Alibaba Cloud
敏感数据保护

API Reference

Issue: 20200423

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

Style	Description	Example
	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 **Danger:** Resetting will result in the loss of user configuration data.
	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 **Notice:** If the weight is set to 0, the server no longer receives new requests.
	A note indicates supplemental instructions, best practices, tips, and other content.	 **Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings** > **Network** > **Set network type**.
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands.	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`

Style	Description	Example
{} or {a|b}	This format is used for a required value, where only one item can be selected.	switch {active|stand}

Contents

1 List of operations by function

The following tables list API operations available for use in Sensitive Data Discovery and Protection (SDDP). For more information, see OpenAPI Explorer.

Security configuration

Operation	Description
CreateConfig	Modifies a configuration item in the general configuration for anomaly alerts.
ModifyDefaultLevel	Modifies the risk levels of data, including the default risk level of data that SDDP cannot classify as sensitive or insensitive and the risk levels of data that SDDP classifies as sensitive.
CreateRule	Creates a custom sensitive data detection rule.
ModifyDataLimit	Modifies configuration items for a data asset that you authorize SDDP to access. Currently, you can only modify configuration items for Relational Database Service (RDS) databases. For example, you can change the username or password for logging on to an RDS database.
ModifyRuleStatus	Enables or disables a sensitive data detection rule in SDDP.
ModifyRule	Modifies a custom sensitive data detection rule in SDDP.
DescribeDataLimits	Queries data assets, for example, MaxCompute projects, RDS databases, or Object Storage Service (OSS) buckets, that you authorize SDDP to access.
DeleteDataLimit	Deletes a data asset, for example, a MaxCompute project , an RDS database, or an OSS bucket, that you authorize SDDP to access.
DescribeConfigs	Queries configuration items in the general configuration for anomaly alerts.
DeleteRule	Deletes a custom sensitive data detection rule from SDDP.
DescribeDataLimitDetail	Queries the details of a data asset, for example, a MaxCompute project, an RDS database, or an OSS bucket, that you authorize SDDP to access.
DescribeRules	Queries sensitive data detection rules in SDDP.

Sensitive data detection

Operation	Description
DescribeDataAssets	Queries the sensitive data detection results of data assets that you authorize SDDP to access.
DescribeColumns	Queries columns in MaxCompute or RDS tables that you authorize SDDP to access
DescribeInstances	Queries MaxCompute, RDS, or OSS instances that you authorize SDDP to access.
DescribeTables	Queries MaxCompute or RDS tables that you authorize SDDP to access.
DescribeOssObjects	Queries OSS objects that you authorize SDDP to access.
DescribePackages	Queries MaxCompute packages that you authorize SDDP to access, including the names of the MaxCompute packages, accounts of the MaxCompute package owners, and risk levels of the MaxCompute packages.
DescribeOssObjectDetail	Queries the details of an OSS object that you authorize SDDP to access.

Anomalous activity processing

Operation	Description
ModifyEventTypeStatus	Enables one or more anomalous activity subtypes in SDDP.
DescribeEvents	Queries anomalous activities.
DescribeEventDetail	Queries the details of an anomalous activity, including the time when the anomalous activity occurred, description of the anomalous activity, and processing status of the anomalous activity.
ModifyEventStatus	Processes an anomalous activity.
DescribeEventTypes	Queries the types of anomalous activities.

2 Make API requests

You can send HTTP GET requests to call the SSL Certificates Service API. Before you send a request, specify the request parameters for the specific operation. A response is returned for each request. Requests and responses are encoded by using UTF-8.

Request syntax

The SSL Certificates Service API is in the remote procedure call (RPC) style. You can call the SSL Certificates Service API by sending an HTTP GET request.

The request syntax is as follows:

```
https://Endpoint/?Action=xx&Parameters
```

In the request:

- **Endpoint**: The endpoint of the SSL Certificates Service API is cas.aliyuncs.com.
- **Action**: The operation that you want to perform. For example, you can call the **DescribeOrderList** operation to query the details list of a single certificate order.
- **Version**: The API version that you want to use. The current version of the SSL Certificates Service API is 2018-08-13.
- **Parameters**: The request parameters. The parameters are separated with ampersands (&).

  Request parameters consist of common request parameters and API operation-specific parameters. Common request parameters include the API version number and authentication information. For more information about common request parameters, see Common parameters.

The following example shows how to call the **DescribeOrderList** operation to query the list of security events:

Note:
To improve readability, the API request is displayed in the following format:

```
http(s)://cas.aliyuncs.com/? Action=DescribeOrderList
&Format=xml
&Version=2018-08-13
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
```

```
&TimeStamp=2012-06-01T12:00:00Z
...
```

API signature

SSL Certificates Service authenticates each API request. Before sending a request by using HTTP or HTTPS, you must add signature information to the request.

SSL Certificates Service implements symmetric encryption through an AccessKey pair (AccessKey ID and AccessKey Secret) to verify the identity of the request sender. An AccessKey pair is an identity credential issued to Alibaba Cloud accounts and RAM users. It is similar to a user logon password. The AccessKey ID is used to verify the identity of the user. The AccessKey Secret is used to encrypt the signature string and is also used by the server to verify the signature string. The AccessKey Secret must be kept confidential.

When you call an RPC API, you need to add the signature to your request by using the following format:

```
https://endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=
CT9X0VtwR86fNWSnsc6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-
4e0ad82fd6cf
```

Take the **DescribeOrderList** operation as an example. If the AccessKey ID is testid and the AccessKey Secret is testsecret, the original request URL is as follows:

```
https://cas.aliyuncs.com/?Action=DescribeOrderList
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2018-08-13
&SignatureVersion=1.0
```

To calculate the signature, perform the following operations:

1. Use the request parameters to create the string to be signed.

```
GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeOrderList&Format%3DXML&
SignatureMethod%3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-
```

```
4e0ad82fd6cf&SignatureVersion%3D1.0&TimeStamp%3D2016-02-23T12%253A46%
253A24Z&Version%3D2018-12-03
```

2. Calculate the HMAC value of the string.

   Append an ampersand (&) to the AccessKey Secret, which will be used as the key to calculate the HMAC value. In this example, the key is `testsecret&`.

   ```
   CT9X0VtwR86fNWSnsc6v8YGOjuE=
   ```

3. Add the signature to the request parameters:

   ```
   https://advs.aliyuncs.com/?Action=DescribeOrderList
   &TimeStamp=2016-02-23T12:46:24Z
   &Format=XML
   &AccessKeyId=testid
   &SignatureMethod=HMAC-SHA1
   &SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
   &Version=2018-08-13
   &SignatureVersion=1.0
   &Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
   ```

Note:

Alibaba Cloud provides SDKs in multiple languages and third-party SDKs to simplify signature algorithm coding. For more information about Alibaba Cloud SDKs, see Alibaba Cloud Development Kit (SDK).

3 Common parameters

This topic describes the common parameters for API operations provided by SSL Certificates Service.

Common request parameters

Common request parameters are request parameters that you must use when you call each API operation.

Table 3-1: Common request parameters

Parameter	Type	Require	Description
Format	String	No	The format of the response. Valid values: JSON, XML(default)
Version	String	Yes	The version number of the API, in the format of YYYY-MM-DD. Valid value: 2018-08-13
AccessKeyId	String	Yes	The AccessKey ID of your Alibaba Cloud account that is used to access SSL Certificates Service.
Signature	String	Yes	The signature string of the current request.
SignatureMethod	String	Yes	The signature algorithm. Valid value: HMAC-SHA1
Timestamp	String	Yes	The timestamp when the request is signed. Specify the time in the ISO 8601 standard in the yyyy-MM-ddTHH:mm:ssZ format. The time must be in UTC. For example, 2013-01-10T12:00:00Z indicates January 10, 2013, 20:00:00 (UTC+8).
SignatureVersion	String	Yes	The signature algorithm version. The current version is 1.0.
SignatureNonce	String	Yes	A unique and randomly generated number used to prevent replay attacks. Users must use different numbers for different requests.

Parameter	Type	Require	Description
ResourceOwnerAccount	String	No	The name of the account that owns the resource to be accessed through this API request.

Examples

```
https://cas.aliyuncs.com/
? Format=xml
&Version=2018-08-13
&Signature=Pc5WB8gokVn0xfeu%2FZV%2BiNM1dgI%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&Timestamp=2012-06-01T12:00:00Z
```

Common response parameters

API responses use the HTTP response format where a status code of 2XX indicates a successful call and a status code of 4XX or 5XX indicates a failed call.

Response data can be returned in either the JSON or XML format. You can specify the response format when you are making the request. The default response format is XML.

Every response has a unique **RequestId** regardless of whether the call was successful or not.

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
   <!--Response root node-->
   <API operation name+response>
      <!--Request ID-->
      <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
      <!--Responses-->
   </API operation name+response>
```

- JSON format

```
{
   "RequestId":"4C467B38-3910-447D-87BC-AC049166F216",
   /*Responses*/
   }
```

4 Security configuration

4.1 CreateConfig

You can call this operation to modify a configuration item in the general configuration for anomaly alerts.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateConfig	The operation that you want to perform. Set the value to CreateConfig.
Code	String	No	access_failed_cnt	The code of the configuration item to modify. Valid values: • access_failed_cnt: the maximum number of access attempts when SDDP fails to access an unauthorized resource. • access_permission_expire_max_days: the maximum idle period for an access permission before an alert is triggered, in days. • log_datasize_avg_days: the lower limit of the output of a type of logs on the current day.

Parameter	Type	Required	Example	Description
Description	String	No	The maximum number of access attempts when SDDP fails to access an unauthorized resource. Currently, the maximum number is 10.	The description of the configuration item.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
Value	String	No	30	The value of the configuration item.

Response parameters

Parameter	Type	Example	Description
RequestId	String	208B016D-4CB9-4A85-96A5-0B8ED1EBF271	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=CreateConfig
&<Common request parameters>
```

Sample success responses

XML format

```
<CreateConfig>
  <RequestId>208B016D-4CB9-4A85-96A5-0B8ED1EBF271</RequestId>
```

```
</CreateConfig>
```

JSON format

```
{
 "RequestId":"208B016D-4CB9-4A85-96A5-0B8ED1EBF271"
}
```

Error codes

For a list of error codes, visit the API Error Center.

4.2 CreateRule

You can call this operation to create a custom sensitive data detection rule.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateRule	The operation that you want to perform. Set the value to CreateRule.
Category	Integer	Yes	0	The content type of the sensitive data detection rule. Valid values: • 0: keyword • 2: regular expression
Content	String	Yes	(?:\\D|^)((?:(?:25[0-4]|2[0-4]\\d|1\\d{2}|[1-9]\\d{1})\\.)(?:(?:25[0-5]|2[0-4]\\d|[01]? \\d? \\d)\\.){2} (?:25[0-5]|2[0-4]\\d|1[0-9]\\d|[1-9]\\d|[1-9]))(?:\\D|$)	The content of the sensitive data detection rule. The content can be a regular expression or keywords used to match sensitive fields or text.

Parameter	Type	Required	Example	Description
Name	String	Yes	rule-tst	The name of the sensitive data detection rule.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
RiskLevelId	Long	No	2	The risk level ID of data that hits the sensitive data detection rule. Valid values: • 1: S1, indicating the low risk level • 2: S2, indicating the medium risk level • 3: S3, indicating the high risk level • 4: S4, indicating the highest risk level

Response parameters

Parameter	Type	Example	Description
RequestId	String	208B016D-4CB9-4A85-96A5-0B8ED1EBF271	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=CreateRule
&<Common request parameters>
```

Sample success responses

`XML` format

```
<CreateRule>
  <RequestId>208B016D-4CB9-4A85-96A5-0B8ED1EBF271</RequestId>
```

```
</CreateRule>
```

JSON format

```
{
 "RequestId":"208B016D-4CB9-4A85-96A5-0B8ED1EBF271"
}
```

Error codes

For a list of error codes, visit the API Error Center.

4.3 CreateDataLimit

You can call this operation to authorize Sensitive Data Discovery and Protection (SDDP) to scan a data asset, such as a MaxCompute project, a Relational Database Service (RDS) database, or an Object Storage Service (OSS) bucket.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateDataLimit	The operation that you want to perform. Set the value to CreateDataLimit.
ResourceType	Integer	Yes	1	The type of the service to which the data asset belongs. Valid values: • 1: MaxCompute • 2: OSS • 5: RDS
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English

Parameter	Type	Required	Example	Description
ServiceRegionId	String	No	cn-hangzhou	The region ID of the data asset. Valid values: • **cn-beijing**: China (Beijing) • **cn-zhangjiakou**: China (Zhangjiakou) • **cn-huhehaote**: China (Hohhot) • **cn-hangzhou**: China (Hangzhou) • **cn-shanghai**: China (Shanghai) • **cn-shenzhen**: China (Shenzhen) • **cn-hongkong**: Hong Kong
ParentId	String	No	test-11**	The name of the data asset.
UserName	String	No	yhm	The username used to connect to the database.
Password	String	No	passwd	The password used to connect to the database.
AuditStatus	Integer	No	1	Specifies whether to enable the log auditing feature. Valid values: • **0**: no • **1**: yes

Parameter	Type	Required	Example	Description
AutoScan	Integer	No	1	Specifies whether to automatically trigger a re-scan after you modify a rule. • **0**: no • **1**: yes **Note:** When a re-scan is triggered, SDDP scans all data in your data asset and charges you for a full scan.
LogStoreDay	Integer	No	30	The retention period of raw logs after you enable the log auditing feature. Unit: day. Valid values: • 30 • 90 • 180 • 365
EngineType	String	No	MySQL	The type of the database. Valid values: • MySQL • SQLServer
Port	Integer	No	3306	The port used to connect to the database.

Response parameters

Parameter	Type	Example	Description
Id	Integer	1	The ID of the data asset.
RequestId	String	7C3AC882-E5A8-4855-BE77-B6837B695EF1	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=CreateDataLimit
&ResourceType=1
&<Common request parameters>
```

Sample success responses

XML format

```
<CreateDataLimitResponse>
  <Id>1</Id>
  <RequestId>7C3AC882-E5A8-4855-BE77-B6837B695EF1</RequestId>
</CreateDataLimitResponse>
```

JSON format

```
{
    "Id":1,
    "RequestId":"7C3AC882-E5A8-4855-BE77-B6837B695EF1"
}
```

Error codes

For a list of error codes, visit the API Error Center.

4.4 ModifyDataLimit

You can call this operation to modify configuration items for a data asset that you authorize Sensitive Data Discovery and Protection (SDDP) to access. Currently, you can only modify configuration items for Relational Database Service (RDS) databases. For example, you can change the username or password for logging on to an RDS database.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyDataLimit	The operation that you want to perform. Set the value to ModifyDataLimit.

Parameter	Type	Required	Example	Description
Id	Long	Yes	11	The unique ID of the data asset for which you want to modify configuration items. **Note:** You can call the **DescribeDataLimits** operation to query the ID of the data asset.
ResourceType	Integer	Yes	1	The type of the service to which the data asset belongs. Set the value to 5. Valid values: • 1: MaxCompute • 2: OSS • 5: RDS
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
Password	String	No	***	The password for logging on to the RDS database that you authorize SDDP to access.
ServiceRegionId	String	No	11	The region ID of the RDS database that you authorize SDDP to access.
UserName	String	No	tstst	The username for logging on to the RDS database that you authorize SDDP to access.

Response parameters

Parameter	Type	Example	Description
RequestId	String	7C3AC882-E5A8-4855-BE77-B6837B695EF1	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ModifyDataLimit
&<Common request parameters>
```

Sample success responses

`XML` format

```
<ModifyDataLimit>
  <RequestId>7C3AC882-E5A8-4855-BE77-B6837B695EF1</RequestId>
</ModifyDataLimit>
```

`JSON` format

```
{
 "RequestId":"7C3AC882-E5A8-4855-BE77-B6837B695EF1"
}
```

Error codes

For a list of error codes, visit the API Error Center.

4.5 ModifyRuleStatus

You can call this operation to enable or disable a sensitive data detection rule in Sensitive Data Discovery and Protection (SDDP).

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyRuleStatus	The operation that you want to perform. Set the value to ModifyRuleStatus.
Id	Long	Yes	12341	The unique ID of the sensitive data detection rule to enable or disable. **Note:** You can call the **DescribeRules** operation to query the ID of the sensitive data detection rule.
Status	Integer	Yes	1	Specifies whether to enable or disable the sensitive data detection rule. Valid values: • 0: Disable the rule. • 1: Enable the rule.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English

Response parameters

Parameter	Type	Example	Description
RequestId	String	7C3AC882-E5A8-4855-BE77-B6837B695EF1	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ModifyRuleStatus
```

```
&<Common request parameters>
```

Sample success responses

XML format

```
<ModifyRuleStatus>
  <RequestId>7C3AC882-E5A8-4855-BE77-B6837B695EF1</RequestId>
</ModifyRuleStatus>
```

JSON format

```
{
 "RequestId":"7C3AC882-E5A8-4855-BE77-B6837B695EF1"
}
```

Error codes

For a list of error codes, visit the API Error Center.

4.6 ModifyRule

You can call this operation to modify a custom sensitive data detection rule in Sensitive Data Discovery and Protection (SDDP).

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyRule	The operation that you want to perform. Set the value to ModifyRule.
Category	Integer	Yes	2	The content type of the sensitive data detection rule. Valid values: • 0: keyword • 2: regular expression

Parameter	Type	Required	Example	Description
Content	String	Yes	(?:\\D|^)((?:(?:25[0-4]|2[0-4]\\d|1\\d{2}|[1-9]\\d{1})\\.)(?:(?:25[0-5]|2[0-4]\\d|[01]? \\d? \\d)\\.){2} (?:25[0-5]|2[0-4]\\d|1[0-9]\\d|[1-9]\\d|[1-9]))(?:\\D|$)	The content of the sensitive data detection rule. The content can be a regular expression or keywords used to match sensitive fields or text.
CustomType	Integer	Yes	1	The type of the sensitive data detection rule. Set the value to 1, indicating a custom sensitive data detection rule.
Id	Long	Yes	11100	The unique ID of the sensitive data detection rule to modify. **Note:** You can call the **DescribeRules** operation to query the ID of the sensitive data detection rule.
Name	String	Yes	esw	The name of the sensitive data detection rule.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English

Parameter	Type	Required	Example	Description
RiskLevelId	Long	No	1	The risk level ID of data that hits the sensitive data detection rule. Valid values: • 1: S1, indicating the low risk level • 2: S2, indicating the medium risk level • 3: S3, indicating the high risk level • 4: S4, indicating the highest risk level

Response parameters

Parameter	Type	Example	Description
RequestId	String	7C3AC882-E5A8-4855-BE77-B6837B695EF1	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ModifyRule
&<Common request parameters>
```

Sample success responses

XML format

```
<ModifyRule>
  <RequestId>7C3AC882-E5A8-4855-BE77-B6837B695EF1</RequestId>
 </ModifyRule>
```

JSON format

```
{
 "RequestId":"7C3AC882-E5A8-4855-BE77-B6837B695EF1"
}
```

Error codes

For a list of error codes, visit the API Error Center.

4.7 DescribeDataLimits

You can call this operation to query data assets, for example, MaxCompute projects, Relational Database Service (RDS) databases, or Object Storage Service (OSS) buckets, that you authorize Sensitive Data Discovery and Protection (SDDP) to access.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeDataLimits	The operation that you want to perform. Set the value to DescribeDataLimits.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
ParentId	String	No	1112	The parent asset ID of the data asset. Examples: • The name or ID of the MaxCompute project. • The name or ID of the OSS bucket. • The name or ID of the RDS instance or database.
ResourceType	Integer	No	1	The type of the service to which the data asset belongs. Valid values: • 1: MaxCompute • 2: OSS • 5: RDS

Response parameters

Parameter	Type	Example	Description
DataLimitList			The list of data assets that were queried.
CheckStatus	Integer	3	The status of the connectivity test between the data asset and SDDP. Valid values: • 2: connectivity test in progress • 3: connectivity test passed • 4: connectivity test failed
CheckStatusName	String	Connectivity test in progress	The name of the status of the connectivity test between the data asset and SDDP.
Connector	String	jdbc:mysql://localhost:***	The connection string of the RDS database.
GmtCreate	Long	12300000	The time when the data asset was created. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Id	Long	12	The unique ID of the data asset.
LocalName	String	China (Hangzhou)	The region where the data asset resides.
ParentId	String	oss-bucket	The parent asset ID of the data asset.
RegionId	String	cn-hangzhou	The region ID of the data asset.

Parameter	Type	Example	Description
ResourceType	Long	1	The type of the service to which the data asset belongs. Valid values: • 1: MaxCompute • 2: OSS • 5: RDS
ResourceTypeCode	String	MaxCompute	The name of the service to which the data asset belongs. Valid values: • MaxCompute • OSS • RDS
UserName	String	tsts	The name of the user who owns the data asset.
RequestId	String	769FB3C1-F4C9-42DF-9B72-7077A8989C13	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeDataLimits
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeDataLimits>
 <RequestId>769FB3C1-F4C9-42DF-9B72-7077A8989C13</RequestId>
 <DataLimitList>
     <ResourceType>1</ResourceType>
     <Id>1</Id>
     <RegionId>cn-***</RegionId>
     <LocalName>China (Hangzhou)</LocalName>
     <ParentId>oss-bucket</ParentId>
     <UserName>Username</UserName>
     <Password>Password</Password>
     <Connector>Connection string</Connector>
 </DataLimitList>
```

```
</DescribeDataLimits>
```

JSON format

```
{
 "RequestId":"769FB3C1-F4C9-42DF-9B72-7077A8989C13",
 "DataLimitList":{
  "ParentId":"oss-bucket",
  "ResourceType":1,
  "Connector":"Connection string",
  "Password":"Password",
  "RegionId":"cn-***",
  "UserName":"Username",
  "Id":1,
  "LocalName":"China (Hangzhou)"
 }
}
```

Error codes

For a list of error codes, visit the API Error Center.

4.8 DeleteDataLimit

You can call this operation to delete a data asset, for example, a MaxCompute project, a Relational Database Service (RDS) database, or an Object Storage Service (OSS) bucket, that you authorize Sensitive Data Discovery and Protection (SDDP) to access.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteDataLimit	The operation that you want to perform. Set the value to DeleteDataLimit.
Id	Long	Yes	12033	The unique ID of the data asset to delete. You can call the DescribeDataLimits operation to query the ID of the data asset.

Parameter	Type	Required	Example	Description
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English

Response parameters

Parameter	Type	Example	Description
RequestId	String	7C3AC882-E5A8-4855-BE77-B6837B695EF1	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DeleteDataLimit
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DeleteDataLimit>
  <RequestId>7C3AC882-E5A8-4855-BE77-B6837B695EF1</RequestId>
</DeleteDataLimit>
```

`JSON` format

```
{
 "RequestId":"7C3AC882-E5A8-4855-BE77-B6837B695EF1"
}
```

Error codes

For a list of error codes, visit the API Error Center.

4.9 DescribeConfigs

You can call this operation to query configuration items in the general configuration for anomaly alerts.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeConfigs	The operation that you want to perform. Set the value to DescribeConfigs.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English

Response parameters

Parameter	Type	Example	Description
ConfigList			The list of configuration items in the general configuration for anomaly alerts.
Code	Integer	1	The code of the configuration item.
DefaultValue	String	The output of a type of logs on the current day is less than 30 % of the average output in the previous 10 days.	The description of the default value for the configuration item.

Parameter	Type	Example	Description
Description	String	Anomalous log output	The description of the configuration item.
Id	Long	2133	The unique ID of the configuration item.
Value	Long	30	The value of the configuration item.
RequestId	String	769FB3C1-F4C9-42DF-9B72-7077A8989C13	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeConfigs
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeConfigs>
 <RequestId>769FB3C1-F4C9-42DF-9B72-7077A8989C13</RequestId>
 <ConfigList>
      <Code>2001</Code>
      <DefaultValue>The output of a type of logs on the current day is less than 30% of the
average output in the previous 10 days.</DefaultValue>
      <Description>Anomalous log output</Description>
      <Id>2133</Id>
      <Value>10</Value>
 </ConfigList>
</DescribeConfigs>
```

JSON format

```
{
 "RequestId":"769FB3C1-F4C9-42DF-9B72-7077A8989C13",
 "ConfigList":[
  {
   "Value":10,
   "Description":"Anomalous log output",
   "DefaultValue":"The output of a type of logs on the current day is less than 30% of the
average output in the previous 10 days.",
   "Id":2133,
   "Code":1
  }
 ]
```

```
}
```

Error codes

For a list of error codes, visit the API Error Center.

4.10 DeleteRule

You can call this operation to delete a custom sensitive data detection rule from Sensitive Data Discovery and Protection (SDDP).

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteRule	The operation that you want to perform. Set the value to DeleteRule.
Id	Long	Yes	122300	The unique ID of the sensitive data detection rule to delete. You can call the **DescribeRules** operation to query the ID of the sensitive data detection rule.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English

Response parameters

Parameter	Type	Example	Description
RequestId	String	7C3AC882-E5A8-4855-BE77-B6837B695EF1	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DeleteRule
&<Common request parameters>
```

Sample success responses

XML format

```
<DeleteRule>
  <RequestId>7C3AC882-E5A8-4855-BE77-B6837B695EF1</RequestId>
 </DeleteRule>
```

JSON format

```
{
 "RequestId":"7C3AC882-E5A8-4855-BE77-B6837B695EF1"
}
```

Error codes

For a list of error codes, visit the API Error Center.

4.11 DescribeDataLimitDetail

You can call this operation to query the details of a data asset, for example, a MaxCompute project, a Relational Database Service (RDS) database, or an Object Storage Service (OSS) bucket, that you authorize Sensitive Data Discovery and Protection (SDDP) to access.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeDataLimitDetail	The operation that you want to perform. Set the value to DescribeDataLimitDetail.

Parameter	Type	Required	Example	Description
Id	Long	Yes	123000	The unique ID of the data asset to query.  **Note:** You can call the DescribeDataLimits operation to query the ID of the data asset.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
NetworkType	Integer	No	1	The network type of the data asset. Valid values: • 1: Virtual Private Cloud (VPC) • 2: classic network

Response parameters

Parameter	Type	Example	Description
DataLimit			The details of the data asset.
CheckStatus	Integer	3	The status of the connectivity test between the data asset and SDDP. Valid values: • 2: connectivity test in progress • 3: connectivity test passed • 4: connectivity test failed
CheckStatusName	String	Connectivity test passed	The name of the status of the connectivity test between the data asset and SDDP.

Parameter	Type	Example	Description
GmtCreate	Long	145600000	The time when the data asset was created. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Id	Long	111	The unique ID of the data asset.
LocalName	String	China (Hangzhou)	The region where the data asset resides.
ParentId	String	oss-bucket	The parent asset ID of the data asset. Examples: • The name or ID of the MaxCompute project. • The name or ID of the OSS bucket. • The name or ID of the RDS instance or database.
RegionId	String	cn-***	The region ID of the data asset.
ResourceType	Long	1	The type of the service to which the data asset belongs. Valid values: • 1: MaxCompute • 2: OSS • 5: RDS
ResourceTypeCode	String	MaxCompute	The name of the service to which the data asset belongs. Valid values: • MaxCompute • OSS • RDS
UserName	String	tsts	The name of the user who owns the data asset.

Parameter	Type	Example	Description
RequestId	String	769FB3C1-F4C9-42DF-9B72-7077A8989C13	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeDataLimitDetail
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeDataLimitDetail>
 <RequestId>769FB3C1-F4C9-42DF-9B72-7077A8989C13</RequestId>
 <DataLimit>
     <ResourceType>1</ResourceType>
     <Id>1</Id>
     <RegionId>cn-***</RegionId>
     <LocalName>China (Hangzhou)</LocalName>
     <ParentId>oss-bucket</ParentId>
     <UserName>tsts</UserName>
     <Password>******</Password>
     <Connector>jdbc:mysql://localhost:***</Connector>
 </DataLimit>
</DescribeDataLimitDetail>
```

`JSON` format

```
{
 "RequestId":"769FB3C1-F4C9-42DF-9B72-7077A8989C13",
 "DataLimit":{
  "ParentId":"oss-bucket",
  "ResourceType":1,
  "Connector":"jdbc:mysql://localhost:***",
  "Password":"******",
  "RegionId":"cn-***",
  "UserName":"tsts",
  "Id":1,
  "LocalName":"China (Hangzhou)"
 }
}
```

Error codes

For a list of error codes, visit the API Error Center.

4.12 DescribeRules

You can call this operation to query sensitive data detection rules in Sensitive Data Discovery and Protection (SDDP).

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeRules	The operation that you want to perform. Set the value to DescribeRules.
Category	Integer	No	2	The content type of the sensitive data detection rule. Valid values: • 0: keyword • 2: regular expression
CurrentPage	Integer	No	1	The number of the page to return.
CustomType	Integer	No	1	The type of the sensitive data detection rule. Valid values: • 0: built-in • 1: custom
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English

Parameter	Type	Required	Example	Description
Name	String	No	*** rule	The name of the sensitive data detection rule. SDDP searches for sensitive data detection rules based on the name that you enter in fuzzy match mode.
PageSize	Integer	No	12	The number of entries to return on each page.
RiskLevelId	Long	No	1	The risk level ID of data that hits the sensitive data detection rule. Valid values: • 1: S1, indicating the low risk level • 2: S2, indicating the medium risk level • 3: S3, indicating the high risk level • 4: S4, indicating the highest risk level

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the returned page.
Items			The list of sensitive data detection rules that were queried.
Category	Integer	2	The content type of the sensitive data detection rule. Valid values: • 0: keyword • 2: regular expression

Parameter	Type	Example	Description
CategoryName	String	Regular expression	The name of the content type of the sensitive data detection rule.
Content	String	(?:\\D|^)((?:(?:25[0-4]|2[0-4]\\d|1\\d{2}|[1-9]\\d{1})\\.){3}(?:(?:25[0-5]|2[0-4]\\d|[01]? \\d? \\d)\\.){2} (?:25[0-5]|2[0-4]\\d|1[0-9]\\d|[1-9]\\d|[1-9]))(?:\\D|$)	The content of the sensitive data detection rule.
CustomType	Integer	1	The type of the sensitive data detection rule. Valid values: • 0: built-in • 1: custom
Description	String	The sensitive data detection rule is used to detect IP addresses.	The description of the sensitive data detection rule.
DisplayName	String	****test	The display name of the account used to create the sensitive data detection rule.
GmtCreate	Long	1545277010000	The time when the sensitive data detection rule was created. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.

Parameter	Type	Example	Description
GmtModified	Long	1545277010000	The time when the sensitive data detection rule was modified. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Id	Long	20000	The unique ID of the sensitive data detection rule.
LoginName	String	det1111	The username of the account used to create the sensitive data detection rule.
Name	String	IP address	The name of the sensitive data detection rule.
RiskLevelId	Long	2	The risk level ID of data that hits the sensitive data detection rule. Valid values: • 1: S1, indicating the low risk level • 2: S2, indicating the medium risk level • 3: S3, indicating the high risk level • 4: S4, indicating the highest risk level
RiskLevelName	String	S2	The risk level of data that hits the sensitive data detection rule. Valid values: • S1: low risk level • S2: medium risk level • S3: high risk level • S4: highest risk level

Parameter	Type	Example	Description
Status	Integer	1	The status of the sensitive data detection rule. Valid values: • 0: disabled • 1: enabled
UserId	Long	0	The ID of the account used to create the sensitive data detection rule.
PageSize	Integer	12	The number of entries returned per page.
RequestId	String	769FB3C1-F4C9-42DF-9B72-7077A8989C13	The ID of the request.
TotalCount	Integer	23	The total number of returned entries.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeRules
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeRules>
  <RequestId>769FB3C1-F4C9-42DF-9B72-7077A8989C13</RequestId>
  <Items>
    <Description>The sensitive data detection rule is used to detect IP addresses.</
Description>
    <Category>2</Category>
    <GmtModified>1545277010000</GmtModified>
    <RiskLevelId>2</RiskLevelId>
    <Name>IP address</Name>
    <GmtCreate>1545277010000</GmtCreate>
    <UserId>0</UserId>
    <Status>1</Status>
    <Content>(?:\D|^)((?:(?:25[0-4]|2[0-4]\d|1\d{2}|[1-9]\d{1})\.)(?:(?:25[0-5]|2[0-4]\d|[01]? \
d? \d)\.){2} (?:25[0-5]|2[0-4]\d|1[0-9]\d|[1-9]\d|[1-9]))(?:\D|$)</Content>
    <CategoryName>Regular expression</CategoryName>
    <RiskLevelName>S2</RiskLevelName>
    <DepartName>test</DepartName>
    <LoginName>det1111</LoginName>
    <Id>2000</Id>
  </Items>
```

```
  <TotalCount>18</TotalCount>
  <PageSize>10</PageSize>
  <CurrentPage>1</CurrentPage>
</DescribeRules>
```

JSON format


```
{
 "Items":[
  {
   "Description":"The sensitive data detection rule is used to detect IP addresses.",
   "CategoryName":"Regular expression",
   "LoginName":"det1111",
   "RiskLevelId":2,
   "DepartName":"test",
   "UserId":0,
   "GmtCreate":1545277010000,
   "GmtModified":1545277010000,
   "Name":"IP address",
   "Status":1,
   "Category":2,
   "RiskLevelName":"S2",
   "Id":2000,
   "Content":"(?:\\D|^)((?:(?:25[0-4]|2[0-4]\\d|1\\d{2}|[1-9]\\d{1})\\.)(?:(?:25[0-5]|2[0-4]\\d|[
01]? \\d? \\d)\\.){2} (?:25[0-5]|2[0-4]\\d|1[0-9]\\d|[1-9]\\d|[1-9]))(?:\\D|$)"
  }
 ],
 "TotalCount":18,
 "PageSize":10,
 "RequestId":"769FB3C1-F4C9-42DF-9B72-7077A8989C13",
 "CurrentPage":1
}
```


Error codes

For a list of error codes, visit the API Error Center.

4.13 ModifyDefaultLevel

You can call this operation to modify the risk levels of data, including the default risk level of data that Sensitive Data Discovery and Protection (SDDP) cannot classify as sensitive or insensitive and the risk levels of data that SDDP classifies as sensitive.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyDefaultLevel	The operation that you want to perform. Set the value to ModifyDefaultLevel.
DefaultId	Long	No	4	The default risk level ID of data that SDDP cannot classify as sensitive or insensitive. Valid values: • 1: S1, indicating the low risk level • 2: S2, indicating the medium risk level • 3: S3, indicating the high risk level • 4: S4, indicating the highest risk level
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
SensitiveIds	String	No	S1,S2,S3,S4	The risk level ID of data that SDDP classifies as sensitive. Separate multiple IDs with commas (,). Valid values: • S1: low risk level • S2: medium risk level • S3: high risk level • S4: highest risk level

Response parameters

Parameter	Type	Example	Description
RequestId	String	208B016D-4CB9-4A85-96A5-0B8ED1EBF271	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ModifyDefaultLevel
&<Common request parameters>
```

Sample success responses

`XML` format

```
<ModifyDefaultLevel>
  <RequestId>208B016D-4CB9-4A85-96A5-0B8ED1EBF271</RequestId>
 </ModifyDefaultLevel>
```

`JSON` format

```
{
 "RequestId":"208B016D-4CB9-4A85-96A5-0B8ED1EBF271"
}
```

Error codes

For a list of error codes, visit the API Error Center.

5 Sensitive data detection

5.1 DescribeDataAssets

You can call this operation to query the sensitive data detection results of data assets that you authorize Sensitive Data Discovery and Protection (SDDP) to access.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeDataAssets	The operation that you want to perform. Set the value to DescribeDataAssets.
CurrentPage	Integer	No	1	The number of the page to return.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
Name	String	No	test	The keyword used to search for the data asset. SDDP searches for data assets based on the keyword that you enter in fuzzy match mode.
PageSize	Integer	No	10	The number of entries to return on each page.

Parameter	Type	Required	Example	Description
RangeId	Integer	No	1	The type of the data asset. Valid values: • 1: MaxCompute project • 2: MaxCompute table • 3: MaxCompute package • 21: Object Storage Service (OSS) bucket • 22: OSS object • 51: Relational Database Service (RDS) database • 52: RDS table
RiskLevels	String	No	S1	The risk level ID of the data asset . Separate multiple IDs with commas (,). Valid values: • S1: low risk level • S2: medium risk level • S3: high risk level • S4: highest risk level
RuleId	Long	No	11122200	The unique ID of the sensitive data detection rule that the data asset hits. **Note:** You can call the **DescribeRules** operation to query the ID of the sensitive data detection rule.

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the returned page.
Items			The list of data assets that were queried.

Parameter	Type	Example	Description
Acl	String	acl	The access control list (ACL) that controls the access permissions of the OSS bucket.
CreationTime	Long	1536751124000	The time when the data asset was created. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
DataType	String	OSS_BUCKET	The data type of the data asset.
Id	Long	268	The unique ID of the data asset.
Labelsec	Integer	0	The security status of the MaxCompute data asset.
Name	String	gxdata	The name of the data asset that was queried.
ObjectKey	String	Internal	The key value of the OSS object.
OdpsRiskLevelName	String	S4	The risk level of the MaxCompute data asset. Valid values: • S1: low risk level • S2: medium risk level • S3: high risk level • S4: highest risk level
Owner	String	dtdep-239-******	The account that owns the data asset.
ProductCode	String	RDS	The name of the service to which the data asset belongs. Valid values: • MaxCompute • OSS • RDS

Parameter	Type	Example	Description
ProductId	String	5	The ID of the service to which the data asset belongs.
Protection	Boolean	false	Indicates whether the MaxCompute data asset is being protected.
RiskLevelId	Long	2	The risk level ID of the data asset.
RiskLevelName	String	Medium risk level	The risk level of the data asset.
RuleName	String	*** rule	The name of the sensitive data detection rule that the data asset hits.
Sensitive	Boolean	true	Indicates whether the data asset contains sensitive data. Valid values: • true: The data asset contains sensitive data. • false: The data asset does not contain sensitive data.
SensitiveCount	Integer	24	The total volume of sensitive data in all data assets. For example, the value can be the total number of sensitive MaxCompute projects, packages, or tables, the total number of sensitive RDS databases or tables, or the total number of sensitive OSS buckets or objects.
SensitiveRatio	String	45%	The percentage of sensitive data in all data assets.

Parameter	Type	Example	Description
TotalCount	Integer	432	The total volume of data in all data assets. For example, the value can be the total number of MaxCompute projects, packages, or tables, the total number of RDS databases or tables, or the total number of OSS buckets or objects.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	71064826-726F-4ADA-B879-05D8055476FB	The ID of the request.
TotalCount	Integer	20	The total number of returned entries.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeDataAssets
&RangeId=1
&CurrentPage=1
&PageSize=10
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeDataAssets>
  <RequestId>71064826-726F-4ADA-B879-05D8055476FB</RequestId>
  <TotalCount>4</TotalCount>
  <PageSize>10</PageSize>
  <CurrentPage>1</CurrentPage>
  <Items>
    <Owner>dtdep-239-******</Owner>
    <ProductCode>RDS</ProductCode>
    <ProductId>5</ProductId>
    <Acl></Acl>
    <RiskLevelId>2</RiskLevelId>
    <RiskLevelName>Medium risk level</RiskLevelName>
    <DepartName>***DemoCenter</DepartName>
    <Name>gxdata</Name>
    <Labelsec>0</Labelsec>
    <CreationTime>1536751124000</CreationTime>
```

```
    <Sensitive>true</Sensitive>
    <Id>268</Id>
    <Protection>false</Protection>
    <RuleName>*** rule</RuleName>
    <ObjectKey>Internal</ObjectKey>
  </Items>
</DescribeDataAssets>
```

JSON format

```
{
 "Items":[
  {
   "Owner":"dtdep-239-******",
   "Sensitive":true,
   "ProductCode":"RDS",
   "RiskLevelId":2,
   "DepartName":"***DemoCenter",
   "ObjectKey":"Internal",
   "Protection":false,
   "RuleName":"*** rule",
   "ProductId":5,
   "Name":"gxdata",
   "CreationTime":1536751124000,
   "RiskLevelName":"Medium risk level",
   "Labelsec":0,
   "Id":268,
   "Acl":""
  }
 ],
 "TotalCount":4,
 "PageSize":10,
 "RequestId":"71064826-726F-4ADA-B879-05D8055476FB",
 "CurrentPage":1
}
```

Error codes

For a list of error codes, visit the API Error Center.

5.2 DescribeColumns

You can call this operation to query columns in MaxCompute or Relational Database Service (RDS) tables that you authorize Sensitive Data Discovery and Protection (SDDP) to access.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeColumns	The operation that you want to perform. Set the value to DescribeColumns.
CurrentPage	Integer	No	1	The number of the page to return.
InstanceId	Long	No	2341234	The ID of the instance to which the column belongs.  **Note:** You can call the **DescribeInstances** operation to query the instance ID.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
Name	String	No	test	The keyword used to search for the column. SDDP searches for columns based on the keyword that you enter in fuzzy match mode.
PageSize	Integer	No	10	The number of entries to return on each page.
ProductCode	String	No	MaxCompute	The name of the service to which the column belongs. Valid values: • MaxCompute • OSS • RDS

Parameter	Type	Required	Example	Description
RiskLevels	String	No	S2	The risk level ID of the column. Separate multiple IDs with commas (,). Valid values: • S1: low risk level • S2: medium risk level • S3: high risk level • S4: highest risk level
RuleId	Long	No	11111	The unique ID of the sensitive data detection rule that the column hits. **Note:** You can call the **DescribeRules** operation to query the ID of the sensitive data detection rule.
TableId	Long	No	11132334	The unique ID of the MaxCompute or RDS table to which the column belongs. **Note:** You can call the **DescribeTables** operation to query the table ID.

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the returned page.
Items			The list of columns that were queried.

Parameter	Type	Example	Description
CreationTime	Long	1536751124000	The time when the column was created. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
DataType	String	String	The data type of the column.
Id	Long	268	The unique ID of the column.
InstanceId	Long	1436009	The ID of the instance to which the column belongs.
Name	String	gxdata	The name of the column.
OdpsRiskLevelName	String	S3	The risk level of the column in the MaxCompute table. Valid values: • S1: low risk level • S2: medium risk level • S3: high risk level • S4: highest risk level
OdpsRiskLevelValue	Integer	3	The risk level ID of the column in the MaxCompute table. Valid values: • 1: S1, indicating the low risk level • 2: S2, indicating the medium risk level • 3: S3, indicating the high risk level • 4: S4, indicating the highest risk level
ProductCode	String	MaxCompute	The name of the service to which the column belongs. Valid values: • MaxCompute • OSS • RDS

Parameter	Type	Example	Description
RiskLevelId	Long	2	The risk level ID of the column. Valid values: • 1: S1, indicating the low risk level • 2: S2, indicating the medium risk level • 3: S3, indicating the high risk level • 4: S4, indicating the highest risk level
RiskLevelName	String	S2	The risk level of the column. Valid values: • S1: low risk level • S2: medium risk level • S3: high risk level • S4: highest risk level
RuleId	Long	1	The ID of the sensitive data detection rule that the column hits.
RuleName	String	** rule	The name of the sensitive data detection rule that the column hits.
Sensitive	Boolean	false	Indicates whether the column contains sensitive data. Valid values: • true: The column contains sensitive data. • false: The column does not contain sensitive data.
TableId	Long	123	The ID of the MaxCompute or RDS table to which the column belongs.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	769FB3C1-F4C9-4******	The ID of the request.

Parameter	Type	Example	Description
TotalCount	Integer	12	The total number of returned entries.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeColumns
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeColumns>
  <RequestId>769FB3C1-F4C9-4******</RequestId>
  <TotalCount>4</TotalCount>
  <PageSize>10</PageSize>
  <CurrentPage>1</CurrentPage>
  <Items>
    <Owner>dtdep-239-***</Owner>
    <ProductCode>RDS</ProductCode>
    <RiskLevelId>2</RiskLevelId>
    <RiskLevelName>S2</RiskLevelName>
    <DepartName>***DemoCenter</DepartName>
    <Name>gxdata</Name>
    <CreationTime>1536751124000</CreationTime>
    <Sensitive>true</Sensitive>
    <Id>268</Id>
    <RuleId>1</RuleId>
    <RuleName>** rule</RuleName>
    <InstanceId>1</InstanceId>
    <TableId>123</TableId>
  </Items>
</DescribeColumns>
```

JSON format

```
{
 "Items":[
  {
   "Owner":"dtdep-239-***",
   "Sensitive":true,
   "ProductCode":"RDS",
   "InstanceId":1,
   "RiskLevelId":2,
   "DepartName":"***DemoCenter",
   "RuleName":"** rule",
   "Name":"gxdata",
   "CreationTime":1536751124000,
   "RiskLevelName":"S2",
   "RuleId":1,
   "Id":268,
   "TableId":123
  }
 ],
```

```
 "TotalCount":4,
 "PageSize":10,
 "RequestId":"769FB3C1-F4C9-4******",
 "CurrentPage":1
}
```

Error codes

For a list of error codes, visit the API Error Center.

5.3 DescribeInstances

You can call this operation to query MaxCompute, Relational Database Service (RDS), or Object Storage Service (OSS) instances that you authorize Sensitive Data Discovery and Protection (SDDP) to access.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeInstances	The operation that you want to perform. Set the value to DescribeInstances.
CurrentPage	Integer	No	1	The number of the page to return.
FeatureType	Integer	No	0	Ignore this parameter.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English

Parameter	Type	Required	Example	Description
Name	String	No	data	The keyword used to search for the instance. SDDP searches for instances based on the keyword that you enter in fuzzy match mode.
PageSize	Integer	No	10	The number of entries to return on each page.
ProductCode	String	No	RDS	The name of the service to which the instance belongs. Valid values: • MaxCompute • OSS • RDS
ProductId	Long	No	1	The ID of the service to which the instance belongs. **Note:** You can call the **DescribeDataAssets** operation to query the service ID.
RiskLevelId	Long	No	2	The risk level ID of the instance. Valid values: • 1: S1, indicating the low risk level • 2: S2, indicating the medium risk level • 3: S3, indicating the high risk level • 4: S4, indicating the highest risk level

Parameter	Type	Required	Example	Description
RuleId	Long	No	333333	The ID of the sensitive data detection rule that the instance hits. **Note:** You can call the **DescribeRules** operation to query the ID of the sensitive data detection rule.

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the returned page.
Items			The list of instances that were queried .
Acl	String	acl	The access control list (ACL) that controls the access permissions of the OSS bucket.
CreationTime	Long	1536751124000	The time when the instance was created. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
DepartName	String	***DemoCenter	The name of the department to which the instance belongs.
Id	Long	268	The unique ID of the instance.
Labelsec	Integer	0	The security status of the MaxCompute data asset.

Parameter	Type	Example	Description
Name	String	gxdata	The name of the instance.
OdpsRiskLevelName	String	Medium risk level	The risk level of the MaxCompute data asset.
Owner	String	dtdep-239-******	The account that owns the instance.
ProductCode	String	RDS	The name of the service to which the instance belongs. Valid values: • MaxCompute • OSS • RDS
ProductId	String	5	The ID of the service to which the instance belongs.
Protection	Boolean	false	Indicates whether the MaxCompute data asset is being protected. Valid values: • true: The MaxCompute asset is being protected. • false: The MaxCompute asset is not protected.
RiskLevelId	Long	4	The risk level ID of the instance.
RiskLevelName	String	Highest risk level	The risk level of the instance.
RuleName	String	*** rule	The name of the sensitive data detection rule that the instance hits.
Sensitive	Boolean	true	Indicates whether the instance contains sensitive data. Valid values: • true: The instance contains sensitive data. • false: The instance does not contain sensitive data.

Parameter	Type	Example	Description
SensitiveCount	Integer	123	The total volume of sensitive data in the instance. For example, the value can be the total number of sensitive MaxCompute projects or packages, the total number of sensitive RDS databases, or the total number of sensitive OSS buckets.
TotalCount	Integer	231	The total volume of data in the instance. For example, the value can be the total number of MaxCompute projects or packages, the total number of RDS databases, or the total number of OSS buckets.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	71064826-726F-4ADA-B879-05D8055476FB	The ID of the request.
TotalCount	Integer	12	The total number of returned entries.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeInstances
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeInstances>
  <RequestId>71064826-726F-4ADA-B879-05D8055476FB</RequestId>
  <TotalCount>4</TotalCount>
  <PageSize>10</PageSize>
  <CurrentPage>1</CurrentPage>
  <Items>
    <Owner>dtdep-239-******</Owner>
```

```
    <ProductCode>RDS</ProductCode>
    <ProductId>1</ProductId>
    <Acl></Acl>
    <RiskLevelId>4</RiskLevelId>
    <RiskLevelName>Highest risk level</RiskLevelName>
    <DepartName>***DemoCenter</DepartName>
    <Name>gxdata</Name>
    <Labelsec>false</Labelsec>
    <CreationTime>1536751124000</CreationTime>
    <Sensitive>true</Sensitive>
    <Id>268</Id>
    <Protection>false</Protection>
  </Items>
</DescribeInstances>
```

JSON format

```
{
 "Items":[
  {
   "Owner":"dtdep-239-******",
   "Sensitive":true,
   "ProductCode":"RDS",
   "RiskLevelId":4,
   "DepartName":"***DemoCenter",
   "Protection":false,
   "ProductId":1,
   "Name":"gxdata",
   "CreationTime":1536751124000,
   "RiskLevelName":"Highest risk level",
   "Labelsec":false,
   "Id":268,
   "Acl":""
  }
 ],
 "TotalCount":4,
 "PageSize":10,
 "RequestId":"71064826-726F-4ADA-B879-05D8055476FB",
 "CurrentPage":1
}
```

Error codes

For a list of error codes, visit the API Error Center.

5.4 DescribeTables

You can call this operation to query MaxCompute or Relational Database Service (RDS) tables that you authorize Sensitive Data Discovery and Protection (SDDP) to access.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeTables	The operation that you want to perform. Set the value to DescribeTables.
CurrentPage	Integer	No	1	The number of the page to return.
InstanceId	Long	No	123432	The ID of the instance to which the MaxCompute or RDS table belongs.  **Note:** You can call the **DescribeInstances** operation to query the instance ID.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
Name	String	No	dats	The keyword used to search for the MaxCompute or RDS table. SDDP searches for MaxCompute or RDS tables based on the keyword that you enter in fuzzy match mode.
PackageId	Long	No	543300	The ID of the MaxCompute package to which the MaxCompute table belongs.  **Note:** You can call the **DescribePackages** operation to query the ID of the MaxCompute package.

Parameter	Type	Required	Example	Description
PageSize	Integer	No	10	The number of entries to return on each page.
ProductCode	String	No	MaxCompute	The name of the service to which the MaxCompute or RDS table belongs. Valid values: • MaxCompute • OSS • RDS
ProductId	Long	No	1111111	The ID of the service to which the MaxCompute or RDS table belongs. **Note:** You can call the **DescribeDataAssets** operation to query the service ID.
RiskLevelId	Long	No	2	The risk level ID of the MaxCompute or RDS table. Valid values: • 1: S1, indicating the low risk level • 2: S2, indicating the medium risk level • 3: S3, indicating the high risk level • 4: S4, indicating the highest risk level

Parameter	Type	Required	Example	Description
RuleId	Long	No	333322	The ID of the sensitive data detection rule that the MaxCompute or RDS table hits. **Note:** You can call the **DescribeRules** operation to query the ID of the sensitive data detection rule.

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the returned page.
Items			The list of MaxCompute or RDS tables that were queried.
CreationTime	Long	1536751124000	The time when the MaxCompute or RDS table was created. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Id	Long	268	The unique ID of the MaxCompute or RDS table.
InstanceId	Long	1	The ID of the instance to which the MaxCompute or RDS table belongs.
Name	String	gxdata	The name of the MaxCompute or RDS table.
Owner	String	dtdep-239-******	The account that owns the MaxCompute or RDS table.

Parameter	Type	Example	Description
ProductCode	String	MaxCompute	The name of the service to which the MaxCompute or RDS table belongs. Valid values: • MaxCompute • OSS • RDS
ProductId	String	1	The ID of the service to which the MaxCompute or RDS table belongs.
RiskLevelId	Long	2	The risk level ID of the MaxCompute or RDS table.
RiskLevelName	String	Highest risk level	The risk level of the MaxCompute or RDS table.
Sensitive	Boolean	true	Indicates whether the MaxCompute or RDS table contains sensitive fields. Valid values: • true: The MaxCompute or RDS table contains sensitive fields. • false: The MaxCompute or RDS table does not contain sensitive fields.
SensitiveCount	Integer	32	The total number of sensitive fields in the MaxCompute or RDS table.
SensitiveRatio	String	21%	The percentage of sensitive fields in the MaxCompute or RDS table.
TotalCount	Integer	1234	The total number of fields in the MaxCompute or RDS table.
PageSize	Integer	10	The number of entries returned per page.

Parameter	Type	Example	Description
RequestId	String	769FB3C1-F4C9-42DF-9B72-7077A8989C13	The ID of the request.
TotalCount	Integer	13	The total number of returned entries.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeTables
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeTables>
  <RequestId>769FB3C1-F4C9-42DF-9B72-7077A8989C13</RequestId>
  <TotalCount>4</TotalCount>
  <PageSize>10</PageSize>
  <CurrentPage>1</CurrentPage>
  <Items>
    <Owner>dtdep-239-******</Owner>
    <ProductCode>MaxCompute</ProductCode>
    <ProductId>1</ProductId>
    <Acl></Acl>
    <RiskLevelId>2</RiskLevelId>
    <RiskLevelName>Highest risk level</RiskLevelName>
    <DepartName>***DemoCenter</DepartName>
    <Name>gxdata</Name>
    <CreationTime>1536751124000</CreationTime>
    <Sensitive>true</Sensitive>
    <Id>268</Id>
    <InstanceId>1</InstanceId>
  </Items>
</DescribeTables>
```

JSON format

```
{
 "Items":[
  {
   "CreationTime":1536751124000,
   "Name":"gxdata",
   "Owner":"dtdep-239-******",
   "Sensitive":true,
   "ProductCode":"MaxCompute",
   "RiskLevelName":"Highest risk level",
   "InstanceId":1,
   "DepartName":"***DemoCenter",
   "RiskLevelId":2,
   "Id":268,
   "Acl":"",
```

```
  "ProductId":1
 }
 ],
 "TotalCount":4,
 "PageSize":10,
 "RequestId":"769FB3C1-F4C9-42DF-9B72-7077A8989C13",
 "CurrentPage":1
}
```


Error codes

For a list of error codes, visit the API Error Center.

5.5 DescribeOssObjects

You can call this operation to query Object Storage Service (OSS) objects that you authorize Sensitive Data Discovery and Protection (SDDP) to access.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeOssObjects	The operation that you want to perform. Set the value to DescribeOssObjects.
CurrentPage	Integer	No	1	The number of the page to return.
InstanceId	String	No	ins-2222	The ID of the instance to which the OSS object belongs. **Note:** You can call the **DescribeInstances** operation to query the instance ID.

Parameter	Type	Required	Example	Description
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
Name	String	No	test	The keyword used to search for the OSS object. SDDP searches for OSS objects based on the keyword that you enter in fuzzy match mode.
PageSize	Integer	No	12	The number of entries to return on each page.
RiskLevelId	Integer	No	2	The risk level ID of the OSS object. Valid values: • 1: S1, indicating the low risk level • 2: S2, indicating the medium risk level • 3: S3, indicating the high risk level • 4: S4, indicating the highest risk level
RuleId	Long	No	1222	The ID of the sensitive data detection rule that the OSS object hits. **Note:** You can call the **DescribeRules** operation to query the ID of the sensitive data detection rule.

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the returned page.
Items			The list of OSS objects that were queried.
Category	Long	900001	The type of the OSS object. For example, the value can be 900001, 800015, or 800005, which indicates the MP4 file, PDF file, and OSS configuration file, respectively.
FileId	String	file-22***	The file ID of the OSS object.
Id	Long	17383	The unique ID of the OSS object.
InstanceId	Long	1232122	The ID of the instance to which the OSS object belongs.
Name	String	obj_id	The name of the OSS object.
RegionId	String	cn-***	The region ID of the OSS object.
RiskLevelId	Long	2	The risk level ID of the OSS object.
RiskLevelName	String	Medium risk level	The risk level of the OSS object.
PageSize	Integer	12	The number of entries returned per page.
RequestId	String	769FB3C1-F4C9-42DF-9B72-7077A8989C13	The ID of the request.
TotalCount	Integer	1	The total number of returned entries.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeOssObjects
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeOssObjects>
  <RequestId>769FB3C1-F4C9-42DF-9B72-7077A8989C13</RequestId>
  <TotalCount>4</TotalCount>
  <PageSize>10</PageSize>
  <CurrentPage>1</CurrentPage>
  <Items>
    <RiskLevelName>Medium risk level</RiskLevelName>
    <Id>17383</Id>
        <Category>900001</Category>
    <RiskLevelId>2</RiskLevelId>
    <RegionId>cn-***</RegionId>
    <Name>obj_id</Name>
  </Items>
</DescribeOssObjects>
```

JSON format

```
{
 "Items":[
  {
   "Name":"obj_id",
   "Category":900001,
   "RiskLevelName":"Medium risk level",
   "RegionId":"cn-***",
   "RiskLevelId":2,
   "Id":17383
  }
 ],
 "TotalCount":4,
 "PageSize":10,
 "RequestId":"769FB3C1-F4C9-42DF-9B72-7077A8989C13",
 "CurrentPage":1
}
```

Error codes

For a list of error codes, visit the API Error Center.

5.6 DescribePackages

You can call this operation to query MaxCompute packages that you authorize Sensitive Data Discovery and Protection (SDDP) to access, including the names of the MaxCompute

packages, accounts of the MaxCompute package owners, and risk levels of the MaxCompute packages.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribePackages	The operation that you want to perform. Set the value to DescribePackages.
CurrentPage	Integer	No	1	The number of the page to return.
InstanceId	Long	No	12321	The ID of the instance to which the MaxCompute package belongs. **Note:** You can call the **DescribeInstances** operation to query the instance ID.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
Name	String	No	test	The keyword used to search for the MaxCompute package. SDDP searches for MaxCompute packages based on the keyword that you enter in fuzzy match mode.

Parameter	Type	Required	Example	Description
PageSize	Integer	No	10	The number of entries to return on each page.
ProductId	Long	No	2566600	The ID of the service to which the MaxCompute package belongs.  **Note:** You can call the **DescribeDataAssets** operation to query the service ID.
RiskLevelId	Long	No	2	The risk level ID of the MaxCompute package. Valid values: • 1: S1, indicating the low risk level • 2: S2, indicating the medium risk level • 3: S3, indicating the high risk level • 4: S4, indicating the highest risk level
RuleId	Long	No	266666	The ID of the sensitive data detection rule that the package hits.  **Note:** You can call the **DescribeRules** operation to query the ID of the sensitive data detection rule.

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the returned page.

Parameter	Type	Example	Description
Items			The list of MaxCompute packages that were queried.
CreationTime	Long	1536751124000	The time when the MaxCompute package was created. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Id	Long	111111	The unique ID of the MaxCompute package.
InstanceId	Long	223453332	The ID of the instance to which the MaxCompute package belongs.
Name	String	gxdata	The name of the MaxCompute package.
Owner	String	cou-2221	The account that owns the MaxCompute package.
RiskLevelId	Long	4	The risk level ID of the MaxCompute package. Valid values: • 1: S1, indicating the low risk level • 2: S2, indicating the medium risk level • 3: S3, indicating the high risk level • 4: S4, indicating the highest risk level
RiskLevelName	String	Highest risk level	The risk level of the MaxCompute package.

Parameter	Type	Example	Description
Sensitive	Boolean	true	Indicates whether the MaxCompute package contains sensitive data. Valid values: • true: The MaxCompute package contains sensitive data. • false: The MaxCompute package does not contain sensitive data.
SensitiveCount	Integer	123	The total volume of sensitive data in the MaxCompute package. For example, the value can be the total number of sensitive tables in the MaxCompute package.
TotalCount	Integer	321	The total volume of data in the MaxCompute package. For example, the value can be the total number of tables in the MaxCompute package.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	769FB3C1-F4C9-42DF-9B72-7077A8989C13	The ID of the request.
TotalCount	Integer	12	The total number of returned entries.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribePackages
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribePackages>
  <RequestId>769FB3C1-F4C9-42DF-9B72-7077A8989C13</RequestId>
```

```
  <TotalCount>4</TotalCount>
  <PageSize>10</PageSize>
  <CurrentPage>1</CurrentPage>
  <Items>
    <Owner>dtdep-239-******</Owner>
    <RiskLevelId>2</RiskLevelId>
    <RiskLevelName>Medium risk level</RiskLevelName>
    <DepartName>***DemoCenter</DepartName>
    <Name>gxdata</Name>
    <CreationTime>1536751124000</CreationTime>
    <Sensitive>true</Sensitive>
    <Id>268</Id>
    <InstanceId>1</InstanceId>
  </Items>
</DescribePackages>
```

JSON format

```
{
 "Items":[
  {
   "CreationTime":1536751124000,
   "Name":"gxdata",
   "Owner":"dtdep-239-******",
   "Sensitive":true,
   "RiskLevelName":"Medium risk level",
   "InstanceId":123400,
   "DepartName":"***DemoCenter",
   "RiskLevelId":2,
   "Id":268
  }
 ],
 "TotalCount":4,
 "PageSize":10,
 "RequestId":"769FB3C1-F4C9-42DF-9B72-7077A8989C13",
 "CurrentPage":1
}
```

Error codes

For a list of error codes, visit the API Error Center.

5.7 DescribeOssObjectDetail

You can call this operation to query the details of an Object Storage Service (OSS) object that you authorize Sensitive Data Discovery and Protection (SDDP) to access.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeOssObjectDetail	The operation that you want to perform. Set the value to DescribeOssObjectDetail.
Id	Long	Yes	12345213	The unique ID of the OSS object to query.  **Note:** You can call the **DescribeOssObjects** operation to query the ID of the OSS object.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English

Response parameters

Parameter	Type	Example	Description
OssObjectDetail			The details of the OSS object.
BucketName	String	bucke***	The name of the OSS bucket that stores the OSS object.
CategoryName	String	Excel file	The type of the OSS object.
Name	String	obj_id	The name of the OSS object.
RegionId	String	cn-***	The region ID of the OSS object.
RiskLevelName	String	Medium risk level	The risk level of the OSS object.
RuleList			The list of sensitive data detection rules that the OSS object hits.

Parameter	Type	Example	Description
Count	Long	2	The number of times that the OSS object hits the sensitive data detection rule.
RuleName	String	*** rule	The name of the sensitive data detection rule that the OSS object hits.
RequestId	String	769FB3C1-F4C9-42DF-9B72-7077A8989C13	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeOssObjectDetail
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeOssObjectDetail>
  <RequestId>769FB3C1-F4C9-42DF-9B72-7077A8989C13</RequestId>
  <OssObjectDetail>
    <RegionId>cn-***</RegionId>
    <BucketName>bucke***</BucketName>
    <RiskLevelName>Medium risk level</RiskLevelName>
    <Id>17383</Id>
    <RiskLevelId>2</RiskLevelId>
    <CategoryName>Excel file</CategoryName>
    <Name>obj_id</Name>
    <RuleList>
      <RuleName>*** rule</RuleName>
      <Count>10</Count>
    </RuleList>
  </OssObjectDetail>
</DescribeOssObjectDetail>
```

JSON format

```
{
 "RequestId":"769FB3C1-F4C9-42DF-9B72-7077A8989C13",
 "OssObjectDetail":{
  "Name":"obj_id",
  "RuleList":[
   {
    "Count":10,
    "RuleName":"*** rule"
   }
  ],
```

```
  "CategoryName":"Excel file",
  "BucketName":"bucke***",
  "RiskLevelName":"Medium risk level",
  "RegionId":"cn-***",
  "RiskLevelId":2,
  "Id":17383
 }
}
```


Error codes

For a list of error codes, visit the API Error Center.

6 Anomalous activity processing

6.1 ModifyEventTypeStatus

You can call this operation to enable one or more anomalous activity subtypes in Sensitive Data Discovery and Protection (SDDP).

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyEventTypeStatus	The operation that you want to perform. Set the value to ModifyEventTypeStatus.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
SubTypeIds	String	Yes	020008	The unique ID of the anomalous activity subtype to enable. Separate multiple IDs with commas (,). **Note:** You can call the **DescribeEventTypes** operation to query the ID of the anomalous activity subtype.

Response parameters

Parameter	Type	Example	Description
RequestId	String	208B016D-4CB9-4A85-96A5-0B8ED1EBF271	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ModifyEventTypeStatus
&<Common request parameters>
```

Sample success responses

XML format

```
<ModifyEventTypeStatus>
  <RequestId>208B016D-4CB9-4A85-96A5-0B8ED1EBF271</RequestId>
</ModifyEventTypeStatus>
```

JSON format

```
{
 "RequestId":"208B016D-4CB9-4A85-96A5-0B8ED1EBF271"
}
```

Error codes

For a list of error codes, visit the API Error Center.

6.2 DescribeEvents

You can call this operation to query anomalous activities.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeEvents	The operation that you want to perform. Set the value to DescribeEvents.
CurrentPage	Integer	No	1	The number of the page to return.
DealUserId	String	No	yundun-***	The ID of the account used to process the anomalous activity.
EndTime	String	No	1698700000	The end of the time range to query anomalous activities. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
PageSize	Integer	No	12	The number of entries to return on each page.
ProductCode	String	No	OSS	The name of the service where the anomalous activity was detected. Valid values: • MaxCompute • OSS • RDS

Parameter	Type	Required	Example	Description
StartTime	String	No	1657900000	The beginning of the time range to query anomalous activities. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Status	String	No	1	The ID of the processing status of the anomalous activity. Valid values: • 0: unprocessed • 1: confirmed as an anomaly • 2: excluded as a false positive
SubTypeCode	String	No	Anomalous downloaded data volume	The name of the anomalous activity subtype. **Note:** You can call the **DescribeEventTypes** operation to query the name of the anomalous activity subtype.
TargetProductCode	String	No	RDS	The name of the destination service to which data is transferred during an anomalous data flow. Valid values: • MaxCompute • OSS • RDS

Parameter	Type	Required	Example	Description
TypeCode	String	No	02	The code of the anomalous activity type. Valid values: • 01: anomalous permission access • 02: anomalous data flow • 03: anomalous data operation
UserId	Long	No	1978132506596529	The ID of the account that triggered the anomalous activity.

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the returned page.
Items			The list of anomalous activities that were queried.
AlertTime	Long	154529000	The time when an alert was triggered for the anomalous activity. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.

Parameter	Type	Example	Description
Backed	Boolean	false	Indicates whether the processing result of the anomalous activity was used to enhance the detection of anomalous activities. By enhancing the detection, you can improve the detection accuracy and the rate of triggering alerts for anomalous activities. Valid values: • true: The detection was enhanced. • false: The detection was not enhanced.
DealDisplayName	String	yundunsr	The display name of the account used to process the anomalous activity.
DealLoginName	String	det1111	The username of the account used to process the anomalous activity.
DealTime	Long	12223300	The time when the anomalous activity was processed. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
DealUserId	Long	229157443385014140	The ID of the account used to process the anomalous activity.
DisplayName	String	yundunsr	The display name of the account that triggered the anomalous activity.

Parameter	Type	Example	Description
EventTime	Long	1545829129000	The time when the anomalous activity occurred. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Id	Long	42233335555	The unique ID of the anomalous activity.
LoginName	String	det1111	The username of the account that triggered the anomalous activity.
ProductCode	String	RDS	The name of the service where the anomalous activity was detected.
Status	Integer	0	The ID of the processing status of the anomalous activity. Valid values: • 0: unprocessed • 1: confirmed as an anomaly • 2: excluded as a false positive
StatusName	String	Unprocessed	The name of the processing status of the anomalous activity.
SubTypeCode	String	020008	The code of the anomalous activity subtype.
SubTypeName	String	Anomalous downloaded data volume	The name of the anomalous activity subtype.
TargetProductCode	String	RDS	The name of the destination service to which data is transferred during an anomalous data flow.

Parameter	Type	Example	Description
TypeCode	String	02	The code of the anomalous activity type.
TypeName	String	Anomalous data flow	The name of the anomalous activity type.
UserId	Long	229157443385014140	The ID of the account that triggered the anomalous activity.
PageSize	Integer	12	The number of entries returned per page.
RequestId	String	769FB3C1-F4C9-42DF-9B72-7077A8989C13	The ID of the request.
TotalCount	Integer	1	The total number of returned entries.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeEvents
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeEvents>
  <RequestId>769FB3C1-F4C9-42DF-9B72-7077A8989C13</RequestId>
  <PageSize>10</PageSize>
  <CurrentPage>1</CurrentPage>
  <TotalCount>1</TotalCount>
  <Items>
      <Status>0</Status>
      <TypeName>Anomalous data flow</TypeName>
      <Backed>false</Backed>
      <TypeCode>02</TypeCode>
      <ProductCode>RDS</ProductCode>
      <SubTypeName>Anomalous downloaded data volume</SubTypeName>
      <EventTime>1545829129000</EventTime>
      <UserId>229157443385014140</UserId>
      <LoginName>det1111</LoginName>
      <DisplayName>yundunsr</DisplayName>
      <Id>54122244</Id>
      <SubTypeCode>020008</SubTypeCode>
      <AlertTime>1545829129000</AlertTime>
```

```
      <StatusName>Unprocessed</StatusName>
      <DealUserId>229157443385014140</DealUserId>
      <DealLoginName>det1111</DealLoginName>
      <DeaulDisplayName>yundunsr</DeaulDisplayName>
      <DepartName>test</DepartName>
  </Items>
</DescribeEvents>
```

JSON format

```
{
 "Items":[
  {
   "ProductCode":"RDS",
   "LoginName":"det1111",
   "DepartName":"test",
   "Backed":false,
   "TypeName":"Anomalous data flow",
   "UserId":229157443385014132,
   "DisplayName":"yundunsr",
   "Status":0,
   "DeaulDisplayName":"yundunsr",
   "TypeCode":"02",
   "EventTime":1545829129000,
   "AlertTime":1545829129000,
   "StatusName":"Unprocessed",
   "Id":54122244,
   "DealLoginName":"det1111",
   "SubTypeName":"Anomalous downloaded data volume",
   "SubTypeCode":"020008",
   "DealUserId":229157443385014132
  }
 ],
 "TotalCount":1,
 "PageSize":10,
 "RequestId":"769FB3C1-F4C9-42DF-9B72-7077A8989C13",
 "CurrentPage":1
}
```

Error codes

For a list of error codes, visit the API Error Center.

6.3 DescribeEventDetail

You can call this operation to query the details of an anomalous activity, including the time when the anomalous activity occurred, description of the anomalous activity, and processing status of the anomalous activity.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeEventDetail	The operation that you want to perform. Set the value to DescribeEventDetail.
Id	Long	Yes	13456723343	The unique ID of the anomalous activity to query. **Note:** You can call the **DescribeEvents** operation to query the ID of the anomalous activity.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English

Response parameters

Parameter	Type	Example	Description
Event			The details of the anomalous activity.
AlertTime	Long	1545829129000	The time when an alert was triggered for the anomalous activity. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.

Parameter	Type	Example	Description
Backed	Boolean	false	Indicates whether the processing result of the anomalous activity was used to enhance the detection of anomalous activities. By enhancing the detection, you can improve the detection accuracy and the rate of triggering alerts for anomalous activities. Valid values: • true: The detection was enhanced. • false: The detection was not enhanced.
DataInstance	String	in-222***	The name of the instance in the service where the anomalous activity was detected.
DealDisplayName	String	yundunsr	The display name of the account used to process the anomalous activity.
DealLoginName	String	det1111	The username of the account used to process the anomalous activity.
DealReason	String	Anomaly confirmed	The reason of the way in which the anomalous activity was processed.
DealTime	Long	1230000	The time when the anomalous activity was processed. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
DealUserId	Long	229157443385014140	The ID of the account used to process the anomalous activity.
Detail			The details of the anomalous activity.

Parameter	Type	Example	Description
Chart			The baseline behavior profile of the anomalous activity.
Data			The data in the baseline behavior profile of the anomalous activity.
X	String	[test1,test2,...]	The value of the data item on the X axis.
Y	String	[1,2,3,...]	The value of the data item on the Y axis.
Label	String	Baseline behavior profile	The name of the baseline behavior profile of the anomalous activity.
XLabel	String	Number of days	The descriptive label of data items on the X axis.
YLabel	String	Value	The descriptive label of data items on the Y axis.
Content			The anomalous activity content.
Label	String	Anomaly description	The name of the anomalous activity content.
Value	String	The account was used to access OSS from an unusual terminal (IP address: 1.2.3.4) from September 9 2019, 00:06:45 to September 9 2019, 00:57:37.	The description of the anomalous activity content.
ResourceInfo			The anomalous activity source.

Parameter	Type	Example	Description
Label	String	Activity risk	The name of the anomalous activity source.
Value	String	Based on the record of authentication through an unusual terminal, an external attacker may have obtained the access permission of the account or the employee accessed data from a personal terminal.	The description of the anomalous activity source.
DisplayName	String	yundunsr	The display name of the account that triggered the anomalous activity.
EventTime	Long	1545829129000	The time when the anomalous activity occurred. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Id	Long	52234	The unique ID of the anomalous activity.
LoginName	String	det1111	The username of the account that triggered the anomalous activity.

Parameter	Type	Example	Description
ProductCode	String	MaxCompute	The name of the service where the anomalous activity was detected. Valid values: • MaxCompute • RDS • OSS
Status	Integer	0	The ID of the processing status of the anomalous activity. Valid values: • 0: unprocessed • 1: confirmed as an anomaly • 2: excluded as a false positive
StatusName	String	Unprocessed	The name of the processing status of the anomalous activity.
SubTypeCode	String	020008	The code of the anomalous activity subtype.
SubTypeName	String	Anomalous downloaded data volume	The name of the anomalous activity subtype.
TypeCode	String	02	The code of the anomalous activity type.
TypeName	String	Anomalous data flow	The name of the anomalous activity type. Valid values: • Anomalous permission access • Anomalous data flow • Anomalous data operation
UserId	Long	2291574433 85014140	The ID of the account that triggered the anomalous activity.
RequestId	String	69FB3C1-F4C9 -42DF-9B72- 7077A8989C13	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeEventDetail
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeEventDetail>
 <RequestId>769FB3C1-F4C9-42DF-9B72-7077A8989C13</RequestId>
 <Event>
     <Status>0</Status>
     <TypeName>Anomalous data flow</TypeName>
     <Backed>false</Backed>
     <TypeCode>02</TypeCode>
     <ProductCode>MaxCompute</ProductCode>
     <SubTypeName>Anomalous downloaded data volume</SubTypeName>
     <EventTime>1545829129000</EventTime>
     <UserId>22915744338501 4140</UserId>
     <LoginName>det1111</LoginName>
     <DisplayName>yundunsr</DisplayName>
     <Id>4</Id>
     <SubTypeCode>020008</SubTypeCode>
     <AlertTime>1545829129000</AlertTime>
     <StatusName>Unprocessed</StatusName>
     <DealUserId>229157443385014140</DealUserId>
     <DealLoginName>det1111</DealLoginName>
     <DealDisplayName>yundunsr</DealDisplayName>
     <DepartName>test</DepartName>
     <Detail>
         <Content>
             <Value>The account was used to access OSS from an unusual terminal (IP
address: 1.2.3.4) from September 9 2019, 00:06:45 to September 9 2019, 00:57:37. </
Value>
             <Label>Anomaly description</Label>
         </Content>
         <Chart>
             <YLabel>Value</YLabel>
             <Label>Baseline behavior profile</Label>
             <Data>
                 <X>1</X>
                 <X>2</X>
                 <X>3</X>
                 <X>4</X>
                 <X>5</X>
                 <X>6</X>
                 <Y>1</Y>
                 <Y>2</Y>
                 <Y>3</Y>
                 <Y>4</Y>
                 <Y>5</Y>
                 <Y>6</Y>
             </Data>
             <XLabel>Number of days</XLabel>
         </Chart>
     </Detail>
     <DealReason>Anomaly confirmed</DealReason>
```

```
  </Event>
</DescribeEventDetail>
```

JSON format

```
{
 "Event":{
  "DealDisplayName":"yundunsr",
  "ProductCode":"MaxCompute",
  "LoginName":"det1111",
  "DepartName":"test",
  "Backed":false,
  "TypeName":"Anomalous data flow",
  "UserId":229157443385014132,
  "DisplayName":"yundunsr",
  "DealReason":"Anomaly confirmed",
  "Status":0,
  "Detail":{
   "Chart":[
    {
     "Data":{
      "Y":[
       1,
       2,
       3,
       4,
       5,
       6
      ],
      "X":[
       1,
       2,
       3,
       4,
       5,
       6
      ]
     },
     "XLabel":"Number of days",
     "Label":"Baseline behavior profile",
     "YLabel":"Value"
    }
   ],
   "Content":[
    {
     "Value":"The account was used to access OSS from an unusual terminal (IP address: 1.
2.3.4) from September 9 2019, 00:06:45 to September 9 2019, 00:57:37.",
     "Label":"Anomaly description"
    }
   ]
  },
  "TypeCode":"02",
  "EventTime":1545829129000,
  "AlertTime":1545829129000,
  "StatusName":"Unprocessed",
  "Id":4,
  "DealLoginName":"det1111",
  "SubTypeName":"Anomalous downloaded data volume",
  "SubTypeCode":"020008",
  "DealUserId":229157443385014132
 },
 "RequestId":"769FB3C1-F4C9-42DF-9B72-7077A8989C13"
```

```
}
```

Error codes

For a list of error codes, visit the API Error Center.

6.4 ModifyEventStatus

You can call this operation to process an anomalous activity.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyEventStatus	The operation that you want to perform. Set the value to ModifyEventStatus.
DealReason	String	Yes	Anomaly confirmed	The reason of the way in which you process the anomalous activity.
Id	Long	Yes	12345	The unique ID of the anomalous activity to process. **Note:** You can call the **DescribeEvents** operation to query the ID of the anomalous activity.
Status	Integer	Yes	1	The way in which you want to process the anomalous activity. Valid values: • 1: Exclude the anomalous activity as a false positive. • 2: Confirm the anomalous activity as an anomaly.

Parameter	Type	Required	Example	Description
Backed	Boolean	No	true	Specifies whether to use the processing result of the anomalous activity to enhance the detection of anomalous activities. By enhancing the detection, you can improve the detection accuracy and the rate of triggering alerts for anomalous activities. Valid values: • true: enhances the detection. • false: does not enhance the detection.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English

Response parameters

Parameter	Type	Example	Description
RequestId	String	8491DBFD-48C0-4E11-B6FC-6F38921244A9	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ModifyEventStatus
&<Common request parameters>
```

Sample success responses

XML format

```
<ModifyEventStatus>
  <RequestId>8491DBFD-48C0-4E11-B6FC-6F38921244A9</RequestId>
```

```
</ModifyEventStatus>
```

JSON format

```
{
 "RequestId":"8491DBFD-48C0-4E11-B6FC-6F38921244A9"
}
```

Error codes

For a list of error codes, visit the API Error Center.

6.5 DescribeEventTypes

You can call this operation to query the types of anomalous activities.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeEventTypes	The operation that you want to perform. Set the value to DescribeEventTypes.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
ParentTypeId	Long	No	01	The ID of the anomalous activity type for which you want to query anomalous activity subtypes. Valid values: • 01: anomalous permission access • 02: anomalous data flow • 03: anomalous data operation

Response parameters

Parameter	Type	Example	Description
EventTypeList			The list of anomalous activity types that were queried. **Note:** If you do not specify the ParentTypeId parameter, anomalous activity types are returned. If you specify the ParentTypeId parameter, anomalous activity subtypes under the specified anomalous activity type are returned.
Code	String	01	The code of the anomalous activity type.
Description	String	Anomalous permission access ,***	The description of the anomalous activity type.
Id	Long	1	The unique ID of the anomalous activity type.
Name	String	Anomalous permission access	The name of the anomalous activity type.
SubTypeList			The list of anomalous activity subtypes that were queried.
Code	String	020008	The code of the anomalous activity subtype.
Description	String	No protection for the MaxCompute sensitive project, ****	The description of the anomalous activity subtype.
Id	Long	1	The unique ID of the anomalous activity subtype.

Parameter	Type	Example	Description
Name	String	No protection for the MaxCompute sensitive project	The name of the anomalous activity subtype.
Status	Integer	1	The status of the anomalous activity subtype. Valid values: • 1: Sensitive Data Discovery and Protection (SDDP) is enabled to detect anomalous activities of this subtype. • 0: SDDP is disabled from detecting anomalous activities of this subtype.
RequestId	String	769FB3C1-F4C9-42DF-9B72-7077A8989C13	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeEventTypes
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeEventTypes>
  <RequestId>769FB3C1-F4C9-42DF-9B72-7077A8989C13</RequestId>
  <EventTypeList>
    <SubTypeList>
      <Id>1</Id>
      <Code>010001</Code>
      <Name>No protection for the MaxCompute sensitive project</Name>
      <Status>1</Status>
    </SubTypeList>
    <Id>1</Id>
    <Code>01</Code>
    <Name>Anomalous permission access</Name>
  </EventTypeList>
</DescribeEventTypes>
```

JSON format

```
{
 "EventTypeList":[
  {
```

```
  "Name":"Anomalous permission access",
  "SubTypeList":[
   {
    "Name":"No protection for the MaxCompute sensitive project",
    "Status":1,
    "Id":1,
    "Code":"010001"
   }
  ],
  "Id":1,
  "Code":"01"
 }
],
"RequestId":"769FB3C1-F4C9-42DF-9B72-7077A8989C13"
}
```


Error codes

For a list of error codes, visit the API Error Center.

7 Sensitive data desensitization

7.1 ExecDatamask

You can call this operation to de-identify sensitive data.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ExecDatamask	The operation that you want to perform. Set the value to ExecDatamask.
Data	String	Yes	{"dataHeaderList":["name","age"],"dataList":[["lily",18],["lucy",17]]}	The sensitive data to be de-identified, which is described in a JSON string. The string contains the following parameters: • dataHeaderList: the names of columns that contain sensitive data to be de-identified. • dataList: the data to be de-identified. The column order of the data to be de-identified is the same as that specified in the dataHeaderList parameter.

Parameter	Type	Required	Example	Description
TemplateId	Long	Yes	1	The ID of the de-identification template. The ID is generated after you create a de-identification template in the Sensitive Data Discovery and Protection (SDDP) console.

Response parameters

Parameter	Type	Example	Description
Data	String	{"dataHeaderList":["name","age"],"dataList":[["l**y",18],["l**y",17]]}	The de-identified data, which is described in a JSON string. The string contains the following parameters: • dataHeaderList: the names of columns that contain de-identified data. • dataList: the de-identified data. The column order of the de-identified data is the same as that specified in the dataHeaderList parameter.
RequestId	String	813BA9FA-D062-42C4-8CD5-11A7640B96E6	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ExecDatamask
&Data={"dataHeaderList":["name","age"],"dataList":[["lily",18],["lucy",17]]}
&TemplateId=1
&<Common request parameters>
```

Sample success responses

XML format

```
<ExecDatamaskResponse>
```

```
 <data>{"dataHeaderList":["name","age"],"dataList":[["l**y",18],["l**y",17]]}</data>
 <requestId>813BA9FA-D062-42C4-8CD5-11A7640B96E6</requestId>
</ExecDatamaskResponse>
```

JSON format

```
{
   "data": "{\"dataHeaderList\":[\"name\",\"age\"],\"dataList\":[[\"l**y\",18],[\"l**y\",17
]]}",
   "requestId": "813BA9FA-D062-42C4-8CD5-11A7640B96E6"
}
```

Error codes

For a list of error codes, visit the API Error Center.

7.2 DescribeDataMaskingTasks

You can call this operation to query de-identification tasks.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeDataMaskingTasks	The operation that you want to perform. Set the value to DescribeDataMaskingTasks.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
SearchKey	String	No	test	The keyword used to search for the de-identification task, which can be the task name or ID.

Parameter	Type	Required	Example	Description
StartTime	Long	No	1582992000000	The beginning of the time range to query. Set the value to a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
EndTime	Long	No	1583856000000	The end of the time range to query. Set the value to a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
DstType	Integer	No	2	The type of the service that stores the original data to be de-identified after de-identification. Valid values: • **1**: MaxCompute • **2**: Object Storage Service (OSS) • **5**: Relational Database Service (RDS)
PageSize	Integer	No	10	The number of entries to return on each page.
CurrentPage	Integer	No	1	The number of the page to return .

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the returned page.

Parameter	Type	Example	Description
Items	Array		The list of de-identification tasks that were queried.
DstPath	String	***/table1	The path for storing the original data to be de-identified after de-identification.
DstType	Integer	5	The type of the service that stores the original data to be de-identified after de-identification. Valid values: • 1: MaxCompute • 2: OSS • 5: RDS
DstTypeCode	String	RDS	The type code of the service that stores the original data to be de-identified after de-identification.
GmtCreate	Long	1582992000000	The time when the de-identification task was created.
HasUnfinishProcess	Boolean	false	Indicates whether the de-identification task is running.
Id	Long	1	The ID of the de-identification task.
Owner	String	owner	The user who created the de-identification task.
RunCount	Integer	1	The number of times that the de-identification task was run.
SrcPath	String	***/table2	The path of the data to be de-identified before de-identification.

Parameter	Type	Example	Description
SrcType	Integer	5	The type of the service to which the data to be de-identified belongs. Valid values: • 1: MaxCompute • 2: OSS • 5: RDS
SrcTypeCode	String	RDS	The type code of the service to which the data to be de-identified belongs.
Status	Integer	1	Indicates whether the de-identification task is enabled. Valid values: • 0: disabled • 1: enabled
TaskId	String	mt4HBgtw1B******	The ID of the de-identification task.
TaskName	String	Task name	The name of the de-identification task.
TriggerType	Integer	1	The mode in which the de-identification task was run. Valid values: • 1: manual • 2: scheduled • 3: manual and scheduled
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	769FB3C1-F4C9-4******	The ID of the request.
TotalCount	Integer	100	The total number of returned entries.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeDataMaskingTasks
```

```
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeDataMaskingTasksResponse>
  <RequestId>769FB3C1-F4C9-4******</RequestId>
  <TotalCount>1</TotalCount>
  <PageSize>5</PageSize>
  <CurrentPage>1</CurrentPage>
  <Items>
      <Status>1</Status>
      <TriggerType>1</TriggerType>
      <Owner>***</Owner>
      <TaskId>mt4HBgtw1B****</TaskId>
      <DstPath>********</DstPath>
      <HasUnfinishProcess>false</HasUnfinishProcess>
      <DstTypeCode>OSS</DstTypeCode>
      <SrcPath>*********</SrcPath>
      <DstType>2</DstType>
      <GmtCreate>1583739870000</GmtCreate>
      <TaskName>Task name</TaskName>
      <SrcType>2</SrcType>
      <RunCount>3</RunCount>
      <Id>1</Id>
      <SrcTypeCode>OSS</SrcTypeCode>
  </Items>
</DescribeDataMaskingTasksResponse>
```

`JSON` format

```
{
   "769FB3C1-F4C9-4******"
   "TotalCount": 1,
   "PageSize": 5,
   "CurrentPage": 1,
   "Items": [
      {
         "Status": 1,
         "TriggerType": 1,
         "Owner": "***",
         "TaskId": "mt4HBgtw1B****",
         "DstPath": "********",
         "HasUnfinishProcess": false,
         "DstTypeCode": "OSS",
         "SrcPath": "*********",
         "DstType": 2,
         "GmtCreate": 1583739870000,
         "TaskName": "Task name",
         "SrcType": 2,
         "RunCount": 3,
         "Id": 1,
         "SrcTypeCode": "OSS"
      }
   ]
```

```
}
```

Error codes

For a list of error codes, visit the API Error Center.

7.3 DescribeDataMaskingRunHistory

You can call this operation to query the running information of de-identification tasks.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeDataMaskingRunHistory	The operation that you want to perform. Set the value to DescribeDataMaskingRunHistory.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
TaskId	String	No	mt4HBgtw1B******	The ID of the de-identification task.
StartTime	Long	No	1582992000000	The beginning of the time range to query. Set the value to a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.

Parameter	Type	Required	Example	Description
EndTime	Long	No	1583856000000	The end of the time range to query. Set the value to a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Status	Integer	No	0	The status of the de-identification task. Valid values: • **-1**: waiting • **0**: running • **1**: successful • **2**: failed • **3**: terminated • **4**: partially failed
SrcType	Integer	No	2	The type of the service to which the data to be de-identified belongs. Valid values: • **1**: MaxCompute • **2**: Object Storage Service (OSS) • **5**: Relational Database Service (RDS)
DstType	Integer	No	2	The type of the service that stores the original data to be de-identified after de-identification. Valid values: • **1**: MaxCompute • **2**: OSS • **5**: RDS
PageSize	Integer	No	10	The number of entries to return on each page.

Parameter	Type	Required	Example	Description
CurrentPage	Integer	No	1	The number of the page to return.

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the returned page.
Items	Array		The list of de-identification tasks that were queried.
ConflictCount	Long	0	The number of rows that were in conflict with the data to be de-identified in the destination table to which the data to be de-identified was moved.
DstType	Integer	2	The type of the service that stores the original data to be de-identified after de-identification. Valid values: • 1: MaxCompute • 2: OSS • 5: RDS
DstTypeCode	String	OSS	The type code of the service that stores the original data to be de-identified after de-identification.
FailCode	String	masking_task_not_found	The error code returned only when the de-identification task failed.
Id	Long	1	The ID of the task running record.
MaskingCount	Long	100	The number of rows that were de-identified.

Parameter	Type	Example	Description
Percentage	Integer	100	The progress of the de-identification task.
RunIndex	Integer	1	The number of times that the de-identification task was run.
SrcType	Integer	2	The type of the service to which the data to be de-identified belongs. Valid values: • 1: MaxCompute • 2: OSS • 5: RDS
SrcTypeCode	String	OSS	The type code of the service to which the data to be de-identified belongs.
StartTime	Long	1582251233000	The time when the de-identification task was run. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Status	Integer	1	The status of the de-identification task. Valid values: • -1: waiting • 0: running • 1: successful • 2: failed • 3: terminated • 4: partially failed
TaskId	String	mt4HBgtw1B******	The ID of the de-identification task.

Parameter	Type	Example	Description
Type	Integer	1	The mode in which the de-identification task was run. Valid values: • 1: manual • 2: scheduled
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	769FB3C1-F4C9-4******	The ID of the request.
TotalCount	Integer	100	The total number of returned entries.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeDataMaskingRunHistory
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeDataMaskingRunHistoryResponse>
  <TotalCount>1</TotalCount>
  <PageSize>5</PageSize>
  <CurrentPage>1</CurrentPage>
  <Items>
      <Status>1</Status>
      <RunIndex>1</RunIndex>
      <TaskId>Vd8Rj80eBXR*****</TaskId>
      <Percentage>100</Percentage>
      <MaskingCount>100000</MaskingCount>
      <StartTime>1582251233000</StartTime>
      <DstTypeCode>RDS</DstTypeCode>
      <ConflictCount>0</ConflictCount>
      <DstType>5</DstType>
      <Type>1</Type>
      <SrcType>1</SrcType>
      <Id>4869</Id>
      <SrcTypeCode>MaxCompute</SrcTypeCode>
  </Items>
  <RequestId>769FB3C1-F4C9-4******</RequestId>
</DescribeDataMaskingRunHistoryResponse>
```

JSON format

```
{
    "TotalCount": 1,
```

```
  "PageSize": 5,
  "CurrentPage": 1,
  "Items": [
    {
      "Status": 1,
      "RunIndex": 1,
      "TaskId": "Vd8Rj80eBXR*****",
      "Percentage": 100,
      "MaskingCount": 100000,
      "StartTime": 1582251233000,
      "DstTypeCode": "RDS",
      "ConflictCount": 0,
      "DstType": 5,
      "Type": 1,
      "SrcType": 1,
      "Id": 4869,
      "SrcTypeCode": "MaxCompute"
    }
  ],
  "RequestId": "769FB3C1-F4C9-4******"
}
```


Error codes

For a list of error codes, visit the API Error Center.