ALIBABA CLOUD

Alibaba Cloud

Security Center

API Reference

Document Version: 20220524

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

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

Table of Contents

1.Make API requests

To send a Security Center API request, you must send an HTTP GET request to the Security Center endpoint. You must add the request parameters that correspond to the API operation being called. After you call the API, the system returns a response. The request and response are encoded in UTF-8.

Request structure

Security Center API operations use the RPC protocol. You can call Security Center API operations by sending HTTP GET requests.

The request syntax is as follows:

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

where:

- Endpoint: The endpoint of the Security Center API is tds.aliyuncs.com.
- Action: the name of the operation being performed. For example, to query security events, you must set the Action parameter to DescribeAlarmEventList.
- Version: the version of the API to be used. The current Security Center API version is *2018-12-03*.
- Parameters: the request parameters for the operation. Separate multiple parameters with ampersands (&).

  Request parameters include both common parameters and operation-specific parameters. Common parameters are used for all Security Center API calls regardless of the operation. For more information, see Common parameters.

The following example demonstrates how to call the DescribeAlarmEventList operation in Security Center.

> **Note** The following code has been formatted for ease reading.

```
http(s)://tds.aliyuncs.com/?Action=DescribeAlarmEventList
&Format=xml
&Version=2018-12-03
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
...
```

API authorization

To ensure the security of your account, we recommend that you call API operations as a Resource Access Management (RAM) user. Before you can call a Security Center API operation as a RAM user, you must create and attach the required permission policy to the RAM user.

Request signatures

You must sign all API requests to ensure security. Security Center uses the request signature to verify the identity of the API caller.

You must add the signature to the RPC API request in the following format:

```
https://Endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=CT9X0VtwR86fNWSn
sc6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
```

where:

- SignatureMethod: the encryption method of the signature string. Set the value to HMAC-SHA1.
- SignatureVersion: the version of the signature encryption algorithm. Set the value to 1.0.
- SignatureNonce: a unique, random number used to prevent replay attacks. You must use different random numbers for different requests. We recommend that you use universally unique identifiers (UUIDs).
- Signature: the signature generated after the request is symmetrically encrypted by using the AccessKey secret.

Security Center implements symmetric encryption with an AccessKey pair to verify the identity of the request sender. An AccessKey pair is an identity credential issued to Alibaba Cloud accounts and RAM users that is similar to a logon username and password. An AccessKey pair consists of an AccessKey ID and an AccessKey secret. The AccessKey ID is used to verify the identity of the user, while the AccessKey secret is used to encrypt and verify the signature string. You must keep your AccessKey secret strictly confidential.

Take the DescribeAlarmEventList operation as an example. If the AccessKey ID is `testid` and the AccessKey secret is `testsecret`, the original request URL is as follows:

```
https://tds.aliyuncs.com/?Action=DescribeAlarmEventList
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2018-01-17
&SignatureVersion=1.0
```

Perform the following operations to calculate the signature:

1. Use the request parameters to compose a string-to-sign.

   ```
   GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeAlarmEventList&Format%3DXML&SignatureMeth
   od%3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&SignatureVersion%3
   D1.0&TimeStamp%3D2016-02-23T12%253A46%253A24Z&Version%3D2018-12-03
   ```

   i. Create a canonicalized query string by arranging the request parameters (including all common and operation-specific parameters except Signature) in alphabetical order.

   If you use the GET method to submit a request, the request parameters are included as a part of the URI. The request parameters in the URI are placed after the question mark (?) and separated by ampersands (&).

ii. Encode the canonicalized query string in UTF-8. The following table describes the encoding rules.

Character	Encoding rule
Uppercase letters, lowercase letters, digits, hyphens (-), underscores (_), periods (.),and tildes (~)	These characters do not need to be encoded.
Other characters	These characters must be percent encoded in the `%XY` format. `XY` represents the ASCII code of the characters in hexadecimal notation. For example, double quotation marks (") are encoded as `%22`.
Extended UTF-8 characters	These characters are encoded in the `%XY%ZA...` format.

Spaces	Spaces must be encoded as `%20`. Do not encode spaces as plus signs (+).
	This encoding rule is different from the rule that is used to encode data in the common Multi-purpose Internet Mail Extensions (MIME) format `application/x-www-form-urlencoded`. For example, `java.net.URLEncoder` in the standard Java library is in this MIME format.
	However, you can apply the MIME encoding algorithm and then replace the plus sign (+) in the encoded string with `%20`, the asterisk (*) with `%2A`, and `%7E` with the tilde (~). To do this, you can use the following `percentEncode` method:
	`private static final String ENCODING = "UTF-8";`
	`private static String percentEncode(String value) throws UnsupportedEncodingException`
	`{`
	`return value != null ? URLEncoder.encode(value, ENCODING).replace("+", "%20").replace("*", "%2A").replace("%7E", "~") : null;`
	`}`

iii. Connect the encoded parameter names and values by using equal signs (=).

iv. Sort the parameter name and value pairs in the order specified in Step i. Then, concatenate the pairs with ampersands (&) to construct the canonicalized query string.

2. Calculate the HMAC value of the string-to-sign.

   Append an ampersand (&) after the AccessKey secret as the key to calculate the HMAC value. In this example, the key is `testsecret&`.

   ```
   CT9X0VtwR86fNWSnsc6v8YGOjuE=
   ```

3. Add the signature string to the request as the Signature parameter.

   ```
   https://tds.aliyuncs.com/?Action=DescribeAlarmEventList
   &TimeStamp=2016-02-23T12:46:24Z
   &Format=XML
   &AccessKeyId=testid
   &SignatureMethod=HMAC-SHA1
   &SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
   &Version=2018-12-03
   &SignatureVersion=1.0
   &Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
   ```

Note Alibaba Cloud offers SDKs for multiple programming languages and third-party SDKs to help you calculate the signature. For more information about Alibaba Cloud SDKs, see Alibaba Cloud SDKs.

2.Common parameters

This topic describes common parameters, including common request parameters and common response parameters. Common parameters are required by all API operations.

Common request parameters

Common request parameters must be included in all API requests.

Common request parameters

Parameter	Type	Required	Description
RegionId	string	Yes	The region where the Security Center instance is deployed. Valid values: • *default*: indicates all regions except the Malaysia (Kuala Lumpur) and Singapore (Singapore) regions. Regions in China are included. • *ap-southeast-1*: the Singapore (Singapore) region. The data in the Malaysia (Kuala Lumpur) and Singapore (Singapore) regions is stored in the Singapore (Singapore) region.
Format	string	No	The format in which to return the response. Valid values: JSON and XML. Default value: *JSON*.
Version	String	Yes	The version number of the API. Specify the version number in the YYYY-MM-DD format. Set the value to *2018-12-03*.
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud.
Signature	String	Yes	The signature string of the current request.
SignatureMethod	String	Yes	The encryption method of the signature string. Set the value to *HMAC-SHA1*.
Timestamp	String	Yes	The timestamp of the request. Specify the time in the ISO 8601 standard in the `YYYY-MM-DDThh:mm:ssZ` format. The time must be in UTC. For example, use `2013-01-10T12:00:00Z` to indicate January 10, 2013, 20:00:00 (UTC+8).
SignatureVersion	String	Yes	The version of the signature encryption algorithm. Set the value to 1.0.
SignatureNonce	String	Yes	A unique, random number used to prevent replay attacks. You must use different numbers for different requests.

Parameter	Type	Required	Description
ResourceOwnerAccount	String	No	The Alibaba Cloud account to which the resource you want to access belongs.

Examples

```
https://tds.aliyuncs.com/?Action=DescribeDomainNames
&Timestamp=2014-05-19T10%3A33%3A56Z
&Format=xml
&AccessKeyId=testid
&SignatureMethod=Hmac-SHA1
&SignatureNonce=NwDAxvLU6tFE0DVb
&Version=2018-12-03
&SignatureVersion=1.0
&Signature=Signature
```

Common response parameters

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

Responses can be returned in either the JSON or XML format. You can specify the response format in the request. The default response format is JSON.

Every response returns a unique RequestId regardless of whether the call is successful.

- XML format

```
<?xml version="1.0" encoding="utf-8"?>
    <!--Result Root Node-->
    <Interface Name+Response>
        <!--Return Request Tag-->
        <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
        <!--Return Result Data-->
    </Interface Name+Response>
```

- JSON format

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

3.Container management

3.1. DescribeGroupedContainerInstances

Queries the details about containers by group type.

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	DescribeGroupedContainerInstances	The operation that you want to perform. Set the value to **DescribeGroupedContainerInstances**.
Criteria	String	No	[{"name":"riskStatus","value":"YES"}, {"name":"riskLevel","value":"2"}]	The search conditions. The value of this parameter is in the JSON format. Separate multiple search conditions with commas (,). Example: `[{"name":"riskStatus","value":"YES"}, {"name":"riskLevel","value":"2"}]`. **Note** Supported search conditions include the instance ID, instance name, virtual private cloud (VPC) ID, region, and public IP address. You can call the DescribeCriteria operation to query the supported search conditions.
LogicalExp	String	No	OR	The logical relationship between search conditions. Valid values: • **OR**: The logical relationship between search conditions is **OR**. • **AND**: The logical relationship between search conditions is **AND**.

Parameter	Type	Required	Example	Description
GroupField	String	Yes	pod	The group type used for the query. Valid values: • **pod** • **appName** • **namespace** • **clusterId**
FieldValue	String	No	cas-adad-qeqwe	The keyword used for the search. You must specify this parameter based on the value of the GroupField parameter. • If the **GroupField** parameter is set to **pod**, set this parameter to the name of the pod that you want to query. • If the **GroupField** parameter is set to **appName**, set this parameter to the name of the application that you want to query. • If the **GroupField** parameter is set to **namespace**, set this parameter to the namespace that you want to query. • If the **GroupField** parameter is set to **clusterId**, set this parameter to the ID of the cluster that you want to query. **Note** Fuzzy match is supported.
PageSize	Integer	No	20	The number of entries to return on each page. Default value: **20**. **Note** We recommend that you do not leave this parameter empty.
CurrentPage	Integer	No	1	The number of the page to return. Default value: **1**.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	4E5BFDCF-B9DD-430D-9DA4-151BCB581C9D	The ID of the request, which is used to locate and troubleshoot issues.
PageInfo	Object		The pagination information.
CurrentPage	Integer	1	The page number of the returned page.
PageSize	Integer	20	The number of entries returned per page. Default value: **20**.
TotalCount	Integer	25	The total number of entries returned.
Count	Integer	20	The number of entries returned on the current page.
GroupedContainerInstanceList	Array of GroupedContainerInstance		An array that consists of the details about the container.
RiskLevel	String	low	The risk level. Valid values: • **high** • **medium** • **low**
HostIp	String	172.114.XX.XX	The IP address of the host in the container cluster.
Pod	String	csi-plugin-2n****	The name of the pod.
RiskStatus	String	NO	Indicates whether risks were detected. Valid values: • **NO**: No risks were detected. • **YES**: Risks were detected.
CreateTime	Long	1600076893000	The time when the cluster was created. Unit: milliseconds.

Parameter	Type	Example	Description
Namespace	String	kube-system	The namespace of the cluster.
CusterState	String	running	The status of the cluster. Valid values: • **running**: The cluster is running. • **stopped**: The cluster is stopped. • **deleted**: The cluster is deleted. • **delete_failed**: The cluster fails to be deleted. • **failed**: The cluster fails to be created.
InstanceId	String	i-8vb9ul5xec4tua4q****	The ID of the server.
RegionId	String	cn-hangzhou	The ID of the region in which the instance resides.
AppName	String	oss-liveness-probe	The name of the application.
InstanceCount	Integer	9	The number of queried pods, applications, clusters, or namespaces.
ClusterType	String	ManagedKubernetes	The type of the cluster. Valid values: • **Kubernetes**: dedicated Kubernetes cluster • **ManagedKubernetes**: standard managed cluster (edge cluster) • **Ask**: standard serverless cluster
ClusterName	String	test	The name of the cluster.
PodIp	String	172.114.XX.XX	The IP address of the pod.
VulCount	Integer	1	The number of vulnerabilities that are detected on the current pod, application, namespace, or cluster.
AlarmCount	Integer	1	The number of alerts that are generated on the current pod, application, namespace, or cluster.

Parameter	Type	Example	Description
RiskInstanceCount	Integer	1	The number of at-risk instances.
ClusterId	String	cf3824769c85441b4bf3****	The ID of the cluster.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeGroupedContainerInstances
&Criteria=[{"name":"riskStatus","value":"YES"},{"name":"riskLevel","value":"2"}]
&LogicalExp=OR
&GroupField=pod
&FieldValue=cas-adad-qeqwe
&PageSize=20
&CurrentPage=1
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeGroupedContainerInstancesResponse>
    <RequestId>4E5BFDCF-B9DD-430D-9DA4-151BCB581C9D</RequestId>
    <PageInfo>
        <CurrentPage>1</CurrentPage>
        <PageSize>20</PageSize>
        <TotalCount>25</TotalCount>
        <Count>20</Count>
    </PageInfo>
    <GroupedContainerInstanceList>
        <RiskLevel>low</RiskLevel>
        <HostIp>172.114.XX.XX</HostIp>
        <Pod>csi-plugin-2n****</Pod>
        <RiskStatus>NO</RiskStatus>
        <CreateTime>1600076893000</CreateTime>
        <Namespace>kube-system</Namespace>
        <CusterState>running</CusterState>
        <InstanceId>i-8vb9ul5xec4tua4q****</InstanceId>
        <RegionId>cn-hangzhou</RegionId>
        <AppName>oss-liveness-probe</AppName>
        <InstanceCount>9</InstanceCount>
        <ClusterType>ManagedKubernetes</ClusterType>
        <ClusterName>test</ClusterName>
        <PodIp>172.114.XX.XX</PodIp>
        <VulCount>1</VulCount>
        <AlarmCount>1</AlarmCount>
        <RiskInstanceCount>1</RiskInstanceCount>
        <ClusterId>cf3824769c85441b4bf3****</ClusterId>
    </GroupedContainerInstanceList>
</DescribeGroupedContainerInstancesResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "4E5BFDCF-B9DD-430D-9DA4-151BCB581C9D",
  "PageInfo" : {
    "CurrentPage" : 1,
    "PageSize" : 20,
    "TotalCount" : 25,
    "Count" : 20
  },
  "GroupedContainerInstanceList" : [ {
    "RiskLevel" : "low",
    "HostIp" : "172.114.XX.XX",
    "Pod" : "csi-plugin-2n****",
    "RiskStatus" : "NO",
    "CreateTime" : 1600076893000,
    "Namespace" : "kube-system",
    "CusterState" : "running",
    "InstanceId" : "i-8vb9ul5xec4tua4q****",
    "RegionId" : "cn-hangzhou",
    "AppName" : "oss-liveness-probe",
    "InstanceCount" : 9,
    "ClusterType" : "ManagedKubernetes",
    "ClusterName" : "test",
    "PodIp" : "172.114.XX.XX",
    "VulCount" : 1,
    "AlarmCount" : 1,
    "RiskInstanceCount" : 1,
    "ClusterId" : "cf3824769c85441b4bf3****"
  } ]
}
```

Error codes

HTTP status code	Error code	Error message	Description
400	IllegalParam	Illegal param	The error message returned because the specified parameters are invalid.
500	ServerError	ServerError	The error message returned because a server error occurred.

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

4.Asset exposure analysis

4.1. DescribeExposedStatistics

Queries the exposure statistics of the assets on the Internet.

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	DescribeExposedStatistics	The operation that you want to perform. Set the value to **DescribeExposedStatistics**.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
ExposedAsapVulCount	Integer	1	The total number of high-risk vulnerabilities that are exposed on the Internet and can be exploited by attackers.
ExposedComponentCount	Integer	7	The total number of server components that are exposed on the Internet. The server components include OpenSSL and OpenSSH.
ExposedInstanceCount	Integer	100	The total number of servers that are exposed on the Internet.
ExposedIpCount	Integer	100	The total number of IP addresses that are exposed on the Internet.

Parameter	Type	Example	Description
ExposedLaterVulCount	Integer	5	The total number of medium-risk vulnerabilities that are exposed on the Internet and can be exploited by attackers.
ExposedNntfVulCount	Integer	0	The total number of low-risk vulnerabilities that are exposed on the Internet and can be exploited by attackers.
ExposedPortCount	Integer	6	The total number of ports that are exposed on the Internet.
GatewayAssetCount	Integer	3	The total number of gateway assets that are exposed on the Internet. The gateway assets include Network Address Translation (NAT) gateways and Server Load Balancer (SLB) instances.
RequestId	String	4B897D10-B3CD-4A93-A5FA-591F3ED12A86	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DescribeExposedStatisticsResponse>
      <ExposedPortCount>6</ExposedPortCount>
      <RequestId>4B897D10-B3CD-4A93-A5FA-591F3ED12A86</RequestId>
      <ExposedInstanceCount>100</ExposedInstanceCount>
      <GatewayAssetCount>3</GatewayAssetCount>
      <ExposedLaterVulCount>5</ExposedLaterVulCount>
      <ExposedComponentCount>7</ExposedComponentCount>
      <ExposedIpCount>100</ExposedIpCount>
      <ExposedNntfVulCount>0</ExposedNntfVulCount>
      <ExposedAsapVulCount>1</ExposedAsapVulCount>
</DescribeExposedStatisticsResponse>
```

`JSON` format

```
{
    "ExposedPortCount": 6,
    "RequestId": "4B897D10-B3CD-4A93-A5FA-591F3ED12A86",
    "ExposedInstanceCount": 100,
    "GatewayAssetCount": 3,
    "ExposedLaterVulCount": 5,
    "ExposedComponentCount": 7,
    "ExposedIpCount": 100,
    "ExposedNntfVulCount": 0,
    "ExposedAsapVulCount": 1
}
```


Error codes

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

4.2. DescribeExposedInstanceList

Queries the information about servers that are exposed on the Internet.

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	DescribeExposedInstanceList	The operation that you want to perform. Set the value to **DescribeExposedInstanceList**.
PageSize	Integer	No	20	The number of entries to return on each page. Default value: 20. If you leave this parameter empty, 20 entries will be returned. **Note** We recommend that you do not leave this parameter empty.
CurrentPage	Integer	No	1	The page number of the current page.

Parameter	Type	Required	Example	Description
GroupId	Long	No	9535356	The ID of the server group. **Note** You can call the DescribeAllGroups operation to query the IDs of server groups.
VulStatus	Boolean	No	true	Specifies whether the servers have vulnerabilities. Valid values: • **true** • **false**
ExposureComponent	String	No	openssl	The server component that is exposed on the Internet.
ExposurePort	String	No	22	The port that is exposed on the Internet.
ExposureIp	String	No	116.12.XX.XX	The public IP address of the server.
InstanceId	String	No	i-bp1g6wxdwps7s9dz****	The ID of the server.
InstanceName	String	No	abc_centos7.2_005	The name of the server.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
ExposedInstances	Array of ExposedInstance		The details of the exposures.
AsapVulCount	Integer	0	The number of high-risk vulnerabilities that are exposed on the Internet and can be exploited by attackers.

Parameter	Type	Example	Description
ExposureComponent	String	openssl,openssh	The server component that is exposed on the Internet.
ExposureIp	String	116.12.XX.XX	The public IP address that is exposed to the Internet.
ExposurePort	String	22	The port that is exposed on the Internet.
ExposureType	String	INTERNET_IP	The resource from which the asset is exposed. Valid values: • **INTERNET_IP**: the public IP address of an Elastic Compute Service (ECS) instance • **SLB**: the public IP address of a Server Load Balancer (SLB) instance • **EIP**: the elastic IP address (EIP) • **DNAT**: the Network Address Translation (NAT) gateway that connects to the Internet by using the Destination Network Address Translation (DNAT) feature
ExposureTypeId	String	i-ew11313a****	The ID of the instance to which the resource belongs. The valid values of this parameter vary based on the ExposureType parameter. • If the value of the ExposureType parameter is **INTERNET_IP**, this parameter is empty. • If the value of the ExposureType parameter is **SLB**, the value of this parameter is the ID of the SLB instance. • If the value of the ExposureType parameter is **EIP**, the value of this parameter is the ID of the EIP. • If the value of the ExposureType parameter is **DNAT**, the value of this parameter is the ID of the NAT gateway.
GroupId	Long	9469268	The ID of the server group.
GroupName	String	Ungrouped	The name of the server group.
InstanceId	String	i-bp1g6wxdwps7s9dz****	The ID of the server.

Parameter	Type	Example	Description
InstanceName	String	abc_centos7.2_005	The name of the server.
InternetIp	String	116.12.XX.XX	The public IP address of the server.
IntranetIp	String	192.168.XX.XX	The private IP address of the server.
LaterVulCount	Integer	0	The number of medium-risk vulnerabilities that are exposed on the Internet and can be exploited by attackers.
NntfVulCount	Integer	0	The number of low-risk vulnerabilities that are exposed on the Internet and can be exploited by attackers.
RegionId	String	cn-hangzhou	The ID of the region where the server resides. **Note** For more information about the mapping between the region IDs and region names, see Regions and zones.
TotalVulCount	Integer	0	The total number of vulnerabilities that are exposed on the Internet and can be exploited by attackers.
Uuid	String	dd803d9e-a337-4add-9c5b-7d503e08****	The UUID of the server.
PageInfo	Struct		The page information.
Count	Integer	2	The number of entries returned on the current page.
CurrentPage	Integer	1	The page number of the current page.
PageSize	Integer	20	The number of entries returned per page.

Parameter	Type	Example	Description
TotalCount	Integer	2	The total number of entries about the servers that are exposed on the Internet.
RequestId	String	598A4A61-ABA7-456B-8725-7378258276D9	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DescribeExposedInstanceListResponse>
      <PageInfo>
            <TotalCount>2</TotalCount>
            <PageSize>20</PageSize>
            <CurrentPage>1</CurrentPage>
            <Count>2</Count>
      </PageInfo>
      <RequestId>598A4A61-ABA7-456B-8725-7378258276D9</RequestId>
      <ExposedInstances>
            <TotalVulCount>0</TotalVulCount>
            <GroupName>Ungrouped</GroupName>
            <ExposureType>INTERNET_IP</ExposureType>
            <InstanceId>i-bp1g6wxdwps7s9dz****</InstanceId>
            <ExposureComponent>openssh</ExposureComponent>
            <ExposurePort>22</ExposurePort>
            <AsapVulCount>0</AsapVulCount>
            <NntfVulCount>0</NntfVulCount>
            <IntranetIp>172.16.XX.XX</IntranetIp>
            <GroupId>9535356</GroupId>
            <InstanceName>abc_centos7.2_005</InstanceName>
            <Uuid>dd803d9e-a337-4add-9c5b-7d503e08****</Uuid>
            <InternetIp>47.114.XX.XX</InternetIp>
            <ExposureTypeId></ExposureTypeId>
            <ExposureIp>47.114.XX.XX</ExposureIp>
            <LaterVulCount>0</LaterVulCount>
            <RegionId>cn-hangzhou</RegionId>
      </ExposedInstances>
      <ExposedInstances>
            <TotalVulCount>0</TotalVulCount>
            <GroupName>Ungrouped</GroupName>
            <ExposureType>INTERNET_IP</ExposureType>
            <InstanceId>i-bp1iy78ba3jgjyqp****</InstanceId>
            <ExposureComponent>rdp</ExposureComponent>
            <ExposurePort>3389</ExposurePort>
            <AsapVulCount>0</AsapVulCount>
            <NntfVulCount>0</NntfVulCount>
            <IntranetIp>172.16.XX.XX</IntranetIp>
            <GroupId>9535356</GroupId>
            <InstanceName>efd_centos7.2_005</InstanceName>
            <Uuid>c9782b85-7015-4359-8b75-5e26f854****</Uuid>
            <InternetIp>120.26.XX.XX</InternetIp>
            <ExposureTypeId></ExposureTypeId>
            <ExposureIp>120.26.XX.XX</ExposureIp>
            <LaterVulCount>0</LaterVulCount>
            <RegionId>cn-hangzhou</RegionId>
      </ExposedInstances>
</DescribeExposedInstanceListResponse>
```

`JSON` format

```
{
    "PageInfo": {
        "TotalCount": 2,
        "PageSize": 20,
        "CurrentPage": 1,
        "Count": 2
    },
    "RequestId": "598A4A61-ABA7-456B-8725-7378258276D9",
    "ExposedInstances": [
        {
            "TotalVulCount": 0,
            "GroupName": "Ungrouped",
            "ExposureType": "INTERNET_IP",
            "InstanceId": "i-bp1g6wxdwps7s9dz****",
            "ExposureComponent": "openssh",
            "ExposurePort": "22",
            "AsapVulCount": 0,
            "NntfVulCount": 0,
            "IntranetIp": "172.16.XX.XX",
            "GroupId": 9535356,
            "InstanceName": "abc_centos7.2_005",
            "Uuid": "dd803d9e-a337-4add-9c5b-7d503e08****",
            "InternetIp": "47.114.XX.XX",
            "ExposureTypeId": "",
            "ExposureIp": "47.114.XX.XX",
            "LaterVulCount": 0,
            "RegionId": "cn-hangzhou"
        },
        {
            "TotalVulCount": 0,
            "GroupName": "Ungrouped",
            "ExposureType": "INTERNET_IP",
            "InstanceId": "i-bp1iy78ba3jgjyqp****",
            "ExposureComponent": "rdp",
            "ExposurePort": "3389",
            "AsapVulCount": 0,
            "NntfVulCount": 0,
            "IntranetIp": "172.16.XX.XX",
            "GroupId": 9535356,
            "InstanceName": "efd_centos7.2_005",
            "Uuid": "c9782b85-7015-4359-8b75-5e26f854****",
            "InternetIp": "120.26.XX.XX",
            "ExposureTypeId": "",
            "ExposureIp": "120.26.XX.XX",
            "LaterVulCount": 0,
            "RegionId": "cn-hangzhou"
        }
    ]
}
```


Error codes

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

4.3. DescribeExposedInstanceDetail

Queries the details about a specific server that is exposed on the Internet.

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	DescribeExposedInstanceDetail	The operation that you want to perform. Set the value to **DescribeExposedInstanceDetail**.
Uuid	String	No	fc82b966-4d70-4e01-bf4f-aa4076a5****	The UUID of the server that is exposed on the Internet. **Note** You can call the DescribeExposedInstanceList operation to query the UUIDs of servers.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
ExposedChains	Array of ExposedChain		The detailed information about the asset exposures.
AllVulList	Array of ScaVulRecord		The details of all vulnerabilities on the server.
AliasName	String	Deserialization vulnerability of remote code execution (RCE) in Fastjson 1.2.68 and earlier versions	The alias of the vulnerability.

Parameter	Type	Example	Description
Name	String	SCA:ACSV-2020-052801	The name of the vulnerability.
Necessity	String	asap	The priority to fix the vulnerability. Valid values: • **asap**: high • **later**: medium • **nntf**: low **Note** We recommend that you fix the vulnerabilities that have the **high** priority at the earliest opportunity.
Type	String	sca	The type of the vulnerability. Valid values: • **cve**: Linux software vulnerability • **sys**: Windows system vulnerability • **cms**: Web-CMS vulnerability • **app**: application vulnerability • **emg**: urgent vulnerability • **sca**: middleware vulnerability
Uuid	String	4f9ce097-4a7d-48fe-baef-6960e5b6****	The UUID of the server.
ExposureComponent	String	openssl,openssh	The server component that is exposed on the Internet.
ExposureIp	String	47.99.XX.XX	The public IP address that is exposed on the Internet.
ExposurePort	String	22	The port that is exposed on the Internet.

Parameter	Type	Example	Description
ExposureType	String	INTERNET_IP	The resource from which the asset is exposed. Valid values: • **INTERNET_IP**: the public IP address of an Elastic Compute Service (ECS) instance • **SLB**: the public IP address of a Server Load Balancer (SLB) instance • **EIP**: the elastic IP address (EIP) • **DNAT**: the Network Address Translation (NAT) gateway that connects to the Internet by using the Destination Network Address Translation (DNAT) feature
ExposureTypeId	String	eip-bp1bkgowzam49rld3****	The ID of the instance to which the resource belongs. The valid values of this parameter vary based on the ExposureType parameter. • If the value of the ExposureType parameter is **INTERNET_IP**, this parameter is empty. • If the value of the ExposureType parameter is **SLB**, the value of this parameter is the ID of the SLB instance. • If the value of the ExposureType parameter is **EIP**, the value of this parameter is the ID of the EIP. • If the value of the ExposureType parameter is **DNAT**, the value of this parameter is the ID of the NAT gateway.
InstanceId	String	i-bp116qem8npvchqc****	The ID of the server.
InstanceName	String	worker-k8s-for-cs-c929ee2a145214f89a8b248005be5****	The name of the server.
InternetIp	String	47.99.XX.XX	The public IP address of the server.
IntranetIp	String	192.168.XX.XX	The private IP address of the server.
RealVulList	Array of ScaVulRecord		The information about the vulnerabilities that are exposed on the Internet and can be exploited by attackers.

Parameter	Type	Example	Description
AliasName	String	Deserialization vulnerability of remote code execution (RCE) in Fastjson 1.2.68 and earlier versions	The alias of the vulnerability.
Name	String	SCA:ACSV-2020-052801	The name of the vulnerability.
Necessity	String	asap	The priority to fix the vulnerability. Valid values: • **asap**: high • **later**: medium • **nntf**: low **Note** We recommend that you fix the vulnerabilities that have the **high** priority at the earliest opportunity.
Type	String	sca	The type of the vulnerability. Valid values: • **cve**: Linux software vulnerability • **sys**: Windows system vulnerability • **cms**: Web-CMS vulnerability • **app**: application vulnerability • **emg**: urgent vulnerability • **sca**: middleware vulnerability
Uuid	String	4f9ce097-4a7d-48fe-baef-6960e5b6****	The UUID of the server.
RegionId	String	cn-hangzhou	The ID of the region where the server resides. **Note** For more information about the mapping between the region IDs and region names, see Regions and zones.
Uuid	String	4f9ce097-4a7d-48fe-baef-6960e5b6****	The UUID of the server.

Parameter	Type	Example	Description
RequestId	String	C590482B-54A7-4273-8115-9DBE2DE46B26	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeExposedInstanceDetail
&Uuid=fc82b966-4d70-4e01-bf4f-aa4076a5****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeExposedInstanceDetailResponse>
      <RequestId>C590482B-54A7-4273-8115-9DBE2DE46B26</RequestId>
      <ExposedChains>
            <ExposureType>EIP</ExposureType>
            <InstanceId>i-bp116qem8npvchqc****</InstanceId>
            <ExposureComponent>openssl,openssh</ExposureComponent>
            <ExposurePort>22</ExposurePort>
            <IntranetIp>192.168.XX.XX</IntranetIp>
            <InstanceName>worker-k8s-for-cs-c929ee2a145214f89a8b248005be5****</InstanceName
>
            <RealVulList>
                  <Type>sca</Type>
                  <Uuid>4f9ce097-4a7d-48fe-baef-6960e5b6****</Uuid>
                  <AliasName>Deserialization vulnerability of RCE in Fastjson 1.2.68 and ea
rlier versions</AliasName>
                  <Necessity>asap</Necessity>
                  <Name>SCA:ACSV-2020-052801</Name>
            </RealVulList>
            <AllVulList>
                  <Type>sca</Type>
                  <Uuid>4f9ce097-4a7d-48fe-baef-6960e5b6****</Uuid>
                  <AliasName>Deserialization vulnerability of RCE in Fastjson 1.2.68 and ea
rlier versions</AliasName>
                  <Necessity>asap</Necessity>
                  <Name>SCA:ACSV-2020-052801</Name>
            </AllVulList>
            <AllVulList>
                  <Type>sca</Type>
                  <Uuid>4f9ce097-4a7d-48fe-baef-6960e5b6****</Uuid>
                  <AliasName>Kubernetes kubelet vulnerability caused by resource management
errors</AliasName>
                  <Necessity>nntf</Necessity>
                  <Name>SCA:CVE-2020-8557</Name>
            </AllVulList>
            <Uuid>4f9ce097-4a7d-48fe-baef-6960e5b6****</Uuid>
            <InternetIp>47.99.XX.XX</InternetIp>
            <ExposureIp>47.99.XX.XX</ExposureIp>
            <ExposureTypeId>eip-bp1bkgowzam49rld3****</ExposureTypeId>
            <RegionId>cn-hangzhou</RegionId>
      </ExposedChains>
</DescribeExposedInstanceDetailResponse>
```

`JSON` format

```
{
    "RequestId": "C590482B-54A7-4273-8115-9DBE2DE46B26",
    "ExposedChains": [
        {
            "ExposureType": "EIP",
            "InstanceId": "i-bp116qem8npvchqc****",
            "ExposureComponent": "openssl,openssh",
            "ExposurePort": "22",
            "IntranetIp": "192.168.XX.XX",
            "InstanceName": "worker-k8s-for-cs-c929ee2a145214f89a8b248005be5****",
            "RealVulList": [
                {
                    "Type": "sca",
                    "Uuid": "4f9ce097-4a7d-48fe-baef-6960e5b6****",
                    "AliasName": "Deserialization vulnerability of RCE in Fastjson 1.2.68 a
nd earlier versions",
                    "Necessity": "asap",
                    "Name": "SCA:ACSV-2020-052801"
                }
            ],
            "AllVulList": [
                {
                    "Type": "sca",
                    "Uuid": "4f9ce097-4a7d-48fe-baef-6960e5b6****",
                    "AliasName": "Deserialization vulnerability of RCE in Fastjson 1.2.68 a
nd earlier versions",
                    "Necessity": "asap",
                    "Name": "SCA:ACSV-2020-052801"
                },
                {
                    "Type": "sca",
                    "Uuid": "4f9ce097-4a7d-48fe-baef-6960e5b6****",
                    "AliasName": "Kubernetes kubelet vulnerability caused by resource manag
ement errors",
                    "Necessity": "nntf",
                    "Name": "SCA:CVE-2020-8557"
                }
            ],
            "Uuid": "4f9ce097-4a7d-48fe-baef-6960e5b6****",
            "InternetIp": "47.99.XX.XX",
            "ExposureIp": "47.99.XX.XX",
            "ExposureTypeId": "eip-bp1bkgowzam49rld3****",
            "RegionId": "cn-hangzhou"
        }
    ]
}
```


Error codes

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

4.4. DescribeExposedInstanceCriteria

Queries the search conditions that are used to search for exposed assets.

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	DescribeExposedInstanceCriteria	The operation that you want to perform. Set the value to **DescribeExposedInstanceCriteria**.
Value	String	No	id	The value of the search condition. Fuzzy match is supported.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
CriteriaList	Array of Criteria		The search conditions that are used to search for exposed assets.
Name	String	instanceId	The name of the search condition.
Type	String	select	The type of the search condition. Valid values: • **input**: indicates that you must manually enter the search condition. • **select**: indicates that you must select a search condition from the **Values** drop-down list.

Parameter	Type	Example	Description
Values	String	i-bp19r0fdd39idxhf****	The value of the search condition. This parameter is returned only when the value of the **Type** parameter is **select**. **Note** If the value of the **Type** parameter is **input**, this parameter is empty.
RequestId	String	6D9CDB47-6191-4415-BE63-7E8B12CD4FBE	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DescribeExposedInstanceCriteriaResponse>
      <CriteriaList>
            <Type>input</Type>
            <Values></Values>
            <Name>exposureIp</Name>
      </CriteriaList>
      <CriteriaList>
            <Type>input</Type>
            <Values></Values>
            <Name>exposurePort</Name>
      </CriteriaList>
      <CriteriaList>
            <Type>input</Type>
            <Values></Values>
            <Name>exposureComponent</Name>
      </CriteriaList>
      <CriteriaList>
            <Type>input</Type>
            <Values></Values>
            <Name>instanceName</Name>
      </CriteriaList>
      <CriteriaList>
            <Type>input</Type>
            <Values></Values>
            <Name>instanceId</Name>
      </CriteriaList>
      <RequestId>6D9CDB47-6191-4415-BE63-7E8B12CD4FBE</RequestId>
</DescribeExposedInstanceCriteriaResponse>
```

`JSON` format

```
{
    "CriteriaList": [
        {
            "Type": "input",
            "Values": "",
            "Name": "exposureIp"
        },
        {
            "Type": "input",
            "Values": "",
            "Name": "exposurePort"
        },
        {
            "Type": "input",
            "Values": "",
            "Name": "exposureComponent"
        },
        {
            "Type": "input",
            "Values": "",
            "Name": "instanceName"
        },
        {
            "Type": "input",
            "Values": "",
            "Name": "instanceId"
        }
    ],
    "RequestId": "6D9CDB47-6191-4415-BE63-7E8B12CD4FBE"
}
```


Error codes

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

4.5. DescribeExposedStatisticsDetail

Queries the information about the gateway assets, ports, server components, or public IP addresses that are exposed on the Internet.

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

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeExposedStatisticsDetail	The operation that you want to perform. Set the value to **DescribeExposedStatisticsDetail**.
StatisticsType	String	Yes	exposureType	The type of the exposed asset. Valid values: • **exposureType**: the gateway asset that is exposed on the Internet. • **exposurePort**: the port that is exposed on the Internet. • **exposureComponent**: the server component that is exposed on the Internet. • **exposureIp**: the IP address that is exposed on the Internet.
PageSize	Integer	No	20	The number of entries to return on each page. Default value: 20. **Note** We recommend that you do not leave this parameter empty.
CurrentPage	Integer	No	1	The page number of the current page.
StatisticsTypeInstanceValue	String	No	lb-2ze4rso39h4nczcqs****	The ID of the gateway asset. This parameter takes effect only when **StatisticsType** is set to **exposureType**.
StatisticsTypeGatewayType	String	No	SLB	The type of the gateway asset. This parameter takes effect only when **StatisticsType** is set to **exposureType**. Valid values: • **SLB**: the public IP address of a Server Load Balancer (SLB) instance • **DNAT**: the Network Address Translation (NAT) gateway that connects to the Internet by using the Destination Network Address Translation (DNAT) feature

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
PageInfo	Struct		The page information.
Count	Integer	2	The number of entries returned on the current page.
CurrentPage	Integer	1	The page number of the current page.
PageSize	Integer	20	The number of entries returned per page.
TotalCount	Integer	2	The total number of entries returned.
RequestId	String	7CBAFB3F-1ED7-4A23-986A-6F67F0466BD1	The ID of the request.
StatisticsDetails	Array of StatisticsDetail		The information about the gateway assets, ports, server components, or public IP addresses that are exposed on the Internet.
ExposureComponent	String	tomcat	The server component that is exposed on the Internet.
ExposureIp	String	123.57.XX.XX	The public IP address that is exposed to the Internet.
ExposurePort	String	22	The port that is exposed on the Internet.

Parameter	Type	Example	Description
ExposureType	String	SLB	The resource from which the asset is exposed. Valid values: • **INTERNET_IP**: the public IP address of an Elastic Compute Service (ECS) instance • **SLB**: the public IP address of an SLB instance • **EIP**: the elastic IP address (EIP) • **DNAT**: the NAT gateway that connects to the Internet by using the DNAT feature
ExposureTypeId	String	lb-2ze4rso39h4nczcqs****	The ID of the instance to which the resource belongs. The valid values of this parameter vary based on the ExposureType parameter. • If the value of the **ExposureType** parameter is **INTERNET_IP**, this parameter is empty. • If the value of the **ExposureType** parameter is **SLB**, the value of this parameter is the ID of the SLB instance. • If the value of the **ExposureType** parameter is **EIP**, the value of this parameter is the ID of the EIP. • If the value of the **ExposureType** parameter is **DNAT**, the value of this parameter is the ID of the NAT gateway.
ExposureTypeInstanceName	String	ngw-bp1vkbju8f3w87c9v****	The name of the gateway asset that is exposed on the Internet.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DescribeExposedStatisticsDetailResponse>
      <PageInfo>
            <TotalCount>2</TotalCount>
            <PageSize>20</PageSize>
            <CurrentPage>1</CurrentPage>
            <Count>2</Count>
      </PageInfo>
      <RequestId>7CBAFB3F-1ED7-4A23-986A-6F67F0466BD1</RequestId>
      <StatisticsDetails>
            <ExposureType>SLB</ExposureType>
            <ExposureTypeId>lb-2ze4rso39h4nczcqs****</ExposureTypeId>
      </StatisticsDetails>
      <StatisticsDetails>
            <ExposureType>SLB</ExposureType>
            <ExposureTypeId>lb-bp1g61a2sdn01n5k8****</ExposureTypeId>
      </StatisticsDetails>
</DescribeExposedStatisticsDetailResponse>
```

`JSON` format

```
{
    "PageInfo": {
        "TotalCount": 2,
        "PageSize": 20,
        "CurrentPage": 1,
        "Count": 2
    },
    "RequestId": "7CBAFB3F-1ED7-4A23-986A-6F67F0466BD1",
    "StatisticsDetails": [
        {
            "ExposureType": "SLB",
            "ExposureTypeId": "lb-2ze4rso39h4nczcqs****"
        },
        {
            "ExposureType": "SLB",
            "ExposureTypeId": "lb-bp1g61a2sdn01n5k8****"
        }
    ]
}
```

Error codes

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

5.Virus defense

5.1. StartVirusScanTask

Performs a virus scan task on a server or multiple servers.

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	StartVirusScanTask	The operation that you want to perform. Set the value to **StartVirusScanTask**.

TargetInfo	String	Yes	[{"type":"uuid","name":"Host001","target":"503201a7-14c6-4280-801b-1169ed42****"}]	The asset on which you want to perform a virus scan task. You can select server or server groups to scan for viruses. This parameter is a string that consists of JSON arrays. Each element in a JSON array is a JSON struct that includes the following fields:
				• **type**: the type of the asset on which you want to perform a virus scan task. Valid values:
				  ◦ **groupId**: server group
				  ◦ **uuid**: server
				• **name**: the name of a server or server group.
				• **target**: the asset on which you want to perform a virus scan task.
				  ◦ If **type** is set to **groupId**, the value of this field is the ID of the server group. You can call the DescribeAllGroups operation to query the IDs of server groups.
				  ◦ If **type** is set to **uuid**, the value of this field is the UUID of the server. You can call the DescribeCloudCenterInstances operation to query the UUIDs of servers.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
ScanTaskId	Long	282832	The ID of the virus scan task.
RequestId	String	DAE17926-4ABE-4DBD-9600-DDCB9B200F35	The ID of the request, which is used to locate and troubleshoot issues.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=StartVirusScanTask
&TargetInfo=[{"type":"uuid","name":"Host001","target":"503201a7-14c6-4280-801b-1169ed42****
"}]
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<StartVirusScanTaskResponse>
    <ScanTaskId>282832</ScanTaskId>
    <RequestId>DAE17926-4ABE-4DBD-9600-DDCB9B200F35</RequestId>
</StartVirusScanTaskResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "ScanTaskId" : 282832,
  "RequestId" : "DAE17926-4ABE-4DBD-9600-DDCB9B200F35"
}
```

Error codes

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

5.2. DescribeSuspiciousUUIDConfig

Queries the UUIDs of servers on which proactive defense takes effect based on a specified defense type.

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	DescribeSuspiciousUUIDConfig	The operation that you want to perform. Set the value to **DescribeSuspiciousUUIDConfig**.
Type	String	Yes	alinet	The type of proactive defense. Valid values: • **auto_breaking**: virus defense • **ransomware_breaking**: ransomware capture • **webshell_cloud_breaking**: webshell defense • **alinet**: malicious behavior defense

Response parameters

Parameter	Type	Example	Description
Count	Integer	2	The total number of servers on which proactive defense of the specified type takes effect.
RequestId	String	6044DC07-86F1-5DDA-A611-EC578EA4EEE6	The ID of the request, which is used to locate and troubleshoot issues.
UUIDList	Array of String	"0011ea53-738c-4bff-93be-ce6a1cc9****", "0029c328-53de-40e6-b432-df820f0e****"	The UUIDs of servers on which proactive defense of the specified type takes effect.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeSuspiciousUUIDConfig
&Type=alinet
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeSuspiciousUUIDConfigResponse>
    <Count>2</Count>
    <RequestId>6044DC07-86F1-5DDA-A611-EC578EA4EEE6</RequestId>
    <UUIDList>"0011ea53-738c-4bff-93be-ce6a1cc9****", "0029c328-53de-40e6-b432-df820f0e****
"</UUIDList>
</DescribeSuspiciousUUIDConfigResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "Count" : 2,
  "RequestId" : "6044DC07-86F1-5DDA-A611-EC578EA4EEE6",
  "UUIDList" : [ "\"0011ea53-738c-4bff-93be-ce6a1cc9****\", \"0029c328-53de-40e6-b432-df820
f0e****\"" ]
}
```

Error codes

HTTP status code	Error code	Error message	Description
400	ConsoleError	The error message is %s %s.	The error message is %s %s.
500	ServerError	ServerError	The error message returned because a server error occurred.

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

5.3. DescribeScanTaskProgress

Queries the progress of a virus scan task.

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

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeScanTaskProgress	The operation that you want to perform. Set the value to **DescribeScanTaskProgress**.
TaskId	Long	Yes	282832	The ID of the virus scan task. **Note** You can call the StartVirusScanTask operation to query the IDs of virus scan tasks.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	EA15BA8A-D631-4375-8D40-CB7C769B0279	The ID of the request.
ScanTaskProgress	String	Success	The progress of the virus scan task. Valid values: • **init**: The task is being initialized. • **Processing**: The task is running. • **Success**: The task is complete. • **Failed**: The task fails.

Parameter	Type	Example	Description

TargetInfo	String	[{"type":"uuid","name":"host001","target":"503201a7-14c6-4280-801b-1169ed42****"}]	The information about the asset on which the virus scan task runs. This parameter is a string that consists of JSON arrays. Each element in a JSON array is a JSON struct that includes the following fields:
			• **type**: the type of the asset on which the virus scan task runs. Valid values:
			  ◦ **groupId**: server group
			  ◦ **uuid**: server
			• **name**: the name of a server group or server
			• **target**: the asset on which the virus scan task runs.
			  ◦ If **type** is set to **groupId**, the value of this field is the ID of the server group.
			  ◦ If **type** is set to **uuid**, the value of this field is the universally unique identifier (UUID) of the server.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeScanTaskProgress
&TaskId=282832
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeScanTaskProgressResponse>
      <TargetInfo>[{"type":"uuid","name":"host001","target":"503201a7-14c6-4280-801b-1169ed42****"}]</TargetInfo>
      <RequestId>EA15BA8A-D631-4375-8D40-CB7C769B0279</RequestId>
      <ScanTaskProgress>Success</ScanTaskProgress>
</DescribeScanTaskProgressResponse>
```

`JSON` format

```
{
 "TargetInfo": "[{\"type\":\"uuid\",\"name\":\"host001\",\"target\":\"503201a7-14c6-4280-801b-1169ed42****\"}]",
 "RequestId": "EA15BA8A-D631-4375-8D40-CB7C769B0279",
 "ScanTaskProgress": "Success"
}
```

Error codes

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

6.protection against ransomware

6.1. AutoBuyBackupProduct

Enables the anti-ransomware feature.

Prerequisites

- Your Alibaba Cloud account is used to log on to the Security Center console.
- Your Alibaba Cloud account passed real-name verification.

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	AutoBuyBackupProduct	The operation that you want to perform. Set the value to **AutoBuyBackupProduct**.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D0D6E6E4-CB8C-4897-B852-46AEFDA04B21	The ID of the request, which is used to locate and troubleshoot issues.

Examples

Sample requests

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

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<AutoBuyBackupProductResponse>
    <RequestId>D0D6E6E4-CB8C-4897-B852-46AEFDA04B21</RequestId>
</AutoBuyBackupProductResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "D0D6E6E4-CB8C-4897-B852-46AEFDA04B21"
}
```

Error codes

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

6.2. InstallBackupClient

Installs the anti-ransomware agent on your server.

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	InstallBackupClient	The operation that you want to perform. Set the value to **InstallBackupClient**.
Uuid	String	No	inet-617eddab-7df4-4a51-b217-a3f59194****	The UUID of the server on which you want to install the anti-ransomware agent. **Note** You must specify at least one of the UuidList.N and Uuid parameters.
PolicyVersion	String	Yes	2.0.0	The version of the anti-ransomware policy. You can call the DescribeBackupPolicies operation to query the versions of anti-ransomware policies. Valid values: • **1.0.0** • **2.0.0**

Parameter	Type	Required	Example	Description
UuidList.N	String	No	["3bb30859-b3b5-4f28-868f-b0892c98****", "3bb30859-b3b5-4f28-868f-b0892c98****"]	The UUIDs of the servers on which you want to install the anti-ransomware agent. You can call the DescribeCloudCenterInstances operation to query the UUIDs of servers. **Note** You must specify at least one of the UuidList.N and Uuid parameters.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D0D6E6E4-CB8C-4897-B852-46AEFDA04B21	The ID of the request, which is used to locate and troubleshoot issues.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=InstallBackupClient
&Uuid=inet-617eddab-7df4-4a51-b217-a3f59194****
&PolicyVersion=2.0.0
&UuidList=["[\"3bb30859-b3b5-4f28-868f-b0892c98****\", \"3bb30859-b3b5-4f28-868f-b0892c98****\"]"]
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<InstallBackupClientResponse>
    <RequestId>D0D6E6E4-CB8C-4897-B852-46AEFDA04B21</RequestId>
</InstallBackupClientResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "D0D6E6E4-CB8C-4897-B852-46AEFDA04B21"
}
```

Error codes

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

6.3. UninstallBackupClient

Uninstalls the anti-ransomware agent from a server.

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	UninstallBackupClient	The operation that you want to perform. Set the value to **UninstallBackupClient**.
Uuid	String	No	D0D6E6E4-CB8C-4897-B852-46AEFDA0****	The UUID of the server from which you want to uninstall the anti-ransomware agent. **Note** You must specify at least one of the UuidList.N and Uuid parameters.
PolicyVersion	String	Yes	2.0.0	The version of the anti-ransomware policy. You can call the DescribeBackupPolicies operation to query the versions of anti-ransomware policies. Valid values: • **1.0.0** • **2.0.0**

Parameter	Type	Required	Example	Description
UuidList.N	String	No	["D0D6E6E4-CB8C-4897-B852-46AEFDA0****", "3bb30859-b3b5-4f28-868f-b0892c98****"]	The UUIDs of the servers from which you want to uninstall the anti-ransomware agent. **Note** You must specify at least one of the UuidList.N and Uuid parameters.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	"8eec3b63-18af-454b-8c17-aabcf7190b70","fb711b59-d49c-4da7-a36f-9a56fb705fbe"	The ID of the request, which is used to locate and troubleshoot issues.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=UninstallBackupClient
&Uuid=D0D6E6E4-CB8C-4897-B852-46AEFDA0****
&PolicyVersion=2.0.0
&UuidList=["[\"D0D6E6E4-CB8C-4897-B852-46AEFDA0****\", \"3bb30859-b3b5-4f28-868f-b0892c98****\"]"]
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<UninstallBackupClientResponse>
    <RequestId>"8eec3b63-18af-454b-8c17-aabcf7190b70","fb711b59-d49c-4da7-a36f-9a56fb705fbe"</RequestId>
</UninstallBackupClientResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "\"8eec3b63-18af-454b-8c17-aabcf7190b70\",\"fb711b59-d49c-4da7-a36f-9a56fb705fbe\""
}
```

Error codes

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

6.4. CreateBackupPolicy

Creates an anti-ransomware policy.

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	CreateBackupPolicy	The operation that you want to perform. Set the value to **CreateBackupPolicy**.
Name	String	Yes	Server anti-ransomware policy 01	The name of the anti-ransomware policy.

				• **IsDefault**: the type of the anti-ransomware policy. Valid values:
				  ◦ **1**: a recommended policy
				  ◦ **0**: a custom policy
				• **Include**: the format of the files that you want to protect. If you want to protect the files in all formats, set this field to **[]**.
				• **Source**: the directory that you want to protect. If you want to protect all directories, set this field to **[]**.
				• **ExcludeSystemPath**: specifies whether to exclude a specific directory from the anti-ransomware policy. If you want to exclude a directory, set this field to **true**. If you do not exclude a directory, you can leave this field empty.

Parameter	Type	Required	Example	Description

Policy	Map	Yes	{"IsDefault":1,"Include":[],"Source":[],"Schedule":"I|1648061040|PT24H","Retention":7,"SpeedLimiter":"","ExcludeSystemPath":true,"Exclude":["/bin/","/usr/bin/","/sbin/","/boot/","/proc/","/sys/","/srv/","/lib/","/selinux/","/usr/sbin/","/run/","/lib32/","/lib64/","/lost+found/","/var/lib/kubelet/","/var/lib/ntp/proc","/var/lib/container","Windows","Python27","Program Files (x86)","Program Files","Boot","$RECYCLE.BIN","System Volume Information","Users\Administrator\NTUSER.DAT*","ProgramData","pagefile.sys","Users\Default\NTUSER.DAT*","Users\Administrator\ntuser.*"],"UseVss":true}"	• **Exclude**: the directory that you want to exclude from the anti-ransomware policy. If you do not exclude a directory, set this field to **[]**.
				• **Schedule**: the start time and interval of a data backup task. We recommend that you specify a start time that begins during off-peak hours but does not start on the hour.
				  ○ If you set this field to I|1583216092|P21D, the data backup task starts from 2020-03-03 14:14:52, and the task is run at an interval of three weeks.
				  ○ If you set this field to I|1583216092|PT24H, the data backup task starts from 2020-03-03 14:14:52, and the task is run at an interval of 24 hours.
				• **Retention**: the period during which backup data is retained. Unit: days. If you set this field to 7, backup data is retained for a week. If you set this field to 365, backup data is retained for a year. If you set this field to -1, backup data is permanently retained.
				• **SpeedLimiter**: the limit on the network bandwidth for data backup tasks. If you set this field to 0:24:30720, the maximum bandwidth for a data backup task is 30 MB/s from 00:00 to 24:00.
				• **UseVss**: specifies whether to enable the VSS feature that is available only for Windows servers. Valid values:
				  ○ **true**: yes
				  ○ **false**: no

Parameter	Type	Required	Example	Description
				Note The VSS feature is available only if you create the anti-ransomware policy for Windows servers. After you enable the feature, the number of backup failures due to running processes is significantly reduced. We recommend that you enable the VSS feature. After you enable the feature, the data of disks that are in the exFAT and FAT32 formats cannot be backed up.
PolicyVersion	String	Yes	2.0.0	The version of the anti-ransomware policy. Set the value to 2.0.0.
PolicyRegionId	String	No	ch-hangzhou	The region ID of the server that is not deployed on Alibaba Cloud. Note Specify the ID of the supported region that is the nearest to the region of the server. You can call the DescribeSupportRegion operation to query the supported regions of the anti-ransomware feature.
UuidList.N	String	Yes	["3bb30859-b3b5-4f28-868f-b0892c98****", "3bb30859-b3b5-4f28-868f-b0892c98****"]	The UUIDs of the servers that you want to protect. Separate multiple UUIDs with commas (,). Note You can call the DescribeCloudCenterInstances operation to query the UUIDs of servers.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	24A20733-10A0-4AF6-BE6B-E3322413BB68	The ID of the request, which is used to locate and troubleshoot issues.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CreateBackupPolicy
&Name=Server anti-ransomware policy 01
&PolicyVersion=2.0.0
&PolicyRegionId=ch-hangzhou
&UuidList=["[\"3bb30859-b3b5-4f28-868f-b0892c98****\", \"3bb30859-b3b5-4f28-868f-b0892c98****\"]"]
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<CreateBackupPolicyResponse>
    <RequestId>24A20733-10A0-4AF6-BE6B-E3322413BB68</RequestId>
</CreateBackupPolicyResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "24A20733-10A0-4AF6-BE6B-E3322413BB68"
}
```

Error codes

HTTP status code	Error code	Error message	Description
500	ServerError	ServerError	The error message returned because a server error occurred.

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

6.5. DeleteBackupPolicy

Deletes an anti-ransomware policy.

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	DeleteBackupPolicy	The operation that you want to perform. Set the value to **DeleteBackupPolicy**.
Id	Long	Yes	12	The ID of the anti-ransomware policy that you want to delete.
PolicyVersion	String	Yes	2.0.0	The version of the anti-ransomware policy that you want to delete. You can call the DescribeBackupPolicies operation to query the versions of anti-ransomware policies. Valid values: • **1.0.0** • **2.0.0**

Response parameters

Parameter	Type	Example	Description
RequestId	String	24A20733-10A0-4AF6-BE6B-E3322413BB68	The ID of the request, which is used to locate and troubleshoot issues.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DeleteBackupPolicy
&Id=12
&PolicyVersion=2.0.0
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DeleteBackupPolicyResponse>
    <RequestId>24A20733-10A0-4AF6-BE6B-E3322413BB68</RequestId>
</DeleteBackupPolicyResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "24A20733-10A0-4AF6-BE6B-E3322413BB68"
}
```

Error codes

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

6.6. DeleteBackupPolicyMachine

Deletes the server to which a specific anti-ransomware policy is applied.

After the call is successful, the server is deleted from the list of servers to which the anti-ransomware policy is applied.

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	DeleteBackupPolicyMachine	The operation that you want to perform. Set the value to **DeleteBackupPolicyMachine**.
PolicyId	Long	Yes	11	The ID of the anti-ransomware policy.
PolicyVersion	String	Yes	2.0.0	The version of the policy. Valid values: • **1.0.0**: If you delete a V1.0.0 anti-ransomware policy that is applied to servers, the anti-ransomware agent is also uninstalled from the servers. • **2.0.0**: If you delete a V2.0.0 anti-ransomware policy that is applied to servers, the anti-ransomware agent is not uninstalled from the servers.

Parameter	Type	Required	Example	Description
Uuid	String	No	D0D6E6E4-CB8C-4897-B852-46AEFDA0****	The UUID of the server to which the anti-ransomware policy is applied. **Note** You must specify at least one of the `UuidList.N` and `UUID` parameters.
UuidList.N	RepeatList	No	["D0D6E6E4-CB8C-4897-B852-46AEFDA0****","D0D6E6E4-CB8C-4897-B852-46AEFDA0****"]	The UUIDs of the servers to which the protection policy is applied. **Note** You must specify at least one of the `UuidList.N` and `UUID` parameters.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D0D6E6E4-CB8C-4897-B852-46AEFDA04B21	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DeleteBackupPolicyMachineResponse>
  <RequestId>D0D6E6E4-CB8C-4897-B852-46AEFDA04B21</RequestId>
</DeleteBackupPolicyMachineResponse>
```

`JSON` format

```
{
    "RequestId": "D0D6E6E4-CB8C-4897-B852-46AEFDA04B21"
}
```

Error codes

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

6.7. ModifyBackupPolicy

Modifies an anti-ransomware policy.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyBackupPolicy	The operation that you want to perform. Set the value to **ModifyBackupPolicy**.
Id	Long	Yes	11	The ID of the anti-ransomware policy that you want to modify.
Name	String	Yes	policy_name_A	The name of the anti-ransomware policy that you want to modify.
				The configurations of the anti-ransomware policy that you want to modify. The value is a JSON string that contains the following fields: • **Source**: the directory that you want to protect after the modification. If you want to protect all directories, set this field to brackets []. • **Include**: the format of the file that you want to protect after the modification. Examples: *.jpg and *.doc. • **Exclude**: the directory that you want to exclude from the anti-ransomware policy after the modification.You can call the DescribeExcludeSystemPath operation to query all directories and specify the directory that you want to exclude. For example, to exclude the /home/user directory, set the value to "/home/user".

Parameter	Type	Required	Example	Description
Policy	Json	Yes	null	• **Schedule**: the start time and interval of a data backup task after the modification. We recommend that you specify a start time that begins during off-peak hours but does not start on the hour. ◦ If you set this field to I|1583216092|P21D, the data backup task starts from 2020-03-03 14:14:52, and the task is run at an interval of three weeks. ◦ If you set this field to I|1583216092|PT24H, the data backup task starts from 2020-03-03 14:14:52, and the task is run at an interval of 24 hours. • **Retention**: the period during which backup data is retained. Unit: days. If you set this field to 7, backup data is retained for a week. If you set this field to 365, backup data is retained for a year. If you set this field to -1, backup data is permanently retained. • **SpeedLimiter**: the limit on the network bandwidth for data backup tasks. If you set this field to 12:15:15360|6:12:5120, the maximum bandwidth for a data backup task is 15 Mbit/s from 12:00 to 15:00 and 5 Mbit/s from 06:00 to 12:00. If you back up data on an Elastic Compute Service (ECS) instance that resides in an internal network, we recommend that you leave this field empty. If this field is left empty, the bandwidth for a data backup task is unlimited.
UuidList.N	RepeatList	Yes	["3bb30859-b3b5-4f28-868f-b0892c98****", "3bb30859-b3b5-4f28-868f-b0892c98****"]	The UUIDs of servers to which the anti-ransomware policy is applied.

Parameter	Type	Required	Example	Description
PolicyVersion	String	No	2.0.0	The version of the anti-ransomware policy. You can call the DescribeBackupPolicies operation to query the versions of anti-ransomware policies. • 1.0.0 • 2.0.0
PolicyRegionId	String	No	cn-hangzhou	The region ID of the server to which the anti-ransomware policy is applied. You can call the DescribeSupportRegion operation to query the regions in which the anti-ransomware feature is supported.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D0D6E6E4-CB8C-4897-B852-46AEFDA04B21	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<ModifyBackupPolicy>
  <RequestId>D0D6E6E4-CB8C-4897-B852-46AEFDA04B21</RequestId>
</ModifyBackupPolicy>
```

`JSON` format

```
{
    "RequestId": "D0D6E6E4-CB8C-4897-B852-46AEFDA04B21"
}
```

Error codes

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

6.8. ModifyBackupPolicyStatus

Enables or disables an anti-ransomware policy.

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	ModifyBackupPolicyStatus	The operation that you want to perform. Set the value to **ModifyBackupPolicyStatus**.
Id	Long	Yes	30490	The ID of the anti-ransomware policy that you want to enable or disable.
Status	String	Yes	enabled	Specifies whether to enable or disable the anti-ransomware policy. Valid values: • **enabled**: enables the anti-ransomware policy. After you enable the anti-ransomware policy, the anti-ransomware feature protects data on your servers. Data on your servers is backed up based on the policy. • **disabled**: disables the anti-ransomware policy. After you disable the anti-ransomware policy, the data backup task that is running based on the policy stops. **Note** When the system runs data backup tasks, your network bandwidth is consumed. We recommend that you enable the anti-ransomware policy during peak-off hours to back up data.

Parameter	Type	Required	Example	Description
PolicyVersion	String	Yes	2.0.0	The version of the anti-ransomware policy. Set the value to **2.0.0**.

Response parameters

Parameter	Type	Example	Description
RequestId	String	E342452B-4401-5F74-9A1B-D24479851173	The ID of the request, which is used to locate and troubleshoot issues.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyBackupPolicyStatus
&Id=30490
&Status=enabled
&PolicyVersion=2.0.0
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyBackupPolicyStatusResponse>
    <RequestId>E342452B-4401-5F74-9A1B-D24479851173</RequestId>
</ModifyBackupPolicyStatusResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "E342452B-4401-5F74-9A1B-D24479851173"
}
```

Error codes

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

6.9. DescribeBackupRestoreCount

Queries the statistics of a restoration task.

If you have created restoration tasks, you can call this operation to query the numbers of restoration tasks that are in the **restored** or **being restored** state.

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	DescribeBackupRestoreCount	The operation that you want to perform. Set the value to **DescribeBackupRestoreCount**.

Response parameters

Parameter	Type	Example	Description
RequestId	String	ECC6B3E3-D496-512D-B46D-E6996A6B63EE	The ID of the request, which is used to locate and troubleshoot issues.
BackupRestoreCount	Object		The statistics of the restoration task.
Total	Integer	30	The total number of the restoration tasks that you create.
Recovering	Integer	3	The number of the restoration tasks that are in the **being restored** state.

Examples

Sample requests

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

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeBackupRestoreCountResponse>
    <RequestId>ECC6B3E3-D496-512D-B46D-E6996A6B63EE</RequestId>
    <BackupRestoreCount>
        <Total>30</Total>
        <Recovering>3</Recovering>
    </BackupRestoreCount>
</DescribeBackupRestoreCountResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "ECC6B3E3-D496-512D-B46D-E6996A6B63EE",
  "BackupRestoreCount" : {
    "Total" : 30,
    "Recovering" : 3
  }
}
```

Error codes

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

6.10. DescribeRestoreJobs

Queries the details about a restoration task.

If the data on your servers is encrypted by ransomware, you can create a restoration task to restore the data on your servers by using backup data in Security Center.

> **Note** After you enable an anti-ransomware policy, the data on your servers is backed up based on the policy. For more information about anti-ransomware policies, see Manage protection policies.

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	DescribeRestoreJobs	The operation that you want to perform. Set the value to **DescribeRestoreJobs**.

Parameter	Type	Required	Example	Description
Status	String	No	RUNNING	The status of the restoration task. Valid values: • **RUNNING**: The task is running. • **COMPLETE**: The task is complete. • **FAILED**: The task fails. • **CANCELING**: The task is being canceled. • **CANCELED**: The task is canceled. • **PARTIAL_COMPLETE**: The task is partially successful. • **CREATED**: The task was created but is not run. • **EXPIRED**: The task is not updated. • **QUEUED**: The task is waiting to be run. • **CLIENT_DELETED**: The task fails because the anti-ransomware agent is uninstalled.
MachineRemark	String	No	1.1.XX.XX	The unique identifier of the server on which the restoration task is run. For example, you can use the IP address or the name of the server.
PageSize	Integer	Yes	10	The number of entries to return on each page. Default value: **10**.
CurrentPage	Integer	Yes	1	The number of the page to return. Default value: **1**.

Response parameters

Parameter	Type	Example	Description
RequestId	String	0ED92280-4363-57D3-A4D3-4D3FBC99B29F	The ID of the request, which is used to locate and troubleshoot issues.
PageInfo	Object		The pagination information.
CurrentPage	Integer	1	The page number of the returned page.

Parameter	Type	Example	Description
PageSize	Integer	10	The number of entries returned per page. Default value: **10**.
TotalCount	Integer	69	The total number of restoration tasks returned.
Count	Integer	2	The number of restoration tasks returned on the current page.
RestoreJobs	Array of RestoreJob		The details about the restoration task.
Status	String	COMPLETE	The status of the restoration task. Valid values: • **RUNNING**: The task is running. • **COMPLETE**: The task is complete. • **FAILED**: The task fails. • **CANCELING**: The task is being canceled. • **CANCELED**: The task is canceled. • **PARTIAL_COMPLETE**: The task is partially successful. • **CREATED**: The task was created but is not run. • **EXPIRED**: The task is not updated. • **QUEUED**: The task is waiting to be run. • **CLIENT_DELETED**: The task fails because the anti-ransomware agent is uninstalled.
SnapshotHash	String	a3992de83f529b844135fe795d949181735a7d20e0ac8539485c61b7983e618f	The hash value of the backup data.
SourceClientId	String	c-000gmcypy5dyf9ey3uv7	The ID of the anti-ransomware agent that is used to back up data.
ErrorFileUrl	String	["/home/user"]	The URL of the CSV file that contains the files failed to be restored.
Includes	String	["/root/disk-uuid-test","/root/install.sh"]	The directory included in the file that is restored. This parameter is specified when you create the anti-ransomware policy. The value is a directory that requires protection.

Parameter	Type	Example	Description
RestoreName	String	Restore	The name of the restoration task.
InternetIp	String	1.1.XX.XX	The public IP address of the server whose data is stored.
VaultId	String	v-000b0v0jqzmse2yz06zw	The ID of the repository in which the backup data is stored.
ActualBytes	Long	20	The size of data that is restored. Unit: bytes.
Message	String	successful	The returned error code.
Percentage	Integer	100	The progress of the restoration task in percentage.
GmtModified	String	2021-04-25T19:11Z	The time when the restoration task is updated.
RestoreType	String	ECS_FILE	The type of the file that is restored. Valid values: • **ECS_FILE**: files on Elastic Compute Service (ECS) instances • **FILE**: files on servers in data centers
ExitCode	String	0	The return value of the restoration task.
ClientId	String	c-000frxwusjauhp9ajpu6	The ID of the anti-ransomware agent.
ItemsDone	Long	0	The number of files that are backed up.
BytesTotal	Long	20	The total size of data that you want to restore. Unit: bytes.
RequestId	String	0ED92280-4363-57D3-A4D3-4D3FBC99B29F	The ID of the request, which is used to locate and troubleshoot issues.

Parameter	Type	Example	Description
InstanceName	String	win2012-01	The name of the server whose data you want to restore.
CompleteTime	Long	1583289054000	The timestamp when the restoration task is complete. Unit: milliseconds.
ErrorType	String	NONE	The error code that is returned for the restoration task.
SnapshotVersion	String	2020-03-03 18:00	The version of the backup file.
Target	String	/home	The folder in which the backup data is stored. After you create the restoration task, the backup data is restored to the specified folder.
CreatedTime	Long	1583289052000	The timestamp when the restoration task is created. Unit: milliseconds.
InstanceId	String	i-bp12xnvdax6307gw****	The ID of the server whose data you want to restore.
Source	String	["/home/admin","\\\\servername\\sharename"]	The path to the file that you want to back up.
IntranetIp	String	2.1.XX.XX	The internal IP address of the server whose data you want to restore.
ErrorFile	String	s-000f4wxm8f7gur6g2otm.csv	The name of the CSV file that contains the files failed to be restored.
Uuid	String	6E3DABB6-3F6A-40DB-9492-2C8B59C****	The UUID of the server whose data you want to restore.
Excludes	String	["/home/user"]	The directory excluded from the file that is restored. This parameter is specified when you create the anti-ransomware policy. The value is a directory that does not require protection.

Parameter	Type	Example	Description
Speed	Long	25766558	The speed of data backup. Unit: byte/s.
SnapshotId	String	s-000gmcypy5dy54e39yny	The hash value ID of the backup data.
UpdatedTime	Long	1583289054000	The timestamp when the restoration task was last updated. Unit: milliseconds.
RestoreId	String	r-000gmcypy5dyf9ey3uv7	The ID of the restoration task.
GmtCreate	String	2021-04-25T19:11Z	The time when the restoration task is created.
Eta	Long	1583299054	The timestamp when the in-progress restoration task is expected to be complete. Unit: seconds.
Duration	Long	100	The duration of the restoration task. Unit: seconds.
ErrorCount	Long	0	The number of the restoration tasks on which errors occur.
ItemsTotal	Long	0	The total number of files that you want to back up.
BytesDone	Long	20	The total size of data that is restored. Unit: bytes.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeRestoreJobs
&Status=RUNNING
&MachineRemark=1.1.XX.XX
&PageSize=10
&CurrentPage=1
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeRestoreJobsResponse>
    <RequestId>0ED92280-4363-57D3-A4D3-4D3FBC99B29F</RequestId>
    <PageInfo>
        <CurrentPage>1</CurrentPage>
        <PageSize>10</PageSize>
        <TotalCount>69</TotalCount>
        <Count>2</Count>
    </PageInfo>
    <RestoreJobs>
        <Status>COMPLETE</Status>
        <SnapshotHash>a3992de83f529b844135fe795d949181735a7d20e0ac8539485c61b7983e618f</Sna
pshotHash>
        <SourceClientId>c-000gmcypy5dyf9ey3uv7</SourceClientId>
        <ErrorFileUrl>["/home/user"]</ErrorFileUrl>
        <Includes>["/root/disk-uuid-test","/root/install.sh"]</Includes>
        <RestoreName>Restore</RestoreName>
        <InternetIp>1.1.XX.XX</InternetIp>
        <VaultId>v-000b0v0jqzmse2yz06zw</VaultId>
        <ActualBytes>20</ActualBytes>
        <Message>successful</Message>
        <Percentage>100</Percentage>
        <GmtModified>2021-04-25T19:11Z</GmtModified>
        <RestoreType>ECS_FILE</RestoreType>
        <ExitCode>0</ExitCode>
        <ClientId>c-000frxwusjauhp9ajpu6</ClientId>
        <ItemsDone>0</ItemsDone>
        <BytesTotal>20</BytesTotal>
        <RequestId>0ED92280-4363-57D3-A4D3-4D3FBC99B29F</RequestId>
        <InstanceName>win2012-01</InstanceName>
        <CompleteTime>1583289054000</CompleteTime>
        <ErrorType>NONE</ErrorType>
        <SnapshotVersion>2020-03-03 18:00</SnapshotVersion>
        <Target>/home</Target>
        <CreatedTime>1583289052000</CreatedTime>
        <InstanceId>i-bp12xnvdax6307gw****</InstanceId>
        <Source>["/home/admin","\\\\servername\\sharename"]</Source>
        <IntranetIp>2.1.XX.XX</IntranetIp>
        <ErrorFile>s-000f4wxm8f7gur6g2otm.csv</ErrorFile>
        <Uuid>6E3DABB6-3F6A-40DB-9492-2C8B59C****</Uuid>
        <Excludes>["/home/user"]</Excludes>
        <Speed>25766558</Speed>
        <SnapshotId>s-000gmcypy5dy54e39yny</SnapshotId>
        <UpdatedTime>1583289054000</UpdatedTime>
        <RestoreId>r-000gmcypy5dyf9ey3uv7</RestoreId>
        <GmtCreate>2021-04-25T19:11Z</GmtCreate>
        <Eta>1583299054</Eta>
        <Duration>100</Duration>
        <ErrorCount>0</ErrorCount>
        <ItemsTotal>0</ItemsTotal>
        <BytesDone>20</BytesDone>
```

```
    </RestoreJobs>
</DescribeRestoreJobsResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "0ED92280-4363-57D3-A4D3-4D3FBC99B29F",
  "PageInfo" : {
    "CurrentPage" : 1,
    "PageSize" : 10,
    "TotalCount" : 69,
    "Count" : 2
  },
  "RestoreJobs" : [ {
    "Status" : "COMPLETE",
    "SnapshotHash" : "a3992de83f529b844135fe795d949181735a7d20e0ac8539485c61b7983e618f",
    "SourceClientId" : "c-000gmcypy5dyf9ey3uv7",
    "ErrorFileUrl" : "[\"/home/user\"]",
    "Includes" : "[\"/root/disk-uuid-test\",\"/root/install.sh\"]",
    "RestoreName" : "Restore",
    "InternetIp" : "1.1.XX.XX",
    "VaultId" : "v-000b0v0jqzmse2yz06zw",
    "ActualBytes" : 20,
    "Message" : "successful",
    "Percentage" : 100,
    "GmtModified" : "2021-04-25T19:11Z",
    "RestoreType" : "ECS_FILE",
    "ExitCode" : "0",
    "ClientId" : "c-000frxwusjauhp9ajpu6",
    "ItemsDone" : 0,
    "BytesTotal" : 20,
    "RequestId" : "0ED92280-4363-57D3-A4D3-4D3FBC99B29F",
    "InstanceName" : "win2012-01",
    "CompleteTime" : 1583289054000,
    "ErrorType" : "NONE",
    "SnapshotVersion" : "2020-03-03 18:00",
    "Target" : "/home",
    "CreatedTime" : 1583289052000,
    "InstanceId" : "i-bp12xnvdax6307gw****",
    "Source" : "[\"/home/admin\",\"\\\\\\\\\\servername\\\\sharename\"]",
    "IntranetIp" : "2.1.XX.XX",
    "ErrorFile" : "s-000f4wxm8f7gur6g2otm.csv",
    "Uuid" : "6E3DABB6-3F6A-40DB-9492-2C8B59C****",
    "Excludes" : "[\"/home/user\"]",
    "Speed" : 25766558,
    "SnapshotId" : "s-000gmcypy5dy54e39yny",
    "UpdatedTime" : 1583289054000,
    "RestoreId" : "r-000gmcypy5dyf9ey3uv7",
    "GmtCreate" : "2021-04-25T19:11Z",
    "Eta" : 1583299054,
    "Duration" : 100,
    "ErrorCount" : 0,
    "ItemsTotal" : 0,
    "BytesDone" : 20
  } ]
}
```

Error codes

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

6.11. DescribeUserBackupMachines

Queries the information about the servers to which an anti-ransomware policy is applied.

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	DescribeUserBackupMachines	The operation that you want to perform. Set the value to **DescribeUserBackupMachines**.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D0D6E6E4-CB8C-4897-B852-46AEFDA04B21	The ID of the request, which is used to locate and troubleshoot issues.
Machines	Array of SimpleBackupMachine		The information about the server to which the anti-ransomware policy is applied.
Uuid	String	D0D6E6E4-CB8C-4897-B852-46AEFDA0****	The UUID of the server to which the anti-ransomware policy is applied.
PolicyName	String	policy_name_A	The name of the anti-ransomware policy that is applied to the server.
Id	Long	123	The ID of the anti-ransomware policy that is applied to the server.

Examples

Sample requests

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

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeUserBackupMachinesResponse>
<RequestId>D0D6E6E4-CB8C-4897-B852-46AEFDA04B21</RequestId>
<Machines>
    <Uuid>D0D6E6E4-CB8C-4897-B852-46AEFDA0****</Uuid>
    <PolicyName>policy_name_A</PolicyName>
    <Id>123</Id>
</Machines>
</DescribeUserBackupMachinesResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "D0D6E6E4-CB8C-4897-B852-46AEFDA04B21",
  "Machines" : {
    "Uuid" : "D0D6E6E4-CB8C-4897-B852-46AEFDA0****",
    "PolicyName" : "policy_name_A",
    "Id" : 123
  }
}
```

Error codes

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

6.12. DescribeSupportRegion

Queries the region in which the anti-ransomware feature is supported.

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	DescribeSupportRegion	The operation that you want to perform. Set the value to **DescribeSupportRegion**.

Response parameters

Parameter	Type	Example	Description
RequestId	String	2C0699D3-4107-5A46-A4C4-E129A5967788	The ID of the request, which is used to locate and troubleshoot issues.
SupportRegion	Array of String	cn-hangzhou	The region in which the anti-ransomware feature is aupported. 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**: China (Hong Kong) • **cn-north-2-gov-1**: China North 2 Ali Gov • **ap-southeast-2**: Australia (Sydney) • **ap-southeast-5**: Indonesia (Jakarta) • **eu-central-1**: Germany (Frankfurt) • **us-west-1**: US (Silicon Valley) • **cn-qingdao**: China (Qingdao) • **ap-northeast-1**: Japan (Tokyo) • **cn-shanghai-finance-1**: China East 2 Finance • **ap-south-1**: India (Mumbai) • **us-east-1**: US (Virginia) • **cn-chengdu**: China (Chengdu) • **me-east-1**: UAE (Dubai) • **cn-shenzhen-finance-1**: China South 1 Finance

Examples

Sample requests

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

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeSupportRegionResponse>
    <RequestId>2C0699D3-4107-5A46-A4C4-E129A5967788</RequestId>
    <SupportRegion>cn-hangzhou</SupportRegion>
</DescribeSupportRegionResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "2C0699D3-4107-5A46-A4C4-E129A5967788",
  "SupportRegion" : [ "cn-hangzhou" ]
}
```

Error codes

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

6.13. DescribeBackupFiles

Queries backup files that you can restore.

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	DescribeBackupFiles	The operation that you want to perform. Set the value to **DescribeBackupFiles**.
Uuid	String	Yes	6d5b361f-958d-48a8-a9d2-d6e82c1a****	The UUID of the server to which an anti-ransomware policy is applied.
Path	String	No	""	The path to the backup file.
SnapshotHash	String	Yes	a7f26223ef3974c6fac324cd37713ab65ab618859d20b4039192a5da44d77b63	The hash value of the backup file.

Parameter	Type	Required	Example	Description
CurrentPage	String	Yes	1	The number of the page to return. Default value: **1**.
PageSize	String	Yes	10	The number of entries to return on each page. Default value: **10**.

Response parameters

Parameter	Type	Example	Description
RequestId	String	00A60A6D-33E0-5D5A-9B7C-E5D4DCA88148	The ID of the request, which is used to locate and troubleshoot issues.
PageInfo	Object		The pagination information.
CurrentPage	Integer	1	The page number of the returned page.
PageSize	Integer	10	The number of entries returned per page. Default value: **10**.
TotalCount	Integer	69	The total number of backup files.
Count	Integer	10	The number of backup files returned on the current page.
BackupFiles	Array of BrowseFile		The details about the backup file.
Type	String	dir	The type of the protected file. Valid values: • **file**: files • **dir**: folders
Name	String	Group 1	The name of the policy.
Subtree	String	Python27\	The path to the subdirectory of the backup file.
Size	Long	100	The size of the backup file. Unit: bytes.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeBackupFiles
&Uuid=6d5b361f-958d-48a8-a9d2-d6e82c1a****
&Path=""
&SnapshotHash=a7f26223ef3974c6fac324cd37713ab65ab618859d20b4039192a5da44d77b63
&CurrentPage=1
&PageSize=10
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeBackupFilesResponse>
    <RequestId>00A60A6D-33E0-5D5A-9B7C-E5D4DCA88148</RequestId>
    <PageInfo>
        <CurrentPage>1</CurrentPage>
        <PageSize>10</PageSize>
        <TotalCount>69</TotalCount>
        <Count>10</Count>
    </PageInfo>
    <BackupFiles>
        <Type>dir</Type>
        <Name>Group 1</Name>
        <Subtree>Python27\</Subtree>
        <Size>100</Size>
    </BackupFiles>
</DescribeBackupFilesResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "00A60A6D-33E0-5D5A-9B7C-E5D4DCA88148",
  "PageInfo" : {
    "CurrentPage" : 1,
    "PageSize" : 10,
    "TotalCount" : 69,
    "Count" : 10
  },
  "BackupFiles" : [ {
    "Type" : "dir",
    "Name" : "Group 1",
    "Subtree" : "Python27\\",
    "Size" : 100
  } ]
}
```

Error codes

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

6.14. DescribeBackupPolicies

Queries the protection policies that are used to prevent ransomware.

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	DescribeBackupPolicies	The operation that you want to perform. Set the value to **DescribeBackupPolicies**.
CurrentPage	Integer	Yes	1	The number of the page to return. Default value: 1.
PageSize	Integer	Yes	10	The number of entries to return on each page. Default value: 10.
Name	String	No	SecurityStrategy-20200303	The name of the protection policy that you want to query.
MachineRemark	String	No	1.1.XX.XX	The information that is used to identify the server to which the protection policy is applied. You can enter the IP address or ID of a server.

Parameter	Type	Required	Example	Description
Status	String	No	enabled	The status of the protection policy. • **enabled**: The protection policy is manually enabled. • **disabled**: The protection policy is manually disabled. After a protection policy is disabled, the data backup task that is running based on the policy stops. • **closed**: The protection policy automatically stops because the anti-ransomware capacity is insufficient.

Response parameters

Parameter	Type	Example	Description
PageInfo	Struct		The pagination information.
Count	Integer	3	The number of entries on the returned page.
CurrentPage	Integer	1	The page number of the returned page. Pages start from page 1. Default value: 1.
PageSize	Integer	20	The number of entries returned per page. Default value: 10.
TotalCount	Integer	30	The total number of protection policies returned.
Policies	Array of BackupPolicy		The details of the protection policy.
ClientErrorCount	Integer	2	The number of the servers on which the anti-ransomware agent is in the abnormal state.
ClientErrorUuidList	List	["3bb30859-b3b5-4f28-868f-b0892c98****","3bb30859-b3b5-4f28-868f-b0892c98****"]	The UUIDs of the servers on which the anti-ransomware agent is in the abnormal state.

Parameter	Type	Example	Description
ClientStatus	String	running	The status of the anti-ransomware agent. Valid values: • **running**: normal • **exception**: abnormal
HealthClientCount	Integer	2	The number of the servers on which the anti-ransomware agent is in the normal state.
HealthClientUuidList	List	["3bb30859-b3b5-4f28-868f-b0892c98****","3bb30859-b3b5-4f28-868f-b0892c98****"]	The UUIDs of the servers on which the anti-ransomware agent is in the normal state.
Id	Long	11	The ID of the protection policy.
Name	String	SecurityStrategy-20200303	The name of the protection policy.
Policy	String	{\"Source\":[\"/home/admin\",\"\\\\servername\\sharename\"],\"Exclude\":[\"/home/user\"],\"Schedule\":\"I|1583216092|P21D\",\"Retention\":365,\"SpeedLimiter\":\"12:15:15360|6:12:5120\",\"ExcludeSystemPath\":true}	The configurations of the protection policy.
PolicyRegionId	String	ch-hangzhou	The ID of the region in which the server in a data center resides. This server refers to the server on which you install the anti-ransomware agent.
PolicyVersion	String	2.0.0	The version of the protection policy. Valid values: • 1.0.0 • 2.0.0

Parameter	Type	Example	Description
RemarkedUuidList	List	["3bb30859-b3b5-4f28-868f-b0892c98****","3bb30859-b3b5-4f28-868f-b0892c98****"]	The UUIDs that are returned from the value of the MachineRemark request parameter.
ServiceErrorCount	Integer	2	The number of servers on which data backup is exceptional.
ServiceErrorUuidList	List	["3bb30859-b3b5-4f28-868f-b0892c98****","3bb30859-b3b5-4f28-868f-b0892c98****"]	The UUIDs of servers on which data backup is exceptional.
Status	String	enabled	The status of the protection policy. • **enabled**: The protection policy is manually enabled. • **disabled**: The protection policy is manually disabled. After a protection policy is disabled, the data backup task that is running based on the policy stops. • **closed**: The protection policy automatically stops because the anti-ransomware capacity is insufficient.
UpgradeStatus	String	Upgrading	The upgrade status of the protection policy. Valid values: • **NotUpgraded** • **Upgrading** • **UpgradeFailed** • **UpgradeSuccess**
UuidList	List	["3bb30859-b3b5-4f28-868f-b0892c98****","3bb30859-b3b5-4f28-868f-b0892c98****"]	The UUIDs of the servers to which the protection policy is applied.
RequestId	String	BE120DAB-F4E7-4C53-ADC3-A97578ABF384	The ID of the request, which is used to locate and troubleshoot issues.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DescribeBackupPolicies>
  <PageInfo>
        <TotalCount>30</TotalCount>
        <PageSize>20</PageSize>
        <CurrentPage>1</CurrentPage>
        <Count>3</Count>
  </PageInfo>
  <Policies>
        <PolicyRegionId>ch-hangzhou</PolicyRegionId>
        <PolicyVersion>2.0.0</PolicyVersion>
        <Policy>{\"Source\":[\"/home/admin\",\"\\\\servername\\sharename\"],\"Exclude\":[\"
/home/user\"],\"Schedule\":\"I|1583216092|P21D\",\"Retention\":365,\"SpeedLimiter\":\"12:15
:15360|6:12:5120\",\"ExcludeSystemPath\":true}</Policy>
        <Status>enabled</Status>
        <ClientStatus>running</ClientStatus>
        <ServiceErrorCount>2</ServiceErrorCount>
        <ClientErrorCount>2</ClientErrorCount>
        <Id>11</Id>
        <HealthClientCount>2</HealthClientCount>
        <Name>SecurityStrategy-20200303</Name>
        <UuidList>["3bb30859-b3b5-4f28-868f-b0892c98****","3bb30859-b3b5-4f28-868f-b0892c98
****"]</UuidList>
        <RemarkedUuidList>["3bb30859-b3b5-4f28-868f-b0892c98****","3bb30859-b3b5-4f28-868f-
b0892c98****"]</RemarkedUuidList>
        <ClientErrorUuidList>["3bb30859-b3b5-4f28-868f-b0892c98****","3bb30859-b3b5-4f28-86
8f-b0892c98****"]</ClientErrorUuidList>
        <ServiceErrorUuidList>["3bb30859-b3b5-4f28-868f-b0892c98****","3bb30859-b3b5-4f28-8
68f-b0892c98****"]</ServiceErrorUuidList>
        <HealthClientUuidList>["3bb30859-b3b5-4f28-868f-b0892c98****","3bb30859-b3b5-4f28-8
68f-b0892c98****"]</HealthClientUuidList>
  </Policies>
  <RequestId>BE120DAB-F4E7-4C53-ADC3-A97578ABF384</RequestId>
</DescribeBackupPolicies>
```

`JSON` format

```
{
    "PageInfo": {
        "TotalCount": "30",
        "PageSize": "20",
        "CurrentPage": "1",
        "Count": "3"
    },
    "Policies": [
        {
            "PolicyRegionId": "ch-hangzhou",
            "PolicyVersion": "2.0.0",
            "Policy": "{\\\"Source\\\":[\\\"/home/admin\\\",\\\"\\\\\\\\\\servername\\\\share
name\\\"],\\\"Exclude\\\":[\\\"/home/user\\\"],\\\"Schedule\\\":\\\"I|1583216092|P21D\\\",\
\\"Retention\\\":365,\\\"SpeedLimiter\\\":\\\"12:15:15360|6:12:5120\\\",\\\"ExcludeSystemPa
th\\\":true}",
            "Status": "enabled",
            "ClientStatus": "running",
            "UpgradeStatus": "Upgrading",
            "ServiceErrorCount": "2",
            "ClientErrorCount": "2",
            "Id": "11",
            "HealthClientCount": "2",
            "Name": "SecurityStrategy-20200303",
            "UuidList": "[\"3bb30859-b3b5-4f28-868f-b0892c98****\",\"3bb30859-b3b5-4f28-868
f-b0892c98****\"]",
            "RemarkedUuidList": "[\"3bb30859-b3b5-4f28-868f-b0892c98****\",\"3bb30859-b3b5-
4f28-868f-b0892c98****\"]",
            "ClientErrorUuidList": "[\"3bb30859-b3b5-4f28-868f-b0892c98****\",\"3bb30859-b3
b5-4f28-868f-b0892c98****\"]",
            "ServiceErrorUuidList": "[\"3bb30859-b3b5-4f28-868f-b0892c98****\",\"3bb30859-b
3b5-4f28-868f-b0892c98****\"]",
            "HealthClientUuidList": "[\"3bb30859-b3b5-4f28-868f-b0892c98****\",\"3bb30859-b
3b5-4f28-868f-b0892c98****\"]"
        }
    ],
    "RequestId": "BE120DAB-F4E7-4C53-ADC3-A97578ABF384"
}
```


Error codes

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

6.15. DescribeBackupClients

Queries the servers on which the anti-ransomware agent is installed in a specific region.

When you create a restoration task, you can use the server information that is returned for the DescribeBackupClients operation to specify the servers whose data you want to restore.

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	DescribeBackupClients	The operation that you want to perform. Set the value to **DescribeBackupClients**.
SupportRegionId	String	Yes	cn-hangzhou	The region in which the anti-ransomware feature is supported. You can call the DescribeSupportRegion operation to query the regions in which the anti-ransomware feature is supported.

Response parameters

Parameter	Type	Example	Description
RequestId	String	E3ED094C-9EB7-4239-962B-D0FB3D5F23C7	The ID of the request, which is used to locate and troubleshoot issues.
Clients	Array of BackupMachineDTO		The information about the anti-ransomware agent.
Uuid	String	22f6550d-f294-449b-b6e6-90638fd1****	The UUID of the Elastic Compute Service (ECS) instance on which the anti-ransomware agent is installed.
InstanceId	String	i-bp15hyph4aci99dv****	The ID of the ECS instance on which the anti-ransomware agent is installed.

Parameter	Type	Example	Description
ClientStatus	String	ONLINE	The status of the anti-ransomware agent. Valid values: • **INSTALLING**: The agent is being installed. • **ONLINE**: The agent is online. • **UNINSTALLING**: The agent is being uninstalled. • **NOT_INSTALLED**: The agent is not installed. • **ACTIVATED**: The agent is enabled. • **CLIENT_CONNECTION_ERROR**: A connection error occurs on the agent.
ClientId	String	c-000az2f537r73dyh****	The ID of the anti-ransomware agent.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeBackupClients
&SupportRegionId=cn-hangzhou
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeBackupClientsResponse>
    <RequestId>E3ED094C-9EB7-4239-962B-D0FB3D5F23C7</RequestId>
    <Clients>
        <Uuid>22f6550d-f294-449b-b6e6-90638fd1****</Uuid>
        <InstanceId>i-bp15hyph4aci99dv****</InstanceId>
        <ClientStatus>ONLINE</ClientStatus>
        <ClientId>c-000az2f537r73dyh****</ClientId>
    </Clients>
</DescribeBackupClientsResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "E3ED094C-9EB7-4239-962B-D0FB3D5F23C7",
  "Clients" : [ {
    "Uuid" : "22f6550d-f294-449b-b6e6-90638fd1****",
    "InstanceId" : "i-bp15hyph4aci99dv****",
    "ClientStatus" : "ONLINE",
    "ClientId" : "c-000az2f537r73dyh****"
  } ]
}
```

Error codes

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

6.16. GetBackupStorageCount

Queries the anti-ransomware capacity that is used.

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	GetBackupStorageCount	The operation that you want to perform. Set the value to **GetBackupStorageCount**.

Response parameters

Parameter	Type	Example	Description
RequestId	String	33C2CCFF-4BF8-5F88-9B5C-22F932F80E5A	The ID of the request, which is used to locate and troubleshoot issues.
BackupStorageCount	Object		The details about the anti-ransomware capacity.

Parameter	Type	Example	Description
Overflow	Integer	0	Indicates whether the anti-ransomware capacity that is used exceeds the anti-ransomware capacity that you purchased. Valid values: • **0**: no • **1**: yes
UniUsageStorageByte	Long	7453049350	The storage capacity that is occupied by the backup data of your databases. Unit: bytes.
BuyStorageByte	Long	2276332666880	The anti-ransomware capacity that you purchased. Unit: bytes.
UsageStorageByte	Long	839621565853	The total anti-ransomware capacity that is used. Unit: bytes.
EcsUsageStorageByte	Long	817262417803	The storage capacity that is occupied by the backup data of your servers. Unit: bytes.

Examples

Sample requests

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

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<GetBackupStorageCountResponse>
    <RequestId>33C2CCFF-4BF8-5F88-9B5C-22F932F80E5A</RequestId>
    <BackupStorageCount>
        <Overflow>0</Overflow>
        <UniUsageStorageByte>7453049350</UniUsageStorageByte>
        <BuyStorageByte>2276332666880</BuyStorageByte>
        <UsageStorageByte>839621565853</UsageStorageByte>
        <EcsUsageStorageByte>817262417803</EcsUsageStorageByte>
    </BackupStorageCount>
</GetBackupStorageCountResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "33C2CCFF-4BF8-5F88-9B5C-22F932F80E5A",
  "BackupStorageCount" : {
    "Overflow" : 0,
    "UniUsageStorageByte" : 7453049350,
    "BuyStorageByte" : 2276332666880,
    "UsageStorageByte" : 839621565853,
    "EcsUsageStorageByte" : 817262417803
  }
}
```

Error codes

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

7.Brute-force attacks protection

7.1. CreateAntiBruteForceRule

You can call this operation to create a defense rule to protect your assets from brute-force attacks.

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	CreateAntiBruteForceRule	The operation that you want to perform. Set the value to: **CreateAntiBruteForceRule**.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Name	String	No	Defense rules against brute-force attacks	Specifies the name of a defense rule.
Span	Integer	No	15	The time period during which the number of logon attempts are calculated.
FailCount	Integer	No	10	The maximum number of logon attempts specified in the defense rule.
ForbiddenTime	Integer	No	10	The time period during which logons from the blocked IP address are blocked.
UuidList.N	RepeatList	No	uuid-1312133-ssas,uuid-1234-qwer-dss	The list of servers to which the defense rule is applied.
DefaultRule	Boolean	No	true	Specifies whether to set the defense rule as the default rule. Valid values: • **true**: Yes • **false**: No

Response parameters

Parameter	Type	Example	Description
CreateAntiBruteForceRule	Struct		The result of the request.
RuleId	Long	6363	The ID of the defense rule.
RequestId	String	FB3E435F-4116-46F9-A5DE-C338DDA04F47	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<CreateAntiBruteForceRuleResponse>
  <CreateAntiBruteForceRule>
        <RuleId>6363</RuleId>
  </CreateAntiBruteForceRule>
  <requestId>FB3E435F-4116-46F9-A5DE-C338DDA04F47</requestId>
</CreateAntiBruteForceRuleResponse>
```

`JSON` format

```
{
 "CreateAntiBruteForceRule": {
  "RuleId": 6363
 },
 "requestId": "FB3E435F-4116-46F9-A5DE-C338DDA04F47"
}
```

Error codes

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

7.2. ModifyAntiBruteForceRule

Modifies a defense rule against brute-force attacks.

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	ModifyAntiBruteForceRule	The operation that you want to perform. Set the value to **ModifyAntiBruteForceRule**.
SourceIp	String	No	1.2.XX.XX	The source IP address of the request.
Id	Long	No	65778	The ID of the defense rule.
Name	String	No	lawtest defense rule	The name of the defense rule.
Span	Integer	No	1	The maximum period of time during which failed logon attempts from an account can occur. Unit: minutes. Valid values: • **1** • **2** • **5** • **10** • **15**
FailCount	Integer	No	10	The maximum number of failed logon attempts from an account. Valid values: • **2** • **3** • **4** • **5** • **10** • **50** • **80** • **100**

Parameter	Type	Required	Example	Description
ForbiddenTime	Integer	No	5	The period of time during which logons from an account are not allowed. Unit: minutes. Valid values: • **5** • **15** • **30** • **60** • **120** • **360** • **720** • **1440** • **10080** • **52560000**: permanent
DefaultRule	Boolean	No	true	Specifies whether to set the defense rule as the default rule. Valid values: • **true**: yes • **false**: no
UuidList.N	String	No	["292dcc68-b60b-4bbd-a0be-beaa1622****","7eb0dfc0-3205-4b8c-b26c-3f4159dc****"]	The UUIDs of the servers to which the defense rule is applied. Separate multiple UUIDs with commas (,).

Response parameters

Parameter	Type	Example	Description
RequestId	String	F35F45B0-5D6B-4238-BE02-A62D0760E840	The ID of the request, which is used to locate and troubleshoot issues.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyAntiBruteForceRule
&SourceIp=1.2.XX.XX
&Id=65778
&Name=lawtest defense rule
&Span=1
&FailCount=10
&ForbiddenTime=5
&DefaultRule=true
&UuidList=["[\"292dcc68-b60b-4bbd-a0be-beaa1622****\",\"7eb0dfc0-3205-4b8c-b26c-3f4159dc***
*\"]"]
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyAntiBruteForceRuleResponse>
    <RequestId>F35F45B0-5D6B-4238-BE02-A62D0760E840</RequestId>
</ModifyAntiBruteForceRuleResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "F35F45B0-5D6B-4238-BE02-A62D0760E840"
}
```

Error codes

HTTP status code	Error code	Error message	Description
400	NotBuy	user not buy service	The error message returned because the service is not purchased.
500	ServerError	ServerError	The error message returned because a server error occurred.

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

7.3. ModifyInstanceAntiBruteForceRule

Modifies the anti-brute-force-attack rule that is applied to a specific server.

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	ModifyInstanceAntiBruteForceRule	The operation that you want to perform. Set the value to **ModifyInstanceAntiBruteForceRule**.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Uuid	String	No	cc62fb70-fa90-4c1a-91a5-25806b36****	The UUID of the server for which you want to modify the anti-brute-force-attack rule. **Note** You can call the DescribeCloudCenterInstances operation to query the UUID of the server.
NewRuleId	Long	No	12	Specify the ID of the rule with which you want to replace the current rule. You can apply only one rule to each server. Therefore, you can specify only one rule ID. **Note** You can call the DescribeAntiBruteForceRules operation to query the rule ID **The value of the Id parameter indicates the rule ID.**.

Response parameters

Parameter	Type	Example	Description
RequestId	String	4E5BFDCF-B9DD-430D-9DA4-151BCB581C9D	The ID of the request.

Sample requests

Sample request

```
http(s)://[Endpoint]/? Action=ModifyInstanceAntiBruteForceRule
&Uuid=cc62fb70-fa90-4c1a-91a5-25806b36****
&NewRuleId=12
&<Common request parameters>
```

Sample success responses

`XML` format

```
<ModifyInstanceAntiBruteForceRuleResponse>
      <RequestId>4E5BFDCF-B9DD-430D-9DA4-151BCB581C9D</RequestId>
</ModifyInstanceAntiBruteForceRuleResponse>
```

`JSON` format

```
{
 "RequestId": "4E5BFDCF-B9DD-430D-9DA4-151BCB581C9D"
}
```

Error codes

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

7.4. DescribeAntiBruteForceRules

Queries the defense rules against brute-force attacks that you create.

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	DescribeAntiBruteForceRules	The operation that you want to perform. Set the value to **DescribeAntiBruteForceRules**.
SourceIp	String	No	1.2.3.4	The source IP address of the request.

Response parameters

Parameter	Type	Example	Description

Parameter	Type	Example	Description
PageInfo	Struct		The pagination information.
Count	Integer	2	The number of entries returned on the current page.
CurrentPage	Integer	1	The page number of the returned page.
PageSize	Integer	20	The number of entries returned per page.
TotalCount	Integer	2	The total number of defense rules against brute-force attacks that you create.
RequestId	String	4E5BFDCF-B9DD-430D-9DA4-151BCB581C9D	The ID of the request.
Rules	Array of AntiBruteForceRule		The details about the defense rule against brute-force attacks.
DefaultRule	Boolean	true	Indicates whether the defense rule is the default rule. Valid values: • **true** • **false** **Note** A default rule takes effect on all servers that are not protected by defense rules against brute-force attacks.
EnableSmartRule	Boolean	false	This parameter is deprecated.
FailCount	Integer	15	The threshold of logon failures that is specified in the defense rule.
ForbiddenTime	Integer	360	The duration in which the IP address of attackers cannot be used to log on to the server on which the defense rule takes effect. Unit: minutes.
Id	Long	1629	The ID of the defense rule.

Parameter	Type	Example	Description
MachineCount	Integer	3	The number of servers to which the defense rule is applied.
Name	String	Alibaba Cloud best practices against brute-force attacks	The name of the defense rule.
Span	Integer	10	The time threshold that is used to determine whether the defense rule takes effect. Unit: minutes. If **Span** is set to 10, the defense rule takes effect when the logon failures exceeds the specified threshold within 10 minutes. The IP address of attackers cannot be used to log on to the server within the specified duration.
UuidList	List	uuid-b3e-867b-1d56cf4d****", "uuid-d86f-47ea-a75d-c87c9fbfbb51", "uuid-018c-4ef7-89fd-988b9b0e****"	The UUIDs of servers to which the defense rule is applied.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DescribeAntiBruteForceRulesResponse>
      <PageInfo>
            <TotalCount>2</TotalCount>
            <PageSize>20</PageSize>
            <CurrentPage>1</CurrentPage>
            <Count>2</Count>
      </PageInfo>
      <Rules>
            <DefaultRule>false</DefaultRule>
            <ForbiddenTime>360</ForbiddenTime>
            <UuidList>uuid-80d2f7d6-ecc42f8****</UuidList>
            <FailCount>80</FailCount>
            <EnableSmartRule>false</EnableSmartRule>
            <MachineCount>1</MachineCount>
            <Id>1781</Id>
            <Span>10</Span>
            <Name>Test</Name>
      </Rules>
      <Rules>
            <DefaultRule>false</DefaultRule>
            <ForbiddenTime>5</ForbiddenTime>
            <UuidList>uuid-b3e-867b-1d56cf4d****</UuidList>
            <UuidList>uuid-d86f-47ea-a75d-c87c9fbf****</UuidList>
            <UuidList>uuid-018c-4ef7-89fd-988b9b0e****</UuidList>
            <FailCount>5</FailCount>
            <EnableSmartRule>false</EnableSmartRule>
            <MachineCount>3</MachineCount>
            <Id>1629</Id>
            <Span>15</Span>
            <Name>Alibaba Cloud best practices against brute-force attacks</Name>
      </Rules>
      <requestId>6AC2CE6A-12DF-4311-8C7E-B2FDEA7BA39A</requestId>
</DescribeAntiBruteForceRulesResponse>
```

`JSON` format

```
{
 "PageInfo": {
  "TotalCount": 2,
  "PageSize": 20,
  "CurrentPage": 1,
  "Count": 2
 },
 "Rules": [{
  "DefaultRule": false,
  "ForbiddenTime": 360,
  "UuidList": ["uuid-80d2f7d6-ecc42f8****"],
  "FailCount": 80,
  "EnableSmartRule": false,
  "MachineCount": 1,
  "Id": 1781,
  "Span": 10,
  "Name": "Test"
 }, {
  "DefaultRule": false,
  "ForbiddenTime": 5,
  "UuidList": ["uuid-b3e-867b-1d56cf4d****", "uuid-d86f-47ea-a75d-c87c9fbf****", "uuid-018c
-4ef7-89fd-988b9b0e****"],
  "FailCount": 5,
  "EnableSmartRule": false,
  "MachineCount": 3,
  "Id": 1629,
  "Span": 15,
  "Name": "Alibaba Cloud best practices against brute-force attacks"
 }],
 "requestId": "6AC2CE6A-12DF-4311-8C7E-B2FDEA7BA39A"
}
```


Error codes

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

7.5. DescribeBruteForceSummary

Queries the statistics of anti-brute-force-attack rules.

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

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeBruteForceSummary	The operation that you want to perform. Set the value to **DescribeBruteForceSummary**.
SourceIp	String	No	1.2.3.4	The source IP address of the request.

Response parameters

Parameter	Type	Example	Description
BruteForceSummary	Struct		The statistics of anti-brute-force-attack rules.
AllStrategyCount	Integer	13	The total number of anti-brute-force-attack rules.
EffectiveCount	Integer	2	The number of enabled anti-brute-force-attack rules.
RequestId	String	AE60EAE3-ABD0-897C-B0F16CAC6C7D	The ID of the request.

Sample requests

Sample request

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

Sample success responses

`XML` format

```
<DescribeBruteForceSummaryResponse>
      <BruteForceSummary>
            <AllStrategyCount>13</AllStrategyCount>
            <EffectiveCount>2</EffectiveCount>
      </BruteForceSummary>
      <requestId>AE60EAE3-ABD0-897C-B0F16CAC6C7D</requestId>
</DescribeBruteForceSummaryResponse>
```

`JSON` format

```
{
 "RequestId": "AE60EAE3-ABD0-897C-B0F16CAC6C7D",
 "BruteForceSummary": {
  "AllStrategyCount": "13",
  "EffectiveCount": "2"
 }
}
```


Error codes

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

7.6. DescribeInstanceAntiBruteForceRules

Queries information about servers to which the defense rules against brute-force attacks are applied.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeInstanceAntiBruteForceRules	The operation that you want to perform. Set the value to **DescribeInstanceAntiBruteForceRules**.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
UuidList.N	RepeatList	No	4fe8e1cd-3c37-4851-b9de-124da32c****	The list of the server UUIDs. **Note** You can call the DescribeCloudCenterInstances operation to obtain the UUIDs.

Response parameters

Parameter	Type	Example	Description
PageInfo	Struct		The page information.

Parameter	Type	Example	Description
Count	Integer	4	The number of servers to which the defense rules are applied is displayed on the current page.
CurrentPage	Integer	1	The page number of the current page. Pages start from page 1. Default value: 1.
PageSize	Integer	20	The number of entries returned per page. Default value: 20.
TotalCount	Integer	4	The total number of servers to which the defense rules are applied.
RequestId	String	97286A-4A6B-4A4-95FA-EC7E3E2451	The ID of the request.
Rules	Array of InstanceAntiBruteForceRule		The list of servers to which the defense rules are applied.
Id	Long	1612	The ID of the defense rule.
Name	String	Alibaba Cloud best practices against brute-force attacks	The name of the defense rule.
Uuid	String	4fe8e1cd-3c37-4851-b9de-124da32c****	The UUID of the server to which the defense rule is applied.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DescribeInstanceAntiBruteForceRulesResponse>
      <PageInfo>
            <TotalCount>4</TotalCount>
            <PageSize>20</PageSize>
            <CurrentPage>1</CurrentPage>
            <Count>4</Count>
      </PageInfo>
      <Rules>
            <Uuid>5f5d204b-aa63-4b3e-867b-1d56cf4d****</Uuid>
            <Id>1639</Id>
            <Name>Alibaba Cloud best practices against brute-force attacks</Name>
      </Rules>
      <Rules>
            <Uuid>uuid-a-a75d-c87c9fbf****</Uuid>
            <Id>1639</Id>
            <Name>Alibaba Cloud best practices against brute-force attacks</Name>
      </Rules>
      <Rules>
            <Uuid>uuid-7f-8ff4-7ecc42f89c****</Uuid>
            <Id>1781</Id>
            <Name>abc</Name>
      </Rules>
      <Rules>
            <Uuid>uuid-639774d6-****</Uuid>
            <Id>1639</Id>
            <Name>Alibaba Cloud best practices against brute-force attacks</Name>
      </Rules>
      <requestId>97286A-4A6B-4A4-95FA-EC7E3E2451</requestId>
</DescribeInstanceAntiBruteForceRulesResponse>
```

`JSON` format

```
{
    "PageInfo": {
        "TotalCount": 4,
        "PageSize": 20,
        "CurrentPage": 1,
        "Count": 4
    },
    "Rules": [{
        "Uuid": "5f5d204b-aa63-4b3e-867b-1d56cf4d****",
        "Id": 1639,
        "Name": "Alibaba Cloud best practices against brute-force attacks"
    }, {
        "Uuid": "uuid-a-a75d-c87c9fbf****",
        "Id": 1639,
        "Name": "Alibaba Cloud best practices against brute-force attacks"
    }, {
        "Uuid": "uuid-7f-8ff4-7ecc42f89c****",
        "Id": 1781,
        "Name": "abc"
    }, {
        "Uuid": "uuid-639774d6-****",
        "Id": 1639,
        "Name": "Alibaba Cloud best practices against brute-force attacks"
    }],
    "requestId": "97286A-4A6B-4A4-95FA-EC7E3E2451"
}
```


Error codes

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

8.Image security scans

8.1. DescribeGroupedMaliciousFiles

Queries malicious image samples.

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	DescribeGroupedMaliciousFiles	The operation that you want to perform. Set the value to **DescribeGroupedMaliciousFiles**.
CurrentPage	Integer	Yes	1	The number of the page to return. Pages start from page **1**. Default value: **1**.
PageSize	String	Yes	20	The number of entries to return on each page. Default value: **20**.
Lang	String	No	zh	The natural language of the request and response. Default value: **zh**. Valid values: • **zh**: Chinese • **en**: English
Levels	String	No	serious	The severity of the malicious image sample that you want to query. You can enter multiple values. Separate the values with commas (,). Valid values: • **serious** • **suspicious** • **remind**

Parameter	Type	Required	Example	Description
FuzzyMaliciousName	String	No	Webshell file	The name of the malicious image sample that you want to query. **Note** Fuzzy match is supported.
RepoRegionId	String	No	cn-shanghai	The region ID of the image repository. Valid values: • **cn-beijing**: China (Beijing) • **cn-zhangjiakou**: China (Zhangjiakou) • **cn-hangzhou**: China (Hangzhou) • **cn-shanghai**: China (Shanghai) • **cn-shenzhen**: China (Shenzhen) • **cn-hongkong**: China (Hong Kong) • **ap-southeast-1**: Singapore (Singapore) • **ap-southeast-5**: Indonesia (Jakarta) • **us-east-1**: US (Virginia) • **us-west-1**: US (Silicon Valley) • **eu-central-1**: Germany (Frankfurt) • **eu-west-1**: UK (London) • **ap-south-1**: India (Mumbai)
RepoInstanceId	String	No	cri-datvailb****	The ID of the container image. **Note** You can call the ListRepository operation to query the ID from the value of the **InstanceId** response parameter.
RepoId	String	No	crr-vridcl4****	The ID of the image repository. **Note** You can call the ListRepository operation to query the ID from the value of the **RepoId** response parameter.

Parameter	Type	Required	Example	Description
RepoName	String	No	centos	The name of the image repository. Note Fuzzy match is supported.
RepoNamespace	String	No	hanghai-namespace	The namespace to which the image repository belongs. Note Fuzzy match is supported.
ImageTag	String	No	0.2	The tag added to the image.
ImageDigest	String	No	6a5e103187b31a94592a47a5858617f7****	The digest of the image.
ImageLayer	String	No	27213ad375b53628dd152a5ca****	The layer of the image.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
GroupedMaliciousFileResponse	Array of GroupedMaliciousFile		The details of malicious image samples.
FirstScanTimestamp	Long	1594907349000	The UNIX timestamp of when the first scan was performed. Unit: milliseconds.
ImageCount	Long	3	The number of affected images.
LatestScanTimestamp	Long	1596533942000	The UNIX timestamp of when the last scan was performed. Unit: milliseconds.

Parameter	Type	Example	Description
Level	String	serious	The severity of the malicious image sample. Valid values: • **serious** • **suspicious** • **remind**
MaliciousMd5	String	d836968041f7683b5459****	The MD5 hash value of the malicious image sample.
MaliciousName	String	Self-mutating trojan	The name of the malicious image sample.
Status	Integer	0	The status of the malicious image sample. Valid values: • **0**: The sample is unhandled. • **1**: The sample is handled. • **2**: The sample is being verified. • **3**: The sample is added to the whitelist.
PageInfo	Struct		The pagination information.
Count	Integer	2	The number of malicious image samples returned on the current page.
CurrentPage	Integer	1	The page number of the current page.
PageSize	Integer	20	The number of entries returned per page. Default value: **20**.
TotalCount	Integer	2	The total number of returned malicious image samples.
RequestId	String	8045E03E-6D91-4C53-9F22-5A1B84BB29D9	The ID of the request, which is used to locate and troubleshoot issues.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeGroupedMaliciousFiles
&CurrentPage=1
&PageSize=20
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeGroupedMaliciousFilesResponse>
      <GroupedMaliciousFileResponse>
            <Status>0</Status>
            <LatestScanTimestamp>1596533942000</LatestScanTimestamp>
            <ImageCount>3</ImageCount>
            <MaliciousName>Self-mutating trojan</MaliciousName>
            <Level>serious</Level>
            <FirstScanTimestamp>1594907349000</FirstScanTimestamp>
            <MaliciousMd5>d836968041f7683b545900****</MaliciousMd5>
      </GroupedMaliciousFileResponse>
      <GroupedMaliciousFileResponse>
            <Status>1</Status>
            <LatestScanTimestamp>1594785387000</LatestScanTimestamp>
            <ImageCount>0</ImageCount>
            <MaliciousName>Webshell file</MaliciousName>
            <Level>serious</Level>
            <FirstScanTimestamp>1594630261000</FirstScanTimestamp>
            <MaliciousMd5>d8b4074715b232d7d41***</MaliciousMd5>
      </GroupedMaliciousFileResponse>
      <PageInfo>
            <TotalCount>2</TotalCount>
            <PageSize>20</PageSize>
            <CurrentPage>1</CurrentPage>
            <Count>2</Count>
      </PageInfo>
      <RequestId>8045E03E-6D91-4C53-9F22-5A1B84BB29D9</RequestId>
</DescribeGroupedMaliciousFilesResponse>
```

`JSON` format

```
{
 "GroupedMaliciousFileResponse": [{
  "Status": 0,
  "LatestScanTimestamp": 1596533942000,
  "ImageCount": 3,
  "MaliciousName": "Self-mutating trojan",
  "Level": "serious",
  "FirstScanTimestamp": 1594907349000,
  "MaliciousMd5": "d836968041f7683b545900****"
 }, {
  "Status": 1,
  "LatestScanTimestamp": 1594785387000,
  "ImageCount": 0,
  "MaliciousName": "Webshell file",
  "Level": "serious",
  "FirstScanTimestamp": 1594630261000,
  "MaliciousMd5": "d8b4074715b232d7d41***"
 }],
 "PageInfo": {
  "TotalCount": 2,
  "PageSize": 20,
  "CurrentPage": 1,
  "Count": 2
 },
 "RequestId": "8045E03E-6D91-4C53-9F22-5A1B84BB29D9"
}
```


Error codes

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

8.2. DescribeImageBaselineCheckSummary

Queries the image baseline risks that are detected.

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	DescribeImageBaselineCheckSummary	The operation that you want to perform. Set the value to **DescribeImageBaselineCheckSummary**.

Parameter	Type	Required	Example	Description
RiskLevel	String	No	high	The severity of the image baseline risk. Separate multiple severities with commas (,). Valid values: • **high** • **medium** • **low**
Criteria	String	No	Identity authentication	The condition that is used to query the image baseline risk.
CriteriaType	String	No	BaselineNameAlias	The type of the condition that is used query the image baseline risk. Valid values: • **BaselineNameAlias**: baseline name • **BaselineClassAlias**: baseline category
PageSize	Integer	No	20	The number of entries to return on each page. Default value: **20**.
CurrentPage	Integer	No	1	The number of the page to return. Pages start from page **1**. Default value: **1**.
Lang	String	No	zh	The language of the content within the request and response. Default value: **zh**. Valid values: • **zh**: Chinese • **en**: English

Response parameters

Parameter	Type	Example	Description
RequestId	String	5BD95679-D63A-4151-97D0-188432F4A57	The ID of the request, which is used to locate and troubleshoot issues.
PageInfo	Object		The pagination information.
CurrentPage	Integer	1	The page number of the returned page.

Parameter	Type	Example	Description
PageSize	Integer	20	The number of entries returned per page. Default value: **20**.
TotalCount	Integer	3	The total number of entries returned.
Count	Integer	3	The number of entries returned on the current page.
BaselineResultSummary	Array of BaselineResultSummary		The details about image baseline risks.
Status	Integer	0	Indicates whether the image baseline risk is fixed. Valid values: • **0**: unfixed • **1**: fixed • **2**: pending verification • **3**: fixing failed
MiddleRiskImage	Integer	0	The number of images on which **medium** baseline risks are detected.
BaselineNameLevel	String	high	The severity of the image baseline risk. Valid values: • **high** • **medium** • **low**
LastScanTime	Long	1626628760000	The timestamp when the last scan was performed. Unit: milliseconds.
HighRiskImage	Integer	15	The number of images on which **high** baseline risks are detected.
BaselineNameKey	String	hc_image_exploit	The keyword of the baseline name.
BaselineClassKey	String	hc_image_exploit	The keyword of the baseline category.
BaselineNameAlias	String	Unauthorized access	The name of the baseline.

Parameter	Type	Example	Description
BaselineClassAlias	String	Unauthorized access	The category of the baseline.
FirstScanTime	Long	1626628760000	The timestamp when the first scan was performed. Unit: milliseconds.
LowRiskImage	Integer	0	The number of images on which **low** baseline risks are detected.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeImageBaselineCheckSummary
&RiskLevel=high
&Criteria=Identity authentication
&CriteriaType=BaselineNameAlias
&PageSize=20
&CurrentPage=1
&Lang=zh
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeImageBaselineCheckSummaryResponse>
    <RequestId>5BD95679-D63A-4151-97D0-188432F4A57</RequestId>
    <PageInfo>
        <CurrentPage>1</CurrentPage>
        <PageSize>20</PageSize>
        <TotalCount>3</TotalCount>
        <Count>3</Count>
    </PageInfo>
    <BaselineResultSummary>
        <Status>0</Status>
        <MiddleRiskImage>0</MiddleRiskImage>
        <BaselineNameLevel>high</BaselineNameLevel>
        <LastScanTime>1626628760000</LastScanTime>
        <HighRiskImage>15</HighRiskImage>
        <BaselineNameKey>hc_image_exploit</BaselineNameKey>
        <BaselineClassKey>hc_image_exploit</BaselineClassKey>
        <BaselineNameAlias>Unauthorized access</BaselineNameAlias>
        <BaselineClassAlias>Unauthorized access</BaselineClassAlias>
        <FirstScanTime>1626628760000</FirstScanTime>
        <LowRiskImage>0</LowRiskImage>
    </BaselineResultSummary>
</DescribeImageBaselineCheckSummaryResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "5BD95679-D63A-4151-97D0-188432F4A57",
  "PageInfo" : {
    "CurrentPage" : 1,
    "PageSize" : 20,
    "TotalCount" : 3,
    "Count" : 3
  },
  "BaselineResultSummary" : [ {
    "Status" : 0,
    "MiddleRiskImage" : 0,
    "BaselineNameLevel" : "high",
    "LastScanTime" : 1626628760000,
    "HighRiskImage" : 15,
    "BaselineNameKey" : "hc_image_exploit",
    "BaselineClassKey" : "hc_image_exploit",
    "BaselineNameAlias" : "Unauthorized access",
    "BaselineClassAlias" : "Unauthorized access",
    "FirstScanTime" : 1626628760000,
    "LowRiskImage" : 0
  } ]
}
```

Error codes

HTTP status code	Error code	Error message	Description
500	ServerError	ServerError	The error message returned because a server error occurred.

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

8.3. DescribeAffectedMaliciousFileImages

Queries the details of malicious image files.

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	DescribeAffectedMaliciousFileImages	The operation that you want to perform. Set the value to **DescribeAffectedMaliciousFileImages**.
CurrentPage	Integer	Yes	1	The page number of the current page. Pages start from page **1**. Default value: **1**.
PageSize	String	Yes	20	The number of entries to return on each page. Default value: **20**.
MaliciousMd5	String	No	d836968041f7683b5459****	The MD5 hash value of the malicious file. **Note** You can call the DescribeGroupedMaliciousFiles operation to query the MD5 hash values of malicious files.

Parameter	Type	Required	Example	Description
Lang	String	No	zh	The natural language of the request and response. Valid values: • **zh**: Chinese • **en**: English
RepoRegionId	String	No	cn-shanghai	The region ID of the image repository. Valid values: • **cn-beijing**: China (Beijing) • **cn-zhangjiakou**: China (Zhangjiakou) • **cn-hangzhou**: China (Hangzhou) • **cn-shanghai**: China (Shanghai) • **cn-shenzhen**: China (Shenzhen) • **cn-hongkong**: China (Hong Kong) • **ap-southeast-1**: Singapore (Singapore) • **ap-southeast-5**: Indonesia (Jakarta) • **us-east-1**: US (Virginia) • **us-west-1**: US (Silicon Valley) • **eu-central-1**: Germany (Frankfurt) • **eu-west-1**: UK (London) • **ap-south-1**: India (Mumbai)
RepoInstanceId	String	No	cri-datvailb****	The ID of the container image. **Note** You can call the ListRepository operation to query the image IDs from the value of the **InstanceId** parameter.
RepoId	String	No	crr-vridcl4****	The ID of the image repository. **Note** You can call the ListRepository operation to query the repository IDs from the value of the **RepoId** response parameter.

Parameter	Type	Required	Example	Description
RepoName	String	No	centos	The name of the image repository. Note Fuzzy match is supported.
RepoNamespace	String	No	hanghai-namespace	The namespace to which the image repository belongs. Note Fuzzy match is supported.
ImageTag	String	No	0.2	The tag of the image.
ImageDigest	String	No	6a5e103187b31a94592a47a5858617f7a179ead61df7606****	The digest of the image.
ImageLayer	String	No	27213ad375b53628dd152a5ca****	The layer of the image.

Response parameters

Parameter	Type	Example	Description
AffectedMaliciousFileImagesResponse	Array of AffectedMaliciousFileImage		The details of the malicious image samples.
Digest	String	6a5e1031a5858617f7d8a179ead6****	The digest of the image.
FilePath	String	/d836968041f7683b5605a****	The path of the image file.
FirstScanTimestamp	Long	1594907349000	The time of the first scan. 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.
ImageUuid	String	e05c0de798217637868ef4****	The UUID of the image.

Parameter	Type	Example	Description
LatestScanTimestamp	Long	1596522785000	The time of the last scan. 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.
LatestVerifyTimestamp	Long	1596522711000	The timestamp of the last verification.
Layer	String	27213ad3447f0209dd152a5cadea****	The layer of the image.
Level	String	serious	The severity of the malicious image sample. Valid values: • **serious** • **suspicious** • **remind**
MaliciousMd5	String	d836968041f768300d9605a****	The MD5 hash value of the file.
Namespace	String	hanghai-namespace	The namespace to which the image repository belongs.
RepoId	String	crr-vridcl4****	The ID of the image repository.
RepoInstanceId	String	cri-datvail3m****	The ID of the container image.
RepoName	String	centos	The name of the image repository.
RepoRegionId	String	cn-shanghai	The region ID of the image repository.
Status	Integer	1	The status of the malicious image sample. Valid values: • **0**: The sample is unhandled. • **1**: The sample is handled. • **2**: The sample is being verified. • **3**: The sample is added to the whitelist.
Tag	String	0.2	The tag of the image.

Parameter	Type	Example	Description
PageInfo	Struct		The page information.
Count	Integer	2	The number of images that have the malicious image sample returned on the current page.
CurrentPage	Integer	1	The page number of the current page. Pages start from page **1**. Default value: **1**.
PageSize	Integer	20	The number of entries returned per page. Default value:**20**.
TotalCount	Integer	2	The total number of images that have the malicious image sample.
RequestId	String	ACF97412-FD09-4D1F-994F-34DF12BREF20	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeAffectedMaliciousFileImages
&CurrentPage=1
&PageSize=20
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeAffectedMaliciousFileImagesResponse>
      <AffectedMaliciousFileImagesResponse>
            <Status>0</Status>
            <FilePath>/d836968041f7683b5605a****</FilePath>
            <LatestScanTimestamp>1596522785000</LatestScanTimestamp>
            <RepoRegionId>cn-shanghai</RepoRegionId>
            <Digest>6a5e1031a5858617f7d8a179ead61df760671bf0a7252b****</Digest>
            <RepoName>centos</RepoName>
            <Layer>27213ad3447f0209dd152a5cadea0eac9b94d44c34a5****</Layer>
            <ImageUuid>e05c0de798217637868ef4****</ImageUuid>
            <Namespace>hanghai-namespace</Namespace>
            <RepoInstanceId>cri-datvail3m****</RepoInstanceId>
            <LatestVerifyTimestamp>1596522711000</LatestVerifyTimestamp>
            <Level>serious</Level>
            <Tag>0.2</Tag>
            <RepoId>crr-vridcl4q****</RepoId>
            <FirstScanTimestamp>1594907349000</FirstScanTimestamp>
            <MaliciousMd5>d836968041f768300d9605a****</MaliciousMd5>
      </AffectedMaliciousFileImagesResponse>
      <AffectedMaliciousFileImagesResponse>
            <Status>0</Status>
            <FilePath>/d836968041f7683b5d9605****</FilePath>
            <LatestScanTimestamp>1596533806000</LatestScanTimestamp>
            <RepoRegionId>cn-hangzhou</RepoRegionId>
            <Digest>640fd38d2efbd2c9ec29439e39c0f01c11b6127518eeb31aec1****</Digest>
            <RepoName>test2</RepoName>
            <Layer>27213ad375b53628dcdea09dd152a5cadea0eac9b94d44c34a5a****</Layer>
            <ImageUuid>fcf8224d5cf26c201a579bcfe59f****</ImageUuid>
            <Namespace>test</Namespace>
            <RepoInstanceId>cri-itxy1bs7****</RepoInstanceId>
            <LatestVerifyTimestamp>1596533801000</LatestVerifyTimestamp>
            <Level>serious</Level>
            <Tag>0.3</Tag>
            <RepoId>crr-2jwz0ee8****</RepoId>
            <FirstScanTimestamp>1596532246000</FirstScanTimestamp>
            <MaliciousMd5>d836968041f7683d9605a****</MaliciousMd5>
      </AffectedMaliciousFileImagesResponse>
      <PageInfo>
            <TotalCount>2</TotalCount>
            <PageSize>10</PageSize>
            <CurrentPage>1</CurrentPage>
            <Count>2</Count>
      </PageInfo>
      <RequestId>ACF97412-FD09-4D1F-994F-34DF12BREF20</RequestId>
</DescribeAffectedMaliciousFileImagesResponse>
```

`JSON` format

```
{
 "AffectedMaliciousFileImagesResponse": [{
  "Status": 0,
  "FilePath": "/d836968041f7683b5605a****",
  "LatestScanTimestamp": 1596522785000,
  "RepoRegionId": "cn-shanghai",
  "Digest": "6a5e1031a5858617f7d8a179ead61df760671bf0a7252ba****",
  "RepoName": "centos",
  "Layer": "27213ad3447f0209dd152a5cadea0eac9b94d44c34a5ac****",
  "ImageUuid": "e05c0de798217637868ef4****",
  "Namespace": "hanghai-namespace",
  "RepoInstanceId": "cri-datvail3m****",
  "LatestVerifyTimestamp": 1596522711000,
  "Level": "serious",
  "Tag": "0.2",
  "RepoId": "crr-vridcl4****",
  "FirstScanTimestamp": 1594907349000,
  "MaliciousMd5": "d836968041f768300d9605a****"
 }, {
  "Status": 0,
  "FilePath": "/d836968041f7683b5d9605a****",
  "LatestScanTimestamp": 1596533806000,
  "RepoRegionId": "cn-hangzhou",
  "Digest": "640fd38d2efbd2c9ec29439e39c0f01c11b6127518eeb31aec1****",
  "RepoName": "test2",
  "Layer": "27213ad375b53628dcdea09dd152a5cadea0eac9b94d44c34a5a****",
  "ImageUuid": "fcf8224d5cf26c201a579bcfe59****",
  "Namespace": "test",
  "RepoInstanceId": "cri-itxy1bs73****",
  "LatestVerifyTimestamp": 1596533801000,
  "Level": "serious",
  "Tag": "0.3",
  "RepoId": "crr-2jwz0ee8****",
  "FirstScanTimestamp": 1596532246000,
  "MaliciousMd5": "d836968041f7683d9605a****"
 }],
 "PageInfo": {
  "TotalCount": 2,
  "PageSize": 10,
  "CurrentPage": 1,
  "Count": 2
 },
 "RequestId": "ACF97412-FD09-4D1F-994F-34DF12BREF20"
}
```


Error codes

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

8.4. DescribeImageScanAuthCount

Queries the details about the quota for container image scan.

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	DescribeImageScanAuthCount	The operation that you want to perform. Set the value to **DescribeImageScanAuthCount**.

Response parameters

Parameter	Type	Example	Description
RequestId	String	892NYH839-0EDC-4CD0-A2EF-5BD294656C99	The ID of the request, which is used to locate and troubleshoot issues.
ImageScan	Object		The details about the quota for container image scan.
ScanCount	Long	5489	The consumed quota for container image scan.
ImageScanCapacity	Long	15340	The quota for container image scan.
InstanceId	String	sas-qdl123412****	The ID of the purchased Security Center instance.

Examples

Sample requests

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

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeImageScanAuthCountResponse>
    <RequestId>892NYH839-0EDC-4CD0-A2EF-5BD294656C99</RequestId>
    <ImageScan>
        <ScanCount>5489</ScanCount>
        <ImageScanCapacity>15340</ImageScanCapacity>
        <InstanceId>sas-qdl123412****</InstanceId>
    </ImageScan>
</DescribeImageScanAuthCountResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "892NYH839-0EDC-4CD0-A2EF-5BD294656C99",
  "ImageScan" : {
    "ScanCount" : 5489,
    "ImageScanCapacity" : 15340,
    "InstanceId" : "sas-qdl123412****"
  }
}
```

Error codes

HTTP status code	Error code	Error message	Description
400	NoPermission	no permission	The error message returned because you do not have access permissions.
500	ServerError	ServerError	The error message returned because a server error occurred.

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

8.5. DescribeTaskErrorLog

Queries the error logs that record tasks failed to fix image vulnerabilities.

Usage notes

You can call the DescribeTaskErrorLog operation to query the error logs that records task failed to fix image vulnerabilities. If a task fails to fix an image vulnerability, Security Center generates an error log. You can identify the cause of the failure based on the error log.

Limits

You can call this operation up to 10 times per second per account. If the number of the calls per second exceeds the limit, throttling is triggered. As a result, your business may be affected. We recommend that you take note of the limit when you call this operation.

Debugging

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

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeTaskErrorLog	The operation that you want to perform. Set the value to **DescribeTaskErrorLog**.
BuildTaskId	String	Yes	ivf-6e520160-205d-4801-b8e9-9e7efd8c	The ID of the task that you create to fix an image vulnerability.
SourceIp	String	No	10.12.XX.XX	The source IP address of the request.

Response parameters

Parameter	Type	Example	Description
Logs	Array of Log		The error logs that are returned.
Text	String	mv: cannot move 'CentOS-Base.repo' to 'CentOS-Base.repo.backup': Permission denied	The content of the log.
RequestId	String	F929E952-EBFC-56C3-BD35-BF8B59024C69	The ID of the request, which is used to locate and troubleshoot issues.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DescribeTaskErrorLogResponse>
  <RequestId>F929E952-EBFC-56C3-BD35-BF8B59024C69</RequestId>
  <Count>100</Count>
  <Logs>
        <Text>mv: cannot move 'CentOS-Base.repo' to 'CentOS-Base.repo.backup': Permission d
enied</Text>
  </Logs>
</DescribeTaskErrorLogResponse>
```

`JSON` format

```
{
    "RequestId": "F929E952-EBFC-56C3-BD35-BF8B59024C69",
    "Count": "100",
    "Logs": [
        {
            "Text": "mv: cannot move 'CentOS-Base.repo' to 'CentOS-Base.repo.backup': Permi
ssion denied"
        }
    ]
}
```

Error codes

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

8.6. DescribeImageFixTask

Queries the tasks that you create to fix image risks.

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	DescribeImageFixTask	The operation that you want to perform. Set the value to **DescribeImageFixTask**.
StartTime	Long	No	1634725571000	The timestamp when the task starts. Unit: milliseconds.
EndTime	Long	No	1635575219000	The timestamp when the task ends. Unit: milliseconds.

Parameter	Type	Required	Example	Description
Status	String	No	1	The status of the task. Valid values: • 1: The task is running. • 2: The task is successful. • 3: The task failed.
CurrentPage	Integer	Yes	1	The number of the page to return. Default value: 1.
PageSize	Integer	Yes	20	The number of entries to return on each page. Default value: 20.

Response parameters

Parameter	Type	Example	Description
RequestId	String	8AC52BBA-85D3-5F64-9B48-D08437CAF916	The ID of the request, which is used to locate and troubleshoot issues.
PageInfo	Object		The pagination information.
CurrentPage	Integer	1	The page number of the returned page. Default value: 1.
PageSize	Integer	20	The number of entries returned per page. Default value: 20.
TotalCount	Integer	12	The total number of tasks returned.
Count	Integer	12	The number of tasks returned on the current page.
BuildTasks	Array of BuildTask		The details about the task.
BuildTaskId	String	ivf-939536b5-c3ca-427b-8183-91007756	The ID of the task.

Parameter	Type	Example	Description
TaskType	String	IMAGE_REPAIR	The type of the task. The value is fixed as IMAGE_REPAIR, which indicates the tasks that you create to fix image risks.
RepoNamespace	String	name-002	The namespace of the image.
RepoName	String	test-redhat	The name of the image repository.
RegionId	String	cn-hangzhou	The region of the image.
OldTag	String	centos8.1-ja	The version of the image.
OldUuid	String	2fa731681911ae8d1b5f11893ace****	The UUID of the image.
NewTag	String	redhat8-vault	The version of the image after image risks are fixed.
NewUuid	String	2fa731681911ae8d1b5f11893ace****	The UUID of the image after image risks are fixed.
FixTime	String	2021-10-14 20:32:05	The timestamp when the task ends. Unit: milliseconds.
FinishTime	String	2021-10-14 20:34:07	The timestamp when the task starts. Unit: milliseconds.
Status	Integer	2	The status of the task. Valid values: • **1**: The task is running. • **2**: The task is successful. • **3**: The task failed.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeImageFixTask
&StartTime=1634725571000
&EndTime=1635575219000
&Status=1
&CurrentPage=1
&PageSize=20
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeImageFixTaskResponse>
    <RequestId>8AC52BBA-85D3-5F64-9B48-D08437CAF916</RequestId>
    <PageInfo>
        <CurrentPage>1</CurrentPage>
        <PageSize>20</PageSize>
        <TotalCount>12</TotalCount>
        <Count>12</Count>
    </PageInfo>
    <BuildTasks>
        <BuildTaskId>ivf-939536b5-c3ca-427b-8183-91007756</BuildTaskId>
        <TaskType>IMAGE_REPAIR</TaskType>
        <RepoNamespace>name-002</RepoNamespace>
        <RepoName>test-redhat</RepoName>
        <RegionId>cn-hangzhou</RegionId>
        <OldTag>centos8.1-ja</OldTag>
        <OldUuid>2fa731681911ae8d1b5f11893ace****</OldUuid>
        <NewTag>redhat8-vault</NewTag>
        <NewUuid>2fa731681911ae8d1b5f11893ace****</NewUuid>
        <FixTime>2021-10-14 20:32:05</FixTime>
        <FinishTime>2021-10-14 20:34:07</FinishTime>
        <Status>2</Status>
    </BuildTasks>
</DescribeImageFixTaskResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "8AC52BBA-85D3-5F64-9B48-D08437CAF916",
  "PageInfo" : {
    "CurrentPage" : 1,
    "PageSize" : 20,
    "TotalCount" : 12,
    "Count" : 12
  },
  "BuildTasks" : [ {
    "BuildTaskId" : "ivf-939536b5-c3ca-427b-8183-91007756",
    "TaskType" : "IMAGE_REPAIR",
    "RepoNamespace" : "name-002",
    "RepoName" : "test-redhat",
    "RegionId" : "cn-hangzhou",
    "OldTag" : "centos8.1-ja",
    "OldUuid" : "2fa731681911ae8d1b5f11893ace****",
    "NewTag" : "redhat8-vault",
    "NewUuid" : "2fa731681911ae8d1b5f11893ace****",
    "FixTime" : "2021-10-14 20:32:05",
    "FinishTime" : "2021-10-14 20:34:07",
    "Status" : 2
  } ]
}
```

Error codes

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

8.7. DescribeImageGroupedVulList

Queries image vulnerabilities.

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	DescribeImageGroupedVulList	The operation that you want to perform. Set the value to **DescribeImageGroupedVulList**.

Parameter	Type	Required	Example	Description
Type	String	No	cve	The type of the vulnerability that you want to query. Valid values: • **CVE**: image system vulnerability • **SCA**: image application vulnerability
GroupId	String	No	1311	The ID of the asset group.
CveId	String	No	CVE-2017-15420	The Common Vulnerabilities and Exposures (CVE) ID of the vulnerability.
Uuids	String	No	uuid-13134124****	The IDs of assets. Separate multiple IDs with commas (,).
Name	String	No	debian:10:CVE-2019-9893	The name of the vulnerability.
AliasName	String	No	DSA-2019 libseccomp security vulnerability	The alias of the vulnerability.
PatchId	Long	No	1341512412	The ID of the patch that is used to fix the vulnerability.
Necessity	String	No	asap	The priority to fix the vulnerability. Valid values: • **asap**: high. You must fix the vulnerability at the earliest opportunity. • **later**: medium. You can fix the vulnerability based on your business requirements. • **nntf**: low. You can ignore the vulnerability.
CurrentPage	Integer	No	1	The number of the page to return. Default value: **1**.
PageSize	Integer	No	20	The number of entries to return on each page. Default value: 20.
RepoRegionId	String	No	cn-hangzhou	The region ID of the image repository.

Parameter	Type	Required	Example	Description
RepoInstanceId	String	No	i-qewqrqcsadf****	The instance ID of the image repository.
RepoId	String	No	qew****	The ID of the image repository.
RepoName	String	No	libssh2	The name of the image repository.
RepoNamespace	String	No	libssh2	The namespace to which the image repository belongs.
ImageTag	String	No	oval	The tag added to the image.
ImageDigest	String	No	w213412341dfsfasdfafadfasfasf	The digest of the image.
ImageLayer	String	No	b1f5b9420803ad0657cf21566e3e20acc08581e7f22991249ef3aa80b8b1c587	The layer of the image.
Lang	String	No	zh	The language of the content within the request and response. Default value: **zh**. Valid values: • **zh**: Chinese • **en**: English
IsLatest	Integer	No	0	Specifies whether to query the vulnerabilities in the latest images. If you do not specify this parameter, the vulnerabilities of all images are queried. Valid values: • **0**: no • **1**: yes

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	2	The page number of the returned page.

Parameter	Type	Example	Description
RequestId	String	5E244439-UJND-8BF7-26F36E21B9AA	The ID of the request, which is used to locate and troubleshoot issues.
PageSize	Integer	20	The number of entries returned per page. Default value: **20**.
TotalCount	Integer	21	The total number of image system vulnerabilities.
GroupedVulItems	Array of GroupedVulItem		The image vulnerabilities.
Status	Integer	0	The status of the vulnerability. Valid values: • **0**: unhandled • **1**: handled • **2**: verifying • **3**: added to the whitelist
Type	String	cve	The type of the vulnerability. Valid values: • **CVE**: image system vulnerability • **SCA**: image application vulnerability
NntfCount	Integer	29	The number of vulnerabilities that have the low priority.
GmtLast	Long	1611201274000	The timestamp when the first scan was performed. Unit: milliseconds.
LastScanTime	Long	1611201274000	The timestamp when the last scan was performed. Unit: milliseconds.
Tags	String	Code execution	The tag added to the vulnerability. Valid values: • Restart required • Remote exploitation • Exploit exists • Exploitable • Privilege escalation • Code execution

Parameter	Type	Example	Description
LaterCount	Integer	26	The number of vulnerabilities that have the medium priority.
AliasName	String	DLA-1730-1: libssh2 LTS security update	The alias of the vulnerability.
Name	String	debian:9:CVE-2019-3858	The name of the vulnerability.
AsapCount	Integer	26	The number of vulnerabilities that have the high priority.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeImageGroupedVulList
&Type=cve
&GroupId=1311
&CveId=CVE-2017-15420
&Uuids=uuid-13134124****
&Name=debian:10:CVE-2019-9893
&AliasName=DSA-2019 libseccomp security vulnerability
&PatchId=1341512412
&Necessity=asap
&CurrentPage=1
&PageSize=20
&RepoRegionId=cn-hangzhou
&RepoInstanceId=i-qewqrqcsadf****
&RepoId=qew****
&RepoName=libssh2
&RepoNamespace=libssh2
&ImageTag=oval
&ImageDigest=w213412341dfsfasdfafadfasfasf
&ImageLayer=b1f5b9420803ad0657cf21566e3e20acc08581e7f22991249ef3aa80b8b1c587
&Lang=zh
&IsLatest=0
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeImageGroupedVulListResponse>
    <CurrentPage>2</CurrentPage>
    <RequestId>5E244439-UJND-8BF7-26F36E21B9AA</RequestId>
    <PageSize>20</PageSize>
    <TotalCount>21</TotalCount>
    <GroupedVulItems>
        <Status>0</Status>
        <Type>cve</Type>
        <NntfCount>29</NntfCount>
        <GmtLast>1611201274000</GmtLast>
        <LastScanTime>1611201274000</LastScanTime>
        <Tags>Code execution</Tags>
        <LaterCount>26</LaterCount>
        <AliasName>DLA-1730-1: libssh2 LTS security update</AliasName>
        <Name>debian:9:CVE-2019-3858</Name>
        <AsapCount>26</AsapCount>
    </GroupedVulItems>
</DescribeImageGroupedVulListResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "CurrentPage" : 2,
  "RequestId" : "5E244439-UJND-8BF7-26F36E21B9AA",
  "PageSize" : 20,
  "TotalCount" : 21,
  "GroupedVulItems" : [ {
    "Status" : 0,
    "Type" : "cve",
    "NntfCount" : 29,
    "GmtLast" : 1611201274000,
    "LastScanTime" : 1611201274000,
    "Tags" : "Code execution",
    "LaterCount" : 26,
    "AliasName" : "DLA-1730-1: libssh2 LTS security update",
    "Name" : "debian:9:CVE-2019-3858",
    "AsapCount" : 26
  } ]
}
```

Error codes

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

8.8. DescribeImageListWithBaselineName

Queries the details about the image baseline risks that are detected.

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	DescribeImageListWithBaselineName	The operation that you want to perform. Set the value to **DescribeImageListWithBaselineName**.
BaselineNameKey	String	Yes	ak_leak	The name of the image baseline risk.
Criteria	String	No	Identity authentication	The condition that is used to query the image baseline risk.
CriteriaType	String	No	BaselineNameAlias	The type of the condition that is used to query the image baseline risk. Valid values: • **BaselineNameAlias**: baseline name • **BaselineClassAlias**: baseline category
RepoInstanceId	String	No	i-qewqrqcsadf****	The instance ID of the image repository.
RepoName	String	No	libssh2	The name of the image repository.
RepoNamespace	String	No	libssh2	The namespace to which the image repository belongs.
ImageDigest	String	No	2e6daffce524ffeae66cccaa90c8fc47de912346dcec295c27395b6d66db6423	The SHA-256 value of the image digest.
PageSize	Integer	No	10	The number of entries to return on each page. Default value: **10**.

Parameter	Type	Required	Example	Description
CurrentPage	Integer	No	1	The number of the page to return. Default value: **1**.
Lang	String	No	zh	The language of the content within the request and response. Default value: **zh**. Valid values: • **zh**: Chinese • **en**: English

Response parameters

Parameter	Type	Example	Description
RequestId	String	5B8C2156-2DB9-5A42-99E7-F2ED5AE9EA1F	The ID of the request, which is used to locate and troubleshoot issues.
PageInfo	Object		The pagination information.
CurrentPage	Integer	1	The page number of the returned page. Default value: **1**.
PageSize	Integer	10	The number of entries returned per page. Default value: **10**.
TotalCount	Integer	1	The total number of images on which baseline risks are detected.
Count	Integer	1	The number of images on which baseline risks are detected and are returned on the current page.
ImageInfos	Array of ImageInfos		Details about images.
MiddleRiskImage	Integer	0	The number of images that have **medium** baseline risks.
RiskStatus	String	YES	Indicates whether the image is at risk. Valid values: • **YES**: yes • **NO**: no

Parameter	Type	Example	Description
ImageCreate	Long	1636962328000	The timestamp when the image was created. Unit: milliseconds.
Digest	String	2e6daffce524ffeae66cccaa90c8fc47de912346dcec295c27395b6d66db6423	The SHA-256 value of the image digest.
Tag	String	v1	The version of the image.
ImageUpdate	Long	1636974116000	The timestamp when the image was updated. Unit: milliseconds.
InstanceId	String	cri-a595qp31knh9****	The ID of the image instance.
LowRiskImage	Integer	0	The number of images that have **low** baseline risks.
RepoType	String	PRIVATE	The type of the image repository.
RegionId	String	cn-beijing	The region ID of the image instance.
Uuid	String	f58681174f944623345379e23b7b****	The UUID of the image.
ImageSize	Integer	157408623	The size of the image.
RepoId	String	crr-1lt6q7167yh6****	The ID of the image repository.
TotalItemCount	Integer	3	The total number of baseline risks that are detected on the image.
HighRiskImage	Integer	1	The number of images that have **high** baseline risks.
NoRiskImage	Integer	0	The number of images that do not have baseline risks.

Parameter	Type	Example	Description
ImageId	String	cddb5fd33b34a1fabb358d0a19497cdfe362fe624821cb250947af0ea5cc****	The ID of the image.
RepoName	String	scanner	The name of the image repository.
RepoNamespace	String	sas	The namespace of the image.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeImageListWithBaselineName
&BaselineNameKey=ak_leak
&Criteria=Identity authentication
&CriteriaType=BaselineNameAlias
&RepoInstanceId=i-qewqrqcsadf****
&RepoName=libssh2
&RepoNamespace=libssh2
&ImageDigest=2e6daffce524ffeae66cccaa90c8fc47de912346dcec295c27395b6d66db6423
&PageSize=10
&CurrentPage=1
&Lang=zh
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeImageListWithBaselineNameResponse>
    <RequestId>5B8C2156-2DB9-5A42-99E7-F2ED5AE9EA1F</RequestId>
    <PageInfo>
        <CurrentPage>1</CurrentPage>
        <PageSize>10</PageSize>
        <TotalCount>1</TotalCount>
        <Count>1</Count>
    </PageInfo>
    <ImageInfos>
        <MiddleRiskImage>0</MiddleRiskImage>
        <RiskStatus>YES</RiskStatus>
        <ImageCreate>1636962328000</ImageCreate>
        <Digest>2e6daffce524ffeae66cccaa90c8fc47de912346dcec295c27395b6d66db6423</Digest>
        <Tag>v1</Tag>
        <ImageUpdate>1636974116000</ImageUpdate>
        <InstanceId>cri-a595qp31knh9****</InstanceId>
        <LowRiskImage>0</LowRiskImage>
        <RepoType>PRIVATE</RepoType>
        <RegionId>cn-beijing</RegionId>
        <Uuid>f58681174f944623345379e23b7b****</Uuid>
        <ImageSize>157408623</ImageSize>
        <RepoId>crr-1lt6q7167yh6****</RepoId>
        <TotalItemCount>3</TotalItemCount>
        <HighRiskImage>1</HighRiskImage>
        <NoRiskImage>0</NoRiskImage>
        <ImageId>cddb5fd33b34a1fabb358d0a19497cdfe362fe624821cb250947af0ea5cc****</ImageId>
        <RepoName>scanner</RepoName>
        <RepoNamespace>sas</RepoNamespace>
    </ImageInfos>
</DescribeImageListWithBaselineNameResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "5B8C2156-2DB9-5A42-99E7-F2ED5AE9EA1F",
  "PageInfo" : {
    "CurrentPage" : 1,
    "PageSize" : 10,
    "TotalCount" : 1,
    "Count" : 1
  },
  "ImageInfos" : [ {
    "MiddleRiskImage" : 0,
    "RiskStatus" : "YES",
    "ImageCreate" : 1636962328000,
    "Digest" : "2e6daffce524ffeae66cccaa90c8fc47de912346dcec295c27395b6d66db6423",
    "Tag" : "v1",
    "ImageUpdate" : 1636974116000,
    "InstanceId" : "cri-a595qp31knh9****",
    "LowRiskImage" : 0,
    "RepoType" : "PRIVATE",
    "RegionId" : "cn-beijing",
    "Uuid" : "f58681174f944623345379e23b7b****",
    "ImageSize" : 157408623,
    "RepoId" : "crr-1lt6q7167yh6****",
    "TotalItemCount" : 3,
    "HighRiskImage" : 1,
    "NoRiskImage" : 0,
    "ImageId" : "cddb5fd33b34a1fabb358d0a19497cdfe362fe624821cb250947af0ea5cc****",
    "RepoName" : "scanner",
    "RepoNamespace" : "sas"
  } ]
}
```

Error codes

HTTP status code	Error code	Error message	Description
500	ServerError	ServerError	The error message returned because a server error occurred.

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

8.9. PublicPreCheckImageScanTask

Queries the number of images to scan in an image scan task and the quota for container image scan to be consumed by the task.

You can call the PublicPreCheckImageScanTask operation to estimate the quota for container image scan to be consumed by the task. This ensures that you know the quota to be consumed before you perform the task. If the remaining quota for container image scan is less than the quota to be consumed by the task, you must purchase a sufficient quota. This prevents the task from being stopped due to an insufficient quota.

When you call this operation, if you do not specify the optional parameters, the total number of protected images and the quota for container image scan to be consumed by scanning all the protected images are queried. If you specify the optional parameters, the number of images that meet the specified conditions and the quota for container image scan to be consumed by scanning the images are queried.

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	PublicPreCheckImageScanTask	The operation that you want to perform. Set the value to **PublicPreCheckImageScanTask**.
SourceIp	String	No	1.2.X.X	The source IP address of the request.
RegistryTypes	String	No	acr	The type of the image repository. Separate multiple types with commas (,). Valid values: • **acr** • **harbor** • **quay**
RegionIds	String	No	cn-hangzhou	The region ID of the image. Separate multiple IDs with commas (,).
InstanceIds	String	No	i-uf6j8vq9l4r5ntht****	The ID of the Container Registry instance in which the image repository is created. Separate multiple IDs with commas (,).
RepoNamespaces	String	No	hanghai-namespace	The namespace to which the image repository belongs. Separate multiple namespaces with commas (,).

Parameter	Type	Required	Example	Description
RepoIds	String	No	crr-vridcl4****	The ID of the image repository. Separate multiple IDs with commas (,).
RepoNames	String	No	centos	The name of the image repository. Separate multiple names with commas (,).
Digests	String	No	6a5e103187b31a94592a47a5858617f7****	The SHA-256 value of the digest of the image. Separate multiple SHA-256 values with commas (,).
Tags	String	No	0.2	The tag added to the image. Separate multiple tags with commas (,).

Response parameters

Parameter	Type	Example	Description
RequestId	String	F9353221-40F4-5F98-B73C-2803DC804033	The ID of the request, which is used to locate and troubleshoot issues.
Data	Object		The data returned if the call is successful.
ScanImageCount	Integer	3	The quota of container image scan to be consumed by the task.
NeedAuthCount	Integer	6	The number of images to scan in the task.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=PublicPreCheckImageScanTask
&SourceIp=1.2.X.X
&RegistryTypes=acr
&RegionIds=cn-hangzhou
&InstanceIds=i-uf6j8vq9l4r5ntht****
&RepoNamespaces=hanghai-namespace
&RepoIds=crr-vridcl4****
&RepoNames=centos
&Digests=6a5e103187b31a94592a47a5858617f7****
&Tags=0.2
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<PublicPreCheckImageScanTaskResponse>
    <RequestId>F9353221-40F4-5F98-B73C-2803DC804033</RequestId>
    <Data>
        <ScanImageCount>3</ScanImageCount>
        <NeedAuthCount>6</NeedAuthCount>
    </Data>
</PublicPreCheckImageScanTaskResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "F9353221-40F4-5F98-B73C-2803DC804033",
  "Data" : {
    "ScanImageCount" : 3,
    "NeedAuthCount" : 6
  }
}
```

Error codes

HTTP status code	Error code	Error message	Description
500	ServerError	ServerError	The error message returned because a server error occurred.

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

8.10. PublicCreateImageScanTask

Creates an image scan task.

Before you call the PublicCreateImageScanTask operation, we recommend that you call the PublicPreCheckImageScanTask operation to query the number of images to scan and the quota for container image scan to be consumed by the image scan task. Make sure that the remaining quota for container image scan is sufficient. This prevents the task from being stopped due to an insufficient quota.

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	PublicCreateImageScanTask	The operation that you want to perform. Set the value to **PublicCreateImageScanTask**.
SourceIp	String	No	1.2.X.X	The source IP address of the request.
RegistryTypes	String	No	acr	The type of the image repository. Separate multiple types with commas (,). Valid values: • **acr** • **harbor** • **quay**
RegionIds	String	No	cn-hangzhou	The region ID of the image. Separate multiple IDs with commas (,).
InstanceIds	String	No	i-uf6j8vq9l4r5ntht****	The ID of the Container Registry instance in which the image repository is created. Separate multiple IDs with commas (,).
RepoNamespaces	String	No	hanghai-namespace	The namespace to which the image repository belongs. Separate multiple namespaces with commas (,).
RepoIds	String	No	crr-vridcl4****	The ID of the image repository. Separate multiple IDs with commas (,).
RepoNames	String	No	centos	The name of the image repository. Separate multiple names with commas (,).
Digests	String	No	6a5e103187b31a94592a47a5858617f7a6c	The SHA-256 value of the digest of the image. Separate multiple SHA-256 values with commas (,).
Tags	String	No	0.2	The tag added to the image. Separate multiple tags with commas (,).

Response parameters

Parameter	Type	Example	Description
RequestId	String	F9353221-40F4-5F98-B73C-2803DC804033	The ID of the request, which is used to locate and troubleshoot issues.
Data	Object		The data returned if the call is successful.
TaskId	String	a410bb3e68c217a3368bc0238c66886d	The ID of the image scan task.
TotalCount	Integer	5	The total number of images to scan.
FinishCount	Integer	5	The number of images that have been scanned.
CollectTime	Long	1644286364150	The timestamp when the information about the image was collected. Unit: milliseconds.
ExecTime	Long	1644286364150	The timestamp when the image scan task started to run. Unit: milliseconds.
Status	String	SUCCESS	The status of the image scan task. Valid values: • **INIT**: The task is being initialized. • **PRE_ANALYZER**: The task is being pre-processed. • **SUCCESS**: The task is successful. • **FAIL**: The task fails.
Progress	Integer	100	The progress of the image scan task in percentage.

Parameter	Type	Example	Description
Result	String	SUCCESS	The result of the image scan task. Valid values: • **SUCCESS**: The task is successful. • **TASK_NOT_SUPPORT_REGION**: The image is deployed in a region that is not supported by container image scan. **Note** For more information about the regions supported by container image scan, see the table that follows the "Response parameters" section of this topic.
CanCreate	Boolean	true	Indicates whether you can continue to create an image scan task. Valid values: • **true**: yes • **false**: no **Note** By default, a maximum of 10 image scan tasks can be running at the same time. If more than 10 image scan tasks are running, you cannot create an image scan task by calling this operation. You must wait for at least one of the 10 existing image scan tasks to complete before you can create an image scan task.

Regions supported by container image scan

Region	City	Region ID
China (Hangzhou)	Hangzhou	cn-hangzhou
China (Shanghai)	Shanghai	cn-shanghai
China (Shenzhen)	Shenzhen	cn-shenzhen
China (Qingdao)	Qingdao	cn-qingdao
China (Beijing)	Beijing	cn-beijing

Region	City	Region ID
China (Zhangjiakou)	Zhangjiakou	cn-zhangjiakou
China (Hohhot)	Hohhot	cn-huhehaote
China (Hong Kong)	Hong Kong	cn-hongkong
Japan (Tokyo)	Tokyo	ap-northeast-1
Indonesia (Jakarta)	Jakarta	ap-southeast-5
US (Silicon Valley)	Silicon Valley	us-west-1
US (Virginia)	Virginia	us-east-1
Germany (Frankfurt)	Frankfurt	eu-central-1
UK (London)	London	eu-west-1

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=PublicCreateImageScanTask
&SourceIp=1.2.X.X
&RegistryTypes=acr
&RegionIds=cn-hangzhou
&InstanceIds=i-uf6j8vq9l4r5ntht****
&RepoNamespaces=hanghai-namespace
&RepoIds=crr-vridcl4****
&RepoNames=centos
&Digests=6a5e103187b31a94592a47a5858617f7****
&Tags=0.2
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<PublicCreateImageScanTaskResponse>
    <RequestId>F9353221-40F4-5F98-B73C-2803DC804033</RequestId>
    <Data>
        <TaskId>a410bb3e68c217a3368bc0238c66886d</TaskId>
        <TotalCount>5</TotalCount>
        <FinishCount>5</FinishCount>
        <CollectTime>1644286364150</CollectTime>
        <ExecTime>1644286364150</ExecTime>
        <Status>SUCCESS</Status>
        <Progress>100</Progress>
        <Result>SUCCESS</Result>
        <CanCreate>true</CanCreate>
    </Data>
</PublicCreateImageScanTaskResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "F9353221-40F4-5F98-B73C-2803DC804033",
  "Data" : {
    "TaskId" : "a410bb3e68c217a3368bc0238c66886d",
    "TotalCount" : 5,
    "FinishCount" : 5,
    "CollectTime" : 1644286364150,
    "ExecTime" : 1644286364150,
    "Status" : "SUCCESS",
    "Progress" : 100,
    "Result" : "SUCCESS",
    "CanCreate" : true
  }
}
```

Error codes

HTTP status code	Error code	Error message	Description
500	ServerError	ServerError	The error message returned because a server error occurred.

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

8.11. PublicSyncAndCreateImageScanTask

Adds images to Security Center on the Assets page and creates an image scan task to scan the images.

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	PublicSyncAndCreateImageScanTask	The operation that you want to perform. Set the value to **PublicSyncAndCreateImageScanTask**.
SourceIp	String	No	1.2.X.X	The source IP address of the request.

Images	String	No	[{"registryType":"acr","repoId":"crr-red9kgqqi0fh75d5","instanceId":"cri-1x2qtjd75ofqvfa8","repoNamespace":"1125","regionId":"cn-hangzhou","repoName":"script1","digest":"b1064a5007786b6f82a50772858e8156bc1e5fbddb7dd20af6922761ad197fe4","tag":"v0113-ver2","createTime":1641267666666,"updateTime":1641267909090}]	The information about the images. The value of this parameter is in the JSON format and contains the following fields:
				• **RegistryType**: the type of the image repository. Valid values:
				  ○ acr
				  ○ harbor
				  ○ quay
				• **RepoId**: the ID of the image repository.
				• **InstanceId**: the ID of the Container Registry instance to which the image repository belongs.
				• **RepoNamespace**: the namespace to which the image repository belongs.
				• **RegionId**: the region ID of the image.
				• **RepoName**: the name of the image repository.
				• **Digest**: the digest of the image.
				• **Tag**: the tag added to the image.
				• **CreateTime**: the timestamp when the image was created. Unit: milliseconds.
				• **UpdateTime**: the timestamp when the image was updated. Unit: milliseconds.

Response parameters

Parameter	Type	Example	Description
RequestId	String	F9353221-40F4-5F98-B73C-2803DC804033	The ID of the request, which is used to locate and troubleshoot issues.
Data	Object		The data returned if the call is successful.
TaskId	String	a410bb3e68c217a3368bc0238c66886d	The ID of the image scan task.
TotalCount	Integer	5	The total number of images to scan.
FinishCount	Integer	5	The number of images that have been scanned.
CollectTime	Long	1644286364150	The timestamp when the information about the image was collected. Unit: milliseconds.
ExecTime	Long	1644286364150	The timestamp when the image scan task started to run. Unit: milliseconds.
Status	String	SUCCESS	The status of the image scan task. Valid values: • **INIT**: The task is being initialized. • **PRE_ANALYZER**: The task is being pre-processed. • **SUCCESS**: The task is successful. • **FAIL**: The task fails.
Progress	Integer	100	The progress of the image scan task.
Result	String	SUCCESS	The result of the image scan task. Valid values: • **SUCCESS**: The task is successful. • **TASK_NOT_SUPPORT_REGION**: The image is in a region that is not supported by container image scan.

Parameter	Type	Example	Description
CanCreate	Boolean	true	Indicates whether you can continue to create an image scan task. Valid values: • **true**: yes • **false**: no **Note** By default, a maximum of 10 image scan tasks can be running at the same time. If more than 10 image scan tasks are running, you cannot create an image scan task by calling this operation. You must wait for at least one of the 10 existing image scan tasks to complete before you can create an image scan task.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=PublicSyncAndCreateImageScanTask
&SourceIp=1.2.X.X
&Images=[{"registryType":"acr","repoId":"crr-red9kgqqi0fh75d5","instanceId":"cri-1x2qtjd75ofqvfa8","repoNamespace":"1125","regionId":"cn-hangzhou","repoName":"script1","digest":"b1064a5007786b6f82a50772858e8156bc1e5fbddb7dd20af6922761ad197fe4","tag":"v0113-ver2","createTime":1641267666666,"updateTime":1641267909090}]
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<PublicSyncAndCreateImageScanTaskResponse>
    <RequestId>F9353221-40F4-5F98-B73C-2803DC804033</RequestId>
    <Data>
        <TaskId>a410bb3e68c217a3368bc0238c66886d</TaskId>
        <TotalCount>5</TotalCount>
        <FinishCount>5</FinishCount>
        <CollectTime>1644286364150</CollectTime>
        <ExecTime>1644286364150</ExecTime>
        <Status>SUCCESS</Status>
        <Progress>100</Progress>
        <Result>SUCCESS</Result>
        <CanCreate>true</CanCreate>
    </Data>
</PublicSyncAndCreateImageScanTaskResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "F9353221-40F4-5F98-B73C-2803DC804033",
  "Data" : {
    "TaskId" : "a410bb3e68c217a3368bc0238c66886d",
    "TotalCount" : 5,
    "FinishCount" : 5,
    "CollectTime" : 1644286364150,
    "ExecTime" : 1644286364150,
    "Status" : "SUCCESS",
    "Progress" : 100,
    "Result" : "SUCCESS",
    "CanCreate" : true
  }
}
```

Error codes

HTTP status code	Error code	Error message	Description
500	ServerError	ServerError	The error message returned because a server error occurred.

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

8.12. DescribeImageVulList

旧版本不翻译

Action	String		DescribeImageVulList	
Lang	String		zh	• •
Type	String		cve	
Uuids	String		0004a32a0305a7f6ab5ff9600d47****	
Name	String		debian:10:CVE-2019-9893	
AliasName	String			

StatusList	String		1	• • •
Necessity	String		asap	• • •
Dealed	String		y	• •
CurrentPage	Integer		1	
PageSize	Integer		10	
RepoRegionId	String		cn-hangzhou	
RepoInstanceId	String		i-qewqrqcsadf****	
RepoId	String		qew****	
RepoName	String		libssh2	
RepoNamespace	String		libssh2	
RegionId	String		cn-hangzhou	
InstanceId	String		1-qeqewqw****	
Tag	String		oval	
Digest	String		8f0fbdb41d3d1ade4ffdf21558443f4c03342010563bb8c43ccc09594d507012	

CurrentPage	Integer	1	
RequestId	String	D6B20156-49B0-5CF0-B14D-7ECA4B50DAAB	
PageSize	Integer	10	
TotalCount	Integer	1	

VulRecords	Array of VulRecord		
CanUpdate	Boolean	true	• •
Type	String	cve	
Status	Integer	1	• •
ModifyTs	Long	1580808765000	
ImageDigest	String	8f0fbdb41d3d1ade4ffdf21558443f4c03342010563bb8c43ccc09594d507012	
PrimaryId	Long	782661	
Tag	String	oval	
RepoNamespace	String	default	
RepoName	String	varnish	
Related	String	CVE-2019-9893	
FirstTs	Long	1620752053000	
LastTs	Long	1631779996000	
Necessity	String	asap	• • •
Uuid	String	0004a32a0305a7f6ab5ff9600d47****	
AliasName	String		
Name	String	debian:10:CVE-2019-9893	
Layers	Array of String	["null"]	
ExtendContentJson	Object		

OsRelease	String	10.9	
Os	String	debian	
RpmEntityList	Array of RpmEntity		
MatchList	String	["libseccomp2 version less than equals 2.3.3-4"]	
Layer	String	b1f5b9420803ad0657cf21566e3e20acc08581e7f22991249ef3aa80b8b1c587	
FullVersion	String	2.3.3-4	
Version	String	2.3.3-4	
MatchDetail	String	libseccomp2 version less than equals 2.3.3-4	
Path	String	/usr/lib64/libssh2.so.1	
Name	String	libseccomp2	
UpdateCmd	String	apt-get update && apt-get install libseccomp2 --only-upgrade	

```
http(s)://[Endpoint]/?Action=DescribeImageVulList
&Lang=zh
&Type=cve
&Uuids=0004a32a0305a7f6ab5ff9600d47****
&Name=debian:10:CVE-2019-9893
&StatusList=1
&Necessity=asap
&Dealed=y
&CurrentPage=1
&PageSize=10
&RepoRegionId=cn-hangzhou
&RepoInstanceId=i-qewqrqcsadf****
&RepoId=qew****
&RepoName=libssh2
&RepoNamespace=libssh2
&RegionId=cn-hangzhou
&InstanceId=1-qeqewqw****
&Tag=oval
&Digest=8f0fbdb41d3d1ade4ffdf21558443f4c03342010563bb8c43ccc09594d507012
```

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeImageVulListResponse>
    <CurrentPage>1</CurrentPage>
    <RequestId>D6B20156-49B0-5CF0-B14D-7ECA4B50DAAB</RequestId>
    <PageSize>10</PageSize>
    <TotalCount>1</TotalCount>
    <VulRecords>
        <CanUpdate>true</CanUpdate>
        <Type>cve</Type>
        <Status>1</Status>
        <ModifyTs>1580808765000</ModifyTs>
        <ImageDigest>8f0fbdb41d3d1ade4ffdf21558443f4c03342010563bb8c43ccc09594d507012</Imag
eDigest>
        <PrimaryId>782661</PrimaryId>
        <Tag>oval</Tag>
        <RepoNamespace>default</RepoNamespace>
        <RepoName>varnish</RepoName>
        <Related>CVE-2019-9893</Related>
        <FirstTs>1620752053000</FirstTs>
        <LastTs>1631779996000</LastTs>
        <Necessity>asap</Necessity>
        <Uuid>0004a32a0305a7f6ab5ff9600d47****</Uuid>
        <Name>debian:10:CVE-2019-9893</Name>
        <Layers>["null"]</Layers>
        <ExtendContentJson>
            <OsRelease>10.9</OsRelease>
            <Os>debian</Os>
            <RpmEntityList>
                <MatchList>["libseccomp2 version less than equals 2.3.3-4"]</MatchList>
                <Layer>b1f5b9420803ad0657cf21566e3e20acc08581e7f22991249ef3aa80b8b1c587</La
yer>
                <FullVersion>2.3.3-4</FullVersion>
                <Version>2.3.3-4</Version>
                <MatchDetail>libseccomp2 version less than equals 2.3.3-4</MatchDetail>
                <Path>/usr/lib64/libssh2.so.1</Path>
                <Name>libseccomp2</Name>
                <UpdateCmd>apt-get update &amp;amp;&amp;amp; apt-get install libseccomp2  --only-up
grade</UpdateCmd>
            </RpmEntityList>
        </ExtendContentJson>
    </VulRecords>
</DescribeImageVulListResponse>
```

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "CurrentPage" : 1,
  "RequestId" : "D6B20156-49B0-5CF0-B14D-7ECA4B50DAAB",
  "PageSize" : 10,
  "TotalCount" : 1,
  "VulRecords" : [ {
    "CanUpdate" : true,
    "Type" : "cve",
    "Status" : 1,
    "ModifyTs" : 1580808765000,
    "ImageDigest" : "8f0fbdb41d3d1ade4ffdf21558443f4c03342010563bb8c43ccc09594d507012",
    "PrimaryId" : 782661,
    "Tag" : "oval",
    "RepoNamespace" : "default",
    "RepoName" : "varnish",
    "Related" : "CVE-2019-9893",
    "FirstTs" : 1620752053000,
    "LastTs" : 1631779996000,
    "Necessity" : "asap",
    "Uuid" : "0004a32a0305a7f6ab5ff9600d47****",
    "Name" : "debian:10:CVE-2019-9893",
    "Layers" : [ "[\"null\"]" ],
    "ExtendContentJson" : {
      "OsRelease" : "10.9",
      "Os" : "debian",
      "RpmEntityList" : [ {
        "MatchList" : "[\"libseccomp2 version less than equals 2.3.3-4\"]",
        "Layer" : "b1f5b9420803ad0657cf21566e3e20acc08581e7f22991249ef3aa80b8b1c587",
        "FullVersion" : "2.3.3-4",
        "Version" : "2.3.3-4",
        "MatchDetail" : "libseccomp2 version less than equals 2.3.3-4",
        "Path" : "/usr/lib64/libssh2.so.1",
        "Name" : "libseccomp2",
        "UpdateCmd" : "apt-get update && apt-get install libseccomp2  --only-upgrade"
      } ]
    }
  } ]
}
```

HttpCode			
500	ServerError	ServerError	

9.Log analysis

9.1. ModifyOpenLogShipper

Activates Log Service.

Prerequisites

A service-linked role is created and Security Center is authorized to access cloud resources. You can call the CreateServiceLinkedRole operation to create service-linked roles and authorize Security Center to access cloud resources.

Scenarios

Before you use the log analysis feature of Security Center, you must call the ModifyOpenLogShipper operation to activate Log Service.

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	ModifyOpenLogShipper	The operation that you want to perform. Set the value to **ModifyOpenLogShipper**.
From	String	No	sas	The ID of the request source. Set the value to **sas**.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	25EC270F-5783-4416-AD7C-1EDF063A039C	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<ModifyOpenLogShipperResponse>
      <RequestId>25EC270F-5783-4416-AD7C-1EDF063A039C</RequestId>
</ModifyOpenLogShipperResponse>
```

`JSON` format

```
{
    "RequestId":"25EC270F-5783-4416-AD7C-1EDF063A039C"
}
```

Error codes

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

9.2. DescribeLogstoreStorage

Queries the purchased log storage capacity.

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	DescribeLogstoreStorage	The operation that you want to perform. Set the value to **DescribeLogstoreStorage**.
Lang	String	No	zh	The natural language of the request and response. Default value: **zh**. Valid values: • **zh**: Chinese • **en**: English
From	String	No	sas	The ID of the request source. Set the value to **sas**.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
Logstore	String	sas-log	The name of the dedicated Logstore that is used to store full logs of Security Center. The value is fixed as **sas-log**.
Preserve	Long	12240	The purchased log storage capacity, in GB.
RequestId	String	25EC270F-5783-4416-AD7C-1EDF063A039C	The ID of the request.
Ttl	Integer	180	The number of days during which logs can be retained. The value is fixed as **180**, which indicates that logs can be retained for 180 days. **Note** You are not allowed to change the value of this parameter.
Used	Long	335	The used log storage capacity, in GB.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DescribeLogstoreStorageResponse>
      <RequestId>25EC270F-5783-4416-AD7C-1EDF063A039C</RequestId>
      <Used>335.14641880244017</Used>
      <Logstore>sas-log</Logstore>
      <Ttl>180</Ttl>
      <Preserve>12240</Preserve>
</DescribeLogstoreStorageResponse>
```

`JSON` format

```
{
    "RequestId":"25EC270F-5783-4416-AD7C-1EDF063A039C",
    "Used":"335",
    "Logstore":"sas-log",
    "Ttl":"180",
    "Preserve":"12240"
}
```


Error codes

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

9.3. ModifyClearLogstoreStorage

Deletes all logs that occupy your log storage.

Deleted logs cannot be restored. Before you call this operation to delete all logs and free up log storage, we recommend that you export and save your logs to your computer.

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	ModifyClearLogstoreStorage	The operation that you want to perform. Set the value to **ModifyClearLogstoreStorage**.
Lang	String	No	zh	The language of the content within the request and response. Default value: **zh**. Valid values: • **zh**: Chinese • **en**: English
From	String	No	sas	The ID of the request source. Set the value to **sas**.

Response parameters

Parameter	Type	Example	Description
RequestId	String	DC84C453-8561-5EC4-B0E9-44E67ACCB5B5	The ID of the request, which is used to locate and troubleshoot issues.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyClearLogstoreStorage
&Lang=zh
&From=sas
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<ModifyClearLogstoreStorageResponse>
    <RequestId>DC84C453-8561-5EC4-B0E9-44E67ACCB5B5</RequestId>
</ModifyClearLogstoreStorageResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "DC84C453-8561-5EC4-B0E9-44E67ACCB5B5"
}
```

Error codes

HTTP status code	Error code	Error message	Description
500	ServerError	ServerError	The error message returned because a server error occurred.

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

10.Notifications

10.1. DescribeDingTalk

You can call this operation to query DingTalk notifications.

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	DescribeDingTalk	The operation that you want to perform. Set the value to DescribeDingTalk.
RuleActionName	String	No	Vulnerability notifications	The name of the notification.
PageSize	Integer	Optional	20	The number of entries to return on each page.
CurrentPage	Integer	No	1	The page number of the returned page.

Response parameters

Parameter	Type	Example	Description
RequestId	String	B256A525-7E42-4BB9-A27C-9017FDDFF1A2	The ID of the request.
ActionList	Array		The list of notifications.
GmtModified	Long	1550828400000	The time when the notification was modified.
Id	Integer	1	The ID of the notification.

Parameter	Type	Example	Description
AliUid	Long	12312412341	The UID of the user.
GmtCreate	Long	1550828400000	The time when the notification was created.
Url	String	https://oapi.dingtalk.com/robot/send	The parameters of the notification.
IntervalTime	Integer	1000	The notification interval.
ActionName	String	Alerts	The name of the notification.
Status	Integer	1	The status of the notification. Valid values: • **0**: Notifications are disabled. • **1**: Notifications are enabled.
ConfigList	String	[{\"type\":\"vul\",\"configItemList\":[{\"key\":\"key\",\"valueList\":\"123\"}]}]	The list of notification settings.
GroupIdList	String	"123,456"	The list of group IDs.
DingTalkLang	String	zh	The language of notifications. Valid values: • **zh**: Chinese • **en**: English
PageInfo	Struct		The pagination information.
PageSize	Integer	20	The number of entries returned per page.
TotalCount	Integer	1	The total number of notifications.
CurrentPage	Integer	1	The page number of the returned page.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DescribeDingTalkResponse>
    <PageInfo>
        <PageSize>20</PageSize>
        <CurrentPage>1</CurrentPage>
        <TotalCount>1</TotalCount>
    </PageInfo>
    <ActionList>
        <ActionName>Alerts</ActionName>
        <GmtCreate>1550828400000</GmtCreate>
        <GmtModified>1550828400000</GmtModified>
        <IntervalTime>1000</IntervalTime>
        <Id>1</Id>
        <Url>https://oapi.dingtalk.com/robot/send</Url>
        <AliUid>12312412341</AliUid>
        <configList>[{"type":"vul","configItemList":[{"key":"key", "valueList":"123"}]}]</c
onfigList>
        <groupIdList>123,456</groupIdList>
    </ActionList>
    <requestId>B256A525-7E42-4BB9-A27C-9017FDDFF1A2</requestId>
</DescribeDingTalkResponse>
```

`JSON` format

```
{
    "PageInfo": {
      "PageSize": 20,
      "CurrentPage": 1,
      "TotalCount":1
    },
    "ActionList": [{
      "ActionName": "Alerts",
      "GmtCreate": "1550828400000",
      "GmtModified": "1550828400000",
      "IntervalTime": 1000,
      "Id": 1,
      "Url": "https://oapi.dingtalk.com/robot/send",
      "AliUid": 12312412341,
      "configList":"[{\"type\":\"vul\",\"configItemList\":[{\"key\":\"key\", \"valueList\":
\"123\"}]}]",
      "groupIdList":"123,456"
    }],
  "requestId": "B256A525-7E42-4BB9-A27C-9017FDDFF1A2"
}
```

Error codes

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

10.2. DescribeNoticeConfig

You can call this operation to query the notification settings.

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	DescribeNoticeConfig	The operation that you want to perform. Set the value to DescribeNoticeConfig.
SourceIp	String	No	1.2.3.4	The source IP address of the request.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D185B7FF-E24C-422D-83D3-C2A25C7A2727	The ID of the request.
NoticeConfigList	Array		The list of notification settings.
TimeLimit	Integer	1	The time period during which notifications can be sent to the recipients. Valid values: • **0**: any time • **1**: 08:00 to 22:00
Route	Integer	7	The notification method.
Project	String	sas_suspicious	The project identifier.
AliUid	Long	121234141424	The AliUid of the user.
CurrentPage	Integer	1	The page number of the returned page.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DescribeNoticeConfigResponse>
    <RequestId>D185B7FF-E24C-422D-83D3-C2A25C7A2727</RequestId>
    <NoticeConfigList>
        <Project>sas_suspicious</Project>
        <CurrentPage>1</CurrentPage>
        <TimeLimit>1</TimeLimit>
        <Route>7</Route>
        <AliUid>1049769453489698</AliUid>
    </NoticeConfigList>
    <NoticeConfigList>
        <Project>sas_healthcheck</Project>
        <CurrentPage>1</CurrentPage>
        <TimeLimit>1</TimeLimit>
        <Route>7</Route>
        <AliUid>1049769453489698</AliUid>
    </NoticeConfigList>
</DescribeNoticeConfigResponse>
```

`JSON` format

```
{
  "RequestId":"D185B7FF-E24C-422D-83D3-C2A25C7A2727",
  "NoticeConfigList":[
    {
      "Project":"sas_suspicious",
      "CurrentPage":1,
      "TimeLimit":1,
      "Route":7,
      "AliUid":10497611111111
    },
    {
      "Project":"sas_healthcheck",
      "CurrentPage":1,
      "TimeLimit":1,
      "Route":7,
      "AliUid":10422222222
    }
  ]
}
```

Error codes

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

11.Agent client

11.1. SasInstallCode

You can call this operation to obtain the verification key used to run the agent installation command.

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	SasInstallCode	The operation that you want to perform. Set the value to **SasInstallCode**.
SourceIp	String	No	1.2.3.4	The source IP address of the request.

Response parameters

Parameter	Type	Example	Description
RequestId	String	B256A525-7E42-4BB9-A27C-9017FDDFF1A2	The ID of the request.
data	String	eDkhGP	The verification key used to run the installation command when you manually install the Security Center agent on your assets.

Examples

Sample requests

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

Sample success responses

`XML` fomat

```
<SasInstallCodeResponse>
  <requestId>B256A525-7E42-4BB9-A27C-9017FDDFF1A2</requestId>
  <data>eDkhGP</data>
</SasInstallCodeResponse>
```

`JSON` format

```
{
  "requestId": "B256A525-7E42-4BB9-A27C-9017FDDFF1A2",
  "data":"eDkhGP"
}
```

Error code

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

11.2. PauseClient

Enables or disables the Security Center agent.

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	PauseClient	The operation that you want to perform. Set the value to **PauseClient**.
Uuids	String	Yes	uuid-1211-sadsd-2131	The list of servers for which you want to enable or disable the Security Center agent.
Value	String	Yes	1	The status of the Security Center agent. Valid values: • **0**: disabled • **1**: enabled

Response parameters

Parameter	Type	Example	Description

Parameter	Type	Example	Description
RequestId	String	6673D49C-A9AB-40DD-B4A2-B92306701AE7	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=PauseClient
&Uuids=uuid-1211-sadsd-2131
&Value=1
&<Common request parameters>
```

Sample success responses

`XML` format

```
<PauseClientResponse>
  <requestId>6673D49C-A9AB-40DD-B4A2-B92306701AE7</requestId>
</PauseClientResponse>
```

`JSON` format

```
{
 "requestId": "6673D49C-A9AB-40DD-B4A2-B92306701AE7"
}
```

Error codes

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

11.3. OperateAgentClientInstall

Installs the Security Center agent on servers.

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	OperateAgentClientInstall	The operation that you want to perform. Set the value to **OperateAgentClientInstall**.

Parameter	Type	Required	Example	Description
InstanceIds	String	No	i-uf6j8vq9l4r5ntht****	The IDs of the servers on which you want to install the Security Center agent. Separate multiple IDs with commas (,). **Note** You must specify at least one of the **InstanceIds** and **Uuids** parameters before you can call this operation.
Uuids	String	No	1587bedb-fdb4-48c4-9330-**********	The UUIDs of the servers on which you want to install the Security Center agent. Separate multiple UUIDs with commas (,). **Note** You must specify at least one of the **InstanceIds** and **Uuids** parameters before you can call this operation.

Response parameters

Parameter	Type	Example	Description
RequestId	String	AE79B457-877C-51C6-AD72-0D34A025D***	The ID of the request, which is used to locate and troubleshoot issues.
AegisCelintInstallResponseList	Array of AegisCelintInstallRespose		The results that are returned.
Uuid	String	1587bedb-fdb4-48c4-9330-****	The UUID of the server.
InstanceId	String	i-uf6j8vq9l4r5ntht****	The instance ID of the server.
RecordId	Long	2856	The ID of the installation task.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=OperateAgentClientInstall
&InstanceIds=i-uf6j8vq9l4r5ntht****
&Uuids=1587bedb-fdb4-48c4-9330-************
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<OperateAgentClientInstallResponse>
    <RequestId>AE79B457-877C-51C6-AD72-0D34A025D***</RequestId>
    <AegisCelintInstallResposeList>
        <Uuid>1587bedb-fdb4-48c4-9330-****</Uuid>
        <InstanceId>i-uf6j8vq9l4r5ntht****</InstanceId>
        <RecordId>2856</RecordId>
    </AegisCelintInstallResposeList>
</OperateAgentClientInstallResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "AE79B457-877C-51C6-AD72-0D34A025D***",
  "AegisCelintInstallResposeList" : [ {
    "Uuid" : "1587bedb-fdb4-48c4-9330-****",
    "InstanceId" : "i-uf6j8vq9l4r5ntht****",
    "RecordId" : 2856
  } ]
}
```

Error codes

HTTP status code	Error code	Error message	Description
500	ServerError	ServerError	The error message returned because a server error occurred.

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

11.4. DescribeInstallCaptcha

Queries the verification code for you to manually install the Security Center agent.

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 a sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeInstallCaptcha	The operation that you want to perform. Set the value to **DescribeInstallCaptcha**.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The natural language of the request and response. Valid values: • **zh**: Chinese • **en**: English
Deadline	String	No	2020-10-11 16:26:22	The validity period of the verification code. If this parameter is not specified, the default validity period is one hour. **Note** The verification code is valid only within the validity period. If the verification code expires, you cannot manually install the Security Center agent.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
CaptchaCode	String	M1HH**	The verification code for you to manually install the agent.

Parameter	Type	Example	Description
Deadline	String	2020-10-10 16:06:38	The validity period of the verification code. **Note** The verification code is valid only within the validity period. An expired verification code cannot be used to install the agent.
RequestId	String	4E5BFDCF-B9DD-430D-9DA4-151BCB581C9D	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DescribeInstallCaptcha>
      <RequestId>A45EB449-0913-4FAF-B5C0-0F2812F69FB4</RequestId>
      <Deadline>2020-10-10 16:06:38</Deadline>
      <CaptchaCode>M1HH**</CaptchaCode>
</DescribeInstallCaptcha>
```

`JSON` format

```
{
    "DescribeInstallCaptcha": {
        "RequestId": "A45EB449-0913-4FAF-B5C0-0F2812F69FB4",
        "Deadline": "2020-10-10 16:06:38",
        "CaptchaCode": "M1HH**"
    }
}
```

Error codes

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

11.5. DescribeInstallCodes

Queries the commands that are used to manually install the Security Center agent.

Usage notes

You can call the DescribeInstallCodes operation to query the commands that are used to manually install the Security Center agent. The returned results contain the installation verification code and the server information. If you want to manually install the Security Center agent on your server, you can call this operation to query installation commands.

Limits

You can call this operation up to 10 times per second per account. If the number of the calls per second exceeds the limit, throttling is triggered. As a result, your business may be affected. We recommend that you take note of the limit when you call this operation.

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	DescribeInstallCodes	The operation that you want to perform. Set the value to **DescribeInstallCodes**.

Response parameters

Parameter	Type	Example	Description
RequestId	String	C0D6119F-92EE-1276-B8B6-C81A7F9D57F5	The ID of the request, which is used to locate and troubleshoot issues.
InstallCodes	Array of InstallCode		The information about the installation command.
OnlyImage	Boolean	false	Indicates whether an image is used to install the Security Center agent. Valid values: • **true**: yes • **false**: no
CaptchaCode	String	15v02r	The verification code for you to manually install the Security Center agent.
GroupId	Long	9165712	The ID of the server group to which the server belongs.

Parameter	Type	Example	Description
GroupName	String	Ungrouped	The name of the server group to which the server belongs.
ExpiredDate	Long	1637810007000	The timestamp when the installation command expires. Unit: milliseconds.
VendorName	String	Tencent Cloud	The name of the server provider.
Os	String	linux	The operating system of the server.

Examples

Sample requests

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

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeInstallCodesResponse>
    <RequestId>C0D6119F-92EE-1276-B8B6-C81A7F9D57F5</RequestId>
    <InstallCodes>
        <OnlyImage>false</OnlyImage>
        <CaptchaCode>15v02r</CaptchaCode>
        <GroupId>9165712</GroupId>
        <GroupName>Ungrouped</GroupName>
        <ExpiredDate>1637810007000</ExpiredDate>
        <VendorName>Tencent Cloud</VendorName>
        <Os>linux</Os>
    </InstallCodes>
</DescribeInstallCodesResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "C0D6119F-92EE-1276-B8B6-C81A7F9D57F5",
  "InstallCodes" : [ {
    "OnlyImage" : false,
    "CaptchaCode" : "15v02r",
    "GroupId" : 9165712,
    "GroupName" : "Ungrouped",
    "ExpiredDate" : 1637810007000,
    "VendorName" : "Tencent Cloud",
    "Os" : "linux"
  } ]
}
```

Error codes

HTTP status code	Error code	Error message	Description
500	ServerError	ServerError	The error message returned because a server error occurred.

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

11.6. UnbindAegis

Unbinds servers that are not deployed on Alibaba Cloud from Security Center.

If you no longer require protection for servers that are not deployed on Alibaba Cloud, you can call this operation to unbind the servers from Security Center. After you unbind a server that is not deployed on Alibaba Cloud from Security Center, the server no longer consumes the quota of protected servers or protected server vCPUs. This way, you can install the Security Center agent on other servers to meet your business requirements.

> **Note** You can unbind only the servers that are not deployed on Alibaba Cloud from Security Center. If you use an Elastic Compute Service (ECS) instance, you do not need to unbind the instance. If you uninstall the Security Center agent from an ECS instance, the ECS instance still exists as an disconnected server in the asset list of the Security Center console. The ECS instance is not removed from the asset list.

Prerequisites

- The server that you want to unbind from Security Center is not deployed on Alibaba Cloud and the Security Center agent is disabled for the server. In this case, the agent is in the Close state and Security Center does not protect the server. You can call the PauseClient operation to disable the agent.
- The client protection feature is disabled for the server. For more information about how to disable client protection, see Use the client protection feature.

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	UnbindAegis	The operation that you want to perform. Set the value to **UnbindAegis**.
Uuids	String	Yes	4fe8e1cd-3c37-4851-b9de-124da32c****	The universally unique identifier (UUID) of the server that you want to unbind. Separate multiple UUIDs with commas (,). **Note** You can call the DescribeCloudCenterInstances operation to query the UUIDs of the servers.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	825F5526-2A17-4279-857F-F790E9590171	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<UnbindAegisResponse>
      <RequestId>825F5526-2A17-4279-857F-F790E9590171</RequestId>
</UnbindAegisResponse>
```

`JSON` format

```
{
 "RequestId": "825F5526-2A17-4279-857F-F790E9590171"
}
```

Error codes

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

12.Export check results

12.1. ExportRecord

You can call this operation to export baseline check, asset fingerprint check, and AccessKey leak check results to Excel files.

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	ExportRecord	The operation that you want to perform. Set the value to:**ExportRecord**.
ExportType	String	Yes	accessKey	The check types that can be exported. Valid values: • **baseline**: Alibaba Cloud service baseline checks • **assetInstance**: assets • **attack**: attack analysis • **accessKey**: AccessKey leaks • **user**: the accounts covered by asset fingerprints • **port**: the ports covered by asset fingerprints • **process**: the processes of an asset fingerprint check • **software**: the software of an asset fingerprint check
Lang	String	No	zh	The language of the request and response. Valid values: Valid values: • **zh**: Chinese • **en**: English
Params	String	No	{"level":"high"}	Sets conditions to filter check results in the files to which the check results are exported.

Response parameters

Parameter	Type	Example	Description
FileName	String	cms_20171101.xlsx	The name of the exported file.
Id	Long	131231	The ID of the exported file.
RequestId	String	6673D49C-A9AB-40DD-B4A2-B92306701AE7	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<ExportRecordResponse>
  <Id>131231</Id>
  <FileName>cms_20171101.xlsx</FileName>
  <requestId>6673D49C-A9AB-40DD-B4A2-B92306701AE7</requestId>
</ExportRecordResponse>
```

`JSON` format

```
{
    "Id": 131231,
    "FileName": "cms_20171101.xlsx",
    "requestId": "6673D49C-A9AB-40DD-B4A2-B92306701AE7"
}
```

Error codes

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

13.Virus detection

13.1. OperateSuspiciousTargetConfig

Configures proactive defense.

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	OperateSuspiciousTargetConfig	The operation that you want to perform. Set the value to **OperateSuspiciousTargetConfig**.
SourceIp	String	No	1.2.XX.XX	The source IP address of the request.
Lang	String	No	zh	The language of the content within the request and response. Default value: **zh**. Valid values: • **zh**: Chinese • **en**: English
Type	String	Yes	auto_breaking	The type of proactive defense. Valid Values: • **auto_breaking**: automatic blocking • **webshell_cloud_breaking**: webshell prevention • **alinet**: malicious behavior prevention • **ransomware_breaking**: ransomware capture • **alisecguard**: client protection
TargetType	String	Yes	uuid	The dimension from which you manage proactive defense. Only server UUIDs are supported. Set the value to **UUID**.

Parameter	Type	Required	Example	Description
TargetOperations	String	Yes	"[{"targetType":"uuid","target":"0585f81a-dd84-4ddf-9971-f59d12345678","flag":"add"},{"targetType":"uuid","target":"01acfd9d-e6a4-4e61-b9eb-aae012345678","flag":"add"},{"targetType":"uuid","target":"04a0e735-ad32-4835-b635-045812345678","flag":"add"}]"	The parameter required to configure proactive defense for your server. The parameter includes the following fields: • **targetType**: specifies the dimension on which proactive defense is configured. UUIDs are supported. Set the value to UUID. • **target**: specifies the UUID of the server for which you want to configure proactive defense. • **flag**: specifies whether to enable or disable proactive defense for your server. Valid values are **add** and **del**. The value add indicates that proactive defense will be enabled for your server. The value del indicates that proactive defense will be disabled for your server.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	ABCD-PSD2-5256-1DSA-4222-JHBN	The ID of the request, which is used to locate and troubleshoot issues.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=OperateSuspiciousTargetConfig
&SourceIp=1.2.XX.XX
&Lang=zh
&Type=auto_breaking
&TargetType=uuid
&TargetOperations="[{"targetType":"uuid","target":"0585f81a-dd84-4ddf-9971-f59d12345678","flag":"add"},{"targetType":"uuid","target":"01acfd9d-e6a4-4e61-b9eb-aae012345678","flag":"add"},{"targetType":"uuid","target":"04a0e735-ad32-4835-b635-045812345678","flag":"add"}]"
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<OperateSuspiciousTargetConfigResponse>
    <RequestId>ABCD-PSD2-5256-1DSA-4222-JHBN</RequestId>
</OperateSuspiciousTargetConfigResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "ABCD-PSD2-5256-1DSA-4222-JHBN"
}
```

Error codes

HTTP status code	Error code	Error message	Description
400	ConsoleError	The error message is %s %s.	The error message is %s %s.
500	ServerError	ServerError	The error message returned because a server error occurred.

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

14.Tamper protection

14.1. ModifyWebLockStart

Activates and enables web tamper proofing for a specific server.

Before you call this operation, make sure that your account has sufficient quota on the servers that web tamper proofing protects. If a server is protected by web tamper proofing, the number of servers that are allowed is deducted by one after the operation is successful.

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	ModifyWebLockStart	The operation that you want to perform. Set the value to **ModifyWebLockStart**.
Mode	String	No	whitelist	The protection mode. Valid values: • **whitelist**: In this mode, web tamper proofing is enabled for the specified directories and types of files. • **blacklist**: In this mode, web tamper proofing is enabled for the unspecified subdirectories, types of files, and files in the protected directory.
LocalBackupDir	String	No	/usr/local/backup	The local path where backup files of the protected directory are stored. The directory format of a Linux operating system is different from that of a Windows operating system. Enter the directory in the required format based on your operating system. Directory formats of Windows and Linux operating systems: • Linux: /usr/local/aegis/bak • Windows: C:\Program Files (x86)\Alibaba\Aegis\bak

Parameter	Type	Required	Example	Description
ExclusiveFile	String	No	/home/admin/tomcat/localhost.log	The file for which you want to disable web tamper proofing. **Note** If **Mode** is set to **blacklist**, you must set this parameter.
Dir	String	No	/home/admin/tomcat	The directory for which you want to enable web tamper proofing. Separate multiple directories with commas (,).
InclusiveFileType	String	No	html	The type of file for which you want to enable web tamper proofing. Separate multiple types with semicolons (;). Valid values: • php • jsp • asp • aspx • js • cgi • html • htm • xml • shtml • shtm • jpg • gif • png **Note** If **Mode** is set to **whitelist**, you must set this parameter.
Uuid	String	No	80d2f7d6-31a9-4d7f-8ff4-7ecc42f89ca****	The UUID of the server for which you want to enable web tamper proofing.

Parameter	Type	Required	Example	Description
ExclusiveFileType	String	No	jpg	The type of file for which you want to disable web tamper proofing. Separate multiple types with semicolons (;). Valid values: • php • jsp • asp • aspx • js • cgi • html • htm • xml • shtml • shtm • jpg • gif • png Note If **Mode** is set to **blacklist**, you must set this parameter.
ExclusiveDir	String	No	/home/admin/java	The directory for which you want to disable web tamper proofing. Note If **Mode** is set to **blacklist**, you must set this parameter.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D9354C1A-D709-4873-9AAE-41513327B247	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyWebLockStart
&Mode=whitelist
&LocalBackupDir=/usr/local/backup
&Dir=/home/admin/tomcat
&Uuid=80d2f7d6-31a9-4d7f-8ff4-7ecc42f89ca****
&InclusiveFileType=*.html
&<Common request parameters>
```

Sample success responses

`XML` format

```
<ModifyWebLockStartResponse>
      <requestId>D9354C1A-D709-4873-9AAE-41513327B247</requestId>
</ModifyWebLockStartResponse>
```

`JSON` format

```
{
    "requestId": "D9354C1A-D709-4873-9AAE-41513327B247"
}
```

Error codes

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

14.2. ModifyWebLockStatus

You can call this operation to enable or disable tamper protection for a server.

To enable tamper protection, make sure that you have sufficient licenses in you account to enable tamper protection. One license allows you to enable tamper protection for one server. The number of licenses that you purchased equals the number of servers for which you can enable tamper protection.

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	ModifyWebLockStatus	The operation that you want to perform. Set the value to **ModifyWebLockStatus**.
SourceIp	String	No	1.2.3.4	The source IP address of the request.

Parameter	Type	Required	Example	Description
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
Uuid	String	No	inet-1234567****	The UUID of the server for which you want to enable or disable tamper protection.
Status	String	No	on	Specifies whether to enable or disable tamper protection for the specified server. Valid values: • **on**: enables tamper protection • **off**: disable tamper protection **Note** After you disable tamper protection, one license is released.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D9354C1A-D709-4873-9AAE-41513327B247	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<ModifyWebLockStatusResponse
    <RequestId>D9354C1A-D709-4873-9AAE-41513327B247</requestId>
</ModifyWebLockStatusResponse>
```

`JSON` format

```
{
    "RequestId": "D9354C1A-D709-4873-9AAE-41513327B247"
}
```

Error codes

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

14.3. DescribeWebLockConfigList

You can call this operation to query the tamper protection configurations of a specific server.

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	DescribeWebLockConfigList	The operation that you want to perform. Set the value to **DescribeWebLockConfigList**.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
Uuid	String	No	inet-1234567****	The UUID of the server to be queried.

Response parameters

Parameter	Type	Example	Description
ConfigList	Array		The list of tamper protection configurations.
Dir	String	/www/tmp/	The directory that has tamper protection enabled.

Parameter	Type	Example	Description
ExclusiveDir	String	/home/admin/tomcat	The directory that has tamper protection disabled. **Note** If the value of **Mode** is **blacklist**, this parameter is returned.
ExclusiveFile	String	/home/admin/tomcat/localhost.log	The file that has tamper protection disabled. **Note** If the value of **Mode** is **blacklist**, this parameter is returned.
ExclusiveFileType	String	*.jpg	The type of file that has tamper protection disabled. **Note** If the value of **Mode** is **blacklist**, this parameter is returned.
Id	String	11	The ID of the directory that has tamper protection enabled.
InclusiveFile	String	/home/admin/tomcat/aaa.log	The file that has tamper protection enabled. **Note** If the value of **Mode** is **whitelist**, this parameter is returned.
InclusiveFileType	String	jpg	The type of file that has tamper protection enabled. **Note** If the value of **Mode** is **whitelist**, this parameter is returned.
LocalBackupDir	String	/usr/local/backup	The local path where backup files of the protected directory are stored.

Parameter	Type	Example	Description
Mode	String	blacklist	The protection mode. Valid values: • **whitelist**: In this mode, tamper protection is enabled for the specified directories and file types. • **blacklist**: In this mode, tamper protection is enabled for the unspecified sub-directories, file types, and files under the protected directory.
Uuid	String	80d2f7d6-31a9-4d7f-8ff4-7ecc42f8****	The UUID of the server that has tamper protection enabled.
RequestId	String	D9354C1A-D709-4873-9AAE-41513327B247	The ID of the request.
TotalCount	Integer	1	The total number of directories that have tamper protection enabled on the specified server.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DescribeWebLockConfigListResponse>
      <TotalCount>1</TotalCount>
      <RequestId>EB7BD248-FBD6-4378-B244-0C9FB299BCBC</RequestId>
      <ConfigList>
            <InclusiveFileType>php;jsp;asp;aspx;js;cgi;html;htm;xml;shtml;shtm;jpg;gif;png<
/InclusiveFileType>
            <ExclusiveFile></ExclusiveFile>
            <Uuid>80d2f7d6-31a9-4d7f-8ff4-7ecc42f8****</Uuid>
            <ExclusiveDir></ExclusiveDir>
            <Mode>whitelist</Mode>
            <LocalBackupDir>/usr/local/aegis/bak</LocalBackupDir>
            <ExclusiveFileType></ExclusiveFileType>
            <Id>9312</Id>
            <Dir>/www/tmp/</Dir>
            <InclusiveFile></InclusiveFile>
      </ConfigList>
</DescribeWebLockConfigListResponse>
```

`JSON` format


```
{
 "TotalCount": 1,
 "RequestId": "EB7BD248-FBD6-4378-B244-0C9FB299BCBC",
 "ConfigList": [
  {
   "InclusiveFileType": "php;jsp;asp;aspx;js;cgi;html;htm;xml;shtml;shtm;jpg;gif;png",
   "ExclusiveFile": "",
   "Uuid": "80d2f7d6-31a9-4d7f-8ff4-7ecc42f8****",
   "ExclusiveDir": "",
   "Mode": "whitelist",
   "LocalBackupDir": "/usr/local/aegis/bak",
   "ExclusiveFileType": "",
   "Id": 9312,
   "Dir": "/www/tmp/",
   "InclusiveFile": ""
  }
 ]
}
```


Error codes

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

14.4. DescribeWebLockBindList

You can call this operation to query the list of servers that have tamper protection enabled.

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	DescribeWebLockBindList	The operation that you want to perform. Set the value to **DescribeWebLockBindList**.
SourceIp	String	No	1.2.3.4	The source IP address of the request.

Parameter	Type	Required	Example	Description
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
Remark	String	No	192.XX.XX.1	The string that allows you to search servers by name or IP address.
Status	String	No	on	The protection status of the servers to be queried. Valid values: • **on**: tamper protection enabled. • **off**: tamper protection disabled.
CurrentPage	Integer	No	1	The number of the page to return. Pages start from page 1. Default value: 1.
PageSize	Integer	No	20	The number of entries to return per page. Default value: 20.

Response parameters

Parameter	Type	Example	Description
BindList	Array		The list of servers that have tamper protection enabled.
DirCount	String	5	The number of protected directories.
InstanceName	String	testName	The name of the server.
InternetIp	String	54.XX.XX.100	The Internet IP address of the server.
IntranetIp	String	192.XX.XX.1	The private IP address of the server.
Os	String	Linux	The operating system that the server runs.
Percent	Integer	99	The starting progress percentage of tamper protection. Valid values: 0% to 100%.

Parameter	Type	Example	Description
ServiceCode	String	2001	Error codes. Valid values: • **2001**: The error code returned because the Security Center agent is not connected to Alibaba Cloud. • **9999**: The error code returned because the connection is timed out.
ServiceDetail	String	client offline	Exception details of tamper protection. Valid values: • **client offline**: The Security Center agent is not connected to Alibaba Cloud. • **timeout**: The connection is timed out.
ServiceStatus	String	stop	The state of tamper protection on the server. Valid values: • **stop**: Tamper protection is disabled. • **initializing**: Tamper protection is being enabled. • **exception**: Tamper protection is not running as expected. • **running**: Tamper protection is running. • **closing**: Tamper protection is being disabled.
Status	String	on	The protection status of the server. Valid values: • **on**: tamper protection enabled. • **off**: tamper protection disabled.
Uuid	String	inet-12345****	The UUID of the server.
CurrentPage	Integer	1	The page number of the returned page. Pages start from page 1. Default value: 1.
PageSize	Integer	20	The number of entries returned on each page. Default value: 20.
RequestId	String	D9354C1A-D709-4873-9AAE-41513327B247	The ID of the request.

Parameter	Type	Example	Description
TotalCount	Integer	2	The total number of servers that have tamper protection enabled.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DescribeWebLockBindListRespone>
      <TotalCount>2</TotalCount>
      <RequestId>D9354C1A-D709-4873-9AAE-41513327B247</RequestId>
      <PageSize>20</PageSize>
      <CurrentPage>1</CurrentPage>
      <BindList>
            <InstanceName>testName</InstanceName>
            <Status>on</Status>
            <Uuid>inet-12345****</Uuid>
            <ServiceCode>2001</ServiceCode>
            <InternetIp>54.XX.XX.100</InternetIp>
            <Os>Linux</Os>
            <Percent>99</Percent>
            <ServiceStatus>stop</ServiceStatus>
            <DirCount>5</DirCount>
            <ServiceDetail>client offline</ServiceDetail>
            <IntranetIp>192.XX.XX.1</IntranetIp>
      </BindList>
</DescribeWebLockBindListRespone>
```

`JSON` format

```
{
 "TotalCount": "2",
 "RequestId": "D9354C1A-D709-4873-9AAE-41513327B247",
 "PageSize": "20",
 "CurrentPage": "1",
 "BindList": [{
  "InstanceName": "testName",
  "Status": "on",
  "Uuid": "inet-12345****",
  "ServiceCode": "2001",
  "InternetIp": "54.XX.XX.100",
  "Os": "Linux",
  "Percent": "99",
  "ServiceStatus": "stop",
  "DirCount": "5",
  "ServiceDetail": "client offline",
  "IntranetIp": "192.XX.XX.1"
 }]
}
```


Error codes

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

14.5. ModifyWebLockDeleteConfig

You can call this operation to delete a directory that has tamper protection enabled.

After you delete a directory that has tamper protection enabled, files under the directory are no longer protected by tamper protection. The corresponding websites may be maliciously modified by attackers. Proceed with caution.

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	ModifyWebLockDeleteConfig	The operation that you want to perform. Set the value to **ModifyWebLockDeleteConfig**.
SourceIp	String	No	1.2.3.4	The source IP address of the request.

Parameter	Type	Required	Example	Description
Lang	String	No	zh	The language of the request and response. Valid values: • **zh**: Chinese • **en**: English
Id	Integer	No	12345	The ID of the protected directory to be deleted. **Note** You can call the DescribeWebLockConfigList operation to query the ID of the protected directory.
Uuid	String	No	inet-12345	The UUID of the server to which the protected directory to be deleted belongs. **Note** You can call the DescribeAllEntity operation to query the UUID of the server.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D9354C1A-D709-4873-9AAE-41513327B247	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<ModifyWebLockDeleteConfigResponse>
      <requestId>D9354C1A-D709-4873-9AAE-41513327B247</requestId>
</ModifyWebLockDeleteConfigResponse>
```

`JSON` format

```
{
    "requestId": "D9354C1A-D709-4873-9AAE-41513327B247"
}
```

Error codes

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

14.6. ModifyWebLockCreateConfig

Adds a directory to protect for a specific server.

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	ModifyWebLockCreateConfig	The operation that you want to perform. Set the value to **ModifyWebLockCreateConfig**.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The natural language of the request and response. Valid values: • **zh**: Chinese • **en**: English
Uuid	String	No	inet-12345****	The UUID of the server for which you want to add a directory to protect. **Note** You can call the DescribeCloudCenterInstances operation to query the UUIDs of servers.

Parameter	Type	Required	Example	Description
Dir	String	No	/home/admin/tomcat	The directory that you want to protect.
ExclusiveDir	String	No	/home/admin/test	The directory for which you want to disable web tamper proofing. **Note** If you set **Mode** to **blacklist**, you must specify this parameter.
ExclusiveFileType	String	No	jpg	The type of file for which you want to disable web tamper proofing. Separate multiple types with semicolons (;). Valid values: • php • jsp • asp • aspx • js • cgi • html • htm • xml • shtml • shtm • jpg • gif • png **Note** If you set **Mode** to **blacklist**, you must specify this parameter.
LocalBackupDir	String	No	/usr/local/backup	The local directory that stores the backup files of the directory to protect.

Parameter	Type	Required	Example	Description
Mode	String	No	whitelist	The protection mode. Valid values: • **whitelist**: In this mode, web tamper proofing is enabled for the specified directories and types of files. • **blacklist**: In this mode, web tamper proofing is enabled for the unspecified subdirectories, types of files, and files in the protected directory.
InclusiveFileType	String	No	jpg	The type of file for which you want to enable web tamper proofing. Separate multiple types with semicolons (;). Valid values: • php • jsp • asp • aspx • js • cgi • html • htm • xml • shtml • shtm • jpg • gif • png **Note** If you set **Mode** to **whitelist**, you must specify this parameter.
ExclusiveFile	String	No	/home/admin/apache.log	The file for which you want to disable web tamper proofing. **Note** If you set **Mode** to **blacklist**, you must specify this parameter.

Parameter	Type	Required	Example	Description
InclusiveFile	String	No	/home/admin/test.log	The file for which you want to enable web tamper proofing. **Note** If you set **Mode** to **whitelist**, you must specify this parameter.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D9354C1A-D709-4873-9AAE-41513327B247	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<ModifyWebLockCreateConfigResponse>
      <RequestId>D9354C1A-D709-4873-9AAE-41513327B247</RequestId>
</ModifyWebLockCreateConfigResponse>
```

`JSON` format

```
{
    "RequestId": "D9354C1A-D709-4873-9AAE-41513327B247"
}
```

Error codes

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

14.7. ModifyWebLockUpdateConfig

Modifies the protected directory for a specific server.

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	ModifyWebLockUpdateConfig	The operation that you want to perform. Set the value to **ModifyWebLockUpdateConfig**.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The natural language of the request and response. Valid values: • **zh**: Chinese • **en**: English
Id	Integer	No	12345	The ID of the protected directory that you want to modify. **Note** You can call the DescribeWebLockConfigListl operation to query the IDs of protected directories.
Uuid	String	No	4fe8e1cd-3c37-4851-b9de-124da32c****	The UUID of the server for which you want to modify the protected directory. **Note** You can call the DescribeCloudCenterInstances operation to query the UUIDs of servers.
Dir	String	No	/home/admin/tomcat	The directory for which you want to enable web tamper proofing.

Parameter	Type	Required	Example	Description
ExclusiveDir	String	No	/home/admin/test	The directory for which you want to disable web tamper proofing. **Note** If you set **Mode** to **blacklist**, you must specify this parameter.
ExclusiveFileType	String	No	jpg	The type of file for which you want to disable web tamper proofing. Separate multiple types with semicolons (;). Valid values: • php • jsp • asp • aspx • js • cgi • html • htm • xml • shtml • shtm • jpg • gif • png **Note** If you set **Mode** to **blacklist**, you must specify this parameter.
LocalBackupDir	String	No	/usr/local/backup	The local directory that stores the backup files of the protected directory to modify. The directory format of a Linux server is different from that of a Windows server. You must enter the directory in the required format based on your operating system. Directory formats of Windows and Linux servers: • Linux server: /usr/local/aegis/bak • Windows server: C:\Program Files (x86)\Alibaba\Aegis\bak

Parameter	Type	Required	Example	Description
Mode	String	No	blacklist	The protection mode. Valid values: • **whitelist**: In this mode, web tamper proofing is enabled for the specified directories and types of files. • **blacklist**: In this mode, web tamper proofing is enabled for the unspecified subdirectories, types of files, and files in the protected directory.
InclusiveFileType	String	No	jpg	The type of file for which you want to enable web tamper proofing. Separate multiple types with semicolons (;). Valid values: • php • jsp • asp • aspx • js • cgi • html • htm • xml • shtml • shtm • jpg • gif • png **Note** If you set **Mode** to **whitelist**, you must specify this parameter.
ExclusiveFile	String	No	/home/admin/apache.log	The file for which you want to disable web tamper proofing. **Note** If you set **Mode** to **blacklist**, you must specify this parameter.

Parameter	Type	Required	Example	Description
InclusiveFile	String	No	/home/admin/test.log	The file for which you want to enable web tamper proofing. **Note** If you set **Mode** to **whitelist**, you must specify this parameter.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D9354C1A-D709-4873-9AAE-41513327B247	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<ModifyWebLockUpdateConfigResponse>
      <RequestId>D9354C1A-D709-4873-9AAE-41513327B247</RequestId>
</ModifyWebLockUpdateConfigResponse>
```

`JSON` format

```
{
    "RequestId": "D9354C1A-D709-4873-9AAE-41513327B247"
}
```

Error codes

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

15.AccessKey Leak Detection

15.1. DescribeAccesskeyLeakList

Queries the details of AccessKey pair leaks in your assets.

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	DescribeAccesskeyLeakList	The operation that you want to perform. Set the value to **DescribeAccesskeyLeakList**.
CurrentPage	Integer	Yes	1	The page number of the current page. Default value: **1**.
PageSize	Integer	Yes	20	The number of entries to return on each page. Maximum value: 100. Default value: 20. If you leave this parameter empty, 20 entries are returned per page by default. **Note** We recommend that you do not leave this parameter empty.
Status	String	No	pending	Specifies whether an AccessKey pair leak is handled. Valid values: • **pending**: unhandled • **dealed**: handled
Query	String	No	LTAI4Fytv7ALKzkNVBV6****	The AccessKey ID that you want to query. Only exact match is supported.

Parameter	Type	Required	Example	Description
StartTs	Long	No	1614155361489	The beginning of the time range to query. You can query all AccessKey pair leaks that are detected later than this time point. 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.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
AccessKeyLeakList	Array of AccessKeyLeak		The details of AccessKey pair leaks.
AccesskeyId	String	LTAI4Fytv7ALKzkNVBV6****	The ID of the AccessKey pair that is leaked.
AliUserName	String	testAccountName	The name of the Alibaba Cloud account that is affected.
Asset	String	Cloud platform	The platform to which the asset belongs. The value is fixed as **Cloud platform**.
DealTime	String	2020-12-03 21:23:38	The time when the AccessKey pair leak is handled.
DealType	String	pending	The method to handle the AccessKey pair leak. Valid values: • **pending**: The AccessKey leak is unhandled. • **manual**: The AccessKey pair leak is manually handled. • **disable**: The leaked AccessKey pair is disabled. • **add-whitelist**: The alert generated for the leaked AccessKey pair is added to the whitelist.

Parameter	Type	Example	Description
GmtModified	Long	1612357897000	The time when the AccessKey pair leak is first detected. 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	389357	The primary key ID of the database.
Status	String	pending	Indicates whether the AccessKey pair leak is handled. Valid values: • **pending**: unhandled • **dealed**: handled
Type	String	AccessKey	The type of the leak. The value is fixed as **AccessKey**.
Url	String	https://github.com/hht312/test-ak/blob/0e466d2ecce55b4c924d773a058e5dc602d8****/1001	The URL of the platform on which the AccessKey pair leak is detected.
UserType	String	master	The type of the account to which the leaked AccessKey pair belongs. Valid values: • **master**: Alibaba Cloud account • **ram**: RAM user
AkLeakCount	Integer	1	The number of AccessKey pair leaks that are unhandled.
CurrentPage	Integer	1	The page number of the current page.
GmtLast	Long	1612357897000	This parameter is deprecated.
PageSize	Integer	20	The number of entries returned per page.
RequestId	String	B37C9052-A73E-4707-A024-9247702852BE	The ID of the request.
TotalCount	Integer	2	The total number of AccessKey pair leaks.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeAccesskeyLeakList
&CurrentPage=1
&PageSize=20
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeAccesskeyLeakListResponse>
      <AkLeakCount>1</AkLeakCount>
      <AccessKeyLeakList>
            <Status>pending</Status>
            <AliUserName>testAccountName</AliUserName>
            <Type>AccessKey</Type>
            <DealType>pending</DealType>
            <AccesskeyId>LTAI4Fytv7ALKzkNVBV6****</AccesskeyId>
            <GmtModified>1612357897000</GmtModified>
            <Asset>Cloud platform</Asset>
            <Id>389357</Id>
            <DealTime>2021-03-03 15:58:34</DealTime>
            <UserType>master</UserType>
            <Url>https://github.com/hht312/test-ak/blob/0e466d2ecce55b4c924d773a058e5dc602d
8****/1001</Url>
      </AccessKeyLeakList>
      <AccessKeyLeakList>
            <Status>dealed</Status>
            <AliUserName>testAccountName</AliUserName>
            <Type>AccessKey</Type>
            <DealType>manual</DealType>
            <AccesskeyId>LTAI4Fytv7ALKzkNVBV6****</AccesskeyId>
            <GmtModified>1612357467000</GmtModified>
            <Asset>Cloud platform</Asset>
            <Id>389351</Id>
            <DealTime>2021-02-08 14:43:43</DealTime>
            <UserType>master</UserType>
            <Url>https://github.com/daijope/testak/blob/1fac284b5b003d3445ea9dcf1d50a9c0e36
7****/test.java</Url>
      </AccessKeyLeakList>
      <TotalCount>2</TotalCount>
      <RequestId>B37C9052-A73E-4707-A024-9247702852BE</RequestId>
      <PageSize>20</PageSize>
      <CurrentPage>1</CurrentPage>
</DescribeAccesskeyLeakListResponse>
```

`JSON` format

```
{
    "AkLeakCount": 1,
    "AccessKeyLeakList": [
        {
            "Status": "pending",
            "AliUserName": "testAccountName",
            "Type": "AccessKey",
            "DealType": "pending",
            "AccesskeyId": "LTAI4Fytv7ALKzkNVBV6****",
            "GmtModified": 1612357897000,
            "Asset": "Cloud platform",
            "Id": 389357,
            "DealTime": "2021-03-03 15:58:34",
            "UserType": "master",
            "Url": "https://github.com/hht312/test-ak/blob/0e466d2ecce55b4c924d773a058e5dc602d8****/1001"
        },
        {
            "Status": "dealed",
            "AliUserName": "testAccountName",
            "Type": "AccessKey",
            "DealType": "manual",
            "AccesskeyId": "LTAI4Fytv7ALKzkNVBV6****",
            "GmtModified": 1612357467000,
            "Asset": "Cloud platform",
            "Id": 389351,
            "DealTime": "2021-02-08 14:43:43",
            "UserType": "master",
            "Url": "https://github.com/daijope/testak/blob/1fac284b5b003d3445ea9dcf1d50a9c0e367****/test.java"
        }
    ],
    "TotalCount": 2,
    "RequestId": "B37C9052-A73E-4707-A024-9247702852BE",
    "PageSize": 20,
    "CurrentPage": 1
}
```


Error codes

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

15.2. DescribeAccessKeyLeakDetail

Queries the details about AccessKey pair leaks.

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	DescribeAccessKeyLeakDetail	The operation that you want to perform. Set the value to **DescribeAccessKeyLeakDetail**.
Id	Long	Yes	389357	The ID of the AccessKey pair leak.

Response parameters

Parameter	Type	Example	Description
Type	String	AccessKey	The type of the leak. The value is fixed as **AccessKey**.
GithubUserPicUrl	String	https://avatars.githubusercontent.com/u/26296896?s=48&v=****	The URL of the profile picture for the GitHub user.
GithubUser	String	Blue00Blue	The username of the GitHub user.
GithubRepoName	String	ExamOnline	The name of the GitHub repository.
GithubFileType	String	Python	The type of the GitHub file. Valid values: • Python • XML • GO • Javascript • INI • JSON • C++
Remark	String	12	The remarks of the AccessKey pair leak.
GithubFileUpdateTime	String	2021-07-06T09:49:33	The time when the GitHub file was updated.
WhitelistStatus	String	no	Indicates whether the AccessKey pair leak is added to the whitelist. Valid values: • **no**: no • **yes**: yes

Parameter	Type	Example	Description
GithubFileName	String	testAkLeak	The name of the GitHub file.
Source	String	GitHub	The platform on which the AccessKey pair leak is detected.
GmtModified	String	2021-07-06 17:49:39	The last time when the AccessKey pair leak was detected.
Asset	String	Cloud platform	The platform to which the asset belongs. The value is fixed as **Cloud platform**.
DealTime	String	2022-01-17 15:47:08	The time when the AccessKey pair leak was handled.
RequestId	String	79CFF74D-E967-5407-8A78-EE03B925FDAA	The ID of the request, which is used to locate and troubleshoot issues.
AccesskeyId	String	LTAI4G4VjkC9wenfEvgX****	The ID of the AccessKey pair that is leaked.
GithubFileUrl	String	https://github.com/Blue00Blue/ExamOnline/blob/6c932c10fc3f217783f3937e2b230f79656c18a7/testAk****	The URL of the GitHub file.
DealType	String	add-whitelist	The solution to the AccessKey pair leak. Valid values: • **manual**: manually deleted • **disable**: manually disabled • **add-whitelist**: added to the whitelist • **pending**: unhandled

Parameter	Type	Example	Description
Code	String	\n1231 \nak=LTAI4G4VjkC9wenfEvgX**** \n12311123 \nsk1999 \nsk1999sk1999 \nsk1999sk1999 \n\n\ntest001 akhht \nak=LTAI4G4VjkC9wenfEvgX**** \nsk=AjEhS9XmnIzllpAx2LxMTMdrTGOqK9	The code snippet that is leaked.
GmtCreate	String	2021-07-06 17:49:41	The first time when the AccessKey pair leak was detected.
GithubRepoUrl	String	https://github.com/Blue00Blue/ExamOn****	The URL of the GitHub repository.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeAccessKeyLeakDetail
&Id=389357
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<DescribeAccessKeyLeakDetailResponse>
    <Type>AccessKey</Type>
    <GithubUserPicUrl>https://avatars.githubusercontent.com/u/26296896?s=48&amp;v=****</Git
hubUserPicUrl>
    <GithubUser>Blue00Blue</GithubUser>
    <GithubRepoName>ExamOnline</GithubRepoName>
    <GithubFileType>Python</GithubFileType>
    <Remark>12</Remark>
    <GithubFileUpdateTime>2021-07-06T09:49:33Z</GithubFileUpdateTime>
    <WhitelistStatus>no</WhitelistStatus>
    <GithubFileName>testAkLeak</GithubFileName>
    <Source>GitHub</Source>
    <GmtModified>2021-07-06 17:49:39</GmtModified>
    <Asset>Cloud platform</Asset>
    <DealTime>2022-01-17 15:47:08</DealTime>
    <RequestId>79CFF74D-E967-5407-8A78-EE03B925FDAA</RequestId>
    <AccesskeyId>LTAI4G4VjkC9wenfEvgX****</AccesskeyId>
    <GithubFileUrl>https://github.com/Blue00Blue/ExamOnline/blob/6c932c10fc3f217783f3937e2b
230f79656c18a7/testAk****</GithubFileUrl>
    <DealType>add-whitelist</DealType>
    <Code>\n1231 \nak=LTAI4G4VjkC9wenfEvgX**** \n12311123 \nsk1999 \nsk1999sk1999 \nsk1999s
k1999 \n\n\ntest001 ak hht \nak=LTAI4G4VjkC9wenfEvgX**** \nsk=AjEhS9XmnIzllpAx2LxMTMdrTGOqK
9</Code>
    <GmtCreate>2021-07-06 17:49:41</GmtCreate>
    <GithubRepoUrl>https://github.com/Blue00Blue/ExamOn****</GithubRepoUrl>
</DescribeAccessKeyLeakDetailResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "Type" : "AccessKey",
  "GithubUserPicUrl" : "https://avatars.githubusercontent.com/u/26296896?s=48&v=****",
  "GithubUser" : "Blue00Blue",
  "GithubRepoName" : "ExamOnline",
  "GithubFileType" : "Python",
  "Remark" : "12",
  "GithubFileUpdateTime" : "2021-07-06T09:49:33Z",
  "WhitelistStatus" : "no",
  "GithubFileName" : "testAkLeak",
  "Source" : "GitHub",
  "GmtModified" : "2021-07-06 17:49:39",
  "Asset" : "Cloud platform",
  "DealTime" : "2022-01-17 15:47:08",
  "RequestId" : "79CFF74D-E967-5407-8A78-EE03B925FDAA",
  "AccesskeyId" : "LTAI4G4VjkC9wenfEvgX****",
  "GithubFileUrl" : "https://github.com/Blue00Blue/ExamOnline/blob/6c932c10fc3f217783f3937e
2b230f79656c18a7/testAk****",
  "DealType" : "add-whitelist",
  "Code" : "\\n1231 \\nak=LTAI4G4VjkC9wenfEvgX**** \\n12311123 \\nsk1999 \\nsk1999sk1999 \\
nsk1999sk1999 \\n\\n\\ntest001 ak hht \\nak=LTAI4G4VjkC9wenfEvgX**** \\nsk=AjEhS9XmnIzllpAx
2LxMTMdrTGOqK9",
  "GmtCreate" : "2021-07-06 17:49:41",
  "GithubRepoUrl" : "https://github.com/Blue00Blue/ExamOn****"
}
```


Error codes

HTTP status code	Error code	Error message	Description
500	ServerError	ServerError	The error message returned because a server error occurred.

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

16.Latest release

16.1. DescribeDialogMessages

Queries the pop-up messages of newly released features and the sales promotions provided by Security Center. This way, you can follow feature updates and sales promotions in a timely manner.

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	DescribeDialogMessages	The operation that you want to perform. Set the value to: **DescribeDialogMessages**.
SourceIp	String	No	1.2.3.4	The source IP address of the request.

Response parameters

Parameter	Type	Example	Description
DialogList	Array		The list of pop-up messages.
DialogKey	String	aliyun_sale_season_01	The key of the pop-up message.
ID	Long	11	The ID of the pop-up message.
Params	String	{'startTime':'2020-01-27','day':'30','priority':'1','promotion':'1'}	The required parameters of the pop-up message.
RequestId	String	965F9282-D403-4FA2-B1B9-10F62DC719BF	The ID of the request.
TotalCount	Integer	1	The total number of pop-up messages.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DescribeDialogMessagesResponse>
      <DialogList>
            <Params>{'startTime':'2020-02-27','day':'30','priority':'1','promotion':'1'}</P
arams>
            <ID>6196670</ID>
            <DialogKey>sale_season_2020_2</DialogKey>
      </DialogList>
      <TotalCount>1</TotalCount>
      <requestId>965F9282-D403-4FA2-B1B9-10F62DC719BF</requestId>
</DescribeDialogMessagesResponse>
```

`JSON` format

```
{
    "DialogList": [{
        "Params": "{'startTime':'2020-02-27','day':'30','priority':'1','promotion':'1'}",
        "ID": 6196670,
        "DialogKey": "sale_season_2020_2"
    }],
    "TotalCount": 1,
    "requestId": "965F9282-D403-4FA2-B1B9-10F62DC719BF"
}
```

Error codes

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

17.Service-linked roles

17.1. CreateServiceLinkedRole

Creates a service-linked role and authorizes Security Center to access cloud resources.

For more information about service-linked roles, see Service-linked roles.

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	CreateServiceLinkedRole	The operation that you want to perform. Set the value to **CreateServiceLinkedRole**.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	B94243D2-9342-4D82-87B9-DF9A038A87E1	The ID of the request.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<CreateServiceLinkedRoleResponse>
      <RequestId>B94243D2-9342-4D82-87B9-DF9A038A87E1</RequestId>
</CreateServiceLinkedRoleResponse>
```

`JSON` format

```
{
    "RequestId":"B94243D2-9342-4D82-87B9-DF9A038A87E1"
}
```

Error codes

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

17.2. DescribeServiceLinkedRoleStatus

Checks whether a service-linked role is created for Security Center.

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	DescribeServiceLinkedRoleStatus	The operation that you want to perform. Set the value to **DescribeServiceLinkedRoleStatus**.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see Common parameters.

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
RequestId	String	39CE98F4-88C0-4539-B906-6B542E5C07B9	The ID of the request.
RoleStatus	Struct		The status information of the service-linked role.

Parameter	Type	Example	Description
Status	Boolean	true	The status of the service-linked role. Valid values: • **true**: The service-linked role is created. • **false**: The service-linked role is not created.

Examples

Sample requests

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

Sample success responses

`XML` format

```
<DescribeServiceLinkedRoleStatusResponse>
      <RequestId>39CE98F4-88C0-4539-B906-6B542E5C07B9</RequestId>
      <RoleStatus>
            <Status>true</Status>
      </RoleStatus>
</DescribeServiceLinkedRoleStatusResponse>
```

`JSON` format

```
{
    "RequestId":"39CE98F4-88C0-4539-B906-6B542E5C07B9",
    "RoleStatus":{
        "Status":"true"
    }
}
```

Error codes

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

18.InstallCloudMonitor

Installs the CloudMonitor agent on specific servers.

> **Note** Before you call this operation, make sure that the Security Center agent installed on the servers is online and the servers can access Alibaba Cloud services.

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	InstallCloudMonitor	The operation that you want to perform. Set the value to **InstallCloudMonitor**.
ArgusVersion	String	Yes	3.5.6	The version of the CloudMonitor agent that you want to install on the servers. For more information about the latest version of the CloudMonitor agent, see Overview.
AgentAccessKey	String	No	usY*****R_U	The AccessKey ID that is required to install the CloudMonitor agent. You can call the DescribeMonitoringAgentAccessKey operation to query the Accesskey ID. **Note** This parameter is required only when you install the CloudMonitor agent on servers that are not deployed on Alibaba Cloud.

Parameter	Type	Required	Example	Description
AgentSecretKey	String	No	UCxF2R1sIO90XlU9****	The AccessKey secret that is required to install the CloudMonitor agent. You can call the DescribeMonitoringAgentAccessKey operation to query the Accesskey secret. **Note** This parameter is required only when you install the CloudMonitor agent on servers that are not deployed on Alibaba Cloud.
InstanceIdList.N	String	No	[VMware-564d4e22ce6d9207-c97c8af3a448****,VMware-564d4a9574e0b8ab-843ba10d8b0c****,VMware-564dbb7fddaf27ce-629271166745****]	The IDs of the servers on which you want to install the CloudMonitor agent. Separate multiple IDs with commas (,). **Note** You must specify at least one of the InstanceIdList.N and UuidList.N parameters. If both the InstanceIdList.N and UuidList.N parameters are specified, the CloudMonitor agent is installed on all specified servers.
UuidList.N	String	No	[inet-c669e5d9-0adf-4d71-a9ce-65ed2730****,inet-2e87cce8-763d-4dcd-b39f-d592e1b0****,inet-7c676676-06fa-442e-90fb-b802e5d6****]	The UUIDs of the servers on which you want to install the CloudMonitor agent. Separate multiple UUIDs with commas (,). **Note** You must specify at least one of the InstanceIdList.N and UuidList.N parameters. If both the InstanceIdList.N and UuidList.N parameters are specified, the CloudMonitor agent is installed on all specified servers.

Response parameters

Parameter	Type	Example	Description
RequestId	String	F92AFB96-FACC-57E7-928E-678D04B94CAE	The ID of the request, which is used to locate and troubleshoot issues.

Parameter	Type	Example	Description
Success	Boolean	false	Indicates whether the request was successful. Valid values: • **true**: yes • **false**: no
Code	String	IllegalParam	The error code returned if the call fails.
Message	String	There was an error with your request.	The error message returned.
HttpStatusCode	Integer	400	The HTTP status code returned.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=InstallCloudMonitor
&ArgusVersion=3.5.6
&AgentAccessKey=usY*****R_U
&AgentSecretKey=UCxF2R1sIO90XlU9****
&InstanceIdList=["[VMware-564d4e22ce6d9207-c97c8af3a448****,VMware-564d4a9574e0b8ab-843ba10
d8b0c****,VMware-564dbb7fddaf27ce-629271166745****]"]
&UuidList=["[inet-c669e5d9-0adf-4d71-a9ce-65ed2730****,inet-2e87cce8-763d-4dcd-b39f-d592e1b
0****,inet-7c676676-06fa-442e-90fb-b802e5d6****]"]
&Common request parameters
```

Sample success responses

`XML` format

```
HTTP/1.1 200 OK
Content-Type:application/xml
<InstallCloudMonitorResponse>
    <RequestId>F92AFB96-FACC-57E7-928E-678D04B94CAE</RequestId>
    <Success>false</Success>
    <Code>IllegalParam</Code>
    <Message>There was an error with your request.</Message>
    <HttpStatusCode>400</HttpStatusCode>
</InstallCloudMonitorResponse>
```

`JSON` format

```
HTTP/1.1 200 OK
Content-Type:application/json
{
  "RequestId" : "F92AFB96-FACC-57E7-928E-678D04B94CAE",
  "Success" : false,
  "Code" : "IllegalParam",
  "Message" : "There was an error with your request.",
  "HttpStatusCode" : 400
}
```

Error codes

HTTP status code	Error code	Error message	Description
400	ConsoleError	The error message is %s %s.	The error message is %s %s.
400	IllegalParam	Illegal param	The error message returned because the specified parameters are invalid.
400	MachineNotExist	The machine does not exist.	The error message returned because the specified servers are invalid. Check the server information and try again.
400	AgentNotOnline	The agent not online.	The error message returned because the Security Center agent installed on the servers is offline. Make sure that the agent is online and try again.
400	InvalidParam	There was an error with your request.	The error message returned because a request error occurred. Try again later.
500	ServerError	ServerError	The error message returned because a server error occurred.

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