ALIBABA CLOUD

阿里云

API参考

文档版本：20210607

阿里云

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 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 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 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 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 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.调用方式

您可以通过发送HTTP GET请求调用安骑士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

安骑士的API是RPC风格，您可以通过发送HTTP GET请求调用安骑士API。

其请求结构如下：

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

其中：

- Endpoint：安骑士API的服务接入地址为*aegis.cn-hangzhou.aliyuncs.com*。
- Action：要执行的操作，如使用DescribeAlarmEventList查询安全事件列表。
- Version：要使用的API版本，安骑士的API版本是*2016-11-11*。
- 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DescribeAlarmEventList接口查询安全事件列表的示例：

> **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)://aegis.cn-hangzhou.aliyuncs.com/?Action=DescribeAlarmEventList
&Format=xml
&Version=2016-11-11
&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API，您需要为该RAM账号创建、附加相应的授权策略。

API签名

安骑士服务会对每个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。

安骑士通过使用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DescribeAlarmEventList为例，假设AccessKey ID是 `testid` ， AccessKey Secret是 `testsecret` ，则签名前的请求URL如下：

```
https://aegis.cn-hangzhou.aliyuncs.com/?Action=DescribeAlarmEventList
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2016-11-11
&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%3DDescribeAlarmEventList&Format%3DXML&SignatureMethod%3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&SignatureVersion%3D1.0&TimeStamp%3D2016-02-23T12%253A46%253A24Z&Version%3D2018-12-03
   ```

2. 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://aegis.cn-hangzhou.aliyuncs.com/?Action=DescribeAlarmEventList
   &TimeStamp=2016-02-23T12:46:24Z
   &Format=XML
   &AccessKeyId=testid
   &SignatureMethod=HMAC-SHA1
   &SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
   &Version=2016-11-11
   &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）。

2.公共参数

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
Region	string	是	安骑士实例所在的地域。 取值： • *aegis.cn-hangzhou*：表示中国地区 • *aegis.ap-southeast-3*：表示海外地区
Format	string	否	返回消息的格式。 取值：*JSON（默认值）*	*XML*
Version	String	是	API版本号，使用YYYY-MM-DD日期格式。 取值：*2016-11-11*
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。 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。 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	唯一随机数，用于防止网络重放攻击。 在不同请求间要使用不同的随机数值。
ResourceOwnerAccount	String	否	本次API请求访问到的资源拥有者账户，即登录用户名。

示例

```
https://aegis.cn-hangzhou.aliyuncs.com/?Action=DescribeAlarmEventList
&Timestamp=2014-05-19T10%3A33%3A56Z
&Format=xml
&AccessKeyId=testid
&SignatureMethod=Hmac-SHA1
&SignatureNonce=NwDAxvLU6tFE0DVb
&Version=2016-11-11
&SignatureVersion=1.0
&Signature=Signature
```

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*/
  }
```

3.获取告警数据

3.1. DescribeAlarmEventList

查询安全事件列表。

告警事件分为告警与异常两个维度，一个告警事件包含多个异常事件。此API可以获取告警事件的列表。

调试

前往【API Explorer】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeAlarmEventList	系统规定参数。取值：DescribeAlarmEventList。
CurrentPage	Integer	是	1	告警事件列表的页码。起始值：1 默认值：1
From	String	是	aqs	请求来源标识，固定为aqs。
PageSize	String	是	20	分页查询时设置的每页行数。默认值：20。
AlarmEventName	String	否	DDOS木马	告警事件名称。
AlarmEventType	String	否	恶意进程（云查杀）	告警事件类型。
Dealed	String	否	Y	告警事件状态。 • N：待处理告警 • Y：已处理告警
Lang	String	否	zh	语言参数。 • zh：中文 • cn：英文

名称	类型	是否必选	示例值	描述
Levels	String	否	serious	告警事件的危险等级，多个严重等级用逗号分隔（严重等级递减）。 • serious：紧急 • suspicious：可疑 • remind：提醒
Remark	String	否	database_server	告警名称/资产。
SourceIp	String	否	1.1.1.1	请求源IP。

返回参数

名称	类型	示例值	描述
PageInfo			分页信息。
└Count	Integer	1	告警事件条数。
└CurrentPage	Integer	1	告警事件列表的页码。
└PageSize	Integer	20	分页大小。
└TotalCount	Integer	1	总条数。
RequestId	String	28267723-D857-4DD8-B295-0131905BA725	请求ID。
SuspEvents			告警事件的列表。
└AlarmEventName	String	Linux计划任务执行异常指令	告警事件名称。
└AlarmEventType	String	进程异常行为	告警事件类型。
└AlarmUniqueInfo	String	8df914418f4211fbf756efe7a6f40cbc	告警事件的唯一标识。
└CanBeDealOnLine	Boolean	true	是否能在线处理（隔离）。

名称	类型	示例值	描述
└CanCancelFault	Boolean	false	能否取消标记为误报。
└DataSource	String	aegis_suspicious_event	数据来源。
└Dealed	Boolean	true	告警事件是否已处理。 • true：已处理 • false：未处理
└Description	String	黑客入侵服务器后，为了让恶意后门程序能持久化运行，黑客常常将恶意SHELL脚本写入crontab、systemd等计划任务。	告警事件的描述。
└EndTime	Long	1543740301000	告警事件结束时间。
└GmtModified	Long	1543740301000	告警事件修改时间，表示同一告警事件再次上报的时间。
└HasTraceInfo	Boolean	true	告警事件是否有溯源数据。 • true：有溯源数据 • false：没有溯源数据
└InstanceName	String	测试服务器	关联实例的名称。
└InternetIp	String	142.1.1.1	关联实例的公网IP。
└IntranetIp	String	192.168.1.1	关联实例的私网IP。
└Level	String	serious	告警事件的危险等级。 • serious：紧急 • suspicious：可疑 • remind：提醒
└SaleVersion	String	4	需要的售卖版本。 • 0：基础版本 • 1：企业版本

名称	类型	示例值	描述
└Solution	String	请及时排查告警中提示的恶意URL，以及所下载的目录下的恶意文件。并及时清理已运行的恶意进程。如果该指令是您自己主动执行，您可以在控制台点击标记为误报，并通过工单方式反馈给我们的安全工程师。	告警事件的处理方法。
└StartTime	Long	1543740301000	告警事件的开始时间。
└SuspiciousEventCount	Integer	1	关联的异常事件的条数。
└Uuid	String	47900178-885d-4fa4-9d77-dba97dba2926	关联实例的唯一标识。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeAlarmEventList
&CurrentPage=1
&From=aqs
&PageSize=20
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeAlarmEventListResponse>
 <RequestId>B5446AFA-58B6-41DC-80E6-E0382AC5A1F4</RequestId>
 <PageInfo>
  <Count>1</Count>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
  <CurrentPage>1</CurrentPage>
 </PageInfo>
 <SuspEvents>
  <Uuid>47900178-885d-4fa4-9d77-XXXXXXXXXXXX</Uuid>
  <Description>黑客入侵服务器后，为了让恶意后门程序能持久化运行，黑客常常将恶意SHELL脚本写入crontab、s
ystemd等计划任务。</Description>
  <CanCancelFault>false</CanCancelFault>
  <InternetIp>10.0.0.0</InternetIp>
  <SuspiciousEventCount>1</SuspiciousEventCount>
  <AlarmUniqueInfo>8df914418f4211fbf756efe7a6f40cbc</AlarmUniqueInfo>
  <AlarmEventName>Linux计划任务执行异常指令</AlarmEventName>
  <AlarmEventType>进程异常行为</AlarmEventType>
  <IntranetIp>10.0.0.0</IntranetIp>
  <Level>serious</Level>
  <EndTime>1543740301000</EndTime>
  <StartTime>1543740301000</StartTime>
  <SaleVersion>1</SaleVersion>
  <CanBeDealOnLine>false</CanBeDealOnLine>
  <InstanceName>server01</InstanceName>
 </SuspEvents>
</DescribeAlarmEventListResponse>
```

`JSON` 格式

```
{
 "RequestId":"B5446AFA-58B6-41DC-80E6-E0382AC5A1F4",
 "SuspEvents":[
 {
  "Uuid":"47900178-885d-4fa4-9d77-XXXXXXXXXXXX",
  "Description":"黑客入侵服务器后，为了让恶意后门程序能持久化运行，黑客常常将恶意SHELL脚本写入crontab、systemd等计划任务。",
  "CanCancelFault":false,
  "InternetIp":"10.0.0.0",
  "SuspiciousEventCount":1,
  "AlarmUniqueInfo":"8df914418f4211fbf756efe7a6f40cbc",
  "AlarmEventName":"Linux计划任务执行异常指令",
  "AlarmEventType":"进程异常行为",
  "IntranetIp":"10.0.0.0",
  "Level":"serious",
  "EndTime":1543740301000,
  "StartTime":1543740301000,
  "CanBeDealOnLine":false,
  "SaleVersion":"1",
  "InstanceName":"server01"
 }
 ],
 "PageInfo":{
  "Count":1,
  "TotalCount":1,
  "PageSize":10,
  "CurrentPage":1
 }
}
```


错误码

查看本产品错误码

3.2. DescribeSuspEvents

查询异常事件列表。

告警事件分为告警与异常两个维度，一个告警事件包含多个异常事件。此API可以获取异常事件的列表。

调试

前往【API Explorer】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

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	DescribeSuspEvents	系统规定参数。取值：DescribeSuspEvents。
AlarmUniqueInfo	String	否	8df914418f4211fbf756efe7a6f40cbc	告警事件的唯一标识。
CurrentPage	String	否	1	当前页码。
Dealed	String	否	Y	异常事件状态： • N：待处理告警 • Y：已处理告警
From	String	否	sas	请求来源标识，固定为aqs。
Lang	String	否	zh	异常事件的语言类型： • zh：中文 • cn：英文
Levels	String	否	serious,suspicious,remind	告警事件的危险等级，多个逗号分隔。以下危险等级严重程度依次递减： • serious：紧急 • suspicious：可疑 • remind：提醒
Name	String	否	挖矿	异常事件名称或者主机名称，支持模糊匹配。
PageSize	String	否	10	分页查询时设置的每页行数。默认值为20。
ParentEventTypes	String	否	网站后门	异常事件分类名称。
Remark	String	否	8.8.8.8	主机IP地址或者名称。
SourceIp	String	否	2.2.2.2	接口访问者源IP。

返回参数

名称	类型	示例值	描述
Count	Integer	10	当前返回结果数量。
CurrentPage	Integer	1	当前页。
PageSize	Integer	20	每页显示告警的条数。
RequestId	String	0C7FAD74-83FA-4671-9250-A5F2A64F437A	请求ID。
SuspEvents			异常事件列表。
└AlarmEventName	String	Linux计划任务执行异常指令	告警事件名称。
└AlarmEventType	String	进程异常行为	告警事件类型。
└AlarmUniqueInfo	String	8df914418f4211fbf756efe7a6f40cbc	告警事件的唯一标识。
└CanBeDealOnLine	Boolean	true	能否在线处理。
└DataSource	String	N/A	忽略该字段。
└Desc	String	webshell	影响概况描述。
└EventStatus	Integer	1	告警事件的状态： • PENDING（1：待处理） • IGNORE（2： 已忽略） • HANDLED（4： 已确认） • FAULT（8： 已标记误报） • DEALING（16： 处理中） • DONE（32： 处理完毕） • EXPIRE（64： 已经过期）
└EventSubType	String	XorDDoS木马	异常事件名称。
└Id	Long	1000	唯一标识。

名称	类型	示例值	描述
└InstanceName	String	nginx	关联实例的名称。
└InternetIp	String	103.1.1.33	关联实例的公网IP。
└IntranetIp	String	10.1.1.109	关联实例的私网IP。
└LastTime	String	2018-09-26 01:51:01	事件发生时间。
└Level	String	serious,suspicious,remind	告警事件的危险等级： • serious：紧急 • suspicious：可疑 • remind：提醒
└Name	String	恶意进程（云查杀）-XorDDoS木马	异常事件的完整名称。
└OccurrenceTime	String	2018-09-26 01:51:01	操作备注消息。
└OperateMsg	String	success	操作备注消息。
└SaleVersion	String	1	需要的售卖版本： • 0：基础版本 • 1：企业版本
└Uuid	String	bf6b30d3-eea8-4924-9f0a-XXXXXXXXXXXX	关联实例的唯一标识。
TotalCount	Integer	100	查询总数量。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeSuspEventsResponse>
 <TotalCount>3</TotalCount>
 <Count>2</Count>
 <PageSize>20</PageSize>
 <RequestId>0C7FAD74-83FA-4671-9250-A5F2A64F437A</RequestId>
 <CurrentPage>1</CurrentPage>
 <SuspEvents>
  <EventStatus>1</EventStatus>
  <SaleVersion>1</SaleVersion>
  <IntranetIp>10.0.0.0</IntranetIp>
  <EventSubType>XorDDoS木马</EventSubType>
  <Name>恶意进程（云查杀）-XorDDoS木马</Name>
  <DataSource>aegis_suspicious_event</DataSource>
  <OccurrenceTime>2018-09-26 01:51:01</OccurrenceTime>
  <InstanceName>server01</InstanceName>
  <Desc>XORDDoS木马入侵后，会在Linux的定时任务中植入恶意代码。</Desc>
  <CanBeDealOnLine>false</CanBeDealOnLine>
  <Uuid>bf6b30d3-eea8-4924-9f0a-XXXXXXXXXXXX</Uuid>
  <InternetIp>10.10.1.1</InternetIp>
  <Level>serious</Level>
  <Id>3682</Id>
  <LastTime>2018-10-24 21:06:01</LastTime>
 </SuspEvents>
 <SuspEvents>
  <EventStatus>1</EventStatus>
  <SaleVersion>1</SaleVersion>
  <IntranetIp>10.0.0.0</IntranetIp>
  <EventSubType>XorDDoS木马</EventSubType>
  <Name>恶意进程（云查杀）-XorDDoS木马</Name>
  <DataSource>aegis_suspicious_event</DataSource>
  <OccurrenceTime>2018-09-26 02:01:01</OccurrenceTime>
  <InstanceName>server01</InstanceName>
  <Desc>XORDDoS木马入侵后，会在Linux的定时任务中植入恶意代码。</Desc>
  <CanBeDealOnLine>false</CanBeDealOnLine>
  <Uuid>bf6b30d3-eea8-4924-9f0a-XXXXXXXXXXXX</Uuid>
  <InternetIp>10.10.1.1</InternetIp>
  <Level>serious</Level>
  <Id>3683</Id>
  <LastTime>2018-10-24 21:01:01</LastTime>
 </SuspEvents>
</DescribeSuspEventsResponse>
```

`JSON` 格式

```
{
 "Count":2,
 "TotalCount":3,
 "PageSize":20,
 "RequestId":"0C7FAD74-83FA-4671-9250-A5F2A64F437A",
 "SuspEvents":[
 {
  "Uuid":"bf6b30d3-eea8-4924-9f0a-XXXXXXXXXXXX",
  "EventStatus":1,
  "LastTime":"2018-10-24 21:06:01",
  "InternetIp":"10.10.1.1",
  "Name":"恶意进程（云查杀）-XorDDoS木马",
  "DataSource":"aegis_suspicious_event",
  "OccurrenceTime":"2018-09-26 01:51:01",
  "IntranetIp":"10.0.0.0",
  "Id":3682,
  "Level":"serious",
  "SaleVersion":"1",
  "CanBeDealOnLine":false,
  "InstanceName":"server01",
  "Desc":"XORDDoS木马入侵后，会在Linux的定时任务中植入恶意代码。",
  "EventSubType":"XorDDoS木马"
 },
 {
  "Uuid":"bf6b30d3-eea8-4924-9f0a-XXXXXXXXXXXX",
  "EventStatus":1,
  "LastTime":"2018-10-24 21:01:01",
  "InternetIp":"10.10.1.1",
  "Name":"恶意进程（云查杀）-XorDDoS木马",
  "DataSource":"aegis_suspicious_event",
  "OccurrenceTime":"2018-09-26 02:01:01",
  "IntranetIp":"10.0.0.0",
  "Id":3683,
  "Level":"serious",
  "SaleVersion":"1",
  "CanBeDealOnLine":false,
  "InstanceName":"server01",
  "Desc":"XORDDoS木马入侵后，会在Linux的定时任务中植入恶意代码。",
  "EventSubType":"XorDDoS木马"
 }
 ],
 "CurrentPage":1
}
```


错误码

查看本产品错误码

3.3. DescribeSuspEventDetail

查询异常事件详情。

告警事件分为告警与异常两个维度，一个告警事件包含多个异常事件。此API可以获取异常事件的详情。

调试

前往【API Explorer】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeSuspEventDetail	系统规定参数。取值：DescribeSuspEventDetail。
From	String	是	aqs	请求来源，固定为aqs。
Lang	String	否	zh	异常事件的语言类型： • zh：中文 • cn：英文
SourceIp	String	否	2.2.2.2	接口访问者源IP。
SuspiciousEventId	Integer	否	199988	要查询的异常告警ID。

返回参数

名称	类型	示例值	描述
CanBeDealOnLine	Boolean	true	是否支持在线处理（隔离）。
DataSource	String	aegis_suspicious_file_v2	数据来源。
Details			异常事件的详情。
└InfoType	String	webshell	字段图标的展示类型。
└Name	String	事件说明	字段名称。
└Type	String	text	字段展示的方式： • text：文本方式 • html：富文本方式

名称	类型	示例值	描述
└Value	String	云盾检测到ECS上运行的网站因为WEB漏洞被黑客利用，导致WEBSHELL的写入，请关注。	字段的内容。
EventDesc	String	该文件极有可能是黑客成功入侵网站后种植的，建议您先确认文件合法性并处理。	异常事件描述。
EventName	String	WEBSHELL	异常事件的名称
EventStatus	String	1	异常事件状态, 取值有： • PENDING（1： 待处理） • IGNORE（2： 已忽略） • HANDLED（4： 已确认） • FAULT（8： 已标记误报） • DEALING（16： 处理中） • DONE（32： 处理完毕） • EXPIRE（64： 已经过期）
EventTypeDesc	String	网站后门-发现后门(Webshell)文件	异常事件类型说明。
Id	Integer	1991	异常事件ID。
InstanceName	String	ca_cpm_test1	关联实例的名称。
InternetIp	String	102.88.91.4	关联实例的公网IP。
IntranetIp	String	10.0.0.161	关联实例的私网IP。
LastTime	String	2018-10-30 11:43:46	该事上次发生的时间。
Level	String	serious	告警事件的危险等级（严重性依次递减）： • serious：紧急 • suspicious：可疑 • remind：提醒
OperateMsg	String	success	操作的扩展信息。

名称	类型	示例值	描述
RequestId	String	17F3C8C2-0504-48D5-8B8F-9CF516968617	请求ID。
SaleVersion	String	1	安骑士服务的版本信息： • 0：基础版本 • 1：企业版本
SasId	String	18819	安骑士系统ID。
Type	String	x	区分是否为DDoS事件。
Uuid	String	bffb12c3-590a-4db2-b538-XXXXXXXXXXXX	关联实例的唯一标识。

示例

请求示例

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

正常返回示例

`XML` 格式

```
<DescribeSuspEventDetailResponse>
 <RequestId>43F670F3-AB40-4E91-BC7D-C57468834F67</RequestId>
 <HostId>aegis.cn-hangzhou.aliyuncs.com</HostId>
 <Code>200</Code>
 <Message>
 illegal parameter, xxxx
</Message>
 <EventDesc>该文件极有可能是黑客成功入侵网站后种植的，建议您先确认文件合法性并处理。</EventDesc>
 <EventTypeDesc>网站后门-发现后门(Webshell)文件</EventTypeDesc>
 <EventStatus>1</EventStatus>
 <EventName>WEBSHELL</EventName>
 <SaleVersion>1</SaleVersion>
 <IntranetIp>10.0.0.161</IntranetIp>
 <DataSource>aegis_suspicious_file_v2</DataSource>
 <InstanceName>ca_cpm_test1</InstanceName>
 <Type>normal</Type>
 <CanBeDealOnLine>true</CanBeDealOnLine>
 <OperateMsg/>
 <Uuid>bffb12c3-590a-4db2-b538-XXXXXXXXXXXX</Uuid>
 <Details>
  <Type>text</Type>
```

```
  <Value>/data/ftpUser/pub/f12cd3bc5b484b0326309b48afb463fb</Value>
  <InfoType>trojan_path</InfoType>
  <Name>木马文件路径</Name>
 </Details>
 <Details>
  <Type>text</Type>
  <Value>--</Value>
  <Name>影响域名</Name>
 </Details>
 <Details>
  <Type>text</Type>
  <Value>2018-10-30 05:00:56</Value>
  <InfoType>frist_found_time</InfoType>
  <Name>首次发现时间</Name>
 </Details>
 <Details>
  <Type>text</Type>
  <Value>2018-10-30 11:43:45</Value>
  <InfoType>update_time</InfoType>
  <Name>更新时间</Name>
 </Details>
 <Details>
  <Type>text</Type>
  <Value>Webshell</Value>
  <InfoType>trojan_type</InfoType>
  <Name>木马类型</Name>
 </Details>
 <Details>
  <Type>html</Type>
  <Value>&lt;a href="http://yundun-aegis-webshell-file.oss-XXXXX"&gt;下载&lt;/a&gt;</Value>
  <InfoType>download_url</InfoType>
  <Name>源文件下载</Name>
 </Details>
 <InternetIp>39.105.41.176</InternetIp>
 <Level>serious</Level>
 <Id>129636</Id>
 <LastTime>2018-10-30 11:43:46</LastTime>
 <SasId>39938056</SasId>
</DescribeSuspEventDetailResponse>
```

JSON 格式

```
{
 "Uuid":"bffb12c3-590a-4db2-b538-XXXXXXXXXXXX",
 "EventName":"WEBSHELL",
 "EventStatus":1,
 "Message":"illegal parameter, xxxx\n",
 "LastTime":"2018-10-30 11:43:46",
 "Details":[
  {
   "Name":"木马文件路径",
   "Value":"/data/ftpUser/pub/f12cd3bc5b484b0326309b48afb463fb",
   "Type":"text",
```

```
  "InfoType":"trojan_path"
 },
 {
  "Name":"影响域名",
  "Value":"--",
  "Type":"text"
 },
 {
  "Name":"首次发现时间",
  "Value":"2018-10-30 05:00:56",
  "Type":"text",
  "InfoType":"frist_found_time"
 },
 {
  "Name":"更新时间",
  "Value":"2018-10-30 11:43:45",
  "Type":"text",
  "InfoType":"update_time"
 },
 {
  "Name":"木马类型",
  "Value":"Webshell",
  "Type":"text",
  "InfoType":"trojan_type"
 },
 {
  "Name":"源文件下载",
  "Value":"<a href=\"http://yundun-aegis-webshell-file.oss-XXXXX\">下载</a>",
  "Type":"html",
  "InfoType":"download_url"
 }
],
"Type":"normal",
"InternetIp":"39.105.41.176",
"HostId":"aegis.cn-hangzhou.aliyuncs.com",
"EventTypeDesc":"网站后门-发现后门(Webshell)文件",
"Code":"200",
"DataSource":"aegis_suspicious_file_v2",
"SasId":"39938056",
"RequestId":"43F670F3-AB40-4E91-BC7D-C57468834F67",
"IntranetIp":"10.0.0.161",
"CauseDetails":[],
"Id":129636,
"Level":"serious",
"EventDesc":"该文件极有可能是黑客成功入侵网站后种植的，建议您先确认文件合法性并处理。",
"OperateMsg":"",
"CanBeDealOnLine":true,
"SaleVersion":"1",
"InstanceName":"ca_cpm_test1"
}
```


错误码

查看本产品错误码

3.4. DescribeAlarmEventDetail

获取告警事件的详细信息。

告警事件分为告警与异常两个维度，一个告警事件包含多个异常事件。此API可以获取一个告警事件的详情。

调试

前往【API Explorer】在线调试，API Explorer 提供在线调用 API、动态生成 SDK Example 代码和快速检索接口等能力，能显著降低使用云 API 的难度，强烈推荐使用。

请求参数

名称	类型	是否必选	示例值	描述
Action	String	是	DescribeAlarmEventDetail	系统规定参数。取值：DescribeAlarmEventDetail。
AlarmUniqueInfo	String	是	8df914418f4211fbf756efe7a6f40cbc	告警事件的唯一标识。
From	String	是	aqs	请求来源标识，固定为aqs。
Lang	String	否	zh	告警事件显示的语言类型。 • zh：中文 • cn：英文
SourceIp	String	否	1.1.1.1	请求源IP。

返回参数

名称	类型	示例值	描述
Data			告警事件详情。
└AlarmEventAliasName	String	进程异常行为-Linux计划任务执行异常指令	告警事件完整名称。
└AlarmEventDesc	String	黑客入侵服务器后，为了让恶意后门程序能持久化运行，黑客常常将恶意SHELL脚本写入crontab、systemd等计划任务。	告警事件描述。

名称	类型	示例值	描述
└AlarmUniqueInfo	String	8df914418f4211fbf756efe7a6f40cbc	告警事件的唯一标识。
└CanBeDealOnLine	Boolean	false	是否能在线处理（隔离）。
└CanCancelFault	Boolean	false	能否取消标记为误报。
└CauseDetails			告警事件发送的原因（溯源信息）。
└Key	String	item	文本展示的方式： • text：文本方式 • html：富文本方式
└Value			溯源信息字段值。
└Name	String	入侵原因	溯源信息字段的key。
└Type	String	text	溯源信息字段展示的类型。
└Value	String	黑客登录ECS后通过编辑文件方式 写WEBSHELL	溯源信息字段的值。
└DataSource	String	aegis_suspicious_event	数据来源。
└EndTime	Long	1542366542000	告警事件结束时间。
└HasTraceInfo	Boolean	true	告警事件是否有溯源数据。 • true：有溯源数据。 • false：没有溯源数据。
└InstanceName	String	测试服务器	关联实例的名称。
└InternetIp	String	42.121.1.1	关联实例的公网IP。
└IntranetIp	String	192.168.1.1	关联实例的私网IP。

名称	类型	示例值	描述
└Level	String	serious	告警事件的危险等级： • serious：紧急 • suspicious：可疑 • remind：提醒
└Solution	String	请及时排查告警中提示的恶意URL，以及所下载的目录下的恶意文件。并及时清理已运行的恶意进程。如果该指令是您自己主动执行，您可以在控制台点击标记为误报，并通过工单方式反馈给我们的安全工程师。	告警事件的处理方法。
└StartTime	Long	1542378601000	告警事件的开始时间。
└Type	String	异常网络连接	事件类型。
└Uuid	String	47900178-885d-4fa4-9d77-XXXXXXXXXXXX	关联实例的唯一标识。
RequestId	String	5A1DDB3C-798C-4A84-BF6E-3DC7F7D7EB4A	请求ID。

示例

请求示例

```
http(s)://[Endpoint]/?Action=DescribeAlarmEventDetail
&AlarmUniqueInfo=8df914418f4211fbf756efe7a6f40cbc
&From=aqs
&<公共请求参数>
```

正常返回示例

`XML` 格式

```
<DescribeAlarmEventDetailResponse>
 <Data>
  <Uuid>47900178-885d-4fa4-9d77-XXXXXXXXXXXX</Uuid>
  <AlarmEventAliasName>进程异常行为-Linux计划任务执行异常指令</AlarmEventAliasName>
  <Type>进程异常行为</Type>
  <InternetIp>10.1.1.1</InternetIp>
  <AlarmEventDesc>黑客入侵服务器后，为了让恶意后门程序能持久化运行，黑客常常将恶意SHELL脚本写入crontab、systemd等计划任务。</AlarmEventDesc>
  <IntranetIp>10.10.1.1</IntranetIp>
  <Level>serious</Level>
  <EndTime>1543741201000</EndTime>
  <StartTime>1543312803000</StartTime>
  <CanBeDealOnLine>false</CanBeDealOnLine>
  <InstanceName>server01</InstanceName>
 </Data>
 <RequestId>5A1DDB3C-798C-4A84-BF6E-3DC7F7DXXXXX</RequestId>
</DescribeAlarmEventDetailResponse>
```

JSON 格式

```
{
 "Data":{
 "Uuid":"47900178-885d-4fa4-9d77-XXXXXXXXXXXX",
 "AlarmEventDesc":"黑客入侵服务器后，为了让恶意后门程序能持久化运行，黑客常常将恶意SHELL脚本写入crontab、systemd等计划任务。",
 "AlarmEventAliasName":"进程异常行为-Linux计划任务执行异常指令",
 "Type":"进程异常行为",
 "IntranetIp":"10.10.1.1",
 "CauseDetails":[],
 "InternetIp":"10.1.1.1",
 "EndTime":1543741201000,
 "Level":"serious",
 "StartTime":1543312803000,
 "CanBeDealOnLine":false,
 "InstanceName":"server01"
 },
 "RequestId":"5A1DDB3C-798C-4A84-BF6E-3DC7F7D7EB4A"
}
```

错误码

查看本产品错误码