百度智能云

IDS 文档

目录

目录 2
功能发布记录 3
产品描述 3
- 产品概述 3
- 产品功能 3
- 产品优势 3
- 使用场景 4

产品定价 4
操作指南 5
- 开通流量审计服务 5
- 注册并开启流量审计 5
- 统计分析 5
- 入侵分析 6
- 配置 7

API参考 9
- 概述 9
- 通用说明 9
- API服务域名 11
- 公共请求头与响应头 11
- 错误码 12
- 入侵分析查询接口 14
- 统计分析查询接口 22
- 设置相关接口 32
- 附录1 37

常见问题 41
- 常见问题 41

功能发布记录

发布时间	功能概述
2018-07	• 新增统计分析Dashboard，可以查看成功入侵事件、攻击事件、流量使用、事件趋势、及TOP5攻击来源及类型分布 • 用户可以配置EIP授权用于对特定的EIP进行流量审计，每月免费的500G分析流量和后付费流量，都仅分析授权的EIP

产品描述

产品概述

基于全流量镜像及大数据处理技术，流量审计旁路分析用户授权后的流量 日志，快速识别web应用攻击，能够深度挖掘黑客针对Web的远程命令执行、webshell后门、敏感文件泄露等攻击事件并做出准确的报警；并保存原始web流量日志及审计报表，满足等保合规审计需求。

产品功能

安全威胁检测

在用户授权下，流量审计会实时分析用户EIP双向HTTP流量日志，快速识别SQL注入、XSS跨站脚本、webshell后门上传、非授权访问等各种常见web攻击。

成功入侵检测

在用户授权下，流量审计会实时分析用户EIP双向HTTP流量日志，快速识别SQL注入、XSS跨站脚本、webshell后门上传、非授权访问等各种常见web攻击。

原始日志存储

流量审计可以将用户的HTTP流量日志推送到用户自有的对象存储的BUCKET上，满足等保合规的需求，安全分析人员也可以基于自己的业务编写数据分析模型。

黑客入侵溯源

充分追溯黑客入侵的全过程，基于攻击入侵和被攻击资产，提供多维度关联报表展示，减少安全运维人员的阅读成本。

产品优势

双向流量，精准规则

基于百度长期安全经验累积的精准规则，完整还原用户访问的整个过程，双向分析HTTP请求与应答内容，力求精准检测，报警准确率达99.5%。

沙箱技术

在特殊的文件行为识别上采用杀箱技术，百度自研的PHP、JSP沙箱都已获得专利，可以在支持的沙箱中“引爆”文件，通过文件行为识别恶意攻击。

网络资产自识别

流量审计通过分析所有HTTP请求及响应的双向数据包，可以学习到客户的网络架构和资产列表，进一步分析是否存在由运维配置不当导致的弱点信息，如运维平台弱口令，管理平台对外等非漏洞问题导致安全威胁。

入侵事件关联分析

利用上下文关联检测引擎，关联同一黑客的同一次攻击行为，追溯黑客入侵的全过程，大大减少报警量，减少安全运维人员的困扰。

使用场景

安全态势感知

用户可以对云上资产安全有一个全面的了解，存证历史入侵事件并规避将来的攻击，保障云上数据信息安全性。

等保合规审计要求

信息安全等级保护条例中明确规定在网络边界处部署入侵防范手段，对网络中的安全事件信息进行记录和审计。

入侵发生后快速止损

用户接收到报警之后，登录控制台查看黑客的入侵过程及被攻击的资产，定位入侵事件，然后通过百度智能云提供的整体安全解决方案，如应急响应、WAF等，修复漏洞，快速止损。

定位黑客并提供追溯线索

不仅对黑客入侵行为进行识别，甚至可以追溯黑客入侵链路，看清黑客一步一步入侵的全过程，做到自动化的入侵取证。

产品定价

计费方式

- 按IDS实际分析流量计费方式，自然月累计阶梯计价。
- 付费方式：后付费。
- 账单周期：账单时间是北京时间整点，出账单时间是计费周期结束后1小时内。例如，10:00-11:00的账单会在12:00之前生成，具体以系统出账时间为准。

计费价格

IDS分析流量在不同的流量阶梯会有不同的单价，且按照分段阶梯累计计费，详情请见：IDS价格。

> **说明：** 分段阶梯为自然月计算，超过部分按照高阶梯的价格计算。

阶梯计费示例

如累计消耗流量为10300GB，则其中10240G属于0GB–10TB阶梯内，单价为0.95元/GB。剩下的60G在10TB-50TB阶梯内，则单价为0.91元/GB。则总账单金额为10240GBx0.95元/GB+60GBx0.91元/GB=9782.6元。

余额不足提醒和欠费处理

余额不足提醒

- 根据您最近3天的账单金额来判断您的账户余额（含可用代金券）是否足够支付未来3天的费用，若不足以支付，系统发送续费提醒。
- 根据您最近1天的账单金额来判断您的账户余额（含可用代金券）是否足以支付未来1天的费用，若不足以支付，系统发送续费提醒。

欠费处理

- 北京时间整点检查您的账户余额是否足以支付本次账单的费用（如北京时间11点整检查账户余额是否足以支付10点至11点的账单费用），若不足以支付，即为欠费，欠费时系统会发送欠费通知。
- 欠费后立即停止分析服务，系统会发送欠费停服通知，IDS分析服务停止，用户仍然可以享受下月提供的免费流量。

操作指南

开通流量审计服务

您可以登录百度智能云官网选择流量审计IDS，然后点击**立即申请**，完成流量审计服务使用申请表的填写，并在需求简述中，简单描写您的主要需求，我们会安排相关的人员跟进为您提供服务。

> **温馨提示：**
>
> 目前流量审计服务通过只有通过官网申请才能开通，如您未通过申请则无法使用该功能。
>
> 您在申请表中填写并提交的上述信息视为您同意百度智能云及百度智能云授权的合作伙伴通过电话方式联系您完善信息，以便能够为您提供更贴心的云服务。

注册并开启流量审计

在通过流量审计服务申请后，您需要创建一个百度智能云账号，请按照下述步骤进行注册、登录。

1. 注册并登录百度智能云平台，请参考注册和登录。
2. 如果未进行实名认证，请参考实名认证操作方法完成认证。
3. 登录成功后，导航栏选择“产品服务>流量审计>入侵分析”，在开启流量授权中，选择**授权并开通服务**后，完成流量审计功能的开启。

统计分析

统计分析

- 成功入侵事件：入侵事件中攻击结果为成功的事件个数。
- 攻击事件：入侵事件总数。
- 流量使用：显示每月使用IDS分析流量的情况，包括“今日使用量”、“本月使用量”、“免费流量剩余”。
- 事件趋势：显示“成功入侵事件”的趋势变化，和显示“攻击事件”的趋势变化。
- TOP5攻击来源：显示统计的近7天TOP5攻击来源的IP和攻击次数。
- TOP5受攻击资产：显示统计的近7天TOP5被攻击的资产和被攻击次数。每个资产包括EIP的IP。
- TOP5攻击类型分布：显示统计的近7天TOP5攻击类型的分布比例。

入侵分析

报表数据

报表中的数据含义如下所示：

- 时间段选择：您可以根据自身业务需求，选择想要查看报表的时间段。
- 攻击来源：显示您受到的攻击的来源ip。
- 被攻击资产：您受到攻击的EIP，并提示该EIP绑定的资源的类型及所在region。
- 被攻击域名：受到攻击的域名名称。
- 攻击类型：受到攻击的类型。
- 攻击次数：在聚合时间段内攻击来源攻击您的资源的合计次数。
- 攻击时间：某一个攻击来源攻击您的资源的具体时间。
- 攻击结果：根据HTTP双向流量，给出智能判断黑客入侵是否攻击成功。
- 溯源：点击“溯源”，详细查看所有攻击次数的攻击细节，可以让您了解本次攻击对您的业务造成了怎样的影响。

攻击视角

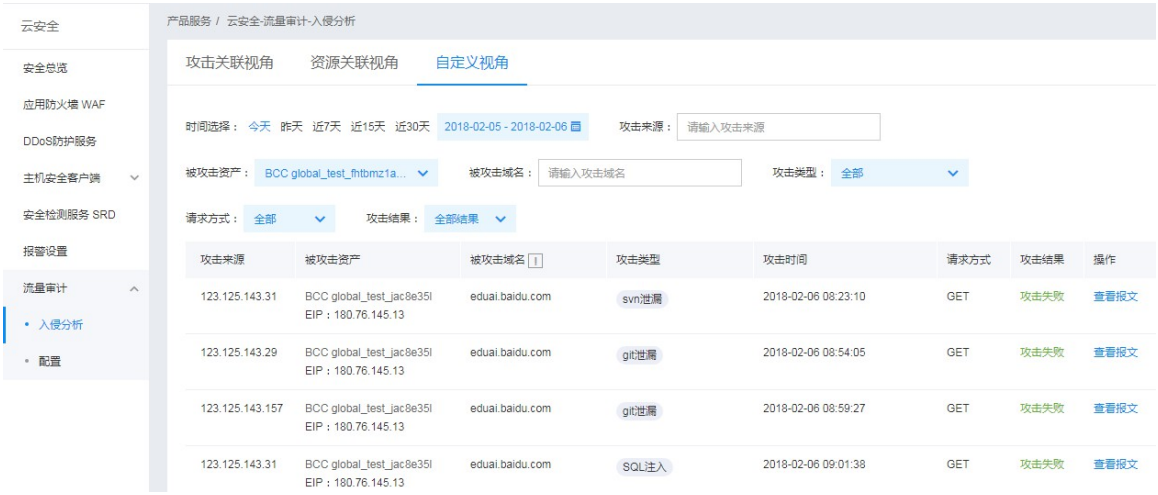
以攻击来源和时间段为维度进行聚合，主要是显示某一个攻击来源在选择时间段内如何攻击您的资源，具体如下图所示：

资源关联视角

以被攻击资产和时间来进行聚合；主要是显示您的某一个资源在选择时间段内受到了哪些攻击，具体如下图所示：

自定义视角

您可以根据个人需要进行报表自定义筛选，方便您快速的定位想要查看的结果，具体如下图所示：



配置

日志归档服务

简介

日志归档服务默认为关闭状态，若您有流量日志归档等合规需求，开启服务后，我们会将您的原始流量日志推送至您选择的bucekt，计费参照BOS计费规则，BOS存储可以保证您的日志永久性存储并方便你进行日志的管理、下载与分析。

操作步骤

1. 导航栏选择“产品服务>云安全>流量审计>配置”，并在配置页面选择**日志归档服务**。
2. 点击**编辑**按钮，在弹出的菜单栏中，选择**开启**日志归档服务，并选择日志存储的地址，点击**确定**完成日志归档服务的开通。如选择存储区域还未创建BOS bucket，则参考创建bucket完成创建。

> **注意：** 日志归档可以存储在多个区域，但每个区域仅支持一个bucket进行存储。

流量后付费

简介

流量后付费默认关闭状态，且我们每月会赠送500GB IDS入侵分析流量供您使用，若您需要更多的IDS入侵检测分析流量享受全量服务，请开通后付费服务。

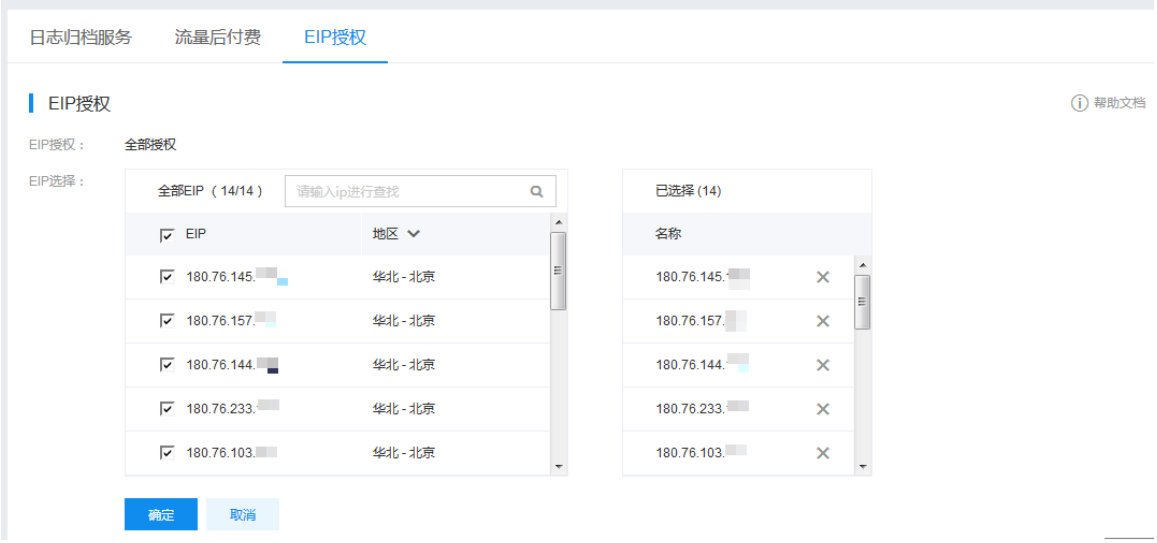
操作步骤

1. 导航栏选择“产品服务>云安全>流量审计>配置”，并在配置页面选择**流量后付费**。
2. 在后付费服务项目中，选择**ON**，开启流量后付费服务。

EIP授权

操作步骤

1. 导航栏选择“产品服务>云安全>流量审计>配置”，并在配置页面选择**EIP授权**。
2. 点击**编辑**按钮，在弹出的菜单栏中，EIP授权默认为全部授权，EIP选择支持部分选择。
3. 点击**确定**即时生效。



> **注意：** 每月免费的500G分析流量，和后付费流量，都仅分析授权的EIP。 用户之前开启了EIP，之后关闭，在统计分析和入侵分析中会保留统计，关闭后的EIP不会有新统计。

API参考

概述

流量审计IDS开放API依据开放云API设计规范进行设计，对外提供Restful API。

如果您是初次调用百度智能云产品的API，可以观看API入门视频指南，快速掌握调用API的方法。

IDS主要提供三类接口：

接口类型	接口描述
入侵分析查询接口	查询攻击记录信息，包括按攻击源查询攻击汇总记录、按被攻击资产查询攻击汇总记录、自定义查询攻击记录等接口
统计分析查询接口	查询攻击统计信息，包括查询top攻击资产、top攻击源等接口
设置相关接口	查询设置信息，包括查询后付费状态、查询日志服务状态、查询授权eip列表等接口，以及设置授权eip接口

通用说明

本产品是全局产品，域名为bss.bj.baidubce.com。

数据交换格式为JSON，所有request/response body内容均采用UTF-8编码。URL参数中所使用的IP均使用点分十进制表示。

实名认证

使用IDS API的用户需要实名认证，没有通过实名认证的可以前往百度开放云官网控制台中的安全认证下的实名认证中进行认证。没有通过实名认证的用户请求将会得到一下错误提示码：

错误码	错误描述	HTTP状态码	中文解释
QualifyNotPass	The User has not pass qualify.	403	账号没有通过实名认证

API认证机制

所有API的安全认证一律采用Access Key与请求签名机制。 Access Key由Access Key ID和Secret Access Key组成，均为字符

串。 对于每个HTTP请求，使用下面所描述的算法生成一个认证字符串。提交认证字符串放在Authorization头域里。服务端根据生成算法验证认证字符串的正确性。 认证字符串的格式为`bce-auth-v{version}/{accessKeyId}/{timestamp}/{expirationPeriodInSeconds}/{signedHeaders}/{signature}`。

- version是正整数。
- timestamp是生成签名时的UTC时间。
- expirationPeriodInSeconds表示签名有效期限。
- signedHeaders是签名算法中涉及到的头域列表。头域名之间用分号（;）分隔，如host;x-bce-date。列表按照字典序排列。（本API签名仅使用host和x-bce-date两个header）
- signature是256位签名的十六进制表示，由64个小写字母组成。

当百度智能云接收到用户的请求后，系统将使用相同的SK和同样的认证机制生成认证字符串，并与用户请求中包含的认证字符串进行比对。如果认证字符串相同，系统认为用户拥有指定的操作权限，并执行相关操作；如果认证字符串不同，系统将忽略该操作并返回错误码。

鉴权认证机制的详细内容请参见鉴权认证机制。

通信协议

IDS API目前仅支持HTTP调用方式，不支持HTTPS调用。

请求结构说明

请求参数包括如下4种：

参数类型	说明
URI	通常用于指明操作实体,如:GET /v2/securityAudit/postpayStatus
Query参数	URL中携带的请求参数
HEADER	通过HTTP头域传入,如:x-bce-date
RequestBody	通过JSON格式组织的请求数据体

响应结构说明

返回值分为两种形式：

返回内容	说明
HTTP STATUS CODE	如200,400,403,404等
ResponseBody	JSON格式组织的响应数据体

API版本号

参数	类型	参数位置	描述	是否必须
version	String	URL参数	API版本号，当前值为2。	是

幂等性

当调用创建接口时如果遇到了请求超时或服务器内部错误，用户可能会尝试重发请求，这时用户通过clientToken参数避免创建出比预期要多的资源，即保证请求的幂等性。

幂等性基于clientToken，clientToken是一个长度不超过64位的ASCII字符串，通常放在query string里，如`http://bcc.bj.baidubce.com/v1/instance?clientToken=be31b98c-5e41-4838-9830-9be700de5a20`。

如果用户使用同一个clientToken值调用创建接口，则服务端会返回相同的请求结果。因此用户在遇到错误进行重试的时候，可

以通过提供相同的clientToken值，来确保只创建一个资源；如果用户提供了一个已经使用过的clientToken，但其他请求参数（包括queryString和requestBody）不同甚至url Path不同，则会返回IdempotentParameterMismatch的错误代码。

clientToken的有效期为24小时，以服务端最后一次收到该clientToken为准。也就是说，如果客户端不断发送同一个clientToken，那么该clientToken将长期有效。

密码加密传输规范

所有涉及密码的接口参数都需要加密，禁止明文传输。密码一律采用AES 128位加密算法进行加密，用SK的前16位作为密钥，加密后生成的二进制字节流需要转成十六进制，并以字符串的形式传到服务端。具体步骤如下：

- byte[] bCiphertext= AES(明文,SK)
- String strHex = HexStr(bCiphertext)

日期与时间规范

日期与时间的表示有多种方式。为统一起见，除非是约定俗成或者有相应规范的，凡需要日期时间表示的地方一律采用UTC时间，遵循ISO 8601，并做以下约束：

1. 表示日期一律采用YYYY-MM-DD方式，例如2014-06-01表示2014年6月1日
2. 表示时间一律采用hh:mm:ss方式，并在最后加一个大写字母Z表示UTC时间。例如23:00:10Z表示UTC时间23点0分10秒。
3. 凡涉及日期和时间合并表示时，在两者中间加大写字母T，例如2014-06-01T23:00:10Z表示UTC时间2014年6月1日23点0分10秒。

规范化字符串

通常一个字符串中可以包含任何Unicode字符。在编程中这种灵活性会带来不少困扰。因此引入“规范字符串”的概念。一个规范字符串只包含百分号编码字符以及URI（Uniform Resource Identifier）非保留字符（Unreserved Characters）。

RFC 3986规定URI非保留字符包括以下字符：字母（A-Z，a-z）、数字（0-9）、连字号（-）、点号（.）、下划线（_）、波浪线（~）。

将任意一个字符串转换为规范字符串的方式是:

- 将字符串转换成UTF-8编码的字节流。
- 保留所有URI非保留字符原样不变。
- 对其余字节做一次RFC 3986中规定的百分号编码（Percent-Encoding），即一个%后面跟着两个表示该字节值的十六进制字母。字母一律采用大写形式。

示例：

原字符串：`this is an example for 测试`，对应的规范字符串：`this%20is%20an%20example%20for%20%E6%B5%8B%E8%AF%95`。

API服务域名

IDS为全局服务，服务域名为

Region	Endpoint	Protocol
全局	bss.bj.baidubce.com	HTTP

公共请求头与响应头

公共请求头

下表列出了所有SecurityAudit API所携带的公共头域。HTTP协议的标准头域不在此处列出

头域（HEADER）	是否必须	说明
Authorization	是	包含Access Key与请求签名
Content-Type	是	application/json; charset=utf-8
x-bce-date	否	表示日期的字符串，符合日期格式规范
Host	是	表示请求API的域名

公共响应头

下表列出了所有SecurityAudit API的公共响应头域。HTTP协议的标准响应头域不在此处列出

头域（HEADER）	说明
Content-Type	只支持JSON格式，application/json; charset=utf-8
x-bce-request-id	后端生成，并自动设置到响应头域中

错误码

当用户访问API出现错误时，会返回给用户相应的错误码和错误信息，便于定位问题，并做出适当的处理。请求发生错误时通过Response Body返回详细错误信息，遵循如下格式：

参数名	类型	说明
code	String	错误码
message	String	错误描述
requestId	String	本次请求的requestId

示例：

```
 {
 "requestId" : "ae2225f7-1c2e-427a-a1ad-5413b762957d",
 "code" : "NoSuchKey",
 "message" : "The resource you requested does not exist"
}
```

BCE公共错误码

错误返回码	错误消息	状态码	说明
AccessDenied	Access denied.	403Forbidden	无权限访问对应的资源。
InappropriateJSON	The JSON you provided was well-formed and valid, but not appropriate forthis operation.	400 Bad Request	请求中的JSON格式正确，但语义上不符合要求。如缺少某个必需项，或值类型不匹配等。出于兼容性考虑，对于所有无法识别的项应直接忽略，不应该返回这个错误。
InternalError	We encountered an internal error Please try again.	500 Internal Server Error	所有未定义的其他错误。在有明确对应的其他类型的错误时（包括通用的和服务自定义的）不应该使用。
InvalidAccessKeyId	The Access Key ID you provided doesnot exist in our records.	403Forbidden	Access Key ID不存在。

d			
InvalidHTTPAuthHeader	The Access Key ID you provided does notexist in our records.	400 BadRequest	Authorization头域格式错误。
InvalidHTTPRequest	There was an error in the body of your HTTP request.	400 Bad Request	HTTP body格式错误。例如不符合指定的Encoding等。
InvalidURI	Could not parse the specified URI.	400 Bad Request	URI形式不正确。例如一些服务定义的关键词不匹配等。对于ID不匹配的问题，应定义更加具体的错误码，如NoSuchKey。
MalformedJSON	The JSON you provided was not well-formed.	400 BadRequest	JSON格式不合法。
InvalidVersion	The API version specified was invalid.	404 NotFound	URI的版本号不合法。
OptInRequired	A subscription for the service is required.	403Forbidden	没有开通对应的服务。
PreconditionFailed	The specified If-Match header doesn’tmatch the ETag header.	412PreconditionFailed	详见Etag。
RequestExpired	Request has expired. Timestamp date is <Data>.	400 BadRequest	请求超时。要改成x-bce-date。若请求中只有Date，需将Date转成datetime。
IdempotentParameterMismatch	The request uses the same client token asa previous, but non-identical request.	403Forbidden	clientToken对应的API参数不一样。
SignatureDoesNotMatch	The request signature we calculated does not match the signature you provided. Check yourSecret Access Key and signing method. Consultthe service documentation for details.	400 Bad Request	Authorization头域中附带的签名和服务端验证不一致。

IDS业务错误码

错误码	错误描述	HTTP状态码	语义
OperateIdsAuthDenied	No operate ids auth permission	403	无开通IDS服务权限
IdsReadDenied	No ids read permission	403	无IDS读权限
IdsAdminDenied	No ids admin permission	403	无IDS管理权限
ReadEipListDenied	No read eip list permission	403	无eip查看权限
IdsReadEipListDenied	No read ids eip list permission	403	无IDS查看eip权限
OperateEipListDenied	No operate eip list permission	403	无eip操作权限
IdsOperateEipListDenied	No operate ids eip list permission	403	无IDS操作eip权限
EipNotFound	eip not found	404	eip未找到
IdsAuthRegionNotFound	auth region not found	404	IDS授权区域未找到

入侵分析查询接口

查询攻击源汇总记录接口

描述

- 可以指定startTime, endTime, attackResult, pageNo, pageSize查询攻击源汇总记录接口
- 查询时间限制：endTime - startTime <= 31天

请求结构

```
POST /v{version}/securityAudit/getAttackSource&clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
startTime	String	是	RequestBody参数	开始时间，UTC标准时间格式
endTime	String	是	RequestBody参数	结束时间，UTC标准时间格式
attackResult	int	是	RequestBody参数	要查询的攻击结果，0表示失败，1表示成功，2表示全部
pageNo	int	是	RequestBody参数	查询的页号
pageSize	int	是	RequestBody参数	查询的页大小
clientToken	String	是	Query参数	幂等性Token，详见clientToken

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
status	int	结果状态码
description	String	结果描述
totalpage	int	总共页数
data	list<AttackSourceSummaryModel>	按攻击源汇总列表

请求示例

```
 POST /v2/securityAudit/getAttackSource&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02

{
    "startTime": "2017-12-01T08:00:02Z",
    "endTime": "2017-12-02T08:00:02Z",
    "attackResult": 1,
    "pageSize": 10,
    "pageNo": 1,
}
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
   "status": 0,
   "description": "ok",
   "totalpage": 5,
   "data": [
      {
         "attackSource": "1.2.3.4",
         "attackSourceType": "",
         "eipList": [
                  {
                     "instanceType": "BCC",
                     "name": "eip-name",
                     "eip": "180.76.1.1",
                     "region": "bj",
                  },
                  ...
         ]
         "domainList": ["www.a.com", "www.b.com", ...],
         "attackTypeList": ["SQL注入", "敏感文件访问", ...],
         "attackCount": 100,
         "startTime": "2017-12-01T09:00:02Z",
         "endTime":   "2017-12-01T15:00:02Z",
         "attackResult": 1
      } ,
      {
      ...
      }
      ...
   ]
}
```

查询被攻击资产汇总记录接口

描述

- 可以指定startTime, endTime, attackResult, pageNo, pageSize查询攻击资产汇总记录接口
- 查询时间限制：endTime - startTime <= 31天

请求结构

```
 POST /v{version}/securityAudit/getAttackTarget&clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
startTime	String	是	RequestBody参数	开始时间，UTC标准时间格式
endTime	String	是	RequestBody参数	结束时间，UTC标准时间格式
attackResult	int	是	RequestBody参数	要查询的攻击结果，0表示失败，1表示成功，2表示全部
pageNo	int	是	RequestBody参数	查询的页号
pageSize	int	是	RequestBody参数	查询的页大小
clientToken	String	是	Query参数	幂等性Token，详见clientToken

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
status	int	结果状态码
description	String	结果描述
totalpage	int	总共页数
data	list<AttackTargetSummaryModel>	按攻击源汇总列表

请求示例

```
 POST /v2/securityAudit/getAttackTarget&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02

{
    "startTime": "2017-12-01T08:00:02Z",
    "endTime": "2017-12-02T08:00:02Z",
    "attackResult": 1,
    "pageSize": 10,
    "pageNo": 1,
}
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
   "status": 0,
   "description": "ok",
   "totalpage": 5,
   "data": [
      {
         "eipInfo":
            {
               "instanceType": "BCC",
               "name": "eip-name",
               "eip": "180.76.1.1",
               "region": "bj",
            },
         "attackSourceList": [
            {
               "attackSource": "1.1.1.1",
               "attackSourceType": ""
            },
            {
               "attackSource":"1.1.1.2",
               "attackSourceType": "CDN"
            },
             ...
         ],
         "domainList": ["www.a.com", "www.b.com", ...],
         "attackTypeList": ["SQL注入", "敏感文件访问", ...],
         "attackCount": 100,
         "startTime": "2017-12-01T09:00:02Z",
         "endTime":   "2017-12-01T15:00:02Z",
         "attackResult": 1
      } ,
      {
      ...
      }
      ...
   ]
}
```

自定义查询攻击记录接口

描述

- 必须指定startTime, endTime, attackResult, pageNo, pageSize自定义查询攻击记录接口
- 可选指定attackSource, eipList, domain, attackTypeKey, request查询条件
- 查询时间限制：endTime - startTime <= 31天

请求结构

```
 POST /v{version}/securityAudit/getCustomAttack&clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
startTime	String	是	RequestBody参数	开始时间，UTC标准时间格式
endTime	String	是	RequestBody参数	结束时间，UTC标准时间格式
attackResult	int	是	RequestBody参数	要查询的攻击结果，0表示失败，1表示成功，2表示全部
pageNo	int	是	RequestBody参数	查询的页号
pageSize	int	是	RequestBody参数	查询的页大小
attackSource	String	否	RequestBody参数	攻击源
eipList	list	否	RequestBody参数	被攻击eip列表
domain	String	否	RequestBody参数	被攻击域名
attackTypeKey	String	否	RequestBody参数	攻击类型key
request	String	否	RequestBody参数	请求方法
clientToken	String	是	Query参数	幂等性Token，详见clientToken

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
status	int	结果状态码
description	String	结果描述
totalpage	int	总共页数
data	list<AttackRecordModel>	按攻击源汇总列表

请求示例

```
 POST /v2/securityAudit/getCustomAttack&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-
date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02

{
    "startTime": "2017-12-01T08:00:02Z",
    "endTime": "2017-12-02T08:00:02Z",
    "attackResult": 1,
    "pageSize": 10,
    "pageNo": 1,


    "attackSource": "1.1.1.1",
    "eipList": ["180.76.1.1", "182.61.1.1",...]
    "domain": "www.a.com",
    "attackTypeKey": "30003",
    "request": "GET",
}
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
    "status": 0,
    "description": "ok",
    "totalpage": 5,
    "data": [
       {
          "attackSource":"1.2.3.4",
          "attackSourceType": "",
          "eipInfo":
             {
                "instanceType": "BCC",
                "name": "eip-name",
                "eip": "180.76.1.1",
                "region": "bj",
             },
          "domain": "www.a.com",
          "attackType": "SQL注入",
          "attackCount": 100,
          "attackTime": "2017-12-01T09:00:02Z",
          "request": "GET",
          "attackResult": 1,
          "headers": {
             "content-length": "1504",
             "accept-language": "zh-cn",
             "connection": "Keep-Alive",
             "accept": "*/*",
             "user-agent": "Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)",
             "host": "tingwen.me",
             "referer": "http://tingwen.me/1.php",
             "content-type": "application/x-www-form-urlencoded"
          },
          "body": "sqzr=@eval(get_magic_quotes_gpc()?stripslashes($_POST[chr(122)",
```

```
            "resheaders": {
                "x-powered-by": "PHP/5.6.15",
                "transfer-encoding": "chunked",
                "set-cookie": "HBJnSD_think_language=zh-cn; expires=Sat, 21-Oct-2017 13:03:27",
                "expires": "Thu, 19 Nov 1981 08:52:00 GMT",
                "vary": "Accept-Encoding",
                "server": "nginx-upupw/1.8.0",
                "connection": "keep-alive",
                "pragma": "no-cache",
                "cache-control": "no-store, no-cache, must-revalidate, post-check=0, pre-check=0",
                "date": "Sat, 21 Oct 2017 12:03:27 GMT",
                "content-type": "text/html; charset=UTF-8"
            },
            "resbody": "4e8\r\n<!DOCTYPE html PUBLIC-//W3C//DTD XHTML 1.0 Transitional//EN",
        },
        {
        ...
        }
        ...
    ]
}
```


获取下拉框信息接口

描述

- 包括eip列表，攻击类型列表，攻击请求方法列表

请求结构

```
 GET /v{version}/securityAudit/getDropdownList&clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
clientToken	String	是	Query参数	幂等性Token，详见clientToken

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
status	int	结果状态码
description	String	结果描述
data	DropdownModel	下拉列表描述

请求示例

```
 GET /v2/securityAudit/getDropdownList&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

  {
  "status": 0,
  "description": "ok",
  "data": {
    "eipList": [
      {
        "instanceType": "BCC",
        "name": "eip-name",
        "eip": "180.76.1.1",
        "region": "bj",
      },
      ...
    ],
    "attackResult": {
      0: "攻击失败",
      1: "攻击成功",
      2: "所有"
    },
    "attackType": {
      10004: "敏感文件访问",
      30003: "SQL注入",
      ...
    }
    "request": {
      "POST": "POST",
      "GET": "GET",
      "HEAD": "HEAD",
      ...
    }
  }
}
```

统计分析查询接口

查询最近攻击次数接口

描述

- 查询最近估计次数

请求结构

```
GET /v{version}/securityAudit/getRecentAttackNum&clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
clientToken	String	是	Query参数	幂等性Token，详见clientToken

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
status	int	结果状态码
description	String	结果描述
data	RecentAttackInfoModel	最近攻击信息描述

请求示例

```
GET /v2/securityAudit/getRecentAttackNum&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
    "status": 0,
    "description": "ok",
    "data": {
        "recentDayAttackInfo": {
            "attackSuccess": 2,
            "attackAll": 100
        }
        "lastDayAttackInfo": {
            "attackSuccess": 2,
            "attackAll": 100
        }
    }
}
```

查询指定时间段内攻击次数接口

描述

- 指定startTime, endTime 查询攻击次数
- 查询时间限制：endTime - startTime <= 31天

请求结构

```
 POST /v{version}/securityAudit/getAttackStat&clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string

{
    "startTime": "2018-04-01T08:00:00Z",
    "endTime": "2018-04-02T08:00:00Z",
}
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
clientToken	String	是	Query参数	幂等性Token，详见clientToken
startTime	String	是	RequestBody	开始时间，UTC标准时间格式
endTime	String	是	RequestBody	结束时间，UTC标准时间格式

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
status	int	结果状态码
description	String	结果描述
data	AttackInfoModel	攻击次数描述

请求示例

```
 POST /v2/securityAudit/getAttackStat&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02

{
    "startTime": "2018-04-01T08:00:00Z",
    "endTime": "2018-04-02T08:00:00Z",
}
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
    "status": 0,
    "description": "ok",
    "data": {
        "attackSuccess": 2,
        "attackAll": 100
    }
}
```

查询攻击事件趋势接口

描述

- 指定最近的天数，查询攻击事件趋势

请求结构

```
 POST /v{version}/securityAudit/getAttackTrend&clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string

{
    "cycleDay": 7
}
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
clientToken	String	是	Query参数	幂等性Token，详见clientToken
cycleDay	int	是	RequestBody	最近的天数，设置范围：[1,31]

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
status	int	结果状态码
description	String	结果描述
data	list<[DayAttackInfoModel]>(#DayAttackInfoModel)	每天攻击次数列表

请求示例

```
 POST /v2/securityAudit/getAttackTrend&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02

{
   "cycleDay": 7
}
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
   "status": 0,
   "description": "ok",
   "data": [
      {
         "attackDate": "2018-04-01",
         "attackSuccess": 2,
         "attackAll": 100
      }
      {

         "attackDate": "2018-04-02",
         "attackSuccess": 5,
         "attackAll": 200
      }
      ...
   ]
}
```

查询top攻击源IP接口

描述

- 指定查询的天数和topN，查询top攻击源IP

请求结构

```
 POST /v{version}/securityAudit/getTopAttackSource&clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string

{
   "cycleDay": 7
   "topN": 5,
}
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
clientToken	String	是	Query参数	幂等性Token，详见clientToken
cycleDay	int	是	RequestBody	最近的天数，设置范围：[1,31]
topN	int	是	RequestBody	查询的前几个攻击源IP，设置范围：[1,10]

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
status	int	结果状态码
description	String	结果描述
data	list<[AttackSourceInfoModel]>(#AttackSourceInfoModel)	攻击源列表

请求示例

```
 POST /v2/securityAudit/getTopAttackSource&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02

{
   "cycleDay": 7
   "topN": 5,
}
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
   "status": 0,
   "description": "ok",
   "data": [
      {
         "attackSource": 1.1.1.1",
         "attackSuccess": 50,
      }
      {
         "attackSource": 2.2.2.2",
         "attackSuccess": 40,
      }
      ...
   ]
}
```

查询top被攻击eip接口

描述

- 指定查询的天数和topN，查询top被攻击eip

请求结构

```
 POST /v{version}/securityAudit/getTopAttackTarget&clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string

{
    "cycleDay": 7
    "topN": 5,
}
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
clientToken	String	是	Query参数	幂等性Token，详见clientToken
cycleDay	int	是	RequestBody	最近的天数，设置范围：[1,31]
topN	int	是	RequestBody	查询的前几个被攻击eip，设置范围：[1,10]

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
status	int	结果状态码
description	String	结果描述
data	list<[AttackedEipInfoModel]>(#AttackedEipInfoModel)	被攻击eip列表

请求示例

```
 POST /v2/securityAudit/getTopAttackTarget&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-
date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02

{
    "cycleDay": 7
    "topN": 5,
}
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
   "status": 0,
   "description": "ok",
   "data": [
      {
         "eip": "180.76.1.1",
         "instanceType": "BCC",
         "name": "eip-name",
         "region": "bj",
         "attackSuccess": 50,
      },
      {
         "eip": "180.76.1.2",
         "instanceType": "BCC",
         "name": "eip-name",
         "region": "bj",
         "attackSuccess": 40,

      },
      ...
   ]
}
```

查询top攻击类型

描述

- 指定查询的天数和topN，查询top攻击类型

请求结构

```
 POST /v{version}/securityAudit/getTopAttackType&clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string

{
   "cycleDay": 7
   "topN": 5,
}
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
clientToken	String	是	Query参数	幂等性Token，详见clientToken
cycleDay	int	是	RequestBody	最近的天数，设置范围：[1,31]
topN	int	是	RequestBody	查询的前几个攻击类型，设置范围：[1,10]

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
status	int	结果状态码
description	String	结果描述
data	list<[AttackTypeInfoModel]>(#AttackTypeInfoModel)	攻击类型列表

请求示例

```
 POST /v2/securityAudit/getTopAttackType&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02

{
    "cycleDay": 7
    "topN": 5,
}
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
   "status": 0,
   "description": "ok",
   "data": [
      {
         "attackType": "SQL注入" ,
         "attackSuccess": 50,
      },
      {
         "attackType": "webShell" ,
         "attackSuccess": 30,

      },
      ...
      {
         "attackType": "others" ,
         "attackSuccess": 10,

      },
   ]
}
```

设置相关接口

查询后付费开关接口

描述

- 查询后付费开关

请求结构

```
 GET /v{version}/securityAudit/postpayStatus&clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
clientToken	String	是	Query参数	幂等性Token，详见clientToken

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
accountId	String	用户id
postpayStatus	PostpayStatus	后付费状态

请求示例

```
 GET /v2/securityAudit/postpayStatus&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
   "accountId": "111",
   "postpayStatus": 1,
}
```

查询日志服务配置接口

描述

- 查询日志服务配置

请求结构

```
 GET /v{version}/securityAudit/logService&clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
clientToken	String	是	Query参数	幂等性Token，详见clientToken

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
accountId	String	用户id
logServiceStatus	LogServiceStatus	日志服务状态
bucket	BucketModel	bucket配置信息

请求示例

```
 GET /v2/securityAudit/logService&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
    "accountId": "111",
    "logServiceStatus": 1,
    "bucket": {
        "bj": "bucket1",
        "gz": "bucket2",
        "su": "bucket3",
    }
}
```

查询授权eip配置接口

描述

- 查询授权eip

请求结构

```
 GET /v{version}/securityAudit/authEipList&clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
clientToken	String	是	Query参数	幂等性Token，详见clientToken

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

参数名称	类型	描述
accountId	String	用户id
authAllEip	AuthAllEipStatus	是否授权全部eip
eipDict	EipDictModel	eip配置列表

请求示例

```
 GET /v2/securityAudit/authEipList&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02
```

响应示例

```
 HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS

{
    "authAllEip": 0,
    "eipDict": {
        "bj": ["180.76.1.1", ...],
        "gz": ["182.61.1.1", ...],
        "su": ["106.12.1.1", ...],
    },
}
```

设置授权eip接口

描述

- 设置授权eip

请求结构

```
 PUT /v{version}/securityAudit/authEipList&clientToken={clientToken} HTTP/1.1
Host: bss.bj.baidubce.com
Authorization: authorization string

{
    "authAllEip": 0,
    "eipDict": {
        "bj": ["180.76.1.1", ...],
        "gz": ["182.61.1.1", ...],
        "su": ["106.12.1.1", ...],
    },
}
```

请求头域

除公共头域外，无其他特殊头域

请求参数

参数名称	类型	是否必需	参数位置	描述
version	String	是	URL参数	API版本号，当前取值2
clientToken	String	是	Query参数	幂等性Token，详见clientToken
authAllEip	AuthAllEipStatus	是	RequestBody	是否授权全部eip
eipDict	EipDictModel	是	RequestBody	eip配置列表

返回状态码

成功返回200，失败返回见错误码

返回头域

除公共头域外，无其他特殊头域

返回参数

无特殊返回参数

请求示例

```
 PUT /v2/securityAudit/authEipList&clientToken=be31b98c-5e41-4838-9830-9be700de5a20 HTTP/1.1
HOST bss.bj.baidubce.com
Authorization bce-auth-v1/5e5a8adf11ae475ba95f1bd38228b44f/2016-04-10T08:26:52Z/1800/host;x-bce-
date/ec3c0069f9abb1e247773a62707224124b2b31b4c171133677f9042969791f02

{
    "authAllEip": 0,
    "eipDict": {
        "bj": ["180.76.1.1", ...],
        "gz": ["182.61.1.1", ...],
        "su": ["106.12.1.1", ...],
    },
}
```

响应示例

```
HTTP/1.1 200 OK
x-bce-request-id: 946002ee-cb4f-4aad-b686-5be55df27f09
Date: Wed, 10 Apr 2016 08:26:52 GMT
Transfer-Encoding: chunked
Content-Type: application/json;charset=UTF-8
Server: BWS
```

附录1

Model对象定义

AttackSourceSummaryModel

参数名称	类型	描述
attackSource	String	攻击源
attackSourceType	String	攻击源类型，空表示一般源IP, "CDN":表示真实源IP最后经CDN IP代理到达服务端, "高防":表示真实源IP最后经高防IP到达服务端
eipList	list<EipModel>	被攻击的eip列表
domainList	list	被攻击域名墙列表
attackTypeList	list	攻击类型列表
attackCount	int	攻击次数
startTime	String	攻击开始时间，UTC标准时间格式
endTime	String	攻击结束时间，UTC标准时间格式
attackResult	int	攻击结果

AttackTargetSummaryModel

参数名称	类型	描述
eipInfo	EipModel	被攻击eip描述
attackSourceList	list<AttackSourceModel>	攻击源列表
domainList	list	被攻击域名墙列表
attackTypeList	list	攻击类型列表
attackCount	int	攻击次数
startTime	String	攻击开始时间，UTC标准时间格式
endTime	String	攻击结束时间，UTC标准时间格式
attackResult	int	攻击结果

AttackRecordModel

参数名称	类型	描述
attackSource	String	攻击源
attackSourceType	String	攻击源类型，空表示一般源IP，"CDN":表示真实源IP最后经CDN IP代理到达服务端，"高防":表示真实源IP最后经高防IP到达服务端
eipInfo	EipModel	被攻击eip描述
domain	String	被攻击域名
attackType	String	攻击类型描述
attackCount	int	攻击次数
attackTime	String	攻击开始时间，UTC标准时间格式
request	String	攻击请求方法
attackResult	int	攻击结果
headers	RequestHeaderModel	请求头描述
body	String	请求体
resheaders	ResponseHeaderModel	响应头描述
resbody	String	响应体

AttackSourceModel

参数名称	类型	描述
attackSource	String	攻击源
attackSourceType	String	攻击源类型，空表示一般源IP，"CDN":表示真实源IP最后经CDN IP代理到达服务端，"高防":表示真实源IP最后经高防IP到达服务端

RequestHeaderModel

参数名称	类型	描述
content-length	String	实体长度
accept-language	String	可接受的语言
connection	String	连接状态
accept	String	可接受的文档类型
user-agent	String	客户端版本
host	String	请求的域名
referer	String	referer
content-type	String	实体类型

ResponeHeaderModel

参数名称	类型	描述
x-powered-by	String	服务端语言版本
transfer-encoding	String	传输编码格式
set-cookie	String	cookie
expires	String	超时
vary	String	vary
server	String	服务端版本
connection	String	链接状态
pragma	String	pragma
cache-control	String	cash设置
date	String	日期
content-type	String	文档类型及编码类型

DropdownModel

参数名称	类型	描述
eipList	list<EipModel>	eip列表
attackResult	attackResultModel	攻击结果描述
attackType	attackTypeModel	攻击类型描述
request	requestModel	请求方式

EipModel

参数名称	类型	描述
eip	String	eip
instanceType	String	绑定的实例类型
name	String	实例名字
region	region	eip所属区域

AttackedEipInfoModel

参数名称	类型	描述
eip	String	eip
instanceType	String	绑定的实例类型
name	String	实例名字
region	region	eip所属区域
attackSuccess	int	攻击成功次数

EipDictModel

参数名称	类型	描述
bj	list	北京的eip列表
gz	list	广州的eip列表
su	list	苏州的eip列表

attackResultModel

参数名称	类型	描述
0	String	攻击失败
1	String	攻击成功
2	String	所有

attackTypeModel

参数名称	类型	描述
10004	String	敏感文件访问
30003	String	SQL注入
..	..	..

requestModel

参数名称	类型	描述
POST	String	POST
GET	String	GET
..	..	..

BucketModel

参数名称	类型	描述
bj	String	北京bucket，NoSuchBucket表示bucket不存在，AccessDenied表示无权访问bucket
gz	String	广州bucket，NoSuchBucket表示bucket不存在，AccessDenied表示无权访问bucket
su	String	苏州bucket，NoSuchBucket表示bucket不存在，AccessDenied表示无权访问bucket

RecentAttackInfoModel

参数名称	类型	描述
recentDayAttackInfo	AttackInfoModel	最近24小时攻击信息
lastDayAttackInfo	AttackInfoModel	上一个24小时攻击信息

AttackInfoModel

参数名称	类型	描述
attackSuccess	int	攻击成功次数
attackAll	int	攻击总次数

DayAttackInfoModel

参数名称	类型	描述
attackDate	String	日期
attackSuccess	int	攻击成功次数
attackAll	int	攻击总次数

AttackSourceInfoModel

参数名称	类型	描述
attackSource	String	攻击源
attackSuccess	int	攻击成功次数

AttackTypeInfoModel

参数名称	类型	描述
attackType	String	攻击类型
attackSuccess	int	攻击成功次数

区域编码定义

region

区域	描述
bj	公有云-北京
gz	公有云-广州
su	公有云-苏州
hk02	公有云-香港二区
hkg	公有云-香港三区
fsh	公有云-上海

状态定义

PostpayStatus

状态	描述
-1	从未开启后付费
0	后付费关闭
1	后付费开启

LogServiceStatus

状态	描述
0	日志服务关闭
1	日志服务开启

AuthAllEipStatus

状态	描述
0	部分ip授权
1	全部ip授权

常见问题

常见问题

黑客入侵成功，产生报警怎么办？

- 可以使用主机安全客户端“网站后门隔离”功能，清除已经上传到服务器内部的恶意后门。 前往 主机安全客户端 配置。

- 强烈推荐开启BLB WAF & CDN WAF，实时拦截web攻击。 前往 应用防火墙WAF 配置。
- 封禁恶意攻击来源IP。

> **注意：** 攻击IP可能为代理节点，封禁将导致该代理的所有正常流量无法访问，封禁需谨慎。

源站前封禁操作见 应用防火墙服务 WAF－自定义规则配置。

CDN节点封禁操作见 内容分发网络 CDN－IP黑名单。

如何获取超过60天的攻击分析日志？

- 流量审计IDS默认在控制台中可查询时的攻击分析日志为60天。60至180天的攻击分析日志进行了归档处理，如果需要提取您的攻击分析日志，可以提交工单进行申请。