-in rule groups cannot be added, edited, and deleted.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Sensitive Data Identification** > **Identification Rule**. On the displayed page, click the **Rule Group** tab.

Figure 5-9 Rule groups

Step 5 In the upper left corner of the rule group list, click **Add Rule Group**.

Step 6 In the displayed dialog box, configure basic parameters. **Table 5-4** describes the parameters.

Figure 5-10 Adding a rule group

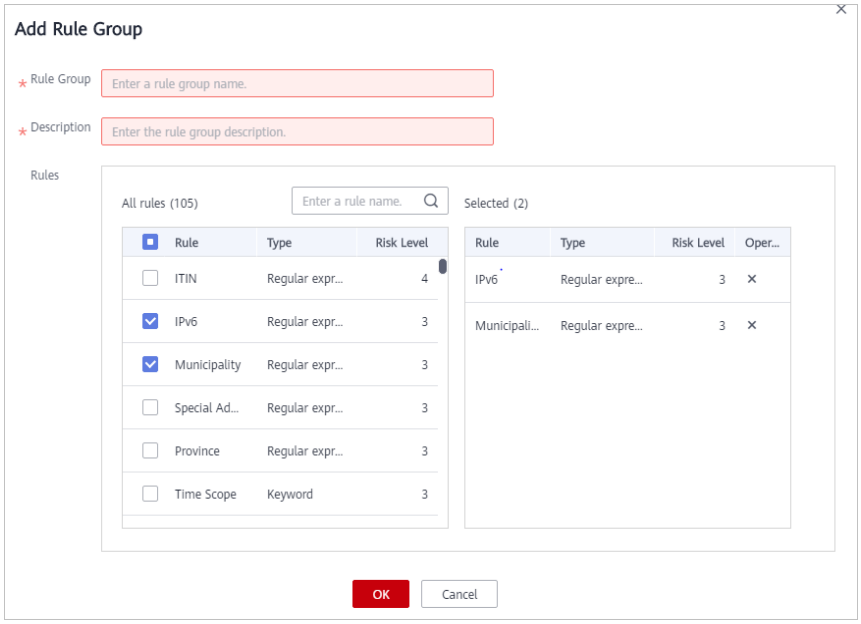


Table 5-4 Parameters for adding a rule group

Name	Description
Rule Group	You can customize a rule group name. The group name must meet the following requirements: ● Contain 1 to 255 characters. ● Consist of letters, digits, underscores (_), and hyphens (-). ● Be unique.
Description	This parameter is used to differentiate this rule from others.
Rules	(Optional) Select the rules to be added. If you want to remove a selected rule, locate the row containing the target rule in the **Selected** box on the right, and click ✕ in the **Operation** column.

Step 7 Click **OK**.

----End

5.2.2 Viewing the Rule Group List

View details about a sensitive data identification rule group.

Prerequisites

Identification rule groups have been added.

Procedure

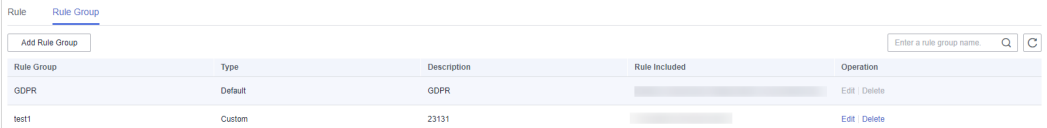
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Sensitive Data Identification** > **Identification Rule**. On the displayed page, click the **Rule Group** tab. Table 5-5 describes the rule group parameters.

Figure 5-11 Rule groups



NOTE

In the search box, enter a rule group name or keyword and click or press **Enter** to search for the specified rule group.

Table 5-5 Rule group parameters

Parameter	Description
Rule Group	Rule group name
Type	Rule group types: • **Custom**: Customized rule groups • **Default**: DSC built-in rule groups
Description	Rule group description
Rule Included	Rules contained in a rule group
Operation	Operations provided in the **Operation** column: • Click **Edit** to modify an identification rule group. For details, see **Editing a Rule Group**. • Click **Delete** to delete a customized identification rule group. For details, see **Deleting a Rule Group**.

----End

5.2.3 Editing a Rule Group

Edit a sensitive data identification rule group. You can perform the following operations:

- Modify **Rule Group** and **Description**.
- Add more rules.
- Remove rules.

Prerequisites

- Identification rule groups have been added.
- The type of rule groups to be edited is **Custom**.

Constraints

DSC built-in sensitive data rule groups cannot be edited.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Sensitive Data Identification** > **Identification Rule**. On the displayed page, click the **Rule Group** tab.

Figure 5-12 Rule groups

Step 5 In the rule group list, locate the row that contains the group to be edited, and click **Edit** in the **Operation** column.

Step 6 In the displayed dialog box, edit the rule group parameters. **Table 5-6** describes the parameters.

Figure 5-13 Editing a rule group

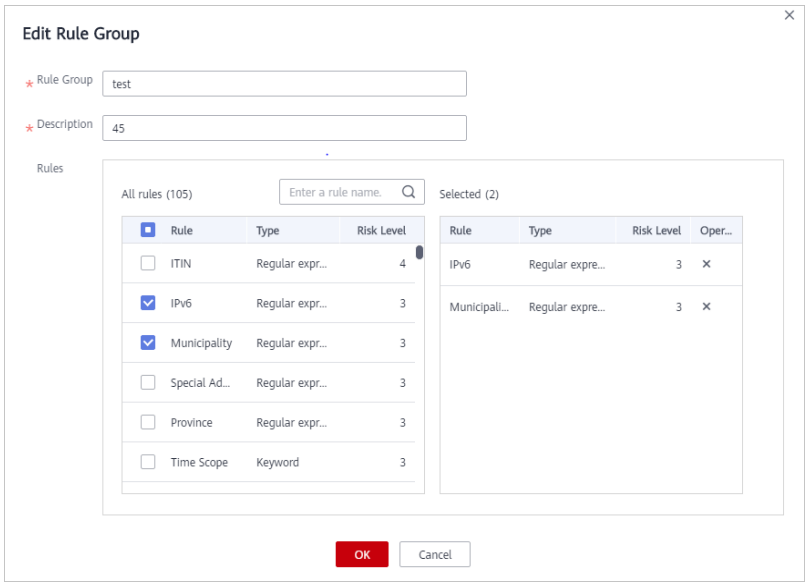


Table 5-6 Parameters for adding a rule group

Name	Description
Rule Group	You can customize a rule group name. The group name must meet the following requirements: ● Contain 1 to 255 characters. ● Consist of letters, digits, underscores (_), and hyphens (-). ● Be unique.
Description	This parameter is used to differentiate this rule from others.
Rules	(Optional) Select the rules to be added. If you want to remove a selected rule, locate the row containing the target rule in the **Selected** box on the right, and click ✕ in the **Operation** column.

Step 7 Click **OK**.

----End

5.2.4 Deleting a Rule Group

You can delete user-defined sensitive data rule groups that are no longer used from the rule group list.

- A rule group that has been used in an identification task cannot be deleted.
- DSC built-in rule groups cannot be deleted.

Prerequisites

Identification rule groups have been added.

Constraints

- DSC built-in rule groups cannot be deleted.
- If the rule group to be deleted has been used in an ongoing identification task, delete the task and then the rule group.
- Deleted rule groups 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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Sensitive Data Identification** > **Identification Rule**. On the displayed page, click the **Rule Group** tab.

Figure 5-14 Rule groups

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

Step 6 Click **OK**.

----End

5.3 Identification Tasks

5.3.1 Creating a Task

Create a sensitive data identification task for DSC to automatically identify sensitive data in a specified database, OBS bucket, MRS, or big data source and generate identification results and reports.

To configure the task to scan the same asset for multiple scenarios, select multiple scenarios for the rule group.

Prerequisites

- You have added OBS buckets, databases, or big data sources to the asset list. For details, see **Assets**.
- Identification rule groups have been created. For creation details, see **Adding a Rule Group**.

Procedure

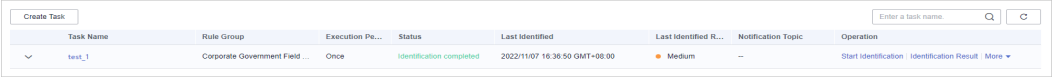
Step 1 Log in to the management console.

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** > **Data Security Center**.

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

Figure 5-15 Identification task



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

Step 6 In the displayed dialog box, configure the basic parameters. **Table 5-7** describes the parameters.

Figure 5-16 Creating an identification task

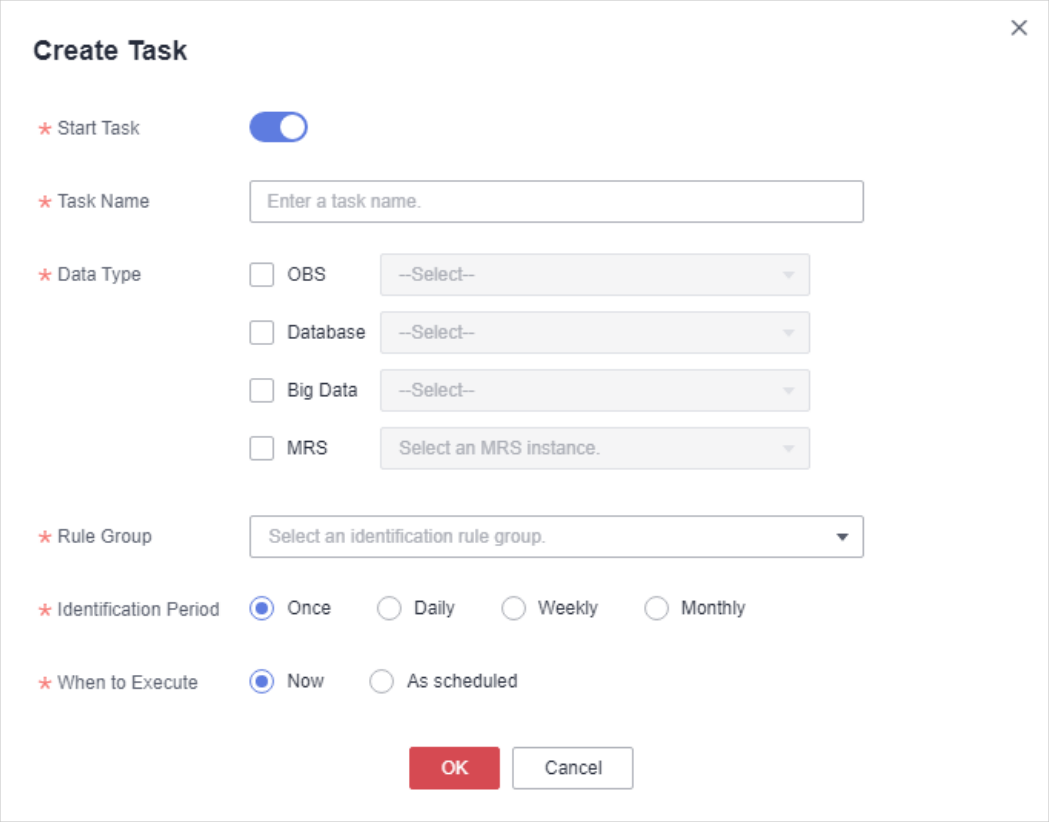


Table 5-7 Parameters for creating an identification task

Name	Description	Example Value
Start Task	Indicates whether to enable the sensitive data identification task. By default, the task is started. ● : enabled ● : disabled	
Task Name	You can customize the task name. The name must meet the following requirements: ● Contain 1 to 255 characters. ● Consist of letters, digits, underscores (_), and hyphens (-). ● Be unique.	N/A

Name	Description	Example Value
Data Type	Select one or more data types for identification. • **OBS**: Add OBS buckets. For details, see **Adding OBS Assets**. • **Database**: Add databases. For details, see **Adding a Database**. • **Big Data**: Add big data sources. For details, see **Adding a Big Data Source**. • **MRS**: Add Hive assets. For details, see **Adding MRS Assets**.	Database
Rule Group	Select one or more rule groups for the identification task. For details about how to create a rule group, see **Adding a Rule Group**.	N/A
Identification Method	Select an identification method. The options are as follows: • **Quick identification**: Quickly identify sensitive data using rule groups. • **Full identification**: Combing the rule groups with NLP, DSC provides more accurate identification results but at a relatively slow speed.	Quick scan
Identification Period	Select the task identification period. • **Once**: The task will be executed once at a specified time as planned. • **Daily**: Set **Start Time**, and the task will be performed at a fixed time every day. • **Weekly**: Set **Start Time**, and the task will be performed at a fixed time every week. • **Monthly**: Set **Start Time**, and the task will be performed at a fixed time every month.	Once
When to Execute	This parameter is displayed when **Once** is selected for **Scan Period**. • **Now**: The task will be executed immediately. • **As scheduled**: The task will be executed at a specified time.	Now
Start Time	This parameter is displayed only when **Scan Period** is set to **Daily**, **Weekly**, or **Monthly**. Set the start time of an identification task. After this parameter is set, the task will be executed at the specified time every day, every week, or every month.	N/A

Step 7 Click **OK**.

----End

5.3.2 Viewing the Job List

In the sensitive data identification task list, you can view the task details.

Prerequisites

Identification tasks have been 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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Sensitive Data Identification** > **Identification Task**. On the displayed page, view the identification task details. **Table 5-8** describes the task parameters.

NOTE

- In the search box, enter a task name or keyword and click or press **Enter** to search for the specified task.
- Click the task name to view the identification job report.
- In the task list, locate the row that contains the task to be viewed, and choose **More** > **Download** in the **Operation** column to download the risk result report in Excel format.

Table 5-8 Identification task parameters

Parameter	Description
Task Name	Identification job name ● In front of a target task, click ⌄ to view the scanning time and task status. In the **Operation** column of a specific object, you can perform the following operations: – Click **Stop** to stop an identification job. – Click **Start Identification** to start an identification job. – Click **View Results** to view the identification result. – Click **Delete** to delete an identification job. ● Click the task name to view the identification job report.
Rule Group	Rule group used by an identification job
Execution Period	Execution period of an identification job Parameters are described as follows: ● **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 month. ● **Monthly**: The task is executed once a week.
Status	Execution status of an identification task ● **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 executing is forcibly stopped.
Last Identified	Last execution time of the task.
Last Identified Result	Result of the last identification. The value can be **No risk**, **Low**, **Medium**, or **High**.

Parameter	Description
Operation	Operations provided in the **Operation** column: ● Execute an identification task immediately. For details, see **Starting a Job**. ● View the identification result. Click **View Result** to go to the result details page. DSC provides a detailed result analysis report. For details, see **Identification Results**. ● Download the risk result. Click **More** to download the risk result and obtain the detailed risk result report. ● Edit an identification job. For details, see **Editing a Task**. ● Delete an identification job. For details, see **Deleting a Task**.

----End

5.3.3 Starting a Job

Start a sensitive data identification task.

Prerequisites

Identification tasks have been created.

Procedure

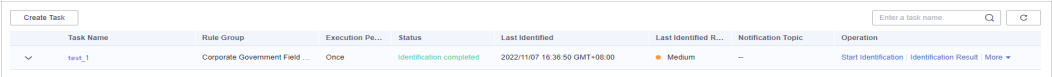
Step 1 Log in to the management console.

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** > **Data Security Center**.

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

Figure 5-17 Identification task



Step 5 In the task list, locate the row that contains the task to be started, Click **Start Identification** in the **Operation** column.

NOTE

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

----End

5.3.4 Editing a Task

Edit a sensitive data identification task.

Prerequisites

Identification tasks have been created.

Procedure

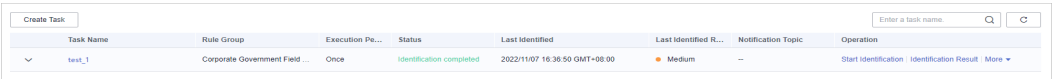
Step 1 Log in to the management console.

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** > **Data Security Center**.

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

Figure 5-18 Identification task



Step 5 In the task list, locate the row that contains the task to be edited, choose **More** > **Edit** in the **Operation** column.

Step 6 In the displayed dialog box, edit the task parameters. For parameter details, see **Table 5-9**.

Figure 5-19 Editing a task

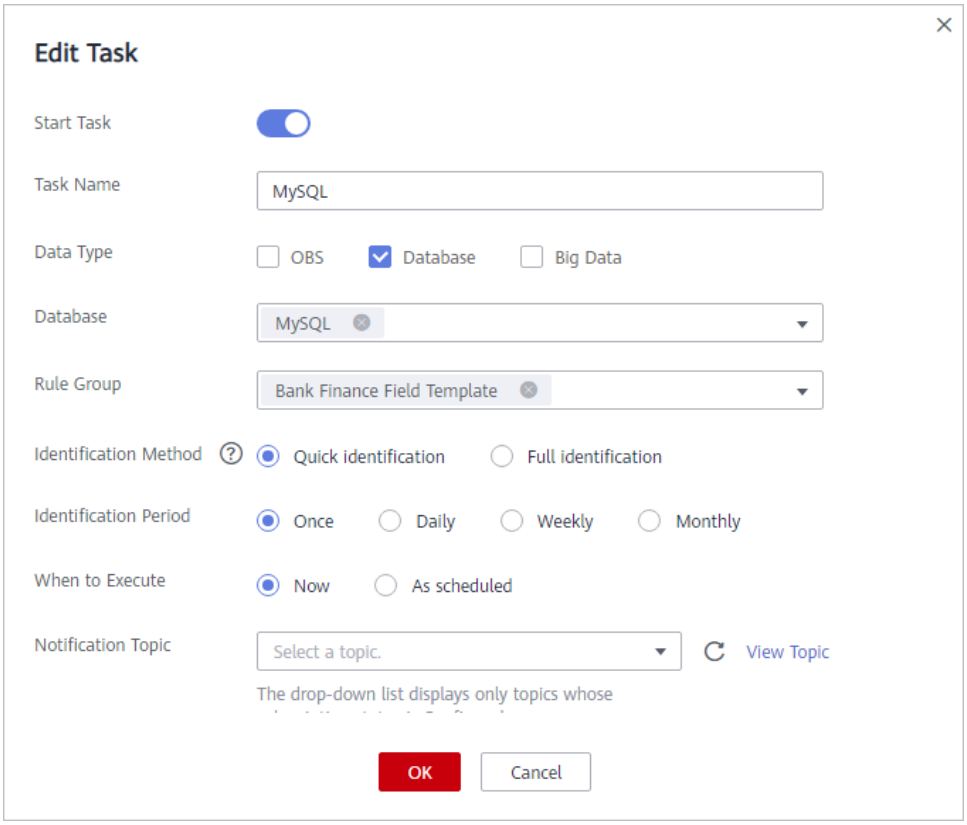


Table 5-9 Parameters for creating an identification task

Name	Description	Example Value
Start Task	Indicates whether to enable the sensitive data identification task. By default, the task is started. • : enabled • : disabled	
Task Name	You can customize the task name. The name must meet the following requirements: • Contain 1 to 255 characters. • Consist of letters, digits, underscores (_), and hyphens (-). • Be unique.	N/A

Name	Description	Example Value
Data Type	Select one or more data types for identification. • **OBS**: Add OBS buckets. For details, see **Adding OBS Assets**. • **Database**: Add databases. For details, see **Adding a Database**. • **Big Data**: Add big data sources. For details, see **Adding a Big Data Source**. • **MRS**: Add Hive assets. For details, see **Adding MRS Assets**.	Database
Rule Group	Select one or more rule groups for the identification task. For details about how to create a rule group, see **Adding a Rule Group**.	N/A
Identification Method	Select an identification method. The options are as follows: • **Quick identification**: Quickly identify sensitive data using rule groups. • **Full identification**: Combing the rule groups with NLP, DSC provides more accurate identification results but at a relatively slow speed.	Quick scan
Identification Period	Select the task identification period. • **Once**: The task will be executed once at a specified time as planned. • **Daily**: Set **Start Time**, and the task will be performed at a fixed time every day. • **Weekly**: Set **Start Time**, and the task will be performed at a fixed time every week. • **Monthly**: Set **Start Time**, and the task will be performed at a fixed time every month.	Once
When to Execute	This parameter is displayed when **Once** is selected for **Scan Period**. • **Now**: The task will be executed immediately. • **As scheduled**: The task will be executed at a specified time.	Now
Start Time	This parameter is displayed only when **Scan Period** is set to **Daily**, **Weekly**, or **Monthly**. Set the start time of an identification task. After this parameter is set, the task will be executed at the specified time every day, every week, or every month.	N/A

Step 7 Click **OK**.

----End

5.3.5 Deleting a Task

Delete a sensitive data identification task.

Prerequisites

Identification tasks have been created.

Constraints

- If the identification task is running, stop or delete the task after the task is complete.
- Deleted nodes cannot be recovered. Exercise caution when performing this operation.

Procedure

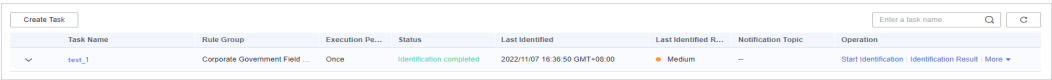
Step 1 Log in to the management console.

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** > **Data Security Center**.

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

Figure 5-20 Identification task



Step 5 In the task list, locate the row that contains the task to be deleted, choose **More** > **Delete** in the **Operation** column.

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

----End

5.3.6 Downloading a Report

Download the task report and identified risk result report. DSC provides task reports in PDF format and identified risk result reports in Excel format.

Prerequisites

- Identification tasks have been created.

- The identification task is complete.

Downloading the Result Report

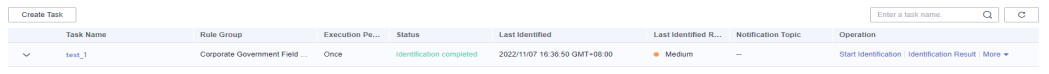
Step 1 Log in to the management console.

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** > **Data Security Center**.

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

Figure 5-21 Identification task



Step 5 In the task list, locate the row that contains the target task, choose **More** > **Identification Result** in the **Operation**, and save the result report in Excel format to your local PC.

----End

5.4 Identification Results

After the sensitive data identification task is complete, you can view the risk distribution, risk level, and sensitive data location on the **Identification Result** page.

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** > **Data Security Center**.

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

DSC collects statistics on the quantity and distribution of objects at different risk levels such as **High**, **Medium**, and **Low** in big data, database, and OBS assets.

In addition, DSC provides detailed identification results. In the upper right corner of the identification result list, view the desired result by risk level, task name,

data type, or object name. **Table 5-10** describes the parameters in the identification result list.

Figure 5-22 Identification results

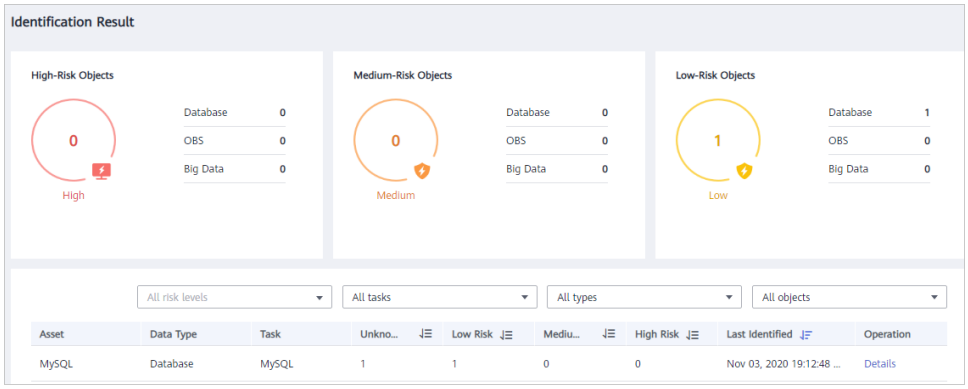


Table 5-10 Identification result parameters

Parameter	Description
Asset	Name of the asset that can be identified
Data Type	• OBS • Database • Big Data • MRS
Task	Name of the sensitive data identification task
Unknown Risk	Number of assets for which no risk is detected based on the identification rules you set
Low Risk	Number of low-risk assets (Level 1 to 3) detected based on the identification rules you set
Medium Risk	Number of medium-risk assets (Level 4 to 7) detected based on the identification rules you set
High Risk	Number of high-risk assets (Level 8 to 10) detected based on the identification rules you set
Last Identified	Latest time when the asset was identified
Operation	Click **View Details** to view the identification results.

Step 5 Locate the row that contains the identified data asset, click **View Details** in the **Operation** column.

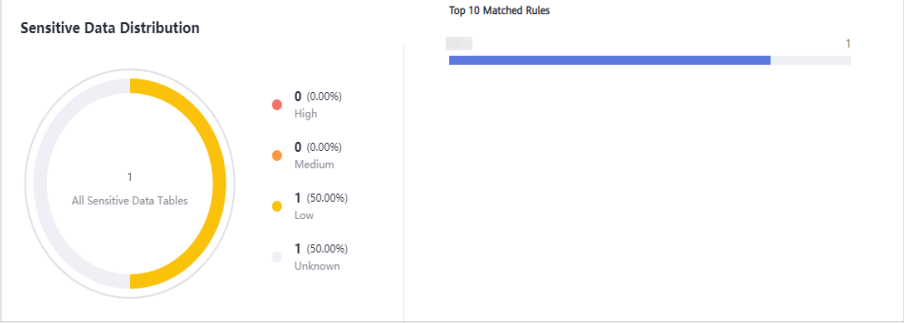
In the upper left corner of the page, select a task name, data type, or object name from the drop-down list box to view the identification result of a specific data asset.

In the upper right corner of the page, click **Download** to download the risk result report.

- Sensitive information distribution

  View the risk distribution of sensitive information, number and proportion of assets at each risk level, and top 10 hit rules.

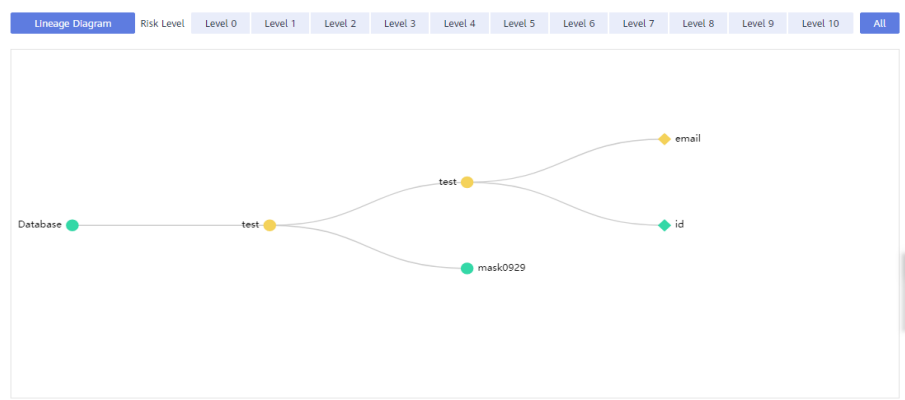
  Figure 5-23 Sensitive information distribution



- Lineage diagram

  View the names, paths, and risk levels of sensitive data in assets.

  Figure 5-24 Lineage diagram



----End

6 Data Masking

6.1 Introduction

DSC supports static data masking and dynamic data masking. You can configure masking rules for specified data assets to implement static masking. **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 Algorithms

Table 6-1 Masking algorithms

Algorithm	Description	Application Scenario
Hash	Use Hash functions to mask sensitive data. DSC supports SHA-256 and SHA-512. ● SHA-256 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. ● SHA-512 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	● Sensitive data: Key information ● Application scenario: data storage

Algorithm	Description	Application Scenario
	(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.	
Character Masking	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: ● 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 **NOTE** DSC has multiple character masking templates.	● Sensitive data: Personal data ● Application scenarios: – Data usage – Data sharing

Algorithm	Description	Application Scenario
Keyword Replacement	Search for keywords in a specified column and replace them. 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". 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.	● Sensitive data: – Personal data – Enterprise data – Device data ● Application scenarios: – Data storage – Data sharing

Algorithm	Description	Application Scenario
Value Change	Set a specified field to **Null** or left it blank for data masking. ● 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**.	● Sensitive data: – Personal data – Enterprise data – Device data ● Applicable scenarios – Data storage – Data sharing

Algorithm	Description	Application Scenario
Roundup	Round a date or number. ● Date Roundup Roundup of fields after the year field Example: 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 Example: 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 Example: 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 Example: 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	● Sensitive data: General data ● Applicable scenarios – Data storage – Data usage

Algorithm	Description	Application Scenario
	Example: 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 Example: 08:08:08.123 -> 08:08:08.000 or 1575612731312 -> 1575612731000 • Number roundup Rounds a specified number.	

Related Operations

- Configuring a Data Masking Rule
- Creating a Data Masking Task
- Executing a Data Masking Task
- Managing a Data Masking Task

6.2 Configuring a Data Masking Rule

This section describes how to configure a masking rule. For more details about masking algorithms, see **Introduction**.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Data Masking**. On the displayed page, click 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 based on **Hash**.
- If you select **Character Masking**, configure a masking rule based on **Character Masking**.
- If you select **Keyword Replacement**, configure a masking rule based on **Keyword Replacement**.
- If you select **Value Change**, configure a masking rule based on **Value Change**.
- If you select **Roundup**, configure a masking rule based on **Roundup**.

----End

Hash

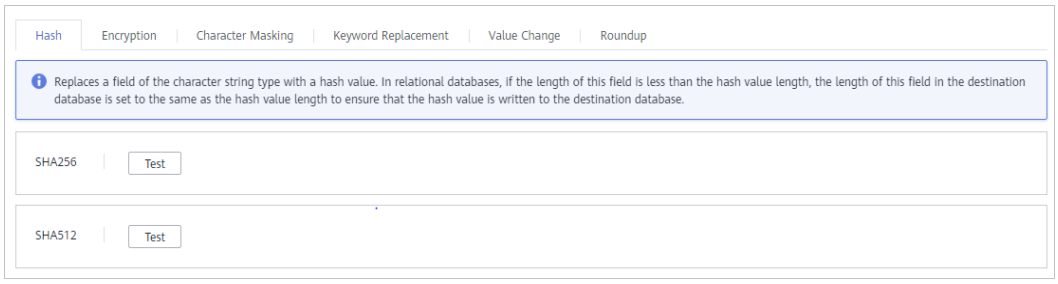
Hash functions are used in data storage to replace a character string fields with hash values. In a relational database, the length of a field must be the same as that of hash values so that the hash values can be completely written to the destination database. By default, two hash algorithms, SHA-256 and SHA-512, are configured for DSC.

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

Step 1 Go to the **Masking Rule** page by following operations provided in **Procedure**.

Step 2 Click the **Hash** tab.

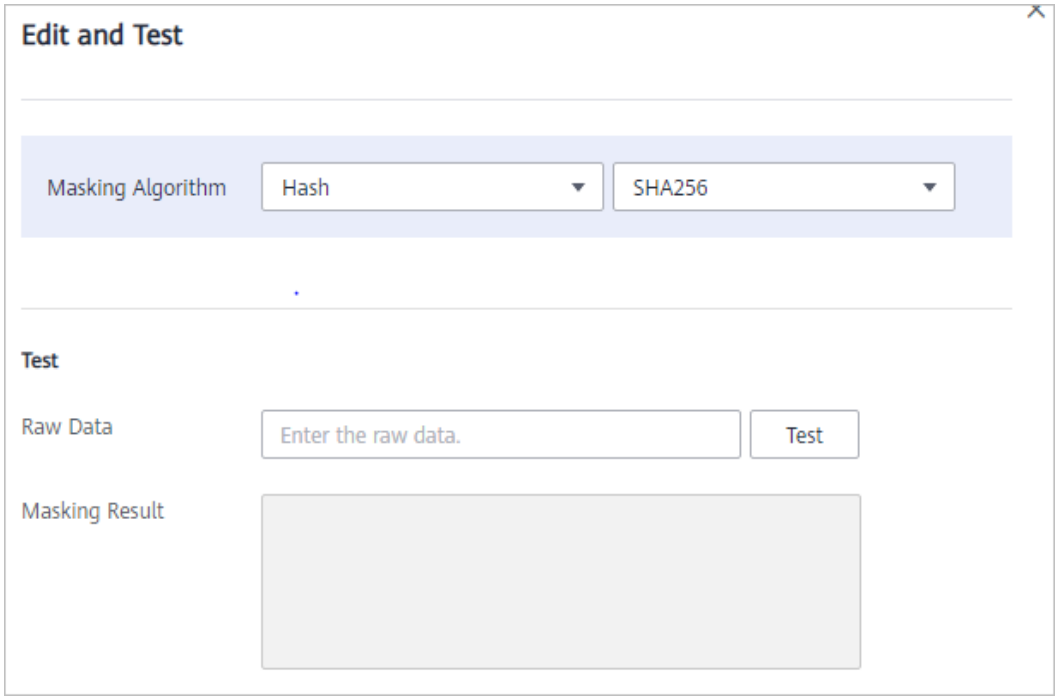
Figure 6-1 Hash algorithm



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

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

Figure 6-2 Hash method



----End

Character Masking

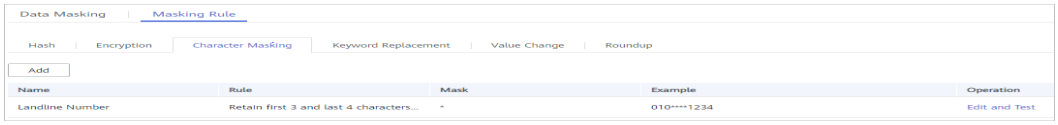
Use the specified character * or a random character to hide part of the content as required.

The following six masking approaches are supported: 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, and Mask data followed by special characters.

Step 1 Go to the **Masking Rule** page by following operations provided in **Procedure**.

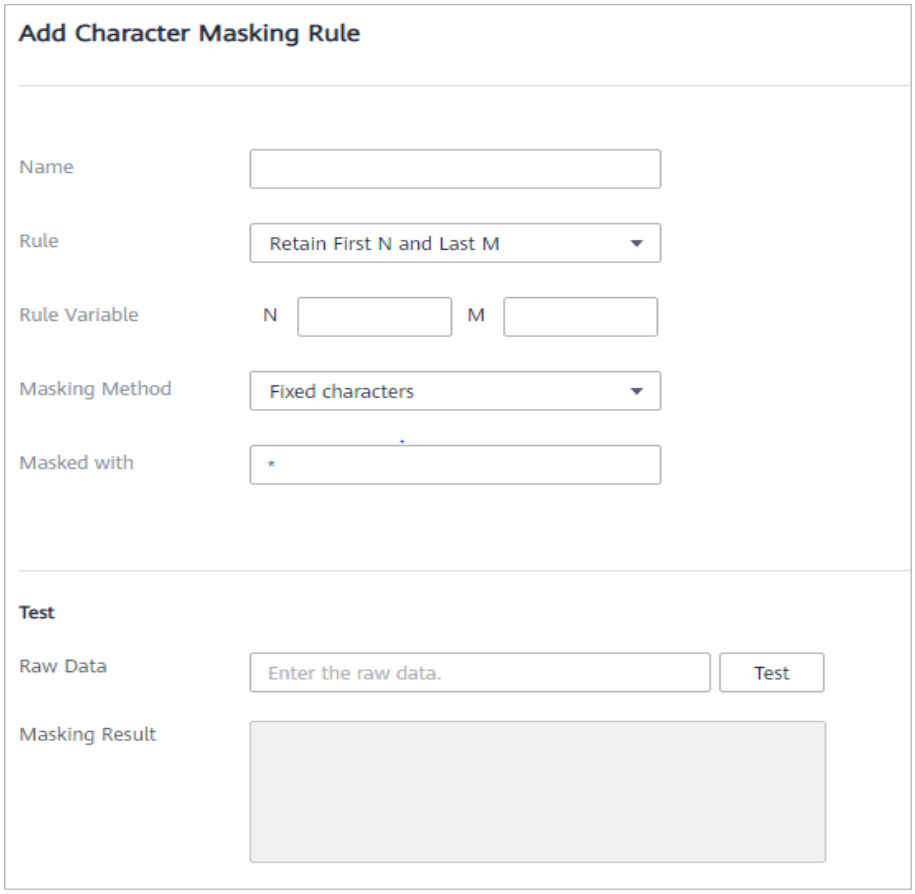
Step 2 Click the **Character Masking** tab.

Figure 6-3 Character masking method



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

Figure 6-4 Adding a character masking rule



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 customized masking rule, click **Delete** in the **Operation** column of the rule list.
- All rules can be edited. In the **Operation** column of the rule list, click **Edit** to modify a rule.

----End

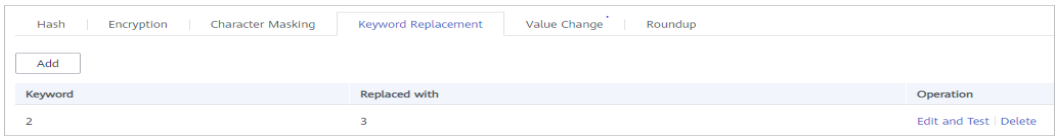
Keyword Replacement

Replace the matched keyword with customized characters. For example, if the original characters are a**bcde**fg**bcde**fgkjkoij, the **keyword** is **bcde**. Replace the preset value **12** with the keyword, and the masking result is **a12fg12fgkjkoij**.

Step 1 Go to the **Masking Rule** page by following operations provided in **Procedure**.

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

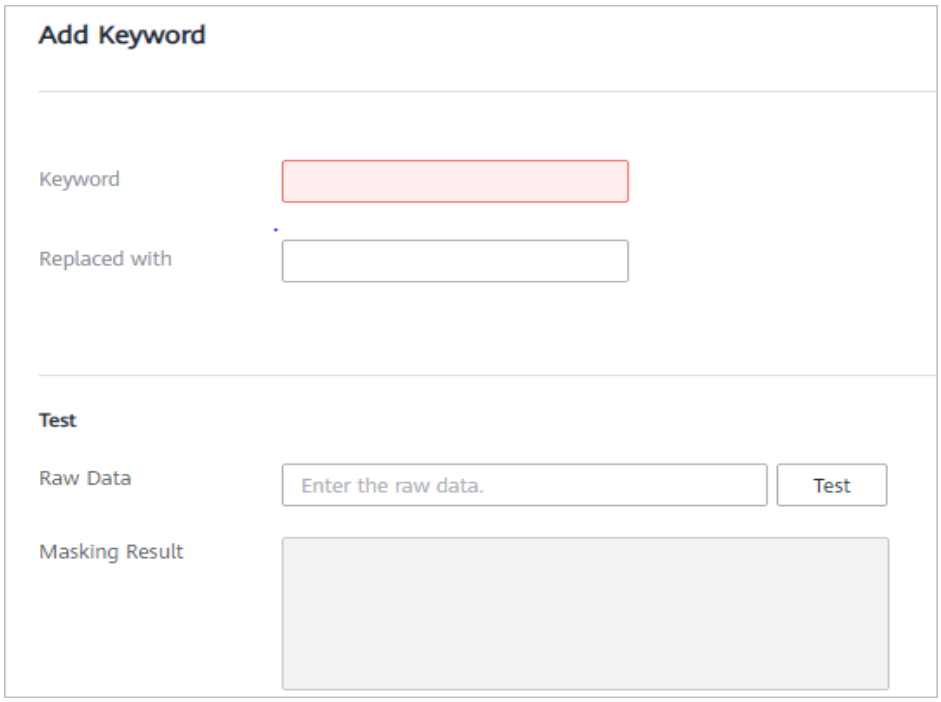
Figure 6-5 Keyword replacement method



Step 3 Set the keyword to be replaced and the characters to be replaced with.

After that, the keywords matched in the raw data will be replaced with the configured replacement characters.

Figure 6-6 Adding a keyword



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**.

- If you want to modify a configured masking rule, click **Edit and Test** in the **Operation**.
- If you want to delete a configured masking rule, click **Delete** in the **Operation** column.

----End

Value Change

DSC has the following two built-in data masking algorithms:

- **Masking Using the Null Value**: Set fields 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.

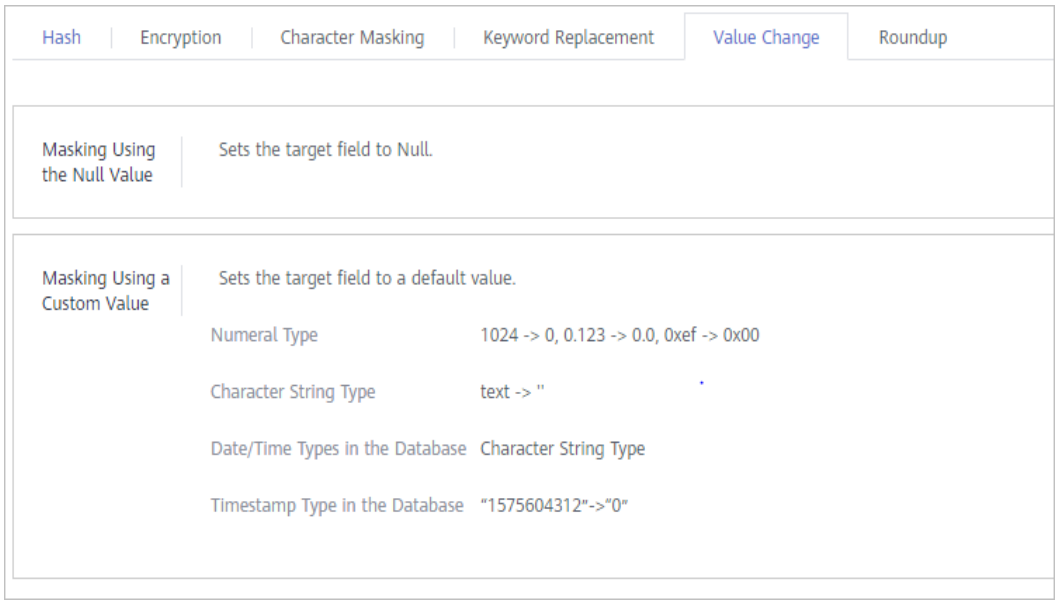
- **Masking Using a Custom Value**: Set the specified field to an empty value. Specifically, a character field is left blank, a numeric field is set to **0**, a date field is set to **1970**, and time field is set to **00:00**.

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

Step 1 Go to the **Masking Rule** page by following operations provided in **Procedure**.

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

Figure 6-7 Accessing the Value Change tab page



----End

Roundup

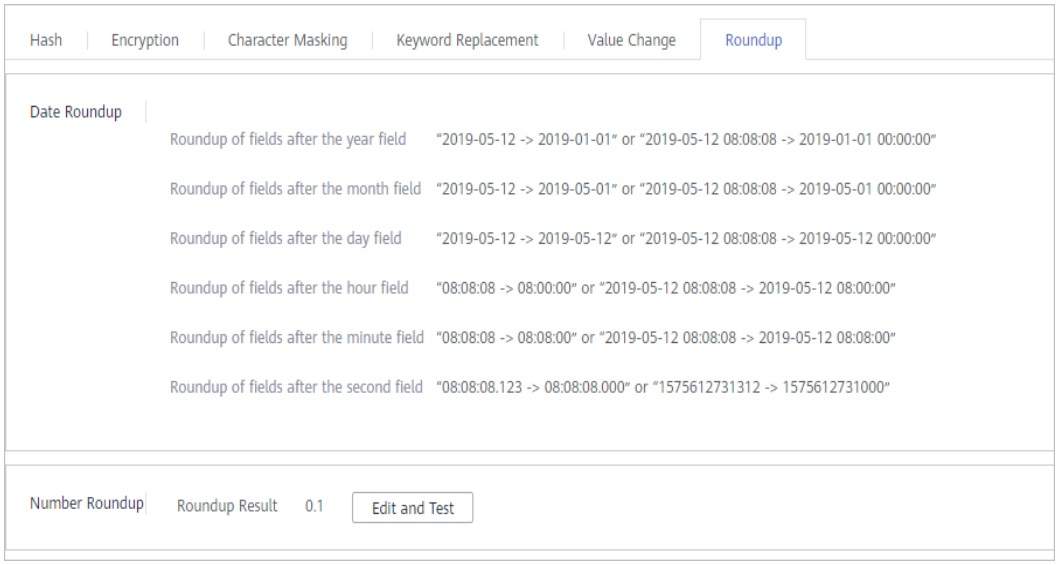
Step 1 Go to the **Masking Rule** page by following operations provided in **Procedure**.

Step 2 Click **Round**.

DSC has the following two built-in data masking algorithms:

- **Date Roundup**: Used for time-related fields such as **timestamp**, **time**, **data**, and **datatime** in RDS.
- **Number Roundup**: Used for value types fields such as **double**, **float**, **int**, and **long**. After data masking, the original field type remains unchanged.

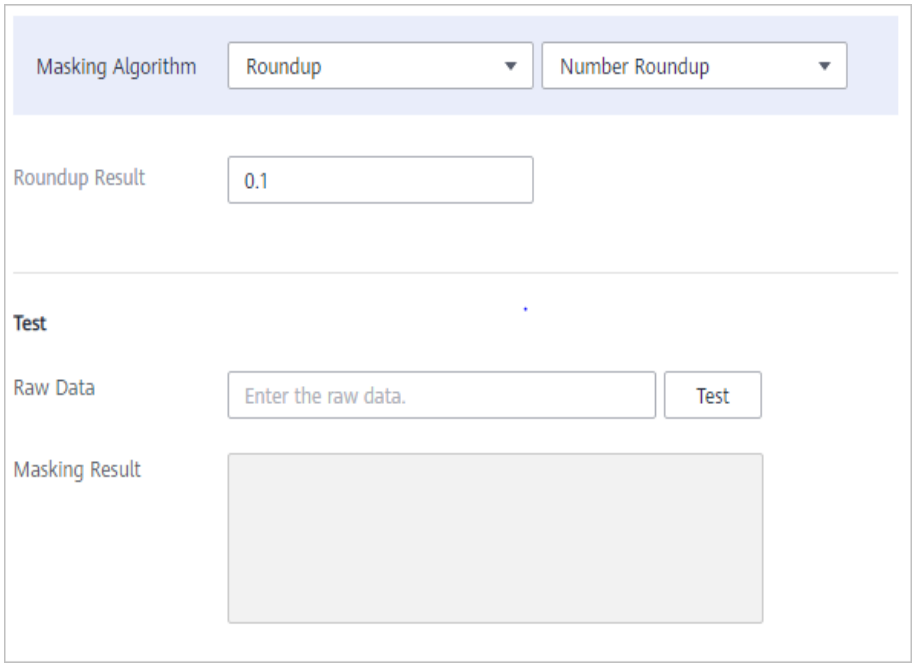
Figure 6-8 Roundup masking algorithms



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

Masking Result: Rounds a given value down towards the closest multiple of the integer. For example, if the given value is set to **5** and the raw data is **14**, the closest multiple of **5** that are close to **14** is rounded down to **10**. That is, the masking result is **10**.

Figure 6-9 Number roundup



Step 4 Enter the raw data, click **Test**.

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

----End

6.3 Static Data Masking

6.3.1 Creating a Data Masking Task

6.3.1.1 Creating a Database Data Masking Task

Create a data masking task for a database to mask sensitive information identified in the database.

Prerequisites

- DSC has been allowed to access the database assets.
- Database assets have been added.
- Sensitive data has been identified. For details, see **Creating a Task**.

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** > **Data Security Center**.

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

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

Step 6 Click **Create Task** and configure required parameters. **Table 6-2** describes the parameters.

Figure 6-10 Configuring a data masking task

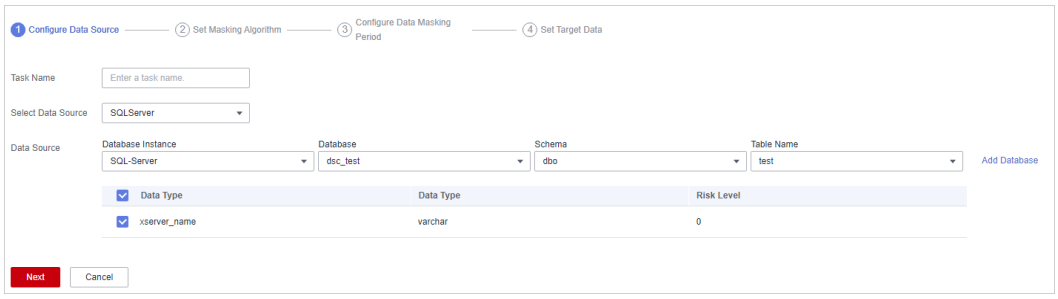
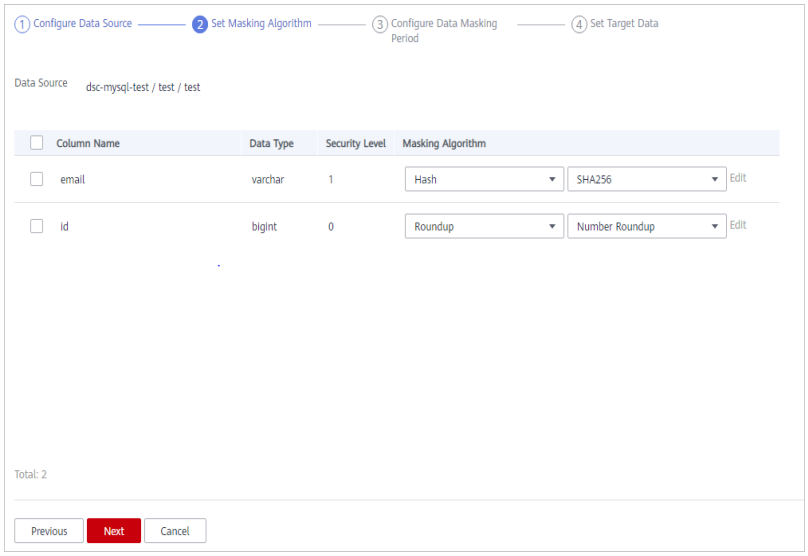


Table 6-2 Parameter description

Parameter	Description
Task Name	You can customize the name of a masking rule. The rule name must meet the following requirements: ● Contain 1 to 255 characters. ● Consist of letters, digits, underscores (_), and hyphens (-).
Select Data Source	Select a data source. Value options are **SQLServer**, **MySQL**, or **PostgreSQL**.
Data Source **NOTE** If no cloud databases are available, click **Add Database** to add cloud database assets. For details, see **Adding a Database**.	**Database Instance**: Select the database instance where the data to be anonymized is located.
	Database: Select the name of the database where the data to be anonymized is located.
	Schema: This parameter is displayed only when **SQLServer** or **PostgreSQL** is selected for **Data Source**.
	Table Name: Select the name of the database table where the data to be anonymized is located.
	Data Type: If you select the check box, data in this column is copied to the target database. The target **Data Type** and **Risk Level** of the data are also displayed.

Step 7 Click **Next**.

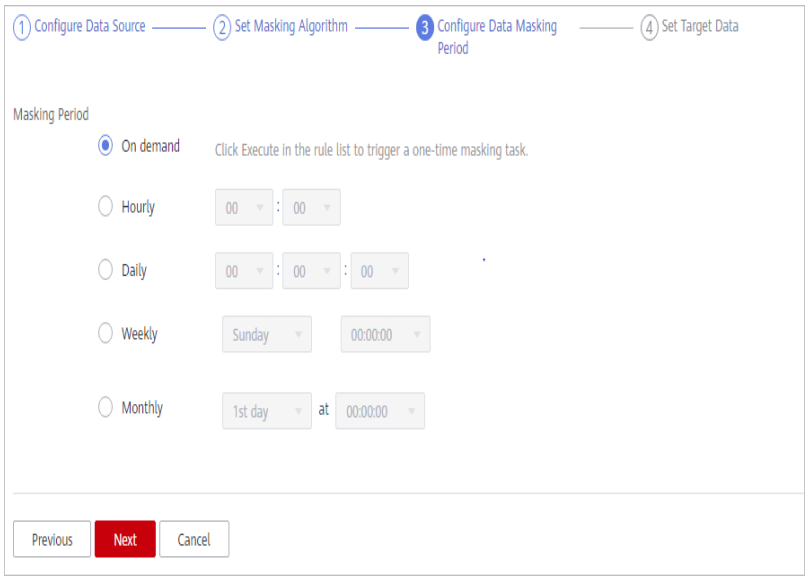
Figure 6-11 Configuring a masking algorithm



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

Step 8 Click **Next**.

Figure 6-12 Configuring data masking period



Select and set the execution period of a masking task.

- **Manual**: Manually enable a masking task and execute it based on masking rules.
- **Hourly**: Execute a data masking task every several hours.

  Example: If the masking task needs to be executed every two hours, set this parameter to **02:00**.
- **Daily**: Execute a data masking task at a specified time every day.

  Example: If the masking task needs to be executed at 12:00 every day, set this parameter to **12:00:00**.
- **Weekly**: Execute a data masking task at a specified time every week.

  Example: If the masking task needs to be executed at 12:00 every Monday, set this parameter to 12:00:00 every Monday.
- **Monthly**: Execute a data masking task at a specified time on a specified day every month.

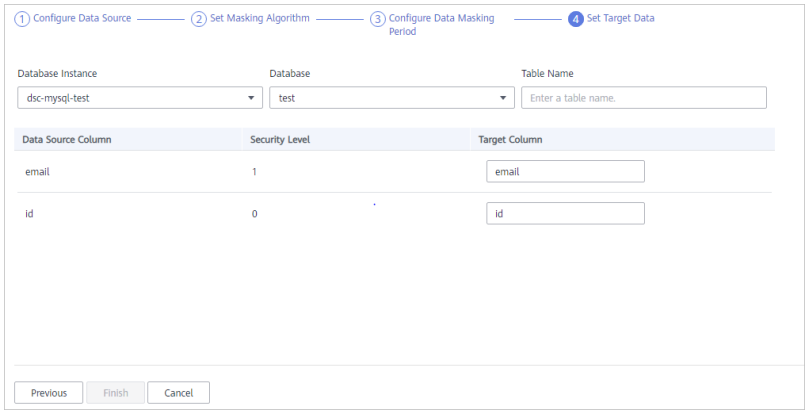
  Example: If the masking task needs to be executed at 12:00 on the 12th day of each month, set this parameter to 12:00:00 12th day of every month.

  NOTE

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

Step 9 Click **Next**.

Figure 6-13 Configuring a target data type



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**.

----End

Follow-up Procedure

After a database data masking task is created, execute the task. For details, see **Executing a Database Data Masking Task**.

6.3.1.2 Creating a Data Masking Task for Elasticsearch

Create a data masking task for Elasticsearch to mask sensitive information in tables or columns of Elasticsearch.

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

Prerequisites

- DSC has been allowed to access the database assets.
- You have added Elasticsearh assets. For details, see **Big Data Assets**.

- Sensitive data has been identified. For details, see **Creating a Task**.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Data Masking**. On the displayed page, click the **Elasticsearch Data Masking** tab.

Step 5 Click switch to to enable the data masking for Elasticsearch.

Step 6 Click **Create Task** and configure required parameters. **Table 6-3** describes the parameters.

Figure 6-14 Creating an Elasticsearch data masking task - Configuring data source

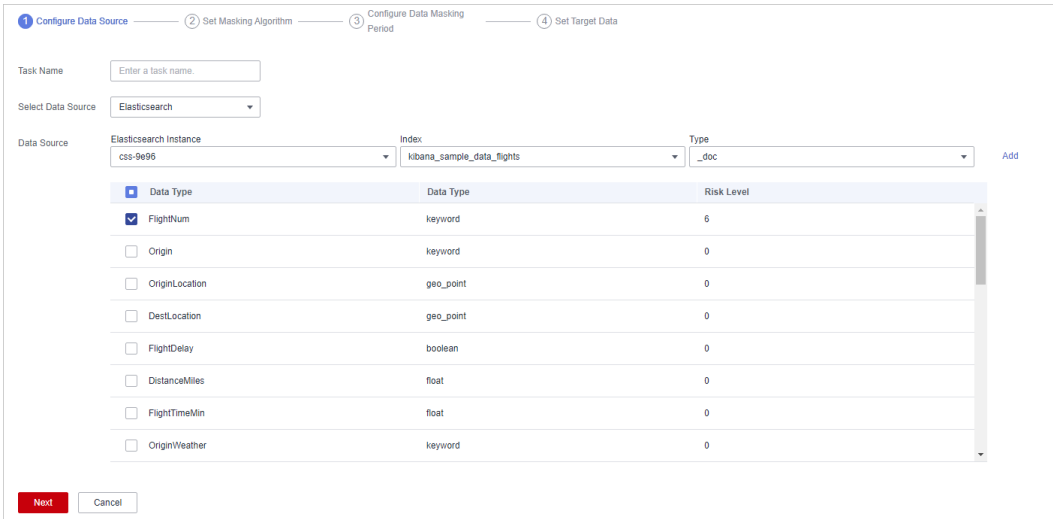


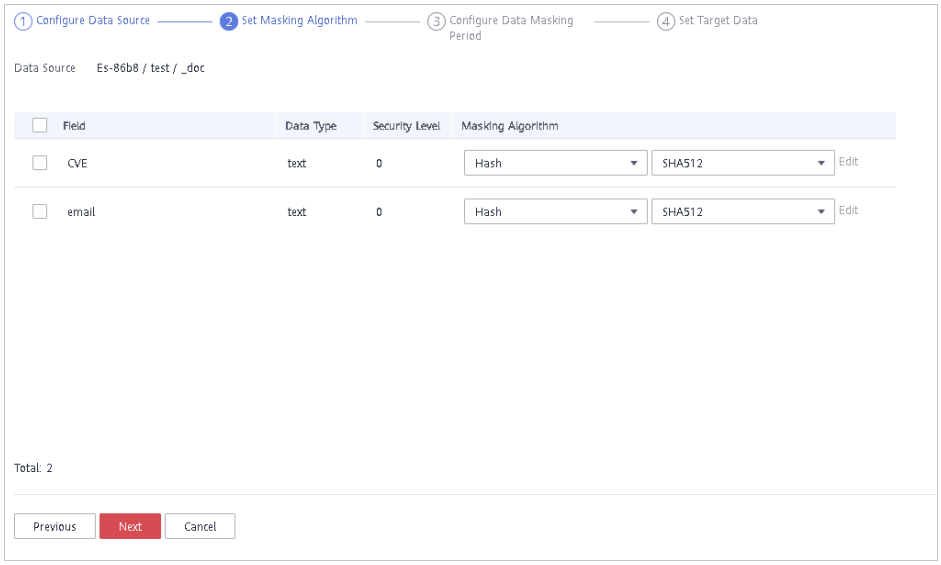
Table 6-3 Parameter description

Parameter	Description
Task Name	You can customize the name of a masking rule. The rule name must meet the following requirements: ● Contain 1 to 255 characters. ● Consist of letters, digits, underscores (_), and hyphens (-).
Select Data Source	Select a data source. Currently, only **Elasticsearch** is supported.

Parameter	Description
Data Source **NOTE** If no assets are available, Click **Add** to add a data source. For details, see **Adding a Big Data Source**.	**Elasticsearch**: Select the Elasticsearch instance where the data to be masked is located.
	Index: Select the index where the data to be masked is located.
	Type: Select the type of the data to be masked.
	Field: If you select the check box, data in this column is copied to the **Data Type** column. The target **Data Type** and **Risk Level** of the data are also displayed.

Step 7 Click **Next**.

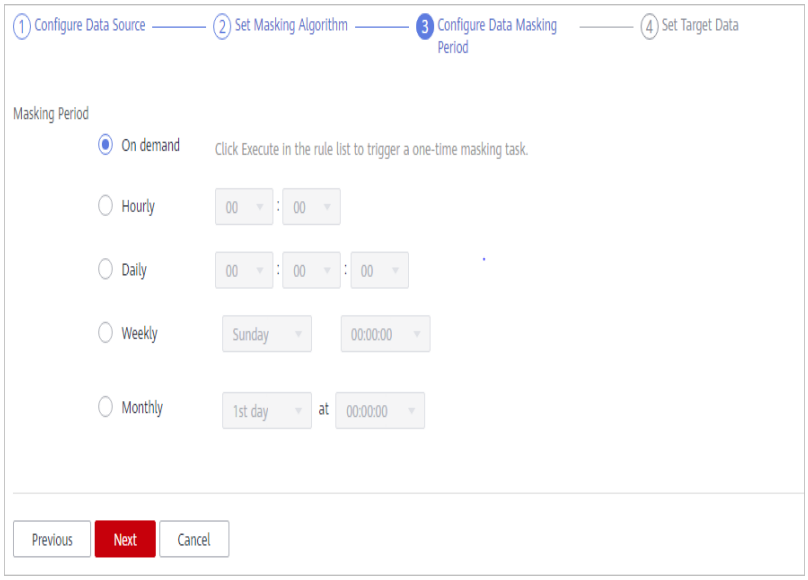
Figure 6-15 Creating an Elasticsearch data masking task - Setting a masking algorithm



1. Select the fields to be masked.
2. Select a data masking algorithm. For details about data masking algorithms, see **Configuring a Data Masking Rule**.

Step 8 Click **Next**.

Figure 6-16 Configuring data masking period



Select and set the execution period of a masking task.

- **Manual**: Manually enable a masking task and execute it based on masking rules.
- **Hourly**: Execute a data masking task every several hours.

  Example: If the masking task needs to be executed every two hours, set this parameter to **02:00**.
- **Daily**: Execute a data masking task at a specified time every day.

  Example: If the masking task needs to be executed at 12:00 every day, set this parameter to **12:00:00**.
- **Weekly**: Execute a data masking task at a specified time every week.

  Example: If the masking task needs to be executed at 12:00 every Monday, set this parameter to 12:00:00 every Monday.
- **Monthly**: Execute a data masking task at a specified time on a specified day every month.

  Example: If the masking task needs to be executed at 12:00 on the 12th day of each month, set this parameter to 12:00:00 12th day of every month.

  NOTE

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

Step 9 Click **Next**.

Figure 6-17 Creating an Elasticsearch data masking task - Setting the target data

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

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

   If the type that 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 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**.

----End

Follow-up Procedure

After the Elasticsearch data masking task is created, execute the task. For details, see **Executing an Elasticsearch Data Masking Task**.

6.3.1.3 Creating a Data Masking Task for MRS

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

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

Prerequisites

- DSC has been allowed to access the MRS assets.
- You have added MRS assets. For details, see **Adding MRS Assets**.
- Sensitive data has been identified. For details, see **Creating a Task**.

Procedure

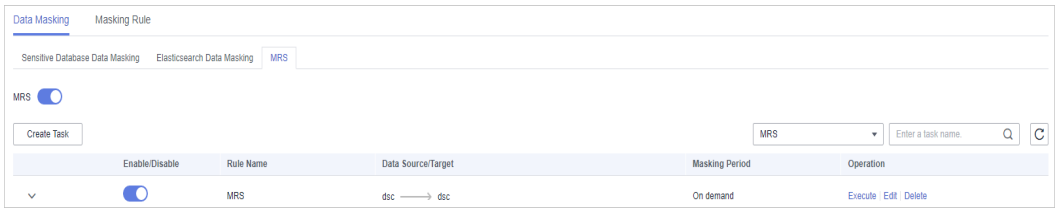
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Data Masking**. On the displayed page, click the **MRS Data Masking** tab.

Figure 6-18 MRS data masking



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

Step 6 Click **Create Task** and configure required parameters. **Table 6-4** describes the parameters.

Figure 6-19 Configuring the data source

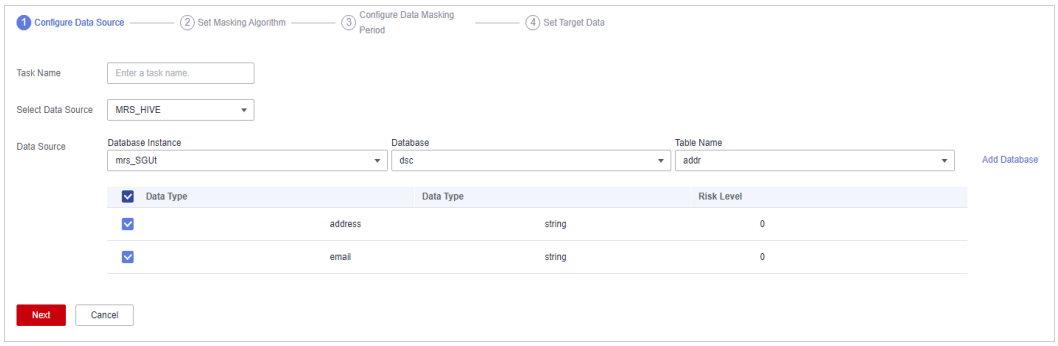


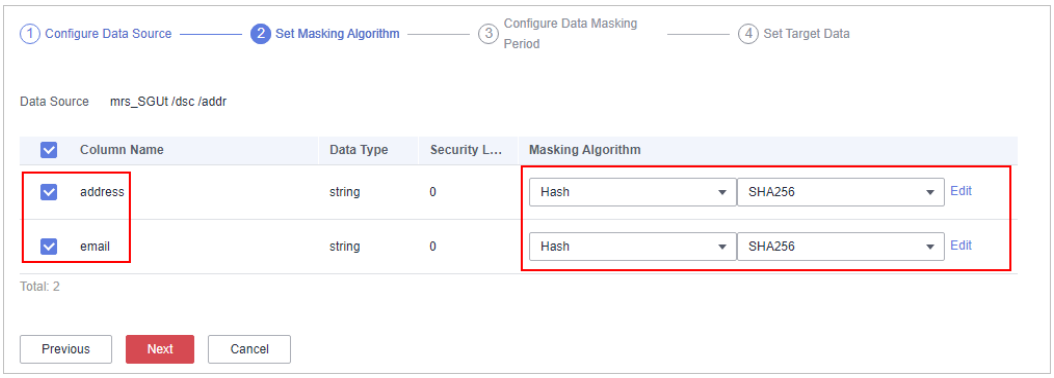
Table 6-4 Parameter description

Parameter	Description
Task Name	You can customize the name of a data masking task. The task name must meet the following requirements: ● Contain 1 to 255 characters. ● Consist of letters, digits, underscores (_), and hyphens (-).
Select Data Source	Select a data source. Only **MRS_HIVE** is available.

Parameter	Description
Data Source **NOTE** If no data is available, click **Add Database** to add database assets. For details, see **Adding MRS Assets**.	**Database Instance**: Select the database instance where the data you want to mask is located.
	Database: Select the name of the database where the data you want to mask is located.
	Table Name: Select the name of the database table where the data you want to mask is located.
	Data Type: If you select the check box, data in this column is copied to the target database. The target **Data Type** and **Risk Level** of the data are also displayed.

Step 7 Click **Next**.

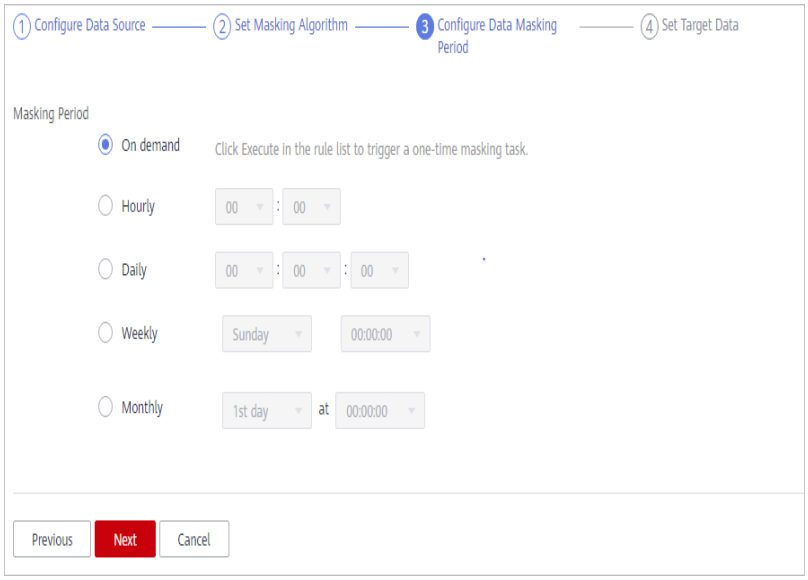
Figure 6-20 Setting a masking algorithm



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

Step 8 Click **Next**.

Figure 6-21 Configuring data masking period



Select and set the execution period of a masking task.

- **Manual**: Manually enable a masking task and execute it based on masking rules.
- **Hourly**: Execute a data masking task every several hours.

  Example: If the masking task needs to be executed every two hours, set this parameter to **02:00**.
- **Daily**: Execute a data masking task at a specified time every day.

  Example: If the masking task needs to be executed at 12:00 every day, set this parameter to **12:00:00**.
- **Weekly**: Execute a data masking task at a specified time every week.

  Example: If the masking task needs to be executed at 12:00 every Monday, set this parameter to 12:00:00 every Monday.
- **Monthly**: Execute a data masking task at a specified time on a specified day every month.

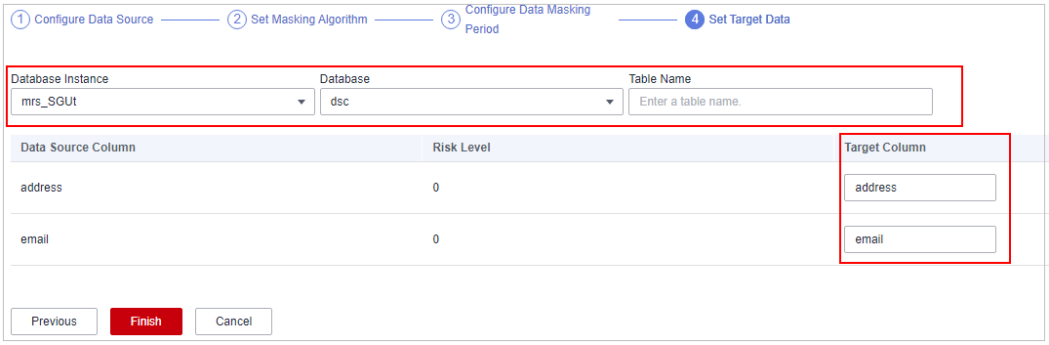
  Example: If the masking task needs to be executed at 12:00 on the 12th day of each month, set this parameter to 12:00:00 12th day of every month.

  NOTE

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

Step 9 Click **Next**.

Figure 6-22 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**.

----End

6.3.2 Executing a Data Masking Task

6.3.2.1 Executing a Database Data Masking Task

After a database data masking task is created, the sensitive information in tables or columns of a specified database can be masked.

This section describes how to execute a database data masking task.

Prerequisites

A data masking task has been created.

Procedure

Step 1 Log in to the management console.

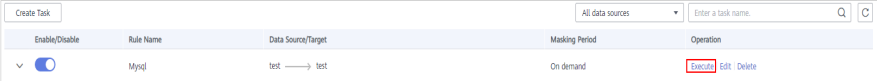
Step 2 Click in the upper left corner of the management console and select a region or project.

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

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

Step 5 On the **Database Data Masking** tab page, locate the row that contains the task to be executed and click **Execute** in the **Operation** column.

Figure 6-23 Executing a database data masking task



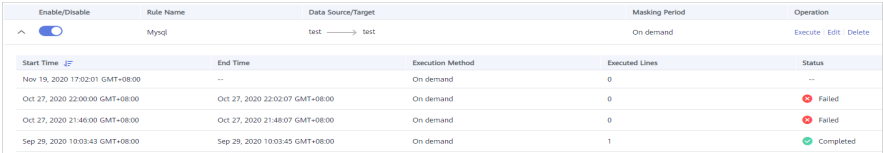
The data masking task is executed as configured.

Step 6 Click in front of a data masking task to view the task status.

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 6-24 Data masking task statuses



----End

6.3.2.2 Executing an Elasticsearch Data Masking Task

After an Elasticsearch data masking task is created, sensitive information in tables or columns of a specified Elasticsearch data source will be masked.

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

Prerequisites

An Elasticsearch data masking task has been 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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Data Masking**. On the displayed page, click the **Elasticsearch Data Masking** tab.

Step 5 On the **Elasticsearch Data Masking** tab page, locate the row that contains the task to be executed and click **Execute** in the **Operation** column.

Figure 6-25 Executing an Elasticsearch data masking task

The data masking task is executed as configured.

NOTE

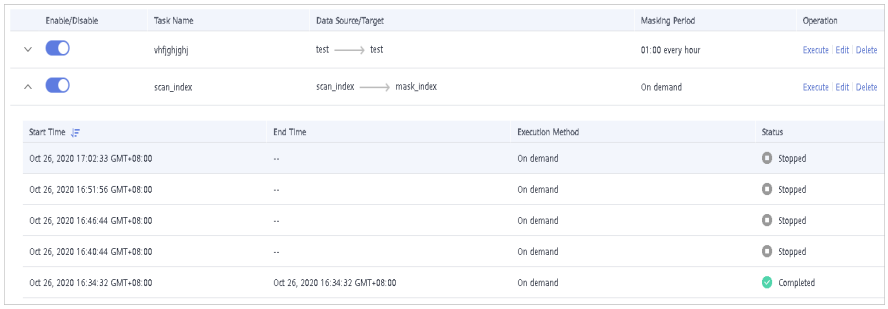
In the **Enable/Disable** column, If is displayed, the task is disabled, you are not allowed to click **Execute**.

Step 6 Click in front of a data masking task to view the task status.

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 6-26 Elasticsearch data masking task statuses



----End

6.3.2.3 Executing an MRS Data Masking Task

After an MRS data masking task is created, sensitive information in tables or columns of a specified MRS data source will be masked.

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

Prerequisites

An MRS data masking task has been created.

Procedures

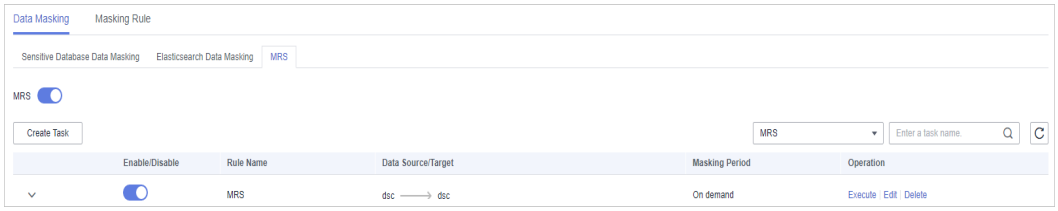
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Data Masking**. On the displayed page, click the **MRS Data Masking** tab.

Figure 6-27 MRS data masking



Step 5 On the **MRS Data Masking** tab page, locate the row that contains the task to be executed and click **Execute** in the **Operation** column.

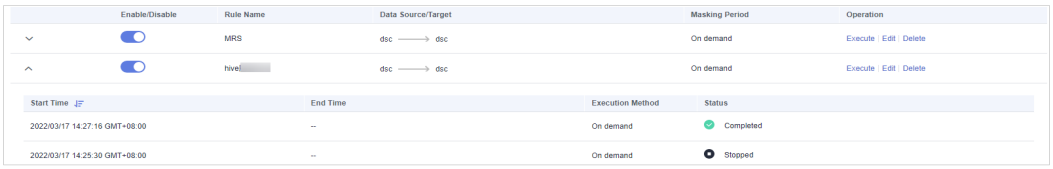
The data masking task is executed as configured.

Step 6 Click in front of a data masking task to view the task status.

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 6-28 Task status



----End

6.3.3 Managing a Data Masking Task

6.3.3.1 Managing a Database Data Masking Task

This section describes how to view, edit, and delete a database data masking task.

Prerequisites

A data masking task has been created.

Viewing a Database 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** > **Data Security Center**.

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

Step 5 In the task list, view the task details. **Table 6-5** describes the parameters.

Figure 6-29 Viewing a database data masking task

NOTE

Enter a task name or a keyword, and click or press **Enter** to search for the data masking task.

Table 6-5 Task parameters

Parameter	Description
Enable/Disable	Whether a data masking task is enabled or disabled. • : Enabled • : Disabled
Task Name	Name of a data masking task
Data Source/Target	Data source and target of a database data masking task

Parameter	Description
Masking Period	Execution period of a database masking task, which can be set as follows: • **Manual**: Manually enable a masking task and execute it based on masking rules. • **Hourly**: Execute a masking task every several hours based on masking rules. • **Daily**: Execute a masking task at a fixed time every day based on masking rules. • **Weekly**: Execute a masking task at a fixed time every week based on masking rules. • **Monthly**: Execute a masking task at a fixed time every month based on masking rules.
Operation	In the **Operation** column, you can execute, edit, or delete a masking task.

----End

Editing 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** > **Data Security Center**.

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

Step 5 In the database masking task list, locate the row that contains the masking task to be edited, and click **Edit** in the **Operation** column.

Figure 6-30 Editing a database masking task

Step 6 Configure the data source. **Table 6-6** describes the parameters.

Figure 6-31 Configuring a data masking task

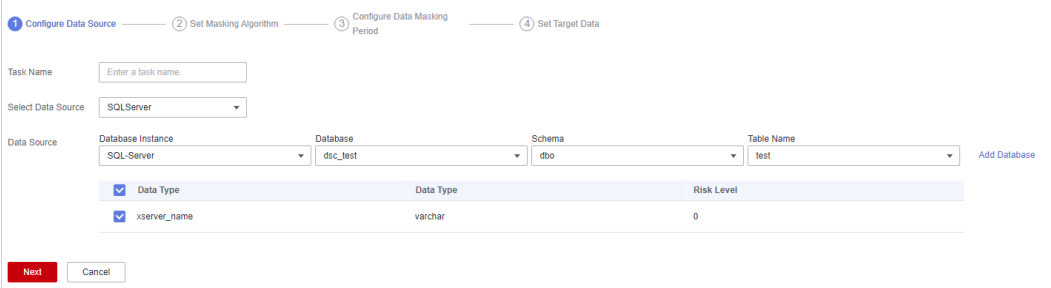
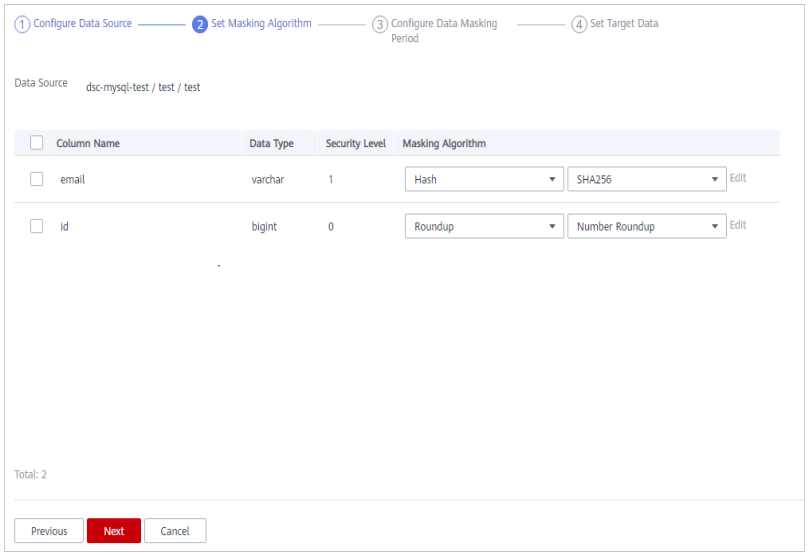


Table 6-6 Parameter description

Parameter	Description
Task Name	You can customize the name of a masking rule. The rule name must meet the following requirements: ● Contain 1 to 255 characters. ● Consist of letters, digits, underscores (_), and hyphens (-).
Select Data Source	Select a data source. Value options are **SQLServer**, **MySQL**, or **PostgreSQL**.
Data Source **NOTE** If no cloud databases are available, click **Add Database** to add cloud database assets. For details, see **Adding a Database**.	**Database Instance**: Select the database instance where the data to be anonymized is located.
	Database: Select the name of the database where the data to be anonymized is located.
	Schema: This parameter is displayed only when **SQLServer** or **PostgreSQL** is selected for **Data Source**.
	Table Name: Select the name of the database table where the data to be anonymized is located.
	Data Type: If you select the check box, data in this column is copied to the target database. The target **Data Type** and **Risk Level** of the data are also displayed.

Step 7 Click **Next**.

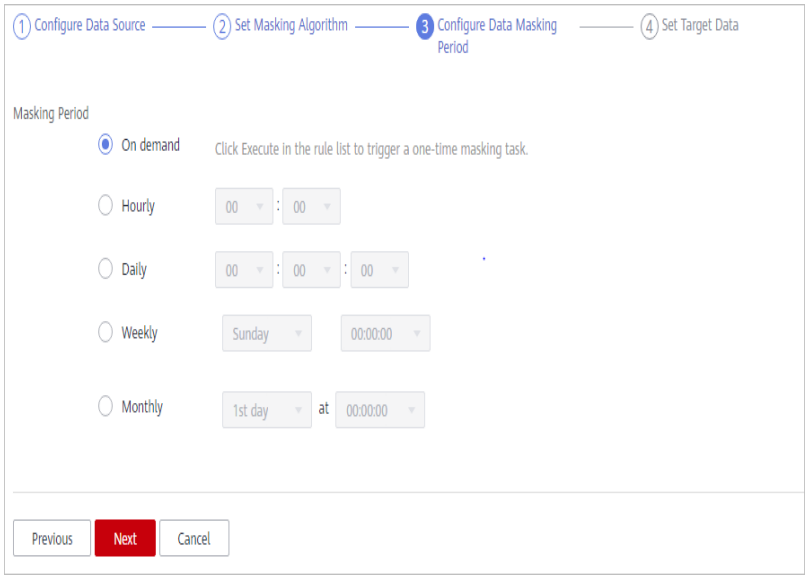
Figure 6-32 Configuring a masking algorithm



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

Step 8 Click **Next**.

Figure 6-33 Configuring data masking period



Select and set the execution period of a masking task.

- **Manual**: Manually enable a masking task and execute it based on masking rules.
- **Hourly**: Execute a data masking task every several hours.

  Example: If the masking task needs to be executed every two hours, set this parameter to **02:00**.

- **Daily**: Execute a data masking task at a specified time every day.

  Example: If the masking task needs to be executed at 12:00 every day, set this parameter to **12:00:00**.
- **Weekly**: Execute a data masking task at a specified time every week.

  Example: If the masking task needs to be executed at 12:00 every Monday, set this parameter to 12:00:00 every Monday.
- **Monthly**: Execute a data masking task at a specified time on a specified day every month.

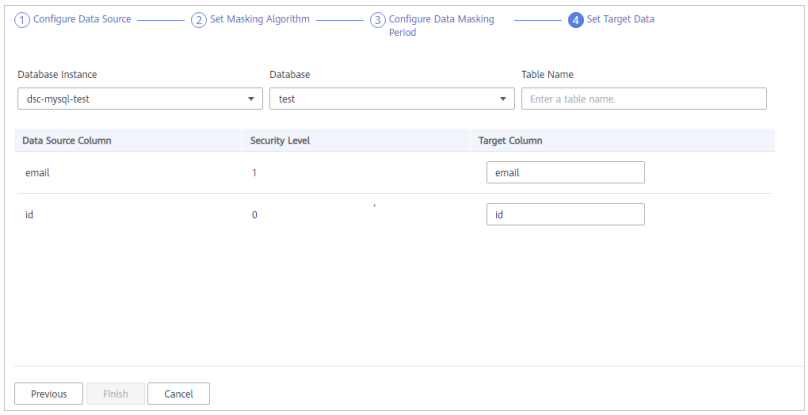
  Example: If the masking task needs to be executed at 12:00 on the 12th day of each month, set this parameter to 12:00:00 12th day of every month.

  NOTE

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

Step 9 Click **Next**.

Figure 6-34 Configuring a target data type



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**.

After a database data masking task is created, execute the task. For details, see **Executing a Database Data Masking Task**.

----End

Deleting 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** > **Data Security Center**.

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

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

Figure 6-35 Deleting a database masking task

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

----End

6.3.3.2 Managing an Elasticsearch Data Masking Task

Scenario

This section describes how to view, edit, and delete an Elasticsearch data masking task.

Prerequisites

An Elasticsearch data masking task has been created.

Viewing 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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Data Masking**. On the displayed page, click the **Elasticsearch Data Masking** tab.

Step 5 In the masking task list, view the task details. For parameter details, see **Table 6-7**.

Figure 6-36 Viewing an Elasticsearch data masking task

NOTE

Enter a task name or a keyword, and click or press **Enter** to search for the data masking task.

Table 6-7 Task parameters

Parameter	Description
Enable/Disable	Whether a data masking task is enabled or disabled. • : Enabled • : Disabled
Task Name	Name of a data masking task
Data Source/Target	Data source and target of a database data masking task
Masking Period	Execution period of a database masking task, which can be set as follows: • **Manual**: Manually enable a masking task and execute it based on masking rules. • **Hourly**: Execute a masking task every several hours based on masking rules. • **Daily**: Execute a masking task at a fixed time every day based on masking rules. • **Weekly**: Execute a masking task at a fixed time every week based on masking rules. • **Monthly**: Execute a masking task at a fixed time every month based on masking rules.
Operation	In the **Operation** column, you can execute, edit, or delete a masking task.

----End

Editing 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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Data Masking**. On the displayed page, click the **Elasticsearch Data Masking** tab.

Step 5 In the Elasticsearch data masking task list, locate the row that contains the masking task to be edited, and click **Edit** in the **Operation** column.

Figure 6-37 Editing an Elasticsearch data masking task

Step 6 Configure the data source. **Table 6-8** describes the parameters.

Figure 6-38 Creating an Elasticsearch data masking task - Configuring data source

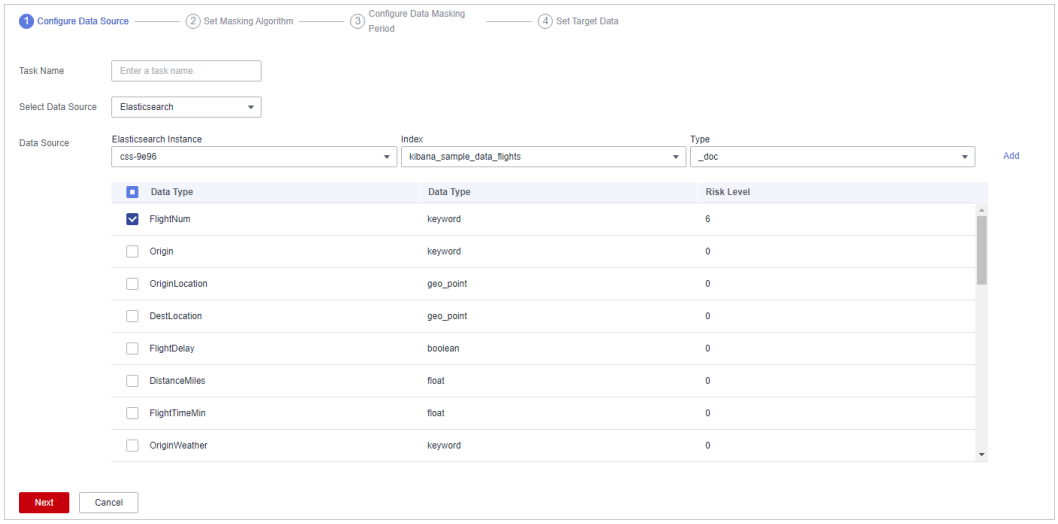


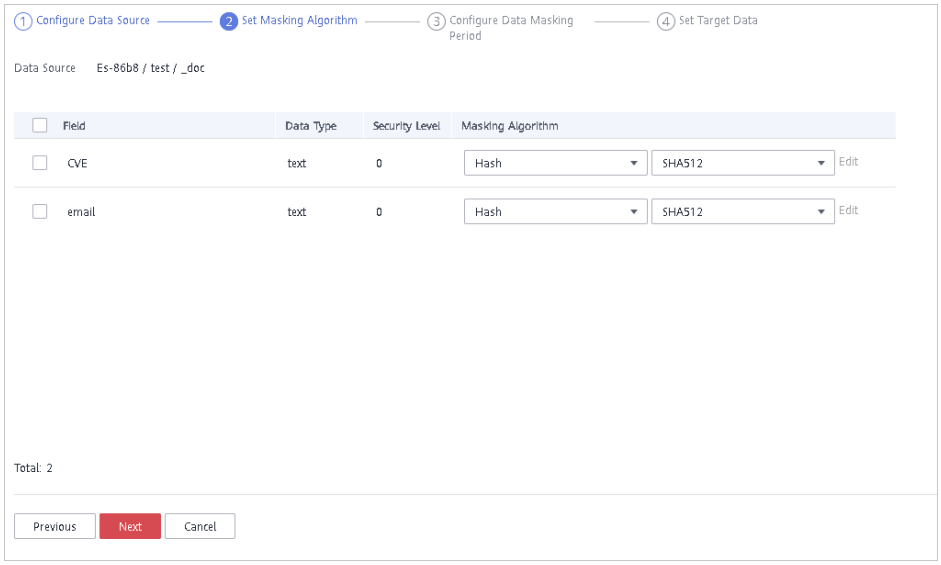
Table 6-8 Parameter description

Parameter	Description
Task Name	You can customize the name of a masking rule. The rule name must meet the following requirements: ● Contain 1 to 255 characters. ● Consist of letters, digits, underscores (_), and hyphens (-).
Select Data Source	Select a data source. Currently, only **Elasticsearch** is supported.

Parameter	Description
Data Source **NOTE** If no assets are available, Click **Add** to add a data source. For details, see **Adding a Big Data Source**.	**Elasticsearch**: Select the Elasticsearch instance where the data to be masked is located.
	Index: Select the index where the data to be masked is located.
	Type: Select the type of the data to be masked.
	Field: If you select the check box, data in this column is copied to the **Data Type** column. The target **Data Type** and **Risk Level** of the data are also displayed.

Step 7 Click **Next**.

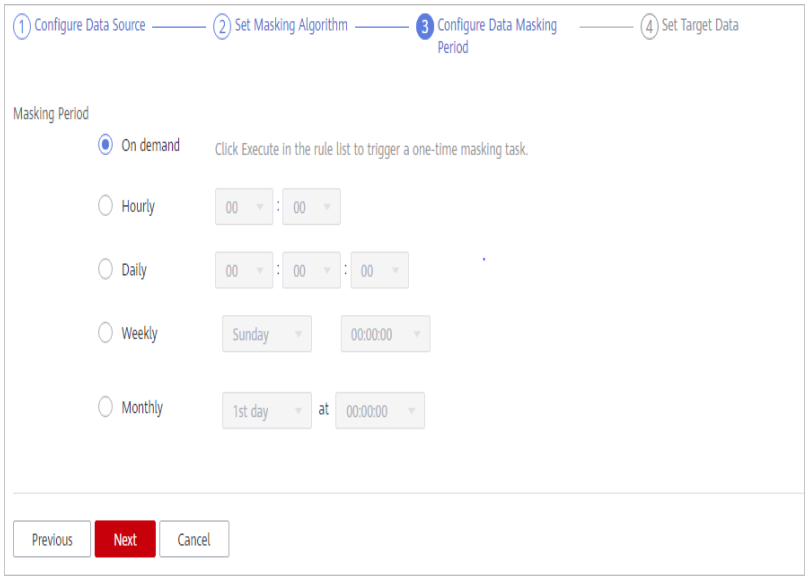
Figure 6-39 Creating an Elasticsearch data masking task - Setting a masking algorithm



1. Select the fields to be masked.
2. Select a data masking algorithm. For details about data masking algorithms, see **Configuring a Data Masking Rule**.

Step 8 Click **Next**.

Figure 6-40 Configuring data masking period



Select and set the execution period of a masking task.

- **Manual**: Manually enable a masking task and execute it based on masking rules.
- **Hourly**: Execute a data masking task every several hours.

  Example: If the masking task needs to be executed every two hours, set this parameter to **02:00**.
- **Daily**: Execute a data masking task at a specified time every day.

  Example: If the masking task needs to be executed at 12:00 every day, set this parameter to **12:00:00**.
- **Weekly**: Execute a data masking task at a specified time every week.

  Example: If the masking task needs to be executed at 12:00 every Monday, set this parameter to 12:00:00 every Monday.
- **Monthly**: Execute a data masking task at a specified time on a specified day every month.

  Example: If the masking task needs to be executed at 12:00 on the 12th day of each month, set this parameter to 12:00:00 12th day of every month.

  NOTE

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

Step 9 Click **Next**.

Figure 6-41 Creating an Elasticsearch data masking task - Setting the target data

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

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

   If the type that 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 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**.

After the Elasticsearch data masking task is created, execute the task. For details, see **Executing an Elasticsearch Data Masking Task**.

----End

Deleting an Elasticsearch Data Masking Task

Step 1 Log in to the management console.

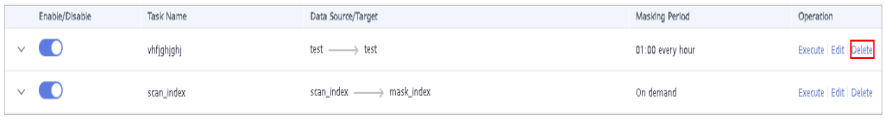
Step 2 Click in the upper left corner of the management console and select a region or project.

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

Step 4 In the navigation pane, choose **Data Masking**. On the displayed page, click the **Elasticsearch Data Masking** tab.

Step 5 In the Elasticsearch data masking task list, locate the row that contains the masking task to be deleted, and click **Delete** in the **Operation** column.

Figure 6-42 Deleting an Elasticsearch data masking task



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

----End

6.3.3.3 Managing an MRS Data Masking Task

This section describes how to view, edit, and delete an MRS data masking task.

Prerequisites

An MRS data masking task has been created.

Viewing an MRS Data Masking Task

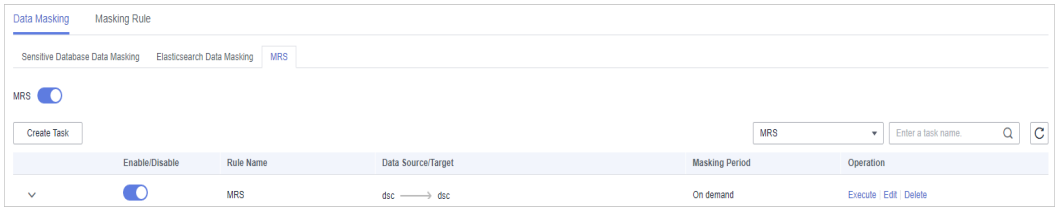
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Data Masking**. On the displayed page, click the **MRS Data Masking** tab.

Figure 6-43 MRS data masking



Step 5 In the data masking task list, view the task details. For parameter details, see **Table 6-9**.

NOTE

Enter a keyword, and click or press **Enter** to search for the data masking task.

Table 6-9 Task parameters

Parameter	Description
Enable/Disable	Whether a data masking task is enabled or disabled. • : Enabled • : Disabled
Rule Name	Name of a data masking task
Data Source/Target	Data source and target of a data masking task
Masking Period	Execution period of a data masking task, which can be set as follows: • **Manual**: Manually enable a masking task and execute it based on masking rules. • **Hourly**: Execute a masking task every several hours based on masking rules. • **Daily**: Execute a masking task at a fixed time every day based on masking rules. • **Weekly**: Execute a masking task at a fixed time every week based on masking rules. • **Monthly**: Execute a masking task at a fixed time every month based on masking rules.
Operation	Execute, edit, or delete a masking task.

----End

Editing an MRS Data Masking Task

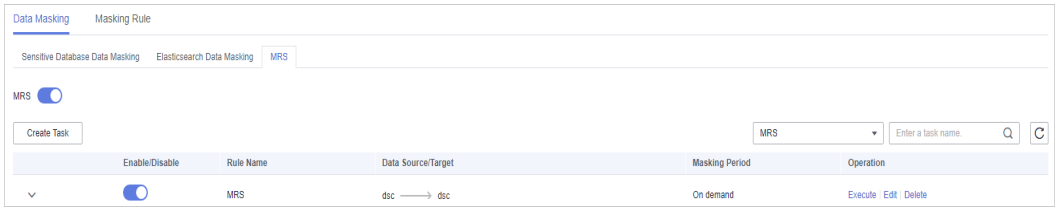
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Data Masking**. On the displayed page, click the **MRS Data Masking** tab.

Figure 6-44 MRS data masking



Step 5 In the MRS data masking task list, locate the row that contains the masking task you want to edit, and click **Edit** in the **Operation** column.

Step 6 Configure the data source. **Table 6-10** describes the parameters.

Figure 6-45 Configuring the data source

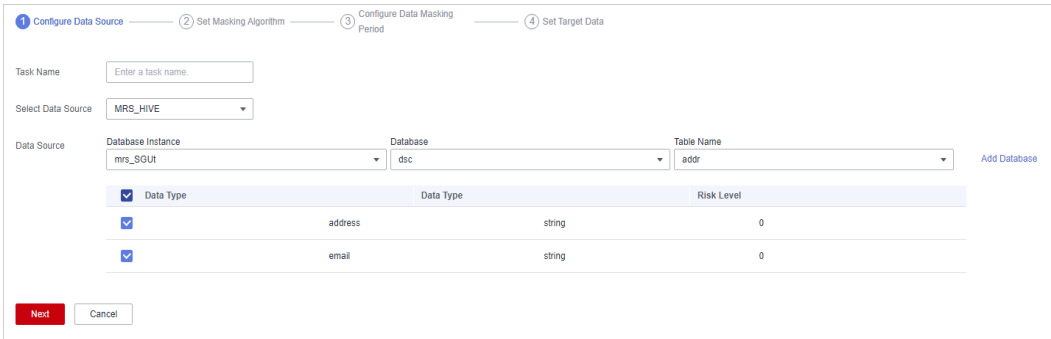
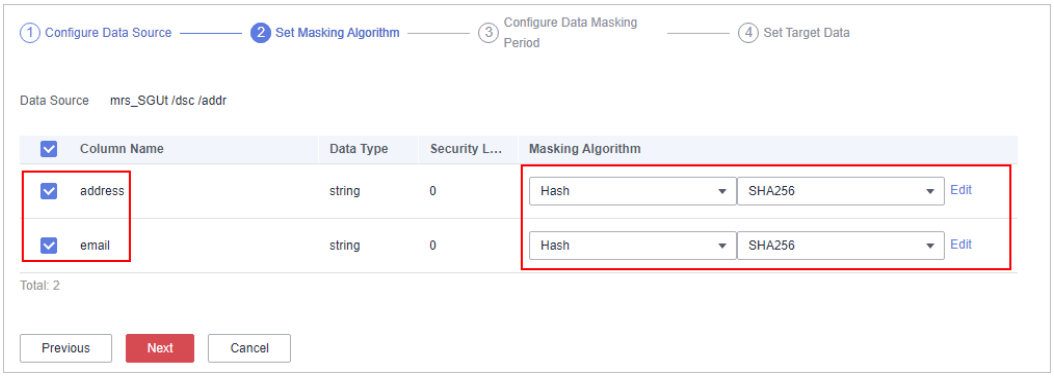


Table 6-10 Parameter description

Parameter	Description
Task Name	You can customize the name of a data masking task. The task name must meet the following requirements: ● Contain 1 to 255 characters. ● Consist of letters, digits, underscores (_), and hyphens (-).
Select Data Source	Select a data source. Only **MRS_HIVE** is available.
Data Source **NOTE** If no data is available, click **Add Database** to add database assets. For details, see **Adding MRS Assets**.	**Database Instance**: Select the database instance where the data you want to mask is located.
	Database: Select the name of the database where the data you want to mask is located.
	Table Name: Select the name of the database table where the data you want to mask is located.
	Data Type: If you select the check box, data in this column is copied to the target database. The target **Data Type** and **Risk Level** of the data are also displayed.

Step 7 Click **Next**.

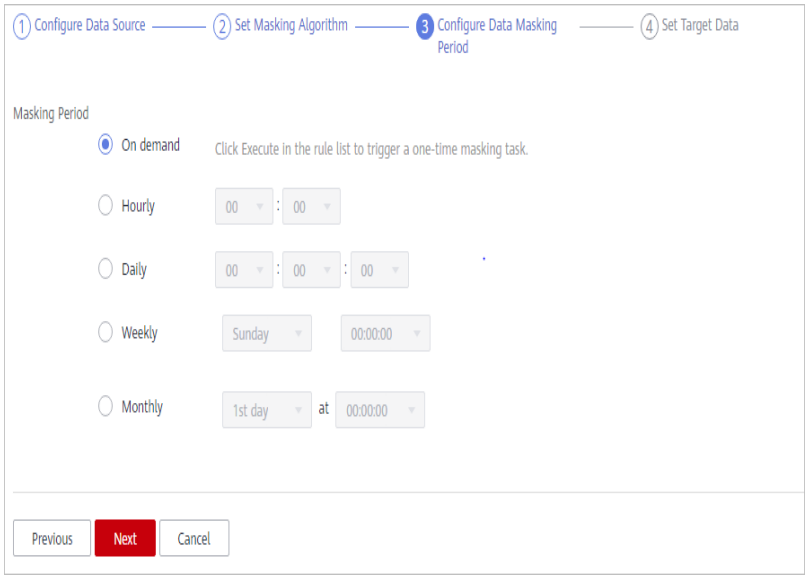
Figure 6-46 Setting a masking algorithm



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 6-47 Configuring data masking period



Select and set the execution period of a masking task.

- **Manual**: Manually enable a masking task and execute it based on masking rules.
- **Hourly**: Execute a data masking task every several hours.

  Example: If the masking task needs to be executed every two hours, set this parameter to **02:00**.
- **Daily**: Execute a data masking task at a specified time every day.

  Example: If the masking task needs to be executed at 12:00 every day, set this parameter to **12:00:00**.
- **Weekly**: Execute a data masking task at a specified time every week.

Example: If the masking task needs to be executed at 12:00 every Monday, set this parameter to 12:00:00 every Monday.

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

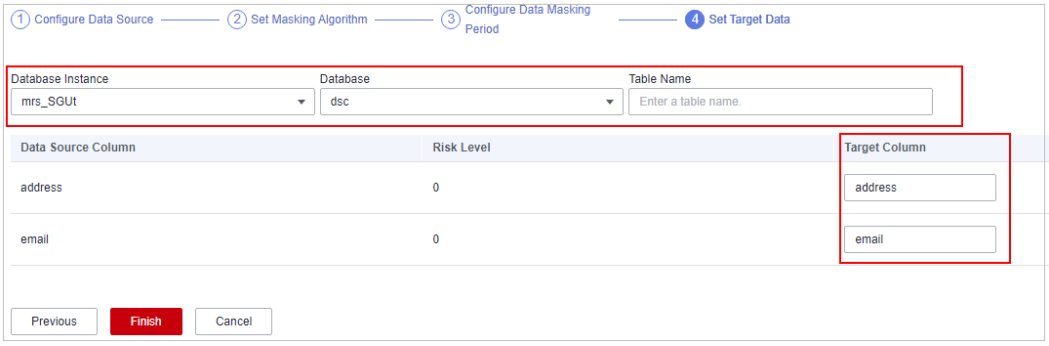
  Example: If the masking task needs to be executed at 12:00 on the 12th day of each month, set this parameter to 12:00:00 12th day of every month.

  NOTE

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

Step 9 Click **Next**.

Figure 6-48 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**.

----End

Deleting an MRS Data Masking Task

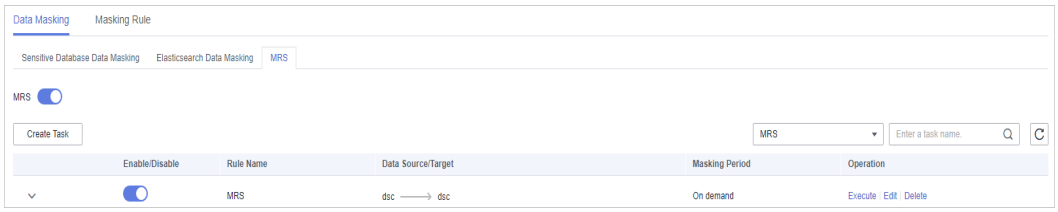
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Data Masking**. On the displayed page, click the **MRS Data Masking** tab.

Figure 6-49 MRS data masking



Step 5 In the MRS data masking task list, locate the row that contains the masking task you want to delete, and click **Delete** in the **Operation** column.

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

----End

7 Data Watermarking

7.1 Overview

You can use DSC to inject custom watermarks into your documents smaller than 50 MB, claiming the ownership.

Table 7-1 Files which watermarks can be injected into or extracted from

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

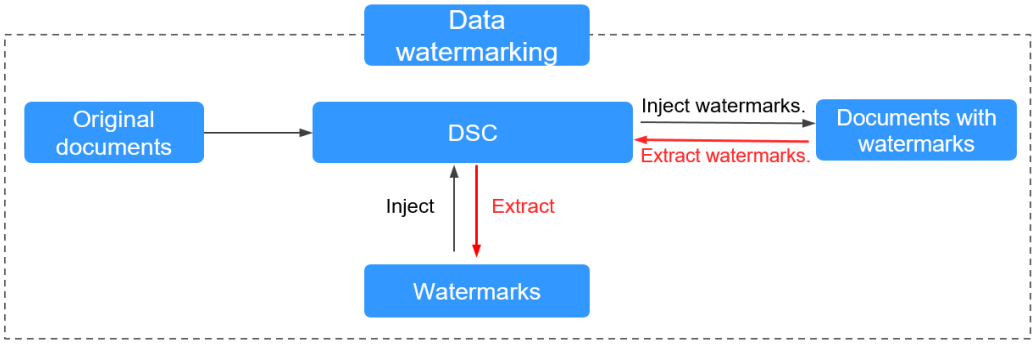
- **Visible and invisible watermarks**: You can inject visible or invisible watermarks into the data as needed to efficiently cope with data theft through image process tools, picture taking, or screenshots.
- **Detectable and tamper-proofing**: Watermarks injected into the data can be detected and will 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.

Constraints

The DSC console supports embedding and extracting watermarks only for PDF, PPT, Word, and Excel documents.

Procedure

Figure 7-1 Data watermarking process



7.2 Watermark Injection

You can inject customized watermarks in PDF, PPT, Word, and Excel files on DSC. This section describes how to inject customized watermarks into local file or cloud files (files stored in the OBS bucket).

Prerequisites

Watermarks can be added for the PDF, PPT, Word, and Excel files.

Constraints

- The operations described in this section apply only to PDF, PPT, Word, and Excel files.
- If you inject an invisible watermark, the watermark is invisible and needs to be extracted using tools. For details, see **Watermark Extraction**.

Procedure

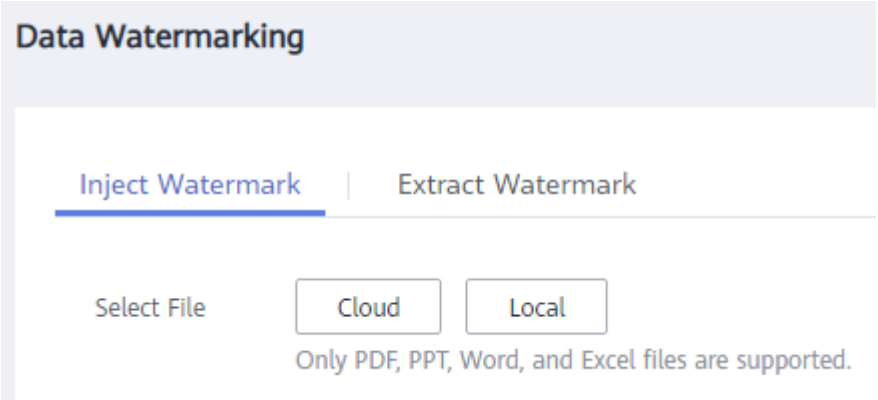
Step 1 Log in to the management console.

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** > **Data Security Center**.

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

Figure 7-2 Accessing the watermark injection page



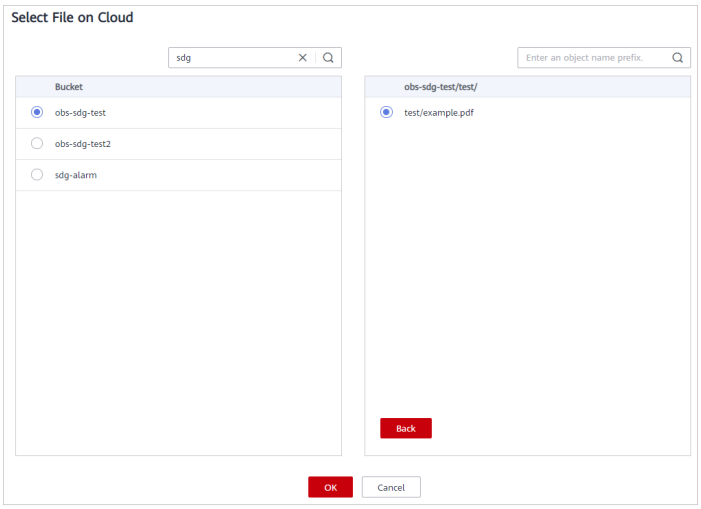
Step 5 Select a file into which you want to inject watermarks.

NOTE

Only PDF, PPT, Word, and Excel files are supported.

- If the files to be injected with watermarks are stored in OBS buckets, select **Cloud** for **Select File**, locate the bucket, and select the target file. Click **OK**.

  Figure 7-3 Selecting a cloud file



- If the files to be injected with watermarks are stored on the local PC, select **Local** for **Select File** and upload a file to DSC.

Step 6 After the file is uploaded, configure related parameters. **Table 7-2** describes the parameters.

Table 7-2 Watermarking parameters

Parameter	Description	Example Value
Watermark Type	Both visible and invisible watermarks are supported. You can select multiple values. • Visible watermark. The watermark text is displayed in the file • Invisible watermark. The watermark text is invisible and needs to be extracted using tools. For details about how to extract an invisible watermark, see **Watermark Extraction**.	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.	• **Font Size**: 45 • **Font Angle**: 46 • **Transparency**: 30
Configure Invisible Watermark	This parameter is mandatory when **Watermark Type** is set to **Invisible**. Set **Text** as required.	**Text**: ZhangSan

Step 7 After parameters are configured, click **OK**. The file with watermark injected is automatically downloaded to the specified path on the local PC.

NOTICE

- If you inject a visible watermark, open the file to view the effect.
- If you inject an invisible watermark, the watermark is invisible and needs to be extracted using tools. For details, see **Watermark Extraction**.

----End

7.3 Watermark Extraction

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

Watermarks can be added for the PDF, PPT, Word, and Excel files.

Constraints

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

Procedure

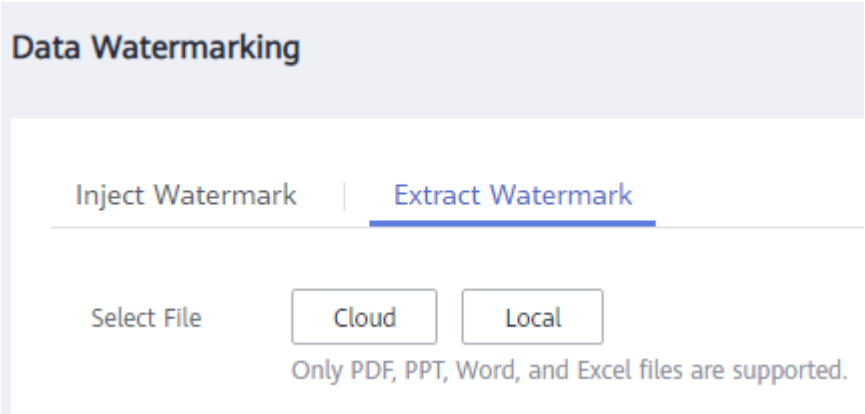
Step 1 Log in to the management console.

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** > **Data Security Center**.

Step 4 In the navigation pane, choose **Data Watermarking**. In the upper left corner of the page, click the **Extract Watermark** tab.

Figure 7-4 Accessing the watermark extraction page



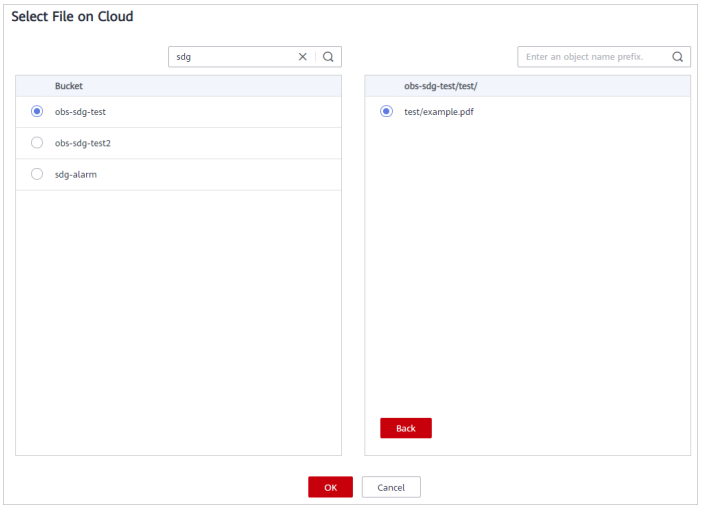
Step 5 Select a file from which you want to extract the watermark text.

NOTE

Only PDF, PPT, Word, and Excel files are supported.

- If the files from which watermarks are extracted are stored in the OBS bucket, select **Cloud** for **Select File**, locate the bucket, and select the target file. Click **OK**.

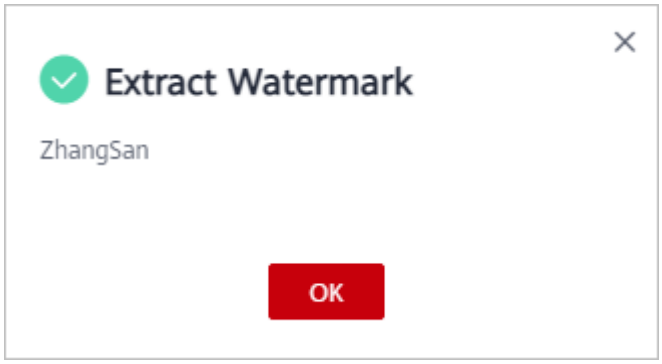
Figure 7-5 Selecting a cloud file



- If the files from which watermarks are extracted are stored on the local PC, select **Local** for **Select File**, select the file, and upload it to DSC.

Step 6 After the file is uploaded, click **OK**.

Figure 7-6 Watermark extraction completed



----End

8 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.
- Before setting alarm notification, you are advised to create a message topic in the SMN service as an administrator.

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** > **Data Security Center**.

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

Step 5 Configure alarm notifications. **Table 8-1** describes the parameters.

Figure 8-1 Configuring alarm notifications

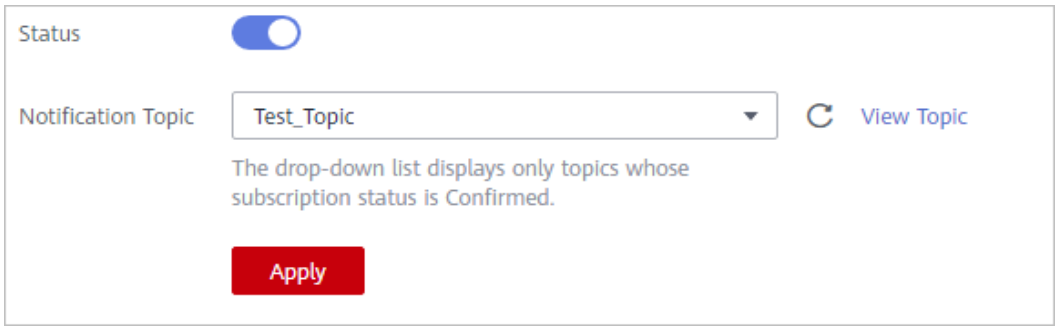


Table 8-1 Parameters

Parameter	Description	Example Value
Status	Whether notification is enabled. •  : 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. For details about topics and subscriptions, see *Simple Message Notification User Guide*.	N/A

Step 6 Click **Apply**.

----End

9 Permissions Management

9.1 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 account or cloud service to perform professional and efficient O&M on your DSC resources.

If your account does not require individual IAM users, skip this section.

This section describes the procedure for granting permissions (see **Figure 9-1**).

Prerequisites

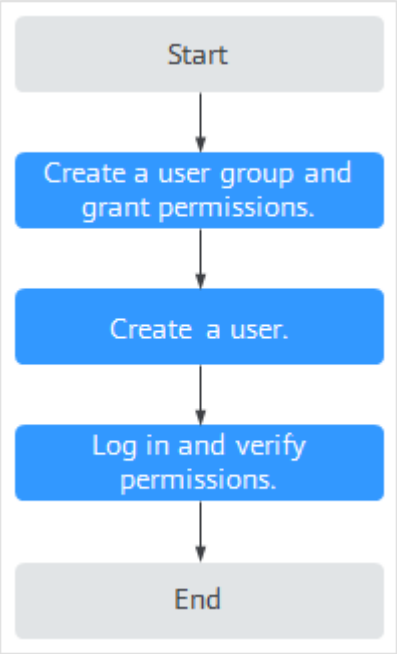
Learn about the permissions supported by DSC in **Table 9-1** and choose policies or roles based on your requirements.

Table 9-1 DSC system-defined policies

Policy	Description	Type	Dependency
DSC DashboardReadOnlyAccess	Read-only permissions for the overview page of DSC	System-defined policy	None
DSC FullAccess	All permissions for DSC	System-defined policy	None
DSC ReadOnlyAccess	Read-only permissions for Data Security Center	System-defined policy	None

Process Flow

Figure 9-1 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.

9.2 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.

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"
            ]
        }
    ]
}
```

9.3 DSC Permissions and Supported Actions

This section describes how to use IAM for fine-grained DSC permissions management. If your 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
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

Permission	Action
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 overview page of DSC	dsc:overview:list
Querying the database list	dsc:databaseAsset:list
Deleting OBS assets	dsc:obsAsset:delete
Deleting big data assets	dsc:bigdataAsset:delete

10 FAQs

10.1 Product Consulting

10.1.1 What is Data Security Center?

Data Security Center (DSC) is a latest-generation cloud data security management platform that protects your data assets by leveraging its data protection capabilities such as data classification, risk identification, data masking, and watermark-based source tracking. DSC gives you an insight into the security status of each stage in data security lifecycle and provides constant visibility of the security status of your data assets.

10.1.2 Does DSC Store My Data Assets or Files?

DSC does not store your data or files. DSC only identifies, anonymizes, or watermarks the data from the data sources you authorize DSC to access.

The data identification results are displayed on the DSC console.

10.1.3 What Types of Unstructured Files Can DSC Parse?

Table 10-1, **Table 10-2**, and **Table 10-3** list the types of unstructured files that can be parsed by DSC.

Table 10-1 Text and code files

No.	File Type	No.	File Type
1	Access database file	74	PDF document
2	ARFF file	75	Perl source code
3	ASP file	76	PGP file
4	ATOM file	77	PHP source code

No.	File Type	No.	File Type
5	BAT file	78	PKCS7 digital certificate file
6	BCPL source code	79	Plist file
7	BIB file	80	PostgreSQL database file
8	C# source code	81	PostScript document
9	C/C+ source code	82	PowerPoint document
10	CAD SldWorks file	83	Properties file
11	CAD document	84	Publisher file
12	CBOR file	85	Python source code
13	CFG file	86	Quattro-Pro spreadsheet
14	CHM file	87	Redis database file
15	Com executable file	88	RSS file
16	CSS file	89	RTF document
17	DataX configuration file	90	Ruby source code
18	DBF file	91	R source code
19	DIF file	92	SAS7BDAT file
20	DITA file	93	SAS file
21	Djvu Document	94	Scala source code
22	DOS executable file	95	Shell script
23	D source code	96	SQLite 3 database file
24	ELF executable file	97	SQLServer database file
25	EPUB eBook file	98	SQL source code
26	Excel document	99	SSH public key
27	FDF document	100	SSH configuration file
28	Fictionbook XML file	101	SSH private key
29	FTP session file	102	Staroffice document
30	GnucCash financial XML file	103	Swift source code
31	Go source code	104	TAB file

No.	File Type	No.	File Type
32	Groovy source code	105	TCL source code
33	HDR file	106	TEXT file
34	HOCON file	107	TFF file
35	HTML file	108	TNEF file
36	HTM file	109	Tomcat Application configuration file
37	HWP file	110	Tomcat Users configuration file
38	Ibooks file	111	Tomcat configuration file
39	Iis configuration file	112	TOML file
40	Initialization file	113	TSD file
41	ISA-Tab file	114	TSV file
42	iWork document	115	VCS file
43	Java Jce Keystore file	116	Visio document
44	Java Keystore file	117	Visual Basic source code
45	JavaScript source code	118	Virtual Reality Modeling Language (VRML) code
46	Java source code	119	Web Archive file
47	JSON file	120	WebLogic configuration file
48	JSP source code	121	WebVTT file
49	LaTeX source code	122	Windowsinf file
50	Log file	123	Windows full-text search index
51	Lua source code	124	Windows precompilation file
52	MariaDB database file	125	WordPerfect document
53	Markdown document	126	DOC file
54	Matlab source code	127	WPD document
55	Mbox file	128	WPS document
56	MIME HTML file	129	XDP file

No.	File Type	No.	File Type
57	Microsoft Reader documentation	130	XFDF file
58	MongoDB database file	131	XHTML file
59	MRS configuration file	132	XLF file
60	Microsoft Works document	133	XLIFF file
61	MySQL database file	134	XLR file
62	NetCDF file	135	XLZ file
63	Objective-C source code	136	XML sitemap file
64	OBS configuration file	137	XML File
65	Office document	138	XMP file
66	OneNote file	139	XPS document
67	OpenDocument file	140	XPT file
68	OpenVPN configuration file	141	YAML file
69	Oracle database file	142	Common digital certificate files
70	Outlook file	143	Empty file
71	PASCAL source code	144	Configuration file **Windows Initialization**
72	PBM file	145	Other unencrypted text files
73	PCX file	146	Email document

Table 10-2 Compressed and binary files

No.	File Type	No.	File Type
1	7-Zip file	26	Lha compressed file
2	APK Android program	27	LZ4 compressed file
3	ARJ file	28	LZMA compressed file
4	AR file	29	MAT file

No.	File Type	No.	File Type
5	BGP file	30	NetCDF file
6	Brotli compressed file	31	Object file
7	Bzip2 compressed file	32	Pack200 compressed file
8	Bzip compressed file	33	RAR compressed file
9	Cabinet compressed file	34	ShareLib file
10	Core dump file	35	Snappy compressed file
11	CPIO compressed file	36	TAR compressed file
12	Deflate64 compressed file	37	TCP dump file
13	DMG file	38	Tika-Unix-Dump file
14	ELF executable file	39	UNIX compressed file
15	GDAL file	40	Xcompress compressed file
16	GRB file	41	XLZ compressed file
17	GRIB2 file	42	XPI Firefox plug-in installation package
18	GRIB file	43	XZ compressed file
19	GZIP file	44	ZIP compressed file
20	HDF file	45	Zlib compressed file
21	HE5 file	46	ZSTD compressed file
22	ISO-19139 geographic information file	47	ZSTD dictionary file
23	ISO compressed file	48	Z compressed file
24	JAR file	49	Executable file
25	Java Class file	50	Common compressed file

Table 10-3 Images

No.	File Type	No.	File Type
1	BMP file	4	JFIF file

No.	File Type	No.	File Type
2	PNM file	5	JPEG file
3	PNG file	6	TIFF file

10.2 Adding Data Assets

10.2.1 How Do I Troubleshoot the Failure in Connecting to the Added Database?

DSC will check the connectivity of the added database. If the connection to the added database fails, perform the following operations to troubleshoot the problem:

Step 1 Check whether the IP address, account, password, and database name of the added database are correct.

- If no, correct it.
- If yes, go to 2.

Step 2 Check whether all ports and protocols are bypassed in the outbound direction of the security group which the added database belongs.

- If no, add outbound rules for the security group. Add the database to DSC again after all ports and protocols are bypassed in the outbound direction of the security group. If the failure persists, go to 3.
- If yes, go to 3.

Step 3 Check whether the number of available IP addresses in the IP subnet corresponding to the database is 0.

At least one IP address is required for DSC to establish connection to the added database. If the number of available IP addresses in the IP subnet corresponding to the database is 0, add available IP addresses to the database.

----End

10.3 Sensitive Data Identification and Masking

10.3.1 What Services Can Use DSC to Scan for Sensitive Data?

DSC can scan data stored in OBS, RDS, CSS, DLI, or GaussDB(DWS) for sensitive information by using built-in and customized rules.

The following table lists the data sources supported by DSC and identification restrictions.

Table 10-4 Supported data sources

Data Source	Data Type	Restriction
RDS	MySQL, SQL Server, and PostgreSQL	The first 500 lines of data records are sampled and scanned. The QPS reaches 300 times per second.
CSS	Big data asset	N/A
OBS	More than 200 file types	Files larger than 200 MB or encrypted files in the OBS bucket cannot be scanned.
DWS	N/A	N/A
ECS	Data in MySQL, SQL Server, PostgreSQL, and Oracle databases, as well as Elasticsearch instances	N/A
Data Lake Insight (DLI)	Big data asset	N/A

10.3.2 How Long Does It Take for DSC to Identify and Mask Sensitive Data?

Identification Duration

The identification duration depends on the data volume, number of identification rules, and scan mode. The information provided in **Table 10-5** is for reference only.

Table 10-5 Identification duration

Data Source	Data Volume	Scan Mode	Duration (Minutes)
RDS	1,000 tables	Quick scan	5
CSS	10 million documents	Quick scan	15
OBS	100 MB	Quick scan	1
OBS	100 MB	Full scan	15

Data Masking Duration

DSC uses preset and customized masking algorithms to mask sensitive data stored in RDS, , MRS, and Elasticsearch. The following table describes the masking duration.

Table 10-6 Data masking duration

Data Source	Data Volume	Duration (Minutes)
RDS	10 million lines	40
Elasticsearch	10 million documents	40
MRS_HIVE	10 million lines	40

10.3.3 Which Types of Sensitive Data Can Be Identified by DSC?

DSC can identify seven types of sensitive data, including sensitive images, personal data, and critical business information. The following table lists the types of sensitive data that can be identified by DSC.

Table 10-7 Sensitive data types that can be identified by DSC

Type	Sensitive Data
Sensitive image	• ID card • Passport
Personal privacy	• ID card • Bank card • Name in Pinyin or English • Phone number • Email address • Passport No. • EEP • License plate No. • Phone number • Officer certificate • Gender • Vehicle identification number

Type	Sensitive Data
Enterprise information	• Business license code • Tax registration certificate No. • Organization code of the enterprise • Unified social credit code
Key information	• PEM certificate • Private key • Access key ID • Secret access key • Hash password
Device information	• IP address • MAC address • JDBC URL • IPv6 address • IMEI • MEID
Location	• Province • City • GPS position • Address
Common information	Date

10.3.4 Does Data Masking Affect My Raw Data?

No. The sensitive data masking function only reads data, masks sensitive information, and saves the data in a specified path without changing your raw data.

10.3.5 Does DSC Have Specific Requirements on the Character Set for Which Sensitive Data Is to Be Identified and Masked?

No.

For details about the data sources for which sensitive data can be identified by DSC, see **What Services Can Use DSC to Scan for Sensitive Data?**.

For details about the types of sensitive data can be identified by DSC, see **Which Types of Sensitive Data Can Be Identified by DSC?**.

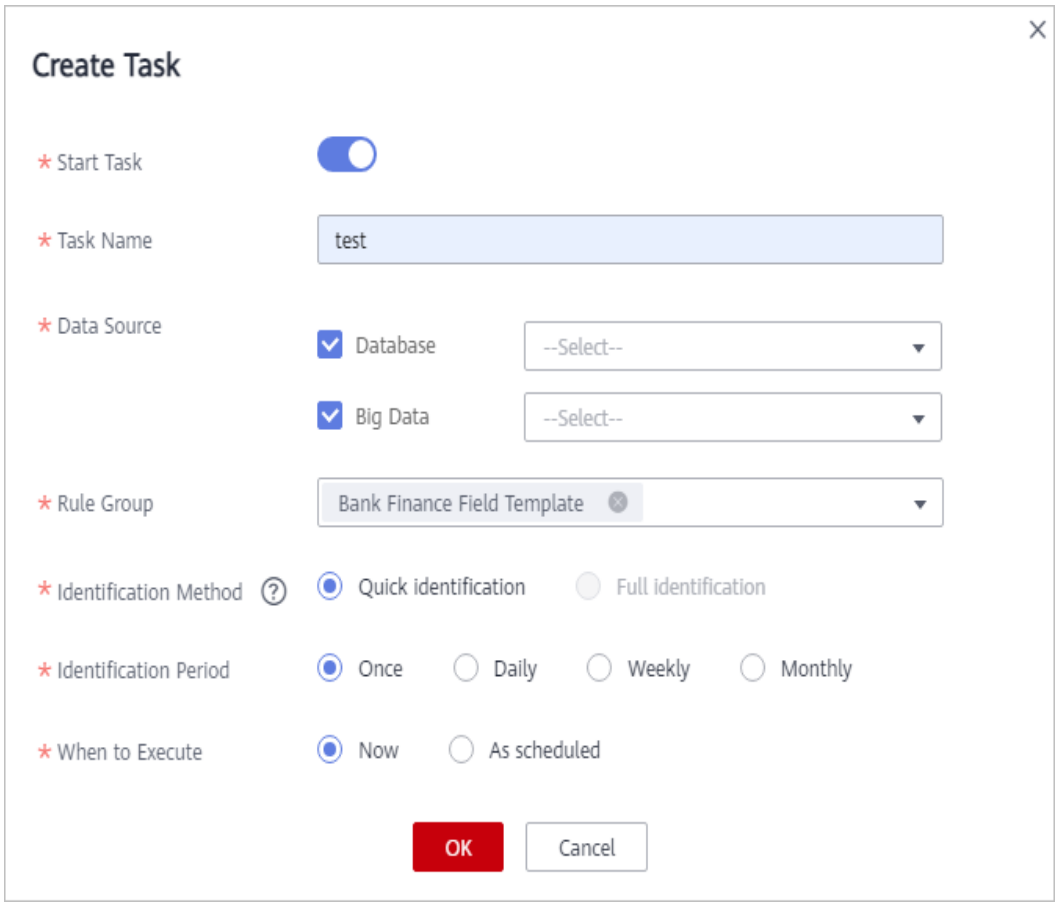
10.3.6 How Do I Add Multiple Identification Rule Groups?

DSC has over 100 sensitive data identification and masking rules for various scenarios and can identify and mask the sensitive information such as personal

information (ID card information, bank card information, names, mobile numbers, email addresses, and more), enterprise information (business license numbers, tax registration certificate numbers, and more), and key information (PEM certificates, HEY private keys, and more), device information (IP addresses, MAC addresses, IPv6 addresses, and more), location information (provinces/states, cities, GPS locations, addresses, and more), and common information (dates and others).

When you create a scanning task for an asset, add multiple identification rule groups to add multiple rules, so you can configure multiple scanning tasks for the asset, as shown in **Figure 10-1**.

Figure 10-1 Creating a sensitive data identification task



10.4 Data Watermarking

10.4.1 Will the Source Data Be Modified During Data Watermarking?

The source data will not be modified during data watermarking.

DSC injects watermarks into the files stored in the OBS bucket or local directory and generates the watermarked files. The files will be automatically downloaded to the directory specified, and there is no any modification to the source data.

10.4.2 Can the Watermark Be Extracted from a Damaged Document?

DSC data watermarking is highly robust. 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.

- If several pages are deleted from a document, the watermarks can still be extracted.
- If an image is rotated, cropped, scaled, or retouched, the watermarks can still be extracted as long as the deformation is small.

10.4.3 What Are the Requirements on the Source Data To Be Watermarked?

Watermark injection is a process to embed atomic watermark information into data with different features. The more source data features, the more complete watermark information can be embedded, and the higher the extraction success rate is. In addition, even if some data is missing, watermark extraction is not affected. The data to be watermarked must meet the following requirements:

- The source data must contain 1000 lines or more.

  If the source data contains less than 1000 lines, the watermark may fail to be extracted due to insufficient features.
- You are advised to select a column with various data values. If all the values of the column can be enumerated, the extraction may fail due to insufficient features.

  Common columns that can be embedded with watermarks include the address, name, UUID, amount, and total amount.

A Change History

Released On	Description
2022-12-20	This issue is the first official release.

