Data Security Center

# Getting Started

**Issue** 03

**Date** 2023-12-15

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

### Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

### Notice

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

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

## Huawei Cloud Computing Technologies Co., Ltd.

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

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

# Contents



# 1 Procedure for Using DSC

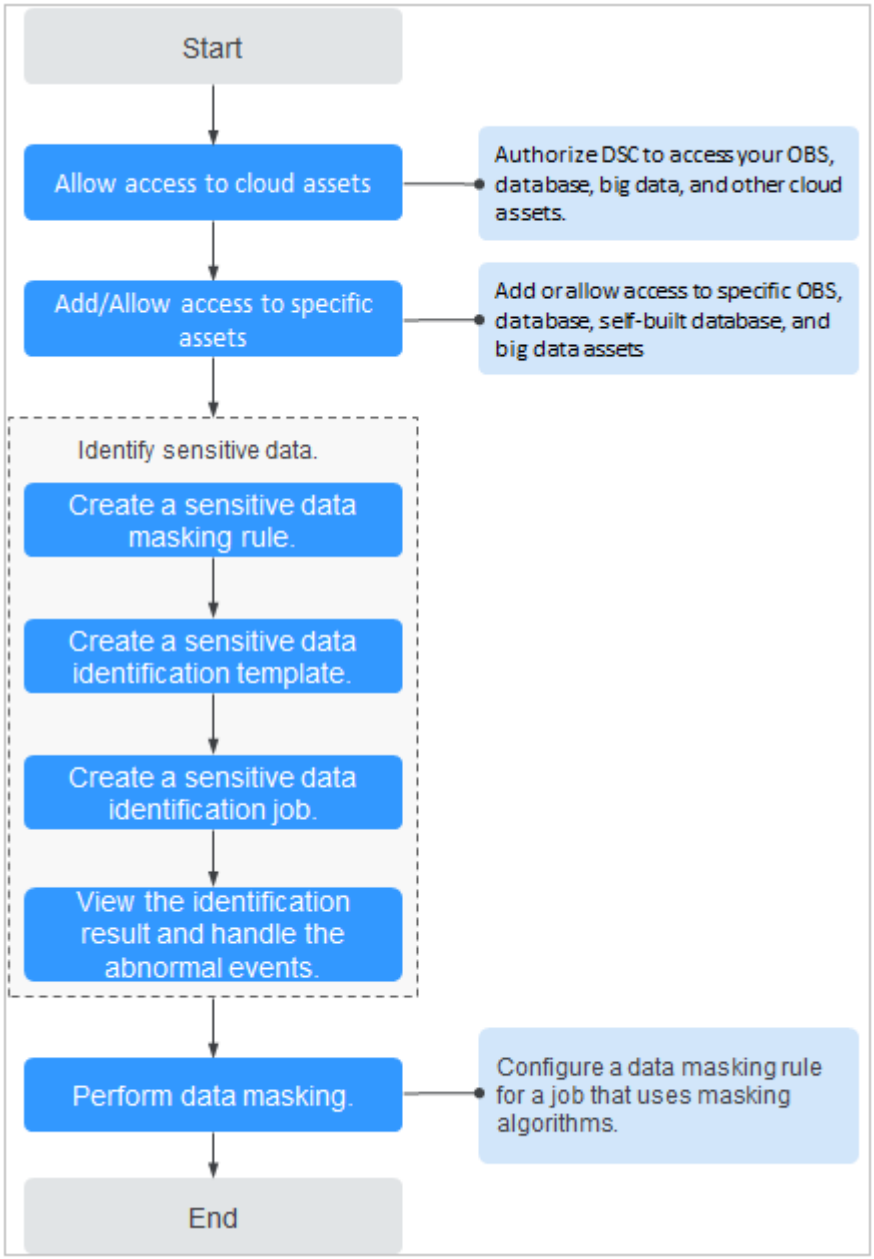
Obtain permissions for DSC to access and protect the data stored in either OBS or RDS.

## Assigning Permissions for DSC

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

**Figure 1-1** Assigning permissions for DSC




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 HUAWEI CLOUD 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 .

  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**.

**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 Getting Started with Common Practices

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

**Table 2-1** 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.<br>Static data masking applies to the following scenarios:<br>• Development and test<br>• Data sharing<br>• 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. |