Data Security Center

Getting Started

Issue	02
Date	2024-09-25

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

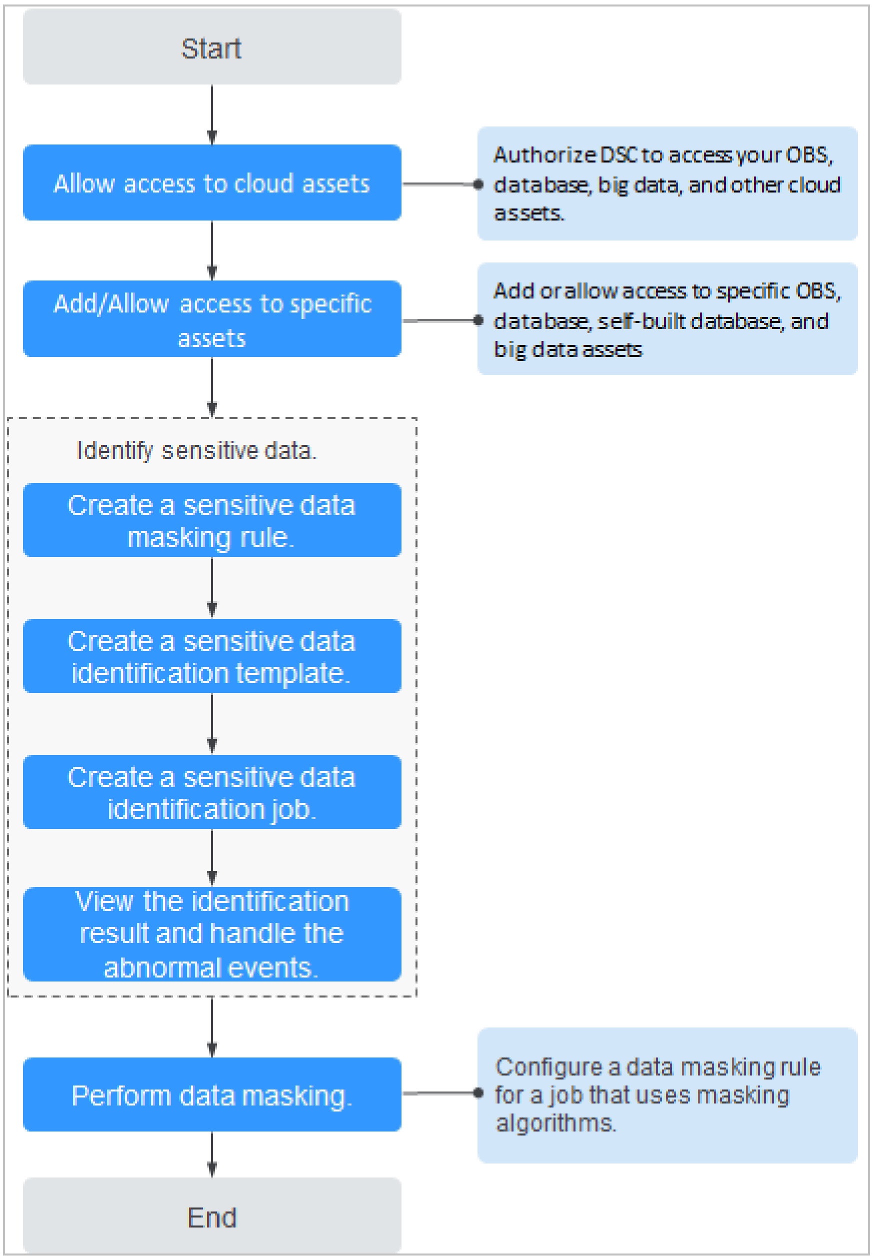
1 Procedure for Using DSC

Obtain permissions for DSC to access and protect the data stored in either OBS or RDS.

Assigning Permissions for DSC

Figure 1-1 shows the process for assigning permissions for DSC.

Figure 1-1 Assigning permissions for DSC


Start
Allow access to cloud assets
Authorize DSC to access your OBS, database, big data, and other cloud assets.
Add/Allow access to specific assets
Add or allow access to specific OBS, database, self-built database, and big data assets
Identify sensitive data.
Create a sensitive data masking rule.
Create a sensitive data identification template.
Create a sensitive data identification job.
View the identification result and handle the abnormal events.
Perform data masking.
Configure a data masking rule for a job that uses masking algorithms.
End

After permissions are granted, DSC will automatically identify sensitive data in the authorized data assets and evaluates data asset risk levels. You can go to the DSC console to view the asset security details on the **Overview** page.

Step 1 (Optional) Enable OBS or RDS to protect data in your OBS self-built buckets.

- If OBS or RDS was enabled, skip to **Step 2**.
- If OBS or RDS was not enabled, enable it and then go to **Step 2**.

  For details about how to enable OBS, see **OBS User Guide**. For details about how to enable RDS, see **RDS User Guide**.

Step 2 (Optional) Create an OBS bucket and upload the files to be stored in the bucket or create a database in an RDS DB instance.

- If the bucket was created, skip to **Step 6**.
- If the bucket was not created, create one and then go to **Step 6**.

  OBS: For details about how to create a bucket, see **Creating a Bucket**. For details about how to upload a file to a bucket, see **Uploading an ObjectUploading an Object**.

  RDS: For details about how to create a database, see **Creating a Database**.

Step 3 (Optional) Set the type of other OBS buckets to **Public** to protect other OBS buckets.

Step 4 (Optional) Obtain the information about the engine, version, and host of a self-built database to protect it.

Step 5 (Optional) Obtain the information about the engine, version, and host of other self-built data sources to protect them.

Step 6 Authorize DSC to access cloud assets.

- For details about how to grant the permission, see **Allowing or Disallowing Access to Cloud Assets**.
- For details about how to add OBS assets, see **Adding OBS Assets**.
- For details about how to authorize cloud database assets, see **Adding an RDS Database**.
- For details about how to authorize big data assets, see **Adding a Big Data Source**.
- For details about how to authorize LTS assets, see **Adding a Log Stream**.

Step 7 Configure sensitive data identification rules.

For details, see **Creating a Task**.

Step 8 View the identified sensitive data or files and their statistics.

For details about how to view the identification result, see **Identification Results**.

Step 9 Handle exceptions or mask sensitive data based on the identification result.

For details, see **Handling an Abnormal Event**.

For details about how to mask sensitive data, see **Data Masking Introduction**.

Step 10 Set alarm notifications for exceptions.

For details about how to configure alarm notifications, see **Alarm Notifications**.

----End

2 Classification and Grading of Data Assets on the Cloud

Data asset classification and grading involve categorizing data based on identification rules and assigning it to different levels according to its sensitivity, importance, and potential impact of leakage. This ensures data is protected appropriately to its significance and impact, while also meeting compliance requirements.

DSC offers a sensitive data identification function and defines 10 sensitivity levels for refined data management. It assists enterprises or organizations in monitoring the flow of sensitive data, formulating corresponding data security policies, and quickly identifying and addressing issues when data leakage or other security events occur.

This section describes how to quickly classify and grade cloud data assets (DSC Standard Edition), including purchasing DSC, authorizing the database, creating a sensitive data identification task, and viewing the classification and grading result.

Procedure

Procedure	Description
Step 1: Purchase DSC and authorize DSC to access your cloud assets.	Purchase DSC and choose the version specifications (using the standard edition as an example) and the extension package. Complete the cloud asset authorization to streamline access policy permissions between other cloud services and DSC.
Step 2: Authorize DSC to access database assets for data identification.	Sensitive data identification, data masking, and database watermark injection/extraction can only be performed once the database and big data assets are authorized. Upon completion of database authorization, DSC can access the database to retrieve data for sensitive data identification and masking.

Procedure	Description
Step 3: Create a sensitive data identification task.	Create an identification task to identify sensitive data of assets and classify and grade data based on the selected identification template.
Step 4: View the classification and grading result.	View the classification and grading result to implement protection for data assets.

Preparations

1. Before purchasing DSC, create a Huawei account and subscribe to Huawei Cloud. For details, see **Registering a HUAWEI ID and Enabling HUAWEI CLOUD Services** and **Real-Name Authentication**.

   If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.
2. Make sure that your account has sufficient balance, or you may fail to pay to your DSC orders.
3. Make sure your account has DSC permissions assigned. For details, see **Creating a User Group and Assigning DSC Permissions**.

Table 2-1 DSC system permissions

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

Step 1: Purchase DSC and Authorize DSC to Access Your Cloud Assets

Step 1 Log in to the management console.

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

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

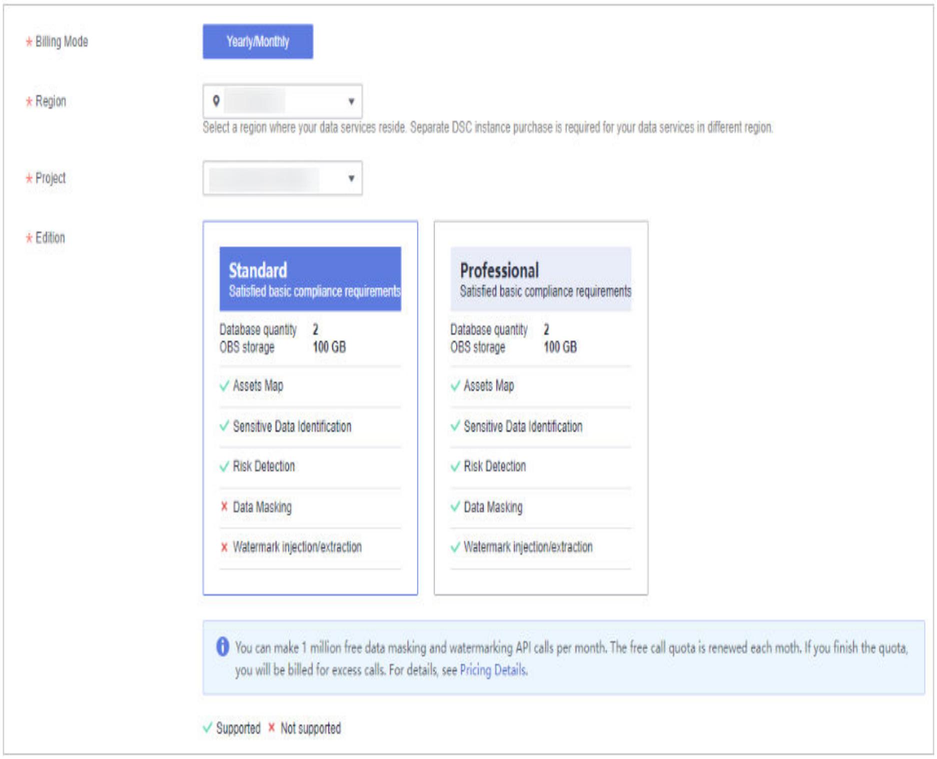
Step 4 If you are a first-time user, click **Buy DSC**.

Step 5 On the **Buy DSC** page, set the purchase parameters listed in **Figure 2-1** and complete the payment.

Table 2-2 Parameters for purchasing an instance

Parameter	Example Value	Description
Edition and specifications	Standard	The standard edition supports the asset map, sensitive data identification, and data risk detection functions. If data masking and watermark injection/ extraction are required, upgrade the edition by referring to section **Upgrading Edition and Specifications**.
OBS expansion package	1	One OBS expansion package offers 1 TB (1024 GB) of OBS storage.
Database expansion package	1	One database expansion package supports the addition of one database (RDS, DWS, self-built databases on ECS, DLI, Elasticsearch, and self-built big data on ECS). For details about the supported database types and versions, see section **Constraints**.
Required duration	1 month	Select the required duration from one month to three years.

Figure 2-1 Parameters for purchasing an instance



* Billing Mode: Yearly/Monthly

* Region:

Select a region where your data services reside. Separate DSC instance purchase is required for your data services in different region.

* Project:

* Edition:

Standard Satisfied basic compliance requirements	Professional Satisfied basic compliance requirements
Database quantity 2 OBS storage 100 GB	Database quantity 2 OBS storage 100 GB
✓ Assets Map	✓ Assets Map
✓ Sensitive Data Identification	✓ Sensitive Data Identification
✓ Risk Detection	✓ Risk Detection
✗ Data Masking	✓ Data Masking
✗ Watermark injection/extraction	✓ Watermark injection/extraction

ⓘ You can make 1 million free data masking and watermarking API calls per month. The free call quota is renewed each moth. If you finish the quota, you will be billed for excess calls. For details, see Pricing Details.

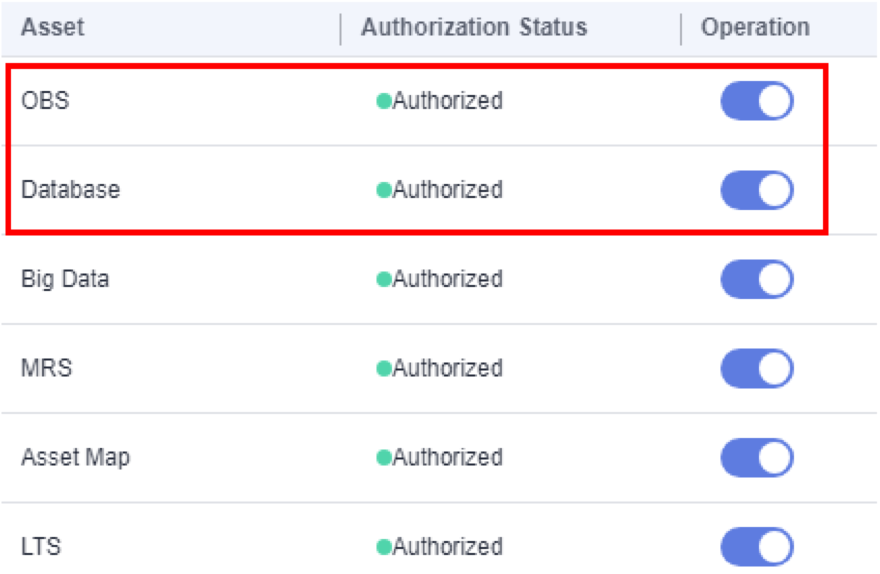
✓ Supported ✗ Not supported

Step 6 After the purchase is complete, return to the console and go to the **Asset Map** page. In the upper left corner of the page, click **Modify** next to **Cloud Asset Authorization** to perform authorization, as shown in **Figure 2-2**.

After you agree to the authorization, DSC will create agency polycies to access your cloud assets based on your choice. For details about the agency polycies, see **Allowing or Disallowing Access to Cloud Assets**.

To stop authorization, ensure that your assets have no ongoing tasks. DSC will delete your authorization information and assets and all related data. Exercise caution when performing this operation.

Figure 2-2 Authorizing access to assets



Asset	Authorization Status	Operation
OBS	●Authorized	●
Database	●Authorized	●
Big Data	●Authorized	●
MRS	●Authorized	●
Asset Map	●Authorized	●
LTS	●Authorized	●

----End

Step 2: Authorize DSC to Access Database Assets

DSC can automatically discover cloud assets and add self-built data assets. After connecting to DSC and authorizing DSC to access to cloud assets, you can delegate and manage your assets in the asset center.

Sensitive data identification, data masking, and database watermark injection and extrration can be performed only after databases and big data assets are authorized.

Step 1 Log in to the management console.

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

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

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

Step 5 On the asset type menu, choose **Database < RDS**. The **Databases** tab page is displayed.

Step 6 Click the **Database Instances** tab. In the **Operation** column of the target database instance, click **Authorize** and enter information according to **Figure 2-3**.

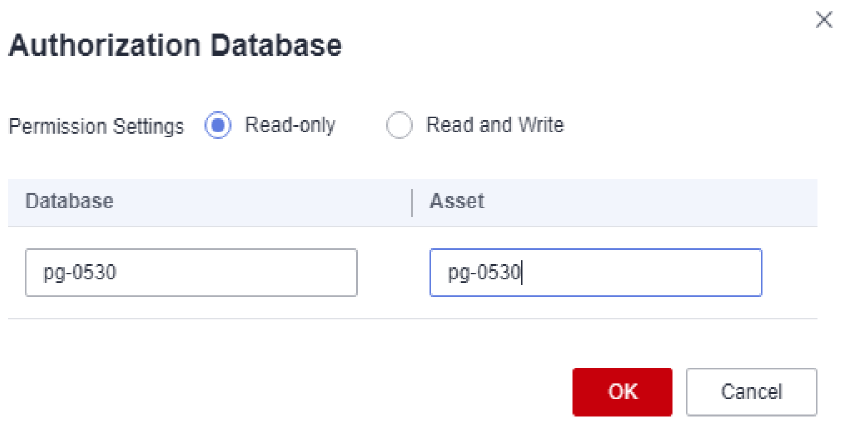
Read-only permission: Only the sensitive data identification function can be used.

Read and Write permission: The sensitive data identification and data masking functions can be used.

⚠ CAUTION

DSC cannot scan and mask sensitive data in MySQL databases within RDS instances where SSL has been enabled.

Figure 2-3 Authorizing databases



Authorization Database

Permission Settings ● Read-only ○ Read and Write

Database	Asset
pg-0530	pg-0530

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

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

DSC can access the added database normally if the **Connection Status** of the database is **Succeeded**.

----End

Step 3: Create a Sensitive Data Identification Task.

DSC identifies sensitive asset data based on the data type and the identification template selected during the creation of the identification task, and then generates an identification result.

Step 1 Log in to the management console.

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

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

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

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

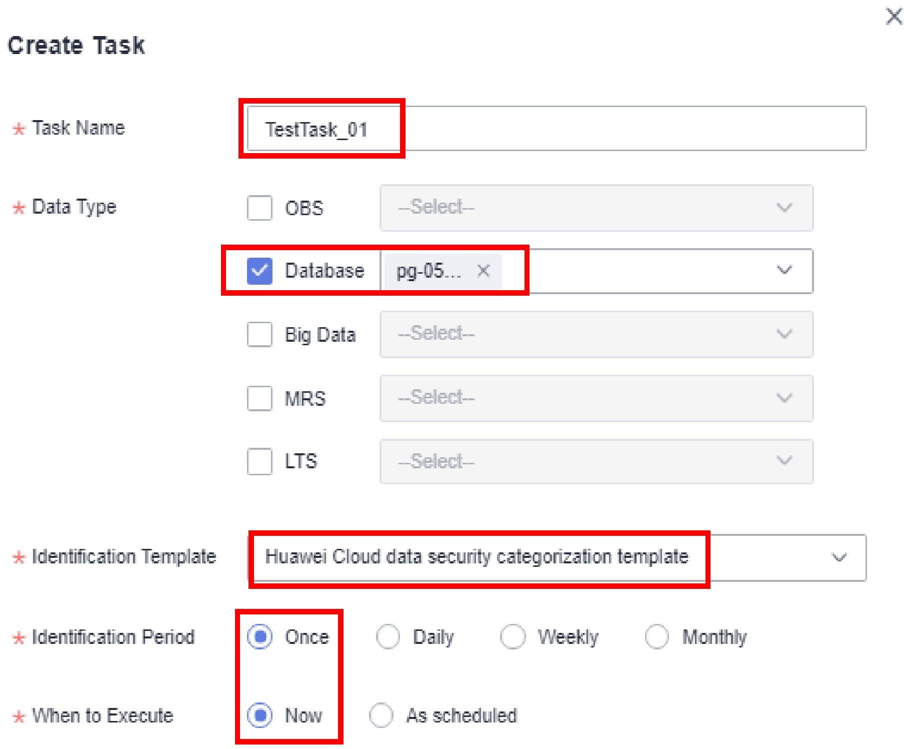
Step 6 In the displayed dialog box, set required parameters based on **Table 2-3**.

Table 2-3 Parameters for creating a task

Parameter	Example Value	Description
Task Name	Test task_01	You can customize the task name. The task name must meet the following requirements: ● Contain 4 to 255 characters. ● Consist of letters, digits, underscores (_), and hyphens (-). ● The name must start with a letter. ● Be unique.
Data Type	Database > pg-0530	Type of data to be identified. You can select multiple types. ● **OBS**: DSC is authorized to access your Huawei Cloud OBS assets and identify sensitive data in the assets. For details about how to add OBS assets, see **Adding OBS Assets**. ● **Database**: DSC identifies sensitive data of authorized database assets. For details about how to authorize database assets, see **Authorizing Access to a Database Asset**. ● **Big Data**: The DSC identifies sensitive data of authorized big data assets. For details about how to authorize big data source assets, see **Authorizing Access to Big Data Assets**. ● **MRS**: DSC identifies sensitive data of authorized MRS assets. For details about authorized MRS assets, see **Authorizing Access to Big Data Assets**.
Identification Template	Huawei Cloud Data Security Classifying and Grading Template	You can select a built-in or custom template. DSC displays data by level and category based on the template you select. For details about how to add a template, see **Adding an Identification Template**.

Parameter	Example Value	Description
Identification Period	Once	Set the execution policy of the data identification task. ● **Once**: The task will be executed once at a specified time. ● **Daily**: The task is executed at a fixed time every day. ● **Weekly**: The task is executed at a specified time every week. ● **Monthly**: The task is executed at a specified time every month.
When to Execute	Now	This parameter is displayed when **Identification Period** is set to **Once**. ● **Now**: Select the option and click **OK**, the system executes the data identification task immediately. ● **As scheduled**: The task will be executed at a specified time.
(Optional) Topic	None	● Select an existing topic from the drop-down list or click **View Topic** to create a topic for receiving alarm notifications. ● If no notification topic is configured, you can view the identification result in the identification task list. For details, see .

Figure 2-4 Parameters for creating a task



Create Task

* Task Name: TestTask_01

* Data Type:
□ OBS --Select--
☑ Database pg-05... ×
□ Big Data --Select--
□ MRS --Select--
□ LTS --Select--

* Identification Template: Huawei Cloud data security categorization template

* Identification Period: ● Once ○ Daily ○ Weekly ○ Monthly

* When to Execute: ● Now ○ As scheduled

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

----End

Step 4: View the Classification and Grading Result

Step 1 Log in to the management console.

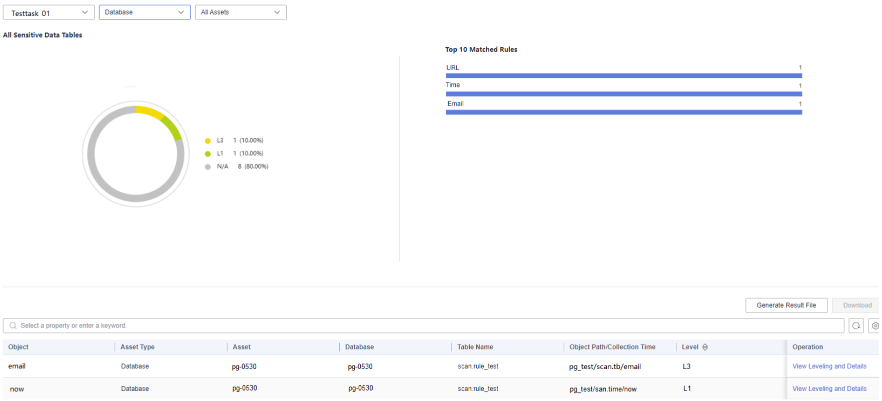
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

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

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

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

Figure 2-5 Identification result details



Object	Asset Type	Asset	Database	Table Name	Object Path/Collection Time	Level	Operation
email	Database	pg-0530	pg-0530	scan.rule_test	pg_test/scan.tb/email	L3	View Leveling and Details
now	Database	pg-0530	pg-0530	scan.rule_test	pg_test/san.time/now	L1	View Leveling and Details

Step 6 In the row containing the desired scan object, click **View Classification and Grading Result Details** in the **Operation** column. The **Classification and Grading Result Details** dialog box is displayed.

View the result details and sample data. For details about how to download the identification result, see **Downloading the Identification Result**.

----End

Related Operations

To protect sensitive information and privacy data after classification and grading and prevent unauthorized access or leakage, you can mask data and add watermarks to the data using the professional edition. For details about how to upgrade to the professional edition, see **Upgrading Edition and Specifications**.

- For details about how to mask data, see **Data Masking**. The masked data can be used for development and test, data sharing, and data research.
- For details about how to add data watermarks, see **Data Watermarking**. A data watermark uniquely identifies an asset to protect the copyright of the asset, helping you track the data leakage source.

3 Getting Started with Common Practices

After you have enabled DSC, you can apply the common practices described in this section to your services.

Table 3-1 Common Practices

Practices	Description
How Do I Prevent Personal Sensitive Data From Being Disclosed During Development and Testing?	DSC provides the static data masking function. You can create masking rules to mask large-scale data in batches. When sensitive data in the production environment is to be delivered to the development, test, or outgoing environment, you can use this function to mask the data. Static data masking applies to the following scenarios: ● Development and test ● Data sharing ● Data Research
Best Practices of OBS Data Security Protection	This section describes how to use the Data Security Center (DSC) to identify, classify, and protect sensitive data stored in OBS.