

# 阿里云

漏洞扫描  
API参考

文档版本：20211018

## 法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

# 通用约定

| 格式                                                                                     | 说明                                 | 样例                                                                                                              |
|----------------------------------------------------------------------------------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------|
|  危险   | 该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。   |  危险<br>重置操作将丢失用户配置数据。          |
|  警告   | 该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。 |  警告<br>重启操作将导致业务中断，恢复业务时间约十分钟。 |
|  注意   | 用于警示信息、补充说明等，是用户必须了解的内容。           |  注意<br>权重设置为0，该服务器不会再接受新请求。    |
|  说明 | 用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。       |  说明<br>您也可以通过按Ctrl+A选中全部文件。  |
| >                                                                                      | 多级菜单递进。                            | 单击设置> 网络> 设置网络类型。                                                                                               |
| 粗体                                                                                     | 表示按键、菜单、页面名称等UI元素。                 | 在结果确认页面，单击确定。                                                                                                   |
| Courier字体                                                                              | 命令或代码。                             | 执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。                                                              |
| 斜体                                                                                     | 表示参数、变量。                           | <code>bae log list --instanceid</code><br><code>Instance_ID</code>                                              |
| [] 或者 [a b]                                                                            | 表示可选项，至多选择一个。                      | <code>ipconfig [-all -t]</code>                                                                                 |
| { } 或者 {a b}                                                                           | 表示必选项，至多选择一个。                      | <code>switch {active stand}</code>                                                                              |

# 目录

|                                         |    |
|-----------------------------------------|----|
| 1.API概览                                 | 07 |
| 2.调用方式                                  | 09 |
| 3.公共参数                                  | 11 |
| 4.资产                                    | 13 |
| 4.1. AddAssets                          | 13 |
| 4.2. AddAssetTags                       | 14 |
| 4.3. DeleteAssets                       | 15 |
| 4.4. DescribeAssets                     | 17 |
| 4.5. DescribeAssetsByTags               | 21 |
| 4.6. DescribeUserTags                   | 25 |
| 5.扫描任务                                  | 28 |
| 5.1. CreateScan                         | 28 |
| 5.2. DescribeAllVulnerabilities         | 31 |
| 5.3. DescribeScans                      | 40 |
| 5.4. DescribeScanSessions               | 47 |
| 5.5. DescribeVulnerability              | 51 |
| 5.6. GenerateVulReport                  | 60 |
| 6.攻击面                                   | 63 |
| 6.1. DescribeAttackSurfacesFacets       | 63 |
| 6.2. DescribeCrawlerRequests            | 65 |
| 6.3. DescribeDNSMap                     | 68 |
| 6.4. DescribeDomainAttackSurfacesFacets | 71 |
| 6.5. DescribeDomains                    | 72 |
| 6.6. DescribeHosts                      | 74 |
| 6.7. DescribeHostAttackSurfacesFacets   | 77 |
| 6.8. DescribePorts                      | 79 |

---

|                                       |     |
|---------------------------------------|-----|
| 6.9. DescribeSubdomains               | 82  |
| 6.10. DescribeWebPaths                | 85  |
| 6.11. DescribeWebServers              | 87  |
| 6.12. DescribeWebTechs                | 90  |
| 7.攻击面透视                               | 94  |
| 7.1. AddOrgDomains                    | 94  |
| 7.2. AddOrgHosts                      | 95  |
| 7.3. AddOrgSubdomains                 | 96  |
| 7.4. AddOrgWebPaths                   | 97  |
| 7.5. CreateOrganization               | 98  |
| 7.6. DeleteOrganizations              | 99  |
| 7.7. DeleteOrgAttackSurfaceRecords    | 101 |
| 7.8. DeleteUserAttackSurfaceRecords   | 102 |
| 7.9. DescribeOrgInfo                  | 103 |
| 7.10. DescribeOrgAttackSurfaceDetails | 105 |
| 7.11. ListOrgAttackSurfaceFacets      | 107 |
| 7.12. ListOrgDNSMap                   | 111 |
| 7.13. ListOrgDomains                  | 114 |
| 7.14. ListOrgHosts                    | 116 |
| 7.15. ListOrgPorts                    | 119 |
| 7.16. ListOrgRiskyAssets              | 126 |
| 7.17. ListOrgSubdomains               | 129 |
| 7.18. ListOrgVulFacets                | 132 |
| 7.19. ListOrgWebPaths                 | 137 |
| 7.20. ListOrgWebTechs                 | 143 |
| 7.21. ListUserAttackSurfaceFacets     | 148 |
| 7.22. ListUserDNSMap                  | 151 |
| 7.23. ListUserDomains                 | 160 |

---

---

|                             |     |
|-----------------------------|-----|
| 7.24. ListUserHosts         | 162 |
| 7.25. ListUserOrganizations | 165 |
| 7.26. ListUserPorts         | 167 |
| 7.27. ListUserSubdomains    | 173 |
| 7.28. ListUserWebPaths      | 175 |
| 7.29. ListUserWebTechs      | 177 |
| 7.30. ModifyOrganization    | 179 |
| 7.31. TagAssetsByRecords    | 180 |
| 7.32. TagAssetsBySearch     | 182 |

# 1.API概览

漏洞扫描提供以下相关API接口。

## 资产

| API                                  | 描述               |
|--------------------------------------|------------------|
| <a href="#">AddAssets</a>            | 调用本接口添加用户资产。     |
| <a href="#">DescribeAssets</a>       | 调用本接口查询资产列表。     |
| <a href="#">DeleteAssets</a>         | 调用本接口删除用户资产。     |
| <a href="#">DescribeUserTags</a>     | 调用本接口查询用户所有标签列表。 |
| <a href="#">AddAssetTags</a>         | 调用本接口为资产添加标签。    |
| <a href="#">DescribeAssetsByTags</a> | 调用本接口查询标签下的资产列表。 |

## 扫描任务

| API                                        | 描述                                 |
|--------------------------------------------|------------------------------------|
| <a href="#">CreateScan</a>                 | 调用本接口创建扫描任务。                       |
| <a href="#">DescribeScans</a>              | 调用本接口获取扫描任务列表。                     |
| <a href="#">DescribeScanSessions</a>       | 调用本接口获取扫描任务实例列表。                   |
| <a href="#">GenerateVulReport</a>          | 调用本接口生成任务实例报表。                     |
| <a href="#">DescribeAllVulnerabilities</a> | 调用本接口获取扫描任务结果，包含检测出的漏洞数量和漏洞严重等级分布。 |
| <a href="#">DescribeVulnerability</a>      | 调用本接口获取漏洞详情。                       |

## 攻击面

| API                                              | 描述                                                              |
|--------------------------------------------------|-----------------------------------------------------------------|
| <a href="#">DescribeSubdomains</a>               | 调用DescribeSubdomains接口，查询任务实例对应攻击面数据项中的子域名信息。                   |
| <a href="#">DescribeCrawlerRequests</a>          | 调用DescribeCrawlerRequests接口，查询任务实例对应攻击面数据项中的爬虫流量信息。             |
| <a href="#">DescribeHostAttackSurfacesFacets</a> | 调用DescribeHostAttackSurfacesFacets接口，查询任务实例对应攻击面数据项中的主机攻击面统计信息。 |
| <a href="#">DescribeAttackSurfacesFacets</a>     | 调用DescribeAttackSurfacesFacets查询任务实例攻击面数据统计信息。                  |
| <a href="#">DescribeWebTechs</a>                 | 调用DescribeWebTechs接口，查询任务实例对应攻击面数据项中的Web应用信息。                   |

| API                                                | 描述                                                                |
|----------------------------------------------------|-------------------------------------------------------------------|
| <a href="#">DescribeDomains</a>                    | 调用DescribeDomains接口，查询任务实例对应攻击面数据项中的域名信息。                         |
| <a href="#">DescribeHosts</a>                      | 调用DescribeHosts接口，查询任务实例对应攻击面数据项中的主机列表信息。                         |
| <a href="#">DescribePorts</a>                      | 调用DescribePorts接口，查询任务实例对应攻击面数据项中的端口服务信息。                         |
| <a href="#">DescribeDomainAttackSurfacesFacets</a> | 调用DescribeDomainAttackSurfacesFacets接口，查询任务实例对应攻击面数据项中的域名攻击面统计信息。 |
| <a href="#">DescribeWebServers</a>                 | 调用DescribeWebServers接口，查询任务实例对应攻击面数据项中的Web服务器信息。                  |
| <a href="#">DescribeWebPaths</a>                   | 调用DescribeWebPaths接口，查询任务实例对应攻击面数据项中的Web路径信息。                     |
| <a href="#">DescribeDNSMap</a>                     | 调用DescribeDNSMap接口，查询任务实例对应攻击面数据项中的DNS解析记录信息。                     |

## 登录态

| API                                  | 描述                                                  |
|--------------------------------------|-----------------------------------------------------|
| <a href="#">DeleteSession</a>        | 调用 DeleteSession 可以删除指定的登录态信息。                      |
| <a href="#">DescribeListSessions</a> | 调用 DescribeListSessions 接口，用户获取登录态列表信息。             |
| <a href="#">DescribeSession</a>      | 调用DescribeSession接口，获取指定登录态信息。                      |
| <a href="#">EditSession</a>          | 调用 EditSession 接口，用户可以对已创建的登录态信息进行编辑。               |
| <a href="#">CreateSession</a>        | 调用 CreateSession 接口，用户可以调用该接口创建登录态信息，并用于对应用进行登录态扫描。 |

## 2.调用方式

您可以通过发送HTTP GET请求调用漏洞扫描API，并按照接口说明在请求中加入相应的请求参数。调用接口后系统会返回处理结果。请求和返回结果都使用UTF-8字符集进行编码。

### 请求结构

漏洞扫描系统的API是RPC风格，您可以通过发送HTTP GET请求调用漏洞扫描的API。

其请求结构如下：

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

其中：

- Endpoint：漏洞扫描API的服务接入地址为avds.aliyuncs.com。
- Action：要执行的操作，如使用DescribeAssets查询用户资产列表。
- Version：要使用的API版本，漏洞扫描的API版本是2017-11-29。
- Parameters：请求参数，每个参数之间用“&”分隔。

请求参数由公共请求参数和API自定义参数组成。公共参数中包含API版本号、身份验证等信息，详细内容参见[公共参数](#)。

下面是一个调用DescribeAssets接口查询用户资产列表的示例：

 说明 为了便于用户查看，本文档中的示例都做了格式化处理。

```
http(s)://avds.aliyuncs.com/?Action=DescribeAssets
&Format=xml
&Version=2017-11-29
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
...
```

### API授权

为了确保您的账号安全，建议您使用子账号的身份凭证调用API。如果您使用RAM账号调用漏洞扫描API，您需要为该RAM账号创建、附加相应的授权策略。

### API签名

漏洞扫描服务会对每个API请求进行身份验证，无论使用HTTP还是HTTPS协议提交请求，都需要在请求中包含签名（Signature）信息。

漏洞扫描通过使用AccessKey ID和AccessKey Secret进行对称加密的方法来验证请求的发送者身份。AccessKey是为阿里云账号和RAM用户发布的一种身份凭证（类似于用户的登录密码），其中AccessKey ID用于标识访问者的身份，AccessKey Secret是用于加密签名字符串和服务器端验证签名字符串的密钥，必须严格保密。

RPC API需按如下格式在请求中增加签名（Signature）：

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

以DescribeAssets为例，假设AccessKey ID是 `testid`，AccessKey Secret是 `testsecret`，则签名前的请求URL如下：

```
https://avds.aliyuncs.com/?Action=DescribeAssets
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2017-11-29
&SignatureVersion=1.0
```

完成以下步骤计算签名：

1. 使用请求参数创建待签名字符串：

```
GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeAssets&Format%3DXML&SignatureMethod%3D
HMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&SignatureVersion%3D1.0&Ti
meStamp%3D2016-02-23T12%253A46%253A24Z&Version%3D2018-12-03
```

2. 计算待签名的HMAC的值。

在AccessKey Secret后添加一个“&”作为计算HMAC值的key。本示例中的key为 `testsecret&`。

```
CT9X0VtwR86fNWSnsc6v8YGOjuE=
```

3. 将签名加到请求参数中：

```
https://avds.aliyuncs.com/?Action=DescribeAssets
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2017-11-29
&SignatureVersion=1.0
&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
```

 **说明** 阿里云提供了多种语言的SDK及第三方SDK，可以免去您对签名算法进行编码的麻烦。更多阿里云SDK信息请参见[阿里云开发工具包（SDK）](#)。

## 3. 公共参数

本文档介绍API接口使用的公共请求参数。

### 公共请求参数

公共请求参数是每个接口都需要使用到的请求参数。

公共请求参数表

| 名称                   | 类型     | 是否必须 | 描述                                                                                                           |
|----------------------|--------|------|--------------------------------------------------------------------------------------------------------------|
| Format               | string | 否    | 返回消息的格式。取值： <ul style="list-style-type: none"><li>JSON（默认值）</li><li>XML</li></ul>                            |
| Version              | String | 是    | API版本号，使用YYYY-MM-DD日期格式。<br>取值：2017-11-29。                                                                   |
| AccessKeyId          | String | 是    | 访问服务使用的密钥ID。                                                                                                 |
| Signature            | String | 是    | 签名结果串。                                                                                                       |
| SignatureMethod      | String | 是    | 签名方式。<br>取值：HMAC-SHA1。                                                                                       |
| Timestamp            | String | 是    | 请求的时间戳，为日期格式。使用UTC时间按照ISO8601标，格式为YYYY-MM-DDThh:mm:ssZ。<br>例如，北京时间2013年1月10日20点0分0秒，表示为2013-01-10T12:00:00Z。 |
| SignatureVersion     | String | 是    | 签名算法版本，目前版本是1.0。                                                                                             |
| SignatureNonce       | String | 是    | 唯一随机数，用于防止网络重放攻击。<br>在不同请求间要使用不同的随机数值。                                                                       |
| ResourceOwnerAccount | String | 否    | 本次API请求访问到的资源所有者账户，即登录用户名。                                                                                   |

示例

```
https://avds.aliyuncs.com/  
?Format=xml  
&Version=2017-11-29  
&Signature=Pc5WB8gokVn0xfeu%2FZV%2BiNM1dgl%3D  
&SignatureMethod=HMAC-SHA1  
&SignatureNonce=15215528852396  
&SignatureVersion=1.0  
&AccessKeyId=key-test  
&Timestamp=2012-06-01T12:00:00Z
```

## 公共返回参数

API返回结果采用统一格式，返回2xx HTTP状态码代表调用成功；返回4xx或5xx HTTP状态码代表调用失败。

调用成功返回的数据格式有XML和JSON两种，可以在发送请求时指定返回的数据格式，默认为JSON格式。

每次接口调用，无论成功与否，系统都会返回一个唯一识别码RequestId。

- XML格式

```
<?xml version="1.0" encoding="utf-8"?>  
  <!--结果的根结点-->  
  <接口名称+Response>  
    <!--返回请求标签-->  
    <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>  
    <!--返回结果数据-->  
  </接口名称+Response>
```

- JSON格式

```
{  
  "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",  
  /*返回结果数据*/  
}
```

# 4.资产

## 4.1. AddAssets

调用AddAssets添加资产列表和标签列表。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

### 请求参数

| 名称       | 类型         | 是否必选 | 示例值                              | 描述                               |
|----------|------------|------|----------------------------------|----------------------------------|
| Action   | String     | 是    | AddAssets                        | 要执行的操作。取值：<br><b>AddAssets</b> 。 |
| Assets.N | RepeatList | 是    | ['a.aliyun.com', 'b.aliyun.com'] | 指定待添加的资产列表。                      |
| SourceIp | String     | 否    | 1.2.3.4                          | 指定访问者的源IP地址。                     |
| Tags.N   | RepeatList | 否    | ['tag1', 'tag2']                 | 指定添加标签列表中各标签下的资产。                |

### 返回数据

| 名称        | 类型      | 示例值                                  | 描述                                                                                                   |
|-----------|---------|--------------------------------------|------------------------------------------------------------------------------------------------------|
| RequestId | String  | 0C992F5D-8568-41B4-9685-05C0DAEAE9D7 | 返回请求结果ID。                                                                                            |
| Success   | Boolean | true                                 | 返回请求添加资产是否成功的结果。取值： <ul style="list-style-type: none"><li><b>true</b></li><li><b>false</b></li></ul> |

### 示例

请求示例

```
http(s)://[Endpoint]/?Action=AddAssets
&Assets.1=['a.aliyun.com', 'b.aliyun.com']
&<公共请求参数>
```

正常返回示例

XML 格式

```
<AddAssetsResponse>
  <code>200</code>
  <requestId>0C992F5D-8568-41B4-9685-05C0DAEAE9D7</requestId>
  <success>true</success>
</AddAssetsResponse>
```

JSON 格式

```
{
  "code": "200",
  "requestId": "0C992F5D-8568-41B4-9685-05C0DAEAE9D7",
  "success": true
}
```

错误码

访问[错误中心](#)查看更多错误码。

## 4.2. AddAssetTags

调用AddAssetTags为资产添加标签。

 **说明** 调用本接口可以为多个资产添加标签，或者为一个资产添加多个标签。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称       | 类型         | 是否必选 | 示例值                                 | 描述                                                                               |
|----------|------------|------|-------------------------------------|----------------------------------------------------------------------------------|
| Action   | String     | 是    | AddAssetTags                        | 要执行的操作。取值：<br><b>AddAssetTags</b> 。                                              |
| Assets.N | RepeatList | 是    | ['a.aliyun.com',<br>'b.aliyun.com'] | 指定待添加标签的资产列表。                                                                    |
| SourceIp | String     | 否    | 1.2.3.4                             | 指定访问者的源IP地址。                                                                     |
| Lang     | String     | 否    | zh                                  | 指定返回结果的语言环境。 <ul style="list-style-type: none"><li>zh：中文</li><li>en：英文</li></ul> |

| 名称     | 类型         | 是否必选 | 示例值             | 描述          |
|--------|------------|------|-----------------|-------------|
| Tags.N | RepeatList | 否    | ['tag1','tag2'] | 指定待添加的标签列表。 |

## 返回数据

| 名称        | 类型     | 示例值                                  | 描述         |
|-----------|--------|--------------------------------------|------------|
| RequestId | String | 0C992F5D-8568-41B4-9685-05C0DAEAE9D7 | 返回结果的请求ID。 |

## 示例

请求示例

```
http(s)://[Endpoint]/?Action=AddAssetTags
&Assets.1=['a.aliyun.com','b.aliyun.com']
&<公共请求参数>
```

正常返回示例

XML 格式

```
<AddAssetTagsResponse>
  <code>200</code>
  <requestId>0C992F5D-8568-41B4-9685-05C0DAEAE9D7</requestId>
  <success>true</success>
</AddAssetTagsResponse>
```

JSON 格式

```
{
  "code": "200",
  "requestId": "0C992F5D-8568-41B4-9685-05C0DAEAE9D7",
  "success": true
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

# 4.3. DeleteAssets

调用DeleteAssets删除不需要进行漏洞扫描的资产。

## 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称         | 类型         | 是否必选 | 示例值                              | 描述                               |
|------------|------------|------|----------------------------------|----------------------------------|
| Action     | String     | 是    | DeleteAssets                     | 要执行的操作。取值： <b>DeleteAssets</b> 。 |
| AssetIds.N | RepeatList | 是    | ['a.aliyun.com', 'b.aliyun.com'] | 指定待删除的资产构成列表。                    |
| SourceIp   | String     | 否    | 1.2.3.4                          | 指定访问源的IP地址。                      |

返回数据

| 名称        | 类型     | 示例值                                  | 描述         |
|-----------|--------|--------------------------------------|------------|
| RequestId | String | 0C992F5D-8568-41B4-9685-05C0DAEAE9D7 | 返回结果的请求ID。 |

示例

请求示例

http(s)://[Endpoint]/?Action=DeleteAssets  
&AssetIds.1=['a.aliyun.com', 'b.aliyun.com']  
&<公共请求参数>

正常返回示例

XML 格式

```
<DeleteAssetsResponse>  
  <code>200</code>  
  <requestId>0C992F5D-8568-41B4-9685-05C0DAEAE9D7</requestId>  
  <success>true</success>  
</DeleteAssetsResponse>
```

JSON 格式

```
{  
  "code": "200",  
  "requestId": "0C992F5D-8568-41B4-9685-05C0DAEAE9D7",  
  "success": true  
}
```

错误码

访问[错误中心](#)查看更多错误码。

## 4.4. DescribeAssets

调用DescribeAssets查询资产列表。

 **说明** 调用本接口可以分页查询所有的资产（包括阿里云资产）。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

### 请求参数

| 名称       | 类型         | 是否必选 | 示例值                    | 描述                                                                                                                                                                                                                        |
|----------|------------|------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action   | String     | 是    | DescribeAssets         | 要执行的操作。取值： <b>DescribeAssets</b> 。                                                                                                                                                                                        |
| SourceIp | String     | 否    | 1.2.3.4                | 指定访问者源的IP地址。                                                                                                                                                                                                              |
| Status   | String     | 否    | WaitingForVerification | 指定查询特定资产的认证状态。取值： <ul style="list-style-type: none"><li>• <b>WaitingForVerification</b>：等待验证</li><li>• <b>VerificationSuccess</b>：验证成功</li><li>• <b>VerificationFailure</b>：验证失败</li><li>• <b>Verifying</b>：验证中</li></ul> |
| Search   | String     | 否    | test                   | 指定查询特定资产信息。                                                                                                                                                                                                               |
| Types.N  | RepeatList | 否    | ip                     | 指定返回特定资产类型下的资产信息。取值： <ul style="list-style-type: none"><li>• <b>domain</b>：资产根域名</li><li>• <b>ip</b>：资产IP</li><li>• <b>subdomain</b>：资产子域名</li></ul>                                                                      |
| Source   | String     | 否    | UserAdd                | 指定返回特定资产来源下的资产信息。取值： <ul style="list-style-type: none"><li>• <b>UserAdd</b>：用户添加</li><li>• <b>AutoImport</b>：自动导入</li><li>• <b>ScanDiscover</b>：资产发现</li></ul>                                                            |
| Assets.N | RepeatList | 否    | ['1.2.3.5']            | 指定待查询的资产列表。                                                                                                                                                                                                               |

| 名称            | 类型      | 是否必选 | 示例值           | 描述               |
|---------------|---------|------|---------------|------------------|
| GmtCreateFrom | Long    | 否    | 1112121000000 | 资产创建时间的开始区间。     |
| GmtCreateTo   | Long    | 否    | 1212121000000 | 资产创建时间的结束区间。     |
| CurrentPage   | Integer | 否    | 1             | 指定返回资产列表的当前页码。   |
| PageSize      | Integer | 否    | 20            | 指定返回资产列表每页的数据条数。 |

## 返回数据

| 名称           | 类型      | 示例值                           | 描述                                      |
|--------------|---------|-------------------------------|-----------------------------------------|
| Count        | Integer | 20                            | 返回结果的当前页显示的数据条数。                        |
| CurrentPage  | Integer | 1                             | 返回结果的当前页码。                              |
| List         | Array   |                               | 资产列表。                                   |
| Asset        | String  | test.cn                       | 返回资产的名称。                                |
| AssetGroupId | String  | 11111                         | 资产标签分组的ID。                              |
| AssetId      | String  | eb293323-ccc9-417d-bb03-***** | 返回资产的ID。                                |
| ExpireTime   | Long    | 1592044480000                 | 返回资产的到期时间。                              |
| GmtCreate    | Long    | 1533543752000                 | 返回资产的创建时间。                              |
| LastScanDate | Long    | 1533543752000                 | 返回资产的最后漏洞扫描时间。                          |
| Source       | String  | UserAdd                       | 返回资产的来源类型。                              |
| Status       | String  | Success                       | （此参数已废弃）资产的验证状态。<br>唯一值：Success，表示验证成功。 |

| 名称                  | 类型      | 示例值                           | 描述                                                                                                                                                           |
|---------------------|---------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type                | String  | domain                        | （此参数已废弃）返回资产的所属资产类型。                                                                                                                                         |
| VerifyFailureReason | String  | Null                          | （此参数已废弃）资产验证失败的原因。                                                                                                                                           |
| VerifyType          | String  | Cname                         | （此参数已废弃）资产的验证类型。取值： <ul style="list-style-type: none"><li>• <b>Cname</b>：域名解析验证。</li><li>• <b>File</b>：MD5文件验证。</li><li>• <b>Html</b>：网站的html文件验证。</li></ul> |
| PageCount           | Integer | 2                             | 返回结果的页数。                                                                                                                                                     |
| PageSize            | Integer | 20                            | 返回结果每页显示的总数据条数。                                                                                                                                              |
| RequestId           | String  | 6D584A17-4DA1-4CFD-BB31-***** | 请求结果ID。                                                                                                                                                      |
| TotalCount          | Integer | 36                            | 返回的资产总数。                                                                                                                                                     |

示例

请求示例

http(s)://[Endpoint]/?Action=DescribeAssets  
&<公共请求参数>

正常返回示例

XML 格式

```
<DescribeAssetsResponse>
  <code>200</code>
  <data>
    <Count>20</Count>
    <CurrentPage>1</CurrentPage>
    <List>
      <Asset>test.cn</Asset>
      <AssetId>eb293323-ccc9-417d-bb03-93f7227ea128</AssetId>
      <GmtCreate>1533543752000</GmtCreate>
      <Source>UserAdd</Source>
      <Type>domain</Type>
    </List>
    <List>
      <Asset>***.***.io</Asset>
      <AssetId>0b77e27e-c0d9-40ef-b52d-7d6588e5ea7a</AssetId>
      <GmtCreate>1531125482000</GmtCreate>
      <LastScanDate>2018-07-10T11:11Z</LastScanDate>
      <Source>UserAdd</Source>
      <Type>subdomain</Type>
    </List>
    <List>
      <Asset>1.2.3.4</Asset>
      <AssetId>b7691e9e-205d-4681-bd39-1b9a7c0d810a</AssetId>
      <GmtCreate>1524177510000</GmtCreate>
      <LastScanDate>2018-05-21T09:38Z</LastScanDate>
      <Source>ScanDiscover</Source>
      <Type>ip</Type>
    </List>
    <PageCount>2</PageCount>
    <PageSize>20</PageSize>
    <TotalCount>36</TotalCount>
  </data>
  <requestId>6D584A17-4DA1-4CFD-BB31-BDABDF60F906</requestId>
  <success>true</success>
</DescribeAssetsResponse>
```

JSON 格式

```
{
  "code":200,
  "data":{
    "Count":20,
    "CurrentPage":1,
    "List":[
      {
        "Asset":"test.cn",
        "AssetId":"eb293323-ccc9-417d-bb03-93f7227ea128",
        "GmtCreate":1533543752000,
        "Source":"UserAdd",
        "Type":"domain"
      },
      {
        "Asset":"***.***.io",
        "AssetId":"0b77e27e-c0d9-40ef-b52d-7d6588e5ea7a",
        "GmtCreate":1531125482000,
        "LastScanDate":"2018-07-10T11:11Z",
        "Source":"UserAdd",
        "Type":"subdomain"
      },
      {
        "Asset":"1.2.3.4",
        "AssetId":"b7691e9e-205d-4681-bd39-1b9a7c0d810a",
        "GmtCreate":1524177510000,
        "LastScanDate":"2018-05-21T09:38Z",
        "Source":"ScanDiscover",
        "Type":"ip"
      }
    ],
    "PageCount":2,
    "PageSize":20,
    "TotalCount":36
  },
  "requestId":"6D584A17-4DA1-4CFD-BB31-BDABDF60F906",
  "success":true
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 4.5. DescribeAssetsByTags

调用DescribeAssetsByTags查询多个标签下的资产列表信息。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

### 请求参数

| 名称          | 类型         | 是否必选 | 示例值                  | 描述                                                                                                                  |
|-------------|------------|------|----------------------|---------------------------------------------------------------------------------------------------------------------|
| Action      | String     | 是    | DescribeAssetsByTags | 要执行的操作。取值： <b>DescribeAssetsByTags</b> 。                                                                            |
| SourceIp    | String     | 否    | 1.2.3.4              | 指定访问者的源IP。                                                                                                          |
| Lang        | String     | 否    | zh                   | 指定返回结果的语言环境。取值： <ul style="list-style-type: none"> <li><b>zh</b>：中文</li> <li><b>en</b>：英文</li> </ul>                |
| Tags.N      | RepeatList | 否    | ['tag1', 'tag2']     | 指定标签下待显示的资产列表。                                                                                                      |
| Type        | String     | 否    | ip                   | 指定目标资产类型的标签信息。取值： <ul style="list-style-type: none"> <li><b>ip</b>：IP类型资产</li> <li><b>domain</b>：根域名类型资产</li> </ul> |
| Search      | String     | 否    | 1.2.3.5              | 指定待查询的目标资产信息。                                                                                                       |
| Untagged    | Integer    | 否    | 0                    | 指定是否获取无标签下的资产信息。                                                                                                    |
| CurrentPage | Integer    | 否    | 2                    | 指定返回资产列表的当前页码。                                                                                                      |
| PageSize    | Integer    | 否    | 20                   | 指定返回资产列表的每页显示数据总条数。                                                                                                 |

## 返回数据

| 名称           | 类型      | 示例值    | 描述                |
|--------------|---------|--------|-------------------|
| Count        | Integer | 14     | 返回结果的当前页中显示的数据条数。 |
| CurrentPage  | Integer | 5      | 返回结果的当前页码。        |
| List         | Array   |        | 返回的资产列表。          |
| Asset        | String  | test   | 返回资产列表中的资产名称。     |
| AssetGroupId | String  | group1 | 资产标签分组的ID。        |

| 名称                  | 类型      | 示例值                                  | 描述                                                                                                                                              |
|---------------------|---------|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| AssetId             | String  | 13183b57-f77c-459b-8512-*****        | 返回资产列表中的资产ID。                                                                                                                                   |
| ExpireTime          | Long    | 1592044480000                        | 返回资产的到期时间。                                                                                                                                      |
| GmtCreate           | Long    | 1545972690000                        | 返回资产列表中资产的创建时间。                                                                                                                                 |
| LastScanDate        | Long    | 1540744470000                        | 返回资产列表中资产的最后漏洞扫描时间。                                                                                                                             |
| Source              | String  | UserAdd                              | 返回资产列表中的资产来源类型。                                                                                                                                 |
| Status              | String  | Success                              | (此参数已废弃) 资产的验证状态。<br>唯一值: Success, 表示验证成功                                                                                                       |
| Type                | String  | ip                                   | (此参数已废弃) 返回资产列表中的资产类型。                                                                                                                          |
| VerifyFailureReason | String  | Null                                 | (此参数已废弃) 资产验证失败的原因。                                                                                                                             |
| VerifyType          | String  | Cname                                | (此参数已废弃) 资产的验证类型。<br>取值: <ul style="list-style-type: none"><li>• Cname: 域名解析验证。</li><li>• File: MD5文件验证。</li><li>• Html: 网站的html文件验证。</li></ul> |
| PageCount           | Integer | 7                                    | 返回结果的总页数。                                                                                                                                       |
| PageSize            | Integer | 20                                   | 返回结果每页显示的数据总条数。                                                                                                                                 |
| RequestId           | String  | 6A218865-5D7C-42EE-9509-33069D66F284 | 返回结果的请求ID。                                                                                                                                      |
| TotalCount          | Integer | 60                                   | 返回结果的资产总数量。                                                                                                                                     |

## 示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeAssetsByTags
&Tags.1=['tag1', 'tag2']
&<公共请求参数>
```

#### 正常返回示例

##### XML 格式

```
<DescribeAssetsByTagsResponse>
  <code>200</code>
  <data>
    <Count>20</Count>
    <CurrentPage>1</CurrentPage>
    <List>
      <Asset>test.cn</Asset>
      <AssetId>eb293323-ccc9-417d-bb03-93f7227ea128</AssetId>
      <GmtCreate>1533543752000</GmtCreate>
      <Source>UserAdd</Source>
      <Type>domain</Type>
    </List>
    <List>
      <Asset>***.***.io</Asset>
      <AssetGroupId>default</AssetGroupId>
      <AssetId>0b77e27e-c0d9-40ef-b52d-7d6588e5ea7a</AssetId>
      <GmtCreate>1531125482000</GmtCreate>
      <LastScanDate>2018-07-10T11:11Z</LastScanDate>
      <Source>UserAdd</Source>
      <Type>subdomain</Type>
    </List>
    <List>
      <Asset>1.2.3.4</Asset>
      <AssetGroupId>default</AssetGroupId>
      <AssetId>b7691e9e-205d-4681-bd39-1b9a7c0d810a</AssetId>
      <GmtCreate>1524177510000</GmtCreate>
      <LastScanDate>2018-05-21T09:38Z</LastScanDate>
      <Source>ScanDiscover</Source>
      <Type>ip</Type>
    </List>
    <PageCount>2</PageCount>
    <PageSize>20</PageSize>
    <TotalCount>36</TotalCount>
  </data>
  <requestId>6D584A17-4DA1-4CFD-BB31-BDABDF60F906</requestId>
  <success>true</success>
</DescribeAssetsByTagsResponse>
```

##### JSON 格式

```
{
  "code":200,
  "data":{
    "Count":20,
    "CurrentPage":1,
    "List":[
      {
        "Asset":"test.cn",
        "AssetId":"eb293323-ccc9-417d-bb03-93f7227ea128",
        "GmtCreate":1533543752000,
        "Source":"UserAdd",
        "Type":"domain"
      },
      {
        "Asset":"***.***.io",
        "AssetGroupId":"default",
        "AssetId":"0b77e27e-c0d9-40ef-b52d-7d6588e5ea7a",
        "GmtCreate":1531125482000,
        "LastScanDate":"2018-07-10T11:11Z",
        "Source":"UserAdd",
        "Type":"subdomain"
      },
      {
        "Asset":"1.2.3.4",
        "AssetGroupId":"default",
        "AssetId":"b7691e9e-205d-4681-bd39-1b9a7c0d810a",
        "GmtCreate":1524177510000,
        "LastScanDate":"2018-05-21T09:38Z",
        "Source":"ScanDiscover",
        "Type":"ip"
      }
    ],
    "PageCount":2,
    "PageSize":20,
    "TotalCount":36
  },
  "requestId":"6D584A17-4DA1-4CFD-BB31-BDABDF60F906",
  "success":true
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 4.6. DescribeUserTags

调用DescribeUserTags查询用户资产的所有标签列表信息。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

## 请求参数

| 名称          | 类型      | 是否必选 | 示例值              | 描述                                                                                 |
|-------------|---------|------|------------------|------------------------------------------------------------------------------------|
| Action      | String  | 是    | DescribeUserTags | 要执行的操作。取值： <b>DescribeUserTags</b> 。                                               |
| SourceIp    | String  | 否    | 1.2.3.4          | 指定访问者源IP地址。                                                                        |
| Lang        | String  | 否    | zh               | 指定返回结果语言环境。取值： <ul style="list-style-type: none"><li>zh：中文</li><li>en：英文</li></ul> |
| Search      | String  | 否    | test.**.com      | 根据搜索信息查询特定资产标签列表。                                                                  |
| CurrentPage | Integer | 否    | 20               | 指定待查询列表的当前页码。                                                                      |
| PageSize    | Integer | 否    | 2                | 指定待查询结果每页显示的数据总数量。                                                                 |

## 返回数据

| 名称          | 类型      | 示例值                                  | 描述             |
|-------------|---------|--------------------------------------|----------------|
| Count       | Integer | 25                                   | 返回结果当前页的数据总条数。 |
| CurrentPage | Integer | 3                                    | 返回结果的当前页码。     |
| List        | Array   |                                      | 返回结果的标签列表信息。   |
| AssetCount  | Integer | 200                                  | 返回结果标签下的资产数量。  |
| TagKey      | String  | tag1                                 | 返回结果的标签名称。     |
| PageCount   | Integer | 5                                    | 返回结果总页数。       |
| PageSize    | Integer | 30                                   | 返回结果每页显示的数据条数。 |
| RequestId   | String  | 0C992F5D-8568-41B4-9685-05C0DAEAE9D7 | 返回结果的请求ID。     |

| 名称         | 类型      | 示例值 | 描述        |
|------------|---------|-----|-----------|
| TotalCount | Integer | 60  | 返回的标签总数量。 |

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeUserTags
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeUserTagsResponse>
  <code>200</code>
  <requestId>0C992F5D-8568-41B4-9685-05C0DAEAE9D7</requestId>
  <success>true</success>
  <data>
    <List>
      <TagKey>mytag</TagKey>
      <AssetCount>1</AssetCount>
    </List>
  </data>
</DescribeUserTagsResponse>
```

JSON 格式

```
{
  "code": "200",
  "requestId": "0C992F5D-8568-41B4-9685-05C0DAEAE9D7",
  "success": true,
  "data": {
    "List": [
      {
        "TagKey": "mytag",
        "AssetCount": 1
      }
    ]
  }
}
```

错误码

访问[错误中心](#)查看更多错误码。

## 5.扫描任务

### 5.1. CreateScan

调用CreateScan创建漏洞扫描任务和内容检测任务。

#### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

#### 请求参数

| 名称                  | 类型         | 是否必选 | 示例值                  | 描述                                                                                                                                                 |
|---------------------|------------|------|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Action              | String     | 是    | CreateScan           | 要执行的操作。取值： <b>CreateScan</b> 。                                                                                                                     |
| Name                | String     | 是    | 单次任务                 | 设置扫描任务名称。                                                                                                                                          |
| ScanType            | String     | 是    | vuln                 | 指定扫描任务的扫描资产的检测类型。取值： <ul style="list-style-type: none"><li><b>vuln</b>：漏洞类型</li><li><b>content</b>：内容风险</li><li><b>asset</b>：资产发现</li></ul>        |
| SourceIp            | String     | 否    | 1.2.3.4              | 指定访问者源IP地址。                                                                                                                                        |
| Targets.N           | RepeatList | 否    | ["***.testfire.net"] | 指定待扫描目标资产列表。                                                                                                                                       |
| ScanAll             | Integer    | 否    | 1                    | 扫描所有资产。                                                                                                                                            |
| FlowName            | String     | 否    | assets               | 指定扫描任务的扫描模式。取值： <ul style="list-style-type: none"><li><b>assets</b>：资产模式</li><li><b>general</b>：标准模式</li><li><b>skynet_vul_scan</b>：深度模式</li></ul> |
| EnableAssetDiscover | Integer    | 否    | 1                    | 漏洞扫描任务是否开启资产发现。取值： <ul style="list-style-type: none"><li><b>0</b>：开启</li><li><b>1</b>：不开启</li></ul>                                                |

| 名称                    | 类型      | 是否必选 | 示例值          | 描述                                                                                                                                       |
|-----------------------|---------|------|--------------|------------------------------------------------------------------------------------------------------------------------------------------|
| TriggerType           | String  | 否    | date         | 指定扫描任务的触发类型。取值： <ul style="list-style-type: none"><li>• <b>date</b>：单次任务</li><li>• <b>interval</b>：周期任务</li></ul>                        |
| Period                | String  | 否    | day          | 指定扫描任务的扫描周期。取值： <ul style="list-style-type: none"><li>• <b>day</b>：每天一次</li><li>• <b>week</b>：每周一次</li><li>• <b>month</b>：每月一次</li></ul> |
| Interval              | Integer | 否    | 5            | 指定扫描任务的扫描间隔，即距离上一次任务扫描的时间。                                                                                                               |
| StartDate             | Long    | 否    | 111122200000 | 指定扫描任务执行的开始时间。                                                                                                                           |
| EndDate               | Long    | 否    | 212212000000 | 指定扫描任务执行的结束时间。                                                                                                                           |
| Qps                   | Integer | 否    | 16           | 指定扫描任务的扫描速度。取值： <ul style="list-style-type: none"><li>• <b>16</b>：慢速</li><li>• <b>32</b>：常速</li><li>• <b>64</b>：快速</li></ul>             |
| RuntimeStart          | String  | 否    | 00:00:00     | 指定扫描任务扫描开始的时间。                                                                                                                           |
| RuntimeEnd            | String  | 否    | 08:00:00     | 指定扫描任务扫描结束的时间。                                                                                                                           |
| IndexIntervalInMinute | Integer | 否    | 5            | 首页检测间隔（分钟）。取值： <ul style="list-style-type: none"><li>• <b>5</b>：间隔5分钟</li><li>• <b>30</b>：间隔30分钟</li><li>• <b>60</b>：间隔60分钟</li></ul>    |
| SiteIntervalInDay     | Integer | 否    | 1            | 全站检测间隔（天）。取值： <ul style="list-style-type: none"><li>• <b>1</b>：每1天一次</li><li>• <b>7</b>：每7天一次</li></ul>                                  |

| 名称                   | 类型         | 是否必选 | 示例值                    | 描述                                                                                    |
|----------------------|------------|------|------------------------|---------------------------------------------------------------------------------------|
| EnableAssetLoginScan | Integer    | 否    | 1                      | 漏洞扫描任务是否开启登录扫描。取值： <ul style="list-style-type: none"><li>0：不开启</li><li>1：开启</li></ul> |
| TargetAssetTags.N    | RepeatList | 否    | []                     | 指定待扫描目标资产的标签列表。                                                                       |
| KeyWords.N           | RepeatList | 否    | []                     | 附加词库列表。                                                                               |
| URLs.N               | RepeatList | 否    | https://www.aliyun.com | Web路径列表。                                                                              |
| OrgIds.N             | RepeatList | 否    | [1, 2, 3]              | 组织机构ID列表。                                                                             |

返回数据

| 名称        | 类型     | 示例值                                  | 描述         |
|-----------|--------|--------------------------------------|------------|
| Data      | String | { "Data": "2018080617471590979" }    | 返回的结果数据。   |
| RequestId | String | 76F297E0-D4C2-442A-AEAD-AABA97975060 | 返回结果的请求ID。 |

示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateScan
&FlowName=assets
&Name=单次任务
&Qps=16
&RuntimeEnd=08:00:00
&RuntimeStart=00:00:00
&ScanType=vuln
&StartDate=111122200000
&TriggerType=date
&<公共请求参数>
```

正常返回示例

XML 格式

```
<CreateScanResponse>
  <requestId>76F297E0-D4C2-442A-AEAD-AABA97975060</requestId>
  <data>
    <Data>2018080617471590979</Data>
  </data>
  <code>200</code>
  <success>true</success>
</CreateScanResponse>
```

JSON 格式

```
{
  "requestId": "76F297E0-D4C2-442A-AEAD-AABA97975060",
  "data": {
    "Data": "2018080617471590979"
  },
  "code": 200,
  "success": true
}
```

错误码

访问[错误中心](#)查看更多错误码。

## 5.2. DescribeAllVulnerabilities

调用DescribeAllVulnerabilities获取漏洞扫描任务结果，包含检测出的漏洞数量和漏洞严重等级分布。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称       | 类型     | 是否必选 | 示例值                        | 描述                                             |
|----------|--------|------|----------------------------|------------------------------------------------|
| Action   | String | 是    | DescribeAllVulnerabilities | 要执行的操作。取值： <b>DescribeAllVulnerabilities</b> 。 |
| SourceIp | String | 否    | 1.2.3.4                    | 访问者源IP地址。                                      |
| ScanId   | String | 否    | 2018042307022680333        | 漏洞扫描任务ID。                                      |
| Name     | String | 否    | test                       | 漏洞扫描任务名称。                                      |

| 名称        | 类型      | 是否必选 | 示例值             | 描述                                                                                                                                                                                                                                                                                                                            |
|-----------|---------|------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Search    | String  | 否    | ***.***.net     | 根据特定的搜索条件（资产名）查询漏洞扫描结果。                                                                                                                                                                                                                                                                                                       |
| Lang      | String  | 否    | zh              | 请求和接收消息的语言类型。取值： <ul style="list-style-type: none"> <li>zh：中文</li> <li>en：英文</li> </ul>                                                                                                                                                                                                                                       |
| Severity  | Integer | 否    | 0               | 漏洞威胁等级。取值： <ul style="list-style-type: none"> <li>3：高危。表示可以直接被利用的漏洞，且利用难度较低。被攻击之后可能对网站或服务器的正常运行造成严重影响，或对用户财产及个人信息造成重大损失。</li> <li>2：中危。表示被利用之后，造成的影响较大，但直接利用难度较高的漏洞。或本身无法直接攻击，但能为进一步攻击造成便利的漏洞。</li> <li>1：低危。表示无法直接实现攻击，但提供的信息可能让攻击者更容易找到其他安全漏洞。</li> <li>0：信息。表示本身对网站安全没有直接影响，提供的信息可能为攻击者提供少量帮助，或可用于其他手段的攻击，如社工等。</li> </ul> |
| Status    | String  | 否    | 0               | 漏洞状态。取值： <ul style="list-style-type: none"> <li>0：未处理</li> <li>1：已处理</li> <li>2：白名单</li> <li>3：忽略</li> </ul>                                                                                                                                                                                                                  |
| BeginTime | Long    | 否    | 11258600000     | 查询特定搜索条件（任务开始时间）下的漏洞扫描结果。                                                                                                                                                                                                                                                                                                     |
| EndTime   | Long    | 否    | 11258400000     | 漏洞扫描任务的扫描结束时间。                                                                                                                                                                                                                                                                                                                |
| TaskId    | Long    | 否    | 1111111         | 漏洞扫描子任务ID。                                                                                                                                                                                                                                                                                                                    |
| Category  | String  | 否    | core            | 根据类别查询漏洞扫描结果。                                                                                                                                                                                                                                                                                                                 |
| Module    | String  | 否    | relation_domain | 根据漏洞模块查询任务实例扫描结果。                                                                                                                                                                                                                                                                                                             |

| 名称      | 类型   | 是否必选 | 示例值 | 描述                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------|------|------|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VulType | Long | 否    | 1   | <p>描述漏洞类型。包含以下类型：</p> <ul style="list-style-type: none"> <li>1: "失效的身份认证"</li> <li>2: "失效的访问控制"</li> <li>3: "命令注入"</li> <li>4: "跨站请求伪造"</li> <li>5: "跨站点脚本（反射型）"</li> <li>6: "跨站点脚本（存储型）"</li> <li>7: "跨站点脚本（DOM型）"</li> <li>8: "加密问题"</li> <li>9: "拒绝服务"</li> <li>10: "违反安全设计原则"</li> <li>11: "HTTP响应CRLF注入"</li> <li>12: "敏感信息泄露"</li> <li>13: "缓冲区溢出"</li> <li>14: "越权"</li> <li>15: "代码执行"</li> <li>16: "SQL注入"</li> <li>17: "服务器端请求伪造"</li> <li>18: "点击劫持"</li> <li>19: "未验证的重定向"</li> <li>20: "XML外部实体（XXE）"</li> <li>21: "明文存储密码"</li> <li>22: "钓鱼"</li> <li>23: "恶意软件/木马"</li> <li>24: "存在后门"</li> <li>25: "业务逻辑错误"</li> <li>26: "敏感信息明文存储"</li> <li>27: "敏感信息明文传输"</li> <li>28: "中间人攻击"</li> <li>29: "目录遍历"</li> <li>30: "文件包含"</li> <li>31: "会话固定"</li> <li>32: "条件竞争漏洞"</li> <li>33: "类型混淆"</li> <li>34: "命令执行"</li> <li>35: "安全配置错误"</li> <li>36: "不安全的反序列化"</li> <li>37: "使用含有已知漏洞的组件"</li> <li>38: "LDAP注入"</li> <li>39: "不足的日志记录和监控"</li> <li>40: "弱口令"</li> <li>41: "文件上传漏洞"</li> </ul> |

| 名称          | 类型      | 是否必选 | 示例值 | 描述                  |
|-------------|---------|------|-----|---------------------|
| CurrentPage | Integer | 否    | 1   | 分页查询时，显示的当前页的页码。    |
| PageSize    | Integer | 否    | 20  | 分页查询时，显示的每页数据的最大条数。 |

## 返回数据

| 名称                   | 类型      | 示例值                      | 描述                                   |
|----------------------|---------|--------------------------|--------------------------------------|
| Count                | Integer | 10                       | 分页查询时，显示的当前页的数据条数。                   |
| CurrentPage          | Integer | 1                        | 分页查询时，显示的当前页的页码。                     |
| List                 | Array   |                          | 漏洞结果信息。                              |
| Hostname             | String  | ***.***.net              | 漏洞对应的资产名称。                           |
| Id                   | Long    | 1833085                  | 漏洞ID。                                |
| LastDiscoveredAt     | Long    | 1531191806000            | 漏洞最后被发现的时间。                          |
| Name                 | String  | Microsoft IIS 版本泄露       | 漏洞名称。                                |
| Severity             | Integer | 0                        | 漏洞的威胁程度。                             |
| Status               | Integer | 0                        | 漏洞的处理状态。                             |
| Target               | String  | http://***.testfire.net/ | 漏洞影响的资产信息。                           |
| TaskId               | Long    | 1232134                  | 漏洞扫描的子任务ID。                          |
| VulnerabilityTypeDes | String  | 失效的身份认证                  | 漏洞类型。例如：失效的身份认证、失效的访问控制、SQL注入、命令注入等。 |
| PageCount            | Integer | 2                        | 分页查询时，显示数据的总页数。                      |

| 名称         | 类型      | 示例值                                  | 描述                  |
|------------|---------|--------------------------------------|---------------------|
| PageSize   | Integer | 20                                   | 分页查询时，显示的每页数据的最大条数。 |
| RequestId  | String  | DFF34FB0-12D9-4B8B-9DD4-1BD89A33950F | 结果的请求ID。            |
| TotalCount | Integer | 22                                   | 漏洞总数量。              |

示例

请求示例

```
/?Action=DescribeAllVulnerabilities
&BeginTime=11111111
&Category=core
&CurrentPage=1
&EndTime=11111111
&Lang=zh
&Module=relation_domain
&Name=test
&PageSize=20
&ScanId=2018042307022680333
&Search=***.testfire.net
&Severity=0
&SourceIp=1.2.3.4
&Status=0
&TaskId=11111111
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeAllVulnerabilitiesResponse>
  <requestId>DFF34FB0-12D9-4B8B-9DD4-1BD89A33950F</requestId>
  <data>
    <PageCount>3</PageCount>
    <Count>10</Count>
    <TotalCount>22</TotalCount>
    <PageSize>10</PageSize>
    <CurrentPage>1</CurrentPage>
    <List>
      <Name>Microsoft IIS 版本泄露</Name>
      <Status>3</Status>
      <Severity>0</Severity>
      <Target>http://***.testfire.net</Target>
      <Id>1833085</Id>
      <LastDiscoveredAt>1531191806000</LastDiscoveredAt>
      <Hostname>***.testfire.net</Hostname>
      <TaskId>11220</TaskId>
```

```
<VulnerabilityTypeDes>失效的身份认证</VulnerabilityTypeDes>
</List>
<List>
  <Name>Microsoft IIS 版本泄露</Name>
  <Status>0</Status>
  <Severity>0</Severity>
  <Target>https://***.testfire.net/</Target>
  <Id>1833086</Id>
  <LastDiscoveredAt>1531191806000</LastDiscoveredAt>
  <Hostname>***.testfire.net</Hostname>
  <TaskId>11221</TaskId>
  <VulnerabilityTypeDes>失效的访问控制</VulnerabilityTypeDes>
</List>
<List>
  <Name>服务器允许OPTIONS方法</Name>
  <Status>0</Status>
  <Severity>1</Severity>
  <Target>http://***.testfire.net:80</Target>
  <Id>1833088</Id>
  <LastDiscoveredAt>1531191612000</LastDiscoveredAt>
  <Hostname>***.testfire.net</Hostname>
  <TaskId>11222</TaskId>
  <VulnerabilityTypeDes>失效的身份认证</VulnerabilityTypeDes>
</List>
<List>
  <Name>ASP.NET DEBUG 模式开启</Name>
  <Status>0</Status>
  <Severity>1</Severity>
  <Target>http://***.testfire.net</Target>
  <Id>1833090</Id>
  <LastDiscoveredAt>1531191612000</LastDiscoveredAt>
  <Hostname>***.testfire.net</Hostname>
  <TaskId>11223</TaskId>
  <VulnerabilityTypeDes>SQL注入</VulnerabilityTypeDes>
</List>
<List>
  <Name>ASP.NET DEBUG 模式开启</Name>
  <Status>0</Status>
  <Severity>1</Severity>
  <Target>https://***.testfire.net</Target>
  <Id>1833091</Id>
  <LastDiscoveredAt>1531191612000</LastDiscoveredAt>
  <Hostname>***.testfire.net</Hostname>
  <TaskId>11224</TaskId>
  <VulnerabilityTypeDes>命令注入</VulnerabilityTypeDes>
</List>
<List>
  <Name>服务器允许OPTIONS方法</Name>
  <Status>0</Status>
  <Severity>1</Severity>
  <Target>https://***.testfire.net:443</Target>
  <Id>1833094</Id>
  <LastDiscoveredAt>1531191612000</LastDiscoveredAt>
  <Hostname>***.testfire.net</Hostname>
```

```
<TaskId>11225</TaskId>
<VulnerabilityTypeDes>失效的身份认证</VulnerabilityTypeDes>
</List>
<List>
  <Name>WEB 敏感目录探测</Name>
  <Status>3</Status>
  <Severity>1</Severity>
  <Target>http://***.testfire.net:8080/docs</Target>
  <Id>1833096</Id>
  <LastDiscoveredAt>1531191612000</LastDiscoveredAt>
  <Hostname>***.testfire.net</Hostname>
  <TaskId>11226</TaskId>
  <VulnerabilityTypeDes>失效的访问控制</VulnerabilityTypeDes>
</List>
<List>
  <Name>服务器允许OPTIONS方法</Name>
  <Status>0</Status>
  <Severity>1</Severity>
  <Target>http://***.testfire.net:80</Target>
  <Id>1833073</Id>
  <LastDiscoveredAt>1531190450000</LastDiscoveredAt>
  <Hostname>***.testfire.net</Hostname>
  <TaskId>11227</TaskId>
  <VulnerabilityTypeDes>SQL注入</VulnerabilityTypeDes>
</List>
<List>
  <Name>ASP.NET DEBUG 模式开启</Name>
  <Status>0</Status>
  <Severity>1</Severity>
  <Target>http://***.testfire.net</Target>
  <Id>1833074</Id>
  <LastDiscoveredAt>1531190450000</LastDiscoveredAt>
  <Hostname>***.testfire.net</Hostname>
  <TaskId>11228</TaskId>
  <VulnerabilityTypeDes>失效的访问控制</VulnerabilityTypeDes>
</List>
<List>
  <Name>服务器允许OPTIONS方法</Name>
  <Status>0</Status>
  <Severity>1</Severity>
  <Target>https://***.testfire.net:443</Target>
  <Id>1833078</Id>
  <LastDiscoveredAt>1531190450000</LastDiscoveredAt>
  <Hostname>***.testfire.net</Hostname>
  <TaskId>11229</TaskId>
  <VulnerabilityTypeDes>代码执行</VulnerabilityTypeDes>
</List>
</data>
<code>200</code>
<success>true</success>
</DescribeAllVulnerabilitiesResponse>
```

JSON 格式

```
{
  "requestId": "DFF34FB0-12D9-4B8B-9DD4-1BD89A33950F",
  "data": {
    "PageCount": 3,
    "Count": 10,
    "TotalCount": 22,
    "PageSize": 10,
    "CurrentPage": 1,
    "List": [
      {
        "Name": "Microsoft IIS 版本泄露",
        "Status": 3,
        "Severity": 0,
        "Target": "http://***.testfire.net/",
        "Id": 1833085,
        "LastDiscoveredAt": 1531191806000,
        "Hostname": "***.testfire.net",
        "TaskId": 11220,
        "VulnerabilityTypeDes": "失效的身份认证"
      },
      {
        "Name": "Microsoft IIS 版本泄露",
        "Status": 0,
        "Severity": 0,
        "Target": "https://***.testfire.net/",
        "Id": 1833086,
        "LastDiscoveredAt": 1531191806000,
        "Hostname": "***.testfire.net",
        "TaskId": 11221,
        "VulnerabilityTypeDes": "失效的访问控制"
      },
      {
        "Name": "服务器允许OPTIONS方法",
        "Status": 0,
        "Severity": 1,
        "Target": "http://***.testfire.net:80",
        "Id": 1833088,
        "LastDiscoveredAt": 1531191612000,
        "Hostname": "***.testfire.net",
        "TaskId": 11222,
        "VulnerabilityTypeDes": "失效的身份认证"
      },
      {
        "Name": "ASP.NET DEBUG 模式开启",
        "Status": 0,
        "Severity": 1,
        "Target": "http://***.testfire.net",
        "Id": 1833090,
        "LastDiscoveredAt": 1531191612000,
        "Hostname": "***.testfire.net",
        "TaskId": 11223,
        "VulnerabilityTypeDes": "SQL注入"
      },
      {

```

```
"Name": "ASP.NET DEBUG 模式开启",
"Status": 0,
"Severity": 1,
"Target": "https://***.testfire.net",
"Id": 1833091,
"LastDiscoveredAt": 1531191612000,
"Hostname": "***.testfire.net",
"TaskId": 11224,
"VulnerabilityTypeDes": "命令注入"
},
{
  "Name": "服务器允许OPTIONS方法",
  "Status": 0,
  "Severity": 1,
  "Target": "https://***.testfire.net:443",
  "Id": 1833094,
  "LastDiscoveredAt": 1531191612000,
  "Hostname": "***.testfire.net",
  "TaskId": 11225,
  "VulnerabilityTypeDes": "失效的身份认证"
},
{
  "Name": "WEB 敏感目录探测",
  "Status": 3,
  "Severity": 1,
  "Target": "http://***.testfire.net:8080/docs/",
  "Id": 1833096,
  "LastDiscoveredAt": 1531191612000,
  "Hostname": "***.testfire.net",
  "TaskId": 11226,
  "VulnerabilityTypeDes": "失效的访问控制"
},
{
  "Name": "服务器允许OPTIONS方法",
  "Status": 0,
  "Severity": 1,
  "Target": "http://***.testfire.net:80",
  "Id": 1833073,
  "LastDiscoveredAt": 1531190450000,
  "Hostname": "***.testfire.net",
  "TaskId": 11227,
  "VulnerabilityTypeDes": "SQL注入"
},
{
  "Name": "ASP.NET DEBUG 模式开启",
  "Status": 0,
  "Severity": 1,
  "Target": "http://***.testfire.net",
  "Id": 1833074,
  "LastDiscoveredAt": 1531190450000,
  "Hostname": "***.testfire.net",
  "TaskId": 11228,
  "VulnerabilityTypeDes": "失效的访问控制"
},
}
```

```
{
  "Name": "服务器允许OPTIONS方法",
  "Status": 0,
  "Severity": 1,
  "Target": "https://***.testfire.net:443",
  "Id": 1833078,
  "LastDiscoveredAt": 1531190450000,
  "Hostname": "***.testfire.net",
  "TaskId": 11229,
  "VulnerabilityTypeDes": "代码执行"
}
],
"code": 200,
"success": true
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 5.3. DescribeScans

调用DescribeScans获取扫描任务列表。

 **说明** 调用该接口可以分页查询所有扫描任务列表，查看扫描进度等信息。

## 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

## 请求参数

| 名称       | 类型     | 是否必选 | 示例值           | 描述                                                                                    |
|----------|--------|------|---------------|---------------------------------------------------------------------------------------|
| Action   | String | 是    | DescribeScans | 要执行的操作。取值： <b>DescribeScans</b> 。                                                     |
| SourceIp | String | 否    | 1.2.3.4       | 指定访问者源IP地址。                                                                           |
| Lang     | String | 否    | zh            | 指定返回任务列表的语言环境。取值： <ul style="list-style-type: none"><li>zh：中文</li><li>en：英文</li></ul> |

| 名称           | 类型         | 是否必选 | 示例值                 | 描述                                                                                                                                                                                                                                       |
|--------------|------------|------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| StatusList.N | RepeatList | 否    | ["finished"]        | 指定待查询任务的扫描状态。取值： <ul style="list-style-type: none"><li>• <b>waiting</b>：等待中</li><li>• <b>finished</b>：已完成</li><li>• <b>running</b>：运行中</li><li>• <b>aborted</b>：已中止</li><li>• <b>invalid</b>：已无效</li><li>• <b>disabled</b>：已失败</li></ul> |
| TriggerType  | String     | 否    | date                | 指定待查询扫描任务的触发类型。取值： <ul style="list-style-type: none"><li>• <b>date</b>：单次任务</li><li>• <b>interval</b>：周期任务</li></ul>                                                                                                                     |
| ScanId       | String     | 否    | 2019031816494923023 | 指定待查询扫描任务的ID。                                                                                                                                                                                                                            |
| Search       | String     | 否    | ***.***.net         | 指定待查询扫描任务的搜索条件（任务名称、IP、域名）。                                                                                                                                                                                                              |
| ScanType     | String     | 否    | vuln                | 指定待查询扫描任务的扫描类型。取值： <ul style="list-style-type: none"><li>• <b>vuln</b>：漏洞类型</li><li>• <b>content</b>：内容风险</li></ul>                                                                                                                      |
| CurrentPage  | Integer    | 否    | 1                   | 指定待查询的扫描任务列表当前页码。                                                                                                                                                                                                                        |
| PageSize     | Integer    | 否    | 20                  | 指定待查询的扫描任务列表每页显示数据条数。                                                                                                                                                                                                                    |

返回数据

| 名称          | 类型      | 示例值 | 描述             |
|-------------|---------|-----|----------------|
| Count       | Integer | 3   | 返回任务列表的扫描任务数量。 |
| CurrentPage | Integer | 1   | 返回任务列表的当前页码。   |
| List        | Array   |     | 扫描任务列表。        |

| 名称                    | 类型      | 示例值                                  | 描述                                                                                                                                                                                       |
|-----------------------|---------|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CronActive            | String  | 1                                    | 任务的调度状态。取值： <ul style="list-style-type: none"> <li><b>1</b>：活跃，表示任务可调度。</li> <li><b>0</b>：无效，表示任务不可调度。</li> </ul>                                                                        |
| EndDate               | Long    | 212212000000                         | 返回任务列表中的任务扫描结束时间。                                                                                                                                                                        |
| FlowName              | String  | skynet_vul_scan                      | 返回任务列表中任务的漏洞扫描模式。取值： <ul style="list-style-type: none"> <li><b>assets</b>：资产模式</li> <li><b>general</b>：标准模式</li> <li><b>skynet_vul_scan</b>：深度模式</li> </ul>                              |
| IndexIntervalInMinute | Integer | 5                                    | 返回任务列表中的任务首页检测间隔时间。                                                                                                                                                                      |
| Interval              | Integer | 10                                   | 返回任务列表中扫描任务的扫描间隔。                                                                                                                                                                        |
| JobStatistics         | String  | running                              | 任务实例的统计情况。取值： <ul style="list-style-type: none"> <li><b>1</b>：running，表示扫描任务运行中。</li> <li><b>2</b>：finished，表示扫描任务已完成。</li> <li><b>3</b>：aborted，表示扫描任务已停止。</li> </ul>                   |
| KeyWords              | List    | 65084125-edc6-4ef3-931f-c3e87945631e | 附加词库的ID。                                                                                                                                                                                 |
| LastScheduleDate      | Long    | 1111000000                           | 上次调度任务的时间戳。                                                                                                                                                                              |
| Name                  | String  | test_0710-3                          | 返回任务列表中的任务名称。                                                                                                                                                                            |
| NextRunDate           | Long    | 1212100000                           | 返回任务列表中显示的各任务下次扫描预计开始时间。                                                                                                                                                                 |
| Period                | String  | minute                               | 返回任务列表中各任务的扫描周期。取值： <ul style="list-style-type: none"> <li><b>minute</b>：每分钟</li> <li><b>hour</b>：每小时</li> <li><b>day</b>：每天</li> <li><b>week</b>：每周</li> <li><b>month</b>：每月</li> </ul> |

| 名称                | 类型      | 示例值                                  | 描述                                                                                                                                                                                    |
|-------------------|---------|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RefJobId          | String  | 65084125-edc6-4ef3-931f-c3e87945631e | 返回任务列表中各任务所关联扫描任务的ID。                                                                                                                                                                 |
| ReportUrl         | String  | http://***.com                       | 返回任务列表中各扫描任务生成的任务报告链接。                                                                                                                                                                |
| RunPercent        | Float   | 100.0                                | 返回任务列表中显示的运行中扫描任务的扫描进度百分比。                                                                                                                                                            |
| RuntimeEnd        | String  | 1545972690000                        | 返回任务列表中扫描任务的扫描开始时间。                                                                                                                                                                   |
| RuntimeStart      | String  | 1545972690000                        | 返回任务列表中扫描任务的扫描结束时间。                                                                                                                                                                   |
| ScanAll           | Integer | 1                                    | 返回任务列表中显示是否扫描了全部资产。取值： <ul style="list-style-type: none"><li>0：未扫描全部资产。</li><li>1：扫描了全部资产。</li></ul>                                                                                  |
| ScanId            | String  | 2018071010171127450                  | 返回任务列表中对应扫描任务的ID。                                                                                                                                                                     |
| ScanType          | String  | vuln                                 | 任务列表中显示的任务扫描类型。取值： <ul style="list-style-type: none"><li>vuln：漏洞类型</li><li>content：内容风险</li></ul>                                                                                     |
| SiteIntervalInDay | Integer | 1                                    | 任务列表中显示的对应该任务在全站检测的间隔（天）时间。                                                                                                                                                           |
| StartDate         | Long    | 111122200000                         | 返回任务列表中各任务的开始时间。                                                                                                                                                                      |
| Status            | String  | running                              | 返回任务列表中各任务的扫描状态。取值： <ul style="list-style-type: none"><li>waiting：等待中</li><li>finished：已完成</li><li>running：运行中</li><li>aborted：已暂停</li><li>invalid：已无效</li><li>disabled：已禁用</li></ul> |

| 名称              | 类型      | 示例值                                  | 描述                                                                                                                   |
|-----------------|---------|--------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Targets         | List    | ["demo.testfire.net"]                | 返回任务列表中的扫描目标（IP/域名/子域名）名称。                                                                                           |
| TargetsOriginal | List    | testtag                              | 创建扫描任务时，扫描目标的原始内容，即扫描资产的分组标签。                                                                                        |
| TriggerType     | String  | date                                 | 返回任务列表中的各任务触发类型。取值： <ul style="list-style-type: none"> <li><b>date</b>：单次任务</li> <li><b>interval</b>：周期任务</li> </ul> |
| URLs            | List    | aliyun.com                           | 扫描的域名资产的URL。                                                                                                         |
| PageCount       | Integer | 1                                    | 返回任务列表的页数。                                                                                                           |
| PageSize        | Integer | 20                                   | 返回任务列表每页显示数据的条数。                                                                                                     |
| RequestId       | String  | B92696EA-44DE-4DE4-B3B7-07655394DC7C | 返回结果的请求ID。                                                                                                           |
| TotalCount      | Integer | 4                                    | 返回任务列表的总任务条数。                                                                                                        |

## 示例

### 请求示例

```
http(s)://[Endpoint]/?Action=DescribeScans
&<公共请求参数>
```

### 正常返回示例

#### XML 格式

```
<?xml version="1.0" encoding="UTF-8" ?>
<DescribeScansResponse>
  <requestId>B92696EA-44DE-4DE4-B3B7-07655394DC7C</requestId>
  <data>
    <PageCount>1</PageCount>
    <Count>3</Count>
    <TotalCount>3</TotalCount>
    <PageSize>20</PageSize>
    <CurrentPage>1</CurrentPage>
    <List>
      <Name>test_0710-3</Name>
      <RefJobId>65084125-edc6-4ef3-931f-c3e87945631e</RefJobId>
```

```
<Status>finished</Status>
<ScanType>vuln</ScanType>
<EndDate>1531191010000</EndDate>
<RunPercent>100</RunPercent>
<StartDate>1531190450000</StartDate>
<ReportUrl>http://***.com/VUL_REPORT/d3ba039d-24cf-46e3-8ffb-ee56d8de40b0?Expires=1533555431&
mp;OSSAccessKeyId=<yourAccessKeyId>&Signature=CmFMLzRIFOqETWWqj01mYpkKZI****</ReportUr
l>
  <FlowName>skynet</FlowName>
  <TriggerType>date</TriggerType>
  <Targets>***.***.net</Targets>
  <ScanAll>0</ScanAll>
  <ScanId>2018071010384940572</ScanId>
</List>
<List>
  <Name>test_0710-2</Name>
  <RefJobId>5c2d86bf-ace4-4c62-86e0-63f0b1e1413b</RefJobId>
  <Status>finished</Status>
  <ScanType>vuln</ScanType>
  <EndDate>1531189680000</EndDate>
  <RunPercent>100</RunPercent>
  <StartDate>1531189151000</StartDate>
  <ReportUrl>http://***.com/VUL_REPORT/29e66729-d571-489d-bc23-9d4cacf9e283?Expires=1533555431&a
mp;OSSAccessKeyId=<yourAccessKeyId>&Signature=x0BVqK%2B4BpKfZkGzYSaKJAWFLB****</Report
Url>
  <FlowName>skynet</FlowName>
  <TriggerType>date</TriggerType>
  <Targets>***.***.net</Targets>
  <ScanAll>0</ScanAll>
  <ScanId>2018071010171127450</ScanId>
</List>
<List>
  <Name>test_0709-7</Name>
  <RefJobId>6e504749-3ddc-47b5-a1e8-4e772a784122</RefJobId>
  <Status>finished</Status>
  <ScanType>vuln</ScanType>
  <EndDate>1531139501000</EndDate>
  <RunPercent>100</RunPercent>
  <StartDate>1531138568000</StartDate>
  <ReportUrl>http://***.com/VUL_REPORT/1a4415a0-ac30-4240-b6ae-7fe137152bdb?Expires=1533555431&a
mp;OSSAccessKeyId=<yourAccessKeyId>&Signature=WJ%2B5TWNQJ6CRshuGvFPPnvBifZ****</Report
Url>
  <FlowName>skynet</FlowName>
  <TriggerType>date</TriggerType>
  <Targets>***.***.net</Targets>
  <ScanAll>0</ScanAll>
  <ScanId>2018070920140740337</ScanId>
</List>
</data>
<code>200</code>
<success>true</success>
</DescribeScansResponse>
```

## JSON 格式

```
{
  "requestId": "B92696EA-44DE-4DE4-B3B7-07655394DC7C",
  "data": {
    "PageCount": 1,
    "Count": 3,
    "TotalCount": 3,
    "PageSize": 20,
    "CurrentPage": 1,
    "List": [
      {
        "Name": "test_0710-3",
        "RefJobId": "65084125-edc6-4ef3-931f-c3e87945631e",
        "Status": "finished",
        "ScanType": "vuln",
        "EndDate": 1531191010000,
        "RunPercent": 100,
        "StartDate": 1531190450000,
        "ReportUrl": "http://***.com/VUL_REPORT/d3ba039d-24cf-46e3-8ffb-ee56d8de40b0?Expires=1533555431&OSSAccessKeyId=<yourAccessKeyId>&Signature=CmFMLzRIFOqETWWqj01mYpkKZI****",
        "FlowName": "skynet",
        "TriggerType": "date",
        "Targets": [
          "****.***.net"
        ],
        "ScanAll": 0,
        "ScanId": "2018071010384940572"
      },
      {
        "Name": "test_0710-2",
        "RefJobId": "5c2d86bf-ace4-4c62-86e0-63f0b1e1413b",
        "Status": "finished",
        "ScanType": "vuln",
        "EndDate": 1531189680000,
        "RunPercent": 100,
        "StartDate": 1531189151000,
        "ReportUrl": "http://***.com/VUL_REPORT/29e66729-d571-489d-bc23-9d4cac9e283?Expires=1533555431&OSSAccessKeyId=<yourAccessKeyId>&Signature=x0BVqK%2B4BpKfZkGzYSaKJAWFLB****",
        "FlowName": "skynet",
        "TriggerType": "date",
        "Targets": [
          "****.***.net"
        ],
        "ScanAll": 0,
        "ScanId": "2018071010171127450"
      },
      {
        "Name": "test_0709-7",
        "RefJobId": "6e504749-3ddc-47b5-a1e8-4e772a784122",
        "Status": "finished",
        "ScanType": "vuln",
        "EndDate": 1531139501000,
        "RunPercent": 100,
```

```
{
  "StartDate": 1531138568000,
  "ReportUrl": "http://***.com/VUL_REPORT/1a4415a0-ac30-4240-b6ae-7fe137152bdb?Expires=1533555431&OSSAccessKeyId=<yourAccessKeyId>&Signature=WJ%2B5TWNQJ6CRshuGvFPPnvBifZ****",
  "FlowName": "skynet",
  "TriggerType": "date",
  "Targets": [
    "****.***.net"
  ],
  "ScanAll": 0,
  "ScanId": "2018070920140740337"
}
},
"code": 200,
"success": true
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 5.4. DescribeScanSessions

调用DescribeScanSessions获取扫描任务实例列表。

 **说明** 调用该接口可以分页查询扫描任务调度产生的任务实例列表信息。

## 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

## 请求参数

| 名称          | 类型      | 是否必选 | 示例值                                  | 描述                                       |
|-------------|---------|------|--------------------------------------|------------------------------------------|
| Action      | String  | 是    | DescribeScanSessions                 | 要执行的操作。取值： <b>DescribeScanSessions</b> 。 |
| SourceIp    | String  | 否    | 1.2.3.4                              | 指定访问源IP地址。                               |
| ScanId      | String  | 否    | 66c07fa5-542b-47df-8501-e0401dc42d3e | 指定查询特定扫描任务ID的实例列表。                       |
| CurrentPage | Integer | 否    | 3                                    | 指定返回结果的当前页码。                             |
| PageSize    | Integer | 否    | 20                                   | 指定返回结果的每页显示数据条数。                         |

| 名称           | 类型         | 是否必选 | 示例值     | 描述                                                                                                                                                                            |
|--------------|------------|------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Search       | String     | 否    | 1.2.*.* | 指定待查询实例的任务搜索字段。                                                                                                                                                               |
| StatusList.N | RepeatList | 否    | waiting | 指定待查询实例中子任务状态。取值： <ul style="list-style-type: none"><li>• <b>waiting</b>：等待中</li><li>• <b>finished</b>：已完成</li><li>• <b>running</b>：运行中</li><li>• <b>aborted</b>：暂停</li></ul> |

## 返回数据

| 名称          | 类型      | 示例值           | 描述                                                                                                                                                                            |
|-------------|---------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Count       | Integer | 20            | 指定当前页显示数据条数。                                                                                                                                                                  |
| CurrentPage | Integer | 5             | 指定返回结果的当前页码。                                                                                                                                                                  |
| List        | Array   |               | 返回的任务实例列表。                                                                                                                                                                    |
| CreatedAt   | Long    | 1565690460000 | 扫描创建时间。                                                                                                                                                                       |
| FinishedAt  | Long    | 1565690260000 | 扫描结束时间。                                                                                                                                                                       |
| Interval    | Integer | 1             | 返回结果中任务的扫描间隔时间。                                                                                                                                                               |
| JobStatus   | String  | waiting       | 返回结果中子任务扫描状态。取值： <ul style="list-style-type: none"><li>• <b>waiting</b>：等待中</li><li>• <b>finished</b>：已完成</li><li>• <b>running</b>：运行中</li><li>• <b>aborted</b>：已暂停</li></ul> |
| Name        | String  | test          | 返回结果中任务名称。                                                                                                                                                                    |

| 名称           | 类型      | 示例值                                  | 描述                                                                                                                                                                                         |
|--------------|---------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Period       | String  | hour                                 | 返回结果中各任务的扫描周期。取值： <ul style="list-style-type: none"><li>• <b>minute</b>：每分钟</li><li>• <b>hour</b>：每小时</li><li>• <b>day</b>：每天</li><li>• <b>week</b>：每周</li><li>• <b>month</b>：每月</li></ul> |
| ReportStatus | String  | running                              | 返回结果中各任务实例生成报表状态。取值： <ul style="list-style-type: none"><li>• <b>failed</b>：生成失败</li><li>• <b>finished</b>：生成完成</li><li>• <b>running</b>：生成中</li><li>• <b>inexistent</b>：不存在</li></ul>      |
| ReportUrl    | String  | http://***.com                       | 返回结果中各任务实例生成的报告链接。                                                                                                                                                                         |
| RunPercent   | Float   | 10.21                                | 返回结果中各任务实例的扫描进度。                                                                                                                                                                           |
| ScanId       | String  | c0065a11-fe41-44f4-a5d2-b921316ddb52 | 返回结果中各扫描任务的子任务ID。                                                                                                                                                                          |
| Targets      | List    | ["1.2.3.5"]                          | 返回结果中各任务实例下扫描目标（IP/域名/子域名）。                                                                                                                                                                |
| TaskId       | Long    | 1236984                              | 返回结果中各任务实例的ID。                                                                                                                                                                             |
| TriggerType  | String  | date                                 | 返回结果中各扫描任务下子任务的任务触发类型。取值： <ul style="list-style-type: none"><li>• <b>date</b>：单次任务</li><li>• <b>interval</b>：周期任务</li></ul>                                                                |
| PageCount    | Integer | 20                                   | 返回任务实例列表总页数。                                                                                                                                                                               |
| PageSize     | Integer | 20                                   | 返回任务实例列表中每页显示数据总条数。                                                                                                                                                                        |
| RequestId    | String  | F8955687-DDFC-4FE1-BC67-5C613657B8E5 | 返回结果的请求ID。                                                                                                                                                                                 |

| 名称         | 类型      | 示例值 | 描述              |
|------------|---------|-----|-----------------|
| TotalCount | Integer | 30  | 返回任务实例列表的实例总数量。 |

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeScanSessions
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeScanSessionsResponse>
  <code>200</code>
  <requestId>F8955687-DDFC-4FE1-BC67-5C613657B8E5</requestId>
  <success>true</success>
  <data>
    <List>
      <TaskId>11</TaskId>
      <ScanId>11111</ScanId>
      <JobStatus>waiting</JobStatus>
      <CreatedAt>111212121</CreatedAt>
      <FinishedAt>12121</FinishedAt>
      <name>test</name>
      <targets>1.2.3.5</targets>
      <triggerType>date</triggerType>
      <period>hour</period>
      <interval>1</interval>
      <reportStatus>running</reportStatus>
      <reportUrl>http://***.com</reportUrl>
    </List>
    <PageNumber>1</PageNumber>
    <PageSize>20</PageSize>
    <TotalCount>100</TotalCount>
  </data>
</DescribeScanSessionsResponse>
```

JSON 格式

```
{
  "code": "200",
  "requestId": "F8955687-DDFC-4FE1-BC67-5C613657B8E5",
  "success": true,
  "data": {
    "List": [
      {
        "TaskId": 11,
        "ScanId": 11111,
        "JobStatus": "waiting",
        "CreatedAt": 111212121,
        "FinishedAt": 12121,
        "name": "test",
        "targets": ["1.2.3.5"],
        "triggerType": "date",
        "period": "hour",
        "interval": 1,
        "reportStatus": "running",
        "reportUrl": "http://***.com"
      }
    ],
    "PageNumber": 1,
    "PageSize": 20,
    "TotalCount": 100
  }
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 5.5. DescribeVulnerability

调用DescribeVulnerability查询单个漏洞详情，包括漏洞描述、分类、漏洞证明、造成影响、解决建议等。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称     | 类型     | 是否必选 | 示例值                   | 描述                                        |
|--------|--------|------|-----------------------|-------------------------------------------|
| Action | String | 是    | DescribeVulnerability | 要执行的操作。取值： <b>DescribeVulnerability</b> 。 |

| 名称       | 类型     | 是否必选 | 示例值      | 描述                                                                                   |
|----------|--------|------|----------|--------------------------------------------------------------------------------------|
| Id       | Long   | 是    | 11507253 | 漏洞ID。<br><div>❓ 说明 查询单个漏洞的详情，需要提供该漏洞的ID，该ID可调用DescribeAllVulnerabilities接口获取。</div>  |
| SourceIp | String | 否    | 1.2.3.4  | 访问者源IP地址。                                                                            |
| Lang     | String | 否    | zh       | 请求和接收消息的语言类型。取值： <ul style="list-style-type: none"><li>zh：中文</li><li>en：英文</li></ul> |

返回数据

| 名称   | 类型     | 示例值                                                          | 描述         |
|------|--------|--------------------------------------------------------------|------------|
| Args | String | {\"host\":<br>\"1.2.3.4\",<br>\"port\": 2181,<br>\"qps\": 1} | 漏洞扫描插件返回值。 |

| 名称          | 类型     | 示例值                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 描述             |
|-------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| Data        | String | <pre>{\"host\":<br/>  \"120.0.0.0\",<br/>  \"port\": 2181,<br/>  \"proof\":<br/>    \"Environment:\\\\nz<br/>ookeeper.version=3.<br/>4.12-<br/>e5259e437540f3496<br/>46870ea94dc2658c4<br/>e44b3b, built on<br/>03/27/2018 03:55<br/>GMT\\\\nhost.name=i<br/>Zbp1fqhknu8ntff13<br/>g4m8Z\\\\njava.versi<br/>on=1.8.0_181\\\\njava<br/>.vendor=Oracle<br/>Corporation\\\\njava.<br/>home=/usr/lib/jvm/j<br/>ava-1.8.0-openjdk-<br/>1.8.0.181-<br/>3.b13.el7_5.x86_64/j<br/>re\\\\njava.class.path<br/>=/home/duwenwen<br/>/tools/zookeeper/b<br/>in/../../build/classes:/<br/>home/duwenwen/t<br/>ools/zookeeper/bin<br/>/../../build/lib/*.jar:/h<br/>ome/duwenwen/to<br/>ols/zookeeper/bin/.<br/>/lib/slf4j-log4j12-<br/>1.7.25.jar:/home/du<br/>wenwen/tools/zoo<br/>keeper/bin/../../\"}</pre> | 漏洞扫描插件返回值描述信息。 |
| Description | String | <p>ZooKeeper 是一个开放源码的分布式应用程序协调服务，提供的功能包括：配置维护、名字服务、分布式同步、组服务等。Zookeeper默认是未授权就可以访问，\\r\\n特别对于公网开放的 Zookeeper 来说，这也导致了信息泄露的存在，具有潜在高风险。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 风险详情描述。        |
| Hostname    | String | 1.2.3.4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 漏洞影响资产名称。      |

| 名称               | 类型     | 示例值                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 描述              |
|------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Id               | Long   | 11507253                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 漏洞ID号。          |
| Impact           | String | 对集群服务造成信息泄露或拒绝服务威胁。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 漏洞详情中影响信息。      |
| LastDiscoveredAt | Long   | 15678900000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 漏洞被发现的时间。       |
| Name             | String | ZooKeeper 未授权访问                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 漏洞的名称。          |
| Poc              | String | <pre> \r\n漏洞地址: 1.2.3.4 端口: 2181\r\n返回内容:\r\n&lt;pre&gt;Environment:\nzookeeper.version=3.4.12-e5259e437540f349646870ea94dc2658c4e44b3b, built on 03/27/2018 03:55 GMT\r\nhost.name=iZbp1fqhknu8ntff13g4m8Z\r\njava.version=1.8.0_181\r\njava.vendor=Oracle Corporation\r\njava.home=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.181-3.b13.el7_5.x86_64/jre\r\njava.class.path=/home/duwenwen/tools/zookeeper/bin/../build/classes:/home/duwenwen/tools/zookeeper/bin/../build/lib/*.jar:/home/duwenwen/tools/zookeeper/bin/../lib/slf4j-log4j12-1.7.25.jar:/home/duwenwen/tools/zookeeper/bin/..&lt;/pre&gt;\r\n </pre> | 漏洞详情中漏洞证明信息。    |
| Reference        | String | http://***.com                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 漏洞详情中的相关技术参考信息。 |

| 名称            | 类型      | 示例值                                                               | 描述                                                                                                          |
|---------------|---------|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| RequestId     | String  | 6AAFCBCE-3494-4BF4-AA20-CD4BE491D22B                              | 结果的请求ID。                                                                                                    |
| Severity      | Integer | 1                                                                 | 漏洞详情中描述的漏洞所属危险等级。                                                                                           |
| Solution      | String  | 1、禁止把Zookeeper直接暴露在公网<br>\r\n2、添加访问控制，根据情况选择对应方式（认证用户，用户名密码，指定IP） | 漏洞详情中解决修复建议。                                                                                                |
| Success       | Boolean | true                                                              | 结果请求是否成功。取值： <ul style="list-style-type: none"><li>• <b>true</b>：请求成功</li><li>• <b>false</b>：请求失败</li></ul> |
| Target        | String  | 1.2.3.4                                                           | 资产目标。                                                                                                       |
| Vulnerability | Struct  |                                                                   | 漏洞详情信息。                                                                                                     |
| Args          | String  | {}                                                                | 漏洞扫描插件返回值。                                                                                                  |
| CommonType    | String  | 失效的访问控制                                                           | 漏洞详情中的通用类别。                                                                                                 |
| Cwe           | String  | CWE-284                                                           | 漏洞详情中的Cwe类别。                                                                                                |

| 名称          | 类型     | 示例值                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 描述             |
|-------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| Data        | String | <pre>{   "host":     "1.2.3.4",   "port": 2181,   "proof":     "Environment:\\nz     ookeeper.version=3.     4.12-     e5259e437540f3496     46870ea94dc2658c4     e44b3b, built on     03/27/2018 03:55     GMT\\nhost.name=i     Zbp1fqhknu8ntff13     g4m8Z\\njava.veri     on=1.8.0_181\\njava     .vendor=Oracle     Corporation\\njava.     home=/usr/lib/jvm/j     ava-1.8.0-openjdk-     1.8.0.181-     3.b13.el7_5.x86_64/j     re\\njava.class.path     =/home/duwenwen     /tools/zookeeper/b     in/./build/classes:/     home/duwenwen/t     ools/zookeeper/bin     /./build/lib/*.jar:/h     ome/duwenwen/to     ols/zookeeper/bin/.     ./lib/slf4j-log4j12-     1.7.25.jar:/home/du     wenwen/tools/zoo     keeper/bin/./\"}</pre> | 漏洞扫描插件返回值描述信息。 |
| Description | String | <p>ZooKeeper 是一个开放源码的分布式应用程序协调服务，提供的功能包括：配置维护、名字服务、分布式同步、组服务等。Zookeeper默认是未授权就可以访问，\r\n特别对于公网开放的 Zookeeper 来说，这也导致了信息泄露的存在，具有潜在高风险。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 返回的漏洞详情描述信息。   |
| Hostname    | String | 120.0.0.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 返回的漏洞影响资产名称。   |

| 名称               | 类型     | 示例值                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 描述              |
|------------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Id               | Long   | 11507253                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 漏洞ID号。          |
| Impact           | String | 对集群服务造成信息泄露或拒绝服务威胁。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 漏洞详情中影响信息。      |
| LastDiscoveredAt | Long   | 2018092100000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 漏洞被发现的时间。       |
| Name             | String | ZooKeeper 未授权访问                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 漏洞的名称。          |
| Owasp            | String | OWASP A5 失效的访问控制                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 漏洞Owasp类别信息。    |
| Poc              | String | \r\n漏洞地址：<br>1.2.3.4 端口：<br>2181\r\n返回内容：<br>\r\n <pre>Environment: \n zookeeper.<br/>version=3.4.12-e5259e437540f349646870ea94dc2658c4e44b3b, built on 03/27/2018 03:55 GMT\n host.name=iZbp1fqhknu8ntff13g4m8Z\n java.version=1.8.0_181\n java.vendor=Oracle Corporation\n java.home=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.181-3.b13.el7_5.x86_64/jre\n java.class.path=/home/duwenwen/tools/zookeeper/bin/../build/classes:/home/duwenwen/tools/zookeeper/bin/../build/lib/*.jar:/home/duwenwen/tools/zookeeper/bin/../lib/slf4j-log4j12-1.7.25.jar:/home/duwenwen/tools/zookeeper/bin/..</pre> | 漏洞详情中漏洞证明信息。    |
| Reference        | String | http://***.com                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 漏洞详情中的相关技术参考信息。 |

| 名称       | 类型      | 示例值                                                               | 描述                |
|----------|---------|-------------------------------------------------------------------|-------------------|
| Severity | Integer | 0                                                                 | 漏洞详情中描述的漏洞所属危险等级。 |
| Solution | String  | 1、禁止把Zookeeper直接暴露在公网<br>\r\n2、添加访问控制，根据情况选择对应方式（认证用户，用户名密码，指定IP） | 漏洞详情中解决修复建议。      |
| Status   | Integer | 1                                                                 | 漏洞对应的处理状态。        |
| Target   | String  | 1.2.3.4                                                           | 漏洞的受影响目标。         |
| Wasc     | String  | WASC-2                                                            | 漏洞详情的Wasc类别信息。    |

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeVulnerability
&Id=11369052
&SourceIp=1.2.3.4
&<公共请求参数>
```

正常返回示例

XML

格式

```

<DescribeVulnerabilityResponse>
  <Vulnerability>
    <Impact>对集群服务造成信息泄露或拒绝服务威胁。</Impact>
    <Status>0</Status>
    <Args>{"host": "1.2.3.4", "port": 2181, "qps": 1}</Args>
    <Description>ZooKeeper 是一个开源码的分布式应用程序协调服务，提供的功能包括:配置维护、名字服务、分布式同步、组服务等。Zookeeper默认是未授权就可以访问，特别对于公网开放的 Zookeeper 来说，这也导致了信息泄露的存在，具有潜在高风险。</Description>
    <Poc>
      漏洞地址: 1.2.3.4 端口: 2181
      返回内容:
      <pre>Environment:
zookeeper.version=3.4.12-e5259e437540f349646870ea94dc2658c4e44b3b, built on 03/27/2018 03:55 GMT
host.name=iZbp1fqhknu8ntff13g4m8Z
java.version=1.8.0_181
java.vendor=Oracle Corporation
java.home=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.181-3.b13.el7_5.x86_64/jre
java.class.path=/home/duwenwen/tools/zookeeper/bin/../build/classes:/home/duwenwen/tools/zookeeper/bin/../build/lib/*.jar:/home/duwenwen/tools/zookeeper/bin/../lib/slf4j-log4j12-1.7.25.jar:/home/duwenwen/tools/zookeeper/bin/..</pre>
    </Poc>
    <LastDiscoveredAt>1546504134000</LastDiscoveredAt>
    <Owasp>OWASP A5 失效的访问控制</Owasp>
    <Reference></Reference>
    <Hostname>1.2.3.4</Hostname>
    <CommonType>失效的访问控制</CommonType>
    <Data>{"host": "1.2.3.4", "port": 2181, "proof": "Environment:\nzookeeper.version=3.4.12-e5259e437540f349646870ea94dc2658c4e44b3b, built on 03/27/2018 03:55 GMT\nhost.name=iZbp1fqhknu8ntff13g4m8Z\njava.version=1.8.0_181\njava.vendor=Oracle Corporation\njava.home=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.181-3.b13.el7_5.x86_64/jre\njava.class.path=/home/duwenwen/tools/zookeeper/bin/../build/classes:/home/duwenwen/tools/zookeeper/bin/../build/lib/*.jar:/home/duwenwen/tools/zookeeper/bin/../lib/slf4j-log4j12-1.7.25.jar:/home/duwenwen/tools/zookeeper/bin/.."}</Data>
    <Severity>3</Severity>
    <Name>ZooKeeper 未授权访问</Name>
    <Cwe>CWE-284</Cwe>
    <Target>1.2.3.4</Target>
    <Wasc>WASC-2</Wasc>
    <Id>11507253</Id>
    <Solution>1、禁止把Zookeeper直接暴露在公网
2、添加访问控制，根据情况选择对应方式（认证用户，用户名密码，指定IP）</Solution>
  </Vulnerability>
  <code>200</code>
  <Success>true</Success>
  <RequestId>6AAFCBCE-3494-4BF4-AA20-CD4BE491D22B</RequestId>
</DescribeVulnerabilityResponse>

```

JSON 格式

```
{
  "Vulnerability": {
    "Impact": "对集群服务造成信息泄露或拒绝服务威胁。",
    "Status": 0,
    "Args": "{\"host\": \"1.2.3.4\", \"port\": 2181, \"qps\": 1}",
    "Description": "ZooKeeper 是一个开源码的分布式应用程序协调服务，提供的功能包括:配置维护、名字服务、分布式同步、组服务等。Zookeeper默认是未授权就可以访问，\r\n特别对于公网开放的 Zookeeper 来说，这也导致了信息泄露的存在，具有潜在高风险。",
    "Poc": "\r\n漏洞地址: 1.2.3.4 端口: 2181\r\n返回内容:\r\n<pre>Environment:\n zookeeper.version=3.4.12-e5259e437540f349646870ea94dc2658c4e44b3b, built on 03/27/2018 03:55 GMT\n host.name=iZbp1fqhknu8ntff13g4m8Z\n java.version=1.8.0_181\n java.vendor=Oracle Corporation\n java.home=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.181-3.b13.el7_5.x86_64/jre\n java.class.path=/home/duwenwen/tools/zookeeper/bin/../build/classes:/home/duwenwen/tools/zookeeper/bin/../build/lib/*.jar:/home/duwenwen/tools/zookeeper/bin/../lib/slf4j-log4j12-1.7.25.jar:/home/duwenwen/tools/zookeeper/bin/./</pre>\r\n",
    "LastDiscoveredAt": 1546504134000,
    "Owasp": "OWASP A5 失效的访问控制",
    "Reference": "",
    "Hostname": "1.2.3.4",
    "CommonType": "失效的访问控制",
    "Data": "{\"host\": \"1.2.3.4\", \"port\": 2181, \"proof\": \"Environment:\n zookeeper.version=3.4.12-e5259e437540f349646870ea94dc2658c4e44b3b, built on 03/27/2018 03:55 GMT\n host.name=iZbp1fqhknu8ntff13g4m8Z\n java.version=1.8.0_181\n java.vendor=Oracle Corporation\n java.home=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.181-3.b13.el7_5.x86_64/jre\n java.class.path=/home/duwenwen/tools/zookeeper/bin/../build/classes:/home/duwenwen/tools/zookeeper/bin/../build/lib/*.jar:/home/duwenwen/tools/zookeeper/bin/../lib/slf4j-log4j12-1.7.25.jar:/home/duwenwen/tools/zookeeper/bin/./\"",
    "Severity": 3,
    "Name": "ZooKeeper 未授权访问",
    "Cwe": "CWE-284",
    "Target": "1.2.3.4",
    "Wasc": "WASC-2",
    "Id": 11507253,
    "Solution": "1、禁止把Zookeeper直接暴露在公网\r\n2、添加访问控制，根据情况选择对应方式（认证用户，用户名密码，指定IP）"
  },
  "code": 200,
  "Success": true,
  "RequestId": "6AAFCBCE-3494-4BF4-AA20-CD4BE491D22B"
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 5.6. GenerateVulReport

调用GenerateVulReport生成任务实例报表。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

### 请求参数

| 名称        | 类型         | 是否必选 | 示例值               | 描述                                                                                  |
|-----------|------------|------|-------------------|-------------------------------------------------------------------------------------|
| Action    | String     | 是    | GenerateVulReport | 要执行的操作。取值： <b>GenerateVulReport</b> 。                                               |
| TaskIds.N | RepeatList | 是    | 111               | 指定待返回报表的任务实例列表。                                                                     |
| Sourcelp  | String     | 否    | 1.2.3.4           | 指定访问源IP地址。                                                                          |
| Lang      | String     | 否    | zh                | 指定返回结果的语言环境。取值： <ul style="list-style-type: none"><li>zh：中文</li><li>en：英文</li></ul> |

返回数据

| 名称        | 类型     | 示例值                           | 描述         |
|-----------|--------|-------------------------------|------------|
| RequestId | String | 6D584A17-4DA1-4CFD-BB31-***** | 返回结果的请求ID。 |

示例

请求示例

```
http(s)://[Endpoint]/?Action=GenerateVulReport
&TaskIds.1=111
&TaskIds.2=112
&Sourcelp=
&<公共请求参数>
```

正常返回示例

XML 格式

```
<GenerateVulReportResponse>
  <code>200</code>
  <requestId>6D584A17-4DA1-4CFD-BB31-*****</requestId>
  <success>true</success>
</GenerateVulReportResponse>
```

JSON 格式

```
{
  "code": "200",
  "requestId": "6D584A17-4DA1-4CFD-BB31-*****",
  "success": true
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

# 6.攻击面

## 6.1. DescribeAttackSurfacesFacets

调用DescribeAttackSurfacesFacets查询任务实例攻击面数据统计信息。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

### 请求参数

| 名称     | 类型      | 是否必选 | 示例值                          | 描述                                               |
|--------|---------|------|------------------------------|--------------------------------------------------|
| Action | String  | 是    | DescribeAttackSurfacesFacets | 要执行的操作。取值： <b>DescribeAttackSurfacesFacets</b> 。 |
| TaskId | Integer | 是    | 12345                        | 任务ID。获取指定任务ID数据。                                 |

### 返回数据

| 名称              | 类型      | 示例值                                  | 描述         |
|-----------------|---------|--------------------------------------|------------|
| CrawlerRequests | Integer | 30                                   | 爬虫流量数量。    |
| DNSMap          | Integer | 10                                   | DNS解析记录数量。 |
| Domains         | Integer | 10                                   | 域名数量。      |
| Hosts           | Integer | 10                                   | 主机数量。      |
| Ports           | Integer | 10                                   | 端口数量。      |
| RequestId       | String  | DD73CB0A-6E99-49AB-9569-5A00C9732795 | 返回结果的请求ID。 |
| Subdomains      | Integer | 10                                   | 子域名数量。     |
| WebPaths        | Integer | 10                                   | Web路径数量。   |

| 名称         | 类型      | 示例值 | 描述        |
|------------|---------|-----|-----------|
| WebServers | Integer | 10  | Web服务器数量。 |
| WebTechs   | Integer | 10  | Web应用数量。  |

## 示例

### 请求示例

```
http(s)://[Endpoint]/?Action=DescribeAttackSurfacesFacets
&<公共请求参数>
```

### 正常返回示例

#### XML 格式

```
<DescribeAttackSurfacesFacetsResponse>
  <code>200</code>
  <requestId>DD73CB0A-6E99-49AB-9569-5A00C9732795</requestId>
  <success>true</success>
  <data>
    <Domains>10</Domains>
    <Subdomains>20</Subdomains>
    <DNSMap>20</DNSMap>
    <Hosts>40</Hosts>
    <Ports>30</Ports>
    <WebTechs>40</WebTechs>
    <WebServers>30</WebServers>
    <WebPaths>20</WebPaths>
    <CrawlerRequests>40</CrawlerRequests>
  </data>
</DescribeAttackSurfacesFacetsResponse>
```

#### JSON 格式

```
{
  "code": "200",
  "requestId": "DD73CB0A-6E99-49AB-9569-5A00C9732795",
  "success": true,
  "requestId": "DD73CB0A-6E99-49AB-9569-5A00C9732795",
  "data": {
    "Domains": 10,
    "Subdomains": 20,
    "DNSMap": 20,
    "Hosts": 40,
    "Ports": 30,
    "WebTechs": 40,
    "WebServers": 30,
    "WebPaths": 20,
    "CrawlerRequests": 40
  }
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 6.2. DescribeCrawlerRequests

调用DescribeCrawlerRequests查询任务实例对应攻击面数据项中的爬虫流量信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称          | 类型      | 是否必选 | 示例值                     | 描述                                          |
|-------------|---------|------|-------------------------|---------------------------------------------|
| Action      | String  | 是    | DescribeCrawlerRequests | 要执行的操作。取值： <b>DescribeCrawlerRequests</b> 。 |
| TaskId      | Integer | 是    | 12345                   | 任务ID。获取指定任务ID数据。                            |
| Asset       | String  | 否    | foo.com                 | 资产名称。查询指定资产下的检测数据。                          |
| CurrentPage | Integer | 否    | 1                       | 指定返回结果的当前页码。默认值为1。                          |
| PageSize    | Integer | 否    | 10                      | 指定列表每页显示数据条数。默认值为10，且可设置值最大为10。             |

返回数据

| 名称        | 类型      | 示例值                                                      | 描述         |
|-----------|---------|----------------------------------------------------------|------------|
| Records   | Array   |                                                          | 返回结果的记录列表。 |
| Cookies   | String  | {"SESSIONID":<br>"3A6FA438DDB20E86<br>0F64FB4F57F315DC"} | Cookies    |
| Data      | String  | foo=bar                                                  | 请求体。       |
| Index     | Integer | 1                                                        | 记录索引号。     |
| Method    | String  | GET                                                      | 请求方法。      |
| URL       | String  | http://***.com                                           | URL地址。     |
| UpdatedAt | Long    | 1561392000000                                            | 扫描时间戳。     |
| RequestId | String  | DD73CB0A-6E99-<br>49AB-9569-<br>5A00C9732795             | 返回结果的请求ID。 |
| Total     | Integer | 120                                                      | 返回数据的总数量。  |

示例

请求示例

http(s)://[Endpoint]/?Action=DescribeCrawlerRequests  
&<公共请求参数>

正常返回示例

XML 格式

```
<DescribeCrawlerRequestsResponse>
  <code>200</code>
  <requestId>DD73CB0A-6E99-49AB-9569-5A00C9732795</requestId>
  <success>true</success>
  <data>
    <Total>123</Total>
    <Records>
      <Index>1</Index>
      <Method>GET</Method>
      <URL>http://***.***.com/user/login?username=admin</URL>
      <Cookies>
        <JSESSIONID>3A6FA438DDB20E860F64FB4F57F315DC</JSESSIONID>
      </Cookies>
      <Data></Data>
      <UpdatedAt>1561392000000</UpdatedAt>
    </Records>
    <Records>
      <Index>2</Index>
      <Method>GET</Method>
      <URL>http://***.***.com/user/login?username=admin</URL>
      <Cookies>
        <JSESSIONID>3A6FA438DDB20E860F64FB4F57F315DC</JSESSIONID>
      </Cookies>
      <Data></Data>
      <UpdatedAt>1561392000000</UpdatedAt>
    </Records>
  </data>
</DescribeCrawlerRequestsResponse>
```

JSON 格式

```
{
  "code": "200",
  "requestId": "DD73CB0A-6E99-49AB-9569-5A00C9732795",
  "success": true,
  "data": {
    "Total": 123,
    "Records": [
      {
        "Index": 1,
        "Method": "GET",
        "URL": "http://***.***.com/user/login?username=admin",
        "Cookies": {
          "JSESSIONID": "3A6FA438DDB20E860F64FB4F57F315DC"
        },
        "Data": "",
        "UpdatedAt": 1561392000000
      },
      {
        "Index": 2,
        "Method": "GET",
        "URL": "http://***.***.com/user/login?username=admin",
        "Cookies": {
          "JSESSIONID": "3A6FA438DDB20E860F64FB4F57F315DC"
        },
        "Data": "",
        "UpdatedAt": 1561392000000
      }
    ]
  }
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 6.3. DescribeDNSMap

调用DescribeDNSMap查询任务实例对应攻击面数据项中的DNS解析记录信息。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

### 请求参数

| 名称     | 类型     | 是否必选 | 示例值            | 描述                                 |
|--------|--------|------|----------------|------------------------------------|
| Action | String | 是    | DescribeDNSMap | 要执行的操作。取值： <b>DescribeDNSMap</b> 。 |

| 名称          | 类型      | 是否必选 | 示例值     | 描述                              |
|-------------|---------|------|---------|---------------------------------|
| TaskId      | Integer | 是    | 12345   | 任务ID。获取指定任务ID数据。                |
| Asset       | String  | 否    | foo.com | 资产名称。查询指定资产下的检测数据。              |
| CurrentPage | Integer | 否    | 1       | 指定返回结果的当前页码。默认值为1。              |
| PageSize    | Integer | 否    | 10      | 指定列表每页显示数据条数。默认值为10，且可设置值最大为10。 |

返回数据

| 名称        | 类型      | 示例值                                  | 描述                                                                                     |
|-----------|---------|--------------------------------------|----------------------------------------------------------------------------------------|
| Records   | Array   |                                      | 返回结果的记录列表。                                                                             |
| Domain    | String  | www.foo.com                          | 域名。                                                                                    |
| Index     | Integer | 1                                    | 记录索引号。                                                                                 |
| Record    | String  | 1.2.3.4                              | 解析记录信息。                                                                                |
| Type      | String  | A                                    | 解析记录类型。取值： <ul style="list-style-type: none"><li>A：IP解析</li><li>CNAME：主机别名解析</li></ul> |
| UpdatedAt | Long    | 1561392000000                        | 扫描时间戳。                                                                                 |
| RequestId | String  | DD73CB0A-6E99-49AB-9569-5A00C9732795 | 返回结果的请求ID。                                                                             |
| Total     | Integer | 1000                                 | 返回数据的总数量。                                                                              |

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDNSMap
&<公共请求参数>
```

## 正常返回示例

## XML 格式

```
<DescribeDNSMapResponse>
  <code>200</code>
  <requestId>DD73CB0A-6E99-49AB-9569-5A00C9732795</requestId>
  <success>true</success>
  <data>
    <Total>120</Total>
    <Records>
      <Index>1</Index>
      <Domain>www.foo.com</Domain>
      <Record>1.2.3.4</Record>
      <Type>A</Type>
      <CreatedAt>1561392000000</CreatedAt>
    </Records>
    <Records>
      <Index>2</Index>
      <Domain>www.foo.com</Domain>
      <Record>1.2.3.4</Record>
      <Type>A</Type>
      <CreatedAt>1561392000000</CreatedAt>
    </Records>
  </data>
</DescribeDNSMapResponse>
```

## JSON 格式

```
{
  "code": "200",
  "requestId": "DD73CB0A-6E99-49AB-9569-5A00C9732795",
  "success": true,
  "data": {
    "Total": 120,
    "Records": [
      {
        "Index": 1,
        "Domain": "www.foo.com",
        "Record": "1.2.3.4",
        "Type": "A",
        "CreatedAt": 1561392000000
      },
      {
        "Index": 2,
        "Domain": "www.foo.com",
        "Record": "1.2.3.4",
        "Type": "A",
        "CreatedAt": 1561392000000
      }
    ]
  }
}
```

错误码

访问[错误中心](#)查看更多错误码。

6.4. DescribeDomainAttackSurfacesFacets

调用DescribeDomainAttackSurfacesFacets查询任务实例对应攻击面数据项中的域名攻击面统计信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称     | 类型      | 是否必选 | 示例值                                | 描述                                            |
|--------|---------|------|------------------------------------|-----------------------------------------------|
| Action | String  | 是    | DescribeDomainAttackSurfacesFacets | 要执行的操作。取值：DescribeDomainAttackSurfacesFacets。 |
| Domain | String  | 是    | test.com                           | 域名。                                           |
| TaskId | Integer | 是    | 12345                              | 任务ID。获取指定任务ID数据。                              |

返回数据

| 名称              | 类型      | 示例值                                  | 描述         |
|-----------------|---------|--------------------------------------|------------|
| CrawlerRequests | Integer | 30                                   | 爬虫流量数量。    |
| RequestId       | String  | DD73CB0A-6E99-49AB-9569-5A00C9732795 | 返回结果的请求ID。 |
| WebPaths        | Integer | 10                                   | Web路径数量。   |
| WebServers      | Integer | 10                                   | Web服务器数量。  |
| WebTechs        | Integer | 10                                   | Web应用数量。   |

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomainAttackSurfacesFacets
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeDomainAttackSurfacesFacetsResponse>
  <code>200</code>
  <requestId>DD73CB0A-6E99-49AB-9569-5A00C9732795</requestId>
  <success>true</success>
  <data>
    <CrawlerRequests>20</CrawlerRequests>
    <WebPaths>22</WebPaths>
    <WebServers>0</WebServers>
    <WebTechs>0</WebTechs>
  </data>
</DescribeDomainAttackSurfacesFacetsResponse>
```

JSON 格式

```
{
  "code": "200",
  "requestId": "DD73CB0A-6E99-49AB-9569-5A00C9732795",
  "success": true,
  "data": {
    "CrawlerRequests": 20,
    "WebPaths": 22,
    "WebServers": 0,
    "WebTechs": 0
  }
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 6.5. DescribeDomains

调用DescribeDomains查询任务实例对应攻击面数据项中的域名信息。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

### 请求参数

| 名称 | 类型 | 是否必选 | 示例值 | 描述 |
|----|----|------|-----|----|
|----|----|------|-----|----|

| 名称          | 类型      | 是否必选 | 示例值             | 描述                                  |
|-------------|---------|------|-----------------|-------------------------------------|
| Action      | String  | 是    | DescribeDomains | 要执行的操作。取值： <b>DescribeDomains</b> 。 |
| TaskId      | Integer | 是    | 12345           | 任务ID。获取指定任务ID数据。                    |
| Asset       | String  | 否    | foo.com         | 资产名称。查询指定资产下的检测数据。                  |
| CurrentPage | Integer | 否    | 1               | 指定返回结果的当前页码。默认值为1。                  |
| PageSize    | Integer | 否    | 10              | 指定列表每页显示数据条数。默认值为10，且可设置值最大为10。     |

返回数据

| 名称        | 类型      | 示例值                                  | 描述         |
|-----------|---------|--------------------------------------|------------|
| Records   | Array   |                                      | 返回结果的记录列表。 |
| Domain    | String  | foo.com                              | 域名。        |
| Index     | Integer | 1                                    | 记录索引号。     |
| UpdatedAt | Long    | 1561392000000                        | 扫描时间戳。     |
| RequestId | String  | DD73CB0A-6E99-49AB-9569-5A00C9732795 | 返回结果的请求ID。 |
| Total     | Integer | 10000                                | 返回数据的总数量。  |

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeDomains
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeDomainsResponse>
  <code>200</code>
  <requestId>DD73CB0A-6E99-49AB-9569-5A00C9732795</requestId>
  <success>true</success>
  <data>
    <Records>
      <Index>1</Index>
      <Domain>www.foo.com</Domain>
      <UpdatedAt>1561392000000</UpdatedAt>
    </Records>
    <Records>
      <Index>2</Index>
      <Domain>www.abc.com</Domain>
      <UpdatedAt>1561392000000</UpdatedAt>
    </Records>
  </data>
</DescribeDomainsResponse>
```

#### JSON 格式

```
{
  "code": "200",
  "requestId": "DD73CB0A-6E99-49AB-9569-5A00C9732795",
  "success": true,
  "data": {
    "Records": [
      {
        "Index": 1,
        "Domain": "www.foo.com",
        "UpdatedAt": 1561392000000
      },
      {
        "Index": 2,
        "Domain": "www.abc.com",
        "UpdatedAt": 1561392000000
      }
    ]
  }
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 6.6. DescribeHosts

调用DescribeHosts查询任务实例对应攻击面数据项中的主机列表信息。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称          | 类型      | 是否必选 | 示例值           | 描述                                |
|-------------|---------|------|---------------|-----------------------------------|
| Action      | String  | 是    | DescribeHosts | 要执行的操作。取值： <b>DescribeHosts</b> 。 |
| TaskId      | Integer | 是    | 12345         | 任务ID。获取指定任务ID数据。                  |
| Asset       | String  | 否    | foo.com       | 资产名称。查询指定资产下的检测数据。                |
| CurrentPage | Integer | 否    | 1             | 指定返回结果的当前页码。默认值为1。                |
| PageSize    | Integer | 否    | 10            | 指定列表每页显示数据条数。默认值为10，且可设置值最大为10。   |

返回数据

| 名称        | 类型      | 示例值                                  | 描述                                                                               |
|-----------|---------|--------------------------------------|----------------------------------------------------------------------------------|
| Records   | Array   |                                      | 返回结果的记录列表。                                                                       |
| Hostname  | String  | foo-hostname                         | 主机名称。                                                                            |
| IP        | String  | 1.2.3.4                              | IP地址。                                                                            |
| Index     | Integer | 1                                    | 记录索引号。                                                                           |
| IsUp      | String  | Up                                   | 机器是否存活。取值： <ul style="list-style-type: none"><li>Up：存活</li><li>Down：关机</li></ul> |
| OS        | String  | Windows                              | 操作系统类型。                                                                          |
| UpdatedAt | Long    | 1561392000000                        | 扫描时间戳。                                                                           |
| RequestId | String  | DD73CB0A-6E99-49AB-9569-5A00C9732795 | 返回结果的请求ID。                                                                       |
| Total     | Integer | 1000                                 | 返回数据的总数量。                                                                        |

## 示例

### 请求示例

```
http(s)://[Endpoint]/?Action=DescribeHosts
&<公共请求参数>
```

### 正常返回示例

#### XML 格式

```
<DescribeHostsResponse>
  <code>200</code>
  <requestId>DD73CB0A-6E99-49AB-9569-5A00C9732795</requestId>
  <success>true</success>
  <data>
    <Total>120</Total>
    <Records>
      <Index>1</Index>
      <IP>1.2.3.4</IP>
      <Hostname></Hostname>
      <OS>AVtech Room Alert 26W environmental monitor </OS>
      <IsUp>Up</IsUp>
      <CreatedAt>1561392000000</CreatedAt>
    </Records>
    <Records>
      <Index>2</Index>
      <IP>1.2.3.4</IP>
      <Hostname></Hostname>
      <OS>AVtech Room Alert 26W environmental monitor </OS>
      <IsUp>Up</IsUp>
      <CreatedAt>1561392000000</CreatedAt>
    </Records>
  </data>
</DescribeHostsResponse>
```

#### JSON 格式

```
{
  "code": "200",
  "requestId": "DD73CB0A-6E99-49AB-9569-5A00C9732795",
  "success": true,
  "data": {
    "Total": 120,
    "Records": [
      {
        "Index": 1,
        "IP": "1.2.3.4",
        "Hostname": "foo-hostname",
        "OS": "AVtech Room Alert 26W environmental monitor ",
        "IsUp": "Up",
        "CreatedAt": 1561392000000
      },
      {
        "Index": 2,
        "IP": "1.2.3.4",
        "Hostname": "foo-hostname",
        "OS": "AVtech Room Alert 26W environmental monitor ",
        "IsUp": "Up",
        "CreatedAt": 1561392000000
      }
    ]
  }
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 6.7. DescribeHostAttackSurfacesFacets

调用DescribeHostAttackSurfacesFacets查询任务实例对应攻击面数据项中的主机攻击面统计信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称     | 类型     | 是否必选 | 示例值                              | 描述                                          |
|--------|--------|------|----------------------------------|---------------------------------------------|
| Action | String | 是    | DescribeHostAttackSurfacesFacets | 要执行的操作。取值：DescribeHostAttackSurfacesFacets。 |
| Host   | String | 是    | 1.2.3.4                          | 主机名。获取指定主机下数据。                              |

| 名称     | 类型      | 是否必选 | 示例值    | 描述               |
|--------|---------|------|--------|------------------|
| TaskId | Integer | 是    | 123456 | 任务ID。获取指定任务ID数据。 |

返回数据

| 名称              | 类型      | 示例值                                  | 描述         |
|-----------------|---------|--------------------------------------|------------|
| CrawlerRequests | Integer | 30                                   | 爬虫流量数量。    |
| Hosts           | Integer | 10                                   | 主机数量。      |
| Ports           | Integer | 10                                   | 端口数量。      |
| RequestId       | String  | DD73CB0A-6E99-49AB-9569-5A00C9732795 | 返回结果的请求ID。 |
| WebPaths        | Integer | 10                                   | Web路径数量。   |
| WebTechs        | Integer | 10                                   | Web应用数量。   |

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeHostAttackSurfacesFacets
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeHostAttackSurfacesFacetsResponse>
  <code>200</code>
  <requestId>DD73CB0A-6E99-49AB-9569-5A00C9732795</requestId>
  <success>true</success>
  <data>
    <CrawlerRequests>0</CrawlerRequests>
    <Ports>304</Ports>
    <WebPaths>14</WebPaths>
    <WebServers>14</WebServers>
    <WebTechs>2</WebTechs>
  </data>
</DescribeHostAttackSurfacesFacetsResponse>
```

JSON 格式

```
{
  "code": "200",
  "requestId": "DD73CB0A-6E99-49AB-9569-5A00C9732795",
  "success": true,
  "data": {
    "CrawlerRequests": 0,
    "Ports": 304,
    "WebPaths": 14,
    "WebServers": 14,
    "WebTechs": 2
  }
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

# 6.8. DescribePorts

调用DescribePorts查询任务实例对应攻击面数据项中的端口服务信息。

## 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

## 请求参数

| 名称          | 类型      | 是否必选 | 示例值           | 描述                                |
|-------------|---------|------|---------------|-----------------------------------|
| Action      | String  | 是    | DescribePorts | 要执行的操作。取值： <b>DescribePorts</b> 。 |
| TaskId      | Integer | 是    | 12345         | 任务ID。获取指定任务ID数据。                  |
| Asset       | String  | 否    | foo.com       | 资产名称。查询指定资产下的检测数据。                |
| CurrentPage | Integer | 否    | 1             | 指定返回结果的当前页码。默认值为1。                |
| PageSize    | Integer | 否    | 10            | 指定列表每页显示数据条数。默认值为10，且可设置值最大为10。   |

## 返回数据

| 名称 | 类型 | 示例值 | 描述 |
|----|----|-----|----|
|----|----|-----|----|

| 名称          | 类型      | 示例值                                  | 描述         |
|-------------|---------|--------------------------------------|------------|
| Records     | Array   |                                      | 返回结果的记录列表。 |
| Fingerprint | String  | HTTP Apache                          | 端口指纹。      |
| IP          | String  | 1.2.3.4                              | IP地址。      |
| Index       | Integer | 1                                    | 记录索引号。     |
| Port        | String  | 843                                  | 端口号。       |
| Product     | String  | Apache Tomcat/***** 1.1              | 产品名。       |
| Protocol    | String  | tcp                                  | 网络协议。      |
| Service     | String  | http                                 | 服务类型。      |
| UpdatedAt   | Long    | 1561392000000                        | 扫描时间戳。     |
| Version     | String  | 1.1                                  | 版本信息。      |
| RequestId   | String  | DD73CB0A-6E99-49AB-9569-5A00C9732795 | 返回结果的请求ID。 |
| Total       | Integer | 120                                  | 返回数据的总数量。  |

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribePorts
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribePortsResponse>
  <code>200</code>
  <requestId>DD73CB0A-6E99-49AB-9569-5A00C9732795</requestId>
  <success>true</success>
  <data>
    <Total>120</Total>
    <Records>
      <Index>1</Index>
      <IP>1.2.3.4</IP>
      <Protocol>tcp</Protocol>
      <Port>843</Port>
      <Service>http</Service>
      <Product>Apache Tomcat/Coyote JSP engine 1.1</Product>
      <Version>1.1</Version>
      <Fingerprint></Fingerprint>
      <UpdatedAt>1561392000000</UpdatedAt>
    </Records>
    <Records>
      <Index>2</Index>
      <IP>1.2.3.5</IP>
      <Protocol>tcp</Protocol>
      <Port>843</Port>
      <Service>http</Service>
      <Product>Apache Tomcat/Coyote JSP engine 1.1</Product>
      <Version>1.1</Version>
      <Fingerprint></Fingerprint>
      <UpdatedAt>1561392000000</UpdatedAt>
    </Records>
  </data>
</DescribePortsResponse>
```

JSON 格式

```
{
  "code": "200",
  "requestId": "DD73CB0A-6E99-49AB-9569-5A00C9732795",
  "success": true,
  "data": {
    "Total": 120,
    "Records": [
      {
        "Index": 1,
        "IP": "1.2.3.4",
        "Protocol": "tcp",
        "Port": "843",
        "Service": "http",
        "Product": "Apache Tomcat/Coyote JSP engine 1.1",
        "Version": "1.1",
        "Fingerprint": "",
        "UpdatedAt": 1561392000000
      },
      {
        "Index": 2,
        "IP": "1.2.3.5",
        "Protocol": "tcp",
        "Port": "843",
        "Service": "http",
        "Product": "Apache Tomcat/Coyote JSP engine 1.1",
        "Version": "1.1",
        "Fingerprint": "",
        "UpdatedAt": 1561392000000
      }
    ]
  }
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 6.9. DescribeSubdomains

调用DescribeSubdomains查询任务实例对应攻击面数据项中的子域名信息。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

### 请求参数

| 名称 | 类型 | 是否必选 | 示例值 | 描述 |
|----|----|------|-----|----|
|----|----|------|-----|----|

| 名称          | 类型      | 是否必选 | 示例值                | 描述                                     |
|-------------|---------|------|--------------------|----------------------------------------|
| Action      | String  | 是    | DescribeSubdomains | 要执行的操作。取值： <b>DescribeSubdomains</b> 。 |
| TaskId      | Integer | 是    | 12345              | 任务ID。获取指定任务ID数据。                       |
| Asset       | String  | 否    | foo.com            | 资产名称。查询指定资产下的检测数据。                     |
| CurrentPage | Integer | 否    | 1                  | 指定返回结果的当前页码。默认值为1。                     |
| PageSize    | Integer | 否    | 10                 | 指定列表每页显示数据条数。默认值为10，且可设置值最大为10。        |

返回数据

| 名称         | 类型      | 示例值                                  | 描述         |
|------------|---------|--------------------------------------|------------|
| Records    | Array   |                                      | 返回结果的记录列表。 |
| Domain     | String  | www.foo.com                          | 域名。        |
| Index      | Integer | 1                                    | 记录索引号。     |
| RootDomain | String  | foo.com                              | 根域名。       |
| UpdatedAt  | Long    | 1561392000000                        | 扫描时间戳。     |
| RequestId  | String  | DD73CB0A-6E99-49AB-9569-5A00C9732795 | 返回结果的请求ID。 |
| Total      | Integer | 1000                                 | 返回数据的总数量。  |

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeSubdomains
&<公共请求参数>
```

正常返回示例

## XML 格式

```
<DescribeSubdomainsResponse>
  <code>200</code>
  <success>true</success>
  <requestId>9D2C9710-A52C-4C4A-9082-9E570C958D5D</requestId>
  <data>
    <Total>120</Total>
    <Records>
      <Index>1</Index>
      <Domain>www.foo.com</Domain>
      <RootDomain>foo.com</RootDomain>
      <UpdatedAt>1561392000000</UpdatedAt>
    </Records>
    <Records>
      <Index>2</Index>
      <Domain>www.bar.com</Domain>
      <RootDomain>foo.com</RootDomain>
      <UpdatedAt>1561392000000</UpdatedAt>
    </Records>
  </data>
</DescribeSubdomainsResponse>
```

## JSON 格式

```
{
  "code": "200",
  "success": true,
  "requestId": "9D2C9710-A52C-4C4A-9082-9E570C958D5D",
  "data": {
    "Total": 120,
    "Records": [
      {
        "Index": 1,
        "Domain": "www.foo.com",
        "RootDomain": "foo.com",
        "UpdatedAt": 1561392000000
      },
      {
        "Index": 2,
        "Domain": "www.bar.com",
        "RootDomain": "foo.com",
        "UpdatedAt": 1561392000000
      }
    ]
  }
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 6.10. DescribeWebPaths

调用DescribeWebPaths查询任务实例对应攻击面数据项中的Web路径信息。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

### 请求参数

| 名称          | 类型      | 是否必选 | 示例值              | 描述                                   |
|-------------|---------|------|------------------|--------------------------------------|
| Action      | String  | 是    | DescribeWebPaths | 要执行的操作。取值： <b>DescribeWebPaths</b> 。 |
| TaskId      | Integer | 是    | 12345            | 任务ID。获取指定任务ID数据。                     |
| Asset       | String  | 否    | foo.com          | 资产名称。查询指定资产下的检测数据。                   |
| CurrentPage | Integer | 否    | 1                | 指定返回结果的当前页码。默认值为1。                   |
| PageSize    | Integer | 否    | 10               | 指定列表每页显示数据条数。默认值为10，且可设置值最大为10。      |

### 返回数据

| 名称        | 类型      | 示例值                                 | 描述         |
|-----------|---------|-------------------------------------|------------|
| Records   | Array   |                                     | 返回结果的记录列表。 |
| Extension | String  | png                                 | 文件的后缀名。    |
| Index     | Integer | 1                                   | 记录索引号。     |
| Path      | String  | /themes/dist/images/test-123***.png | 路径信息。      |
| Site      | String  | http://1.2.3.4:88**                 | 站点URL地址。   |
| UpdatedAt | Long    | 1561392000000                       | 扫描时间戳。     |

| 名称        | 类型      | 示例值                                  | 描述         |
|-----------|---------|--------------------------------------|------------|
| RequestId | String  | DD73CB0A-6E99-49AB-9569-5A00C9732795 | 返回结果的请求ID。 |
| Total     | Integer | 120                                  | 返回数据的总数量。  |

## 示例

### 请求示例

```
http(s)://[Endpoint]/?Action=DescribeWebPaths
&<公共请求参数>
```

### 正常返回示例

#### XML 格式

```
<DescribeWebPathsResponse>
  <code>200</code>
  <requestId>DD73CB0A-6E99-49AB-9569-5A00C9732795</requestId>
  <success>true</success>
  <data>
    <Records>
      <Index>1</Index>
      <Site>http://icourse.*****.com:8899</Site>
      <Path> /themes/dist/images/sg1-476744*****.png</Path>
      <Extension>png</Extension>
      <CreatedAt>1561392000000</CreatedAt>
    </Records>
    <Records>
      <Index>2</Index>
      <Site>http://icourse.*****.com:88**</Site>
      <Path> /themes/dist/images/sg1-4767*****.png</Path>
      <Extension>png</Extension>
      <CreatedAt>1561392000000</CreatedAt>
    </Records>
  </data>
</DescribeWebPathsResponse>
```

#### JSON 格式

```
{
  "code": "200",
  "requestId": "DD73CB0A-6E99-49AB-9569-5A00C9732795",
  "success": true,
  "data": {
    "Records": [
      {
        "Index": 1,
        "Site": "http://icourse.*****.com:8899",
        "Path": " /themes/dist/images/sg1-476744*****.png",
        "Extension": ".png",
        "CreatedAt": 1561392000000
      },
      {
        "Index": 2,
        "Site": "http://icourse.*****.com:88**",
        "Path": " /themes/dist/images/sg1-4767*****.png",
        "Extension": ".png",
        "CreatedAt": 1561392000000
      }
    ]
  }
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 6.11. DescribeWebServers

调用DescribeWebServers查询任务实例对应攻击面数据项中的Web服务器信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称          | 类型      | 是否必选 | 示例值                | 描述                                     |
|-------------|---------|------|--------------------|----------------------------------------|
| Action      | String  | 是    | DescribeWebServers | 要执行的操作。取值： <b>DescribeWebServers</b> 。 |
| TaskId      | Integer | 是    | 12345              | 任务ID。获取指定任务ID数据。                       |
| Asset       | String  | 否    | foo.com            | 资产名称。查询指定资产下的检测数据。                     |
| CurrentPage | Integer | 否    | 1                  | 指定返回结果的当前页码。默认值为1。                     |

| 名称       | 类型      | 是否必选 | 示例值 | 描述                              |
|----------|---------|------|-----|---------------------------------|
| PageSize | Integer | 否    | 10  | 指定列表每页显示数据条数。默认值为10，且可设置值最大为10。 |

返回数据

| 名称        | 类型      | 示例值                                  | 描述         |
|-----------|---------|--------------------------------------|------------|
| Records   | Array   |                                      | 返回结果的记录列表。 |
| Host      | String  | 1.2.3.4                              | Web服务主机。   |
| Index     | Integer | 1                                    | 记录索引号。     |
| Port      | String  | 80                                   | Web服务端口号。  |
| Scheme    | String  | http                                 | 请求协议。      |
| UpdatedAt | Long    | 1561392000000                        | 扫描时间戳。     |
| RequestId | String  | DD73CB0A-6E99-49AB-9569-5A00C9732795 | 返回结果的请求ID。 |
| Total     | Integer | 120                                  | 返回数据的总数量。  |

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeWebServers
&TaskId=12345
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeWebServersResponse>
  <code>200</code>
  <requestId>DD73CB0A-6E99-49AB-9569-5A00C9732795</requestId>
  <success>true</success>
  <data>
    <Records>
      <Index>1</Index>
      <Scheme>http</Scheme>
      <Host>1.2.3.4</Host>
      <Port>80</Port>
      <UpdatedAt>1561392000000</UpdatedAt>
    </Records>
    <Records>
      <Index>2</Index>
      <Scheme>http</Scheme>
      <Host>1.2.3.4</Host>
      <Port>80</Port>
      <UpdatedAt>1561392000000</UpdatedAt>
    </Records>
  </data>
</DescribeWebServersResponse>
```

#### JSON 格式

```
{
  "requestId":"DD73CB0A-6E99-49AB-9569-5A00C9732795",
  "data":{
    "Records":[
      {
        "UpdatedAt":1561392000000,
        "Port":80,
        "Scheme":"http",
        "Index":1,
        "Host":"1.2.3.4"
      },
      {
        "UpdatedAt":1561392000000,
        "Port":80,
        "Scheme":"http",
        "Index":2,
        "Host":"1.2.3.4"
      }
    ]
  },
  "code":"200",
  "success":true
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 6.12. DescribeWebTechs

调用DescribeWebTechs查询任务实例对应攻击面数据项中的Web应用信息。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

### 请求参数

| 名称          | 类型      | 是否必选 | 示例值              | 描述                                   |
|-------------|---------|------|------------------|--------------------------------------|
| Action      | String  | 是    | DescribeWebTechs | 要执行的操作。取值： <b>DescribeWebTechs</b> 。 |
| TaskId      | Integer | 是    | 12345            | 任务ID。获取指定任务ID数据。                     |
| Asset       | String  | 否    | foo.com          | 资产名称。查询指定资产下的检测数据。                   |
| CurrentPage | Integer | 否    | 1                | 指定返回结果的当前页码。默认值为1。                   |
| PageSize    | Integer | 否    | 10               | 指定列表每页显示数据条数。默认值为10，且可设置值最大为10。      |

### 返回数据

| 名称        | 类型      | 示例值            | 描述         |
|-----------|---------|----------------|------------|
| Records   | Array   |                | 返回结果的记录列表。 |
| Index     | Integer | 1              | 记录索引号。     |
| Name      | String  | Apache         | IP地址。      |
| PoweredBy | String  | Java           | 编程语言。      |
| Server    | String  | Apache         | Web服务器。    |
| Title     | String  | 开放平台-首页        | Web服务标题。   |
| URL       | String  | http://***.com | 应用URL地址。   |

| 名称        | 类型      | 示例值                                  | 描述         |
|-----------|---------|--------------------------------------|------------|
| UpdatedAt | Long    | 1561392000000                        | 扫描时间戳。     |
| Version   | String  | 1.7                                  | 版本信息。      |
| RequestId | String  | DD73CB0A-6E99-49AB-9569-5A00C9732795 | 返回结果的请求ID。 |
| Total     | Integer | 120                                  | 返回数据的总数量。  |

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeWebTechs
&TaskId=12345
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeWebTechsResponse>
  <code>200</code>
  <requestId>DD73CB0A-6E99-49AB-9569-5A00C9732795</requestId>
  <success>true</success>
  <data>
    <Records>
      <Index>1</Index>
      <Name>Apache</Name>
      <URL>https://1.2.3.4:443/</URL>
      <Version>1.7.2</Version>
      <Server>Apache</Server>
      <PoweredBy></PoweredBy>
      <Title>CPOS开放平台-首页</Title>
      <UpdatedAt>1561392000000</UpdatedAt>
    </Records>
    <Records>
      <Index>2</Index>
      <Name>Apache</Name>
      <URL>https://1.2.3.4:443/</URL>
      <Version>1.7.2</Version>
      <Server>Apache</Server>
      <PoweredBy></PoweredBy>
      <Title>CPOS开放平台-首页</Title>
      <UpdatedAt>1561392000000</UpdatedAt>
    </Records>
  </data>
</DescribeWebTechsResponse>
```

JSON 格式

```
{
  "code": "200",
  "requestId": "DD73CB0A-6E99-49AB-9569-5A00C9732795",
  "success": true,
  "data": {
    "Records": [
      {
        "Index": 1,
        "Name": "Apache",
        "URL": "https://1.2.3.4:443/",
        "Version": "1.7.2",
        "Server": "Apache",
        "PoweredBy": "",
        "Title": "CPOS开放平台-首页",
        "UpdatedAt": 1561392000000
      },
      {
        "Index": 2,
        "Name": "Apache",
        "URL": "https://1.2.3.4:443/",
        "Version": "1.7.2",
        "Server": "Apache",
        "PoweredBy": "",
        "Title": "CPOS开放平台-首页",
        "UpdatedAt": 1561392000000
      }
    ]
  }
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 7.攻击面透视

### 7.1. AddOrgDomains

调用AddOrgDomains添加根域名列表。

#### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

#### 请求参数

| 名称        | 类型         | 是否必选 | 示例值                         | 描述                                |
|-----------|------------|------|-----------------------------|-----------------------------------|
| Action    | String     | 是    | AddOrgDomains               | 要执行的操作。取值： <b>AddOrgDomains</b> 。 |
| Domains.N | RepeatList | 是    | ["baidu.com", "aliyun.com"] | 根域名列表。                            |
| OrgId     | Integer    | 是    | 1                           | 组织机构ID。                           |

#### 返回数据

| 名称        | 类型     | 示例值                                  | 描述         |
|-----------|--------|--------------------------------------|------------|
| RequestId | String | 73D1B3B5-B2A5-45CF-84B7-4C73A6EEF5C5 | 返回结果的请求ID。 |

#### 示例

##### 请求示例

```
http(s)://[Endpoint]/?Action=AddOrgDomains
&Domains.1=["baidu.com", "aliyun.com"]
&OrgId=1
&<公共请求参数>
```

##### 正常返回示例

###### XML 格式

```
<AddOrgDomainsResponse>
  <RequestId>D4F99513-88A6-4FDB-B6ED-0AC64C16C256</RequestId>
</AddOrgDomainsResponse>
```

###### JSON 格式

```
{
  "RequestId": "D4F99513-88A6-4FDB-B6ED-0AC64C16C256"
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 7.2. AddOrgHosts

调用AddOrgHosts新增组织机构主机列表。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称      | 类型         | 是否必选 | 示例值                                           | 描述                              |
|---------|------------|------|-----------------------------------------------|---------------------------------|
| Action  | String     | 是    | AddOrgHosts                                   | 要执行的操作。取值： <b>AddOrgHosts</b> 。 |
| Hosts.N | RepeatList | 是    | ["192.168.1.1", "192.168.1.2", "192.168.1.3"] | 主机列表。                           |
| OrgId   | Integer    | 是    | 1                                             | 组织机构ID。                         |

返回数据

| 名称        | 类型     | 示例值                                  | 描述         |
|-----------|--------|--------------------------------------|------------|
| RequestId | String | 73D1B3B5-B2A5-45CF-84B7-4C73A6EEF5C5 | 返回结果的请求ID。 |

示例

请求示例

```
http(s)://[Endpoint]/?Action=AddOrgHosts
&Hosts.1=["192.168.1.1", "192.168.1.2", "192.168.1.3"]
&OrgId=1
&<公共请求参数>
```

正常返回示例

XML 格式

```
<AddOrgHostsResponse>
  <RequestId>F9717DC5-363E-4D3D-AA22-75243BEE373C</RequestId>
</AddOrgHostsResponse>
```

JSON 格式

```
{
  "RequestId": "F9717DC5-363E-4D3D-AA22-75243BEE373C"
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 7.3. AddOrgSubdomains

调用AddOrgSubdomains添加组织机构子域名列表。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称           | 类型         | 是否必选 | 示例值                 | 描述                                   |
|--------------|------------|------|---------------------|--------------------------------------|
| Action       | String     | 是    | AddOrgSubdomains    | 要执行的操作。取值： <b>AddOrgSubdomains</b> 。 |
| OrgId        | Integer    | 是    | 1                   | 组织机构ID。                              |
| Subdomains.N | RepeatList | 是    | testphp.vulnweb.com | 子域名。                                 |

返回数据

| 名称        | 类型     | 示例值                                  | 描述         |
|-----------|--------|--------------------------------------|------------|
| RequestId | String | B4E8BB43-CC60-49D3-BD4B-57CABDC00CA4 | 返回结果的请求ID。 |

示例

请求示例

```
http(s)://[Endpoint]/?Action=AddOrgSubdomains
&OrgId=1
&Subdomains.1=testphp.vulnweb.com
&<公共请求参数>
```

正常返回示例

XML 格式

```
<AddOrgSubdomainsResponse>
  <RequestId>32122AE9-9187-437A-B52C-BB53D061C82A</RequestId>
</AddOrgSubdomainsResponse>
```

JSON 格式

```
{
  "RequestId": "32122AE9-9187-437A-B52C-BB53D061C82A"
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 7.4. AddOrgWebPaths

调用AddOrgWebPaths添加组织机构Web路径。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称     | 类型         | 是否必选 | 示例值                    | 描述                                 |
|--------|------------|------|------------------------|------------------------------------|
| Action | String     | 是    | AddOrgWebPaths         | 要执行的操作。取值： <b>AddOrgWebPaths</b> 。 |
| OrgId  | Integer    | 是    | 1                      | 组织机构ID。                            |
| URLs.N | RepeatList | 是    | https://www.aliyun.com | Web路径列表。                           |

返回数据

| 名称 | 类型 | 示例值 | 描述 |
|----|----|-----|----|
|----|----|-----|----|

| 名称        | 类型     | 示例值                                  | 描述         |
|-----------|--------|--------------------------------------|------------|
| RequestId | String | D9E86C06-7DF6-4741-B6D2-C3EE38A74A08 | 返回结果的请求ID。 |

示例

请求示例

```
http(s)://[Endpoint]/?Action=AddOrgWebPaths
&OrgId=1
&URLs.1=https://www.aliyun.com
&<公共请求参数>
```

正常返回示例

XML 格式

```
<AddOrgWebPathsResponse>
  <RequestId>A6E12B8E-DCBB-4409-9E1E-F542BE3F598D</RequestId>
</AddOrgWebPathsResponse>
```

JSON 格式

```
{
  "RequestId": "A6E12B8E-DCBB-4409-9E1E-F542BE3F598D"
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 7.5. CreateOrganization

调用CreateOrganization创建企业组织机构。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称     | 类型     | 是否必选 | 示例值                | 描述                            |
|--------|--------|------|--------------------|-------------------------------|
| Action | String | 是    | CreateOrganization | 要执行的操作。取值：CreateOrganization。 |
| Name   | String | 否    | 新的组织机构             | 组织机构名称。                       |

| 名称          | 类型         | 是否必选 | 示例值                   | 描述      |
|-------------|------------|------|-----------------------|---------|
| Description | String     | 否    | 这是一个企业组织机构描述          | 组织机构描述。 |
| Domains.N   | RepeatList | 否    | aliyun.com\nbaidu.com | 根域名列表。  |

## 返回数据

| 名称        | 类型     | 示例值                                  | 描述         |
|-----------|--------|--------------------------------------|------------|
| RequestId | String | 5E4879DC-8527-4A3B-97BC-5FE0C3DE4C47 | 返回结果的请求ID。 |

## 示例

请求示例

```
http(s)://[Endpoint]/?Action=CreateOrganization
&<公共请求参数>
```

正常返回示例

XML 格式

```
<CreateOrganizationResponse>
  <RequestId>580C3EB1-AF91-45D4-A5DE-9CCABB48A9C2</RequestId>
</CreateOrganizationResponse>
```

JSON 格式

```
{
  "RequestId": "580C3EB1-AF91-45D4-A5DE-9CCABB48A9C2"
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

# 7.6. DeleteOrganizations

调用DeleteOrganizations删除组织机构。

## 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

## 请求参数

| 名称       | 类型         | 是否必选 | 示例值                 | 描述                                      |
|----------|------------|------|---------------------|-----------------------------------------|
| Action   | String     | 是    | DeleteOrganizations | 要执行的操作。取值： <b>DeleteOrganizations</b> 。 |
| OrgIds.N | RepeatList | 是    | 1                   | 企业组织ID。                                 |

返回数据

| 名称        | 类型     | 示例值                                  | 描述         |
|-----------|--------|--------------------------------------|------------|
| RequestId | String | 5E4879DC-8527-4A3B-97BC-5FE0C3DE4C47 | 返回结果的请求ID。 |

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteOrganizations
&OrgIds.1=1
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DeleteOrganizationsResponse>
  <code></code>
  <message></message>
  <success>true</success>
  <requestId></requestId>
  <data></data>
</DeleteOrganizationsResponse>
```

JSON 格式

```
{
  "code": "",
  "message": "",
  "success": true,
  "requestId": "",
  "data": {}
}
```

错误码

访问[错误中心](#)查看更多错误码。

## 7.7. DeleteOrgAttackSurfaceRecords

调用DeleteOrgAttackSurfaceRecords删除企业攻击面数据，可以删除指定组织机构的攻击面数据源。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

### 请求参数

| 名称        | 类型         | 是否必选 | 示例值                           | 描述                                                                                                                                                                                                                                                 |
|-----------|------------|------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action    | String     | 是    | DeleteOrgAttackSurfaceRecords | 要执行的操作。取值： <b>DeleteOrgAttackSurfaceRecords</b> 。                                                                                                                                                                                                  |
| OrgId     | Integer    | 是    | 1                             | 组织机构ID。                                                                                                                                                                                                                                            |
| Records.N | RepeatList | 是    | 1                             | 记录ID。                                                                                                                                                                                                                                              |
| Source    | String     | 是    | Ports                         | 支持的数据源，取值： <ul style="list-style-type: none"><li>• <b>Subdomains</b>：子域名列表。</li><li>• <b>Ports</b>：端口服务。</li><li>• <b>Hosts</b>：主机列表。</li><li>• <b>DNSMap</b>：DNS解析记录。</li><li>• <b>WebPaths</b>：Web路径。</li><li>• <b>WebTechs</b>：Web应用。</li></ul> |

### 返回数据

| 名称        | 类型     | 示例值                                  | 描述         |
|-----------|--------|--------------------------------------|------------|
| RequestId | String | E345DD9F-3800-42DC-8E8E-47C57888373C | 返回结果的请求ID。 |

### 示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteOrgAttackSurfaceRecords
&OrgId=1
&Records.1=1
&Source=Ports
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DeleteOrgAttackSurfaceRecordsResponse>
  <RequestId>ED817C83-F11A-430C-99E1-34A30A8DF42E</RequestId>
  <HostId>avds.aliyuncs.com</HostId>
  <Code>Forbidden</Code>
  <Message>operation permitted</Message>
</DeleteOrgAttackSurfaceRecordsResponse>
```

JSON 格式

```
{
  "RequestId": "ED817C83-F11A-430C-99E1-34A30A8DF42E",
  "HostId": "avds.aliyuncs.com",
  "Code": "Forbidden",
  "Message": "operation permitted"
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

# 7.8. DeleteUserAttackSurfaceRecords

调用DeleteUserAttackSurfaceRecords删除用户对应的攻击面数据源，您可以指定具体的攻击面数据源和具体的记录ID删除对应的攻击面数据源记录数据。

## 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

## 请求参数

| 名称        | 类型         | 是否必选 | 示例值                            | 描述                                        |
|-----------|------------|------|--------------------------------|-------------------------------------------|
| Action    | String     | 是    | DeleteUserAttackSurfaceRecords | 要执行的操作。取值：DeleteUserAttackSurfaceRecords。 |
| Records.N | RepeatList | 是    | 1                              | 记录ID。                                     |

| 名称     | 类型     | 是否必选 | 示例值        | 描述                                                                                                                                                                                                    |
|--------|--------|------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source | String | 是    | Subdomains | 支持的攻击面数据源。取值： <ul style="list-style-type: none"><li>• Subdomains：子域名</li><li>• Ports：端口服务</li><li>• Hosts：主机列表</li><li>• DNSMap：DNS解析记录</li><li>• WebPaths：Web路径列表</li><li>• WebTechs：Web应用</li></ul> |

返回数据

| 名称        | 类型     | 示例值                                  | 描述         |
|-----------|--------|--------------------------------------|------------|
| RequestId | String | E345DD9F-3800-42DC-8E8E-47C57888373C | 返回结果的请求ID。 |

示例

请求示例

```
http(s)://[Endpoint]/?Action=DeleteUserAttackSurfaceRecords
&Records.1=1
&Source= Subdomains
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DeleteUserAttackSurfaceRecordsResponse>
  <RequestId>E345DD9F-3800-42DC-8E8E-47C57888373C</RequestId>
</DeleteUserAttackSurfaceRecordsResponse>
```

JSON 格式

```
{
  "RequestId":"E345DD9F-3800-42DC-8E8E-47C57888373C"
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 7.9. DescribeOrgInfo

调用DescribeOrgInfo获取企业组织机构信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称     | 类型      | 是否必选 | 示例值             | 描述                                  |
|--------|---------|------|-----------------|-------------------------------------|
| Action | String  | 是    | DescribeOrgInfo | 要执行的操作。取值： <b>DescribeOrgInfo</b> 。 |
| OrgId  | Integer | 否    | 1               | 企业组织ID。                             |

返回数据

| 名称          | 类型      | 示例值                                  | 描述         |
|-------------|---------|--------------------------------------|------------|
| AliUid      | Long    | 11111111111111                       | 用户UID。     |
| CreatedAt   | Long    | 1557369649000                        | 公司创建的时间。   |
| Description | String  | 中国知名云计算有限公司                          | 组织机构描述信息。  |
| Name        | String  | 阿里云计算有限公司                            | 组织机构名称     |
| OrgId       | Integer | 1                                    | 企业组织ID。    |
| RequestId   | String  | 1F5F356A-D2F1-4AFD-886A-086881B121C4 | 返回结果的请求ID。 |

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeOrgInfo
&<公共请求参数>
```

正常返回示例

```
XML 格式
```

```
<DescribeOrgInfoResponse>
  <code></code>
  <message></message>
  <success>true</success>
  <requestId></requestId>
  <data>
    <AliUid>1234567</AliUid>
    <Name>Foobar</Name>
    <Description>Foo Description</Description>
    <OrgId>123</OrgId>
    <CreatedAt>1557369649000</CreatedAt>
  </data>
</DescribeOrgInfoResponse>
```

JSON 格式

```
{
  "code": "",
  "message": "",
  "success": true,
  "requestId": "",
  "data": {
    "AliUid": 1234567,
    "Name": "Foobar",
    "Description": "Foo Description",
    "OrgId": 123,
    "CreatedAt": 1557369649000
  }
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

# 7.10. DescribeOrgAttackSurfaceDetails

调用DescribeOrgAttackSurfaceDetails获取组织机构攻击面详情。

## 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

## 请求参数

| 名称 | 类型 | 是否必选 | 示例值 | 描述 |
|----|----|------|-----|----|
|----|----|------|-----|----|

| 名称       | 类型      | 是否必选 | 示例值                             | 描述                                                                                                                                                                                                                                                                  |
|----------|---------|------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action   | String  | 是    | DescribeOrgAttackSurfaceDetails | 要执行的操作。取值： <b>DescribeOrgAttackSurfaceDetails</b> 。                                                                                                                                                                                                                 |
| OrgId    | Integer | 是    | 1                               | 组织机构ID。                                                                                                                                                                                                                                                             |
| RecordId | Integer | 是    | 1                               | 记录ID。                                                                                                                                                                                                                                                               |
| Source   | String  | 是    | Subdomains                      | 支持的攻击面数据源。取值： <ul style="list-style-type: none"> <li><b>Domains</b>：根域名</li> <li><b>Subdomains</b>：子域</li> <li><b>Ports</b>：端口列表</li> <li><b>Hosts</b>：主机列表</li> <li><b>DNSMap</b>：DNS解析记录</li> <li><b>WebPaths</b>：Web路径</li> <li><b>WebTechs</b>：Web应用</li> </ul> |

## 返回数据

| 名称             | 类型      | 示例值                                  | 描述            |
|----------------|---------|--------------------------------------|---------------|
| FirstScannedAt | Long    | 1585738707000                        | 攻击面第一次出现的时间。  |
| LastScannedAt  | Long    | 1585738707000                        | 攻击面最后一次出现的时间。 |
| Occurrences    | Integer | 1                                    | 攻击面出现的次数。     |
| RequestId      | String  | 338E7324-DDEF-4BCF-B560-1ED572FD64A1 | 返回结果的请求ID。    |

## 示例

### 请求示例

```
http(s)://[Endpoint]/?Action=DescribeOrgAttackSurfaceDetails
&OrgId=1
&RecordId=1
&Source=Subdomains
&<公共请求参数>
```

正常返回示例

XML 格式

```
<DescribeOrgAttackSurfaceDetailsResponse>
  <code>200</code>
  <data>
    <LastScannedAt>1585738707000</LastScannedAt>
    <FirstScannedAt>1585738707000</FirstScannedAt>
    <Occurrences>1</Occurrences>
  </data>
  <requestId>338E7324-DDEF-4BCF-B560-1ED572FD64A1</requestId>
  <success>true</success>
</DescribeOrgAttackSurfaceDetailsResponse>
```

JSON 格式

```
{
  "code": 200,
  "data": {
    "LastScannedAt": 1585738707000,
    "FirstScannedAt": 1585738707000,
    "Occurrences": 1
  },
  "requestId": "338E7324-DDEF-4BCF-B560-1ED572FD64A1",
  "success": true
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 7.11. ListOrgAttackSurfaceFacets

调用ListOrgAttackSurfaceFacets获取组织机构攻击面统计信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称     | 类型      | 是否必选 | 示例值                        | 描述                                    |
|--------|---------|------|----------------------------|---------------------------------------|
| Action | String  | 是    | ListOrgAttackSurfaceFacets | 要执行的操作。取值：ListOrgAttackSurfaceFacets。 |
| OrgId  | Integer | 否    | 1                          | 组织机构ID。                               |

返回数据

| 名称         | 类型      | 示例值                                  | 描述         |
|------------|---------|--------------------------------------|------------|
| DNSMap     | Struct  |                                      | DNS解析记录。   |
| New        | Integer | 1                                    | 新增记录数。     |
| Total      | Integer | 1                                    | 记录总数。      |
| Domains    | Struct  |                                      | 根域名。       |
| New        | Integer | 1                                    | 新增记录总数。    |
| Total      | Integer | 1                                    | 记录总数。      |
| Hosts      | Struct  |                                      | 主机列表。      |
| New        | Integer | 1                                    | 新增记录总数。    |
| Total      | Integer | 1                                    | 记录总数。      |
| Ports      | Struct  |                                      | 端口服务。      |
| New        | Integer | 1                                    | 新增记录数。     |
| Total      | Integer | 1                                    | 记录总数。      |
| RequestId  | String  | 20E9A617-74A9-48A6-88C1-8246EAE1F4F9 | 返回结果的请求ID。 |
| Subdomains | Struct  |                                      | 子域名。       |
| New        | Integer | 1                                    | 新增记录总数。    |
| Total      | Integer | 1                                    | 记录总数。      |
| WebPaths   | Struct  |                                      | Web路径。     |

| 名称       | 类型      | 示例值 | 描述      |
|----------|---------|-----|---------|
| New      | Integer | 1   | 新增记录总数。 |
| Total    | Integer | 1   | 记录总数。   |
| WebTechs | Struct  |     | Web应用。  |
| New      | Integer | 1   | 新增记录总数。 |
| Total    | Integer | 1   | 记录总数。   |

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListOrgAttackSurfaceFacets
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ListOrgAttackSurfaceFacetsResponse>
  <code>200</code>
  <data>
    <Domains>
      <New>0</New>
      <Total>0</Total>
    </Domains>
    <Hosts>
      <New>1</New>
      <Total>1</Total>
    </Hosts>
    <WebPaths>
      <New>34</New>
      <Total>34</Total>
    </WebPaths>
    <DNSMap>
      <New>1</New>
      <Total>1</Total>
    </DNSMap>
    <Ports>
      <New>12</New>
      <Total>12</Total>
    </Ports>
    <WebTechs>
      <New>6</New>
      <Total>6</Total>
    </WebTechs>
    <Subdomains>
      <New>1</New>
      <Total>1</Total>
    </Subdomains>
  </data>
  <requestId>20E9A617-74A9-48A6-88C1-8246EAE1F4F9</requestId>
  <success>true</success>
</ListOrgAttackSurfaceFacetsResponse>
```

JSON 格式

```
{
  "code": 200,
  "data": {
    "Domains": {
      "New": 0,
      "Total": 0
    },
    "Hosts": {
      "New": 1,
      "Total": 1
    },
    "WebPaths": {
      "New": 34,
      "Total": 34
    },
    "DNSMap": {
      "New": 1,
      "Total": 1
    },
    "Ports": {
      "New": 12,
      "Total": 12
    },
    "WebTechs": {
      "New": 6,
      "Total": 6
    },
    "Subdomains": {
      "New": 1,
      "Total": 1
    }
  },
  "requestId": "20E9A617-74A9-48A6-88C1-8246EAE1F4F9",
  "success": true
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 7.12. ListOrgDNSMap

调用ListOrgDNSMap获取组织机构DNS解析记录列表。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

### 请求参数

| 名称          | 类型      | 是否必选 | 示例值           | 描述                                |
|-------------|---------|------|---------------|-----------------------------------|
| Action      | String  | 是    | ListOrgDNSMap | 要执行的操作。取值： <b>ListOrgDNSMap</b> 。 |
| OrgId       | Integer | 是    | 1             | 组织机构ID。                           |
| Search      | String  | 否    | foobar        | 查询DNS解析记录列表。                      |
| CurrentPage | Integer | 否    | 1             | 返回结果的当前页码。默认值为1。                  |
| PageSize    | Integer | 否    | 10            | 返回结果列表每页显示数据条数。                   |

## 返回数据

| 名称          | 类型      | 示例值                 | 描述               |
|-------------|---------|---------------------|------------------|
| CurrentPage | Integer | 1                   | 返回结果的当前页码。默认值为1。 |
| PageSize    | Integer | 10                  | 返回结果列表每页显示数据条数。  |
| Records     | Array   |                     | 记录列表。            |
| Domain      | String  | aliyun.com          | 根域名。             |
| Id          | Integer | 1                   | 记录ID。            |
| Index       | Integer | 1                   | 索引号。             |
| OrgId       | Integer | 1                   | 组织ID。            |
| Record      | String  | 192.168.1.1         | 解析记录。            |
| Subdomain   | String  | testphp.vulnweb.com | 子域名。             |
| Type        | String  | A                   | 解析类型。            |
| UpdatedAt   | Long    | 1585737159000       | 更新时间。            |

| 名称         | 类型      | 示例值                                  | 描述         |
|------------|---------|--------------------------------------|------------|
| RequestId  | String  | 20E9A617-74A9-48A6-88C1-8246EAE1F4F9 | 返回结果的请求ID。 |
| TotalCount | Integer | 10                                   | 记录总数。      |

## 示例

### 请求示例

```
http(s)://[Endpoint]/?Action=ListOrgDNSMap
&OrgId=1
&<公共请求参数>
```

### 正常返回示例

#### XML 格式

```
<ListOrgDNSMapResponse>
  <code>200</code>
  <data>
    <TotalCount>1</TotalCount>
    <PageSize>10</PageSize>
    <CurrentPage>1</CurrentPage>
    <Records>
      <OrgId>1</OrgId>
      <Type>A</Type>
      <Subdomain>testphp.vulnweb.com</Subdomain>
      <Index>1</Index>
      <Record>192.28.50.165</Record>
      <Id>1</Id>
      <Domain>vulnweb.com</Domain>
      <UpdatedAt>1585737159000</UpdatedAt>
    </Records>
  </data>
  <requestId>35EB9EFB-82AF-438A-8DFA-94C707BF264A</requestId>
  <success>true</success>
</ListOrgDNSMapResponse>
```

#### JSON 格式

```
{
  "code": 200,
  "data": {
    "TotalCount": 1,
    "PageSize": 10,
    "CurrentPage": 1,
    "Records": [
      {
        "OrgId": 1,
        "Type": "A",
        "Subdomain": "testphp.vulnweb.com",
        "Index": 1,
        "Record": "192.28.50.165",
        "Id": 1,
        "Domain": "vulnweb.com",
        "UpdatedAt": 1585737159000
      }
    ]
  },
  "requestId": "35EB9EFB-82AF-438A-8DFA-94C707BF264A",
  "success": true
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 7.13. ListOrgDomains

调用ListOrgDomains获取组织机构域名列表。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

### 请求参数

| 名称          | 类型      | 是否必选 | 示例值            | 描述                                 |
|-------------|---------|------|----------------|------------------------------------|
| Action      | String  | 是    | ListOrgDomains | 要执行的操作。取值： <b>ListOrgDomains</b> 。 |
| OrgId       | Integer | 是    | 1              | 组织机构ID。                            |
| Search      | String  | 否    | foobar         | 查询组织机构域名列表。                        |
| CurrentPage | Integer | 否    | 1              | 返回结果的当前页码。默认值为1。                   |

| 名称       | 类型      | 是否必选 | 示例值 | 描述              |
|----------|---------|------|-----|-----------------|
| PageSize | Integer | 否    | 10  | 返回结果列表每页显示数据条数。 |

返回数据

| 名称          | 类型      | 示例值                                  | 描述               |
|-------------|---------|--------------------------------------|------------------|
| CurrentPage | Integer | 1                                    | 返回结果的当前页码。默认值为1。 |
| PageSize    | Integer | 10                                   | 返回结果列表每页显示数据条数。  |
| Records     | Array   |                                      | 记录列表。            |
| Domain      | String  | vulnweb.com                          | 根域名。             |
| Id          | Integer | 1                                    | 记录ID。            |
| Index       | Integer | 1                                    | 索引号。             |
| OrgId       | Integer | 1                                    | 组织机构ID。          |
| UpdatedAt   | Long    | 1587716346000                        | 更新时间。            |
| RequestId   | String  | B6AF2F2A-822A-41A2-85D4-E97899001944 | 返回结果的请求ID。       |
| TotalCount  | Integer | 10                                   | 记录总数。            |

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListOrgDomains
&OrgId=1
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ListOrgDomainsResponse>
  <code>200</code>
  <data>
    <TotalCount>1</TotalCount>
    <PageSize>10</PageSize>
    <CurrentPage>1</CurrentPage>
    <Records>
      <OrgId>1</OrgId>
      <Index>1</Index>
      <Id>12</Id>
      <Domain>vulnweb.com</Domain>
      <UpdatedAt>1587716346000</UpdatedAt>
    </Records>
  </data>
  <requestId>B6AF2F2A-822A-41A2-85D4-E97899001944</requestId>
  <success>true</success>
</ListOrgDomainsResponse>
```

#### JSON 格式

```
{
  "code": 200,
  "data": {
    "TotalCount": 1,
    "PageSize": 10,
    "CurrentPage": 1,
    "Records": [
      {
        "OrgId": 1,
        "Index": 1,
        "Id": 12,
        "Domain": "vulnweb.com",
        "UpdatedAt": 1587716346000
      }
    ]
  },
  "requestId": "B6AF2F2A-822A-41A2-85D4-E97899001944",
  "success": true
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 7.14. ListOrgHosts

调用ListOrgHosts获取组织机构主机列表。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称          | 类型      | 是否必选 | 示例值          | 描述                                 |
|-------------|---------|------|--------------|------------------------------------|
| Action      | String  | 是    | ListOrgHosts | 要执行的操作。取值：ListOrgHosts。            |
| OrgId       | Integer | 是    | 1            | 组织机构ID。                            |
| Search      | String  | 否    | foobar       | 查询组织机构主机列表。                        |
| CurrentPage | Integer | 否    | 1            | 指定返回结果的当前页码。<br>默认值为1。             |
| PageSize    | Integer | 否    | 10           | 指定列表每页显示数据条数。<br>默认值为10，可设置值最大为10。 |

返回数据

| 名称          | 类型      | 示例值           | 描述                                 |
|-------------|---------|---------------|------------------------------------|
| CurrentPage | Integer | 1             | 指定返回结果的当前页码。<br>默认值为1。             |
| PageSize    | Integer | 10            | 指定列表每页显示数据条数。<br>默认值为10，可设置值最大为10。 |
| Records     | Array   |               | 记录列表。                              |
| Hostname    | String  | guest         | 主机名。                               |
| IP          | String  | 176.28.50.165 | IP地址。                              |
| Id          | Integer | 1             | 记录ID。                              |
| Index       | Integer | 1             | 索引号。                               |
| OS          | String  | windows       | 操作系统。                              |

| 名称         | 类型      | 示例值                                  | 描述         |
|------------|---------|--------------------------------------|------------|
| OrgId      | Integer | 1                                    | 组织机构ID。    |
| State      | String  | up                                   | 主机状态。      |
| UpdatedAt  | Long    | 1585738707000                        | 更新时间。      |
| RequestId  | String  | 2AF23E43-BFF9-4A36-8B4F-B354B806B08B | 返回结果的请求ID。 |
| TotalCount | Integer | 1                                    | 记录总数。      |

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListOrgHosts
&OrgId=1
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ListOrgHostsResponse>
  <code>200</code>
  <data>
    <TotalCount>1</TotalCount>
    <PageSize>10</PageSize>
    <CurrentPage>1</CurrentPage>
    <Records>
      <OrgId>1</OrgId>
      <OS>Linux 2.6.31 - 2.6.35</OS>
      <State>up</State>
      <IP>192.28.50.165</IP>
      <Hostname></Hostname>
      <Index>1</Index>
      <Id>1</Id>
      <UpdatedAt>1585738707000</UpdatedAt>
    </Records>
  </data>
  <requestId>2AF23E43-BFF9-4A36-8B4F-B354B806B08B</requestId>
  <success>true</success>
</ListOrgHostsResponse>
```

JSON 格式

```
{
  "code": 200,
  "data": {
    "TotalCount": 1,
    "PageSize": 10,
    "CurrentPage": 1,
    "Records": [
      {
        "OrgId": 1,
        "OS": "Linux 2.6.31 - 2.6.35",
        "State": "up",
        "IP": "192.28.50.165",
        "Hostname": "",
        "Index": 1,
        "Id": 1,
        "UpdatedAt": 1585738707000
      }
    ]
  },
  "requestId": "2AF23E43-BFF9-4A36-8B4F-B354B806B08B",
  "success": true
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 7.15. ListOrgPorts

调用ListOrgPorts获取组织机构端口列表。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称          | 类型      | 是否必选 | 示例值          | 描述                      |
|-------------|---------|------|--------------|-------------------------|
| Action      | String  | 是    | ListOrgPorts | 要执行的操作。取值：ListOrgPorts。 |
| OrgId       | Integer | 是    | 1            | 组织机构ID。                 |
| Search      | String  | 否    | foobar       | 查询组织机构端口列表。             |
| CurrentPage | Integer | 否    | 1            | 指定返回结果的当前页码。<br>默认值为1。  |

| 名称       | 类型      | 是否必选 | 示例值 | 描述                                 |
|----------|---------|------|-----|------------------------------------|
| PageSize | Integer | 否    | 10  | 指定列表每页显示数据条数。<br>默认值为10，可设置值最大为10。 |

返回数据

| 名称          | 类型      | 示例值           | 描述                                 |
|-------------|---------|---------------|------------------------------------|
| CurrentPage | Integer | 1             | 指定返回结果的当前页码。<br>默认值为1。             |
| PageSize    | Integer | 10            | 指定列表每页显示数据条数。<br>默认值为10，可设置值最大为10。 |
| Records     | Array   |               | 记录列表。                              |
| Fingerprint | String  | foobar        | 端口指纹记录。                            |
| IP          | String  | 192.168.1.1   | IP地址。                              |
| Id          | Integer | 1             | 记录ID。                              |
| Index       | Integer | 1             | 索引号。                               |
| OrgId       | Integer | 1             | 组织机构ID。                            |
| Port        | Integer | 80            | 端口号。                               |
| Product     | String  | Apache Httpd  | 产品名称。                              |
| Protocol    | String  | tcp           | 协议。                                |
| Service     | String  | http          | 服务。                                |
| UpdatedAt   | Long    | 1585738707000 | 更新时间。                              |

| 名称         | 类型      | 示例值                                  | 描述         |
|------------|---------|--------------------------------------|------------|
| Version    | String  | 1.2                                  | 版本号。       |
| RequestId  | String  | F4A5123A-E926-4B83-8C62-62A9490163D3 | 返回结果的请求ID。 |
| TotalCount | Integer | 10                                   | 总数。        |

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListOrgPorts
&OrgId=1
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ListOrgPortsResponse>
  <code>200</code>
  <data>
    <TotalCount>12</TotalCount>
    <PageSize>10</PageSize>
    <CurrentPage>1</CurrentPage>
    <Records>
      <OrgId>1</OrgId>
      <Fingerprint></Fingerprint>
      <Version>1.3.3e</Version>
      <IP>192.28.50.165</IP>
      <Port>21</Port>
      <Service>ftp</Service>
      <Product>ProFTPD</Product>
      <Index>1</Index>
      <Id>1</Id>
      <Protocol>tcp</Protocol>
      <UpdatedAt>1585738707000</UpdatedAt>
    </Records>
    <Records>
      <OrgId>1</OrgId>
      <Fingerprint></Fingerprint>
      <Version>5.3p1 Debian 3ubuntu7.1</Version>
      <IP>192.28.50.165</IP>
      <Port>22</Port>
      <Service>ssh</Service>
      <Product>OpenSSH</Product>
      <Index>2</Index>
      <Id>2</Id>
      <Protocol>tcp</Protocol>
```

```
<UpdatedAt>1585738707000</UpdatedAt>
</Records>
<Records>
  <OrgId>1</OrgId>
  <Fingerprint></Fingerprint>
  <Version></Version>
  <IP>192.28.50.165</IP>
  <Port>53</Port>
  <Service>domain</Service>
  <Product></Product>
  <Index>3</Index>
  <Id>3</Id>
  <Protocol>tcp</Protocol>
  <UpdatedAt>1585738707000</UpdatedAt>
</Records>
<Records>
  <OrgId>1</OrgId>
  <Fingerprint></Fingerprint>
  <Version>1.4.1</Version>
  <IP>192.28.50.165</IP>
  <Port>80</Port>
  <Service>http</Service>
  <Product>nginx</Product>
  <Index>4</Index>
  <Id>4</Id>
  <Protocol>tcp</Protocol>
  <UpdatedAt>1585738707000</UpdatedAt>
</Records>
<Records>
  <OrgId>1</OrgId>
  <Fingerprint></Fingerprint>
  <Version></Version>
  <IP>192.28.50.165</IP>
  <Port>106</Port>
  <Service>pop3pw</Service>
  <Product>poppassd</Product>
  <Index>5</Index>
  <Id>5</Id>
  <Protocol>tcp</Protocol>
  <UpdatedAt>1585738707000</UpdatedAt>
</Records>
<Records>
  <OrgId>1</OrgId>
  <Fingerprint></Fingerprint>
  <Version></Version>
  <IP>192.28.50.165</IP>
  <Port>110</Port>
  <Service>pop3</Service>
  <Product>Courier pop3d</Product>
  <Index>6</Index>
  <Id>6</Id>
  <Protocol>tcp</Protocol>
  <UpdatedAt>1585738707000</UpdatedAt>
</Records>
```

```
<Records>
  <OrgId>1</OrgId>
  <Fingerprint></Fingerprint>
  <Version></Version>
  <IP>192.28.50.165</IP>
  <Port>143</Port>
  <Service>imap</Service>
  <Product>Plesk Courier imapd</Product>
  <Index>7</Index>
  <Id>7</Id>
  <Protocol>tcp</Protocol>
  <UpdatedAt>1585738707000</UpdatedAt>
</Records>
<Records>
  <OrgId>1</OrgId>
  <Fingerprint></Fingerprint>
  <Version></Version>
  <IP>192.28.50.165</IP>
  <Port>465</Port>
  <Service>smtp</Service>
  <Product>Postfix smtpd</Product>
  <Index>8</Index>
  <Id>8</Id>
  <Protocol>tcp</Protocol>
  <UpdatedAt>1585738707000</UpdatedAt>
</Records>
<Records>
  <OrgId>1</OrgId>
  <Fingerprint></Fingerprint>
  <Version></Version>
  <IP>192.28.50.165</IP>
  <Port>993</Port>
  <Service>imap</Service>
  <Product>Plesk Courier imapd</Product>
  <Index>9</Index>
  <Id>9</Id>
  <Protocol>tcp</Protocol>
  <UpdatedAt>1585738707000</UpdatedAt>
</Records>
<Records>
  <OrgId>1</OrgId>
  <Fingerprint></Fingerprint>
  <Version></Version>
  <IP>192.28.50.165</IP>
  <Port>995</Port>
  <Service>pop3</Service>
  <Product>Courier pop3d</Product>
  <Index>10</Index>
  <Id>10</Id>
  <Protocol>tcp</Protocol>
  <UpdatedAt>1585738707000</UpdatedAt>
</Records>
</data>
<requestId>F4A5123A-E926-4B83-8C62-62A9490163D3</requestId>
```

```
<success>true</success>
</ListOrgPortsResponse>
```

#### JSON 格式

```
{
  "code": 200,
  "data": {
    "TotalCount": 12,
    "PageSize": 10,
    "CurrentPage": 1,
    "Records": [
      {
        "OrgId": 1,
        "Fingerprint": "",
        "Version": "1.3.3e",
        "IP": "192.28.50.165",
        "Port": 21,
        "Service": "ftp",
        "Product": "ProFTPD",
        "Index": 1,
        "Id": 1,
        "Protocol": "tcp",
        "UpdatedAt": 1585738707000
      },
      {
        "OrgId": 1,
        "Fingerprint": "",
        "Version": "5.3p1 Debian 3ubuntu7.1",
        "IP": "192.28.50.165",
        "Port": 22,
        "Service": "ssh",
        "Product": "OpenSSH",
        "Index": 2,
        "Id": 2,
        "Protocol": "tcp",
        "UpdatedAt": 1585738707000
      },
      {
        "OrgId": 1,
        "Fingerprint": "",
        "Version": "",
        "IP": "192.28.50.165",
        "Port": 53,
        "Service": "domain",
        "Product": "",
        "Index": 3,
        "Id": 3,
        "Protocol": "tcp",
        "UpdatedAt": 1585738707000
      },
      {
        "OrgId": 1,
        "Fingerprint": "",
```

```
"Version": "1.4.1",
"IP": "192.28.50.165",
"Port": 80,
"Service": "http",
"Product": "nginx",
"Index": 4,
"Id": 4,
"Protocol": "tcp",
"UpdatedAt": 1585738707000
},
{
  "OrgId": 1,
  "Fingerprint": "",
  "Version": "",
  "IP": "192.28.50.165",
  "Port": 106,
  "Service": "pop3pw",
  "Product": "poppassd",
  "Index": 5,
  "Id": 5,
  "Protocol": "tcp",
  "UpdatedAt": 1585738707000
},
{
  "OrgId": 1,
  "Fingerprint": "",
  "Version": "",
  "IP": "192.28.50.165",
  "Port": 110,
  "Service": "pop3",
  "Product": "Courier pop3d",
  "Index": 6,
  "Id": 6,
  "Protocol": "tcp",
  "UpdatedAt": 1585738707000
},
{
  "OrgId": 1,
  "Fingerprint": "",
  "Version": "",
  "IP": "192.28.50.165",
  "Port": 143,
  "Service": "imap",
  "Product": "Plesk Courier imapd",
  "Index": 7,
  "Id": 7,
  "Protocol": "tcp",
  "UpdatedAt": 1585738707000
},
{
  "OrgId": 1,
  "Fingerprint": "",
  "Version": "",
  "IP": "192.28.50.165",
```

```
"Port": 465,
"Service": "smtp",
"Product": "Postfix smtpd",
"Index": 8,
"Id": 8,
"Protocol": "tcp",
"UpdatedAt": 1585738707000
},
{
  "OrgId": 1,
  "Fingerprint": "",
  "Version": "",
  "IP": "192.28.50.165",
  "Port": 993,
  "Service": "imap",
  "Product": "Plesk Courier imapd",
  "Index": 9,
  "Id": 9,
  "Protocol": "tcp",
  "UpdatedAt": 1585738707000
},
{
  "OrgId": 1,
  "Fingerprint": "",
  "Version": "",
  "IP": "192.28.50.165",
  "Port": 995,
  "Service": "pop3",
  "Product": "Courier pop3d",
  "Index": 10,
  "Id": 10,
  "Protocol": "tcp",
  "UpdatedAt": 1585738707000
}
],
"requestId": "F4A5123A-E926-4B83-8C62-62A9490163D3",
"success": true
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 7.16. ListOrgRiskyAssets

调用ListOrgRiskyAssets获取组织机构风险资产。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称     | 类型      | 是否必选 | 示例值                | 描述                            |
|--------|---------|------|--------------------|-------------------------------|
| Action | String  | 是    | ListOrgRiskyAssets | 要执行的操作。取值：ListOrgRiskyAssets。 |
| OrgId  | Integer | 否    | 1                  | 企业组织ID。                       |

返回数据

| 名称          | 类型      | 示例值                                  | 描述                  |
|-------------|---------|--------------------------------------|---------------------|
| Assets      | Array   |                                      | 资产列表。               |
| Asset       | String  | testphp.vulnweb.com                  | 资产名称。               |
| Count       | Integer | 10                                   | 风险资产数量。             |
| Type        | String  | Domain                               | 资产类型。               |
| CurrentPage | Integer | 1                                    | 当前页，默认值为1。          |
| PageSize    | Integer | 10                                   | 页面大小，默认值为10，最大值为10。 |
| RequestId   | String  | 13B841A7-F5B4-49D6-A9D1-210D5C8E69BF | 返回结果请求ID。           |
| Total       | Integer | 39                                   | 返回结果总数。             |
| TotalCount  | Integer | 2                                    | 资产总数。               |

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListOrgRiskyAssets
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ListOrgRiskyAssetsResponse>
  <code></code>
  <message></message>
  <success>true</success>
  <data>
    <Total>10</Total>
    <Assets>
      <Asset>1.2.3.4</Asset>
      <Type>Host</Type>
      <Count>123</Count>
    </Assets>
    <Assets>
      <Asset>foo.com</Asset>
      <Type>Domain</Type>
      <Count>123</Count>
    </Assets>
    <Assets>
      <Asset>bar.com</Asset>
      <Type>Domain</Type>
      <Count>123</Count>
    </Assets>
    <CurrentPage>1</CurrentPage>
    <PageSize>10</PageSize>
    <TotalCount>10</TotalCount>
  </data>
</ListOrgRiskyAssetsResponse>
```

JSON 格式

```
{
  "code": "",
  "message": "",
  "success": true,
  "data": {
    "Total": 123,
    "Assets": [
      {
        "Asset": "1.2.3.4",
        "Type": "Host",
        "Count": 123
      },
      {
        "Asset": "foo.com",
        "Type": "Domain",
        "Count": 123
      },
      {
        "Asset": "bar.com",
        "Type": "Domain",
        "Count": 123
      }
    ],
    "Total": 10,
    "CurrentPage": 1,
    "PageSize": 10,
    "TotalCount": 10
  }
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 7.17. ListOrgSubdomains

调用ListOrgSubdomains获取组织机构子域名列表。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称     | 类型      | 是否必选 | 示例值               | 描述                           |
|--------|---------|------|-------------------|------------------------------|
| Action | String  | 是    | ListOrgSubdomains | 要执行的操作。取值：ListOrgSubdomains。 |
| OrgId  | Integer | 是    | 1                 | 组织机构ID。                      |

| 名称          | 类型      | 是否必选 | 示例值    | 描述                                 |
|-------------|---------|------|--------|------------------------------------|
| Search      | String  | 否    | foobar | 查询组织机构子域名列表。                       |
| CurrentPage | Integer | 否    | 1      | 指定返回结果的当前页码。<br>默认值为1。             |
| PageSize    | Integer | 否    | 10     | 指定列表每页显示数据条数。<br>默认值为10，可设置值最大为10。 |

返回数据

| 名称          | 类型      | 示例值                                 | 描述                                 |
|-------------|---------|-------------------------------------|------------------------------------|
| CurrentPage | Integer | 1                                   | 指定返回结果的当前页码。<br>默认值为1。             |
| PageSize    | Integer | 10                                  | 指定列表每页显示数据条数。<br>默认值为10，可设置值最大为10。 |
| Records     | Array   |                                     | 记录列表。                              |
| Domain      | String  | aliyun.com                          | 根域名。                               |
| Id          | Integer | 1                                   | 记录ID。                              |
| Index       | Integer | 1                                   | 索引号。                               |
| OrgId       | Integer | 1                                   | 组织机构ID。                            |
| Subdomain   | String  | testphp.vulnweb.com                 | 子域名。                               |
| UpdatedAt   | Long    | 1585737153000                       | 更新时间。                              |
| RequestId   | String  | F4A5123A-E926-4B83-8C62-62A9490163D | 返回结果的请求ID。                         |

| 名称         | 类型      | 示例值 | 描述  |
|------------|---------|-----|-----|
| TotalCount | Integer | 10  | 总数。 |

## 示例

### 请求示例

```
http(s)://[Endpoint]/?Action=ListOrgSubdomains
&OrgId=1
&<公共请求参数>
```

### 正常返回示例

#### XML 格式

```
<ListOrgSubdomainsResponse>
  <code>200</code>
  <data>
    <TotalCount>1</TotalCount>
    <PageSize>10</PageSize>
    <CurrentPage>1</CurrentPage>
    <Records>
      <OrgId>1</OrgId>
      <Subdomain>testphp.vulnweb.com</Subdomain>
      <Index>1</Index>
      <Id>1</Id>
      <Domain>vulnweb.com</Domain>
      <UpdatedAt>1585737153000</UpdatedAt>
    </Records>
  </data>
  <requestId>ADE203B0-24F9-487E-AB36-671AB90FDC2E</requestId>
  <success>true</success>
</ListOrgSubdomainsResponse>
```

#### JSON 格式

```
{
  "code": 200,
  "data": {
    "TotalCount": 1,
    "PageSize": 10,
    "CurrentPage": 1,
    "Records": [
      {
        "OrgId": 1,
        "Subdomain": "testphp.vulnweb.com",
        "Index": 1,
        "Id": 1,
        "Domain": "vulnweb.com",
        "UpdatedAt": 1585737153000
      }
    ]
  },
  "requestId": "ADE203B0-24F9-487E-AB36-671AB90FDC2E",
  "success": true
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

# 7.18. ListOrgVulFacets

调用ListOrgVulFacets获取组织机构资产风险信息。

## 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

## 请求参数

| 名称          | 类型      | 是否必选 | 示例值              | 描述                                   |
|-------------|---------|------|------------------|--------------------------------------|
| Action      | String  | 是    | ListOrgVulFacets | 要执行的操作。取值： <b>ListOrgVulFacets</b> 。 |
| OrgId       | Integer | 否    | 1                | 组织机构ID。                              |
| Asset       | String  | 否    | www.aliyun.com   | 资产。                                  |
| CurrentPage | Integer | 否    | 1                | 指定返回结果的当前页码。<br>默认值为1。               |

| 名称       | 类型      | 是否必选 | 示例值 | 描述                                                                                     |
|----------|---------|------|-----|----------------------------------------------------------------------------------------|
| Lang     | String  | 否    | en  | 指定请求和接收消息的语言类型。取值： <ul style="list-style-type: none"><li>zh：中文</li><li>en：英文</li></ul> |
| PageSize | Integer | 否    | 10  | 指定列表每页显示数据条数。<br>默认值为10，可设置值最大为10。                                                     |

返回数据

| 名称             | 类型      | 示例值                                  | 描述                                 |
|----------------|---------|--------------------------------------|------------------------------------|
| CurrentPage    | Integer | 1                                    | 指定返回结果的当前页码。<br>默认值为1。             |
| PageSize       | Integer | 10                                   | 指定列表每页显示数据条数。<br>默认值为10，可设置值最大为10。 |
| RequestId      | String  | 14B0B62A-72C5-44E0-866D-55817A31353A | 返回结果的请求ID。                         |
| Total          | Integer | 10                                   | 总数。                                |
| TotalCount     | Integer | 17                                   | 资产总数。                              |
| Vuls           | Array   |                                      | 漏洞总数。                              |
| Classification | String  | SQL注入                                | 漏洞类别。                              |
| Count          | Integer | 7                                    | 漏洞个数。                              |
| Index          | Integer | 1                                    | 索引号。                               |
| ModuleID       | Integer | 1                                    | 模块ID。                              |
| Name           | String  | SQL 注入漏洞                             | 漏洞名称。                              |

| 名称       | 类型     | 示例值  | 描述                                                                                                                                                    |
|----------|--------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Severity | String | High | 漏洞等级。取值： <ul style="list-style-type: none"><li>• <b>High</b>：高危</li><li>• <b>Medium</b>：中危</li><li>• <b>Low</b>：低危</li><li>• <b>Info</b>：信息</li></ul> |

示例

请求示例

http(s)://[Endpoint]/?Action=ListOrgVulFacets  
&<公共请求参数>

正常返回示例

XML 格式

```
<ListOrgVulFacetsResponse>
  <code>200</code>
  <data>
    <TotalCount>17</TotalCount>
    <PageSize>10</PageSize>
    <CurrentPage>1</CurrentPage>
    <Vuls>
      <ModuleID>98</ModuleID>
      <Classification>SQL注入</Classification>
      <Index>1</Index>
      <Severity>High</Severity>
      <Count>7</Count>
      <Name>SQL 注入漏洞</Name>
    </Vuls>
    <Vuls>
      <ModuleID>2308</ModuleID>
      <Classification>SQL注入</Classification>
      <Index>2</Index>
      <Severity>High</Severity>
      <Count>1</Count>
      <Name>SQL报错注入</Name>
    </Vuls>
    <Vuls>
      <ModuleID>116</ModuleID>
      <Classification>敏感信息泄露</Classification>
      <Index>3</Index>
      <Severity>High</Severity>
      <Count>1</Count>
      <Name>备份文件压缩包下载</Name>
    </Vuls>
    <Vuls>
      <ModuleID>2045</ModuleID>
      <Classification></Classification>
```

```
<Index>4</Index>
<Severity>High</Severity>
<Count>1</Count>
<Name>Web 应用配置不当导致源码泄露</Name>
</Vuls>
<Vuls>
  <ModuleID>894</ModuleID>
  <Classification>服务器端请求伪造</Classification>
  <Index>5</Index>
  <Severity>High</Severity>
  <Count>1</Count>
  <Name>服务端伪造请求</Name>
</Vuls>
<Vuls>
  <ModuleID>2068</ModuleID>
  <Classification></Classification>
  <Index>6</Index>
  <Severity>High</Severity>
  <Count>1</Count>
  <Name>Macromedia Dreamweaver远程数据库脚本</Name>
</Vuls>
<Vuls>
  <ModuleID>2311</ModuleID>
  <Classification>跨站点脚本（反射型）</Classification>
  <Index>7</Index>
  <Severity>Medium</Severity>
  <Count>7</Count>
  <Name>跨站脚本攻击漏洞（XSS）</Name>
</Vuls>
<Vuls>
  <ModuleID>1074</ModuleID>
  <Classification>敏感信息泄露</Classification>
  <Index>8</Index>
  <Severity>Medium</Severity>
  <Count>7</Count>
  <Name>目录开放可访问</Name>
</Vuls>
<Vuls>
  <ModuleID>2019</ModuleID>
  <Classification></Classification>
  <Index>9</Index>
  <Severity>Medium</Severity>
  <Count>1</Count>
  <Name>Nginx SPDY 堆缓冲区溢出漏洞 CVE-2014-0133</Name>
</Vuls>
<Vuls>
  <ModuleID>118</ModuleID>
  <Classification>敏感信息泄露</Classification>
  <Index>10</Index>
  <Severity>Medium</Severity>
  <Count>1</Count>
  <Name>phpinfo文件泄露服务器信息</Name>
</Vuls>
</data>
```

```
<requestId>14B0B62A-72C5-44E0-866D-55817A31353A</requestId>
<success>true</success>
</ListOrgVulFacetsResponse>
```

#### JSON 格式

```
{
  "code": 200,
  "data": {
    "TotalCount": 17,
    "PageSize": 10,
    "CurrentPage": 1,
    "Vuls": [
      {
        "ModuleID": 98,
        "Classification": "SQL注入",
        "Index": 1,
        "Severity": "High",
        "Count": 7,
        "Name": "SQL 注入漏洞"
      },
      {
        "ModuleID": 2308,
        "Classification": "SQL注入",
        "Index": 2,
        "Severity": "High",
        "Count": 1,
        "Name": "SQL报错注入"
      },
      {
        "ModuleID": 116,
        "Classification": "敏感信息泄露",
        "Index": 3,
        "Severity": "High",
        "Count": 1,
        "Name": "备份文件压缩包下载"
      },
      {
        "ModuleID": 2045,
        "Classification": "",
        "Index": 4,
        "Severity": "High",
        "Count": 1,
        "Name": "Web 应用配置不当导致源码泄露"
      },
      {
        "ModuleID": 894,
        "Classification": "服务器端请求伪造",
        "Index": 5,
        "Severity": "High",
        "Count": 1,
        "Name": "服务端伪造请求"
      }
    ]
  }
}
```

```
{
  "ModuleID": 2068,
  "Classification": "",
  "Index": 6,
  "Severity": "High",
  "Count": 1,
  "Name": "Macromedia Dreamweaver远程数据库脚本"
},
{
  "ModuleID": 2311,
  "Classification": "跨站点脚本（反射型）",
  "Index": 7,
  "Severity": "Medium",
  "Count": 7,
  "Name": "跨站脚本攻击漏洞（XSS）"
},
{
  "ModuleID": 1074,
  "Classification": "敏感信息泄露",
  "Index": 8,
  "Severity": "Medium",
  "Count": 7,
  "Name": "目录开放可访问"
},
{
  "ModuleID": 2019,
  "Classification": "",
  "Index": 9,
  "Severity": "Medium",
  "Count": 1,
  "Name": "Nginx SPDY 堆缓冲区溢出漏洞 CVE-2014-0133"
},
{
  "ModuleID": 118,
  "Classification": "敏感信息泄露",
  "Index": 10,
  "Severity": "Medium",
  "Count": 1,
  "Name": "phpinfo文件泄露服务器信息"
}
],
"requestId": "14B0B62A-72C5-44E0-866D-55817A31353A",
"success": true
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 7.19. ListOrgWebPaths

调用ListOrgWebPaths获取组织机构的Web路径。

## 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

## 请求参数

| 名称          | 类型      | 是否必选 | 示例值             | 描述                                  |
|-------------|---------|------|-----------------|-------------------------------------|
| Action      | String  | 是    | ListOrgWebPaths | 要执行的操作。取值： <b>ListOrgWebPaths</b> 。 |
| OrgId       | Integer | 是    | 1               | 组织机构ID。                             |
| Search      | String  | 否    | foobar          | 查询组织机构的Web路径。                       |
| CurrentPage | Integer | 否    | 1               | 指定返回结果的当前页码。<br>默认值为1。              |
| PageSize    | Integer | 否    | 10              | 指定列表每页显示数据条数。<br>默认值为10，可设置值最大为10。  |

## 返回数据

| 名称          | 类型      | 示例值 | 描述                                 |
|-------------|---------|-----|------------------------------------|
| CurrentPage | Integer | 1   | 指定返回结果的当前页码。<br>默认值为1。             |
| PageSize    | Integer | 10  | 指定列表每页显示数据条数。<br>默认值为10，可设置值最大为10。 |
| Records     | Array   |     | 记录列表。                              |
| Id          | Integer | 1   | 记录ID。                              |
| Index       | Integer | 2   | 索引号。                               |
| OrgId       | Integer | 1   | 组织机构ID。                            |

| 名称         | 类型      | 示例值                                              | 描述         |
|------------|---------|--------------------------------------------------|------------|
| Path       | String  | foobar.php                                       | 路径名称。      |
| Site       | String  | https://www.aliyun.com/price/product#/ecs/detail | 站点。        |
| UpdatedAt  | Long    | 1585745428000                                    | 更新时间。      |
| RequestId  | String  | 325C5AD1-33F6-4AE7-A17F-80CE9C910950             | 返回结果的请求ID。 |
| TotalCount | Integer | 20                                               | 记录总数。      |

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListOrgWebPaths
&OrgId=1
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ListOrgWebPathsResponse>
  <code>200</code>
  <data>
    <TotalCount>34</TotalCount>
    <PageSize>10</PageSize>
    <CurrentPage>1</CurrentPage>
    <Records>
      <Site>https://www.aliyun.com/</Site>
      <Path>/foobar.php</Path>
      <OrgId>1</OrgId>
      <Index>1</Index>
      <Id>37</Id>
      <UpdatedAt>1585745428000</UpdatedAt>
    </Records>
    <Records>
      <Site>http://192.28.50.165:8443</Site>
      <Path>/</Path>
      <OrgId>1</OrgId>
      <Index>2</Index>
      <Id>1</Id>
      <UpdatedAt>1585739394000</UpdatedAt>
    </Records>
  </data>
</ListOrgWebPathsResponse>
```

```
<Site>http://192.28.50.165:8880</Site>
<Path>/</Path>
<OrgId>1</OrgId>
<Index>3</Index>
<Id>2</Id>
<UpdatedAt>1585739394000</UpdatedAt>
</Records>
<Records>
  <Site>https://www.aliyun.com/</Site>
  <Path>/</Path>
  <OrgId>1</OrgId>
  <Index>4</Index>
  <Id>3</Id>
  <UpdatedAt>1585739394000</UpdatedAt>
</Records>
<Records>
  <Site>https://www.aliyun.com/</Site>
  <Path>/.idea/</Path>
  <OrgId>1</OrgId>
  <Index>5</Index>
  <Id>4</Id>
  <UpdatedAt>1585739394000</UpdatedAt>
</Records>
<Records>
  <Site>https://www.aliyun.com/</Site>
  <Path>/admin/</Path>
  <OrgId>1</OrgId>
  <Index>6</Index>
  <Id>5</Id>
  <UpdatedAt>1585739394000</UpdatedAt>
</Records>
<Records>
  <Site>https://www.aliyun.com/</Site>
  <Path>/AJAX/titles.php</Path>
  <OrgId>1</OrgId>
  <Index>7</Index>
  <Id>6</Id>
  <UpdatedAt>1585739394000</UpdatedAt>
</Records>
<Records>
  <Site>https://www.aliyun.com/</Site>
  <Path>/artists.php</Path>
  <OrgId>1</OrgId>
  <Index>8</Index>
  <Id>7</Id>
  <UpdatedAt>1585739394000</UpdatedAt>
</Records>
<Records>
  <Site>https://www.aliyun.com/</Site>
  <Path>/cart.php</Path>
  <OrgId>1</OrgId>
  <Index>9</Index>
  <Id>8</Id>
  <UpdatedAt>1585739394000</UpdatedAt>
</Records>
```

```
</Records>
<Records>
  <Site>https://www.aliyun.com/</Site>
  <Path>/categories.php</Path>
  <OrgId>1</OrgId>
  <Index>10</Index>
  <Id>9</Id>
  <UpdatedAt>1585739394000</UpdatedAt>
</Records>
</data>
<requestId>325C5AD1-33F6-4AE7-A17F-80CE9C910950</requestId>
<success>true</success>
</ListOrgWebPathsResponse>
```

#### JSON 格式

```
{
  "code": 200,
  "data": {
    "TotalCount": 34,
    "PageSize": 10,
    "CurrentPage": 1,
    "Records": [
      {
        "Site": "https://www.aliyun.com/",
        "Path": "/foobar.php",
        "OrgId": 1,
        "Index": 1,
        "Id": 37,
        "UpdatedAt": 1585745428000
      },
      {
        "Site": "http://192.28.50.165:8443",
        "Path": "/",
        "OrgId": 1,
        "Index": 2,
        "Id": 1,
        "UpdatedAt": 1585739394000
      },
      {
        "Site": "http://192.28.50.165:8880",
        "Path": "/",
        "OrgId": 1,
        "Index": 3,
        "Id": 2,
        "UpdatedAt": 1585739394000
      },
      {
        "Site": "https://www.aliyun.com/",
        "Path": "/",
        "OrgId": 1,
        "Index": 4,
        "Id": 3,
        "UpdatedAt": 1585739394000
      }
    ]
  }
}
```

```
,
{
  "Site": "https://www.aliyun.com/",
  "Path": "/.idea/",
  "OrgId": 1,
  "Index": 5,
  "Id": 4,
  "UpdatedAt": 1585739394000
},
{
  "Site": "https://www.aliyun.com/",
  "Path": "/admin/",
  "OrgId": 1,
  "Index": 6,
  "Id": 5,
  "UpdatedAt": 1585739394000
},
{
  "Site": "https://www.aliyun.com/",
  "Path": "/AJAX/titles.php",
  "OrgId": 1,
  "Index": 7,
  "Id": 6,
  "UpdatedAt": 1585739394000
},
{
  "Site": "https://www.aliyun.com/",
  "Path": "/artists.php",
  "OrgId": 1,
  "Index": 8,
  "Id": 7,
  "UpdatedAt": 1585739394000
},
{
  "Site": "https://www.aliyun.com/",
  "Path": "/cart.php",
  "OrgId": 1,
  "Index": 9,
  "Id": 8,
  "UpdatedAt": 1585739394000
},
{
  "Site": "https://www.aliyun.com/",
  "Path": "/categories.php",
  "OrgId": 1,
  "Index": 10,
  "Id": 9,
  "UpdatedAt": 1585739394000
}
]
},
"requestId": "325C5AD1-33F6-4AE7-A17F-80CE9C910950",
"success": true
}
```

错误码

访问[错误中心](#)查看更多错误码。

7.20. ListOrgWebTechs

调用ListOrgWebTechs获取组织机构的Web应用列表。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称          | 类型      | 是否必选 | 示例值             | 描述                                  |
|-------------|---------|------|-----------------|-------------------------------------|
| Action      | String  | 是    | ListOrgWebTechs | 要执行的操作。取值： <b>ListOrgWebTechs</b> 。 |
| OrgId       | Integer | 是    | 1               | 组织机构ID。                             |
| Search      | String  | 否    | foobar          | 搜索组织机构的Web应用列表。                     |
| CurrentPage | Integer | 否    | 1               | 指定返回结果的当前页码。<br>默认值为1。              |
| PageSize    | Integer | 否    | 10              | 指定列表每页显示数据条数。<br>默认值为10，可设置值最大为10。  |

返回数据

| 名称          | 类型      | 示例值 | 描述                                 |
|-------------|---------|-----|------------------------------------|
| CurrentPage | Integer | 1   | 指定返回结果的当前页码。<br>默认值为1。             |
| PageSize    | Integer | 10  | 指定列表每页显示数据条数。<br>默认值为10，可设置值最大为10。 |
| Records     | Array   |     | 记录列表。                              |

| 名称         | 类型      | 示例值                                  | 描述         |
|------------|---------|--------------------------------------|------------|
| Id         | Integer | 1                                    | 记录ID。      |
| Index      | Integer | 1                                    | 索引号。       |
| Name       | String  | Nginx                                | 应用名称。      |
| OrgId      | Integer | 1                                    | 组织机构ID。    |
| PoweredBy  | String  | PHP/5.3.10-1~lucid+2uwsgi2           | 编程语言。      |
| Server     | String  | nginx/1.4.1                          | Web服务器。    |
| Title      | String  | Home of Acunetix Art                 | 标题。        |
| URL        | String  | http://testphp.vulnweb.com           | URL地址。     |
| UpdatedAt  | Long    | 1585738885000                        | 更新时间。      |
| Version    | String  | 1.4.1                                | 版本。        |
| RequestId  | String  | EB080B27-A148-4C86-A839-78986C022891 | 返回结果的请求ID。 |
| TotalCount | Integer | 20                                   | 总数。        |

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListOrgWebTechs
&OrgId=1
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ListOrgWebTechsResponse>
  <code>200</code>
  <data>
    <TotalCount>6</TotalCount>
```

```
<PageSize>10</PageSize>
<CurrentPage>1</CurrentPage>
<Records>
  <OrgId>1</OrgId>
  <PoweredBy>PHP/5.3.10-1~lucid+2uwsgi2</PoweredBy>
  <Server>nginx/1.4.1</Server>
  <Version>1.4.1</Version>
  <Title>Home of Acunetix Art</Title>
  <Index>1</Index>
  <Id>5</Id>
  <UpdatedAt>1585738885000</UpdatedAt>
  <URL>https://www.aliyun.com/</URL>
  <Name>Nginx</Name>
</Records>
<Records>
  <OrgId>1</OrgId>
  <PoweredBy>PHP/5.3.10-1~lucid+2uwsgi2</PoweredBy>
  <Server>nginx/1.4.1</Server>
  <Version></Version>
  <Title>Home of Acunetix Art</Title>
  <Index>2</Index>
  <Id>6</Id>
  <UpdatedAt>1585738885000</UpdatedAt>
  <URL>https://www.aliyun.com//admin/</URL>
  <Name>Index Of</Name>
</Records>
<Records>
  <OrgId>1</OrgId>
  <PoweredBy></PoweredBy>
  <Server>sw-cp-server</Server>
  <Version></Version>
  <Title>404 - Not Found</Title>
  <Index>3</Index>
  <Id>3</Id>
  <UpdatedAt>1585738731000</UpdatedAt>
  <URL>https://www.aliyun.com/:8443</URL>
  <Name>Plesk</Name>
</Records>
<Records>
  <OrgId>1</OrgId>
  <PoweredBy></PoweredBy>
  <Server>sw-cp-server</Server>
  <Version></Version>
  <Title>404 - Not Found</Title>
  <Index>4</Index>
  <Id>4</Id>
  <UpdatedAt>1585738731000</UpdatedAt>
  <URL>https://www.aliyun.com/:8880</URL>
  <Name>Plesk</Name>
</Records>
<Records>
  <OrgId>1</OrgId>
  <PoweredBy></PoweredBy>
  <Server>sw-cp-server</Server>
```

```
<Version></Version>
<Title>404 - Not Found</Title>
<Index>5</Index>
<Id>1</Id>
<UpdatedAt>1585738728000</UpdatedAt>
<URL>http://192.28.50.165:8443</URL>
<Name>Plesk</Name>
</Records>
<Records>
  <OrgId>1</OrgId>
  <PoweredBy></PoweredBy>
  <Server>sw-cp-server</Server>
  <Version></Version>
  <Title>404 - Not Found</Title>
  <Index>6</Index>
  <Id>2</Id>
  <UpdatedAt>1585738728000</UpdatedAt>
  <URL>http://192.28.50.165:8880</URL>
  <Name>Plesk</Name>
</Records>
</data>
<requestId>EB080B27-A148-4C86-A839-78986C022891</requestId>
<success>true</success>
</ListOrgWebTechsResponse>
```

#### JSON 格式

```
{
  "code": 200,
  "data": {
    "TotalCount": 6,
    "PageSize": 10,
    "CurrentPage": 1,
    "Records": [
      {
        "OrgId": 1,
        "PoweredBy": "PHP/5.3.10-1~lucid+2uwsgi2",
        "Server": "nginx/1.4.1",
        "Version": "1.4.1",
        "Title": "Home of Acunetix Art",
        "Index": 1,
        "Id": 5,
        "UpdatedAt": 1585738885000,
        "URL": "https://www.aliyun.com/",
        "Name": "Nginx"
      },
      {
        "OrgId": 1,
        "PoweredBy": "PHP/5.3.10-1~lucid+2uwsgi2",
        "Server": "nginx/1.4.1",
        "Version": "",
        "Title": "Home of Acunetix Art",
        "Index": 2,
        "Id": 6.
      }
    ]
  }
}
```

```
    "UpdatedAt": 1585738885000,  
    "URL": "https://www.aliyun.com//admin/",  
    "Name": "Index Of"  
  },  
  {  
    "OrgId": 1,  
    "PoweredBy": "",  
    "Server": "sw-cp-server",  
    "Version": "",  
    "Title": "404 - Not Found",  
    "Index": 3,  
    "Id": 3,  
    "UpdatedAt": 1585738731000,  
    "URL": "https://www.aliyun.com/:8443",  
    "Name": "Plesk"  
  },  
  {  
    "OrgId": 1,  
    "PoweredBy": "",  
    "Server": "sw-cp-server",  
    "Version": "",  
    "Title": "404 - Not Found",  
    "Index": 4,  
    "Id": 4,  
    "UpdatedAt": 1585738731000,  
    "URL": "https://www.aliyun.com/:8880",  
    "Name": "Plesk"  
  },  
  {  
    "OrgId": 1,  
    "PoweredBy": "",  
    "Server": "sw-cp-server",  
    "Version": "",  
    "Title": "404 - Not Found",  
    "Index": 5,  
    "Id": 1,  
    "UpdatedAt": 1585738728000,  
    "URL": "http://192.28.50.165:8443",  
    "Name": "Plesk"  
  },  
  {  
    "OrgId": 1,  
    "PoweredBy": "",  
    "Server": "sw-cp-server",  
    "Version": "",  
    "Title": "404 - Not Found",  
    "Index": 6,  
    "Id": 2,  
    "UpdatedAt": 1585738728000,  
    "URL": "http://192.28.50.165:8880",  
    "Name": "Plesk"  
  }  
]  
},
```

```
"requestId": "EB080B27-A148-4C86-A839-78986C022891",
"success": true
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 7.21. ListUserAttackSurfaceFacets

调用ListUserAttackSurfaceFacets获取您资产的攻击面统计信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称     | 类型     | 是否必选 | 示例值                         | 描述                                      |
|--------|--------|------|-----------------------------|-----------------------------------------|
| Action | String | 是    | ListUserAttackSurfaceFacets | 需要执行的操作。取值：ListUserAttackSurfaceFacets。 |

返回数据

| 名称      | 类型      | 示例值 | 描述            |
|---------|---------|-----|---------------|
| DNSMap  | Struct  |     | 资产的DNS解析记录。   |
| New     | Integer | 10  | 新增DNS解析记录的数量。 |
| Total   | Integer | 20  | DNS解析记录的总数。   |
| Domains | Struct  |     | 您拥有的域名。       |
| New     | Integer | 10  | 新增域名数量。       |
| Total   | Integer | 20  | 域名的总数。        |
| Hosts   | Struct  |     | 您拥有的主机。       |
| New     | Integer | 10  | 新增主机的数量。      |

| 名称         | 类型      | 示例值                                  | 描述                |
|------------|---------|--------------------------------------|-------------------|
| Total      | Integer | 20                                   | 您拥有的主机的总数。        |
| Ports      | Struct  |                                      | 您主机中开启的端口服务。      |
| New        | Integer | 10                                   | 新增的端口数量。          |
| Total      | Integer | 20                                   | 开放的端口总数。          |
| RequestId  | String  | 714FE3CF-1755-440D-856A-97E8A082EE63 | 阿里云为该请求生成的唯一标识符。  |
| Subdomains | Struct  |                                      | 您拥有的子域名。          |
| New        | Integer | 10                                   | 新增子域名的数量。         |
| Total      | Integer | 20                                   | 您拥有的子域名的总数。       |
| WebPaths   | Struct  |                                      | 域名网站的Web文件的路径。    |
| New        | Integer | 10                                   | 新增Web路径的数量。       |
| Total      | Integer | 20                                   | Web路径的总数。         |
| WebTechs   | Struct  |                                      | 您所有域名网站中使用的Web应用。 |
| New        | Integer | 10                                   | 新增Web站点数量。        |
| Total      | Integer | 20                                   | 您所有网站中Web应用的总数。   |

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListUserAttackSurfaceFacets
&<公共请求参数>
```

正常返回示例



## XML 格式

```
<ListUserAttackSurfaceFacetsResponse>
  <DNSMap>
    <New>37097</New>
    <Total>37097</Total>
  </DNSMap>
  <WebPaths>
    <New>5599</New>
    <Total>5599</Total>
  </WebPaths>
  <Subdomains>
    <New>193901</New>
    <Total>193901</Total>
  </Subdomains>
  <RequestId>FED005E5-833F-4C61-AF07-B0C8AF03A554</RequestId>
  <WebTechs>
    <New>33177</New>
    <Total>33177</Total>
  </WebTechs>
  <Hosts>
    <New>603</New>
    <Total>603</Total>
  </Hosts>
  <Domains>
    <New>57</New>
    <Total>57</Total>
  </Domains>
  <Ports>
    <New>2417</New>
    <Total>2417</Total>
  </Ports>
</ListUserAttackSurfaceFacetsResponse>
```

## JSON 格式

```
{
  "DNSMap": {
    "New": 37097,
    "Total": 37097
  },
  "WebPaths": {
    "New": 5599,
    "Total": 5599
  },
  "Subdomains": {
    "New": 193901,
    "Total": 193901
  },
  "RequestId": "FED005E5-833F-4C61-AF07-B0C8AF03A554",
  "WebTechs": {
    "New": 33177,
    "Total": 33177
  },
  "Hosts": {
    "New": 603,
    "Total": 603
  },
  "Domains": {
    "New": 57,
    "Total": 57
  },
  "Ports": {
    "New": 2417,
    "Total": 2417
  }
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 7.22. ListUserDNSMap

调用ListUserDNSMap获取用户DNS解析记录列表信息。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

### 请求参数

| 名称 | 类型 | 是否必选 | 示例值 | 描述 |
|----|----|------|-----|----|
|----|----|------|-----|----|

| 名称          | 类型      | 是否必选 | 示例值            | 描述                                 |
|-------------|---------|------|----------------|------------------------------------|
| Action      | String  | 是    | ListUserDNSMap | 要执行的操作。取值： <b>ListUserDNSMap</b> 。 |
| Search      | String  | 否    | type:cname     | 查询内容。                              |
| CurrentPage | Integer | 否    | 1              | 指定返回结果的当前页码。<br>默认值为1。             |
| PageSize    | Integer | 否    | 10             | 指定列表每页显示数据条数。<br>默认值为10，可设置值最大为10。 |

## 返回数据

| 名称          | 类型      | 示例值              | 描述                                                                                                            |
|-------------|---------|------------------|---------------------------------------------------------------------------------------------------------------|
| CurrentPage | Integer | 1                | 返回结果的当前页码。<br>默认值为1。                                                                                          |
| PageSize    | Integer | 10               | 返回结果列表每页显示数据条数。                                                                                               |
| Records     | Array   |                  | 记录列表。                                                                                                         |
| Domain      | String  | aliyun.com       | 域名。                                                                                                           |
| Id          | Integer | 1                | 记录ID。                                                                                                         |
| Index       | Integer | 1                | 记录索引。                                                                                                         |
| Record      | String  | a.aliyun.com.com | 解析记录。                                                                                                         |
| Subdomain   | String  | a.aliyun.com     | 子域名。                                                                                                          |
| Type        | String  | cname            | 解析记录类型。取值： <ul style="list-style-type: none"> <li><b>cname</b>：表示CNAME记录。</li> <li><b>a</b>：表示A记录。</li> </ul> |

| 名称         | 类型      | 示例值                                  | 描述           |
|------------|---------|--------------------------------------|--------------|
| UpdatedAt  | Long    | 1581562324000                        | 攻击面数据查询更新时间。 |
| RequestId  | String  | 6E4DC5A2-1870-477D-91FC-56F95F9F7455 | 返回结果的请求ID。   |
| TotalCount | Integer | 20                                   | 返回结果总数量。     |

## 示例

### 请求示例

```
http(s)://[Endpoint]/?Action=ListUserDNSMap
&<公共请求参数>
```

### 正常返回示例

#### XML 格式

```
<ListUserDNSMapResponse>
  <Records>
    <UpdatedAt>1581356497000</UpdatedAt>
    <Index>21</Index>
    <Record>o-o.preferred.tm-kul1.v18.cache.c.pack.aliyun.com.</Record>
    <Domain>aliyun.com</Domain>
    <Type>CNAME</Type>
    <Subdomain>o-o---preferred---tm-kul1---v18---cache.c.pack.aliyun.com</Subdomain>
    <Id>39359</Id>
  </Records>
  <Records>
    <UpdatedAt>1581356497000</UpdatedAt>
    <Index>22</Index>
    <Record>o-o.preferred.telkom-cpt1.v19.cache.c.pack.aliyun.com.</Record>
    <Domain>aliyun.com</Domain>
    <Type>CNAME</Type>
    <Subdomain>o-o---preferred---telkom-cpt1---v19---cache.c.pack.aliyun.com</Subdomain>
    <Id>39357</Id>
  </Records>
  <Records>
    <UpdatedAt>1581356497000</UpdatedAt>
    <Index>23</Index>
    <Record>o-o.preferred.teksavvy-xcm1.v24.cache.c.pack.aliyun.com.</Record>
    <Domain>aliyun.com</Domain>
    <Type>CNAME</Type>
    <Subdomain>o-o---preferred---teksavvy-xcm1---v24---cache.c.pack.aliyun.com</Subdomain>
    <Id>39355</Id>
  </Records>
  <Records>
    <UpdatedAt>1581356497000</UpdatedAt>
    <Index>24</Index>
```

```
<Record>o-o.preferred.suddenlink-crw1.v2.cache.c.pack.aliyun.com.</Record>
<Domain>aliyun.com</Domain>
<Type>CNAME</Type>
<Subdomain>o-o---preferred---suddenlink-crw1---v2---cache.c.pack.aliyune.com</Subdomain>
<Id>39339</Id>
</Records>
<Records>
  <UpdatedAt>1581356497000</UpdatedAt>
  <Index>25</Index>
  <Record>o-o.preferred.stcigw-ruh1.v17.cache.c.pack.aliyun.com.</Record>
  <Domain>aliyun.com</Domain>
  <Type>CNAME</Type>
  <Subdomain>o-o---preferred---stcigw-ruh1---v17---cache.c.pack.aliyun.com</Subdomain>
  <Id>39337</Id>
</Records>
<Records>
  <UpdatedAt>1581356497000</UpdatedAt>
  <Index>26</Index>
  <Record>o-o.preferred.sonet-hnd1.v21.cache.c.pack.aliyun.com.</Record>
  <Domain>aliyun.com</Domain>
  <Type>CNAME</Type>
  <Subdomain>o-o---preferred---sonet-hnd1---v21---cache.c.pack.aliyun.com</Subdomain>
  <Id>39331</Id>
</Records>
<Records>
  <UpdatedAt>1581356497000</UpdatedAt>
  <Index>27</Index>
  <Record>o-o.preferred.sn-xjpm-q0nl.v23.cache.c.pack.aliyun.com.</Record>
  <Domain>aliyun.com</Domain>
  <Type>CNAME</Type>
  <Subdomain>o-o---preferred---sn-xjpm-q0nl---v23---cache.c.pack.aliyun.com</Subdomain>
  <Id>39326</Id>
</Records>
<Records>
  <UpdatedAt>1581356497000</UpdatedAt>
  <Index>28</Index>
  <Record>o-o.preferred.sn-x5guiapo3uxax-cbfl.v12.cache.c.pack.aliyun.com.</Record>
  <Domain>aliyun.com</Domain>
  <Type>CNAME</Type>
  <Subdomain>o-o---preferred---sn-x5guiapo3uxax-cbfl---v12---cache.c.pack.aliyun.com</Subdomain>
  <Id>39322</Id>
</Records>
<Records>
  <UpdatedAt>1581356497000</UpdatedAt>
  <Index>29</Index>
  <Record>o-o.preferred.sn-x1x7sn7k.v6.cache.c.pack.aliyun.com.</Record>
  <Domain>aliyun.com</Domain>
  <Type>CNAME</Type>
  <Subdomain>o-o---preferred---sn-x1x7sn7k---v6---cache.c.pack.aliyun.com</Subdomain>
  <Id>39321</Id>
</Records>
<Records>
  <UpdatedAt>1581356497000</UpdatedAt>
  <Index>30</Index>
```

```
<Record>o-o.preferred.sn-vgqelned.v16.lscache2.c.android.clients.aliyun.com.</Record>
<Domain>aliyun.com</Domain>
<Type>CNAME</Type>
<Subdomain>o-o---preferred---sn-vgqelned---v16---lscache2.c.android.clients.aliyun.com</Subdomain>
<Id>39315</Id>
</Records>
<Records>
  <UpdatedAt>1581356497000</UpdatedAt>
  <Index>31</Index>
  <Record>o-o.preferred.sn-ugvoqgxgxoqgbp-ugqe.v2.cache.c.pack.aliyun.com.</Record>
  <Domain>aliyun.com</Domain>
  <Type>CNAME</Type>
  <Subdomain>o-o---preferred---sn-ugvoqgxgxoqgbp-ugqe---v2---cache.c.pack.aliyun.com</Subdomain>
  <Id>39292</Id>
</Records>
<Records>
  <UpdatedAt>1581356497000</UpdatedAt>
  <Index>32</Index>
  <Record>o-o.preferred.sn-qxa7en7e.v3.cache.c.pack.aliyun.com.</Record>
  <Domain>aliyun.com</Domain>
  <Type>CNAME</Type>
  <Subdomain>o-o---preferred---sn-qxa7en7e---v3---cache.c.pack.aliyun.com</Subdomain>
  <Id>39277</Id>
</Records>
<Records>
  <UpdatedAt>1581356497000</UpdatedAt>
  <Index>33</Index>
  <Record>o-o.preferred.sn-q0c7dn7e.v8.cache.c.pack.aliyun.com.</Record>
  <Domain>aliyun.com</Domain>
  <Type>CNAME</Type>
  <Subdomain>o-o---preferred---sn-q0c7dn7e---v8---cache.c.pack.aliyun.com</Subdomain>
  <Id>39274</Id>
</Records>
<Records>
  <UpdatedAt>1581356497000</UpdatedAt>
  <Index>34</Index>
  <Record>o-o.preferred.sn-q0c7dn7e.v18.cache.c.pack.aliyun.com.</Record>
  <Domain>aliyun.com</Domain>
  <Type>CNAME</Type>
  <Subdomain>o-o---preferred---sn-q0c7dn7e---v18---cache.c.pack.aliyun.com</Subdomain>
  <Id>39273</Id>
</Records>
<Records>
  <UpdatedAt>1581356497000</UpdatedAt>
  <Index>35</Index>
  <Record>o-o.preferred.sn-p5qlsn7z.v5.cache.c.pack.aliyun.com.</Record>
  <Domain>aliyun.com</Domain>
  <Type>CNAME</Type>
  <Subdomain>o-o---preferred---sn-p5qlsn7z---v5---cache.c.pack.aliyun.com</Subdomain>
  <Id>39260</Id>
</Records>
<Records>
  <UpdatedAt>1581356497000</UpdatedAt>
  <Index>36</Index>
```

```

<Record>o-o.preferred.sn-p5qlsn/z.v13.nonxt6.c.pack.aliyun.com.</Record>
<Domain>aliyun.com</Domain>
<Type>CNAME</Type>
<Subdomain>o-o---preferred---sn-p5qlsn7z---v13---nonxt6.c.pack.aliyun.com</Subdomain>
<Id>39258</Id>
</Records>
<Records>
  <UpdatedAt>1581356497000</UpdatedAt>
  <Index>37</Index>
  <Record>o-o.preferred.sn-p5qlsn7l.v18.cache.c.pack.aliyun.com.</Record>
  <Domain>aliyun.com</Domain>
  <Type>CNAME</Type>
  <Subdomain>o-o---preferred---sn-p5qlsn7l---v18---cache.c.pack.aliyun.com</Subdomain>
  <Id>39256</Id>
</Records>
<Records>
  <UpdatedAt>1581356497000</UpdatedAt>
  <Index>38</Index>
  <Record>o-o.preferred.sn-p5qlsn7l.v17.cache.c.pack.aliyun.com.</Record>
  <Domain>aliyun.com</Domain>
  <Type>CNAME</Type>
  <Subdomain>o-o---preferred---sn-p5qlsn7l---v17---cache.c.pack.aliyun.com</Subdomain>
  <Id>39255</Id>
</Records>
<Records>
  <UpdatedAt>1581356497000</UpdatedAt>
  <Index>39</Index>
  <Record>o-o.preferred.sn-oxujvhcc-inbe.v21.cache.c.pack.aliyun.com.</Record>
  <Domain>aliyun.com</Domain>
  <Type>CNAME</Type>
  <Subdomain>o-o---preferred---sn-oxujvhcc-inbe---v21---cache.c.pack.aliyun.com</Subdomain>
  <Id>39253</Id>
</Records>
<Records>
  <UpdatedAt>1581356497000</UpdatedAt>
  <Index>40</Index>
  <Record>o-o.preferred.sn-o097zne.v18.cache.c.pack.aliyun.com.</Record>
  <Domain>aliyun.com</Domain>
  <Type>CNAME</Type>
  <Subdomain>o-o---preferred---sn-o097zne---v18---cache.c.pack.aliyun.com</Subdomain>
  <Id>39249</Id>
</Records>
<TotalCount>441</TotalCount>
<PageSize>20</PageSize>
<RequestId>90AE338C-0AD1-4185-9584-D3FDE2CB3005</RequestId>
<CurrentPage>2</CurrentPage>
</ListUserDNSMapResponse>

```

## JSON 格式

```

{
  "Records": [
    {
      "UpdatedAt": 1581356497000,

```

```
"Index": 21,
"Record": "o-o.preferred.tm-kul1.v18.cache.c.pack.aliyun.com.",
"Domain": "aliyun.com",
"Type": "CNAME",
"Subdomain": "o-o---preferred---tm-kul1---v18---cache.c.pack.aliyun.com",
"Id": 39359
},
{
  "UpdatedAt": 1581356497000,
  "Index": 22,
  "Record": "o-o.preferred.telkom-cpt1.v19.cache.c.pack.aliyun.com.",
  "Domain": "aliyun.com",
  "Type": "CNAME",
  "Subdomain": "o-o---preferred---telkom-cpt1---v19---cache.c.pack.aliyun.com",
  "Id": 39357
},
{
  "UpdatedAt": 1581356497000,
  "Index": 23,
  "Record": "o-o.preferred.teksavvy-xcm1.v24.cache.c.pack.aliyun.com.",
  "Domain": "aliyun.com",
  "Type": "CNAME",
  "Subdomain": "o-o.teksavvy-xcm1---v24---cache.c.pack.aliyun.com",
  "Id": 39355
},
{
  "UpdatedAt": 1581356497000,
  "Index": 24,
  "Record": "o-o.preferred.suddenlink-crw1.v2.cache.c.pack.aliyun.com.",
  "Domain": "aliyun.com",
  "Type": "CNAME",
  "Subdomain": "o-o---preferred---suddenlink-crw1---v2---cache.c.pack.aliyun.com",
  "Id": 39339
},
{
  "UpdatedAt": 1581356497000,
  "Index": 25,
  "Record": "o-o.preferred.stcigw-ruh1.v17.cache.c.pack.aliyun.com.",
  "Domain": "aliyun.com",
  "Type": "CNAME",
  "Subdomain": "o-o---preferred---stcigw-ruh1---v17---cache.c.pack.aliyun.com",
  "Id": 39337
},
{
  "UpdatedAt": 1581356497000,
  "Index": 26,
  "Record": "o-o.preferred.sonet-hnd1.v21.cache.c.pack.aliyun.com.",
  "Domain": "aliyun.com",
  "Type": "CNAME",
  "Subdomain": "o-o---preferred---sonet-hnd1---v21---cache.c.pack.aliyun.com",
  "Id": 39331
},
{
  "UpdatedAt": 1581356497000,
```

```

"Index": 27,
"Record": "o-o-preferred.sn-xjpm-q0nl.v23.cache.c.pack.aliyun.com.",
"Domain": "aliyun.com",
"Type": "CNAME",
"Subdomain": "o-o---preferred---sn-xjpm-q0nl---v23---cache.c.pack.aliyun.com",
"Id": 39326
},
{
"UpdatedAt": 1581356497000,
"Index": 28,
"Record": "o-o-preferred.sn-x5guiapo3uxax-cbfl.v12.cache.c.pack.aliyun.com.",
"Domain": "aliyun.com",
"Type": "CNAME",
"Subdomain": "o-o---preferred---sn-x5guiapo3uxax-cbfl---v12---cache.c.pack.aliyun.com",
"Id": 39322
},
{
"UpdatedAt": 1581356497000,
"Index": 29,
"Record": "o-o-preferred.sn-x1x7sn7k.v6.cache.c.pack.aliyun.com.",
"Domain": "aliyun.com",
"Type": "CNAME",
"Subdomain": "o-o---preferred---sn-x1x7sn7k---v6---cache.c.pack.aliyun.com",
"Id": 39321
},
{
"UpdatedAt": 1581356497000,
"Index": 30,
"Record": "o-o-preferred.sn-vgqelned.v16.lscache2.c.android.clients.aliyun.com.",
"Domain": "aliyun.com",
"Type": "CNAME",
"Subdomain": "o-o---preferred---sn-vgqelned---v16---lscache2.c.android.clients.aliyun.com",
"Id": 39315
},
{
"UpdatedAt": 1581356497000,
"Index": 31,
"Record": "o-o-preferred.sn-ugvoqgxgxoqgbp-ugqe.v2.cache.c.pack.aliyun.com.",
"Domain": "aliyun.com",
"Type": "CNAME",
"Subdomain": "o-o---preferred---sn-ugvoqgxgxoqgbp-ugqe---v2---cache.c.pack.aliyun.com",
"Id": 39292
},
{
"UpdatedAt": 1581356497000,
"Index": 32,
"Record": "o-o-preferred.sn-qxa7en7e.v3.cache.c.pack.aliyun.com.",
"Domain": "aliyun.com",
"Type": "CNAME",
"Subdomain": "o-o---preferred---sn-qxa7en7e---v3---cache.c.pack.aliyun.com",
"Id": 39277
},
{
"UpdatedAt": 1581356497000,
"Index": 33,

```

```
    "Index": 33,  
    "Record": "o-o.preferred.sn-q0c7dn7e.v8.cache.c.pack.aliyun.com.",  
    "Domain": "aliyun.com",  
    "Type": "CNAME",  
    "Subdomain": "o-o---preferred---sn-q0c7dn7e---v8---cache.c.pack.aliyun.com",  
    "Id": 39274  
  },  
  {  
    "UpdatedAt": 1581356497000,  
    "Index": 34,  
    "Record": "o-o.preferred.sn-q0c7dn7e.v18.cache.c.pack.aliyun.com.",  
    "Domain": "aliyun.com",  
    "Type": "CNAME",  
    "Subdomain": "o-o---preferred---sn-q0c7dn7e---v18---cache.c.pack.aliyun.com",  
    "Id": 39273  
  },  
  {  
    "UpdatedAt": 1581356497000,  
    "Index": 35,  
    "Record": "o-o.preferred.sn-p5qlsn7z.v5.cache.c.pack.aliyun.com.",  
    "Domain": "aliyun.com",  
    "Type": "CNAME",  
    "Subdomain": "o-o---preferred---sn-p5qlsn7z---v5---cache.c.pack.aliyun.com",  
    "Id": 39260  
  },  
  {  
    "UpdatedAt": 1581356497000,  
    "Index": 36,  
    "Record": "o-o.preferred.sn-p5qlsn7z.v13.nonxt6.c.pack.aliyun.com.",  
    "Domain": "aliyun.com",  
    "Type": "CNAME",  
    "Subdomain": "o-o---preferred---sn-p5qlsn7z---v13---nonxt6.c.pack.aliyun.com",  
    "Id": 39258  
  },  
  {  
    "UpdatedAt": 1581356497000,  
    "Index": 37,  
    "Record": "o-o.preferred.sn-p5qlsn7l.v18.cache.c.pack.aliyun.com.",  
    "Domain": "aliyun.com",  
    "Type": "CNAME",  
    "Subdomain": "o-o---preferred---sn-p5qlsn7l---v18---cache.c.pack.aliyun.com",  
    "Id": 39256  
  },  
  {  
    "UpdatedAt": 1581356497000,  
    "Index": 38,  
    "Record": "o-o.preferred.sn-p5qlsn7l.v17.cache.c.pack.aliyun.com.",  
    "Domain": "aliyun.com",  
    "Type": "CNAME",  
    "Subdomain": "o-o---preferred---sn-p5qlsn7l---v17---cache.c.pack.aliyun.com",  
    "Id": 39255  
  },  
  {  
    "UpdatedAt": 1581356497000,  
    "Index": 39
```

```
    "Record": "o-o.preferred.sn-oxujvhcc-inbe.v21.cache.c.pack.aliyun.com.",
    "Domain": "aliyun.com",
    "Type": "CNAME",
    "Subdomain": "o-o---preferred---sn-oxujvhcc-inbe---v21---cache.c.pack.aliyun.com",
    "Id": 39253
  },
  {
    "UpdatedAt": 1581356497000,
    "Index": 40,
    "Record": "o-o.preferred.sn-o097znezh.v18.cache.c.pack.aliyun.com.",
    "Domain": "aliyun.com",
    "Type": "CNAME",
    "Subdomain": "o-o---preferred---sn-o097znezh---v18---cache.c.pack.aliyun.com",
    "Id": 39249
  }
],
"TotalCount": 441,
"PageSize": 20,
"RequestId": "90AE338C-0AD1-4185-9584-D3FDE2CB3005",
"CurrentPage": 2
}
```

错误码

访问[错误中心](#)查看更多错误码。

7.23. ListUserDomains

调用ListUserDomains获取用户域名列表信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称          | 类型      | 是否必选 | 示例值             | 描述                                   |
|-------------|---------|------|-----------------|--------------------------------------|
| Action      | String  | 是    | ListUserDomains | 需要执行的操作。取值： <b>ListUserDomains</b> 。 |
| Search      | String  | 否    | aliyun.com      | 需要查询的域名。                             |
| CurrentPage | Integer | 否    | 1               | 返回结果的当前页码。<br>默认值为1。                 |
| PageSize    | Integer | 否    | 10              | 返回结果列表每页显示的数据条数。                     |

返回数据

| 名称          | 类型      | 示例值                                  | 描述                    |
|-------------|---------|--------------------------------------|-----------------------|
| CurrentPage | Integer | 1                                    | 返回结果的当前页码。            |
| PageSize    | Integer | 10                                   | 返回结果列表每页显示数据条数。       |
| Records     | Array   |                                      | 查询返回的域名信息列表。          |
| Domain      | String  | aliyun.com                           | 需要查询的域名。              |
| Id          | Integer | 1                                    | 漏洞扫描为该域名分配的ID号。       |
| Index       | Integer | 1                                    | 查询返回的域名信息列表中每条记录的索引号。 |
| UpdatedAt   | Long    | 1582166786000                        | 攻击面数据查询更新的时间。         |
| RequestId   | String  | 40D177A1-75A0-4192-9848-823AD8705C22 | 返回结果请求ID。             |
| TotalCount  | Integer | 10                                   | 返回结果总数量。              |

示例

请求示例

http(s)://[Endpoint]/?Action=ListUserDomains  
&<公共请求参数>

正常返回示例

XML 格式

```
<ListUserDomainsResponse>
  <Records>
    <UpdatedAt>1558579833000</UpdatedAt>
    <Index>1</Index>
    <Domain>aliyun.com</Domain>
    <Id>530</Id>
  </Records>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>37EC8071-9B31-4E4F-8EE5-F4687BAB55F8</RequestId>
  <CurrentPage>1</CurrentPage>
</ListUserDomainsResponse>
```

#### JSON 格式

```
{
  "Records": [
    {
      "UpdatedAt": 1558579833000,
      "Index": 1,
      "Domain": "aliyun.com",
      "Id": 530
    }
  ],
  "TotalCount": 1,
  "PageSize": 10,
  "RequestId": "37EC8071-9B31-4E4F-8EE5-F4687BAB55F8",
  "CurrentPage": 1
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 7.24. ListUserHosts

调用ListUserHosts获取主机列表信息。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

### 请求参数

| 名称     | 类型     | 是否必选 | 示例值           | 描述                                 |
|--------|--------|------|---------------|------------------------------------|
| Action | String | 是    | ListUserHosts | 需要执行的操作。取值： <b>ListUserHosts</b> 。 |

| 名称          | 类型      | 是否必选 | 示例值        | 描述                                    |
|-------------|---------|------|------------|---------------------------------------|
| Search      | String  | 否    | ip:1.1.1.1 | 需要查询的主机。                              |
| CurrentPage | Integer | 否    | 1          | 返回结果的当前页码。<br>默认值为1。                  |
| PageSize    | Integer | 否    | 10         | 返回结果列表每页显示数据条数。<br>默认值为10，可设置的最大值为10。 |

返回数据

| 名称          | 类型      | 示例值           | 描述                                                                                                                      |
|-------------|---------|---------------|-------------------------------------------------------------------------------------------------------------------------|
| CurrentPage | Integer | 1             | 返回结果的当前页码。                                                                                                              |
| PageSize    | Integer | 10            | 返回结果列表每页显示数据条数。                                                                                                         |
| Records     | Array   |               | 查询返回的主机信息列表。                                                                                                            |
| Hostname    | String  | guest         | 查询返回的主机信息列表中的主机名。                                                                                                       |
| IP          | String  | 192.168.1.1   | 查询返回的主机信息列表中的IP地址。                                                                                                      |
| Id          | Integer | 1             | 主机信息列表中的漏洞扫描为该主机分配的ID号。                                                                                                 |
| Index       | Integer | 1             | 查询返回的主机列表中每条记录的索引号。                                                                                                     |
| OS          | String  | windows       | 查询返回的域名信息列表中主机的操作系统。                                                                                                    |
| State       | String  | up            | 查询返回的域名信息列表中主机的状态。取值： <ul style="list-style-type: none"><li>• <b>up</b>：表示主机在线。</li><li>• <b>down</b>：表示主机离线。</li></ul> |
| UpdatedAt   | Long    | 1581348080000 | 主机查询列表更新时间。                                                                                                             |

| 名称         | 类型      | 示例值                                  | 描述         |
|------------|---------|--------------------------------------|------------|
| RequestId  | String  | 7DC8391E-D5D8-4E00-A457-1F861F86E78A | 返回结果的请求ID。 |
| TotalCount | Integer | 269                                  | 返回结果总数。    |

## 示例

### 请求示例

```
http(s)://[Endpoint]/?Action=ListUserHosts
&<公共请求参数>
```

### 正常返回示例

#### XML 格式

```
<ListUserHostsResponse>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>4A1AA1D7-F806-475B-8B9B-B9B0B889EA9F</RequestId>
  <CurrentPage>1</CurrentPage>
  <Records>
    <OS>Linux 3.10 - 4.11</OS>
    <State>up</State>
    <IP>1.1.1.1</IP>
    <Hostname></Hostname>
    <Index>1</Index>
    <Id>4741</Id>
    <UpdatedAt>1582625412000</UpdatedAt>
  </Records>
</ListUserHostsResponse>
```

#### JSON 格式

```
{
  "TotalCount": 1,
  "PageSize": 10,
  "RequestId": "4A1AA1D7-F806-475B-8B9B-B9B0B889EA9F",
  "CurrentPage": 1,
  "Records": [
    {
      "OS": "Linux 3.10 - 4.11",
      "State": "up",
      "IP": "1.1.1.1",
      "Hostname": "",
      "Index": 1,
      "Id": 4741,
      "UpdatedAt": 1582625412000
    }
  ]
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 7.25. ListUserOrganizations

调用ListUserOrganizations获取用户已创建的组织机构列表。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称          | 类型      | 是否必选 | 示例值                   | 描述                               |
|-------------|---------|------|-----------------------|----------------------------------|
| Action      | String  | 是    | ListUserOrganizations | 要执行的操作。取值：ListUserOrganizations。 |
| Search      | String  | 否    | foobar                | 查询用户已创建的组织机构列表。                  |
| CurrentPage | Integer | 否    | 1                     | 当前页，默认值为1。                       |
| PageSize    | Integer | 否    | 10                    | 页面大小，默认值为10，最大值为10。              |

返回数据

| 名称            | 类型      | 示例值                                  | 描述                  |
|---------------|---------|--------------------------------------|---------------------|
| CurrentPage   | Integer | 1                                    | 当前页，默认值为1。          |
| Organizations | Array   |                                      | 组织机构列表。             |
| CreatedAt     | Long    | 1585821325000                        | 组织机构创建时间戳。          |
| Description   | String  | 这是一个新的组织                             | 组织机构名称描述。           |
| Index         | Integer | 1                                    | 索引号。                |
| Name          | String  | 新的组织                                 | 组织机构名称。             |
| OrgId         | Integer | 1                                    | 组织机构ID。             |
| UpdatedAt     | Long    | 1585821325000                        | 更新时间戳。              |
| PageSize      | Integer | 10                                   | 页面大小，默认值为10，最大值为10。 |
| RequestId     | String  | 22EBC167-D59C-4E8D-8AEE-11BCDDD49946 | 返回结果的请求ID。          |
| TotalCount    | Integer | 4                                    | 组织机构总数。             |

示例

请求示例

http(s)://[Endpoint]/?Action=ListUserOrganizations  
&<公共请求参数>

正常返回示例

XML 格式

```
<ListUserOrganizationsResponse>  
  <TotalCount>0</TotalCount>  
  <RequestId>744F6A47-A80F-4557-9222-AD337E902265</RequestId>  
  <PageSize>10</PageSize>  
  <CurrentPage>1</CurrentPage>  
</ListUserOrganizationsResponse>
```

JSON 格式

```
{
  "TotalCount": 0,
  "RequestId": "744F6A47-A80F-4557-9222-AD337E902265",
  "PageSize": 10,
  "CurrentPage": 1,
  "Organizations": []
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 7.26. ListUserPorts

调用ListUserPorts获取主机开启的端口和端口提供的服务信息列表。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称          | 类型      | 是否必选 | 示例值           | 描述                                  |
|-------------|---------|------|---------------|-------------------------------------|
| Action      | String  | 是    | ListUserPorts | 需要执行的操作。取值： <b>ListUserPorts</b> 。  |
| Search      | String  | 否    | port:80       | 需要查询的主机端口或端口提供的服务。                  |
| CurrentPage | Integer | 否    | 1             | 指定返回结果的当前页码。<br>默认值为1。              |
| PageSize    | Integer | 否    | 10            | 指定列表每页显示数据条数。<br>默认值为10，可设置的最大值为10。 |

返回数据

| 名称          | 类型      | 示例值 | 描述               |
|-------------|---------|-----|------------------|
| CurrentPage | Integer | 1   | 指定返回结果的当前页码。     |
| PageSize    | Integer | 10  | 返回结果列表每页显示数据的条数。 |

| 名称          | 类型      | 示例值                                  | 描述                    |
|-------------|---------|--------------------------------------|-----------------------|
| Records     | Array   |                                      | 查询返回的主机开放端口和端口服务信息列表。 |
| Fingerprint | String  | HTTAPI httpd                         | 端口指纹信息                |
| IP          | String  | 192.168.1.1                          | IP 地址                 |
| Id          | Integer | 1                                    | 记录 ID                 |
| Index       | Integer | 1                                    | 索引号                   |
| Port        | Integer | 80                                   | 端口号                   |
| Product     | String  | Microsoft HTTAPI httpd               | 产品名称                  |
| Protocol    | String  | tcp                                  | 协议名称                  |
| Service     | String  | http                                 | 服务名称                  |
| UpdatedAt   | Long    | 1581348084000                        | 更新时间                  |
| Version     | String  | 1.0                                  | 版本名称                  |
| RequestId   | String  | 8F39E2EA-2CED-48CD-8F98-C50F3D910975 | 返回结果请求ID。             |
| TotalCount  | Integer | 10                                   | 返回结果总数量。              |

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListUserPorts
&<公共请求参数>
```

正常返回示例

```
XML 格式

<ListUserPortsResponse>
  <Records>
```

```
<UpdatedAt>1582630431000</UpdatedAt>
<Service>http</Service>
<Port>80</Port>
<Index>1</Index>
<Product>Tengine httpd</Product>
<IP>1.1.1.1</IP>
<Id>18970</Id>
<Version></Version>
<Protocol>tcp</Protocol>
<Fingerprint></Fingerprint>
</Records>
<Records>
  <UpdatedAt>1582561718000</UpdatedAt>
  <Service>http</Service>
  <Port>80</Port>
  <Index>2</Index>
  <Product>Tengine httpd</Product>
  <IP>2.2.2.2</IP>
  <Id>18576</Id>
  <Version></Version>
  <Protocol>tcp</Protocol>
  <Fingerprint></Fingerprint>
</Records>
<Records>
  <UpdatedAt>1582544019000</UpdatedAt>
  <Service>http</Service>
  <Port>80</Port>
  <Index>3</Index>
  <Product>Tengine httpd</Product>
  <IP>3.3.3.3</IP>
  <Id>18369</Id>
  <Version></Version>
  <Protocol>tcp</Protocol>
  <Fingerprint></Fingerprint>
</Records>
<Records>
  <UpdatedAt>1581356439000</UpdatedAt>
  <Service>http</Service>
  <Port>80</Port>
  <Index>4</Index>
  <Product>unknown http service</Product>
  <IP>4.4.4.4</IP>
  <Id>20348</Id>
  <Version></Version>
  <Protocol>tcp</Protocol>
  <Fingerprint></Fingerprint>
</Records>
<Records>
  <UpdatedAt>1581356439000</UpdatedAt>
  <Service>http</Service>
  <Port>80</Port>
  <Index>5</Index>
  <Product>Microsoft IIS httpd</Product>
  <IP>5.5.5.5</IP>
```

```
<Id>20346</Id>
<Version>8.5</Version>
<Protocol>tcp</Protocol>
<Fingerprint></Fingerprint>
</Records>
<Records>
  <UpdatedAt>1581356439000</UpdatedAt>
  <Service>http</Service>
  <Port>80</Port>
  <Index>6</Index>
  <Product>Apache httpd</Product>
  <IP>6.6.6.6</IP>
  <Id>20292</Id>
  <Version>2.2.8</Version>
  <Protocol>tcp</Protocol>
  <Fingerprint></Fingerprint>
</Records>
<Records>
  <UpdatedAt>1581356439000</UpdatedAt>
  <Service>http</Service>
  <Port>80</Port>
  <Index>7</Index>
  <Product>Tengine httpd</Product>
  <IP>7.7.7.7</IP>
  <Id>20145</Id>
  <Version></Version>
  <Protocol>tcp</Protocol>
  <Fingerprint></Fingerprint>
</Records>
<Records>
  <UpdatedAt>1581356439000</UpdatedAt>
  <Service>http</Service>
  <Port>80</Port>
  <Index>8</Index>
  <Product>Tengine httpd</Product>
  <IP>8.8.8.8</IP>
  <Id>20143</Id>
  <Version></Version>
  <Protocol>tcp</Protocol>
  <Fingerprint></Fingerprint>
</Records>
<Records>
  <UpdatedAt>1581356439000</UpdatedAt>
  <Service>http</Service>
  <Port>80</Port>
  <Index>9</Index>
  <Product>nginx</Product>
  <IP>9.9.9.9</IP>
  <Id>20142</Id>
  <Version>1.10.2</Version>
  <Protocol>tcp</Protocol>
  <Fingerprint></Fingerprint>
</Records>
<Records>
```

```
<UpdatedAt>1581356439000</UpdatedAt>
<Service>http</Service>
<Port>80</Port>
<Index>10</Index>
<Product>Tengine httpd</Product>
<IP>10.10.10.10</IP>
<Id>20139</Id>
<Version></Version>
<Protocol>tcp</Protocol>
<Fingerprint></Fingerprint>
</Records>
<TotalCount>553</TotalCount>
<PageSize>10</PageSize>
<RequestId>FD9203C8-528D-4072-B00D-1ED688D31D00</RequestId>
<CurrentPage>1</CurrentPage>
</ListUserPortsResponse>
```

#### JSON 格式

```
{
  "Records": [
    {
      "UpdatedAt": 1582630431000,
      "Service": "http",
      "Port": 80,
      "Index": 1,
      "Product": "Tengine httpd",
      "IP": "1.1.1.1",
      "Id": 18970,
      "Version": "",
      "Protocol": "tcp",
      "Fingerprint": ""
    },
    {
      "UpdatedAt": 1582561718000,
      "Service": "http",
      "Port": 80,
      "Index": 2,
      "Product": "Tengine httpd",
      "IP": "2.2.2.2",
      "Id": 18576,
      "Version": "",
      "Protocol": "tcp",
      "Fingerprint": ""
    },
    {
      "UpdatedAt": 1582544019000,
      "Service": "http",
      "Port": 80,
      "Index": 3,
      "Product": "Tengine httpd",
      "IP": "3.3.3.3",
      "Id": 18369,
      "Version": "",

```

```
"Protocol": "tcp",
"Fingerprint": ""
},
{
  "UpdatedAt": 1581356439000,
  "Service": "http",
  "Port": 80,
  "Index": 4,
  "Product": "unknown http service",
  "IP": "4.4.4.4",
  "Id": 20348,
  "Version": "",
  "Protocol": "tcp",
  "Fingerprint": ""
},
{
  "UpdatedAt": 1581356439000,
  "Service": "http",
  "Port": 80,
  "Index": 5,
  "Product": "Microsoft IIS httpd",
  "IP": "5.5.5.5",
  "Id": 20346,
  "Version": "8.5",
  "Protocol": "tcp",
  "Fingerprint": ""
},
{
  "UpdatedAt": 1581356439000,
  "Service": "http",
  "Port": 80,
  "Index": 6,
  "Product": "Apache httpd",
  "IP": "6.6.6.6",
  "Id": 20292,
  "Version": "2.2.8",
  "Protocol": "tcp",
  "Fingerprint": ""
},
{
  "UpdatedAt": 1581356439000,
  "Service": "http",
  "Port": 80,
  "Index": 7,
  "Product": "Tengine httpd",
  "IP": "7.7.7.7",
  "Id": 20145,
  "Version": "",
  "Protocol": "tcp",
  "Fingerprint": ""
},
{
  "UpdatedAt": 1581356439000,
  "Service": "http",
```

```
"Port": 80,
"Index": 8,
"Product": "Tengine httpd",
"IP": "8.8.8.8",
"Id": 20143,
"Version": "",
"Protocol": "tcp",
"Fingerprint": ""
},
{
  "UpdatedAt": 1581356439000,
  "Service": "http",
  "Port": 80,
  "Index": 9,
  "Product": "nginx",
  "IP": "9.9.9.9",
  "Id": 20142,
  "Version": "1.10.2",
  "Protocol": "tcp",
  "Fingerprint": ""
},
{
  "UpdatedAt": 1581356439000,
  "Service": "http",
  "Port": 80,
  "Index": 10,
  "Product": "Tengine httpd",
  "IP": "10.10.10.10",
  "Id": 20139,
  "Version": "",
  "Protocol": "tcp",
  "Fingerprint": ""
}
],
"TotalCount": 553,
"PageSize": 10,
"RequestId": "FD9203C8-528D-4072-B00D-1ED688D31D00",
"CurrentPage": 1
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 7.27. ListUserSubdomains

调用ListUserSubdomains获取用户子域名的列表信息。

### 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称          | 类型      | 是否必选 | 示例值                | 描述                                     |
|-------------|---------|------|--------------------|----------------------------------------|
| Action      | String  | 是    | ListUserSubdomains | 要执行的操作。取值： <b>ListUserSubdomains</b> 。 |
| Search      | String  | 否    | baidu.com          | 搜索子域名列表信息。                             |
| CurrentPage | Integer | 否    | 1                  | 返回结果的当前页码。默认值为1。                       |
| PageSize    | Integer | 否    | 10                 | 返回结果列表每页显示的数据条数。                       |

返回数据

| 名称          | 类型      | 示例值                                  | 描述               |
|-------------|---------|--------------------------------------|------------------|
| CurrentPage | Integer | 1                                    | 返回结果的当前页码。默认值为1。 |
| PageSize    | Integer | 10                                   | 返回结果列表每页显示的数据条数。 |
| Records     | Array   |                                      | 记录列表             |
| Domain      | String  | baidu.com                            | 域名               |
| Id          | Integer | 1                                    | 记录ID             |
| Index       | Integer | 1                                    | 记录索引号            |
| Subdomain   | String  | foo.baidu.com                        | 子域名              |
| UpdatedAt   | Long    | 1582166968000                        | 更新时间             |
| RequestId   | String  | 665EEE60-E78C-4F3A-A231-8D1C379AB512 | 返回结果请求ID         |
| TotalCount  | Integer | 34013                                | 返回结果总数量          |

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListUserSubdomains
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ListUserSubdomainsResponse>
  <TotalCount>0</TotalCount>
  <RequestId>5A71FF12-FC30-496F-A79F-6FE08C598CC7</RequestId>
  <PageSize>10</PageSize>
  <CurrentPage>1</CurrentPage>
</ListUserSubdomainsResponse>
```

JSON 格式

```
{
  "TotalCount": 0,
  "RequestId": "5A71FF12-FC30-496F-A79F-6FE08C598CC7",
  "PageSize": 10,
  "CurrentPage": 1,
  "Records": []
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 7.28. ListUserWebPaths

调用ListUserWebPaths获取用户Web路径的列表信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称          | 类型      | 是否必选 | 示例值              | 描述                          |
|-------------|---------|------|------------------|-----------------------------|
| Action      | String  | 是    | ListUserWebPaths | 要执行的操作。取值：ListUserWebPaths。 |
| Search      | String  | 否    | baidu.com        | 搜索Web路径的列表信息。               |
| CurrentPage | Integer | 否    | 1                | 指定返回结果的当前页码。默认值为1。          |

| 名称       | 类型      | 是否必选 | 示例值 | 描述                               |
|----------|---------|------|-----|----------------------------------|
| PageSize | Integer | 否    | 10  | 指定列表每页显示的数据条数。默认值为10，且可设置值最大为10。 |

返回数据

| 名称          | 类型      | 示例值                                  | 描述               |
|-------------|---------|--------------------------------------|------------------|
| CurrentPage | Integer | 1                                    | 返回结果的当前页码。默认值为1。 |
| PageSize    | Integer | 10                                   | 返回结果列表每页显示的数据条数。 |
| Records     | Array   |                                      | 记录列表             |
| Id          | Integer | 1                                    | 记录ID             |
| Index       | Integer | 1                                    | 索引号              |
| Path        | String  | /zh-Hans/faq/                        | 路径信息             |
| Site        | String  | https://1.1.1.1                      | 站点信息             |
| UpdatedAt   | Long    | 1581438561000                        | 更新时间             |
| RequestId   | String  | F54F0536-5501-426E-BEB2-890397E5EE3C | 返回结果的请求ID        |
| TotalCount  | Integer | 206                                  | 返回结果总数           |

示例

请求示例

```
http(s)://[Endpoint]/?Action=ListUserWebPaths
&<公共请求参数>
```

正常返回示例

XML 格式

```
<ListUserWebPathsResponse>
  <TotalCount>0</TotalCount>
  <RequestId>FDE01380-176F-4217-B010-0A3EF6D48D8D</RequestId>
  <PageSize>10</PageSize>
  <CurrentPage>1</CurrentPage>
</ListUserWebPathsResponse>
```

JSON 格式

```
{
  "TotalCount": 0,
  "RequestId": "FDE01380-176F-4217-B010-0A3EF6D48D8D",
  "PageSize": 10,
  "CurrentPage": 1,
  "Records": []
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 7.29. ListUserWebTechs

调用ListUserWebTechs获取用户Web应用列表信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称          | 类型      | 是否必选 | 示例值              | 描述                              |
|-------------|---------|------|------------------|---------------------------------|
| Action      | String  | 是    | ListUserWebTechs | 要执行的操作。取值：ListUserWebTechs。     |
| Search      | String  | 否    | baidu.com        | 搜索用户Web应用列表信息。                  |
| CurrentPage | Integer | 否    | 1                | 指定返回结果的当前页码。默认值为1。              |
| PageSize    | Integer | 否    | 10               | 指定列表每页显示数据条数。默认值为10，且可设置值最大为10。 |

返回数据

| 名称          | 类型      | 示例值                                  | 描述                              |
|-------------|---------|--------------------------------------|---------------------------------|
| CurrentPage | Integer | 1                                    | 指定返回结果的当前页码。默认值为1。              |
| PageSize    | Integer | 10                                   | 指定列表每页显示数据条数。默认值为10，且可设置值最大为10。 |
| Records     | Array   |                                      | 记录列表                            |
| Id          | Integer | 1                                    | 记录ID                            |
| Index       | Integer | 1                                    | 索引号                             |
| Name        | String  | Font Awesome                         | Web应用名称                         |
| PoweredBy   | String  | PHP                                  | 应用编程语言                          |
| Server      | String  | beegoServer:1.10.1                   | Web服务器                          |
| Title       | String  | nps admin login                      | 应用站点标题                          |
| URL         | String  | http://192.168.1.1:8081/login/index  | 站点URL                           |
| UpdatedAt   | Long    | 1581348094000                        | 更新时间                            |
| Version     | String  | 1.1                                  | 版本号                             |
| RequestId   | String  | 4F2D6C61-24E2-4EB7-80F9-69CEA6B283BB | 用户请求ID                          |
| TotalCount  | Integer | 237                                  | 返回结果总数                          |

示例

请求示例

http(s)://[Endpoint]/?Action=ListUserWebTechs  
&<公共请求参数>

正常返回示例

XML 格式

```
<ListUserWebTechsResponse>
  <TotalCount>0</TotalCount>
  <RequestId>9E4D51AB-A22D-4D76-83D9-D3F9AC39D5C0</RequestId>
  <PageSize>10</PageSize>
  <CurrentPage>1</CurrentPage>
</ListUserWebTechsResponse>
```

JSON 格式

```
{
  "TotalCount": 0,
  "RequestId": "9E4D51AB-A22D-4D76-83D9-D3F9AC39D5C0",
  "PageSize": 10,
  "CurrentPage": 1,
  "Records": []
}
```

错误码

访问[错误中心](#)查看更多错误码。

# 7.30. ModifyOrganization

调用ModifyOrganization修改用户组织机构相关信息。

调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

请求参数

| 名称          | 类型      | 是否必选 | 示例值                  | 描述                                     |
|-------------|---------|------|----------------------|----------------------------------------|
| Action      | String  | 是    | ModifyOrganization   | 要执行的操作。取值： <b>ModifyOrganization</b> 。 |
| Name        | String  | 否    | 阿里云计算有限公司            | 组织机构名称。                                |
| Description | String  | 否    | 阿里云计算有限公司，是国内知名云计算公司 | 组织机构描述信息。                              |
| OrgId       | Integer | 否    | 1                    | 企业组织ID。                                |

返回数据

| 名称        | 类型     | 示例值                                  | 描述         |
|-----------|--------|--------------------------------------|------------|
| RequestId | String | 1814D014-ED65-47BC-B48A-6CD8CAC788BE | 返回结果的请求ID。 |

## 示例

### 请求示例

```
http(s)://[Endpoint]/?Action=ModifyOrganization
&<公共请求参数>
```

### 正常返回示例

#### XML 格式

```
<ModifyOrganizationResponse>
  <code></code>
  <message></message>
  <success>true</success>
  <requestId></requestId>
  <data></data>
</ModifyOrganizationResponse>
```

#### JSON 格式

```
{
  "code": "",
  "message": "",
  "success": true,
  "requestId": "",
  "data": {}
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

# 7.31. TagAssetsByRecords

调用TagAssetsByRecords可以设置相应的标签。

## 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

## 请求参数

| 名称          | 类型         | 是否必选 | 示例值                | 描述                                                                                                                                                                                                                                                                               |
|-------------|------------|------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action      | String     | 是    | TagAssetsByRecords | 要执行的操作。取值： <b>TagAssetsByRecords</b> 。                                                                                                                                                                                                                                           |
| AssetType   | String     | 是    | IP                 | 资产类型。                                                                                                                                                                                                                                                                            |
| RecordIds.N | RepeatList | 是    | 1                  | 记录列表的ID号。                                                                                                                                                                                                                                                                        |
| Source      | String     | 是    | Domains            | 攻击面数据源。取值： <ul style="list-style-type: none"><li>• <b>Domains</b>（域名）</li><li>• <b>Subdomains</b>（子域名）</li><li>• <b>Ports</b>（端口服务）</li><li>• <b>Hosts</b>（主机列表）</li><li>• <b>DNSMap</b>（DNS解析记录）</li><li>• <b>WebPath</b>（Web路径信息）</li><li>• <b>WebTechs</b>（Web应用信息）</li></ul> |
| Tags.N      | RepeatList | 是    | foobar             | 标签列表。                                                                                                                                                                                                                                                                            |

返回数据

| 名称        | 类型     | 示例值                                  | 描述         |
|-----------|--------|--------------------------------------|------------|
| RequestId | String | FBA4F565-9C63-452A-860F-2974679A8EC1 | 返回结果的请求ID。 |

示例

请求示例

```
http(s)://[Endpoint]/?Action=TagAssetsByRecords
&AssetType=IP
&RecordIds.1=1
&Source=Domains
&Tags.1=foobar
&<公共请求参数>
```

正常返回示例

XML 格式

```
<TagAssetsByRecordsResponse>
  <RequestId>BEBFB0C4-D2A9-4B65-80EB-2032E8BC3FD7</RequestId>
</TagAssetsByRecordsResponse>
```

## JSON 格式

```
{
  "RequestId": "BEBFB0C4-D2A9-4B65-80EB-2032E8BC3FD7",
}
```

## 错误码

访问[错误中心](#)查看更多错误码。

## 7.32. TagAssetsBySearch

调用TagAssetsBySearch对需要标记的资产添加标签。

## 调试

您可以在OpenAPI Explorer中直接运行该接口，免去您计算签名的困扰。运行成功后，OpenAPI Explorer可以自动生成SDK代码示例。

## 请求参数

| 名称        | 类型         | 是否必选 | 示例值               | 描述                                                                                                                                                                                                                                                       |
|-----------|------------|------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action    | String     | 是    | TagAssetsBySearch | 要执行的操作。取值： <b>TagAssetsBySearch</b> 。                                                                                                                                                                                                                    |
| AssetType | String     | 是    | IP                | 攻击面对应的资产类型。取值： <ul style="list-style-type: none"><li><b>Domains</b>：域名</li><li><b>Subdomains</b>：子域名</li><li><b>Ports</b>：端口</li><li><b>Hosts</b>：主机</li><li><b>DNSMap</b>：DNS解析记录</li><li><b>WebPaths</b>：Web路径</li><li><b>WebTechs</b>：Web应用</li></ul> |
| Source    | String     | 是    | Domains           | 攻击面数据源。取值： <ul style="list-style-type: none"><li><b>Domains</b>：域名</li><li><b>Subdomains</b>：子域名</li><li><b>Ports</b>：端口服务</li><li><b>Hosts</b>：主机列表</li><li><b>DNSMap</b>：DNS解析记录</li><li><b>WebPaths</b>：Web路径</li><li><b>WebTechs</b>：Web应用</li></ul> |
| Tags.N    | RepeatList | 是    | foobar            | 标签列表。                                                                                                                                                                                                                                                    |

| 名称     | 类型     | 是否必选 | 示例值    | 描述      |
|--------|--------|------|--------|---------|
| Search | String | 否    | foobar | 搜索资产类型。 |

返回数据

| 名称        | 类型     | 示例值                                  | 描述         |
|-----------|--------|--------------------------------------|------------|
| RequestId | String | 9D67D400-2EC8-4353-BAB9-683891DD5323 | 返回结果的请求ID。 |

示例

请求示例

```
http(s)://[Endpoint]/?Action=TagAssetsBySearch
&AssetType=IP
&Source=Domains
&Tags.1=foobar
&<公共请求参数>
```

正常返回示例

XML 格式

```
<TagAssetsBySearchResponse>
  <AssetType>Domain</AssetType>
  <Tags>Top</Tags>
  <Source>DNSMap</Source>
  <Search>s0x</Search>
</TagAssetsBySearchResponse>
```

JSON 格式

```
{
  "AssetType": "Domain",
  "Tags": [
    "Top"
  ],
  "Source": "DNSMap",
  "Search": "s0x"
}
```

错误码

访问[错误中心](#)查看更多错误码。